2016

GRAPHICAL ONE-TIME PASSWORD AUTHENTICATION

Alsaiari, Hussain

INFOSECURITY
WITH
PLYMOUTH
UNIVERSITY

GRAPHICAL ONE-TIME PASSWORD

AUTHENTICATION

HUSSAIN S. ALSAIARI

Ph.D. 2016

COPYRIGHT STATEMENT

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior consent.

GRAPHICAL ONE-TIME PASSWORD AUTHENTICATION

By

HUSSAIN S. ALSAIARI

A thesis submitted to the Plymouth University
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics
Faculty of Science and Engineering

May 2016

Abstract

Graphical One-Time Password Authentication

HUSSAIN S. ALSAIARI (MSc)

Complying with a security policy often requires users to create long and complex passwords to protect their accounts. However, remembering such passwords appears difficult for many and may lead to insecure practices, such as choosing weak passwords or writing them down. One-Time Passwords (OTPs) aim to overcome such problems; however, most implemented OTP techniques require special hardware, which not only adds costs, but also raises issues regarding availability. This type of authentication mechanism is mostly adopted by online banking systems to secure their clients' accounts. However, carrying around authentication tokens was found to be an inconvenient experience for many customers. Not only the inconvenience, but if the token was unavailable, for any reason, this would prevent customers from accessing their accounts securely.

In contrast, there is the potential to use graphical passwords as an alternative authentication mechanism designed to aid memorability and ease of use. The idea of this research is to combine the usability of recognition-based and draw-based graphical passwords with the security of OTP. A new multi-level user-authentication solution known as: **G**raphical **O**ne-**T**ime **Pass**word (GOTPass) was proposed and empirically evaluated in terms of usability and security aspects.

The usability experiment was conducted during three separate sessions, which took place over five weeks, to assess the efficiency, effectiveness, memorability and user satisfaction of the new scheme. The results showed that users were able to easily create and enter their credentials as well as remember them over time. Eighty-one participants carried out a total of 1,302 login attempts with a 93% success rate and an average login time of 24.5 seconds.

With regard to the security evaluation, the research simulated three common types of graphical password attacks (guessing, intersection, and shoulder-surfing). The participants' task was to act as attackers to try to break into the system. The GOTPass scheme showed a high resistance capability against the attacks, as only 3.3% of the 690 total attempts succeeded in compromising the system.

Table of Contents

APPENDICES

Appendix A   Review of additional graphical password schemes and list of scheme names with references

    i. Graphical password schemes names and references

    ii. Review of additional schemes

        1)   Draw-based schemes

        2)   Click-based techniques

        3)   Choice-based techniques

List of Tables

List of Figures

Acknowledgements

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

Relevant seminars and conferences were regularly attended at which work was often presented and several papers were published and prepared for publication. Other research skills development courses were also attended.

Word count of the main body of thesis (Chapters 1 to 8): 59,533

Signed _____

Date _____

Chapter One

Introduction

In today's globalised digital life, services over the Internet have evolved rapidly, and they now play an essential role in fulfilling people's daily needs. With the ever increasing dependency on computers and digital information, the task of keeping people's data secure is of the utmost importance. As a matter of fact, information assets are crucial to the interests of both individuals and organisations. Thus, data must be protected and unauthorised access prevented in order to hinder data manipulation and theft. One significant way to achieve the required sort of protection is through authentication, which verifies the identity of the claiming user. However, it is often a challenge to make authentication systems both secure and usable, since a trade-off between these two necessary requirements often occurs.

The traditional text-based password is the foremost knowledge-based authentication method and the primary form of user authentication to date (De Angeli et al., 2005) (Fu et al., 2001). While many techniques are used to secure passwords (Pinkas & Sander, 2002), most are insufficient in the face of attackers' tools (Chakrabarti & Singbal, 2007) (AuthenticationWorld.com, 2012). Yet, the text-based password system is widely used despite its well-recognised deficiencies, which affect both usability and security (Dhamija & Perrig, 2000) (Xiaoyuan, Ying & Owen, 2005). The difficulty of remembering strong, complex passwords is one of the fundamental problems that users encounter, leading them to choose weaker passwords or to adopt insecure behaviours (Dhamija & Perrig, 2000) (Por et al., 2008) (Xiaoyuan, Ying & Owen, 2005). Another major issue with textual password authentication is its susceptibility to credential theft (Dhamija & Perrig, 2000).

Due to the aforementioned shortcomings of the traditional textual authentication method, the need for alternatives has emerged. Consequently, a diverse range of alternative technologies have been proposed to replace the text-based password, such as biometrics,

security tokens, OTPs and cognitive passwords. Nonetheless, it is expected that each alternative has its own weaknesses and strengths. The graphical password is among the most promising alternative proposals and occupies an important position within user-authentication research (Ray, 2012).

1.1 Motivations

As time passes, and with the accelerated pace of technology development, the use of the traditional form of authentication (i.e. textual password) is no longer sufficient to fulfil the increasing demand for a secure, usable authentication mechanism to protect users' accounts. Thus, an alternative authentication technique which has less of a burden on human memory is always sought after. For this reason, the idea of utilising images either by recognition or easy recall, has gained an increased research interest.

One field that has benefited from the evolution of the Internet is the financial industry. The opportunity to provide clients with a range of electronic services that are available anywhere and anytime over the Internet has been an area of growing interest for financial institutions. A vital requirement of online systems, particularly for financial firms, is to grant access to legitimate users only while preventing others from gaining unauthorised access. In order to achieve this in the online banking systems, various types of authentication mechanisms have been implemented (e.g. textual username and password, OTP security token and OTP via SMS). In addition, a combination of multiple authentication methods is mostly used in such a critical environment as a way to safeguard the systems from any potential fraud. However, that does not guarantee the optimal security and usability of the Internet banking system. For example, the use of security tokens to generate an OTP could add a significant degree of security; however, in practice, carrying around a token (or more) can be inconvenient experience for clients, and

forgetting/losing the token can be even worse, since it is impossible to gain authentication without the token. Thus, extending the investigation into this crucial area is needed in order to discover more about the limitations of the authentication techniques of the current system and, consequently, propose a suitable alternative solution to overcome the main security/usability issues. One potential solution can be through the use of graphical password as it does not require a device or phone connectivity to operate.

This research has made use of the online banking context to explore the security, usability and user convenience of an alternative authentication mechanism that depends on the utilisation of various graphics.

1.2 Aims and objectives of the research

The research aims to establish a tokenless graphical authentication system capable of generating one-time passwords without complexity or dependency on devices as a prospective alternative authentication solution. Thus, this research focuses entirely on graphical password authentication as a key potential alternative to the traditional authentication method. The objectives of the research are outlined as follows:

- Review the common user-authentication mechanisms to highlight their strengths and weaknesses, and then conduct a comprehensive review of graphical password schemes to explore their characteristics in an attempt to find an opportunity for enhancement.

- Assess the authentication mechanisms offered by online banking systems to explore the authentication limitations, and then investigate the users' perceptions of the idea of carrying around multiple authentication tokens and how they perceive the adoption of the graphical password method as an alternative authentication method to protect their accounts.

- Design and develop a novel authentication scheme and then empirically evaluate its security and usability.

- Investigate the users' perceptions of the security and usability aspects of the new proposed authentication scheme.

The aim of the novel authentication scheme is to tackle some of the main issues with the earlier authentication proposals, including the following issues:

- Low memorability for secure passwords.

- The need for an additional device to generate or receive OTPs.

- Susceptibility to guessing and observation attacks.

- Exploiting the recognition feature of visual -based schemes.

These issues are included in the literature that will be discussed later in this thesis, as they are some of the main issues facing alternative authentication techniques.

Of great value to the information security would be to propose and develop a graphical authentication scheme with the security capability and adequate usability to serve the purpose of securing critical systems, such as the online banking system. The proposed scheme should then undergo intensive evaluations including security and usability aspects to ensure its suitability for such a system.

1.3   Research outcomes and contributions

A summary of the main contributions of this research is listed below:

- Suggest a new data-entry classification within the field of graphical authentication that utilises keyboard-typing entry as a way to submit the secrets and add some

distinguishing classification details, involving several design aspects, such as input approach and display style, to enable better representation.

- Develop a hybrid multi-layer authentication system, combining several graphical password methods along with one-time password technique (draw-based, recognition-based and OTP). Figure 1-1 illustrates a summary of the main contribution of the proposed authentication solution.

- Employ a dynamic one-time password combination obtained through a multi-step graphical password.

- Implement a web-based 4×4 unlock pattern to provide an effective proactive protection.

- Reduce the selection of hot-images by using system-assigned themes along with a user-chosen images approach.

- Evaluate the security of a hybrid graphical authentication by utilising two methods: theoretical and empirical.
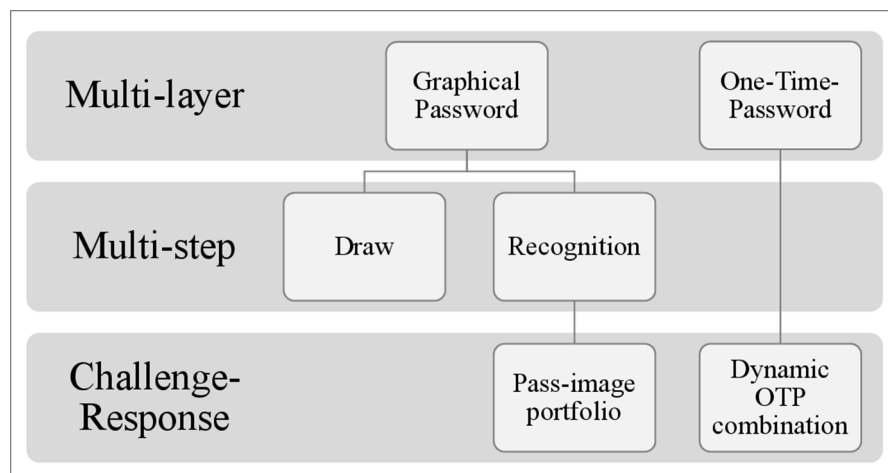
Figure 1-1: Overview of the contribution of the proposed solution

Part of the research work presented in this thesis has already been published in several peer-reviewed publications as enumerated below:

- Graphical One-Time Password (GOTPass): A Usability Evaluation. *Information Security Journal: A Global Perspective*, May 2016, pp. 1–15.

- Secure Graphical One Time Password (GOTPass): An Empirical Study. *Information Security Journal: A Global Perspective*, *24*(4-6), December 2015, pp. 207–220.

- Alternative Graphical Authentication for Online Banking Environments. In *HAISA,* 2014, pp. 122–136.

- A Review of Graphical Authentication Utilising a Keypad Input Method. In *Proceedings of the Eighth Saudi Students Conference in the UK*, February 2016, pp. 359–374.

The researcher was the corresponding author in the above-listed publications. For a full-text copy of each publication, please refer to Appendix G.

1.4   Structure of the thesis

The remainder of the main body of the thesis is organised into seven further chapters as summarised below.

Chapter 2 provides a general overview of the user-authentication domain, starting with the threats to authentication, classification, various enhancement implementations, textual password issues and, finally, highlighting the need for alternative authentication and the requirements of such alternatives.

Chapter 3 introduces the notion of graphical authentication by reviewing the main schemes under different categories. A comparative summary of each category is also provided. Moreover, the applicability of one-time password to graphical authentication is discussed. This chapter also highlights password space and entropy and then concludes by outlining the issues associated with, and the vulnerabilities of graphical authentication.

Chapter 4 begins with an overview of authentication in the online banking environment. It then addresses the limitations of the current authentication in this field and finally reports the details of the preliminary research survey that seek the users' perception of the online banking authentication and the extent of accepting a graphical password as an alternative authentication.

In Chapter 5, the new enhanced method (GOTPass) is described in details; including the design and development. It also explains the process flaw of the registration and authentication tasks, in addition to the explanation of each component of the system. Moreover, the characteristics and advantages of the proposed system are presented.

The main focus of the sixth chapter is to report the result of the conducted experiment to evaluate the usability of the GOTPass scheme as well as the analysis of the outcomes. The usability experiment shows the performance stages that were carried out over several time periods with certain evaluation conditions, to ensure sufficient data was gathered for a reliable investigation.

Chapter 7 elaborates on the security aspects of the new proposal. At the beginning of the chapter security concerns and threats are outlined, then the security features of the GOTPass scheme are presented, followed by a detailed demonstration of various security evaluation approaches. The results of the evaluations are analysed and discussed, before closing the chapter with the presentation of the supplementary security study and its outcomes.

The final chapter concludes by summarising the major research findings and achievements reported in this thesis along with the research limitations and future work opportunities.

Chapter Two

User Authentication

2.1 Introduction

As the previous chapter introduced the importance of the Internet security and authenticating users to systems in particular, now this chapter generally takes us through user authentication methods to explore some of their advantages and disadvantages as well as the related threats. In addition, the last section will talk about the requirements of alternative authentication techniques.

With the global evolution of the Internet-based information services, more platforms have been connected, not only the traditional computers but also smartphones, wearables, gaming consoles, Internet of things (IoT) and even smart cars. This has created enormous networks interconnected globally and increased the requirement for the accessibility and availability of information. In such cyber era, the entity (possibly a friend, a machine, or an attacker) on the other end of a remote connected network cannot be seen and thus difficult to be verified. There is always a concern to keep the sensitive information, that is exchanged online, private and protected from attackers who are not required to be physically presented to breach the data.

One of the Internet activities that is growing fast and gaining popularity is the online banking services which facilitate many of the customers' banking tasks. With that widespread growth in the online banking services and usage worldwide, threats and vulnerabilities are also on the rise. Hackers and fraudsters are attracted by the illegal financial gain (Ortiz, 2007) which expose online banking to numerous threats. Therefore, banks have to undertake strong security countermeasures to protect their customers from those adversaries with malicious intentions who always develop means to be at least one step ahead of their targets (Sule, 2013).

Thus, the need for more robust safeguards and system security to protect the resources and services of the connected users has become a vital requirement. A fundamental

security measure for computer systems and services is to accurately allow access for legitimate users while preventing others from gaining unauthorised access. Therefore, researchers have been interested in developing various types of authentication mechanisms including textual password enhancements, token-based and biometrics authentications. Authentication is a key aspect of the access control system that lies at the core of information security importance (Anderson, 2010a). Before a user can access a certain system, they must identify themselves through the presentation of their credentials which is known as the identification step (Meyer, 2007). Then, the process of granting access to the system begins with authenticating people to that system, which in turn proves that the requester is who s/he claims to be and then determines whether access is permitted or not. This is followed by the authorisation operation where privilege controls are applied to link access rights with specific system resources. Although authentication and authorisation are tightly bound, it is important to note that they are two distinct mechanisms. Due to this close correlation, authentication and authorisation are sometimes wrongly considered as one method (Rescorla & Lebovitz, 2010). Authentication is the first step in the access control process, and it will remain the main concern throughout this research.

2.2   Common authentication-related threats

According to the First Half Review of 2015 breach level index originated by Gemalto, identity theft was the leading type of data breach accountable for 53% of the total attacks and almost 75% of compromised data records. Furthermore, most of the highest severity data breaches were caused by identity theft-based attacks. The report also indicated that the first step towards mitigating the overall consequences caused by a security breach is through controlling access and authentication of users (Gemalto, 2015).

Security attacks can be categorised into human-based and technology-based attacks. In the human-based attacks, the attacker interacts with the victim who possesses valuable information (e.g. social engineering attacks), whereas in the technology-based attacks, confidential information is accessed by employing other non-interactive means (e.g. phishing emails) (Luo *et al.*, 2011).

Various types of threats are exploited to breach data such as phishing, spyware/keylogger, guessing credentials, eavesdropping, and social engineering. Regardless of the attack type, attackers have one unified goal that is stealing secret information to gain an unauthorised access. The following subsections present a brief overview of some of these threats classes.

2.2.1 Phishing

Phishing attacks build a counterfeit website, which apparently looks legitimate with all official graphics and logos, to fool victims to submit confidential, personal and financial information. The phishing scam is then distributed via e-mail or other electronic means to reach as many users as possible.

2.2.2 Social engineering

A social engineering attack is used to manipulate legitimate users by tricking them into performing insecure practices such as revealing personal/account information. The common methods used in this attack is telephone calls or Internet.

2.2.3 Dictionary attack

A dictionary attack is based on searching a large number of possibilities to determine the correct password. The dictionary is typically built from a list of words that are most likely to succeed. In contrast, a brute force attack uses an exhaustive search to try all possible combinations of password's characters.

2.2.4 Spying

Tracing users' activities in a computer system is achieved by using a variety of spying techniques. The first of these is physical observation, which is usually referred to as shoulder-surfing. This simply involves watching victims during authentication to obtain their passwords. Second, is the so-called spyware, which is an electronic form of software spying that is designed to run silently in the background to observe, collect and log the actions of a victim's system. Keystrokes, screenshots and the interactions of a user can be all recorded through spyware. An important use of such attack on compromised devices is to capture payment card information and user's sensitive data. One way of defending against spying is through the implementation of encryption to secure the communication and transmission of data (Gordon, 2005).

2.2.5 Guessing

Users often tend to choose easy to guess passwords, including things like first or last name, family member name, special date or even trivially the word 'password'. Attempting to guess several likely values might eventually lead the attacker to succeed and break into the system. Password guessing attempts can be controlled by applying account lockout mechanisms, which lock out access to the vulnerable account for a certain amount of time when a number of failed login attempts is exceeded (Federal Financial Institutions Examination Council 'FFIEC', 2006).

2.2.6 Eavesdropping

Eavesdropping is a type of attack in which users' credentials are stolen through listening to the communication channel between the client and the requested system in order to record login information in transit. As a result, the valid but stolen credential allows attackers to gain access to the target system or device. Therefore, users must protect their accounts by accessing them over an encrypted connection that utilises a cryptographic protocol such as SSL or TLS (Smetters & Jacobson, 2009).

2.3 Categorisation of user authentication

One of the key research areas in the field of information security is user authentication, which is mainly concerned with the approach of authenticating people to systems. The main authentication methods can be simply formulated as "Something we know", like passwords, "Something we have", such as Smart/ATM cards, or "Something we are", such as biometrics (Stamp, 2011). In addition, there are other categories which can be involved into this taxonomy; "Something we do", such as access point push button (WPS) (Stamp, 2011), "Somewhere we are in", like the Cellular Network Based Positioning (Kuseler & Lami, 2012), which can be used to verify or challenge a claimed identity. The latter categories can mitigate risks but do not directly enhance the authentication assurance level (Burr et al., 2013). The main authentication methods can act either alone or in collaboration with others. Combining more than one authentication method is called "Multi-factor authentication", and this is said to produce an enhanced authentication mechanism and improve system security (will be further discussed later in subsection 2.4.1).

The following subsections will discuss the three main categories and then will be followed by outlines of some major authentication implementations.

2.3.1 Knowledge-based authentication – KBA (Secret)

Knowledge-based authentication relies on some secret information known only to the user. This authentication mechanism can be provided in different formats, one of which is a username and its associated password. Graphical password is another branch of the KBA as well. The process of knowledge-based authentication involves different parties mainly the Claimant: the applicant to be authenticated, and the Verifier: the party to verify the identity of the claimant. When a claimant provides the correct identity information to

a verifier through an authentication protocol, the verifier validates the credential and asserts the claimant identity (Burr *et al.*, 2013).

As a matter of fact, KBA is the most common and widely used authentication method since it includes the textual password (Dhamija & Perrig, 2000). The text-based scheme occupies an advanced position within the users' interest in spite of its well-known drawbacks (Xiaoyuan, Ying & Owen, 2005). There are several factors that help the knowledge-based authentication to dominant such as the inexpensive and easy implementation and scalability as well as the vast user familiarity (Zippy & Moshe, 2009). In addition, knowledge-based authentication and in particular text-based password can provide other significant advantages such as cross device, ease of entry and accessibility (Kessler, 1996).

2.3.2   Attribute-based authentication (Biometric)

The uniqueness of human attributes of a specific user is the characteristic of the attribute-based authentication. A human body biometric is a feature that can be distinguished to be utilised for user authentication based on "who you are" (O'Gorman, 2003). A biometric authentication system usually operates by obtaining biometric data from a user, extract a feature set, and then compare it against the stored template set in the database. There are two operational modes for a biometric system; verification or identification. The verification mode – determines whether the claiming identity is true or not by conducting one-to-one comparison whereas in the identification mode – the system carries out a one-to-many comparison to identify a user which means searching for a match among all users' templates in the database (Jain, Ross & Prabhakar, 2004). A practical biometric system should meet the performance requirements; accuracy, speed and resources. In addition, it should also be harmless and acceptable to the users besides being sufficiently resistant to various fraudulent methods and attacks (Jain, Ross & Prabhakar, 2004). Biometric

features can be categorised as physical or behavioural as illustrated in Figure 2-1 (Jain, Ross & Nandakumar, 2011).
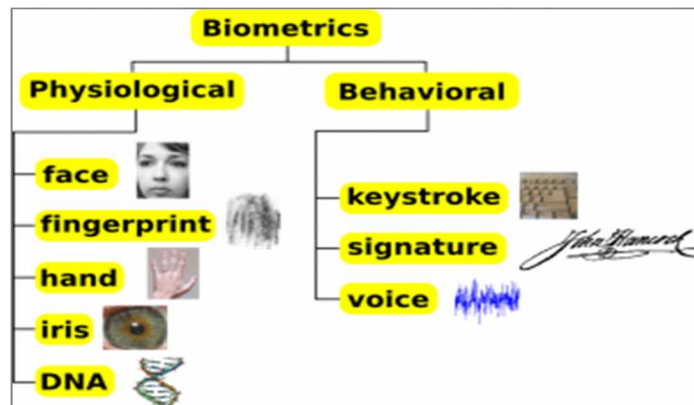
Figure 2-1: Biometric classifications (Gibson, 2011)

According to Jain, Ross & Prabhakar, (2004), any human physiological or behavioral characteristic should satisfy certain requirements in order to be used as a biometric characteristic. These requirements are enumerated as follows:

• *Universality*: the characteristic should be in each person.

• *Distinctiveness*: the characteristic should be sufficiently different for any two persons.

• *Permanence*: the characteristic should be sufficiently unchangeable over the time.

• *Collectability*: the characteristic should be quantitatively measurable.

Physical features are based on the stable body including fingerprints, the eye (iris and retina), the face and hands, whilst behavioural features are based on learned movements, such as a handwritten signature, keyboard typing (keystroke) and the way of walking (gait). The ability to link the authentication information to its owner is an interesting property of biometrics that passwords and tokens lack since they can be lent or stolen. However, gaining unauthorised access to a security system operated by biometric is not infeasible since biometric features can be copied or counterfeited with different levels of difficulty. In such cases, it is impossible for the legitimate user to revoke the stolen biometric and request a replacement. Moreover, another frustrating issue is the output

errors, where users are refused access to the system because of a device fault. Similarly, another permission-related problem is the rate of the False Positives (where illegitimate user is falsely granted access) and False Negatives (where the legitimate user is falsely denied access). The need for a capture device to enter the biometric information along with the associated cost of such hardware might prevent this authentication mechanism from being widely used (O'Gorman, 2003) (Renaud, 2004).

In the case of the recent biometrically-enabled mobile devices that are equipped with various integrated biometric sensors such as fingerprint, manufacturers ensure that the biometric template is securely stored into the user's device. However, securing services other than the device unlock utilising fingerprint biometric may require allowing third party to access the fingerprint sensor which in turn raise the privacy concern of the users (Goode, 2014). Ivor Lewis stated that *"Despite this rigorous process, public perception of risk is actually often the biggest hurdle and suspicion that fingerprints can be stolen and reused persists"* (Lewis, 2014).

The device usage is also utilised by the continuous transparent authentication to extract characteristic and measureable patterns that can be collected from most mobile device users without requiring specific action. Gathering such patterns can be through common tasks like email composition and phone calls that help to determine the ownership of the mobile device for that user. This type of authentication is carried out transparently as no explicit interaction is required from the user. In addition, it is a continuous authentication since it runs dynamically in the background in response to certain user actions (Crawford, Renaud & Storer, 2013).

One of the disadvantages of using the integrated biometrics on mobile devices for user's authentication is that it is being tied down to the mobile device, besides targeting a

specific platform (mobile) only and not universally usable across different platforms such as web-based application on a desktop or laptop. Furthermore, a demonstration of a fake finger fooling a smartphone's fingerprint sensor was undertaken at the Mobile World Congress tech show. In relation to that, the BBC was told that fingers made of modelling clay can fool lower-resolution sensors (BBC, 2016). Another obstacle that face the reliance on mobile phone for sensitive tasks including authentication is the mobile theft. According to the Crime Survey for England and Wales, there were 538,000 victims of mobile phone theft between 2014 and 2015 (Office for National Statistics, 2015). The Home Secretary Theresa May said: *"However, the level of mobile phone theft remains a concern and people are increasingly carrying their lives in their pockets, with bank details, emails and other sensitive personal information easily accessible through mobile phones."* (Home Office and The Rt Hon Theresa May MP, 2014).

2.3.3 Possession-based authentication (Token)

This authentication type is characterised by the physical possessing of objects to indicate the identity or eligibility of a user to access the system. This kind of devices is commonly referred to as a token including USB token devices, smart cards and active password-generating security tokens (O'Gorman, 2003). Rather than depending on human memory, this sort of authentication mechanism relies mainly on carrying a token and proving its ownership as an essential part of the entire authentication process. Various types of token devices are generally temper-resistant that makes it difficult to duplicate and manipulate (Federal Financial Institutions Examination Council, 2011). Still, tokens can be used illegally by sharing them with others (Ratha, Connell & Bolle, 2001). The need for additional hardware readers or software drivers is the primary disadvantage of such an authentication mechanism. Furthermore, the inconvenience and high cost associated with

the hardware tokens, when compared to a textual password, are other disadvantages of this kind of authentication technique (O'Gorman, 2003).

Recently, mobile phones were proposed to be used for authentication that can fall under different categories depending on the purpose of use, which will be discussed in subsections (**Error! Reference source not found.**) (**Error! Reference source not found.**).

2.4   Implementations of authentication

Having discussed the different authentication classifications in the previous section, this section reviews the major authentication implementations that fall into these categories such as multi-factor and one-time authentication techniques.

2.4.1   Multi-factor authentication (M-FA)

Any composite authentication mechanism derived from more than one form of identity verification (any combination of the authentication factors: Knowledge-based, Possession-based, or Attribute-based) is called "Multi-factor authentication". In general, multi-factor authentication is usually employed to enhance the security of the common text-based password. However, using several authentication factors improves the security but may complicates the process of authentication (Sabzevar & Stavrou, 2008).

Implementing multi-factor authentication makes the system more secure since a successful attack would need an extra means of authentication rather than merely the details of the user's credentials. This should result in reducing the impact of Internet identity theft and phishing attack (SecurEnvoy, 2013a). The condition to form a strong multi-factor authentication is to ensure that at least one of the factors is not reusable, replicable, nor easily stolen online (European Central Bank, 2013). It is also

recommended to physically separate one of the factors from the device accessing the system to increase the effectiveness (The Defence Signals Directorate, 2014).

A layered authentication is another variation that verifies the identity of a user through multiple layers of authentication. These layers involve more than one authentication technique derived from the same category i.e. password and passphrase (knowledge-based), fingerprint and retina scans (attribute-based) (Sollie, 2005). The key aspect is to ensure that the combinations among a particular authentication factor are distinct and not the same. In practice, several UK banks still support multi-layer authentication by implementing more than one text-based credentials (Just & Aspinall, 2012).

Multi-factor mechanism is the required implementation to comply with the Federal Financial Institutions Examination Council (FFIEC) authentication guidance to safeguard sensitive systems (Federal Financial Institutions Examination Council, 2011). Although multi-layer authentication provides less security compared to multi-factor (Al Abdulwahid et al., 2015), but still can increase the level of assurance since a successful authentication will require resolving several secrets.

2.4.2   One-Time-Password (OTP)

In crucial systems, such as those found in financial organisations, robust security is constantly demanded. One of the solutions to meeting that goal is through the implementation of One-Time-Password approach. The key idea of OTP is to encode the password for a single use, producing a unique password for each login session or transaction. In other words, the user will end up using different dynamic passwords in each login trial. Interestingly, illegitimate obtainment of OTP should be of no use to attackers in generating any further encoded passwords. Thus, an already used OTP would be totally unusable for upcoming login attempts since OTP loses its validity (expire and

discard) after first use. As a result, OTP systems are protected against replay attacks (Rubin, 1996) (McDonald, Atkinson & Metz, 1995).

The operation of OTP involves two main processes: OTP generation and OTP delivery. First, the generation of OTP is achievable through a number of approaches mainly mathematical (e.g. previous password-based algorithm or challenge-based algorithm) or based on time-synchronisation (valid for a limited time only) (Ortiz, 2007). Next, comes the delivery of the generated OTP to clients which represents how the end user receives and views the OTP. Several approaches have been used to fulfil this operation requirement, such as hardware (proprietary tokens, mobile phones), text messaging, image-based methods or paper-based (codebooks) (Bonneau et al., 2012). These mediums are not free of shortcomings, for instance, the hardware-based approach is expensive to implement and maintain, besides being burdensome to users (to carry around, exposure to loss/damage) (Khot, Kumaraguru & Srinathan, 2012). Whereas, the paper-based approach is cheap but vulnerable due to the possibility of it falling into unauthorised hands or captured by a camera (Bonneau *et al.*, 2012). Mainly, One-Time Password mitigates the problems related to the poor choice of passwords, however, the reliance on additional hardware or special software decreases its availability and thus limits its wide deployment. Also, the synchronisation between the client and server can possibly get out of synch which requires intervention for resynchronisation (Renaud, 2004).

There are various types of one-time password technique, which are outlined next.

i. Token-based OTP

One of the important factors that usually forms part of a multi-factor implementation is the hardware tokens which are physical devices used to authenticate users by generating random numerical codes. The device is equipped with a small screen on one side to display the generated code. As a consequence of using this type of technique, crackers and keyloggers are avoided and password sharing is prevented. However, lending the

device or sharing it with others is still possible. One downside of such a method is the incurred cost which was further classified by (Grand, 2001) into different stages; Immediate cost (initial purchasing and deployment), Support/Maintenance cost (on-going), and Remediation cost (e.g., revoking and reissuing of hardware token).

Another drawback of using a hardware token is the process of issuing a new token or reissuing a replacement, which can be slow as it needs to be ordered and prepared specifically for each user, which in turn delays gaining access to the user's own data. In addition, although the small size of the token is appreciated but at the same time it exposes the token to be easily lost or forgotten (SecurEnvoy, 2013a). According to (Levy, 2011), the time when most people forget to carry their devices is when they need them most, such as while travelling.

ii. Non-Hardware-Based OTP (Tokenless)

Non-Hardware-Based aka 'Tokenless' authentication usually plays a part of two-factor authentication which was proposed to resolve the hardware token problems by utilising, for instance, mobile phone devices via an SMS service or mobile software. In some applications, OTP can be generated by an installable software either on the user's computer, smartphone or tablet. RSA SecurID Software Tokens (EMC, 2015) and Google Authenticator (Google, 2015) are examples of this type of technology that are also called software token (soft-token).

This form of authentication can usually be accomplished using the existing infrastructure with no much additional requirements, such as software, hardware or devices (Meyer, 2007). The use of individual's mobile phone is said to be an advantage since such device is supposed to be carried around with the user all time in contrast to the token-based solutions. However, losing the registered mobile phone is possible which is considered a drawback that may cause a distressful experience for the users to access their account

(Borgohain et al., 2015). Nonetheless, since a hard-token is not often in frequent use, users are unlikely to miss it if stolen or lost until they need to use it again, whereas a missing mobile phone would usually be noticed shortly (SecurEnvoy, 2013b).

Although using an SMS service to deliver the one-time password to the user provides strong authentication, but it is not broadly popular due to the high implementation cost, user experience (e.g. poor network signalling coverage, latency of message delivery, and longevity of the phone battery) (Borgohain *et al.*, 2015). In addition, SMS OTPs are limited in terms of their inability to provide in-app or in-browser authentication as well as the lack of support for non-SIM based smart devices, such as tablets, notebooks and laptops (ENCAP, 2012).

The flexibility and lower cost of the non-hardware techniques make them more appealing than hardware-based solutions. On the other hand, they are vulnerable to malware and keylogger attacks as well as visual spoofing attacks (Meyer, 2007).

Token and tokenless OTP techniques utilise an out-of-band transmission approach where a different channel than the one initiated by the user (e.g. token, mobile application, SMS, e-mail, or phone call) is used to deliver the generated OTP. Separating channels adds an extra security layer to complicate the task of the attacker as a successful attack would involve intercepting both channels (StrikeForce Technologies Inc., 2015). However, one way an attacker may use to bypass the out-of-band authentication is by attempting to change the registered phone number on the customer's account with the attacker's own phone number (Rouse, 2014). In addition, out-of-band technique is prone to man-in-the-middle attacks that target the user's browsers (man-in-the-browser - MITB) or mobile phones. This type of embedded Trojan can intercept and manipulate messages while in transit (Sule, 2013).

Still some people may argue that the use of out-of-band technique complicates the authentication process since these systems require the user to look somewhere else, other than the current screen, to complete the authentication request. For example, the user may need to use a hardware-token, mobile phone, or home phone to receive a code or answer a voice prompt.

Another way to deliver the OTP is through the use of an in-band channel authentication. In this method, the system utilises the same channel to initiate the authentication request and deliver the code, for instance, using the browser to accomplish such tasks. However, although this method appears easy to implement and use, but it does not seem to provide the same security level as that offered by the out-of-band channel due to its vulnerability to malware that can capture important data on that single channel.

iii. Graphic-based OTP

The human ability to recognise and recall images has made it possible to utilise images or drawings to authenticate users to computers. In addition, this idea has been extended to use image recognition to provide OTP. Several techniques have been proposed, including various graphic-based methods to generate OTP (ConfidentTech, 2012) (CRYPTOCard Inc, 2010b) (Gupta et al., 2012) (Ku et al., 2013), and these will be reviewed later in the next chapter.

Table 2-1 gathers and summarises the advantages and disadvantages of the main commonly used OTP techniques.

Type of OTP technique		Pros	Cons
Token-based	Hard-Token (Hardware)	Safe against keylogger.	High cost. Inconvenient to carry multiple tokens. Slow process of issuing /replacing tokens. Easily lost or forgotten due to small size.
Tokenless	Soft-Token (Software)	Use existing infrastructure.	Vulnerable to malware, keylogger.
Tokenless	(SMS)	Use existing devices. Phones are tied to user, so quickly discovered when missing.	Affected by poor cellular network. Delay of message delivery. Lack of in-browser authentication. No support for non-SIM based devices.

Table 2-1: Comparison between OTP techniques

2.4.3 Other implementations

Attempts to enhance and strengthen user authentication are continuing and evolving to meet the changing needs of the end users. Recently, a 'One Touch Authentication' technique has been launched (Swivel Secure, 2014) (AuthShield, 2015). The concept of this technique is to exempt the user from re-entering the authentication code. Instead, users will receive the authentication request through a 'push' notification on their smartphones or desktop. The notification contains two options at a click of a button; 'approve' to accept the authentication or 'deny' to reject it.

2.5 Issues with the conventional Text-based authentication

Despite the fact that text-based authentication being widely used, it is well-known for deficiencies that affect both usability and security (Dhamija & Perrig, 2000) (Xiaoyuan, Ying & Owen, 2005). One of the main problems with textual passwords is the difficulty to comply with the security policy for authentication, such as remembering strong complex passwords, which leads to increase user's tendency to choose weak passwords. Although easy to remember passwords are often simple or meaningful, at the same time

they are vulnerable to attack since they can be easily guessed or cracked. On the other hand, long or arbitrarily chosen passwords seem secure and are thus hard to guess or crack but are often difficult to remember. The limitation of human memory to remember secure passwords has led to the adoption of other insecure behaviours, such as writing passwords down or using the same password for multiple accounts. Although the password memorability is deemed as a significant problem, but in fact there are other factors that make remembering passwords a lot more difficult such as the number of passwords to remember and the complexity of rules (Adams & Sasse, 1999). Furthermore, the possibility to share passwords with others is also considered a problem as the password is then no longer secret (Dhamija & Perrig, 2000) (O'Gorman, 2003). Another major issue with password authentication is the credential theft, which makes use of different intelligent techniques to acquire victims credentials (Balfanz et al., 2012).

2.6   The need for alternative authentications

The most common cause of system break-ins is a weak password, nevertheless, text-based authentication is still predominant (Dhamija & Perrig, 2000). A number of solutions to strengthen the text-based password and to overcome the flaws of weak passwords have been proposed. Nonetheless, the majority of these solutions fall into three main categories. The first is known as proactive security measures, and this aims to identify and prevent weak passwords by running password checker programs in advance of them getting broken. The second is based on the technical capability to intensively increase the computational overhead of cracking passwords. The last category relies on raising the security awareness of the users through training and education in addition to establishing security guidelines. However, the aforementioned solutions are unable to address the human memory's inability to remember secure passwords, which is the main cause of textual password insecurity (Dhamija & Perrig, 2000).

Proposals for replacing text-based passwords have been offered occasionally but with low expectations of success. That proves the popularity of textual passwords and how reliant the users are on this technique. Previous attempts to replace passwords have revealed uncertainty about which threats to address. Consequently, *"Inability to quantify harm precludes quantifying the expected improvement from alternatives"* as stated by Herley & van Oorschot (2012). Moreover, displacing passwords is often costly and most alternatives would not be vulnerability free as well.

In addition to the obvious need for a strong authentication technique in terms of security requirements, usability is an increasingly important factor of the authentication process that needs to be taken into consideration while designing any authentication scheme. However, there is often a conflict between the requirements to achieve a higher level of security and the requirements to maintain adequate level of usability at the same time. In some cases, users tend to misuse complicated authentication techniques as they might find themselves unable to keep up with the increasing workload of such technique (Braz & Robert, 2006). Thus, a trade-off between potential security and usability requirements must be considered depending on the sensitivity of the target system.

2.7   Alternative authentication mechanism requirements

According to Patrick Elftmann (2006), several existing alternatives to alphanumeric authentication mechanism have not been broadly adopted by computer systems nor accepted by end-users. The reasons behind that are varied including resistance to change on the side of the users, additional hardware costs or a low level of security and usability. In order to consider an authentication method as an ideal alternative, it is important that it meets the following essential criteria, as introduced in (Elftmann, 2006).

A. Elimination of the need for additional hardware

Unless a unified infrastructure is built, it seems illogical to force users to carry multiple tokens for different systems everywhere. Moreover, adding hardware, such as smart cards or biometrics readers, to all users' systems may cause inconvenience to users. This includes other convenience issues, like hardware renew, recover and revoke. On top of the expected high cost of purchasing and deploying such hardware, these approaches involve additional expense for ongoing maintenance and customer support. More importantly, lost or broken hardware will prevent users from gaining access to their accounts. Therefore, the requirement of additional hardware should be avoided when planning for a convenient/low cost alternative authentication mechanism.

B. Higher level of security

When the purpose is to find an alternative to text-based authentication, it would be obvious to aim for better security in any new scheme than that existing in the traditional password. That is to say, the alternative should have an increased password space to be more resistant to security attacks, like brute force or dictionary. Also, reduce the possibility of writing down passwords or disclosing them to others. Thus, the alternative authentication method should achieve adequate security.

C. Better memorability

The problem with passwords is that humans find difficulty in creating a secure complex password that is easy to remember at the same time. Thus, it is important for the alternative to be memorisable for better memory retrieval and to avoid any possible subsequent problem that may occur as a result of memory limitation.

D. Simplicity and ease of use

The problem with security is not always technical, as used to be thought, but rather involves aspects of human-computer interaction (HCI). In other words, the security mechanism is effective when taking into account the usability and the interaction between

the security mechanisms and user practices. Therefore, a quick and easy process of enrolment, training and authentication should be the style of the alternative method.

E. Compatibility/Applicability on various areas

The conventional textual password has been used and applied on various platforms and applications, such as computer log-on, mobile and tablet devices, Internet banking applications, email and ATM machines, etc. Thus, the alternative authentication method should be applicable to cross-platforms, freely usable and compatible with different applications.

In addition, Pinkas and Sander (2002) outlined some functional requirements and criteria for authentication methods. The identified requirements include availability, portability, robustness, reliability, friendliness, seamlessness and low cost of implementation and operation.

The design of a successful authentication mechanism should be evaluated against several aspects of security and usability (De Angeli et al., 2005). The usability evaluation consists of objective data on mechanism performance and subjective data on user experience (Beautement & Sasse, 2010). Hence, the usability of the new proposal will be evaluated based on the main usability components of the ISO 9241-11 (International Organization for Standardization, 1998) that involve effectiveness, efficiency and satisfaction. In addition, memorability is another significant usability component that will be also included in the evaluation. As far as the security evaluation is concerned, De Angeli *et al.* (2005) have considered three basic dimensions (guessability, observability and recordability) to assess different aspects of the authentication system's security which will be used to evaluate the security of the new proposal.

2.8 Summary

To summarise, secure/usable alternatives to text-based authentication mechanises are needed. Although several alternative authentication systems have been proposed such as biometrics and token-based authentication, but most have not managed to be widely adopted for reasons such as costs for extra hardware, low security or a complex authentication process. In accordance to the study by Zippy and Moshe (2009) which compared the main authentication categories, the result of the study showed that knowledge-based authentication performed very well across all factors except the security. That has motivated this research to be confined to alternatives of the knowledge-based authentication type to ensure that there is no additional hardware requirement and potentially can provide higher security with better memorisation.

The focus of this research will be mainly on a branch of the knowledge-based authentication that is graphical password along with one-time password technique since combining both of these techniques could potentially lead to a successful alternative method to the conventional alphanumeric authentication method. At the same time, this should also intend to be a suitable alternative authentication method in the absence of security hardware tokens. The reasons for this are derived from the characteristics of each method. In the first place, making use of graphics to authenticate users will eliminate the need for any additional hardware. Furthermore, the burden on human memory will be reduced since both OTP and graphical passwords do not normally rely on password memorisation, as opposed to the traditional username and password scheme.

The next chapter will review various types of graphical authentication schemes along with comprehensive comparisons of similar schemes. Reviewing these schemes allows discovering the characteristics, advantages and disadvantages of each scheme in particular as well as its relevant category in general.

Chapter Three

Graphical Authentication Techniques

3.1. Introduction

Alternative knowledge-based authentication approaches to replace the traditional text-based authentication have emerged with the potential to succeed, for example graphical passwords (recognising graphical elements – e.g. images, iconography, grids) (Gyorffy, Tappenden & Miller, 2011) or associative/cognitive questions (Alexander, 2008). Instead of remembering long set of characters, a user can be authenticated by recognising predefined images or recreating graphical drawings (Rittenhouse, Chaudry & Lee, 2013). The idea of using images rather than text or numbers was motivated by the assumption that presenting items as pictures is easier to remember than presenting items as words (Snodgrass & Asiaghi, 1977). Thus, the picture superiority effect is of particular importance to this research domain, which will be highlighted in the coming paragraphs.

In a study conducted by Shepard (1967), the recognition level for images was examined. A set of 600 images were used and individually displayed for the participants, each of which last for a few seconds. Afterwards, participants were challenged to recognise and distinguish the previously seen images out of the others on the display. Participants performed very well by recognising 98% of the images.

The effect of long term memory on image recognition was studied by Nickerson (1968). The study was conducted over four time intervals (Day: 1, 7, 28, and 360). Similar to Shepard study's methodology, this study used 200 pictures and displayed each for 5 seconds. The participants' task was to determine whether the displayed pictures were previously seen in the initial task or otherwise. The overall result indicated that there was a decrease in the success rate throughout the study periods. Despite the falling success rate, the study concluded that the long-term memory for image recognition was still better compared to words.

In 1970, Standing, Conezio and Haber (1970) examined the relationship between perception and memory through 4 experiments, two of them investigated the recognition memory for images. With 1100 magazine images in experiment 1, participants obtained 95% successful recognitions while they scored 85% in experiment 2 which used 2560 photographic pictures and were viewed over 4 days. As for the remaining two experiments, both were concerned about the effect of different aspects on recognition during viewing such as duration, reversing, and orienting. The results returned a success rate of over than 90% even with reversed images and a lower average score of above 50% when images were oriented. Overall, participants achieved high chance level of success for image recognition.

With regard to the capacity of memory and speed of retrieval, an investigation on that respect was carried out by Standing (1973). A total of 4 experiments were conducted to examine both images and words in several forms including ordinary images, visual and verbal words. The study used a large set of 11,000 images and changed the recognition approach (sequential display of images instead of simultaneous). In summary, the outcome of the recognition tests on the basis of memory capacity indicated that the use of images was superior to words or audios. However, there was a superiority for verbal words with respect to retrieval time. Additionally, Nelson, Reed and Walling (1976) proved that the image superiority effect can be disrupted or eliminated when the visual similarity in pictures is high.

The dual coding theory explained the picture superiority effect (Paivio, 1986) (Paivio & Csapo, 1973). It states that there are two methods the brain uses to remember information depending on the type. That means imagery information is remembered in a different way than verbal information (spoken or written). The process of remembering images involves the dual coding technique which form the representation of images in memory. The first code is visual where images are stored as imagery information while the second code is

verbal in which images are translated into a semantic form and stored as descriptive information. In order to recognise images, the memory utilises both code representations. On contrast, remembering text-based information requires symbolic representation only.

In the generate-recognise theory, the retrieval process of free recall is accomplished in two steps. The first is the generation step where a list of candidate words is formed by searching the long-term memory. Then the recognition step starts which involves evaluating the list of words to decide whether it matches the sought-after memory (Anderson & Bower, 1972). This theory explains why the recognition memory is faster and easier to perform than recall, as the former makes no use of the generation phase while depending only on the recognition phase.

Various types of memory retrieval are leveraged by different graphical password mechanisms. Although these varieties affect memory in the first place, but can also have an impact on other factors like login time or ease of use. Recall and recognition are aspects of memory processes for retrieving information. The process is called 'recall' when the context is provided and a particular event is missing, whereas it is called 'recognition' when the event is given and the contextual information (setting, list) is required (Hollingworth, 1913).

To sum up, the picture superiority effect appears to substantially increase memorability since storing or retrieving pictures from long-term memory is more effective. In addition, recall for recent pictures is higher than recent words which apparently mean that retrieving pictures from short-term memory is even better (Paivio, Rogers & Smythe, 1968). According to Renaud and De Angeli (2009), *"humans have a vast, almost limitless memory for pictures which they remember far better and for longer than words"*. Thus, types of authentication that depend on graphics are likely to overcome the memorability problems that negatively affect text-based authentication. Remembering complex passwords as well as multiple passwords for different systems is a difficult task (Furnell,

2005) (Furnell & Zekri, 2006) while humans find it relatively easier to recognise images even after a period of time (Anderson, 2010b). In addition, pictorial passwords include other possible advantages, such as enlargement of the passwords space, reduction of choosing trivial passwords, difficulty to share and note down password (Gołofit, 2007). Since the mid 1990s, many graphical password schemes have been proposed aiming to enhance the password memorability and strengthen the security. More recently, some graphical password approaches have started to gain popularity as they are assumed to have desirable usability and memorability properties (Von Zezschwitz, Dunphy & De Luca, 2013) (Chiang and Chiasson, 2013). That is inline with the revolution of online services and mobile devices that demand friendlier alternatives to traditional methods.

3.2. Categorisation of graphical authentication

Researchers have mainly categorised graphical password authentication based on the cognitive tasks used to remember or retrieve the password. Monrose and Reiter (2005) divided graphical authentication into three main types: image recognition, tapping or drawing and image interpretation. Whereas Suo, Zhu and Owen (2005) classified it into two categories: recognition-based and recall-based techniques. As for Wiedenbeck et al. (2005c) they expanded the aforementioned categories to include recognition, pure-recall, and cued-recall. This latter type of classification is the one this research has found most appropriate to adopt throughout the rest of the work. However, combining any of these categories is also a feasible option. Furthermore, for better clarification, this study has suggested adding some distinguishing details in a manner that involves several design aspects, as illustrated in Figure 3-1.
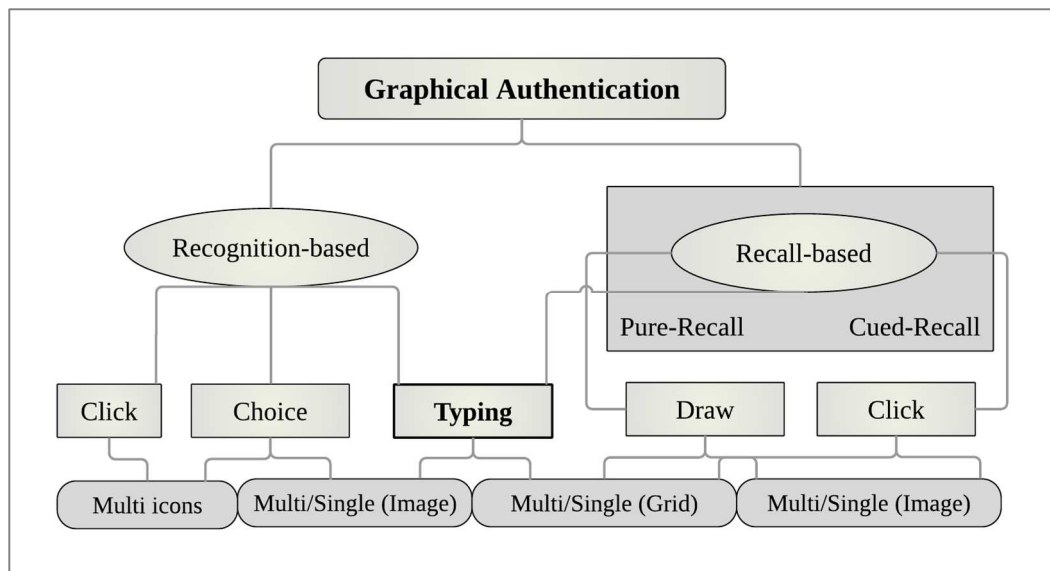
Figure 3-1: Categorisation of graphical authentication

Firstly, the input approach, for instance, is what the user needs to submit as the login information for the authentication session. The major input approaches include the following: Draw, Click, or Choice. In addition, Typing entry is another newly introduced input approach that uses keyboard/keypad in conjunction to the graphical password. Some graphical password schemes use obfuscated entry or indirect input method to obfuscate the password entry process in order to mitigate the observation attacks so that by the time an input is observed, it should be too late for an attacker to link that input data back to the password of that user (Bianchi, Oakley & Kwon, 2011) (Komanduri & Hutchings, 2008). The second aspect is the display style, which refers to the presentation mode that forms the password challenge, such as: Grid, Image, or Icon.

This work will include many graphical password schemes that fall under different categories as shown in Figure 3-2. These schemes will be reviewed and compared to enable better understanding of their characteristics, advantages and disadvantages.
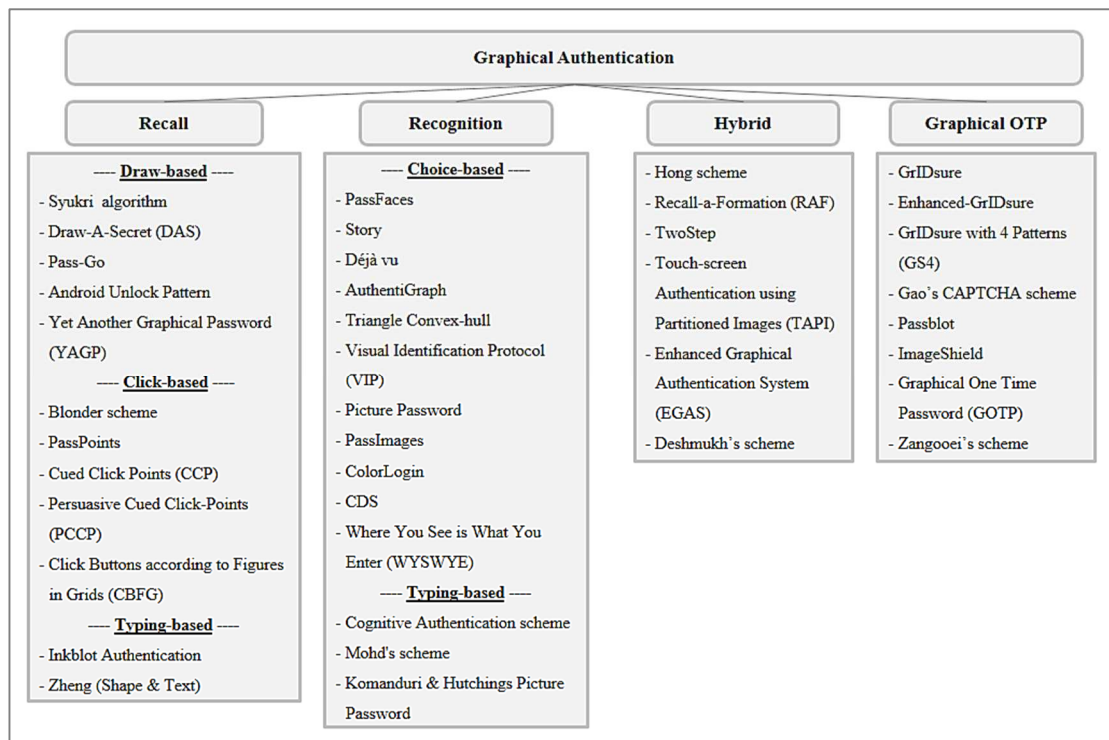
Figure 3-2: List of the discussed graphical password schemes

3.3. Recall-based techniques

The recall-based techniques are a type of authentication where access is granted by reproducing a secret – (e.g. drawing or clicking on image locations) that was previously created or chosen during the registration phase. The recall-based category can be further divided into pure-recall and cued-recall. Pure-recall is difficult in practice due to its reliance on human memory to access the information directly without aids whereas in cued-recall users are helped to remember their passwords by providing the necessary associated cues that trigger the memory (Malempati & Mogalla, 2011). As far as the password space is concerned, many recall-based schemes offer a large password space compared to that of textual passwords (Jermyn et al., 1999) (Tao & Adams, 2008).

There are three subdivisions in this type of graphical authentication that depend on the required action by the user to authenticate (Draw-based, Click-based, and Typing-based entry). Schemes of each type will be reviewed and later compered in the following subsections.

3.3.1. Draw-based schemes

In a typical model of a draw-based scheme, the registration phase would require the user to digitally draw a certain shape on a blank or gridded background. During authentication, the same shape must be redrawn correctly. Schemes of this type use different types of encoding (e.g. coordinates, grid intersections, or values of occupied grid cells) to store the drawing information and matching them later for authentication. In addition, drawing task can be carried out using different means such as computer mouse, touchpad, digital pen or fingers on touch-enabled devices.

In 1998, Syukri, Okamoto and Mambo (1998) developed a system whereby the user needs to use a mouse for signature drawing. During the registration stage, after the user draws the signature, the signing area is extracted and normalised by the system before storing it. The verification stage then begins with the user's input being taken and normalised to extract the signature parameters. It was claimed that the successful verification rate was satisfactory. In addition, a review of this scheme was included in a survey of Graphical Passwords by Xiaoyuan, Ying and Owen (2005). They stated that although this approach does not require users to memorise any information other than their own signatures, which are supposed to be hard to counterfeit but it was found that they encountered problems due to the lack of familiarity with the use of a mouse as a writing device for drawing the signature. A pen-like input device is one possible solution to this problem, but such devices are not commonly used, and it would be expensive to add additional hardware to the existing system. Small devices, such as a PDA that may already have a stylus, can benefit from such a technique.
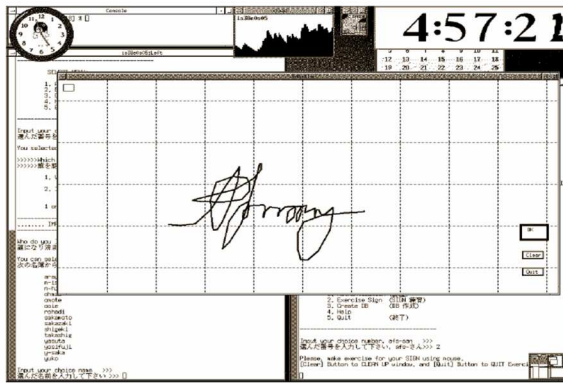
Figure 3-3: A sample of **"Syukri"** algorithm (Syukri, Okamoto & Mambo, 1998)

Jermyn *et al.* (1999) launched an authentication mechanism called "Draw-A-Secret" (DAS), which gives the user the ability to draw their desired password. Put simply, the user is required to draw a secret shape on a grid. The system then records the coordinates on the grid occupied by the drawn shape in the drawing sequence. During authentication, the user must re-draw the secret shape closely enough to the pre-stored input. The authors claim that the full password space of DAS when using an adequate length on a 5x5 grid is larger than that of the full textual password space. However, other studies (Goldberg, Hagman & Sazawal, 2002) (Nali & Thorpe, 2004) showed that forgetting the stroke order or marking adjacent cells inaccurately are considered to be the main reasons for incorrect match of the original password redrawing.
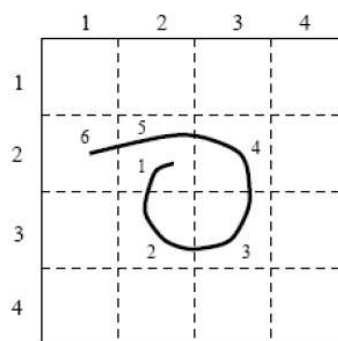
Figure 3-4: Sample password: **"Draw-A-Secret"** (DAS) (Jermyn *et al.*, 1999)

Thorpe and van Oorschot (2004) investigated the role and impact of the number of composite strokes, the length of the password and the dimensions of the grid as complexity properties in the DAS scheme. The largest impact on the password space of

39

the DAS scheme was from the stroke-count. They also found that for a fixed length password, fewer strokes result in a significant reduction in the size of the DAS password space. The password length has an impact on security but less than what the number of strokes has. The grid size provides negligible security unless supported by the use of a larger number of strokes.

Since the introduction of the DAS scheme, many researchers have utilised the concept of DAS to build new schemes with different enhancement aims (e.g. "Grid Selection" (Thorpe & van Oorschot, 2004), "Multi-Grid DAS" (MGDAS) (Chalkias, Alexiadis & Stephanides, 2006), "Qualitative Draw-A-Secret" (QDAS) (Lin et al., 2007), "Background Draw-A-Secret" (BDAS) (Dunphy & Yan, 2007), "DAS with Rotation" (R-DAS) (Chakrabarti, Landon & Singhal, 2007)).

Tao and Adams (2008) designed and improved a DAS algorithm named "Pass-Go". This scheme retains the advantages of DAS whilst adding some extra security features. Pass-Go is a grid-based scheme and is referred to as a matrix of intersections since passwords are drawn using grid intersection points. Grid lines and intersections are displayed as dot and line indicators to eliminate the impact of small variations in the input trace. The password encoding is formed, similarly to DAS, by aggregating the sequence of intersections, movement encodings, pen-up separator code, in addition to adding colour codes (if applicable). Furthermore, Pass-Go achieved stronger security and better usability. According to Gao et al. (2013), this algorithm offers a large full password space with additional parameters, such as diagonal movements and pen colour, to further increase the theoretical password space.
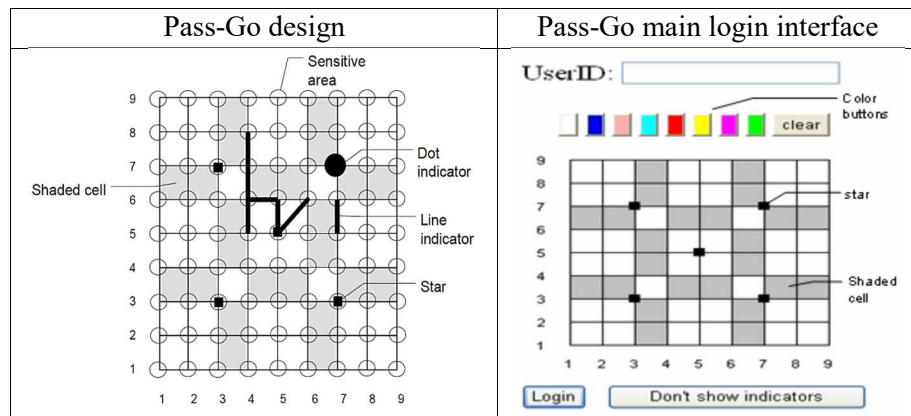
Figure 3-5: "Pass-Go" scheme (Tao & Adams, 2008)

In the same context, the authors also proposed some variations on the basic Pass-Go scheme which offer either better usability or stronger security. First was "PassCells" which replaces the grid with a matrix of cells making the boundary of sensitive areas visible to users. Second, was called "Cell Indicator" where the right button of a mouse may be used to choose cells in the grid. Last, was named "Curved Line Indicator" in which an invisible cell centre point is defined as an area surrounding the centre of each cell in a grid that made the drawing of a curved line possible.

Moreover, a number of researchers have investigated the Pass-Go scheme and have pointed out some improvements (i.e. "Background Pass-Go" (BPG) (Por, Lim & Kianoush, 2008), "Multi-Grid Background Pass-Go" (MGBPG) (Por & Lin, 2008)).

"Android Unlock Pattern" is an adapted scheme of Pass-Go with some slight modifications to fit for the smaller screen sizes of mobile devices (Biddle, Chiasson & van Oorschot, 2012) (Uellenbeck et al., 2013). The scheme operates by presenting a 3×3 grid that contains nine dots. To enrol, a pattern must be chosen by drawing lines to connect the dots. During authentication, the user has to recall the pattern and redraw it in the correct sequence. The system enforces some constraints to create an acceptable pattern. The length of a pattern should be between 4 and 9 connected dots, each dot can be selected only once, jumping over an unselected dot is not allowed, and a selected dot

can be used to reach another unselected dot. According to Aviv et al. (2010), there are 389,112 distinct patterns in the total size of the pattern space. Their research investigated the smudge attacks that exploit the oily marks of finger touches left on screen devices. The outcomes of the study stated that by using smudge attack, the pattern can be recovered either fully or partially. In addition, the gathered information from a smudge attack can be used to increase the chance of guessing user's patterns. However, the success of a smudge attack is conditioned to a prior physical obtainment of a user's phone which is not always feasible (Chiang & Chiasson, 2013).
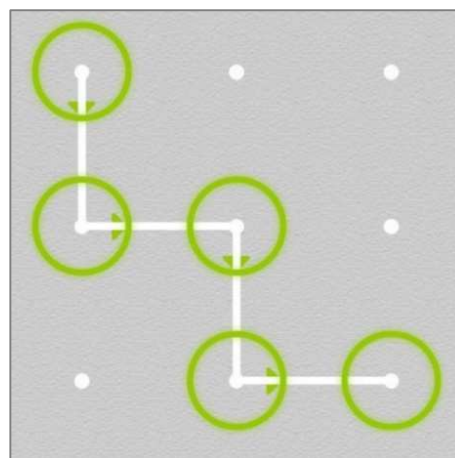
Figure 3-6: "Android Unlock Pattern" scheme

Haichang et al. (2008) inspired by the DAS technique and proposed a position-free graphical password strategy called "Yet Another Graphical Password" (YAGP). This approach has the advantage of free drawing positions that permit redrawing anywhere. Also, it attains a large password space through the use of more precise grid cells. The YAGP password is formatted based on the extended concept of DAS neighbour cells, which means that every stroke of a drawing is composed of one of three types of movement elements: pen-down, pen-move and pen-up. Each pen-movement obtains a code represented by the numbers 1, 2, 3, 4, 6, 7, 8, 9 according to the last neighbour cell. The code '5' is used to represent pen-up and pen-down in a stroke. When authenticating the re-entered drawings, YAGP provides a more flexible judgment mechanism. Still, the difficulty of redrawing the password precisely is a drawback of the YAGP scheme.
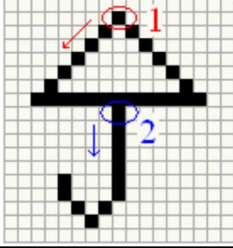
| The neighbour grid | Example: the code of the string of the whole drawing is: '577777766666666666611111155888888771125' |

Figure 3-7: The **"YAGP"** strategy (Haichang *et al.*, 2008)

A review of additional draw-based schemes can be found in 'Appendix A' including "PassShapes" by (Weiss & Luca, 2008) and Touchscreen Multi-layered Drawing "TMD" by (Chiang & Chiasson, 2013). Moreover, the Android unlock pattern scheme has drawn the interest of many researchers, thus several studies to enhance this scheme have been published. Most of which have been reviewed and added to 'Appendix A' including (von Zezschwitz, Dunphy & De Luca, 2013), (Uellenbeck *et al.*, 2013), (Andriotis et al., 2013), (Andriotis, Tryfonas & Oikonomou, 2014), (Schneegass et al., 2014), (Song et al., 2015), (Zezschwitz et al., 2015), and (Siadati et al., 2015).

3.3.2. Click-based schemes

A click-based scheme is usually formed by a set of user-selected click-points. During the registration process, the system first displays an image consisting of enough details to typically offer a wide range of click points. Then the user can create a password by clicking on several secret locations on that image. To authenticate, the approximate areas of the pre-chosen locations must be clicked. In such schemes, the image can play an assistant role for the users to easily recall their passwords which makes these schemes more convenient to use than pure recall.

Blonder (1996) is regarded as the founder of the graphical authentication notion. He developed a graphical password scheme that allows users to create a password by clicking

on various permitted locations on an image. This method is a cued-recall since the image plays an important role in assisting users to retrieve their passwords. One drawback of Blonder's scheme is the limited password space, which is affected by the predefined boundaries that restrict user selection of clicking areas.
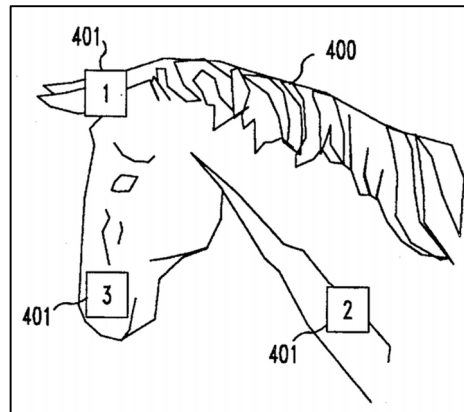
Figure 3-8: "Blonder" scheme (Blonder, 1996)

Wiedenbeck et al. proposed a further extension of Blonder's design known as "PassPoints" (Wiedenbeck *et al.*, 2005c) (Wiedenbeck et al., 2005b) (Wiedenbeck et al., 2005a). In this scheme, arbitrary images are allowed to be used and the predefined boundaries are eliminated to expand the clickable areas of the image background. As a result, users are able to make free clicks anywhere on an image. Additionally, the tolerance area around each chosen location is calculated to enhance usability and security. To achieve that, the 'robust discretization' technique (Birget, Hong & Memon, 2004) (Birget, Dawei & Memon, 2006) was implemented with three overlapping grids. This method ensures the determination of the tolerance square of a click-point and the corresponding grid. As a result, attempts to enter approximately correct click points (passwords) are accepted and regarded as an exact match to the originally stored click value despite the slight difference between the original click and the repeated one.

In short, PassPoints password is composed of a number of anywhere click points on a single image. In order to gain authentication, the user needs to accurately click on all the preselected spots within the defined tolerance of each chosen area. Interestingly, the idea

of allowing the use of any type of images increases the amount of memorable password space.
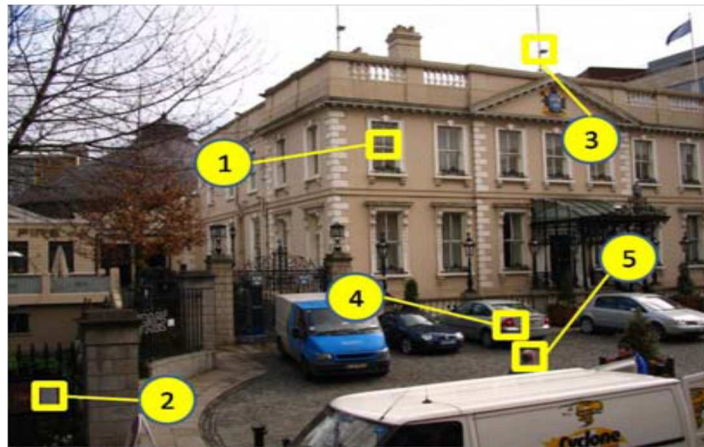
Figure 3-9: A sample of **"PassPoints"** Scheme (Gani, 2010)

Following the launch of the PassPoints scheme, several user studies including both lab and field ones have been carried out by a number of researchers to examine different aspects of the PassPoints system. Wiedenbeck et al. conducted a number of user lab-studies to examine PassPoints system's usability compared to textual password, measure the impact of image choosing on usability, and define the minimum size that can be assigned to the tolerance square (Wiedenbeck *et al.*, 2005c) (Wiedenbeck *et al.*, 2005a). They concluded that the memorability of both text-based and graphical passwords was almost similar. Next conclusion stated that although using a smaller tolerance square led to a larger password space, but too small squares pixels turn into unusable system. Last, password memorability was found not that much affected by the image choice.

Other studies were carried out by Chiasson, Biddle and van Oorschot (2007) involving both lab and field studies to explore the claimed usability when using a wider range of images as well as collecting information about users' chosen passwords (click points). In the field study, the scale of participation was large to practically test the click-based graphical passwords. The studies' conclusion stated that there were differences between results; the result of the lab study was mostly positive compared to the field study result.

Nevertheless, the studies showed a good usability level in terms of success login rates and time duration for password-entry and positive participants' opinions. Additionally, it was confirmed that the accuracy of targeting click-points was higher than previously suggested which may lead to accepting smaller tolerance squares. Finally, success rates were found influenced significantly by the choice of images in contrary to previous works. Furthermore, interference of multiple passwords was found apparently problematic due to the lower success rates recorded when using more than one password.

Thorpe and van Oorschot (2007) extended the study domain to focus on the security of click-based graphical password schemes such as PassPoints. Mainly, the security examinations included the impact of the use of various background images as well as the different techniques to guess users' passwords. As a result, an empirical evidence of the existence of hotspot points (the most popular clicked areas) for many images was provided. On top of that, two diverse types of attack exploiting hotspots were explored and evaluated: (i) a "human-seeded" attack which uses a small set of users to harvest click-points information in order to attack other larger targets, and (ii) a purely automated attack utilising image processing techniques to help predicting hotspots automatically for efficient exhaustive search. Although the human-seeded attack was more effective, but the entirely automated attack could also be an interesting tool possibly used as a proactive password checker. Overall, whenever an offline attack is absent then click-based graphical password schemes may still be considered a suitable alternative solution for authentication.

Devlin et al. (2015) studied the extent of the predictability of PassPoints password based on knowledge of the user. The result proved that predicting PassPoints password is somewhat possible. In addition, the tendency of users to select similar password points was observed which is responsible for creating hotspots. Another finding was the influence of the background image on the user selection of the click-points.

Chiasson, van Oorschot and Biddle (2007) introduced a cued-recall graphical password technique called "Cued Click Points" (CCP) as an alternative method to PassPoints. The characteristic of the CCP scheme seem to be drawn from a combination of several techniques: PassPoints, Passfaces (Passfaces Corporation, 2015b) and Story (Davis, Monrose & Reiter, 2004). In CCP, a password is composed of one click-point per image for a series of images. Thus, users need to click on one point of each image rather than on multiple points of a single image. The discretization method (Birget, Hong & Memon, 2004) (Birget, Dawei & Memon, 2006) was also used here. Displaying the next image depends on the previously clicked-point, so users are cued during logging in process as to whether they are on the correct path or not. Being on an incorrect path means that a wrong point was clicked and therefore a wrong image is displayed, but more importantly an explicit indication of authentication failure is only shown after the final click to avoid any potential online attack. However, CCP is susceptible to shoulder-surfing attacks like most other graphical passwords. Observation of username, image sequence and click-points is enough to ensure supplying the attacker with all the information needed to break into the account. Attacks can exploit the areas that have a higher probability of being selected by users as part of their passwords, which are also known as (hotspots). With CCP, attacks based on hotspot analysis have been made more challenging due to the significant increase in the number of images and the associated difficulty of analysing corresponding images on multiple levels throughout the authentication process.
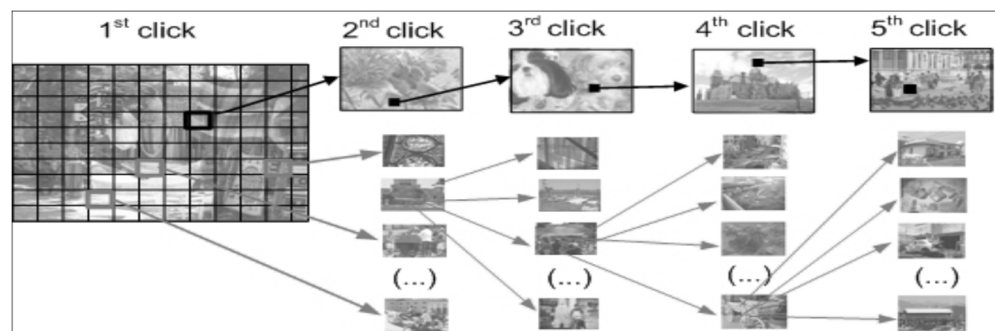
Figure 3-10: "Cued Click Points" (CCP) passwords: a choice-dependent path of images
(Chiasson, van Oorschot & Biddle, 2007)

Chiasson et al. (2008) used CCP as a base system to implement a variation called "Persuasive Cued Click-Points" (PCCP). The motivation behind this idea was to persuade users to choose random passwords as well as to make the selection of hotspots for all click-points much harder to provide better security. It has the same CCP functionality but differs slightly in the password creation stage when only a small square viewport area, randomly positioned on the image, is enabled to accept clicking while the rest of the image is dimmed.
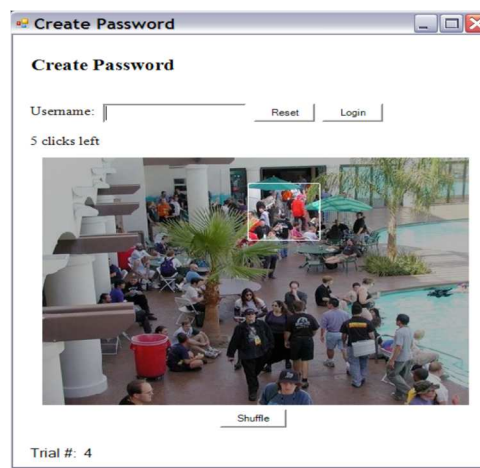
Figure 3-11: "Persuasive Cued Click-Points" (PCCP) (Chiasson *et al.*, 2008)
Password creation interface with the viewport highlighting a portion of the image.

Liu et al. (2011) proposed a new cued-recall graphical authentication technique named "Click Buttons according to Figures in Grids" (CBFG). To register, the user needs to choose either single or multiple passimages (max four images). The selected passimages are partitioned into a 12×8 grid matrix then presented again to the user to select a number of password cells (pass-cells). Last registration step involves the selection of a start-icon which acts as an indicator to begin entering password sequence. As for the authentication, this phase consists of 4 background images and one centric icon. Each cell displays a random number between 0 and 9. The actual login process does not start unless the correct pre-chosen start-icon become on display. Afterwards, the user should start entering the password by looking for the numbers on the pass-cells and then click on the corresponding numeric buttons on the side of the screen in any order.

The performance of the scheme was evaluated through a lab experiment with 24 participants. First statement showed a reasonably high success login percentage of 92.3% and 21.4 seconds of average login time. After ten days, a memorability test was conducted in which users were asked to re-login again for several times. 87.5% of the participants were able to recall their credentials correctly with a mean login time of 26.7 seconds. Moreover, two further security experiments were undertaken. In the first test, users were asked to observe their counterparts' passwords and record information that may help them to attack the account. The result indicated that all attempts failed to login using the collected information within 3 given times. In the second test, users' input sequences were recorded and an intersection analysis attack was carried out on them. By analysing the outcomes, it was found that this type of attack is ineffective.
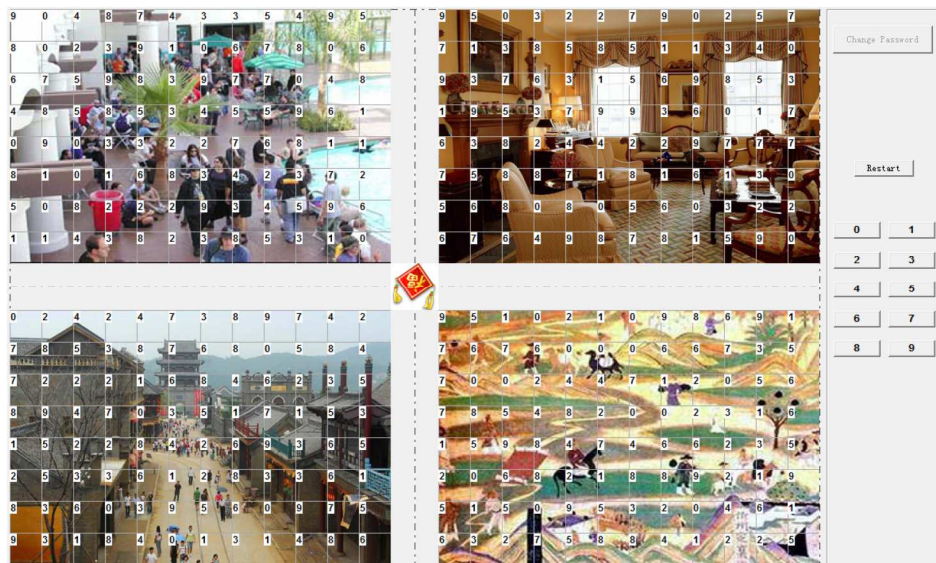
Figure 3-12: "CBFG" authentication screen

Additional click-based schemes were reviewed and added to 'Appendix A' including "Multi-Factor Graphical Authentication" by (Sabzevar & Stavrou, 2008), "Multitouch Image-Based Authentication on Smartphones" (MIBA) by (Ritter et al., 2013), and "Tri-Pass" (Yesseyeva et al., 2014).

3.3.3. Typing-based recall schemes

An interesting feature to be introduced in this research is the use of keyboard/keypad as an input mechanism instead of using the mouse, which is the method commonly used with graphical passwords. In this section, attention is paid to those schemes that utilise graphics as an authentication means in addition to the use of keystrokes as an entry approach to submit the necessary access data. According to the study conducted by Tari, Ozok and Holden (2006), replacing the regular use of a mouse for data entry in many graphical password schemes with a keypad is effective in terms of reducing the risk of a shoulder-surfing attack. In other words, this makes it more difficult to gain enough information about the password since both keystroke logger and screen scraping are required. Several schemes have already made use of this approach each of which will be reviewed next.

Stubblefield and Simon (2004) outlined a simple cued-recall scheme called "Inkblot Authentication". This scheme works as an aid for the user to create and memorise strong textual passwords by generating and displaying a series of inkblots. During password registration, the user is asked to associate each of the ten displayed inkblots with a memorable word. The final password is derived from concatenating these words in a certain manner (e.g. first and last letters of each word). This scheme protects users from shoulder-surfing attack since an attacker cannot obtain the password by only watching the inkblots without knowing the word associations. Unfortunately, using a small set of fixed blots is considered one of the scheme's limitations as it might prevent the use of the system in multiple environments due to the difficulty of keeping track of several associations for each blot by the user. One drawback of this scheme is that an attacker can build a list of popular letter pairs associated with each substitute image by replacing inkblot images sent to a user with other inkblot images. Subsequently, the list can be used to crack users' passwords. Another problem is that the number of printable ASCII

characters available for association is limited. However, these issues can be solved through the use of an algorithm that produces an almost limitless supply of images similar to inkblots to replace the static images.

Figure 3-13: Example of **"Inkblot"** Authentication login screen (Stubblefield & Simon, 2004)

Zheng et al. (2010) proposed their authentication scheme based on Shape and Text. This scheme provides a grid with characters that requires users to choose shapes of strokes as the original passwords and finally utilises traditional input devices to login with text passwords. All what a user needs to remember for authentication is the pre-chosen shapes and strokes. During login, the grid will be filled with some similar symbols like numbers or characters. The input of a successful login needs to match the correct symbols appeared in the user's original sequence of the grid. With regard to security, the scheme reported being highly resistant to shoulder-surfing as the attackers must record both of the login grid and the entire typing process in order to obtain the original shape password. In addition, the scheme is resistant to brute force and random click attacks.
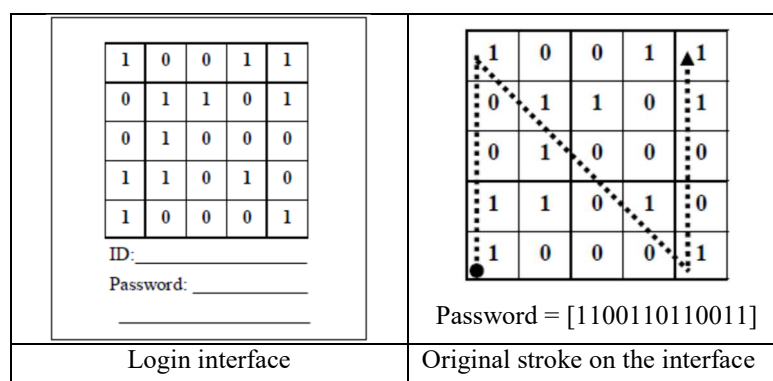
Figure 3-14: Zheng's scheme (Shape & Text) (Zheng *et al.*, 2010)

Although only a couple of schemes that have implemented this supportive technique (utilisation of keypad/keyboard typing as a means of password entry) which works alongside the main authentication mechanism were included in this subsection, however, more schemes of this type will be discussed later in section 3.6.

3.3.4. Comparative summary of Recall-based techniques

Table 3-1, Table 3-3 and Table 3-4 show comparative summaries of the recall-based technique involving three main aspects: technique attributes, security, and usability. The data was harvested from the existing literature, which explains why some schemes were included in and others excluded from some comparisons depending on the availability of information. In this regard, Renaud et al. have also expressed the same limitations as: *"These levels are based on the literature which often reports findings that are extremely difficult to compare, so the comparison should not be considered definitive, but rather based on an understanding of whether the approach is prone to show vulnerabilities. Moreover, it becomes apparent that there are many aspects that do not allow a rating due to missing data or data that only allows a very rough estimation instead of a real assessment"* (Renaud et al., 2013).

The layout of the comparison tables was aimed to be informative and expressive. Table 3-1 includes a comprehensive comparison of schemes based on their attributes. The data shows that the graphical authentication notion was first introduced in 1996 and since then, the number of research inventions in the area of recall-based graphical authentication has been increasing over the time. One of the reasons behind that might be due to the fact that in recent times mobile devices with touch screen and stylus have been becoming more popular which facilitate the drawing and clicking tasks. It can be also inferred from the results of the conducted comparison that there is a general pattern linking the categories,

approaches and styles of the schemes, as illustrated in Table 3-2. For instance, the majority of the pure-recall categorised schemes use a drawing with grid approach whereas most schemes within the cued-recall category utilise clicking with image approach.

	Graphical Password System	Year	Category		Approach			Style	
			Pure-Recall	Cued-Recall	Draw	Click	Typing Entry	Grid	Image
1	Syukri Algorithm – (draw a signature)	1998	✓	-	✓	-	-	✓	-
2	Draw-A-Secret (DAS)	1999	✓	-	✓	-	-	✓	-
3	Pass-Go	2008	✓	-	✓	-	-	✓	-
4	Multi-Grid Background Pass-Go (MGBPG)	2008	-	✓	✓	-	-	✓ M	✓
5	Yet another Graphical Password (YAGP)	2008	✓	-	✓	-	-	✓	-
6	PassShapes	2008	✓	-	✓	-	-	PAD	
7	TMD	2013	✓	-	✓	-	-	✓	-
8	Blonder Scheme	1996	-	✓	-	✓	-	-	✓
9	PassPoints	2005	-	✓	-	✓	-	-	✓
10	Cued Click Points (CCP)	2007	-	✓	-	✓	-	-	✓ M
11	Persuasive Cued Click-Points (PCCP)	2008	-	✓	-	✓	-	-	✓ M
12	Multi-Factor Graphical Authentication	2008	-	✓	-	✓	-	-	✓
13	CBFG	2011	-	✓	-	✓	-	✓	✓ S/M
14	MIBA	2013	-	✓	-	✓ M	-	-	✓ M
15	Tri-Pass	2014	-	✓	-	✓	-	-	✓
16	Inkblot Authentication	2004	-	✓	-	-	✓	-	✓ M
17	Zheng (Shape & Text)	2010	✓	-	SHAPE		✓	✓	-

M= Multi

Table 3-1: Attributes comparison of Recall-based schemes

Category	Approach	Style
Pure-recall	Draw	Grid
Cued-recall	Click	Image

Table 3-2: A descriptive linking pattern

Table 3-3 presents some of the security features and vulnerabilities that were covered most by the existing schemes. Unfortunately, it was found that a vast amount of information is missing due to the lack of details published on the security aspects of the schemes as well as the absence of general standard for security requirements and recommendations, which is surprising for such an important authentication domain. This had a negative impact on the evaluation of the schemes. However, the security features were compared on the basis of the following factors:

- **Multiple rounds:** pass-clicks or drawings are distributed over multiple screens (i.e. one click in each page).

- **Hash function:** it is a type of cryptography that allows encrypting data in a way that it is difficult to invert.

In terms of the vulnerability comparison, it was based on the susceptibility to various types of attack such as:

- **Shoulder-surfing:** The use of direct observation techniques to obtain victims' passwords or other security information.

- **Guessing:** The ability to guess another user's password by predicting higher probability passwords.

- **Dictionary attack:** In text-based password, a dictionary of common words is used to identify the password of a legitimate user. In a similar way, a dictionary of graphical password can be built by the most clickable areas or the common drawings.

- **Spyware:** A hidden unauthorised software component that capture information about user's activities such as keyboard, mouse, or screen outputs.

- **Hotspots:** The selection of specific areas in an image by a high percentage of users that make them more predictable. Combinations of these click points with higher probability can be used to build a password dictionary.

#	Recall-based Graphical Password System	Security Features & Vulnerabilities							
		Multiple Rounds	Hash Function	Shoulder-Surfing Resistant	Difficult to Guess	Dictionary attacks Resistant	Safe against: Spyware – Recordability	Safe against Hotspots	Other aspects
1	Draw-A-Secret (DAS)	-	✓	-	-	-	-	-	
2	PassPoints	-	✓	-	-	✓	-	✗	
3	Cued Click Points (CCP)	✓	✗	✗	-	-	✗	✗	
4	Persuasive Cued Click-Points (PCCP)	✓	-	-	-	-	-	✓	
5	Pass-Go	-	-	✓	-	✓	-	-	
6	Yet another Graphical Password (YAGP)	-	✓	✓	-	-	-	-	
7	Multi-Factor Graphical Authentication	-	✓	✓	✓	✓	✓	✓	Resistant to: physical security, Brute force, social engineering attacks
8	CBFG	-	-	✓	✓	-	-	-	Safe against intersection attack Offer large password space
9	MIBA	✓	-	✓	✓	-	-	-	Resist brute force attacks
10	Zheng (Shape & Text)	-	-	✓	✓	-	✓	-	Resist brute force & random click Offer large password space

Table 3-3: Comparison of security features and vulnerabilities of Recall-based schemes

According to Table 3-3, shoulder-surfing and guessing attacks seem to be the types of attacks that most recall-based research attempted to resist. This might indicate that many recall-based schemes are more concerned about these types of attacks. Additionally, dictionary and brute force attacks are other types of threats included in a number of studies of this authentication category. Some schemes of this type seemed concerned about hotspots and spyware attacks as only a few of them have reported related data. Another finding was the limited use of multiple rounds and hashing function with the recall-based techniques.

	Recall-based Graphical Password System	Usability Features						
		Arbitrary Click	Input Tolerant	Easy to use	Memorability	Mnemonic	Lab(L) /Field(F) Study	Other Features\ Limitations
1	Draw-A-Secret (DAS)	-	×	×	×	×	-	On Paper - Difficult password entry
2	PassPoints	✓	✓	-	✓	✓	L / F	User-provided images
3	Cued Click Points (CCP)	✓	✓	-	-	-	L	
4	Persuasive Cued Click-Points (PCCP)	✓	✓	-	-	-	L	Implicit Feedback
5	Pass-Go	-	✓	✓	✓	-	F	
6	TMD	-	-	✓	✓	-	L	
7	CBFG	-	-	×	✓	-	L	Multiple background images

Table 3-4: Usability features comparison of Recall-based schemes

In Table 3-4, recall-based schemes are compared against major usability features on the basis of the following factors:

- **Arbitrary click:** This feature is specific for click-based schemes. The predefined click areas limit the password space. Arbitrary click allows clicking on any location on the image and thus more choices are offered.

- **Input tolerant:** This is a click-based feature. Some schemes are equipped with a tolerance around the click points which make them easier to click and therefore more flexible and usable system.

- **Ease of use:** How easy it is to perform an authentication task in a natural and friendly manner.

- **Memorability:** The ability to remember a password either on a short or long term.

- **Mnemonics:** The use of any aid to help human memory to better retain and remember information. They come in different forms and can ease the memorisation of many information types.

- **Study type:** Research evaluation can be carried out in a laboratory which provide more control on the running activities and allow better research-related observations.

The second type of study is a field study which is typically conducted in the wild to gather real user performance data usually over longer period of time.

It is clear from Table 3-4 that the number of the compared schemes against usability has dropped to less than a half. Moreover, only a small number of them have provided a reasonable amount of details (e.g. Passpoints and Pass-Go). At the same time, these two schemes were the only ones to undertake field studies which emphasise the importance of this type of study for producing sufficient data and proofs.

One of the issues with the beginnings of click-based technique was the tolerant square area. Apparently, this was taken into account with most of the subsequent schemes which managed to overcome the issue. Similarly, the predetermined clicking area used to be one of the main limitations of click-based schemes. This has seemingly led many techniques of this type to adopt the click anywhere technique, which in turn has helped in mitigating the consequent usability and security issues. As far as the ease of use is concerned, some schemes have claimed to be easy to use despite the fact that in some cases there was no clear report of the evaluation criteria that can independently judge whether the scheme was easy to use or otherwise. Although memorability is one of the significant usability features, it can be inferred from the comparative table that not all schemes included it into the reported work. In relation to this, mnemonics have been used with the aim of providing an aid to facilitate the recall of the required authentication task. In most cases, as can be depicted from the comparison data, the use of mnemonics is mostly linked with good memorability levels, which means that this can be regarded as a complementary feature. Moreover, enabling users to upload and choose their own images is another feature that has not been found to be widely implemented in recall-based schemes for several reasons, such as the avoidance of bias selection or predictability through the pre-knowledge of personal preferences.

3.4. Recognition-based technique

Image recognition schemes have been proposed as a replacement for precise password recall to minimise the burden on users' cognitive memory and thus reduce the amount of mistakes they make and boost their usability experience (Dhamija & Perrig, 2000). Nevertheless, schemes of this kind have their own problems too. To ensure easier recognition task, the target images should be semantically different from the distractors. However, in order to avoid the possible predictability, the semantic difference should not simplify the distinguishing task for intruders (Renaud, 2004).

Generally, there are two stages involved in this type of authentication technique. The first stage is registration, where a set of images are presented to users. They are required to form their password by selecting some target images from within the displayed set. The second stage is authentication, which involves single or multiple rounds. At each login round, users are asked to recognise and identify the pre-defined target images, which are usually presented among other decoy-images.

Normally, this sort of scheme requires the presentation of the same images within each panel to avoid an obvious determination of repeatedly appearing images in the panel. Additionally, the images should be displayed randomly over the panel to ensure that user's selection is dependent on the recognition of the image itself not on the position occupied by the image. With regards to the password space, the majority of recognition-based schemes are limited in size, which makes them suitable for authentication only when accompanied by an online reference validation mechanism to prevent an automated search (Monrose & Reiter, 2005).

3.4.1. Choice-based schemes

A choice-based approach refers to the action where the user needs to select a required image that is usually achieved by mouse tapping on the target image. A plenty of schemes utilising choice-based approach have been developed and studied. A decent number of them are reviewed and compered next.

Passfaces Corporation developed an authentication technique based on facial recognition called "PassFaces™" (Passfaces Corporation, 2015b) (Passfaces Corporation, 2015a). In simple terms, the system assigns the user with a random set of human face images from a large portfolio of face images as a login password. Next, the user is presented with a panel consists of eight decoy face images plus one face image from the previously assigned password face images. The authentication requirement is met when users correctly recognise and identify all of their PassFaces in each repeated round by simply clicking anywhere on the known face image.
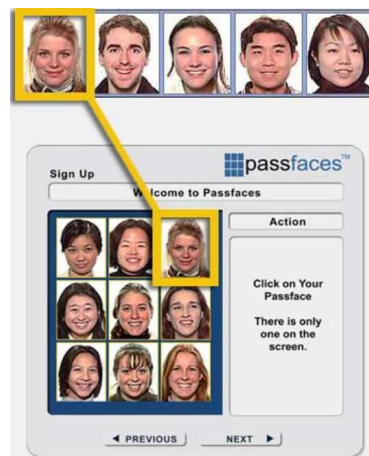
Figure 3-15: "PassFaces" Scheme (Passfaces Corporation, 2015a)

A number of research studies have investigated the PassFaces scheme in relation to some significant usability and security issues. Brostoff & Sasse (2000) performed a field study to evaluate the PassFaces system which showed that the login errors rate when using PassFaces was only one third of the rate compared to that in alphanumeric password. Despite the less frequent access to the system, the study showed a better memorability

than traditional passwords even over longer period of time in accordance to the previous studies by Valentine as stated by the authors of this study.

In a lab study, Tari, Ozok and Holden (2006) compared the risk of shoulder-surfing on PassFaces, textual password, and PINs. The findings indicated that adopting a keypad for data entry with PassFaces instead of the regular mouse click was very effective mitigation to shoulder-surfing. By implementing a keyboard entry, an extra challenge is added before an attacker since in this case keystroke logger and screen scraping are both needed to gain enough information about the password entry.

Dunphy, Nicholson and Olivier (2008) looked into the reality of the claim that graphical passwords are secure against both verbal and written disclosure. In PassFaces, the absence of cues that stand out (background, eye glasses, and clothing) is an essential characteristic of facial graphical passwords to reduce the users' tendency of revealing passwords either by writing them down or verbally describe them to others. Notably, it was found that just a few participants were able to login based on verbal descriptions of the portfolio images. In addition, when the system uses a strategic manner to select decoys similarly matching the portfolio image, the participants were less likely to identify the correct portfolio images within the panel. Nevertheless, other forms of attacks such as social engineering can still induce users to share their password images through capturing photographs or screenshots.

Everitt et al. (2009) chose PassFaces for their evaluation to study the interference of multiple passwords. Over several weeks, email messages used to be sent to the participants prompting them to login to 4 various fabricated accounts on a diverse schedules basis. With more frequent logging-in and practicing of each new password over the study period, users managed to remember their passwords successfully.

Davis, Monrose and Reiter (2004) invented another graphical password scheme called "Story" to compete with the 'Face' system that was similarly modelled after PassFaces scheme. This approach uses various image categories instead of restricting the choices to a single category, such as human faces. A story-based password is composed of a sequence of images chosen by the user to create a story, as a memory aid, from a single pool of images each of which is from distinct image category that depict objects from daily life (cars, food, animals, etc.). The authentication process runs for several rounds to allow the user to select the predetermined images in the correct sequence. However, the results of the conducted field study revealed that users have recorded exploited patterns, such as gender-related desires. In addition, remembering a story password proved difficult in addition to the password sequencing, which was the most frequently occurring error. As for the password space of this scheme, it can be exhaustively searched in a short time whenever an offline dictionary search is possible. Hence, making use of such an approach requires a trusted online procedure for mediating and confirming guesses. In regards to the Face system, the study warned against permitting users to choose passwords without a method to mitigate the bias choices.

Figure 3-16: "Story" Scheme (Davis, Monrose & Reiter, 2004)

Dhamija and Perrig (2000) developed a graphical scheme called "Déjà vu" utilising the Hash Visualization algorithm 'Random Art' that produces abstract structured images from meaningless strings that are referred to as seeds. The difficulty associated with

writing images down and sharing them with others is an important security feature of Random Art images. There are three stages in the Déjà vu scheme: portfolio creation, training and authentication. To begin with, users are required to create an image portfolio by selecting a number of desired images among a set of different sample images. During authentication, the system displays a challenge set consisting of the predefined images plus other decoy images. The images that form part of the portfolio should be correctly identified in order to ensure authentication. As a matter of fact, the scheme was designed to store the hashed values in the system not the images. Thus, a weakness point of the proposed system has been reported in relation to the seeds of the portfolio images of each user being stored on the server in cleartext.
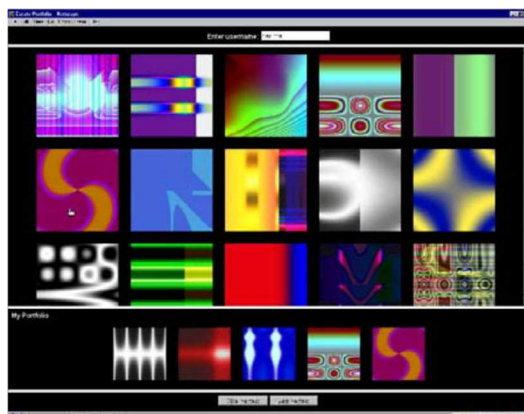
Figure 3-17: "Déjà vu" technique (Dhamija & Perrig, 2000)

Pierce et al. (2003) prototyped an alternative authentication solution called "AuthentiGraph". It is an extended design of the Déjà vu scheme that borrows concepts from text-based passwords on the one hand and smartcard and biometrics on the other. AuthentiGraph uses a server key to generate unique random character bitmaps containing all characters that the login or password may include. In order to authenticate, the user is asked to identify and click on the right characters in the correct order. A set of (X,Y) coordinates representing the mouse selection of the character bitmaps is then transferred to the server to authenticate the user. Moreover, the character bitmaps are not statically positioned, which means that in each authentication attempt the coordinates' data will be

different. However, the difficulty of identifying and locating the characters within a congested bitmap compared to character identification on a keyboard is considered to be one of the system's disadvantages in addition to being vulnerable to shoulder-surfing and observation attacks. An adjusted system that allows various types of information to be presented and chosen was proposed. For example, characters are replaced with simple shapes like squares and circles along with colour variations.

| (Character bitmap) | (Shape/Colour bitmap) |
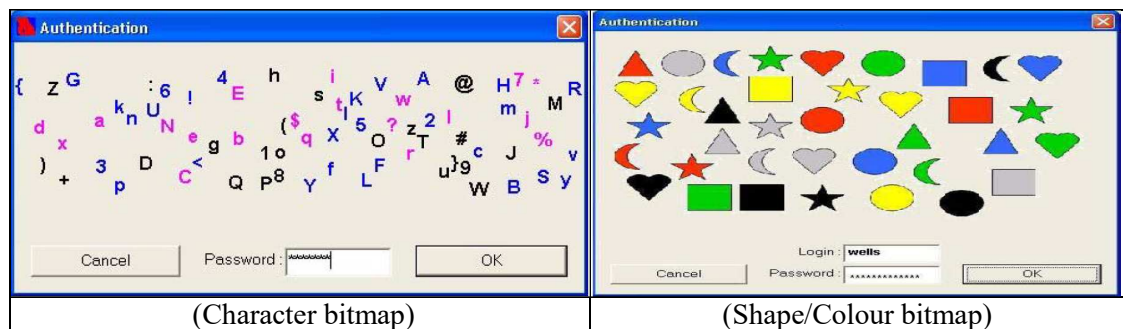
Figure 3-18: "AuthentiGraph" Scheme (Pierce *et al.*, 2003)

In 2007, Minne et al. (2007) investigated the usability of the AuthentiGraph scheme by examining the effect of different interface designs. 20 students participated in the study, which comprised of user trials and surveys. The result showed that colour coordination in the grid arrangement was effective in increasing the accuracy of locating the required characters. In addition, participants were asked about the scheme's security where 85% stated they would use the scheme if it was proven to be secure.

Sobrado and Birget (2002) designed three shoulder-surfing resistant graphical password techniques. The first of them was the "Triangle scheme", where pre-chosen pass-objects form a convex-hull. The user needs to click somewhere inside this area to complete the authentication process. In the second scheme, which was called the "Moveable frame scheme", authentication is achieved by twirling the frame until all the pass-objects are located on a straight line. The last scheme was "Other special geometric configurations". This depends on the intersection of invisible lines formed by four previously chosen pass-

objects that produce a convex quadrilateral inside of which the user needs to click for authentication. Overall, these schemes suffer mainly from a slow login process.

Triangle scheme Convex-hull	Moveable frame scheme	The special geometric configuration
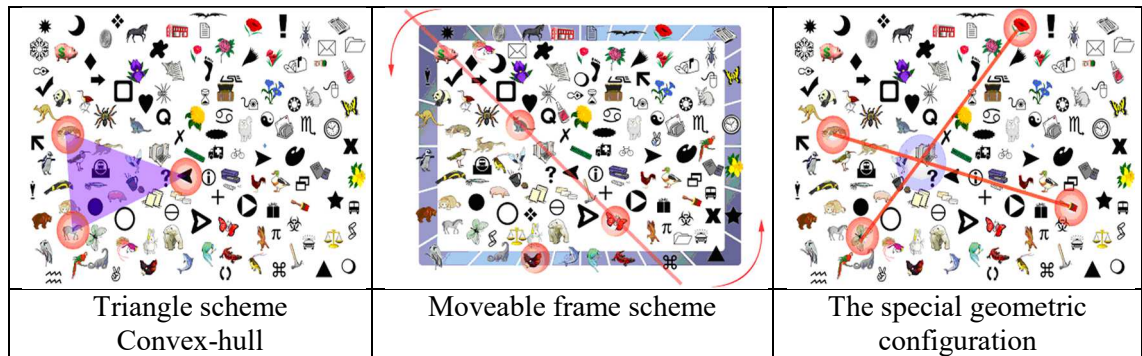
Figure 3-19: Sobrado and Birget shoulder-surfing resistant schemes (Sobrado & Birget, 2002)

De Angeli et al. presented an innovative concept for user authentication called "Visual Identification Protocol" (VIP) (De Angeli et al., 2002) (De Angeli et al., 2003). Basically, VIP was built to replace the conventional numerical authentication by pictures. An authentication attempt is successful when the user correctly selects the images that are part of their portfolio among other decoys within the display panel. Three different systems were implemented to allow authentication through multiple rounds or sequencing of images. The first proposal was VIP1, which always displays the four secret pictures of the user in fixed locations on the visual keypad. The user is required to memorise the sequence of their password pictures and must enter them in the correct order. VIP2 differs by locating the four password pictures randomly over the visual keypad. However, the concept is a bit different in VIP3, where a portfolio of eight pictures is assigned to the user. At every login attempt, a 4x4 challenge set is presented to the user containing four random portfolio pictures together with additional 12 distractors. To authenticate, users have to identify their pre-set images amongst the 16 images shown on the interface in any sequence.

The authors also evaluated the usability and security of the VIP schemes in comparison with the traditional PIN. The study that involved 61 participants revealed that pictures cause less error than numbers. The sequence errors when retrieving sequences of numbers

were more frequent than when recognising sequences of pictures. Although VIP3 from among the three schemes underperformed as participants of this type were the slowest, but it provides more security features. Besides, VIP3 received a relatively good user satisfaction of over than 5 out of 7 positive attitude. Overall, in comparison with PIN, VIP was preferred by users and perceived as more secure and memorable.
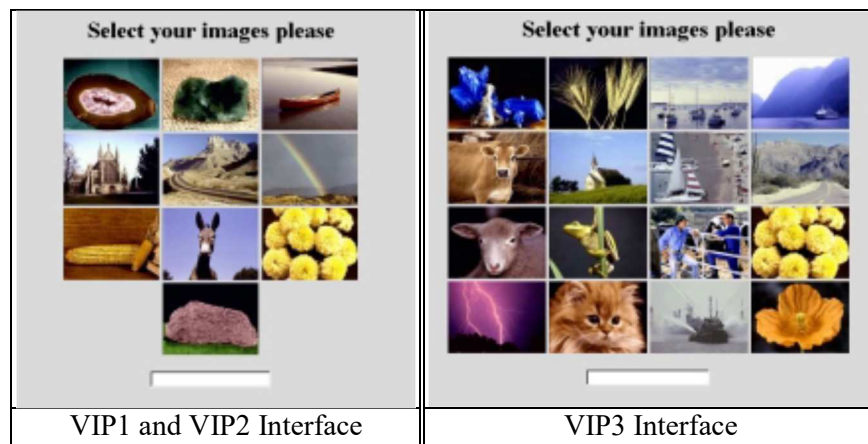
Figure 3-20: "Visual Identification Protocol" (VIP) challeng sets (De Angeli *et al.*, 2002)

Jansen et al. (2003) proposed a scheme to authenticate users to mobile devices, especially PDAs, making use of themes and thumbnails. Their scheme's design was built over a visual login technique known as "Picture Password". The first step in this technique is the password enrolment stage, which involves choosing a theme among a set of predefined themes (e.g. sea, cat and dog, etc.) or flexibly provides a favourite set of images for display. The theme is a 5×6 matrix consists of thumbnail photos either randomly laid out or possibly shaped as a single composite image. Each thumbnail image and selection sequence is assigned a numerical value, which will be combined to generate a numerical password entry. An authentication attempt is successfully verified when all the enrolled thumbnail photos are recognised and clicked in the correct sequence. One drawback of this system is its small password space due to the number of thumbnail photos being limited to only 30. Another addressed issue is that the resulting passcode is short in length compared to the textual password. This problem can be tackled by enlarging the size of

the password space through selecting one or two thumbnail photos in one single action (similar to the use of a shift key on a traditional keyboard).
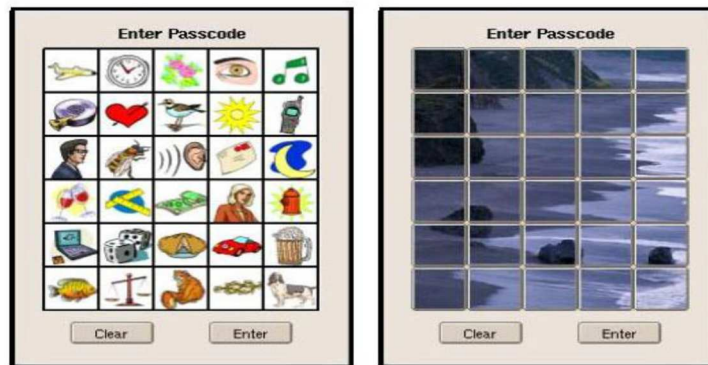
Figure 3-21: "Picture Password" scheme: **1.** Theme layout, **2.** Single composite image
(Jansen *et al.*, 2003)

Charruau, Furnell and Dowland proposed an alternative authentication method based on graphics recognition named "PassImages" (Charruau, Furnell & Dowland, 2005) (Charruau, 2004). The method allows users to select six images out of a total of 100 images on 5×5 grids. In order to authenticate, the user needs to click on the target images. For security purposes, a 'traffic lights' system is employed to make the display of chosen images invisible for prying eyes to avoid capturing the selection. However, after a short period of usage the average time spent on authentication was still somewhat longer compared to the typical time taken in text-based authentication. As a prevention measure, due to the threat of social engineering, it has been suggested that the image database should be increased and hobbies-related images that the user might choose in accordance with a pre-questionnaire data should be filtered out.

Over 90 days of experiment duration, 29 users participated in the method assessment. In this experiment, PassImage scheme attained a high success authentication rate (90%). However, time taken for authentication (around 20 seconds) was considered somewhat long.
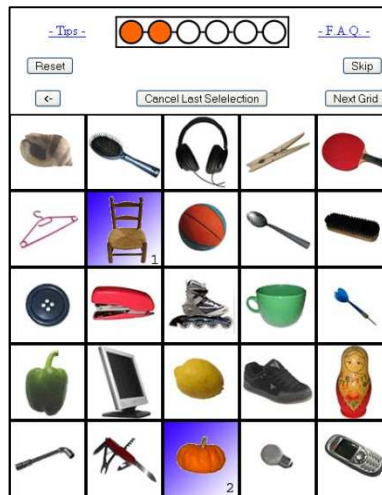
Figure 3-22: "PassImage" Technique (Charruau, 2004)

"ColorLogin" is a graphical password scheme proposed by Gao et al. that aims to decrease the login time via the use of background colours (Gao et al., 2009c) (Gao et al., 2009a). Using colours was designed to confuse the observers without burdening the real users. ColorLogin avoids the issue of the visual mouse click selection, which may cause shoulder-surfing attack, by allowing the user to click on any deceptive icons on the same row rather than pass-icons. In the registration phase, the user needs to choose a colour from a random set of system colours. Among the icons of the chosen colour, the user should select a set of icons as pass-icons. To login, the user is challenged over a number of rounds each of which displays random icons on the screen. Using background colours organise and ease the process of searching for pass-icons within many others, which greatly reduces the login time. Moreover, ColorLogin resists intersection attack by considering the appearance probability of each icon. In other words, display equal probabilities for both pass-icons and decoy icons.

Thirty participants involved in an experiment to evaluate the usability and security of the proposed scheme. In general, ColorLogin performed well compared to similar schemes but slightly slower than text-based password. According to the post-test questionnaire, participants found the login time still acceptable. The results showed 93.3% success rate with the first login attempt and 100% within three chances. All users remembered their

predefined colours correctly. As for the memorability test, participants were asked to re-login after one month, and all of them succeeded within three login attempts. In the security part of the experiment, the resistance of shoulder-surfing attack was examined by requesting participants to act as onlookers to catch the credentials of their colleagues and then try to use the stolen information to access ColorLogin. The result demonstrated a high immunity against shoulder-surfing since none of the onlookers managed to login successfully.

| The displayed screen. | A completed round. |
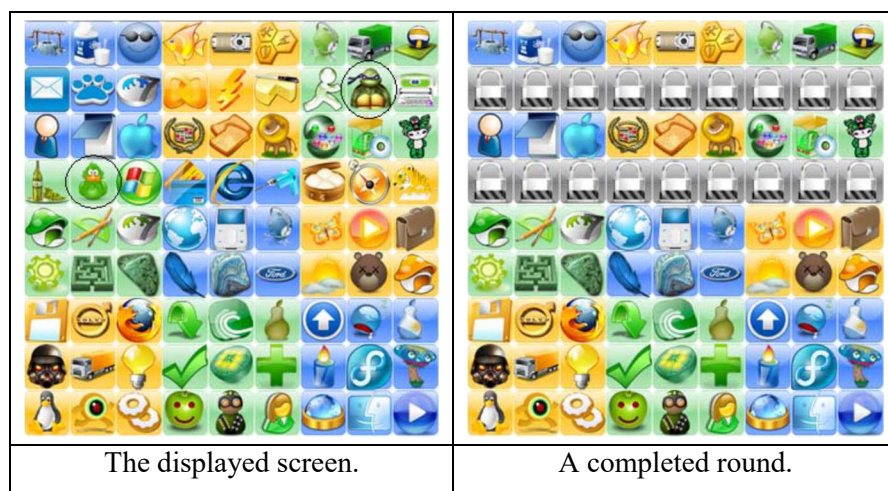
Figure 3-23: The login interface of **"ColorLogin"** (Gao *et al.*, 2009c)

Gao et al. (2010) inspired by DAS (Jermyn *et al.*, 1999) and Story (Davis, Monrose & Reiter, 2004) schemes and proposed a new shoulder-surfing resistant scheme called "CDS". The scheme replaces the direct clicking on pass-images with drawing a line across them. That is aimed at confusing peepers as the drawing curve passes through both pass-images and decoys. CDS password is composed of several images selected orderly by the user as pass-images. To aid the user memory, pass-images can be connected mentally by constructing a story. In addition, CDS enhance the resistance of shoulder-surfing attack by displaying degraded version of the images to reduce the viewing ability from a distance or a side. To login, users need to identify their pass-images and then draw a line starting with a given start image (head) crossing all pass-images in the correct order and finish with a given end image (tail).

Twenty participants were invited to a user study that evaluates the usability and compares it against Story scheme. The study was conducted in two sessions; first day and a week later. The results demonstrated a longer password creation time and login time for CDS group compared to Story group. The success rate of CDS scheme was high 96.5% but not as high as the Story scheme which achieved 98.2%. In the long-term recall test that took place one week later, CDS participants performed better which also showed an improvement in the login time in the favour of CDS.

Figure 3-24: "CDS" scheme login interface: A possible drawing trace (Gao *et al.*, 2010)

Khot, Kumaraguru and Srinathan (2012) proposed a scheme named "WYSWYE" (Where You See is What You Enter) to protect recognition-based graphical passwords against shoulder-surfing threat. Two variations of the proposed approach were implemented in the form of: Horizontal Reduce (HR) and Dual Reduce (DR). Although they are different in terms of the challenge grid size and the process of identifying and mapping the image pattern, the underlying strategy stays the same. In the registration phase of the Dual Reduce (DR) scheme, users are presented with a set of 28 images and required to create a password of four distinct images. During the login time, the scheme generates two side-by-side grids; the Challenge grid contains random images, four of which correspond to the password and the remaining 21 are decoys. The user is expected to interact with the second grid only, the Response grid, which is smaller in size, it is initially empty and used

for the input entry purposes. In order to map between the different size grids, the user must reduce the bigger challenge grid to the size of the response grid. That is done by a mental elimination of the rows and columns that do not contain any of the password images from the challenge grid. Login is achieved by locating the password images positions inside the reduced Challenge grid and by subsequently using the Response grid to map them accurately. The user is authenticated when the mapped positions match the positions of the password images. In this technique, users are not required to select their password images by clicking on them. Instead, they are only used to locate the associated positions to be marked in the response grid. This would make shoulder-surfing attacks ineffective, since it is hard to correlate the marked positions back to the password images in the challenge grid.

A controlled lab study was conducted that involved 24 participants who evaluated several usability elements. The mean login time was 35.5 seconds, even with practice there was no significant improvement. As far as the security study is concerned, only 16 out of the 24 users did participate in the security study. The users were shown screenshots of a login session and were challenged to recognise the password images. Within the 3 tries given to each user, only 1 participant managed to guess part of the challenge, 2 out of the 4 required images.
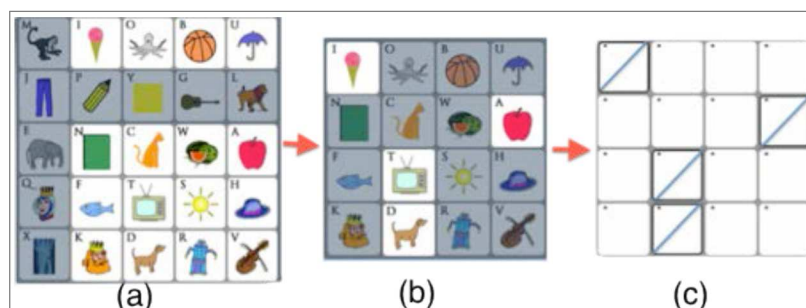
Figure 3-25: "WYSWYE" Dual Reduce (DR) scheme (Khot, Kumaraguru & Srinathan, 2012)
a) Main challenge grid, **b)** Reduced challenge grid, **c)** Response grid

Additional choice-based schemes were reviewed and added to 'Appendix A' including "Gaze-Contingent" (Dunphy, Fitch & Olivier, 2008), "Image Based Registration and Authentication System" (IBRAS) (Akula & Devisetty, 2004), "Convex Hull Click scheme" (CHC) (Wiedenbeck et al., 2006), "Shoulder-Surfing-Proof" (SSP) (Wu et al., 2014), "Weinshall approach" (Weinshall, 2004), "DynaHand" (Renaud & Olsen, 2007), "Graphical Password with Icons" (GPI) and "Graphical Password with Icons suggested by the System" (GPIS) (Bicakci et al., 2009). However, these schemes are included in the comparison studies at the end of the section, which should help in gaining better outcomes.

3.4.2. Typing-based recognition schemes

The use of keyboard/keypad as an input mechanism instead of using mouse has been discussed previously in subsection (3.3.3). In this section, attention is paid to those recognition schemes that utilise keystrokes as an entry approach to submit the necessary access data.

Weinshall (2006) developed a protocol named "Cognitive Authentication scheme" to resist spyware and shoulder-surfing. The technique requires users to set up and memorise an image portfolio containing their password images. To login, users need to distinguish their portfolio images within the panel. The authentication path is mentally computed by navigating the panel from the top-left corner searching for the user's portfolio. Two conditions control this navigation; if the stood on image is one of the previously chosen password images, then the required action is 'move down', otherwise it is 'move right'. Once the right or bottom edge of the panel is reached, the corresponding label for that

row or column should be noted down. The process is repeated over several rounds. This protocol aimed to increase the resistance to dictionary attacks and eavesdropping attacks.

The protocol was tested by 9 users over 6 months to examine the memorability and ease of use. The result demonstrated a high success rate as well as memory retention. However, later in 2007, Golle and Wagner (2007) proved the incorrectness of Weinshall's claim (Weinshall, 2006) that the Cognitive Authentication scheme is secure against eavesdropping attacks. By observing only a couple of successful logins, it was possible to recover the secret key of a user in a few seconds.

Figure 3-26: A high complexity query panel of **"Cognitive Authentication scheme"**
(Weinshall, 2006)

In 2008, Mohammed et al. (2008) worked on a new scheme that depends on multiple rounds of challenge-response authentication to resist shoulder-surfing attacks. Creating a password requires the users to select multiple icons as their pass-icons. Users of this scheme are only required to remember the password pictures in sequence. The authentication challenges the user to recognise a minimum number of the password icons from a larger set of random icons. In a response to the challenge, the user must enter the pass-icon's position where it is located on the screen in a form of numbers (0 – 9). Thus, the user must look for the pass-icon and then enter the number of the row and column where the pass-icon is positioned. Challenges are repeated for several rounds and then

authenticate the user when all responses are correct. In case of authentication failure, the system does not provide specific feedback about the error location.

Usability evaluation was carried out by ten participants over two sessions. At the first day session, users were asked to login repeatedly for ten successful attempts. One week later, participants were requested to recognise the five pass-icons that were presented within a list of 100 random unlabeled icons. The result demonstrated that the required ten correct logins were achieved by all participants. The mean login time was about 64 seconds for correct password inputs consist of 5 icons. In regards to security, the scheme was resistant to dictionary attacks, brute-force, guessing and shoulder-surfing attacks.
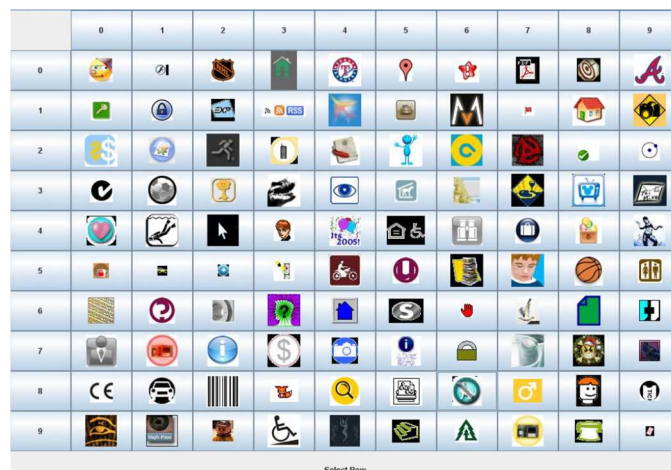
Figure 3-27: Login interface: Mohd's scheme (Mohammed *et al.*, 2008)

Komanduri and Hutchings (2008) implemented a picture password system with the ability to produce a memorable, high-entropy password. An easy to guess password is a general problem associated with user-selected passwords. Thus, their system attempts to avoid this problem by assigning users with a composed random password. The proposed system consists of 80 unrepeated pictures each one of which is labelled with a character. Each participant is assigned with a unique arrangement of eight items known as the 'home grid', which they need to recognise to fulfil the future authentication requirements. Pictures are always placed in a fixed-location within the home grid with the same correspondent keyboard key. In this system, a dual input ability is enabled by using either

the keyboard or an on-screen mouse cursor. Furthermore, another initiative was launched to accept an unordered input thus allowing the selection of the correct images in any order. A study was conducted on three time intervals (day 1, 2, and 9) respectively and involved 15 participants in the picture-based study. The outcomes of the memorability test showed an average result of 67% success rate after one week for the ordered input task whereas the unordered task achieved 100% correct attempts. According to that, a successful authentication system could benefit more from the unordered recall. In terms of the entry time, the scheme performed well with a mean login time of 13.7 seconds.

Figure 3-28: "Komanduri & Hutchings" Picture Password (Komanduri & Hutchings, 2008)

3.4.3. Comparative summary of Recognition-based techniques

This section uses a similar comparing process to that used previously for the Recall-based schemes in subsection 3.3.4, but this time the recognition-based schemes are compared. Comparative summaries of these techniques are presented in Table 3-5, Table 3-6 and Table 3-7, involving three main aspects that are technique attributes, security and usability. As mentioned earlier, the source of the collected data was the existing literature. Some schemes were included in the comparison whereas others were excluded depending on the sufficiency of the available data. The comparison tables were designed to include as much meaningful information as possible.

#	Graphical Password System	Year	Category: *Recognition*				
			Approach			Style	
			Choice	Click	Typing Entry	Image	Icon
1	PassFaces	1998	✓	-	-	✓ M	-
2	Déjà vu	2000	✓	-	-	✓ M	-
3	Triangle scheme, Moveable frame scheme, Other special geometric configurations	2002	✓	-	-	-	✓ M
4	Visual Identification Protocol (VIP)	2002	✓	-	-	✓ M	-
5	Picture Password	2003	✓	-	-	✓ S/M	-
6	Story	2004	✓	-	-	✓ M	-
7	Weinshall approach	2004	✓	-	-	✓ M	-
8	PassImages	2005	✓	-	-	✓ M	-
9	CHC	2006	✓	-	-	-	✓ M
10	Gaze-Contingent	2008	✓	-	-	✓ M	-
11	Colorlogin	2009	✓	-	-	-	✓ M
12	GPI & GPIS	2009	✓	✓	-	-	✓ M
13	CDS	2010	-	Draw		✓ M	-
14	WYSWYE	2012	✓	-	-	✓ M	-
15	SSP	2014	✓	Press a key		-	✓ M
16	AuthentiGraph	2003	-	✓	✓	-	✓ M
17	Cognitive Authentication	2006	-	-	✓	✓ M	-
18	Mohd's Scheme	2008	-	-	✓	-	✓ M
19	Komanduri & Hutchings Picture Password	2008	✓	-	✓	-	✓ M
						M= Multi, **S**= Single	

Table 3-5: Recognition-based attributes comparison

A comprehensive attributes-based comparison was conducted, and the results are presented in Table 3-5. This table shows that there is an increase in the number of the research inventions in the area of recognition-based graphical authentication over the years. The output of the conducted comparison shows that almost all recognition-based

graphical authentication schemes utilise multiple images or icons to allow users to identify and choose password images from amongst other images. However, the Picture Password scheme offered the option to use either a single image or multiple images as preferred.

It can be also inferred that the recognition-based technique is fundamentally associated with a direct choice-based approach or with the additional support of the keypad typing entry approach otherwise. Only a few schemes failed to correlate such as AuthentiGraph and GPI & GPIS since they make use of a click-based approach while SSP makes use of key pressing instead. Furthermore, a single scheme (CDS) has used drawing approach within the recognition-based technique. A number of recognition-based techniques have benefited from the keypad typing entry approach, which seems more viable with choice-based schemes than others.

Recognition-based schemes were also compared based upon some of the major security features and vulnerabilities that were covered in the existing literature. The compared features were almost the same as that in the Recall-based techniques (subsection 3.3.4) including the use of multiple rounds, and hash function, while the comparison of vulnerability involved the susceptibility to various types of attack, such as shoulder-surfing, guessing, dictionary attack and spyware. The only difference is the addition of the following related features:

- **Shuffling images:** dynamic image locations, always changeable.
- **System assigned images:** users are not allowed to select their secret images; instead the system will assign images for them, which can help to avoid vulnerabilities such as the choice of predictable images.

	Recognition-based Graphical Password System	Security Features & Vulnerabilities							
		Images/Objects Shuffling	System Assigned Images	Multiple Rounds	Hash Function	Shoulder-Surfing Resistant	Difficult to Guess	Safe against: Spyware – Recordability	Other Features
1	Déjà vu	✓	-	-	✓	-	✓	-	Safe against Secret Disclosure - Resist Social Engineering
2	Triangle scheme, Moveable frame scheme, Other special geometric configurations	-	-	✓	-	✓	-	-	Resistant to exhaustive-search attack
3	Visual Identification Protocol (VIP), (VIP2), (VIP3)	✓ VIP 2,3	✓ VIP 3	✗	-	✓ VIP 2,3	-	-	Safe against Secret Disclosure
4	Picture Password	✗	✓	-	✓	-	-	-	
5	AuthentiGraph	✓	-	-	-	✗	-	✓	Safe against password cracking and sniffing
6	Weinshall approach	-	✓	✓	-	✗	✓	✓	Challenge-Response protocol
7	PassImages	✓	-	✓	-	✓	-	-	Vulnerable to Social Engineering
8	CHC	✓	-	✓	-	✓	✓	✓	Very large password space Safe against Brute force
9	Story	✓	✗	✓	-	-	-	-	
10	PassFaces	✗	✓	✓	-	✗	✗	-	Vulnerable to Social Engineering Safe against verbal discloser
11	Cognitive Authentication	-	-	✓	-	✓	-	✓	Challenge-Response protocol Safe against Dictionary attack Vulnerable to eavesdropping
12	Mohd's Scheme	✓	-	✓	-	✓	✓	-	Safe against: Brute force, Social Engineering, Dictionary attacks
13	Colorlogin	✓	-	✓	-	✓	-	✓	Safe against: Intersection & Brute force attacks Vulnerable to Hotspot
14	GPI	-	✗	-	-	✗	-	-	Safe against: Hotspots
15	GPIS	-	✓	-	-	✓	-	-	Large password space
16	WYSWYE	✓	-	-	-	✓	✓	-	Safe against: Brute force attack Vulnerable to Intersection attack
17	SSP	✓	-	-	-	✓	✓	✓	

Table 3-6: Recognition-based security features and vulnerabilities comparison

It was found that the recognition-based techniques also suffer from a lack of available security details, as already mentioned earlier. According to Table 3-6, the majority of schemes are featured with image shuffling and multiple rounds. However, system assigned images have been implemented in just a few schemes. The use of hashing

function was rather limited. As far as the security vulnerability is concerned, Table 3-6 shows that more than half of the compared schemes have managed to resist shoulder-surfing attacks whereas above the third have prevented guessing or spyware attacks. An interesting finding is that schemes tend to focus on a certain type of attack and provide the necessary safeguard but unfortunately other threatening attacks are neglected. Although it is infeasible to protect the authentication mechanism from all types of attacks, but schemes should at least consider as much protections as possible.

	Recognition-based Graphical Password System	Usability Features				
		Themes\ Categories	Memorability	Mnemonic	Lab(L)/Field(F) Study	Other Features
1	PassFaces	✘	✓	-	L/F	
2	Déjà vu	✘	✘	-	L	
3	Visual Identification Protocol (VIP), (VIP2), (VIP3)	✓	✓	✘	F	
4	Picture Password	✓	-	✓	-	User-provided images
5	Story	✓	✘	✓	F	Difficult to remember story and password sequence
6	CHC	-	✓	-	L	User-provided icons
7	CDS	-	-	✓	L	

Table 3-7: Recognition-based usability features comparison

Recognition-based schemes were also compared based upon common usability features (Table 3-7), such as the use of themes, memorability, mnemonics and the conducted user study. Providing themes and image categories for users to choose from is one of the usability features that has been implemented in some of the recognition-based schemes. This feature may help in better remembering user's images. User-provided images is another feature, but it has not been widely used. Despite the fact that allowing users to provide their own images appears to be a good usability feature that may contribute in

making the technique easier to remember but on the other hand it allows advisory to easily distinguish the image sources and identify the secret images of the user. In terms of memorability, some of the compared schemes claim to excel in this area; however, mnemonic in the choice-based techniques does not seem to be linked with memorability unlike the recall-based techniques.

3.5. Hybrid graphical technique

The Hybrid technique category contains any scheme that falls into more than one category or utilises multiple approaches. Most researches in this area aim to combine interesting features that exist in some techniques but not in another or to overcome the shortcomings of the available schemes. The integration is aimed to bring more strength to the proposed system and mitigate known issues. This category of the graphical authentication excludes any scheme with optional (non-combined) features such as that offered by AuthentiGraph scheme where more than one entry approach are provided for the user to choose whichever convenient. A collection of schemes of this type are reviewed and compared next.

Motivated by the "Where Is Waldo" (WIW) technique, Hong et al. further enhanced the scheme by adding a flexibility feature as a way of assigning each pass-object variant with the user's own codes (Hong et al., 2004) (Man, Hong & Matthews, 2003). Simply, password creation is achieved by choosing 4 pass-icons from an icon library. Each icon consists of 4 variations. The user is required to assign a corresponding string to every variation. In order to login, the user needs to identify the pre-chosen pass-icons from the grid and enter the pre-determined string corresponding to each pass-icon variation. Although this method aims to produce a password strongly resistant to spyware, it shares the same weakness of the text-based password where users are forced to memorise many texts.

| Variations & codes of pass-icons | Login Screen |
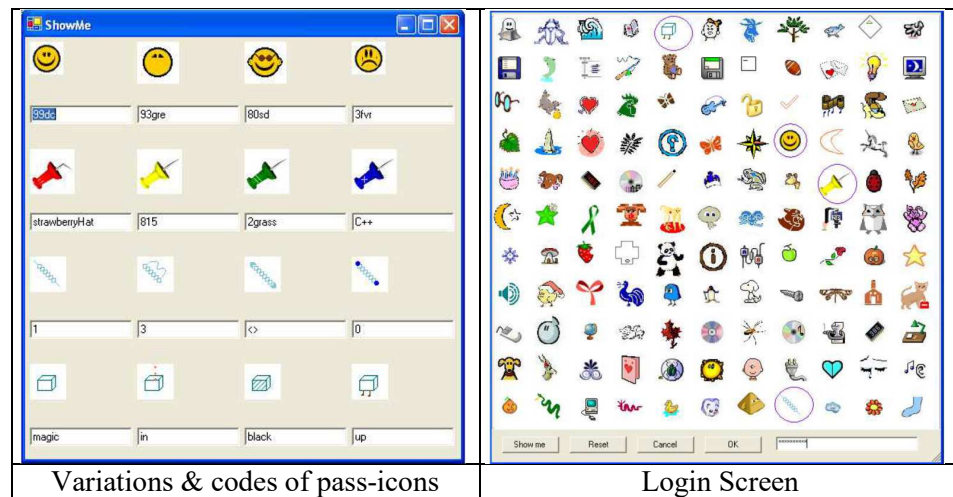
Figure 3-29: Hong authentication technique (Hong *et al.*, 2004)

Suo, Zhu and Owen (2006) developed a hybrid graphical password technique, derived from both recognition and recall based techniques, called "Recall-a-Formation" (RAF). The scheme is composed of two 8×8 tables: a data table and an input table. The data table contains the possible choices of icons from different themes and the input table on which the user needs to place the recalled pre-registered formation of icons in the correct locations. In the registration stage, the user registers the icons formation to model the graphical password by selecting icons from the data table then drag and drop them into the desired cells on the input table. In the authentication stage, users must correctly recognise and select the target icons among the distracting icons and precisely place each icon into the exact input table cell. Although the data table can be very large with pages of icons of different themes, just one theme page is capable of producing a large password space. To evaluate the scheme, 30 users participated in a preliminary study to use and interact with the system, and on the next day users were asked to recall their passwords. Only 11 users managed to remember the pre-chosen formation and icons correctly. 50% of the users succeeded in remembering half of the icons. As a result, memorability was identified as a usability issue that needs improvement.

Figure 3-30: main interface of **"RAF"** (Suo, Zhu & Owen, 2006)

In 2009, van Oorschot and Wan (2009) proposed a hybrid authentication method called "TwoStep" to increase the security using a two-step process that keeps the traditional use of text passwords and adds the recognition-based graphical passwords. Graphical password is created by choosing a number of images from several verification rounds to form the user image portfolio. The first login step requires entering a text password as normal and then the second step involves graphical password verification. The system displays a set of images in each round and users need to select their pre-chosen images. A successful user login is achieved by completing all rounds with correct text and graphical passwords.

The authors also described a simple method to reduce the threat of shoulder-surfing attack (Figure 3-31). The idea is to associate each displayed image with an index number. A selection panel is located in the lower part of the screen, which displays all index numbers in an ascending order. In this approach, users need to look for their images and click on the corresponding index number on the selection panel. Although this method can mitigate normal human peeping but cannot protect against such attacks with camera recording. However, this approach can reduce the vulnerability against naive keylogger attacks and phishing attacks since the latter requires knowing the image portfolios of the users beforehand, which is quite difficult. Another advantage is the indirect alert that users can have when seeing unfamiliar images other than their portfolios after submitting wrong

text-based passwords. The password strength of TwoStep was measured by entropy in bits. Thus, the graphical part of the scheme may enhance the security significantly, as it can add 12.8 bits of entropy for un-ordered images, or 25.6 bits for ordered images.
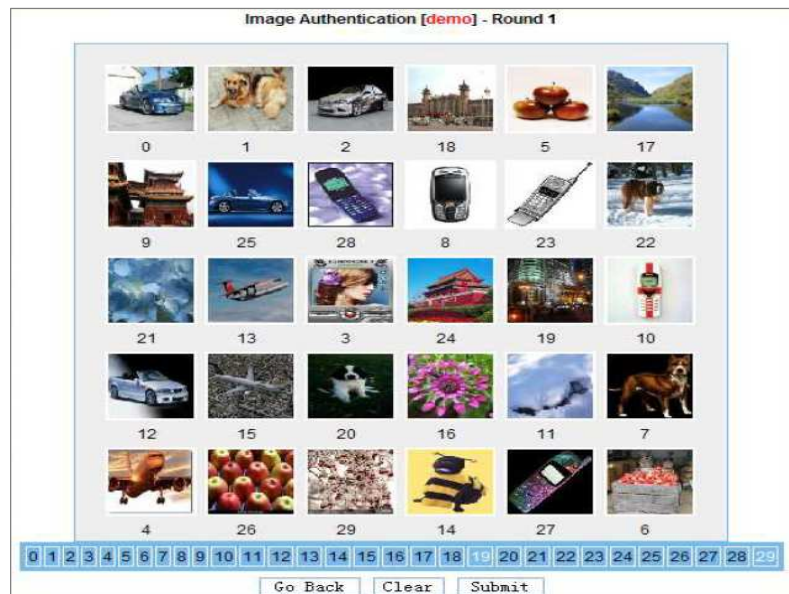
Figure 3-31: "TwoStep" Graphical authentication step (van Oorschot & Wan, 2009)

Citty and Hutchings (2010) introduced a system called "Touch-screen Authentication using Partitioned Images" (TAPI) that works similarly as a Personal Identification Number (PIN) system but uses partitioned images instead. The user of this method needs to enter not only one of 16 images, but also to choose the right partition of the image. At each login time, there are 64 possible options (4 partitions × 16 images) for the user to select from rather than 10 options in most PIN systems. The image is partitioned in the shape of X, which appeal to the ease of remembering the physical regions such as top, right, left, and bottom. When the user selects the image partition, the system shows no feedback of the selection to improve the authentication entry security. Applying the image partition can mitigate the shoulder-surfing attack since it would be less likely for an observer to be able to recognise the exact selected partition of an image. In addition, the increased number of possible sequences increase the difficulty for guessing attack but at the same time decreases target size which can cause errors and thus likely extend the entry time.

Thirty participants involved in two lab studies to examine the scheme. The results demonstrate that the level of memorability and entry time provided by TAPI scheme is fairly high. However, the scheme is not overly burdensome and enhances the overall security. After one week of non-use, 90% of users managed to remember their authentication with a median best entry time of 3.5 seconds.
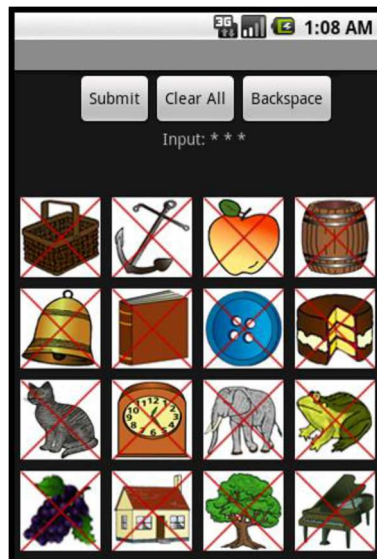
Figure 3-32: **"TAPI"** entry system (Citty & Hutchings, 2010)

Jali, Furnell and Dowland (2011) studied the idea of joining two graphical password techniques to enhance the security. A prototype named "Enhanced Graphical Authentication System" (EGAS) was implemented that combines click-based and choice-based graphical authentications. The system requires the user to remember 6 images in total. The first 2 images are assigned randomly by the system and the other 4 images are left for the user to choose from different image categories. Following the images selection, the user needs to create secret clicks by clicking once on each image. As far as the login is concerned, four scenarios were tested with variation in the number of rounds and the displayed images. The login task is the same in all scenarios where the system displays secret images and decoys on the screen. Whether the image is a secret one or decoy, the user still needs to click on them all to make it harder for an attacker to guess users' real secret images. Access is granted when all secret images are clicked correctly.

To evaluate the scheme, 30 users participated in lab trials which covered the usability performance. The results showed a maintained memorability with a reasonable creation/login time, high clicking accuracy, and positive users' preference. Nevertheless, some serious issues were reported in the trial such as the user tendency to select similar and guessable images as well as clicking on easy to guess objects and areas.

Figure 3-33: "EGAS" Login Interface - Scenario Four (Jali, 2011)

A combination of features from several schemes has formed the base of the new scheme proposed by Deshmukh and Devale (2013). To create a password, the system displays 4 random images. Users need to select click points and add single number/character on each of the first 3 images. The last image is for users to draw a secret and add single number/character. In order to login, users must identify the images, click on the correct points, enter the right number/character, and draw the secret on correct image. Failure to provide any part of the password would result in an unsuccessful authentication attempt. Unfortunately, this scheme has not reported information about any type of experiment to evaluate the aspect of usability and security.

Figure 3-34: Login interface for Deshmukh's scheme (Deshmukh & Devale., 2013)

3.5.1. Comparative summary of the Hybrid graphical techniques

The same comparison process used in the previous categories is also followed in this section putting the hybrid schemes this time under assessment. Table 3-8, Table 3-9 and Table 3-10 present different comparative summaries of these techniques including technique attributes, security and usability. It is clear from Table 3-8 that the interest in hybrid techniques has a relatively recent start about a decade ago. The number of proposed schemes of this category is considerably low so far. The reason for that might be due to the difficulty of the integration or the low performance expected as a result of joining several techniques. On the other hand, the combination can take advantage of the identified good features and work towards eliminating bad ones. Thus, a further investigation is needed to find out more about the feasibility of such proposals.

Apparently, almost all hybrid schemes depend on choice approach and use multi-images and none has used grids as a style for the challenge set. Besides, some schemes used clicking as a second approach whereas only one scheme has used drawing alongside with clicking and typing approaches. Typing entry approach has been also utilised by some schemes in the hybrid graphical technique.

	Graphical Password System	Year	Category		Approach			Style	
			Recognition	Recall	Click	Choice	Typing Entry	Image	Icon
1	Hong scheme	2004	✓	Cued	-	-	✓	-	✓ M
2	Recall-a-Formation (RAF)	2006	✓	Pure	-	✓	-	-	✓ M
3	TwoStep	2009	✓	Pure	-	✓	✓	✓ M	-
4	TAPI	2010	✓	Cued	✓	✓	-	✓ M	-
5	EGAS	2011	✓	Cued	✓	✓	-	✓ M	-
6	Deshmukh's scheme	2013	✓	Cued	✓	Draw	✓	✓ M	-

M= Multi

Table 3-8: Hybrid technique attributes comparison

Hybrid schemes were compared against the major security features and vulnerabilities that were already available in the literature (Table 3-9). The compared security features were the same as that used earlier in recognition-based techniques (subsection 3.4.3). It seems that schemes of this kind are more resistant to guessing and shoulder-surfing attacks. Additionally, only one scheme reported data with respect to its resistance to spyware or recordability.

	Hybrid Graphical Password System	Security Features & Vulnerabilities							
		Images/Objects Shuffling	System Assigned Images	Multiple Rounds	Hash Function	Shoulder-Surfing Resistant	Difficult to Guess	Safe against: Spyware – Recordability	Other Features
1	Hong scheme	✓	-	✓	-	-	-	✓	
2	TwoStep	✓	-	✓	-	-	-	✗	Safe against: Key-logger, Phishing, MITM
3	TAPI	✗	✓	-	-	✓	✓	-	
4	EGAS	✓	✓	✓	-	✓	✓	-	Susceptible to hot-images hot-spots
5	Deshmukh's scheme	-	-	✓	-	-	✓	-	

Table 3-9: Hybrid technique security features and vulnerabilities comparison

Table 3-10 presents the hybrid schemes which were compared based upon common usability features, such as the use of themes, memorability, mnemonics and the type of the conducted user study. Unfortunately, the result of the comparison is very poor and does not reveal any significant data that might help in exploring the usability features of such category. However, EGAS was the only scheme to report sufficient data about the conducted study. It can be depicted that none of the hybrid schemes has conducted a field study.

	Hybrid Graphical Password System	Usability Features				
		Themes\ Categories	Memorability	Mnemonic	Lab(L)/Field(F) Study	Other Features
1	Recall-a-Formation (RAF)	✓	✗	-	L	
2	TAPI	-	✓	-	L	
3	EGAS	✓	✓	-	L	

Table 3-10: Hybrid techniques usability features comparison

3.6. The integration of Graphical authentication and One-time password

One of the methods to produce one-time password without resorting to the conventional means (devices) is through the use of graphical authentication. It should be noted here that this section is not a graphical password category by itself but rather consists of a collection of schemes falling under different graphical authentication categories with a special feature in common that is the use of One-time password technique. However, the literature of some schemes included here has not necessarily mentioned the production of pseudo-random passwords but rather realised to do so by reviewing the scheme process. Thus, these schemes are reviewed and compared separately in this section for the sake of understanding how researchers managed to combine between these important techniques

– graphical password and one-time password, and what are the advantages and disadvantages of such integration.

In 2005, Craymer and Howes invented a secure authentication methodology called "GrIDsure" (Blair, 2007), which was later acquired in 2010 by CRYPTOCard Inc. (CRYPTOCard Inc, 2010b) (CRYPTOCard Inc, 2010a) to be re-launched in a commercial technique form. GrIDsure generates a dynamic one-time password excluding the need for any additional hardware or software requirements. On the first use, a registration stage should be completed whereby a 5×5 grid of cells is presented to the user to select a favourite 'Personal Identification Pattern' (PIP), which is composed of 4 cells of any shape in any order. This chosen pattern (PIP) is all what the user needs to remember to login, which enables them to provide dynamic characters shown on their (PIP) cells in order to be securely authenticated. In each authentication attempt, the grid cells will be filled in with a random set of characters. The user is required to use a keyboard to input the corresponding characters occupying the (PIP) cells of the previously selected pattern.
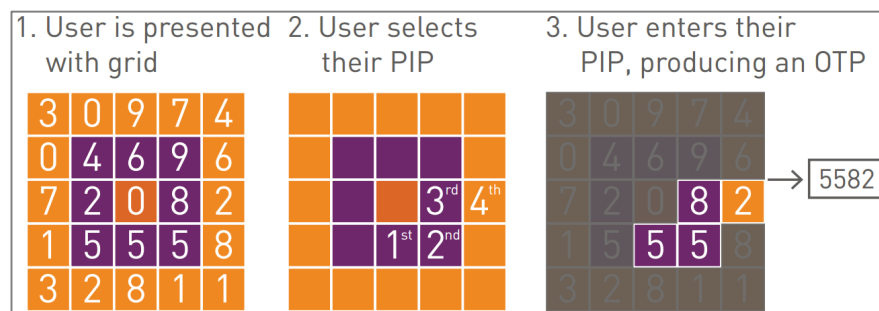
Figure 3-35: Authentication stage of **"GrIDsure"** technique (SafeNet, 2015)

In 2006, Weber revealed an initial security analysis of GrIDsure in comparison to the traditional PIN as reported in (Biddle, Chiasson & van Oorschot, 2012). The study outcomes showed that GrIDsure passwords attain better security, especially in terms of shoulder-surfing attacks. However, several weaknesses of the system were noted by Bond (2008) in his initial comments. The report argued that GrIDsure is not more secure than

a static PIN if secret observation is possible. Security is also compromised due to the users' tendency to select from a limited subset of predictable patterns. In addition, susceptibility to screen scraping and challenge grids retrieval from PCs were also mentioned as security issues associated with the system that lead to a lack of protection against phishing and man-in-the-middle attacks.

Brostoff, Inglesant and Sasse (2010) evaluated the GrIDsure scheme independently and concluded that having one pass-pattern for people to use lead to high usability and memorability of the system. As far as the security was concerned, the study showed that the security level depends on the usage circumstances with, for instance, scores being better in situations where repeated observations of transactions are unlikely to occur. User instructions and guidance, which aim to narrow down the likelihood of choosing obvious or easy to guess patterns, were also found to positively impact upon security. However, GrIDsure may be hindered from being more secure than a conventional PIN when there is a small effective pattern space or when it is possible to capture multiple sessions of the one-time PIN along with the displayed grid.

Dimitropoulos (2011) proposed an enhanced version of GrIDsure using background images in an attempt to persuade users to choose more complicated patterns and hence stronger passwords. The same technique as the original GrIDsure was used but with the help of a background image. An experiment was conducted in order to measure the impact of the background images with the GrIDsure on the usability and the users' choice. The result showed that using background images had a positive effect on the pattern choice.

Figure 3-36: "Enhanced-GrIDsure" with a background image (Dimitropoulos, 2011)

GrIDsure security was also analysed by Jhawar et al. (2011). The outcomes of the study stated that the current form of GrIDsure is vulnerable to communications interception. Identifying the security issues motivated the authors to suggest some security improvements. Thus, they proposed a system called "GrIDsure with 4 Patterns" (GS4), which involves two enhancements to harden the original implementation of GrIDsure scheme against Man-in-the-Middle or alike attacks. GS4 requires the user to select and register several patterns in association with their user account. In each authentication attempt, the user is first notified through an Out-Of-Band (OOB) technique (e.g. sending out an SMS to the registered mobile number of the legitimate user) to indicate which pattern amongst the pre-registered ones is necessary to be used for authentication at this specific time. As Out-Of-Band service is utilised, the second proposed enhancement involves sending another parameter (e.g. a random one-time string) to the user's mobile phone in addition to the required pattern number. As a result, a further security complexity is added since the attacker is supposedly unable to keep control of both communication channels (the grid and the user response).

Figure 3-37: "GrIDsure with 4 Patterns" (GS4) (Jhawar *et al.*, 2011)
Patterns authentication (**P1:** PVRN, **P2:** AGMS, **P3:** KCWX, **P4:** IDNJ)

Gao et al. innovated a solution based on a challenge-response protocol to enhance the security via protecting the graphical passwords against spyware attacks by utilising CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) technique (Gao et al., 2009b) (Wang et al., 2010). The new authentication scheme is a combination of graphical password and textual CAPTCHA, and it stands in the face of the automated programs to prevent passwords harvesting, whilst nonetheless remains a human solvable task.

The authors proposed two schemes called the 'Basic scheme' and the 'Improved scheme'. In the basic one, a CAPTCHA instance is assigned and embedded into each displayed image. To register, users need to choose and remember what is called (pass-images) as their password. In order to authenticate, users are required to pass two tests. First is the image recognition, where they need to look for their pass-images among other decoy images. That is followed by the second test, which involves solving and typing the assigned CAPTCHA string that appears underneath each pass-image. One main weakness of the basic scheme is the invertible relationship between passwords and the entered string, which may result in a simplification of the analysis and distinguishing process.

The second scheme is an improvement of the aforementioned basic scheme, and it aims to overcome the vulnerabilities discussed earlier in the basic scheme. The improved technique uses a predefined random length as opposed to the uniform length used in the

basic scheme. Consequently, users need to select and memorise the letter positions of each pass-image, which are also called pass-positions. For example, the code can be formed by the letters in 1st, 3rd and 7th position of the string. The characters corresponding to the pass-positions of each pass-image should be entered correctly by the user during the authentication.

The scheme was evaluated in-lab by 36 users over 3 sessions (day one, after a week, and after a month). The success login rate appeared to be considerably high with 87.8% and the mean login time when using 4 pass-images was 24.8 second. As far as the memorability is concerned, 80.6% of the login attempts were successful after one week while participants managed to obtain 72.2% correct attempts a month later. That shows that the scheme is relatively easy to remember after some time of non-use.

Figure 3-38: The interface of Gao's CAPTCHA scheme (Gao *et al.*, 2009b)

Gupta et al. implemented an authentication technique based on inkblots' mnemonics called "Passblot" similar to the scheme introduced by (Stubblefield & Simon, 2004) but with an added security (Gupta *et al.*, 2012) (Gupta et al., 2011). Passblot uses a set of inkblots unique to each user to generate pseudo random one-time passwords. In this scheme, only ten inkblot-like random images are used. During the first use of the system, users are presented with 10 inkblots one after another and asked to assign a description to each inkblot. The inkblot association is formed by the first and last letters of the

description. In the authentication phase, four out of the ten inkblots are shown to the users, and they should enter the corresponding associations. Getting at least three correct associations out of four leads the user to gain access. Lastly, a user study conducted on the proposed system showed on the one hand a good memorability level and on the other resistance capability to a number of active and passive security attacks. Nevertheless, some users encountered difficulty in describing inkblots and thus memorising those descriptions later on.
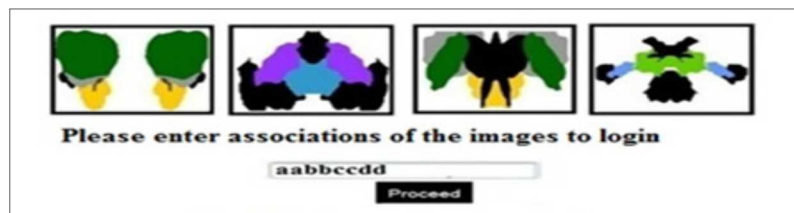
Figure 3-39: Login screen for **"Passblot"** (Gupta *et al.*, 2012)

Confident Technologies® has introduced a new approach that provides an image-based one-time password named "Confident ImageShield™" (Roman Yudkin - Confident Technologies®, 2011). In this technique, the registration phase involves selecting a few easy to remember categories. Each authentication attempt displays a 3×3 grid full of random images overlaid by alphanumeric characters. The user is then prompted to identify the images that match the pre-selected themes. Finally, the user needs to type in the alphanumeric characters associated with the password images. A feature of this scheme is the changeable location of the pictures and their characters. As a result, a unique one-time password or PIN is submitted at each login attempt.

Figure 3-40: "ImageShield" scheme (Roman Yudkin - Confident Technologies®, 2011)

Ku et al. proposed a solution to generate a "Graphical One Time Password" (GOTP) for financial services using smartphones (Ku et al., 2012) (Ku *et al.*, 2013). The password creation is based on selecting an image portfolio over four rounds that should form a story to act as a recall assistant. Each authentication round displays images on a 4×9 grid frame in the correct order. The respective alphanumeric OTP code is shown on the top left corner of each image, and the user needs to memorise these codes for the next round. The final fifth round is the password input step, which contains a random layout display of 12 buttons to allow entering the memorised four OTP codes matching the image portfolio. The result of the study showed that the average registration time was quite fast with positive results that evaluated the password recall convenience, recall interference, and authentication time.

However, GOTP approach still requires the user to memorise alphanumerical code obtained through identifying the pass-images over several rounds and then enter that code in the final round. That in turn may require memory recall from the user, resulting in usability issues. In addition, GOTP is designed for mobile platform that can be used as an out-of-band channel for authentication to be carried out away from the browser. In other words, there is a need for an additional device (smartphone) to be present in order to use GOTP scheme which is not always an issue for many users nowadays. Furthermore, the length of the OTP code generated by GOTP is considered short.

Figure 3-41: Authentication process of **"GOTP"** scheme (Ku *et al.*, 2012)

Zangooei, Mansoori and Welch (2012) aimed at overcoming the drawbacks of existing graphical authentication designs by integrating usability and security attributes of recognition-based and recall-based algorithms. The registration process of this scheme requires the user to select password images between three and five. The authentication process uses two matrices; one is a recognition-based scheme to provide the required usability features, the second matrix is a recall-based algorithm to satisfy the requirements of the security features. During the login, the user will be displayed a matrix of pictures that includes the pre-selected images. The user is required to look for the selected images and remember their cell positions in the matrix. Subsequently, the second matrix will be presented which contains cells filled by random alphanumerical strings. The user needs to type in the codes within the cells that correspond to the selected photos in the correct sequence as shown in the first matrix.

The security of the system was assessed by its ability to resist shoulder-surfing and password guessing attacks. Security testing involved two participants acting as attackers to steal other user's password while being entered. At each testing attempt of the 10 total times, two random attackers were assigned and placed in random positions and distances away from participants. Afterwards, the attackers were given a questionnaire to realise the number of password pictures they managed to identify. The result of the experiment demonstrated that attempts to compromise the entire password pictures were unsuccessful. However, identifying the first 3 letters was achieved by only 3 attackers.

A study to evaluate the usability features was performed involving 30 participants who were given the chance to use the system on two separate days (a week apart) and then fill-in the questionnaire to leave additional comments about the system. Despite the longer time taken to login, the feedback indicated that the system satisfies the users' requirements.

| First grid: Recognition-based approach | Second grid: Recall-based approach |
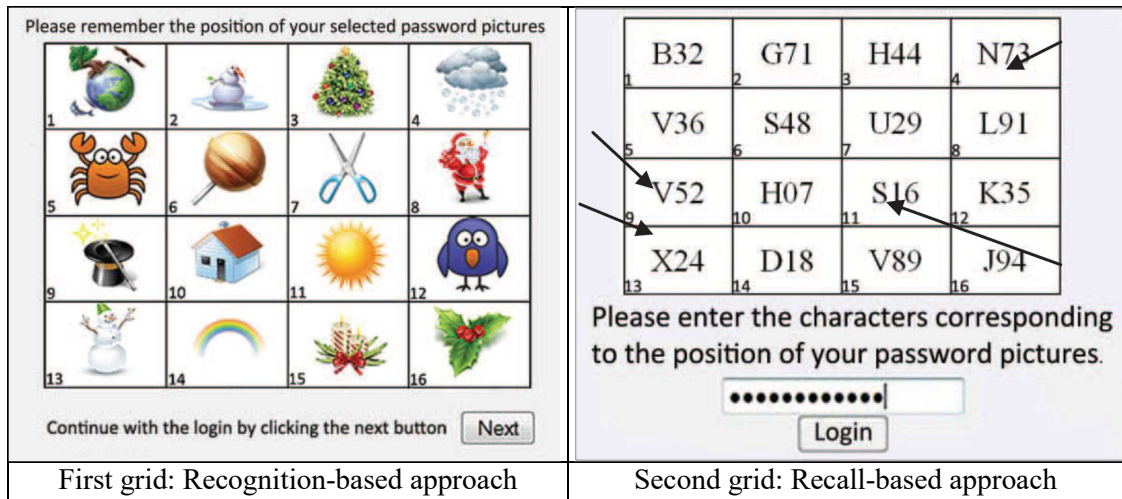
Figure 3-42: Zangooei's Hybrid scheme (Zangooei, Mansoori & Welch, 2012)

3.6.1. Comparative summary of the OTP-based graphical techniques

This section followed the same comparison process as that used in the previous graphical password categories. Table 3-11, Table 3-12 and Table 3-13 present comparative summaries of these techniques including technique attributes, security and usability. It is clear from Table 3-11 that most graphical password schemes with the utilisation of one-time password technology were relatively recent proposals, which may indicate that this research domain is still rich and there are opportunities for enhancements.

Apparently, all OTP-based graphical schemes depend on typing approach for data entry. Thus, there is a clear correlation between the use of keypad typing entry approach and the one-time password output, which seems viable relation. The majority of schemes use multi-images and just a few pattern-based schemes used grids as a style for the challenge set. Besides, none of the schemes utilised clicking nor drawing approaches.

#	Graphical Password System	Year	Category		Approach		Style	
			Recall	Recognition	Pattern	Typing Entry	Grid	Image
1	GrIDsure	2006	Pure	-	✓	✓	✓	-
2	Gao CAPTCHA	2009	-	✓	-	✓	-	✓ M
3	Enhanced-GrIDsure with Background	2011	Cued	-	✓	✓	✓	✓
4	GrIDsure with 4 Patterns (GS4)	2011	Pure	-	✓	✓	✓ M	-
5	Passblot	2011	Cued	-	-	✓	-	✓ M
6	ImageShield	2011	-	✓	-	✓	-	✓ M
7	GOTP	2012	-	✓	-	✓	-	✓ M
8	Zangooei Hybrid approach	2012	Pure	✓	-	✓	-	✓ M
							M= Multi	

Table 3-11: Attributes comparison of OTP-based schemes

The schemes in this section were compared against the major security features and vulnerabilities based on the available literature (Table 3-12). The compared security features were similar to those used earlier to compare the recall-based and recognition-based techniques. It seems that schemes of this kind are more resistant to shoulder-surfing and spyware attacks, while dictionary and guessing attacks were also resisted by a few schemes. Additionally, only one scheme reported data with respect to its resistance to hotspot or hot-images. It was also found that hash function has not been implemented in any scheme of this type at all.

	Graphical Password System	Security Features & Vulnerabilities								
		Images/Objects Shuffling	Multiple Rounds	One Time Password	Shoulder-Surfing Resistant	Difficult to Guess	Dictionary attacks Resistant	Safe against: Spyware - Recordability	Safe against Hotspots	Other aspects
1	GrIDsure	-	-	✓	✓	-	-	✗	-	Vulnerable to Eavesdropping & Phishing
2	Enhanced-GrIDsure with Background	-	-	✓	-	-	✓	-	✓	
3	GrIDsure with 4 Patterns 'GS4'	-	-	✓	✓	-	-	✓	-	Safe against Eavesdropping Out-Of-Band technique Depends on additional devices
4	Goa CAPTCHA	-	✗	✓	-	✓	-	✓	-	CAPTCHA
5	Passblot	-	-	✓	✓	-	✓	✓	-	Resist social engineering
6	ImageShield	✓	-	✓	-	-	✓	✓	-	Safe against: Brute force attack Anti-phishing
7	GOTP	✓	✓	✓	✓	-	-	-	-	Safe against: Smudge attack Depends on additional devices
8	Zangooei Hybrid approach	✓	-	✓	✓	✓	-	-	-	

Table 3-12: Comparing security features and vulnerabilities of OTP-based graphical schemes

As far as the usability comparison is concerned, Table 3-13 presents the schemes which were compared based upon common usability features, such as the use of themes, memorability, mnemonics and the type of the conducted user study. Unfortunately, the result was not better than that obtained earlier in the hybrid graphical techniques comparison as no significant result can be revealed that might help in realising the usability features of such group of schemes. However, it can be depicted from the reported data that some of the schemes were easy to remember.

	Graphical Password System	Usability Features				
		Themes\ Categories	Memorability	Mnemonic	Lab(L) /Field(F) Study	Other Features\ Limitations
1	Enhanced-GrIDsure with Background	-	✓	✓	-	
2	GrIDsure with 4 Patterns 'GS4'	-	-	-	F	
3	ImageShield	✓	✓	-	-	
4	GOTP	✓	-	-	L	Story-based approach

Table 3-13: Usability features comparison of OTP-based graphical schemes

3.7. Password space and Entropy

The theoretical password space (keyspace) is the set of all possible passwords for a certain password scheme with a given setting of parameters, as defined by Wiedenbeck *et al.* (2005c). With regard to the term 'guessing entropy', it can be defined as an average measure of the difficulty involved in guessing a password. Thus, password space and guessing entropy are directly related, and both play a critical role in measuring the strength of the password system since they determine how safe a system is in relation to resisting various guessing and brute force attacks (Burr *et al.*, 2013). O'Gorman (2003) has described the relevant difference between keyspace and entropy as the keyspace is an absolute measure of the topmost or best-case, while the entropy is a statistical measure of how users select from the keyspace. Thus, the larger the keyspace and entropy are, the harder it is to successfully guess or break a password.

Usually, users choose their passwords from smaller subsets of the available keys which limit the full password space of the system (i.e. select only letters without numbers). For that reason, the effective password space is used to calculate the number of passwords

that users are likely to select (Thorpe & van Oorschot, 2007). However, measuring the effective password space accurately is hard due to the variation of schemes and user choice preferences (Gao *et al.*, 2013).

The way to calculate the theoretical password space can be illustrated as follows: if a textual password has 'N' characters chosen from an alphanumeric of 'M' characters, then the password entropy 'E' is represented as $E = log_2(M^N)$, and the password space 'S' is represented as $S = M^N = 2^E$ (O'Gorman, 2003). So the password is said to have E bits of entropy, and there are 2^E possible values. For instance, a password of 8 characters picked from 95 printable keyboard characters will produce $95^8 \approx 6.63 \times 10^{15}$ – this is approximately 2^{53} possible passwords and about 53 bits of entropy.

Generally, ensuring that the password space of graphical passwords is comparable to that of alphanumeric passwords is a major issue. Thus, success in achieving a relatively large password space is one important factor in claiming that the proposed scheme potentially has a good if not better security level. Nevertheless, password space size is not all that matters; password usability and memorability are also significant key factors. For instance, applying a system account lockout threshold should limit the number of failed authentication attempts and reject any further attempts. Hence, even if the password has low entropy, a guessing attack is unlikely to succeed easily (O'Gorman, 2003).

As far as the graphical passwords are concerned, three main factors determine the password space size of the majority of the draw-based/grid-based graphical password schemes: the density of the grid, the number of strokes and the length of each stroke (Haichang *et al.*, 2008). In most existing recognition-based schemes the password space is influenced by the authentication rounds, the number of images in each round and the number of targeted (password) images (Haichang et al., 2009). In click-based schemes,

the password space is usually sufficiently large due to the effect of the number of click points, image size and tolerance square.

	Approach type	Authentication Mechanism	Range of available selections	Length of password entry	Size of password space	Password Entropy (Bits)
1	Text-based	Textual Password	95 printable characters	8 alphanumerics	$95^8 = 2^{53}$	53
2		PIN Number	10 numbers	4 numbers	$10^4 = 2^{13}$	13
3	Draw-based	Draw-A-Secret (DAS)	5 x 5 grid size	length= 10	2^{48}	48
4		Pass-Go	9 x 9 grid size	length= 10		64
5		YAGP	48 x 64 grid size 3072 cells	20 strokes	$3072^{20} = 2^{232}$	232
6	Click-based	PassPoints	image size = 451 x 331 373 squares	5 click points	$373^5 = 2^{43}$	43
			image size = 1024 x 752 1925 squares	5 click points	$1925^5 = 2^{55}$	55
7		CCP	400 squares/5 images	5 click points	$(400 \text{x} 5)^5 \approx 2^{54}$	54
8		Multi-Factor Graphical Authentication	64 Clickable areas	8 Clicks	$64^8 = 2^{48}$	48
9	Choice-based	PassFaces	9 images/4 rounds	4 images	$9^4 = 2^{13}$	13
10		Déjà vu	20 images	5 images	$\binom{20}{5} \approx 2^{14}$	14
11		Visual Identification Protocol (VIP)	10 images	4 images	$10^4 \approx 2^{13}$	13
12	Typing-based	Zheng (Shape & Text)	5x5 Grid = 25 cells	13 strokes	$25^{13} \approx 2^{60}$	60
13		Komanduri & Hutchings Picture Password	80 images	8 items	$80^8 \approx 2^{50}$	50
14	Hybrid	Hong scheme	121 icons/4 rounds	4 icons	$\binom{121}{4} \approx 2^{23}$	23
15		TwoStep (Graphical step)	36 images/1 round	3 images	$\binom{36}{3} \approx 2^{13}$	13
16	OTP-based	GrIDsure	5x5 Grid = 25 cells	4 cell pip	$25^4 \approx 2^{19}$	19
17		Gao CAPTCHA	CAPTCHA length = 8 50 images	4 images		30
18		Passblot	26 possibilities	6 characters	$26^6 = 2^{28}$	28

Table 3-14: Password space sizes for some authentication schemes

Table 3-14 highlights the size of the password space and the entropy of various authentication mechanisms, considering a number of parameter settings and details. In this review, a collection of schemes was chosen to represent each authentication category. As mentioned earlier, the length of password plays an important role in calculating the password space. Thus, it should be noted that reasonable password lengths were selected for calculation in this study to avoid any unpractical enlargement of the password space results. For instance, the entropy of Pass-go scheme could reach 256 bits if the length of password increased to 30, but in reality, it seems difficult for many users to select and remember a drawing consists of 30 strokes. By exploring the data of the above table, some general outcomes can be inferred such as that the draw-based schemes can lead the providers of a large password space. As for the click- and typing -based schemes, they offer a comparable password space to that in textual passwords. It can be said that the password space provided by choice-based and hybrid schemes is relatively small. The password space offered by OTP-based graphical schemes seems reasonably average. More importantly, it was found that there was no specific method to calculate the password space for schemes of the same category, which might cause inconsistent results. Therefore, it is recommended to further investigate this issue and come up with standard methods and procedures for each category to calculate the password space consistently.

3.8. Challenges in graphical authentication

This section reviews and summarises the issues and disadvantages of the main graphical authentication techniques. Simply put, Table 3-15 outlines the specific issues of each approach as stated in the literature.

Category	Approach	Disadvantage
Recognition	Choice-based	Time consuming (Bhanushali et al., 2015)
		Easy to share with others (Dunphy, Nicholson & Olivier, 2008)
		Most suffer from a small password space size (Weiss & Luca, 2008)
		Usability issues due to the crowded content arrangement (Suo, Zhu & Owen, 2006) (Wiedenbeck *et al.*, 2006)
		Processing large number of icons reduces the system efficiency (Suo, Zhu & Owen, 2006)
		Many authentication rounds take users through several pages of images (Suo, Zhu & Owen, 2006)
		Can be influenced by gender/race or hot-image /category /theme /personal preferences (Weiss & Luca, 2008) (Davis, Monrose & Reiter, 2004) (Wiedenbeck *et al.*, 2006) (Suo, Zhu & Owen, 2006)
Recall	Click-based	Time consuming (Bhanushali *et al.*, 2015)
		High predictability (Renaud & De Angeli, 2004)
		Susceptible to hotspots/similar click-points (Gupta *et al.*, 2012) (Chiasson *et al.*, 2008)
		Difficult for users to pinpoint a precise position (Renaud & De Angeli, 2004)
		Remembering the click points and their order is difficult (Chiasson *et al.*, 2008) (Bhanushali *et al.*, 2015)
		Self-selected graphical codes have lower entropy than textual passwords (Renaud & De Angeli, 2004)
		Difficult to find an image which offers a wide enough range of available memorable locations (Renaud & De Angeli, 2004)
	Draw-based	Difficulty of using the input devices for drawing (Bhanushali *et al.*, 2015) (Suo, Zhu & Owen, 2006)
		Difficult to repeat the same steps/accurately duplicate password drawings with precise stroke order (Wu *et al.*, 2014) (Gupta *et al.*, 2012) (Bhanushali *et al.*, 2015)
		Difficult memory task because retrieval is done without memory prompts or cues (Biddle, Chiasson & Van Oorschot, 2012)
		Users' habit of drawing symmetric images with few strokes decreases the password space (Gupta *et al.*, 2012)

Table 3-15: Summary list of graphical password techniques' disadvantages

Time consumption seems one of the significant issues affecting the performance of the graphical passwords in general. However, entering image-based passwords should not be expected to perform better than text-based passwords from time perspective due to its very nature that requires a number of actions to complete the password submission. Additionally, learning and practicing the graphical password scheme would likely enhance the time taken for authentication but unlikely to shorten it to be competitive to textual passwords.

The user tendency of choosing obvious patterns or being attracted to certain images is an apparent challenge for choice-based schemes. Another difficulty is the number of images, distractors, and rounds involved in such type of schemes which eventually affect the overall system performance. Therefore, it is important to select proper configurations while designing a graphical scheme. One way of confirming the right numbers for the scheme components is through statistical analysis of perceptions of largely enough group of users to ensure that the scheme fits for the intended purpose.

Similarly, in click-based schemes users tend to select similar click-points which turn out to increase the predictability chances. One related obstacle of this approach is the difficulty of remembering the precise order of the click-points. Hence, it is essential to provide an image rich of memorable click areas to help users choosing easy to remember points. However, finding such images is relativity hard and needs careful selection.

Memorability tends to be a serious issue for the draw-based approach by which reduce the likelihood of redrawing the password accurately. Moreover, the less familiarity of using the input devices for drawing is another obstacle that may limit the adoptability of such schemes. However, with the widespread use of touch-enabled devices, users can easily utilise such devices to perform the authentication drawings.

Generally, most graphical password mechanisms depend mainly on visual displays which add fundamental accessibility barriers (Hochheiser, Feng & Lazar, 2008).

It is worth mentioning that although this section has gathered different challenges and disadvantages related to various types of graphical authentication, however, that does not necessarily mean that they apply for all schemes. On the contrary, many schemes have been introduced to overcome some of these reported issues in the first place.

In spite of the above-mentioned challenges facing the graphical password authentications, they can offer many other potentials and advantages such as passwords space enlargement, higher memorability, and complicating the disclosure of passwords in either written or verbal form.

3.9. Summary

In summary, there is a growing interest in replacing traditional text-based passwords with graphical authentication techniques. This chapter has focused comprehensively on graphical authentication schemes. Various types of graphical passwords from diverse range of categories have been reviewed to end up with an overall comparison including the advantages and disadvantages of this mechanism. Another outcome was the suggestion of an enhanced way of classification that led to introducing keyboard\keypad typing as a new input approach within the graphical password domain. From security prospective, the diversity between the authentication challenge and the data entry method can mitigate some common security attacks such as shoulder-surfing and keylogger.

The high potentiality of a combined graphical password alongside one-time password as an alternative authentication has motivated the research to locate a sort of on the ground application to prove its capability not only in theory but in practice as well. Besides, an

important aspect of designing graphical password schemes is the context of use which should be considered carefully in advance. That will help in addressing any authentication issues or requirements in such context and then examine the capability of the proposed solution to fulfil that needs.

It is important to note that the goal of this research is not to replace the textual password entirely but rather to realistically define a work context where the conventional authentication mechanism cannot satisfy the authentication requirements for that application. This research is particularly intended for scenarios in which both the service provider and the user expect a stronger level of security than traditional passwords, want something that remains usable, and do not want to invest in (or assume the availability of) tokens or biometrics. Thus, a critical system was chosen for further study, in particular, the online banking authentication system. This system is one of the sensitive and critical systems which is gaining a special attention from different parties i.e. end users, financial services providers, hackers and security experts. For that reason, E-banking was the selected system for this investigation. Additionally, this choice would be more supportive for the research direction if the target system was found to be in need for a kind of authentication enhancement that creates a real environment for evaluation.

The next chapter investigates the area of online banking authentication to address any system access issues and then seeks user's views on the proposition to use a graphical password as a solution for the predetermined login limitation.

Chapter Four

A Study of Users' Perceptions of

Online Banking Authentication

4.1 Introduction

The term online banking, also known as Internet banking, is commonly defined as a remote channel to deliver banking services electronically to customers. Online banking services include accessing account information, the transfer of funds between different accounts and making electronic payments and settlements (Dube & Gulati, 2005) (Federal Financial Institutions Examination Council 'FFIEC', 2003). A major advantage of online banking for customers is the convenience and flexibility of being able to bank anytime and anywhere without restrictions. In addition, banks are also attracted to providing services online since this should result in lowering the running costs than those incurred with physical branches (Xue, Hitt & Chen, 2011).

According to the joint report by the BBA and EY (The BBA, 2015), there was a 10% increase in the number of daily Internet banking logins for UK customers which reached 9.6 million – logins by March 2015. The report also revealed that the amount of online transactions was £2.9 billion per week. This shows the overwhelming trend towards the online banking services and the huge amount of money in transactions which is indeed worthy of higher protection.

Online banking is continually growing but is now faced with major challenges, one of which is the high risk of data being compromised. Thus, in order to reduce the threats to online banking and at the same time increase customer security, confidence and acceptance of this electronic service channel, the online accounts of customers must be securely protected via enhancing user authentication without adversely impacting upon the users' experience (Williamson, 2006).

Generally, there are several levels of online banking activities (Ramakrishnan, 2001) (Dube & Gulati, 2005). The informational is a basic level that includes information on the bank and its available online services, and this is of a relatively low security risk. The

communicative level which allows limited interaction tasks between banking systems and customers, such as updating static data (e.g. addresses) and account inquiries. Thus, there is an operational risk involved at this level. At the transactional level customers can execute banking transactions (i.e. e-payment, fund transfer). This level is the one associated with a high security risk.

The importance and criticality of the security of the wide range of banking services being deployed over the Internet is a major concern for both service providers and customers. Thus, extreme caution is always paid to safeguarding the e-banking system as well as customer information. The first line of defence is through protecting the authentication system from fraud and identity theft. Banks should carefully select from a variety of available authentication technologies and mechanisms to authenticate customers in a secure manner. These techniques include textual passwords, PIN numbers, (PKI) digital certificates, hardware devices; such as smart cards, one-time passwords (OTPs) and biometric identification (Williamson, 2006).

4.2 The provided authentication by leading banking institutes

In order to have a closer look at the authentication approaches offered by banking services providers, the study assessed the practices of the top four banks, as ranked by (relbanks.com, 2015), in the UK and Saudi Arabia on the basis that respondents from these countries would form the basis for later survey data collection. The purpose was to gain tangible results from a field review that investigate and compare different authentication experiences within the electronic banking domain.

The comparison data (valid on January 2016) was collected by visiting each online banking service of these banks to explore the provided authentication features. The services were compared based on the following factors:

- **Authentication options**: when more than one authentication method are available for the user to choose from (e.g. OTP hardware-token or subset digits of textual password). Combining more than one form of authentication mechanism is called **Two-factor authentication**.

- **Static password**: The conventional text-based password approach.

- **Subset digits of password**: challenges the user by requesting to submit different digit locations of the full password (e.g. 2nd, 4th, 7th digits of the static password).

- **Memorable information**: a type of personal questions that can be easy and short to answer by legitimate user.

- **OTP (SMS)**: a one-time password sent to mobile phone through carrier short messages.

- **OTP (Soft-Token)**: a type of one-time password that is generated by software application usually installed on smartphones.

- **OTP (Hard-Token)**: a special hardware device that directly generates a one-time password.

- **PIN-dependent token**: an additional protection feature to the Soft/Hard tokens where a PIN is needed to generate a one-time password.

- **Card-dependent token**: another additional feature to the hard-token device where a smart-card is required to generate a one-time password.

- **Authorisation site image**: a feature that allows the selection of a picture that will be displayed at every login time to indicate a correct access to the genuine online banking website and not a phishing website.

- **Authorisation personal image**: allows uploading a personal picture that will be shown at every login to ensure accessing the official online banking website.

- **Designation of safe computer**: a computer that typically being used to access online banking accounts can be designated to be recognised as a Trusted Computer, any access from any other PCs will be denied.

- **Audio PINsentry:** an audio card reader device that can optionally display the OTP code on the card reader screen or read it back to the user (audio).

	Bank	Region	Authentication options	Two-factor authentication	Static password	Subset digits of password	Memorable information	OTP (SMS)	OTP (Soft-Token)	OTP (Hard-Token)	Token needs PIN	Token needs Card	Other
1	HSBC Holdings	UK	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	
2	Barclays	UK	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	Audio PINsentry
3	Royal Bank of Scotland Group	UK	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	
4	Lloyds Banking Group	UK	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	
5	National Commercial Bank	SA	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	- Authorisation site image
6	Al-Rajhi Bank	SA	✓	✓	✓	✗	✗	✓	✓	✗	✓	✗	
7	Samba Financial Group	SA	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗	- Authorisation personal image - Designation of safe computer
8	Riyad Bank	SA	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	

Table 4-1: Authentications by leading banking institutes

The comparison table above shows the diversity of authentication techniques and features used to secure access to the electronic banking system. The text-based password is still occupying a key position among the used methods, appearing in different forms, such as fixed password, subset digits or memorable information. Usually, textual passwords are used in conjunction with other authentication methods such as one-time password (OTP) which in turn forms a two-factor authentication. In addition, the majority of banking

systems have fortified their systems by implementing two-factor authentication instead of relying on a single factor. One-time password is another significant method that has captured the interest of the banking system administrators. A number of banking systems have offered a various types of OTP implementations using short messages (SMS), hardware or software tokens with the support of some additional security features.

Furthermore, it can be inferred that some authentication features are widely applied in one country but not in the other. For instance, while most UK online banking systems, included in this study, utilise subset digits of textual password and memorable information, none of the Saudi Arabian banks offer such authentication technique. In contrast, static password is used in every Saudi Arabian online banking system, whereas, only one UK bank still uses such type of authentication. However, soft-token OTP has been implemented in Saudi Arabia a while ago and has also started to roll out recently in some UK banks. Notably, this part of the study was focused solely on the login authentication service which means it does not cover any further authentication like transaction-based authentication or adding a new payee.

4.3 Limitation of online banking authentication

Giving the option for the user to choose the appropriate authentication method is a fundamental usability feature that adds flexibility to the system. Despite the fact that this feature does exist in some current systems, it is realised that the available options depend mainly on giving the customer the choice of selecting between the use of a software/hardware token or SMS to obtain the required OTP or in some cases on phone banking services providing the required access. In addition, other systems may offer the traditional passcode option or allow authentication via a series of Q&A challenges in case the user is unwilling/unable to use the recommended secure authentication options. That might potentially lead to falling back into the weaknesses of the traditional textual

password. However, none of the discussed authentication options other than the text-based password offer in-session authentication which uses the web browser to process any extra login task. That in turn emphasises the dependency on an additional out-of-band means (e.g. token, mobile) to accomplish the authentication task.

More recently, many banks have adopted OTP authentication using hardware tokens that are supplied to each client as part of a multi-factor authentication scheme. Although this method is effective, it has a fundamental downside due to the reliance of the applied OTP authentication being mostly on a single OTP delivery method. Moreover, many online banking systems are not equipped with a secondary authentication method to back up the primary Soft-/Hard-Token OTP authentication. In other words, lost/ stolen/ forgotten/ damaged hardware tokens or smartphone will prevent clients from gaining access to the online banking system due to the absence of an operative alternative means of logging in under such critical circumstances. However, some online banking systems utilise an out-of-band method, such as mobile SMS messaging, as a parallel means of obtaining the OTP. Still, this service can encounter several problems, such as message delivery delay, weak signalling, roaming availability and charges (Weir et al., 2010) (The Royal Bank of Scotland ©, 2014). Therefore, the need for a secure, usable secondary authentication method to play an alternative role alongside the primary hardware-/software-based OTP scheme has emerged in cases where such tokens are unavailable.

OTP Type	Advantages	Disadvantages
Hard-Token	- Can be protected by PIN or chip & PIN.	- Additional device to carry around. - Different services may require different devices. - High cost. - Hard to reissue and replace. - Availability issue of being: lost, stolen, forgotten, damaged.
Soft-Token	- No need for Internet, the use of smartphones is wide spreading. - Several soft-tokens for different services can be installed on one smartphone. - Can be protected by PIN.	- Dependent on smartphone which might cause the same availability issue of the Hard-token (mentioned above).
SMS	- Very common and friendly service.	- Dependent on mobile phone which might cause the same availability issue of the Hard-token (mentioned above). - Service problems: message delivery delay, weak signalling, roaming availability and charges. - Not protected by PIN.
Prospective Solution	**Aims**	**Concerns**

	- No extra cost.
	- No need for additional devices.
	- No need for carrier services.
	- Can be protected by PIN or alike.
	- Can be deployed on different systems.
		- Need to ensure:
		  System security and usability
		  User perception and acceptance

Table 4-2: Comparative review of the OTP types

Table 4-2 presents a review of the advantages and disadvantages of different types of the one-time password (OTP) techniques. The review data was helpful to determine the prospective aims and concerns of the prospective solution as illustrated in the last section of the table. The listed aims form a baseline for the requirements needed to fulfil the

authentication gap in the current online banking system. Therefore, any new proposal should take the above mentioned points into consideration while planning the solution.

4.4 Research survey

Beside the importance of the authentication security, the ease of use and convenience of the authentication process are usability factors that also have a direct impact on security. Secure and usable authentication is a key factor in the adoption and expansion of the electronic commerce and banking activities. A significant concern for an effective security is the users' acceptance and willingness to apply the required security procedures (Schultz et al., 2001). Hence, investigating the effect of alternative authentication systems on customer perceptions is a necessary step.

Therefore, a structured questionnaire was designed and published to investigate the authentication issues associated with online banking in addition to polling to gauge the participants' perceptions and attitudes towards the current authentication methods for online banking. Another aim of the survey was to measure the user acceptance level of using a graphical password mechanism as a possible alternative within the context of online banking system.

4.4.1 Survey design and methodology

The survey was carried out over the Internet and was hosted online by the Centre for Security, Communications and Network Research at Plymouth University. The interface of the survey was bilingual, which offer the respondents the choice to view the questions either in English or Arabic language as the main expected languages within the regional distribution of the survey. Closed-ended questions were the most used form of questions in this survey to allow smooth gathering of information while keeping the participant's

task of completing the survey as simple as possible. In some questions, a Five-Point Likert's scale was used for more precise rated answers. In addition, illustrative images along with brief descriptions were added to some questions to ensure clarity and better understanding for users.

All users participated in this survey of their own accord, it was clearly stated at the beginning of the survey that participation is optional and withdrawal is possible at any stage. Moreover, the survey was designed anonymously throughout the entire process to ensure the confidentiality of the participants' information.

The survey was comprised of a total of twenty-nine questions divided into five sections. *Section 1* captured the respondents' demographic information, consisting of age, gender, education background, employment status and computing skills. *Section 2* studied the respondents' experiences of user authentication schemes and security-related techniques. *Section 3* acquired background information about the participants' usage of the banking system. *Section 4* analysed the respondents' experiences of authentication within the online banking system, while *Section 5* sought users' opinions and the acceptance level of the alternative authentication mechanisms.

The questionnaire began with two consent-related questions to confirm the age of the participant was 18 or above and to ensure their understanding of the provided information, which lead to obtaining the necessary agreement to take part in the survey. Following that, the respondent was taken gradually through the survey questions. In order to obtain a professional statistical analysis, the IBM Statistical Package for Social Science (SPSS) was used as an assisting tool to analyse the survey data.

4.4.2 Results interpretation and analysis

A total number of 250 respondents participated in this online survey over a period of 3 weeks of live time. Interestingly, the response rate was encouraging and exceeded the expectations of the researcher. As far as the survey data is concerned, responses were recoded where appropriate to aggregate similar answers with the aim of enhancing the outcomes of the survey. Moreover, the resulted percentages of the answers were rounded to the nearest integer number for easier representation of the data.

Demographics Variable	Categories	Response Freq.	Percent %
Age (years)	18-29	84	33.6
	30-39	107	42.8
	40-49	39	15.6
	50-59	14	5.6
	60+	6	2.4
Gender	Male	165	66.0
	Female	85	34.0
Country of Resident	United Kingdom	115	46.0
	Saudi Arabia	109	43.6
	Others	26	10.4
Educational Level	Higher education	109	43.6
	Postgraduate	97	38.8
	Further education	37	14.8
	Other	7	2.8
Employment Status	Employed	167	66.8
	Student	61	24.4
	Self-employed	9	3.6
	Other	13	5.2
Computer Skill Experience	Advanced	121	48.4
	Intermediate	118	47.2
	Basic	11	4.4

Table 4-3: Demographic information for participants

Descriptive statistics were used to analyse the demographic characteristics of the participants. Table 4-3 shows that nearly two thirds of the respondents were males and the remaining third were females. The age group between 30 and 39 years comprised the majority of the sample which represented 43 percent of the total number of participants. The residential location shows that almost 90% of the respondents resided either in the UK (46%) or Saudi Arabia (44%). Regarding the educational background, the highest percentage of participants (44%) had studied at Higher education level, while 39% were Postgraduates. As for the employment status, the highest percentage of participants (67%) were employed followed by 24% being students. In regard to the level of computer experience, most participants (48%) considered themselves to be at an advanced level followed closely by 47% at an intermediate level with only a small percent (4%) having a basic level of computer skills.

The result of the second section revealed that most respondents, over 90%, had used alternative authentication methods. ATM cards (chip & PIN) occupied the most used alternative methods with 78% of the participants having used them. One-time password came next with 57%. Moreover, a selection of both techniques together was made by almost half of the participants. Only a few participants, about 8%, stated that they had not previously used alternative authentication approaches. In regard to the importance of multiple levels of authentication where users are asked to go through several verification steps before gaining access, 62% of the participants were supportive of this technique agreeing that it is very important, whilst 28% stated it is important. On the other hand, only a few participants of less than 2% had an opposite view.

An important question asked in this section aimed to measure the users' opinions on carrying around multiple security devices to fulfil the authentication requirements of multiple online accounts. Table 4-4 demonstrates that most of the respondents opposed

the idea with 69% feeling that carrying multiple tokens is not convenient and 38%

thinking it is unnecessary. However, 38% of the participants said it is acceptable on

balance.

	Convenient		Necessary		Acceptable	
	Frequency	%	Frequency	%	Frequency	%
Agree	44	17.6	90	36.0	96	38.4
Neutral	34	13.6	64	25.6	71	28.4
Disagree	172	68.8	96	38.4	83	33.2

Table 4-4: Participants' opinion about carrying multiple tokens

With regard to the participants' knowledge about image-based authentication, the study

shows that more than three quarters (80%) of the total number of participants had prior

knowledge of various types of such authentication mechanism, as presented in Table 4-5.

The draw-based technique was the most known one with 70% followed by the

recognition-based with 28%, and the least known technique was the click-based with

25%. It was also found that 16% of the participants responded to this question had made

a cross selection of recognition-based and draw-based techniques both together.

Graphical password Technique	Frequency	Percent %
Draw-based	174	69.6
Recognition-based	71	28.4
Click-based	62	24.8
Never heard of these techniques	49	19.6

Table 4-5: Participants knowledge of graphical password techniques

Starting from the third section onwards, the participants were asked banking-related

questions. As per the survey results shown in Table 4-6, the vast majority of the

respondents, representing 94%, indicated that they were online banking users. Among

those users 66% were managing more than one online account out of which 56% had

between 2 and 5 online accounts. Noticeably, 23 respondents had more than five online

accounts, while approximately a quarter of the participants had a single online account.

In contrast, only a small percentage of participants, about 6%, had no online accounts to manage. The majority of those participants who do not use online banking had no bank account in the first place or they preferred to conduct financial transactions in person. Around two thirds of the online banking respondents stated that they access their online banking accounts on a regular basis (e.g. daily, weekly), while nearly a quarter of the respondents access their accounts occasionally (e.g. couple of times a month). The final part of this section investigated the purpose of using online banking services. The results showed that 40% of the participants were utilising this service to conduct a variety of online payment services, such as paying bills or transferring fund, while 36% of them used the service for checking bank account information/transactions.

Number of online banking accounts	Frequency	Percent %
None	8	3.2
One	70	28.0
2-5	141	56.4
6-9	14	5.6
10+	9	3.6
N/A	8	3.2

Table 4-6: Number of online banking accounts

The fourth section of the survey focused on the online banking experience. More than 85% of the participants' online banking systems required multi-factor authentication. Remarkably, one-time password authentication was offered by 90 percent of the participants' banks, as appears in Table 4-7. The most offered type of one-time password was found to be the SMS text message with 44% of the total responses, followed by the security hardware token device with 37%, while only a very small portion (8%) of the responses using software tokens. Furthermore, since most of the participants were from the UK and Saudi Arabia, a further analysis was carried out to assess the popularity of certain types of one-time password techniques in these countries. The findings indicated

that the most used technique in the UK was the security token device whereas SMS text messages recorded the maximum utilisation ratio in Saudi Arabia.

Type of OTP	Count	Responses %
None - the online banking system does not facilitate a One-time password	32	10.4%
SMS text message	136	44.2%
Hardware token device (Hard-token)	114	37.0%
Software token (Soft-token)	26	8.4%

Table 4-7: The offered types of One-time password

Table 4-8 illustrates that 76% of the responses pointed out that users were satisfied with using one-time password authentication, while in contrast a very small percentage of nearly 6% were dissatisfied with this type of technique. As part of multi-factor and one-time password authentication, the participants were asked if they had failed to login using these methods before. The result shows that 65% of the users had experienced failure in fulfilling the login requirements for several reasons, such as mistyping the code which came in the forefront (48%), the lack of mobile services (21%) and lost token/mobile (9%). However, 43% of these incidents occurred only rarely, while less than 3% happened frequently.

OTP experience	Frequency	Percent %
Satisfied	160	76.2
Neutral	38	18.1
Dissatisfied	12	5.7

Table 4-8: Participants experience with OTP technique

Those participants who had not experienced login problems were asked for their opinions on the possible causes of failure. From Table 4-9, it can be inferred that the results were relatively close to each other. The majority of responses (23%) indicated that forgotten token/mobile was the most possible reason followed closely by losing the token/mobile and mistyping codes (22%).

Login failure reasons (opinion)	Count	Responses %
Forgotten token/Mobile	41	22.8
Lost token/Mobile	39	21.7
Mistyped the code	39	21.7
Lack of mobile service	37	20.6
Token/Software failure issues	24	13.3

Table 4-9: Participants opinion about the login failure reason

The last section concerned about the participants' opinions of alternative authentication mechanisms. To start with, the respondents were asked about their agreement level regarding utilising visual secret images to enhance system security. The results demonstrated that 47% of the participants agreed to the use of images in this manner, whereas 17% had an opposite view point. In terms of accepting the idea of replacing or supplementing the existing one-time-password method with a graphical one-time password technique, the responses in Table 4-10 shows that almost half of the participants (49%) accepted the idea but in contrast less than a quarter (23%) rejected it.

Adopting graphical one-time password	Freq.	Percent
Strongly Accept	28	11.2
Accept	95	38.0
Neutral	69	27.6
Reject	52	20.8
Strongly Reject	6	2.4

Table 4-10: The adoption of graphical one-time password technique

Another question in this regard was about the participants' confidence in using an alternative graphical authentication method for online banking. 49% of the participants responded with "confident" and 26% with "un-confident", as appears in Table 4-11. Those respondents who showed no confidence were asked for their reasons which were varied. Quarter of them of about 33% chose insecurity of the system as their reason, 27% were concerned about the unfamiliarity of such technique, and 23% thought the technique is impractical. As the method is not yet widely adopted for use, that was considered a

reason for a small number of participants (17%) to feel unconfident. In addition, a complementary question was asked to those 64 unconfident participants to find out if fixing their identified issues in the previous question would help in changing their minds so they would accept and use the proposed alternative graphical authentication method. It was found that many respondents (41%) were uncertain about whether fixing these issues would make a difference or not. On the positive side, a quarter of the responses thought that they would use the alternative graphical authentication method if the issues they raised were fixed.

Confidence level	Freq.	Percent %
Very Confident	32	12.8
Confident	90	36.0
Neutral	64	25.6
Un-confident	59	23.6
Very Un-confident	5	2.0

Table 4-11: The confidence of using alternative graphical password method

Lastly, Table 4-12 reveals that more than half of the participants (58%) preferred to use the proposed alternative graphical one-time password authentication as a secondary (supplementary) one-time-password authentication alongside the current one-time-password system only when needed, while 23% preferred to use it as a replacement for the existing (primary) one-time-password authentication.

Usage Preferences	Freq.	Percent %
as a secondary (supplementary) method	118	58.4
as a replacement for the existing primary system	46	22.8
Not sure	33	16.3
Other	5	2.0

Table 4-12: Preferences of using the proposed authentication

4.4.3 Discussion of research survey

The collected survey data showed a diversity in the participants' experiences and knowledge about authentication and online banking. It appears that plenty of participants had a reasonable understanding of user authentication within the online banking environment. The positive record of participants' computer experiences indicates the development of users computing skills and their competency to perform more complex computer tasks. In addition, this can give the survey responses more credibility as most participants have the skills and knowledge that enable them to provide more accurate answers.

As per the survey results, it was found that a high percentage of respondents hold and manage several online banking accounts. This demonstrates a trend towards the utilisation of the online channel to simplify performing banking transactions as well as other account management tasks. Moreover, the result also emphasises the difficulty of using multiple security tokens to manage these accounts. Thus, many participants disagreed with the idea of carrying around multiple devices for login purposes describing it as inconvenient and unnecessary. Additionally, the results of the survey showed that a high percentage of the total sample number access their accounts regularly on a daily or weekly basis, which obviously proves the increasing popularity and demand of online banking services. Consequently, these critical accounts would need adequate protection.

One of the interesting results was the high percentage of responses indicating that the online systems of the participants' banks require multi-factor authentication as part of the security measures. Furthermore, many of those systems make use of the one-time password authentication method. More than half of the participants had already been using one-time password as an alternative method of authentication. That in turn represents the importance and feasibility of both techniques (multi-factor and one-time-password) for the online banking environment.

Interestingly, the results also revealed that the majority of respondents have had satisfactory experiences using one-time password techniques. In spite of this positive statistic, failing to satisfy login requirements for multi-factor or one-time password authentication has recorded a relatively high ratio but with rare occurrence frequency. By excluding half of the incidents (experienced failures) caused by mistyping the code, which is a common human mistake, it can be inferred that the lack of mobile service is the cause of many login failures. However, a number of participants have different views in this regard since they think forgetting or losing a token/mobile can be the main reason for login failure.

Although the satisfaction level with the existing one-time password methods is apparently high, that does not contradict with the need for consolidating the overall authentication mechanism for such a crucial system. In other words, the current system is able to some extent to fulfil the authentication need of large amount of clients and reach to the functioning expectations of many clients and providers of online banking services, however there are some cases where some clients can find themselves unable to access their accounts because of the inability to fulfil the login requirements for the primary authentication method and at the same time the absence of secure alternative authentication methods. From here the demand for further investigation and consideration of this issue has emerged. The authentication system should cover most possible login scenarios to ensure high availability and less restriction authentication system. Figure 4-1 illustrates the limitations of the current online banking authentication methods and shows how the new proposal of graphical authentication can fit into the context and overcome the existing shortcoming.
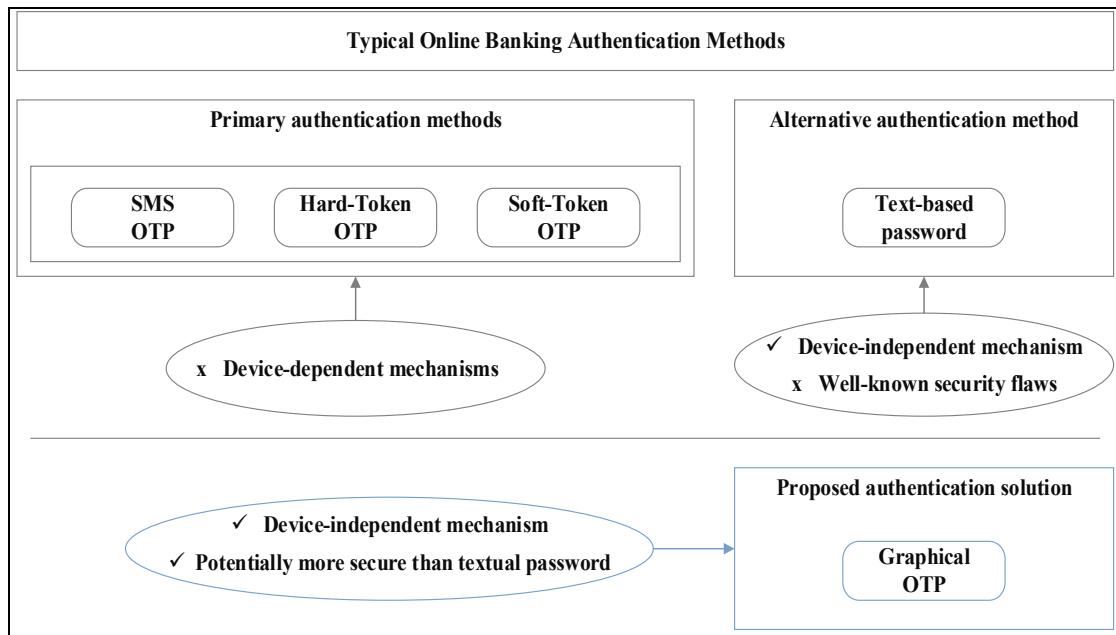
Figure 4-1: The limitations of the current online banking authentication methods

Of those respondents who indicated they have prior knowledge of image-based authentication, the majority have specified the draw-based graphical authentication as the technique they know most. This was expected, as this type of authentication includes the unlock pattern scheme which is widely used on many smartphones in recent time. However, knowing about recognition-based and click-based schemes by a number of participants is generally a good indicator towards the spread of graphical password authentication. Thus, this can be a motivation finding for the graphical authentication research area since new techniques in this domain will be less resisted by users in contrast to those schemes that being completely new and never been known before.

The aim of the final section of the survey was to determine participants' views towards alternative authentication mechanisms. Specific questions were asked about graphics utilisation for authentication purposes which were positively answered with acceptance of such technique's implementation. In addition, the participants were asked about how acceptable it would be to replace or supplement the existing one-time password system with graphical one-time password system. The result was somewhat astonishing as a large

amount of participants were open to the idea of using such graphical authentication in the context of online banking system with confidence. The concern regarding insecurity and unfamiliarity of using the alternative graphical authentication method was found to be the main potential threats to the participants' confidence towards this type of technique. Nevertheless, part of those respondents showed their willingness to accept and use the proposed alternative scheme whenever their raised issues are fixed. However, asking such exploratory questions have been useful in order to understand the concerns of those who were not in favour of graphical authentication. Despite this fact, the survey result shows that participants seem ready to accept the alternatives.

With regard to the preference form of using the proposed system, many respondents have preferred to use it as a secondary means of authentication to be used side by side with the existing primary one-time password system. Primarily, choosing this implementation option in this stage seems sensible choice that should reduce any potential risk by conducting complete replacement of the current system. On top of that, having this alternative graphical one-time password in place should positively influence the usability of the online banking system while maintaining its security.

From the viewpoint of the researcher, equipping the online banking system with a graphical authentication technique is one step forward towards a robust and flexible authentication system. Currently, the goal is to patch the shortage within the existing system (as shown in Figure 4-1) then it would be worthwhile to examine the suitability of the proposed solution for other roles of authentication such as being part of the primary multi-factor authentication, resetting password process, or adding new beneficiary. Later, the proposed solution may act as a practical model that enables measuring the user satisfaction, and familiarity with such technique as well as the method limitations to properly plan a further system enhancement or different application utilisation.

Interestingly, the respondents overwhelmingly accepted the initial form of authentication that makes a combined use of two significant techniques; the graphical password and one-time password, which might show the participants' preference to have some sort of alternative authentication methods. Thus, the researcher believes that having this type of alternative authentication should add a remarkable feature to the field of user authentication. Moreover, implementing the proposed scheme is hoped to boost the usability as well as security of the online banking system.

4.5 Summary

This chapter presented a comparative review of the authentication methods provided by a number of online banking systems. The goal was to obtain an actual data to explore the authentication-related aspects that need enhancement. The review concluded that many online banking systems provide authentication methods utilising one-time password as part of the two-factor authentication. In spite of the effectiveness of such methods, they still rely on a single source to deliver the generated OTP. In cases where the offered OTP technique is not available (i.e. forgotten Hard-token, technical difficulty in receiving SMS), authentication process cannot be carried out and therefore users will be prevented access to the system.

With the idea of further addressing the above-mentioned findings, this chapter presented the result of the conducted online survey that investigated the user experience with various types of user authentication methods in general and with online banking in particular. In addition, the questionnaire aimed to understand the participant's opinion about a new form of authentication method using graphical one-time password.

The results showed that many participants manage multiple online banking accounts, most of which use OTP. Although the majority of participants were satisfied with the

OTP authentication, they find it inconvenient to carry around security devices. Moreover, many participants were unable to accomplish their login requests as the OTP cannot be obtained due to the lack of mobile services or lost token\mobile. This part of the survey clearly confirms the finding of the earlier review of the online banking limitations discussed in (section 4.3) that there is a shortcoming in the current provided authentication services as a result of the dependency on additional devices or the availability of the mobile network services. That is also in line with what previously mentioned in the related literature in (section 2.4.2).

The survey also investigated the participants' acceptance to use a graphical one-time password technique instead of or in parallel with the current OTP methods. Almost half of the responses were positive and, more importantly, participants stated that they would be confident to use the proposed solution for online banking. The results of this part give an encouraging impression since many users were in favour of the idea of the graphical one-time password and willing to use it in a critical system like online banking.

Based on the results and findings of this study, the research will proceed by introducing and developing the proposed graphical one-time password scheme with the anticipation of solving the aforementioned problems.

Chapter Five

Graphical One Time Password System (GOTPass)

5.1 Introduction

The interest in the graphical authentication mechanism is derived mainly from the believe that graphical passwords might be less susceptible to several drawbacks of the conventional textual password including both aspects of usability and security (e.g. memorability, guessing, shoulder-surfing, spyware, credential theft, revealing password, writing password down).

The previous chapters have provided detailed review of the current state of graphical authentication techniques and studied the users' experience with authentication in general and within online banking environment in particular. Besides, the study explored the users' attitudes and preferences toward alternative authentications especially graphical authentication.
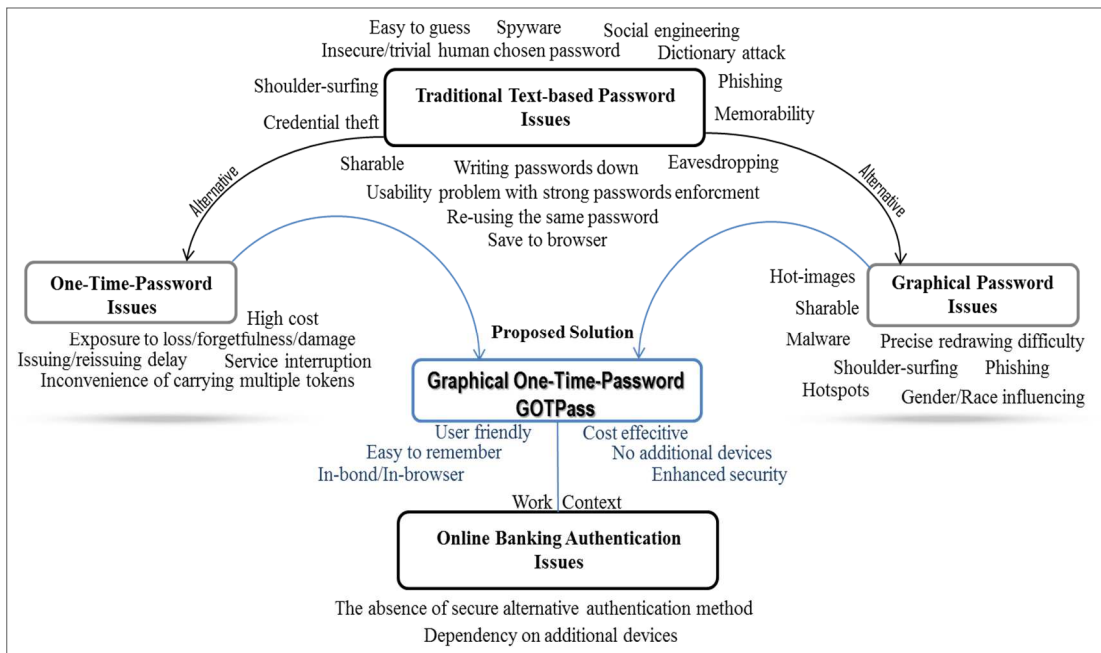
Figure 5-1: General linkage diagram between the research issues and the proposed solution

The conducted review of the current state of graphical authentication techniques along with the outcome of the study has pointed out to the need for an enhanced authentication method to fulfil the security and usability requirements. This research aims to overcome the major issues within the existing graphical passwords to obtain an improved scheme

that can be utilised to fill-in the authentication gap in the online banking systems (Figure 5-1).

According to the study conducted by Renaud (2004) to quantify the quality of various web authentication mechanisms, the quality of one-time password mechanisms for the web environment was high (8.99 out of the highest quality coefficient of 13) but lack a critical requirement with respect to the need for a special hardware/software. Semantic password mechanisms came second with quality of 7.9 and then recognition-based mechanisms with 7.72. Based on these results, a conclusion can be drawn that joining some of these authentication mechanisms can potentially produce a considerable secure alternative mechanism.

Therefore, the research in this chapter will continue towards the design and implementation of a new hybrid authentication solution named "**G**raphical **O**ne **T**ime **Pass**word" (GOTPass), which uses graphical authentication techniques to produce a one-time password that can be also viable for use in a context like online banking.

This stage of the work would not be particularly confined to the online banking environment, since the proposed scheme under investigation is considered to be generally applicable in many other systems as well. Therefore, the study at this level is independent and not limited to the online banking domain.

5.2   Prototype designing

In order to practically prove the concept and feasibility of the proposed solution, a prototype was developed with consideration of the testing and refinement cycle that properly shaped the final version. Moreover, specific evaluation criteria were defined to enable an appropriate assessment of the assurance and suitability of the proposed method

as an alternative means of authentication. The design and operation of the new technique is discussed in details in this section.

5.2.1 Arguments for GOTPass scheme

One of the significant features of an image-based authentication technique is the ease of recall, which is something that a conventional text-based password lacks. Thus, this has motivated the research to investigate and develop an enhanced graphical authentication mechanism. However, most recognition-based graphical password schemes are vulnerable to observation attacks (e.g. shoulder-surfing), due to their very nature of being visible to surrounding peepers. Therefore, a user-friendly graphical technique (unlock pattern) was employed that acts as a front-line defender before the recognition-based technique. Moreover, the role of the unlock pattern can be similar to the PIN-protection that is used to fortify the Hard-/Soft- token. That is also in line with the results of an earlier online survey conducted to measure participants' experience with user authentication (Chapter four - 4.4.2), which showed that the draw-based technique (android unlock pattern) was chosen by about 70% of the participants as the most familiar technique among other graphical authentications. Similarly, another field study carried out for 21 days confirmed that users were in favour of the pattern mechanism despite the repeated errors they made (Von Zezschwitz, Dunphy & De Luca, 2013). According to Chiang and Chiasson (2013), the Android screen unlock technique is the most well-known deployed graphical password. Finally, the system's security is strengthened by the implementation of the OTP technique. Moreover, the use of one-time password (OTP) technologies have been spreading, as 90% of the survey's respondents stated that they used this type of authentication technology, and they did so with an overall satisfaction rate of 76%. Table 5-1 summarises the rationale behind the selection of these various authentication techniques.

	Authentication technique	Rationale of selection
1	**Pattern unlock**	Protect the main image-based scheme User-friendly and familiar
2	**Image recognition**	Easy to remember Easy to use
3	**GOTPass input format**	Add a security feature

Table 5-1: Rationale behind the selection of various authentication techniques

5.2.2 Characteristics of GOTPass scheme

GOTPass is a hybrid secure solution that leverage a multi-layer authentication to ensure a robust secure authentication. An integration of multiple authentication mechanisms has been employed utilising a graphical password along with a one-time password. Moreover, a combination of various graphical password methods has been implemented to form a mixed technique of Recall-based [Draw] and Recognition-based. The final component of this authentication system involves a determination task of GOTPass input format which indicate the location of the associated random codes. More precisely, the method is established by solving the unlock pattern (draw-based), followed by identifying pass-images (image recognition) and the last step will be to enter the corresponding OTP codes according to the pre-chosen format (knowledge-based).

As illustrated in Table 5-2, the proposed scheme GOTPass is a hybrid technique falling under several categories of graphical authentication. First is a pure recall-based where two recall operations are required to be performed; redrawing an unlock pattern and determining the OTP input format. Second is recognition-based where users need to recognise their images.

	Category		Approach		Style
	Recognition	Pure–Recall	Draw	Typing Entry	Image
Graphical One-Time Password **GOTPass**	✓	✓	✓	✓	✓ M
				M= Multi	

Table 5-2: Categories and characteristics of GOTPass scheme

The process flow for the registration and authentication phases is summarised in Table 5-3, which defines the requirements and procedures for each phase as well as showing the authentication classifications of each part.

General process flow	Registration phase	Authentication phase
Secret knowledge (username)	- Select a unique username	- Enter the correct username
Unlock pattern Graphical password (recall-based, draw)	- 4×4 pattern grid will be displayed - The user needs to draw a secret pattern in any preferred shape	- Unlock the pattern grid by redrawing the pre-chosen secret pattern
Image recognition Graphical password (recognition-based)	- The system will assign four random themes for the user - A panel of images from each of the assigned themes will be presented and the user will make his/her own selection	- The system displays a 4×4 panel of images containing two random pass-images out of the four previously registered pass-images, plus 14 decoy images - The user needs to identify the two pass-images
One-Time Password Knowledge-based (Typing-based entry)	- Since the left & top edges of each row and column of the panel will be assigned 4 random digits, the user can choose from two available security level options: basic or advanced. Each level has two different GOTPass input format combinations and the system will randomly assign one to the user	- Enter the associated GOTPass code with each image based on the previously chosen format and in the correct order

Table 5-3: Process flow details for the registration and authentication phases

The system consists of 400 images in total, distributed on 12 different themes; namely 'Animal', 'Clock', 'Computer', 'Earth', 'Flag', 'Food', 'House', 'Paint', 'Sign', 'Sport', 'Stationery', and 'Transportation'. The number of images and themes were determined on an empirical dynamic basis and do not necessarily represent optimal settings. They were simply used to demonstrate the capabilities of the prototype system. The selection of these themes for this prototype was based on their representation of daily or commonly seen images aiming to help in making them easy to remember. Each theme contains an average of 33 images, all of which were taken from a free Internet source for images (www.iconfinder.com) available under different types of licenses (see Appendix B) and processed for study purposes only. Images were 128×128 pixels in size and chosen manually to ensure suitability for the intended theme and to prevent repetition. However, acquiring suitable images for the authentication purpose is quite difficult since the memorability and the security of the mechanism can be affected by the characteristics of the available images. Thus, the image acquisition process should consider the following basic properties:

- image quality that ensures a display of the image at a high enough resolution on various displays using the same size.
- easy to name images for better memorability.
- secrecy of the user's images to remain difficult to guess.

However, image properties are often difficult to test in isolation which complicate the task of acquiring suitable images to be used in the context of graphical authentication (Renaud, 2009).

5.3 Registration

The registration stage involves four main phases; user information, unlock pattern registration, pass-images selection, and input format determination (Figure 5-2).

Registration

Enter user information

Draw unlock pattern

Choose pass-images

GOTPass input format selection
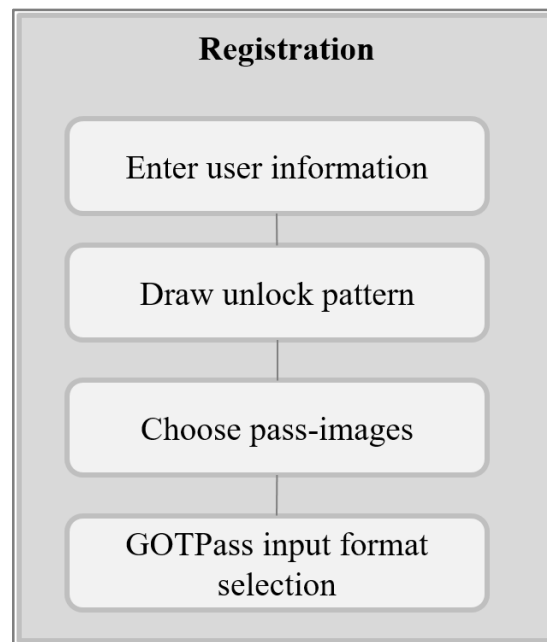
Figure 5-2: Registration process flow diagram

5.3.1 Unlock pattern

Creating a password pattern is formed by connecting several grid points that appear as a sequence of straight lines on the grid. For a successful login, the registered pattern needs to be recalled and redrawn correctly.

In GOTPass scheme, the user first needs to choose a unique username and draw any shape on a lock pattern grid. This pattern scheme is similar to the original Android unlock pattern scheme but differ in the grid size where it uses a matrix size of 4×4 to offer 16 contact points. The aim of utilising larger grid was to increase the security of the proposed system as well as keeping the simplicity of swiping to draw a password. As a web-based scheme, drawing the pattern can be performed by mouse or swiping finger on the touch-enabled devices. The following grid representation (Figure 5-3) is used to designate the 4×4 unlock pattern.

Figure 5-3: Pattern nodes representation

The rules and constraints of the 4×4 unlock pattern scheme is detailed as follows:

1. A minimum of 5 nodes should be connected (and obviously, not more than 16). That is to ensure no straight strokes are used.

2. Starting point can be made from any node.

3. One or several 'knight moves' can be used which can connect to non-neighbour node, such as (1, 7, 11, 10, 4) in the following illustration Figure 5-4:
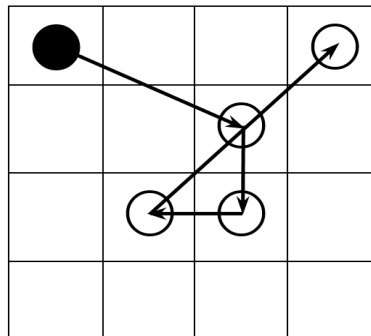
Figure 5-4: Example of the knight move (between 1 & 7).

4. Going over (jump) an unvisited node without connecting it is forbidden. For example, the pattern (1, 3, 7, 6, 5) is illegal, because moving between (1) and (3) must visit (2) in the middle.

5. Passing over a visited node is possible but without connecting it again. For example, both (1, 6, 7, 5, 2) and (1, 6, 5, 7, 2) are legal. In the last example (1, 6, 5) were visited then (6) was passed over again to reach (7, 2).

6. Moving between nodes must only be in straight lines.

7. Direction may only be changed when visiting a node.

138

5.3.2 Selection of pass-images

As pointed out by Biddle, Chiasson and van Oorschot (2012), allowing users to choose their own passwords can enable a personalised attack where the probability of guessing the user's password by a person who knows the user might be higher than other attackers. In further support of that claim, Davis, Monrose and Reiter (2004) stated that users will keep selecting predictable passwords, therefore giving the user the option to choose a password is unadvisable. On the other hand, system assigned images lead to usability issues derived mainly from the difficulty of remembering random images (Chiasson *et al.*, 2008). Due to the conflicting problems mentioned above, a new balanced approach has been adopted to benefit from the advantages of both techniques and overcome their problems. The idea is to have themes assigned by the system and then give the user the chance to select the favourite images within those specific assigned themes. This can reduce the bias choice, hot-images, and personal preference images but at the same time should keep the task simple for users to remember their own selection of images.

In this step, the system will automatically assign four random themes for the user, one after another in a separate page. The name of the random theme will be displayed on the top of the page. Each theme will display 30 images (Figure 5-5) for the user to select one pass-image from each of the given themes (a total of four altogether). This is called the pass-images portfolio, which aims to provide a dynamic pass-images pool without requiring memory recall from the user. Furthermore, the pass-images portfolio can also provide a sort of challenge-response protocol since the system will challenge the user with a subset pass-images at each login time.
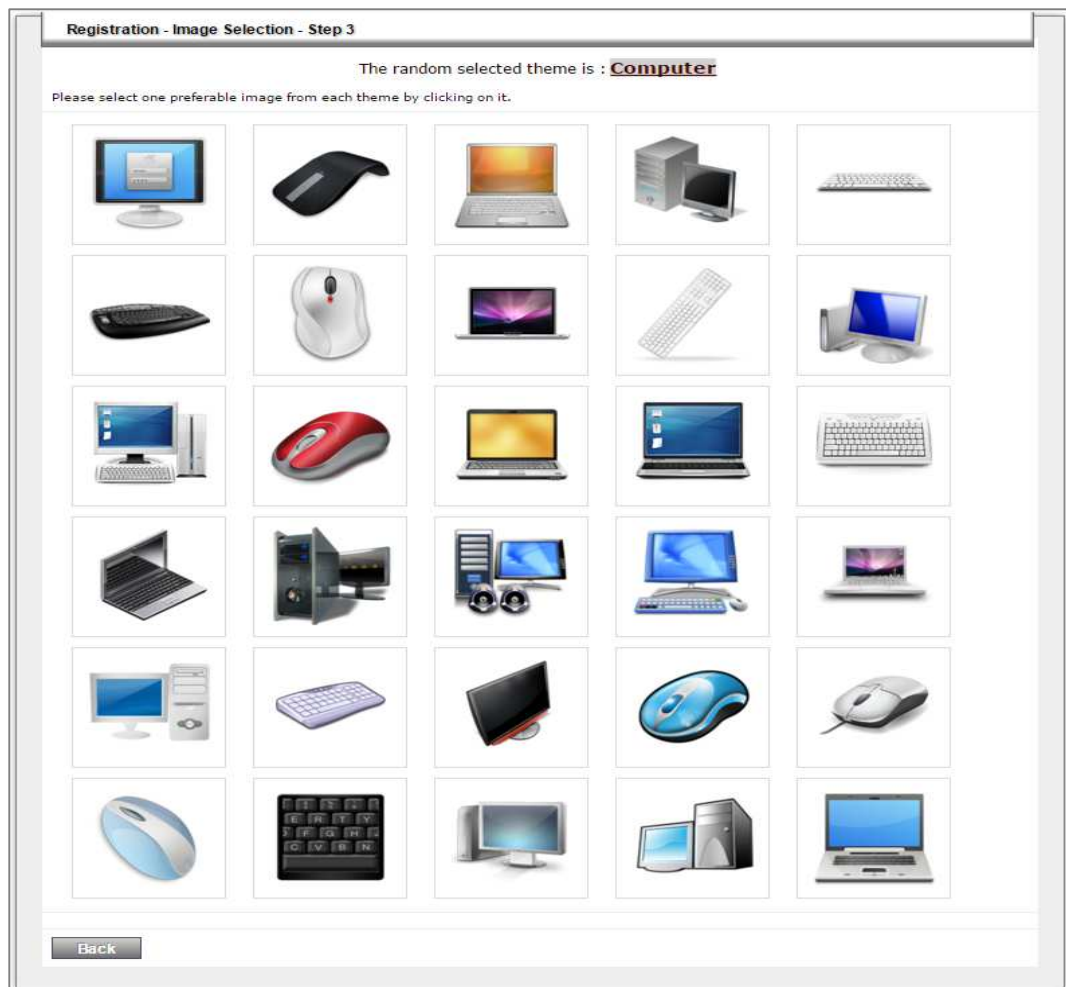
Figure 5-5: Registration - Pass-images selection

Determining the number of pass-images to be four in this scheme was in accordance to some similar schemes which implemented the same number of password images such as VIP3 (De Angeli *et al.*, 2002). Besides, in a study by Suo, Zhu and Owen (2006) which had no restriction on the number of secret images to be selected, they found that the number of the chosen images by 80% of the users did not exceed four.

The user needs to select the preferred image on each page by clicking on it. The system then displays a pop-up confirmation screen (Figure 5-6) to ensure that the user is happy with the selected image. For a security purpose, the number of theme's images in the database is always larger than 30 which ensures that the displayed set of images is always changeable. Moreover, that should also prevent any adversary from acquiring the entire images which can be used to build a fake system to deceive users.

Figure 5-6: Confirmation of the selected pass-image

5.3.3 Determination of input format

The position of the pass-images in the grid will be used to indicate a code that needs to be entered using the keypad/keyboard, which is referred to as the GOTPass input format. These codes are located on the top or left-hand axis of each pass-image as illustrated in Figure 5-7.

Figure 5-7: Registration - Input format

There are two security level options for the user to choose from: basic or advanced. At the basic security level, the numeric codes for both pass-images are taken from the same axis, whereas the numeric codes in the advanced level are taken from different axis for each pass-image. Inside each level there are further code combination options for the system to randomly assign to the user. The assigned input format is clearly presented to the user with an illustration example (e.g. top axis for the 1st pass-image + left axis for the 2nd pass-image). The GOTPass input format is implemented to hinder the observation attack as each pass-image can have various code combination options. Table 5-4 shows details of the GOTPass input format combination options.

User choice	Random system assigning		
Security level	Option	Pass-image	Code
Basic	Option **1**	**1st** pass-image	from **TOP** axis
		2nd pass-image	from **TOP** axis
	Option **2**	**1st** pass-image	from **LEFT** axis
		2nd pass-image	from **LEFT** axis
Advanced	Option **3**	**1st** pass-image	from **TOP** axis
		2nd pass-image	from **LEFT** axis
	Option **4**	**1st** pass-image	from **LEFT** axis
		2nd pass-image	from **TOP** axis

Table 5-4: GOTPass input format combination options

Finally, on the lower part of the last registration page, the system will display the four selected pass-images (see Figure 5-7) as a way to remind the users of their selections before hitting the button to create the account.

For security enhancement, the system stores three random images from distinct themes in association with each chosen pass-image as illustrated in Figure 5-8. Thus, in total the system will store 4 pass-images and 12 distractor-images for each user. The role of the

so-called distractor-images is to be displayed alongside the original pass-images in every login attempt to confuse the illegitimate peepers.
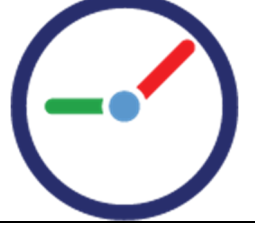
	Pass-images	Distractor 1	Distractor 2	Distractor 3
Pass-image 1				
Pass-image 2				

Figure 5-8: Example of the associated distractor-images

5.4 Authentication

The login part of the system comprises of four steps; the username and unlock pattern, pass-images recognition, and GOTPass code determination and entry (Figure 5-9).

Authentication

- Enter username
- Redraw unlock pattern
- Recognise pass-images
- Determine & enter GOTPass code combination
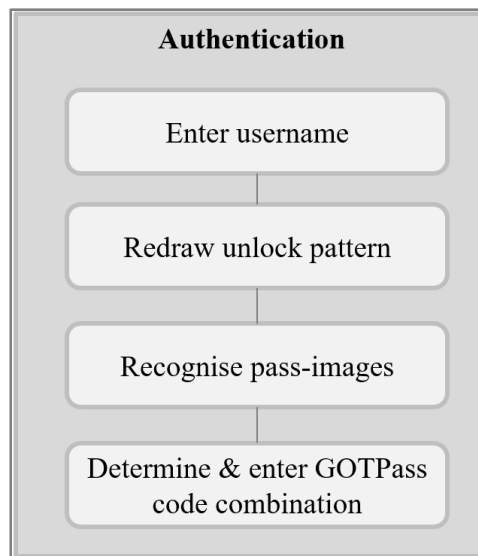
Figure 5-9: Authentication process flow diagram

5.4.1 Unlock pattern

At first, the system will prompt the registered user for their username and display an on-screen unlock pattern (Figure 5-10), which requires the user to redraw the pre-registered unlock pattern shape by connecting nodes together to re-form the correct pattern shape.
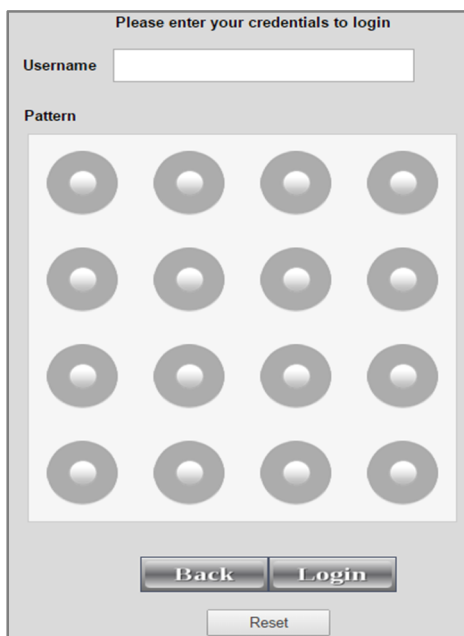
Figure 5-10: GOTPass unlock pattern step

5.4.2 Recognition of Pass-images

The image-based step consists of 4×4 grid of images with an extra top row and left column to accommodate the random codes. The 4×4 layout was designed to be easy and quick for users to search for their pass-images among other images and at the same time maintain the potential security of being hard for illegitimate user to distinguish those pass-images. Moreover, the chosen layout was also motivated by several previous studies. The personal observations by Citty and Hutchings (2010) led them to use the 4×4 matrix of images for their 'TAPI' scheme. Similarly, the challenge set used in the experiments conducted by Jebriel and Poet (2011) comprised of 16 doodles.

The display of the content of the image panel depends on the correctness of the provided information of the previous step (username and unlock pattern). Firstly, the

authentication process will display a fresh (4×4) image panel containing dummy images when the information given in the previous step is incorrect. The implementation of this technique serves as an implicit authentication feedback to protect the scheme from a guessing attack and trial & error method, since the system gives no indication of which step in the login process was incorrect, and therefore confuses the attacker. However, the inability to spot the correct pass-images by legitimate users acts as an alert that something went wrong with that login attempt which they need to correct.

Secondly, in case the preceding step is correct, the panel will contain two random pass-images out of the four previously chosen pass-images (as illustrated in Figure 5-11), six distractor-images that are associated with the pass-images (three for each) and another eight random decoy images. However, the system will coordinate the distribution of the pass-images to ensure that both are never placed on the same horizontal-axis (row) neither the same vertical-axis (column).

As a fundamental part of the authentication process, the user must identify the password images among others in the panel (this is done only mentally, there is no need to touch/click on the images). The search navigation for the pass-images should be carried out on a row basis starting from the top-left corner down to the bottom-right of the panel.

5.4.3   Determination of GOTPass code

The system generates new OTP codes and fills the panel edges (axis) of each row and column (only the locations that are occupied by the correct pass-images will contain the correct GOTPass codes). Therefore, each image has two four-digit random numbers, one presented on the horizontal-axis and another on the vertical-axis. From the grid top or left axis, the user needs to locate and enter the codes associated with each pass-image (these should be entered in the correct format, as previously assigned and shown in the

registration phase). In other words, the user has to combine the 4 digits of the first pass-image with the 4 digits of the second pass-image to form the final 8 digits OTP code. Moreover, it is necessary to select the pass-images and, thereafter, the associated codes in the correct order depending on which pass-image appears first.

To enter these credentials, the user is required to use a separate means than the challenge one; keyboard or keypad. The idea behind that is to enhance the security of the graphical passwords by avoiding the unshielded mouse clicks. A study by Jebriel and Poet (2011) suggested that using keyboard for inputting graphical passwords was more secure than mouse selection.

Once the system ensures that all of the information that has been provided is correct, then the user is successfully authenticated and granted access.

Figure 5-11: GOTPass image recognition and OTP code entry
Assuming security level option 3 is in use (top axis code for the first pass-image + left axis code for the second pass-image)

5.5 Prototype development

Following the completion of the GOTPass design, the development of the prototype started to prove the concept of the proposed solution and to enable carrying out actual evaluations. The GOTPass prototype was developed as a web-based application using Microsoft Visual Studio 2013 – C#, and SQL Server 2012 as the Database Management System. The prototype application was hosted on a laptop with 15.6" touch screen display set at a resolution of 1366 × 768 pixels and running windows 8.1. As far as the associated coding work is concerned, it should be noted that the prototype development was supported by an additional developer, Farhan Jamil, who was contracted to carry out the coding under the direction of the researcher. However, all supporting aspects for this activity, such as application and database designs, have been finalised and documented exclusively by the researcher (i.e. the developer was not involved in the creative design or contribution to the research).

From a developmental perspective, the system was simply designed to save the application images on the web-server and store their unique IDs (based on a naming convention) into the database. In a preparation step, all images were categorised and arranged into their relevant themes. During registration, users are asked to provide their names and username, which will be checked against duplication before accepting it, and then a pattern must be drawn. In the background, the system deals with patterns in their digital representations as described earlier in Figure 5-3. In case of making mistake or dislike the drawn pattern, there is an option to clear the provided information and start over again. Next, the system selects 4 random themes and displays the related images of each one separately in sequential pages. Last, the system chooses one of the two security level options for the user who still be able to change this selection as preferred. However, the user is unable to change the input format inside each security level which is assigned automatically by the system. To complete the account creation (registration), the submit

button needs to be clicked which will insert a record for that specific account into the database.

The system tracks each step throughout the registration process to attain statistical data for further analysis. In line with the account creation process, a record is added into the database containing the start and end times of several elements; username entry, drawing pattern, selecting (4) pass-images, and determining the GOTPass input format (Table 5-5).

Description of log data	Remarks
User ID	Unique number to identify every user.
Start time of typing user information	Begins when the user puts the curser on the user full name field and starts typing in.
End time of typing user information	Finishes when the user starts the next step; drawing the unlock pattern.
Start time of drawing pattern	Begins when the user clicks to draw the pattern.
End time of drawing pattern	Finishes when the user clicks on the 'Register Pattern' button.
Start time of choosing images	Begins when the user clicks on the first image.
End time of choosing images	Finishes when the user confirms the fourth pass-image by clicking on 'Yes, go to next step' button.
Start time of selecting GOTPass input format	Begins after the upload of the input format page.
End time of selecting GOTPass input format	Finishes when the user clicks on the submission button.

Table 5-5: Description of the registeration log data

During authentication, after inputting the username and unlock pattern, the system fills the login grid with 2 pass-images (selected randomly out of the registered 4 portfolio images) along with their 6 associated distractor-images and other 8 arbitrary chosen decoy-images. The system then generates two sets of random 4-numerical codes and place them in the designated boxes corresponding to the correct pass-images whereas the remaining boxes are filled in with other arbitrary codes. Hence, a successful login attempt

requires identifying the pass-images and entering their associated one-time codes in the right order.

To obtain a statistical data for later analysis, the system also tracks each step throughout the authentication process. With each click on submit button, the system inserts a record into the database linked to that particular user. Regardless of the correctness of the login attempt, the record contains some significant data as described in Table 5-6.

Description of log data	Remarks
The username used for login	Whether the username is correct or wrong
Authentication status	Overall assessment – Success/Failure
Date/time of the login attempt	Record the date and time when the login was occurred
User ID for correct/existing user	Leave blank if the username does not exist
Start time of typing username	Begins when the user puts the curser on the username field and starts typing in.
End time of typing username	Finishes when the user starts the next step; drawing the unlock pattern.
Success status of username	Individual assessment, if the username is correct or not (OK=1, NO=0)
Start time of drawing pattern	Begins when the user clicks to draw the pattern.
End time of drawing pattern	Finishes when the user clicks on the login button.
Success status of pattern	Individual assessment, if the drawn pattern is correct or not (OK=1, NO=0)
Start time of login GOTPass input format	Begins when the image-based page uploads.
End time of login GOTPass input format	Finishes when the user clicks on the submission button.
Success status of GOTPass input format	Individual assessment, if the provided OTP format is correct or not (OK=1, NO=0)

Table 5-6: Description of the authentiaction log data

It should be noted here that the activity log for the last element – GOTPass input format was not as effective as expected. In its current state, it only checks the correctness of the code similar to that done by the 'Authentication status'. The ideal action should be to check each part of the code (4-digits) aside and find out whether that specific part is correct or otherwise. Not only this but also should be capable of determining which combination option of the GOTPass input format (as explained in Table 5-4) was followed based on the analysis of the entered codes compared to the available codes on the login grid edges. That means that there are some other cases that should be considered to allow better and more precise analysis such as: code could be mistyped, the input format option could be correct even though the final code was wrong, the input format option could be wrong even though the selected pass-images were correct, or the input format option could be partially correct (one of the two codes is correct) (Table 5-7).

	Pass-images	Input format option	Final code
1	✗	✓	✗
2	✗	✓	✓ (coincident)
3	✓	✗	✗
4	✓	✗ (one correct code/ missing order)	✗
5	✓	✓	✓
6	✗	✗	✗

Table 5-7: Input format cases

5.6   Piloting, testing and evaluation

The development process went through the essential phases including testing and modification. The goal of the pilot phase was to test and confirm that the proposed solution would function as it is supposed to, otherwise, it undergoes the required

refinement. In other words, testing was helpful in identifying faults, which in turn brought in considerable improvements to the system.

Passing the testing phase successfully made the prototype ready for real experiment's deployment involving users to take part in the trials and provide their valuable comments and feedbacks. Generally, user evaluations allow assessing the feasibility of the prototype to succeed as an alternative authentication method. In addition, that was helpful to identify the strength and weakness aspects of the system from the end user perspective.

5.7 GOTPass as an alternative authentication

Having implemented and tested the proposed solution, it is worthwhile to revisit the requirements needed for a new alternative authentication mechanism to succeed and check whether GOTPass is capable of satisfying them or not. Chapter two – 2.7, discussed the essential criteria that need to be met by the new authentication proposal. The following table consists of the criteria along with the GOTPass compliance status.

Criteria	GOTPass compliance
Elimination of the need for additional hardware	Device-independent scheme which works on the web browser without any extra devices.
Simplicity and ease of use	Based on the usability study (Chapter 6), users found GOTPass easy to use.
Better memorability	The conducted usability study (Chapter 6) demonstrated a high level of memorability.
Higher level of security	The initial security study (Chapter 7) showed a relatively high security safeguarding against common security threats.
Compatibility/Applicability on various areas	Web-based application capable to work across platforms.

Table 5-8: GOTPass compliance with alternative authentication criteria

Generally, Table 5-8 shows that the GOTPass scheme is able to satisfy all criteria of an alternative authentication. However, the level of compliance varies which may satisfy one criterion more than others. Furthermore, the GOTPass scheme is also able to satisfy the aims of the prospective authentication solution that were discussed in (Chapter four – 4.3) as part of the comparative review of the OTP types. The use of this scheme does not involve extra cost, additional devices, nor carrier services. Besides, it is protected by PIN alike (unlock pattern) and can be deployed on different platforms as it is a web-based solution. However, fulfilling these criteria and aims should not be taken as a claim for best solution but rather as an indication of potentiality.

5.8 Summary

This chapter explained the proposed GOTPass scheme, which produces a one-time password utilising multiple graphical authentication techniques that is suitable for an online banking context or alike. The design of GOTPass scheme was presented in details including the advantages and characteristics. Being a composite scheme, it was necessary to explain the rationales to select these various authentication techniques. On top of that, the registration and authentication components were described along with their process flow.

The scheme comprised of three main components; pattern unlock as a protection layer, image recognition that is easy to remember and use, and GOTPass input format to strengthen the security provided by OTP. During registration, the user needs to choose a username and draw a shape on a 4×4 unlock pattern. Next, four random themes are randomly chosen by the system and assigned for the user. One pass-image should be selected from each of the given themes which result in a selection of four pass-images in total. At the end, the GOTPass input format, which depends on the position of the pass-

images in the grid, needs to be selected to indicate the random codes that need to be entered during login using the keypad/keyboard. With reference to the authentication process, the method simply begins with entering the username and drawing the unlock pattern, followed by recognising the pre-chosen pass-images and lastly entering the OTP codes matching the registered input format. For real evaluation purposes, the prototype system was developed and prepared with 400 images in 12 distinct themes. Moreover, the collection of analytical data was enabled by recording some users' activity logs.

Clearly defined evaluation criteria plays an important guidance role for evaluative judgments related to functionalities and performances of the overall goals of the authentication solution. A solid evaluation is a fundamental determination of the merit dimensions of any system. The evaluative criteria include attributes covering both system aspects of security and usability such as features and impacts to realise how robust, how acceptable, how effective the system is. Therefore, the next two chapters will continue by carrying out essential assessments that cover the usability and security aspects of the proposed GOTPass scheme.

Chapter Six

Usability Evaluation of the GOTPass System

6.1 Introduction

Image-based authentication technique has several interesting features that distinguish it from others, one of which is the ease of recall. Thus, this has motivated the research to develop an enhanced graphical authentication mechanism and investigate its usability. The GOTPass scheme intends to improve the usability features of the existing graphical authentication system by developing a new multi-graphical password technique that fulfils most of the usability requirements. The main usability characteristics that the GOTPass authentication system aims to satisfy can be highlighted as follows.

The first requirement is the ability to create a new password using a simple process and a minimal amount of steps. Second, the password should be easy to remember, so users are not overwhelmed by complex secrets that they have to memorise. Third, it should be a simple to use scheme that is reliable (an unreliable system may result in denial of access). Fourth, it should be efficient to use, and the registration and login time should be acceptably short. Fifth, there should be nothing to carry, which means that a user should not rely on auxiliary devices (e.g. tokens) to perform the authentication task, excluding devices that users usually carry around at all times, such as mobile phones. However, mobile phones are exposed to lose or stealing which is considered another type of limitation. Finally, it should be easy to recover, allowing users to regain the ability to login in case the authentication credentials are forgotten.

A successful authentication system should maintain a balance between usability and security. System usability is an essential design aspect that should not be compromised for the sake of security (and vice versa). The GOTPass proposal contains some interesting usability design features (Table 6-1), such as the use of image themes that prompt users to remember password images. Although the system prohibits users from using their own

155

images, to protect against a guessing attack by a familiar person and help to reduce the impact of users' tendency to choose predictable images, they are however allowed to choose preferable images from a given theme, which adds flexibility to the system as well as freedom of choice for the user. In relation to that, Catuogno and Galdi (2014) expected that allowing self-selected secrets would help users to remember them easily and therefore reduce the average login time. However, even if that hold true, the attention level of their selections is decreased which makes users prone to incorrect inputs in the future.

	Usability features				
	System-assigned Themes	User-own images	User-selected images	Memorability	Mnemonic
GOTPass Scheme	✓	✗	✓	✓	✗

Table 6-1: GOTPass usability features

One of the GOTPass goals is to offer a reasonable level of memorability so users manage to remember their pass-images easily. However, there is no use of mnemonics to assist users in remembering their passwords, since the proposed scheme uses multiple authentication mechanisms which makes applying such a feature on each mechanism both difficult and pointless.

6.2   Usability evaluation design

The study conducted by Biddle, Chiasson and van Oorschot (2012) stated that the consistency of the published research data within the domain of graphical authentication is almost absent, which complicates the task of reproducing results or comparing schemes. Many graphical password system proposals have an inadequate evaluation of either security or usability, or even both. The lack of an accepted usability standard in this area of research might be a result of the missing coordination work between researchers,

which led to the use of different evaluation criteria for nearly every system proposal. Furthermore, Bonneau *et al.* (2012) realised that the original publications on such schemes have included optimistic and incomplete ratings. Therefore, standard evaluation methods and measurements are required to carry out a reasonable comparison against other works.

A reliable evaluation of a new authentication mechanism must consist of objective data on mechanism performance and subjective data on user experience with such system (Beautement & Sasse, 2010). A proper framework is required to evaluate the design of a successful authentication mechanism against several aspects of security and usability (De Angeli *et al.*, 2005). Hence, a collection of evaluation criteria and guidelines has been carefully identified by exploring the characteristics and methods of the existing graphical authentication schemes alongside a review of the available evaluation studies. However, it should be noted that fulfilling all the requirements of security and usability in a single authentication scheme is unlikely to be achievable (Schaub et al., 2013).

To establish an appropriate evaluation plan, a review of studies conducted by similar graphical password techniques was undertaken. As Table 6-2 illustrates, almost all schemes carried out in-lab studies. Most schemes were evaluated over several sessions with various time intervals. The maximum number of sessions used was three and the minimum was one. With regard to the number of trials, two schemes allowed 10 authentication attempts. The number of participants ranged between 10 and 61. Essential evaluation elements, such as effectiveness, efficiency, memorability and user satisfaction, were the components of most of the conducted studies. In addition, at the end of the table, a summary of the study proposal of the GOTPass scheme was also included to enable an easy basis for comparison.

Scheme	Type of study	Sessions	Trials	Participants	Evaluation elements
Komanduri Picture Passwords	In-lab and any location	Day 1: in-lab Day 2: any location Day 9: in-lab	8 complete correct inputs	- 23 participants - Only 15 participants in picture-based passwords	Effectiveness, efficiency and memorability
TwoStep	No user study	Future work: lab/field studies	–	–	–
WYSWYE (DR)	Controlled lab	One login session	3 login attempts	- 24 participants - None of them knew about GP	Accuracy, efficiency, learnability and user satisfaction
VIP	Controlled lab	Two login sessions: first day & after one week	10 login trials – 3 allowed incorrect attempts	61 participants	Effectiveness, efficiency and user satisfaction
TAPI	In-lab	One session	5 correct login attempts	30 participants – two groups of 15 each	Login time, correct logins and user satisfaction
GOTP	In-lab	–	–	10–20 participants with prior knowledge of use	Password creation & login times, recall convenience & recall disturbance
Gao CAPTCHA	In-lab	Three login sessions: day one, one week later and one month later	Test 1 (day 1): 10 times, Test 2 (one week) Test 3 (one month): three times	36 participants unfamiliar with the scheme	Login success %, login time and memorability

GOTPass	In-lab	Three login sessions: first day, one week later and one month later	Allowed: maximum10 login attempts for each session. Required: only 5 correct logins	81 participants	Effectiveness, efficiency, user satisfaction and memorability

Table 6-2: Summary of the graphical password technique studies

6.3 Experiment procedure and framework

A user study was designed to conduct three separate trial sessions; on the first day of the study, one week later and after one month. A within-subjects design method was used in which the same users participate in all experimental tasks – that is, repeated measures are taken from the same people. Participants performed two main assignments; firstly, to enrol to the system then authenticate for several times over specific time intervals, and secondly, to act as observers to try and capture the experimenter's login password using various attacking techniques. This study is a longitudinal testing method, since several observations of the same subjects were conducted over a period of time.

The experiment to evaluate the usability aspects of the GOTPass approach was conducted in a controlled lab environment, as all users were required to be physically present and use the same computer to perform the study tasks. For study purposes, the implemented prototype generated some significant activity logs in such a way that it stores timestamps, login status (successful, failed) as well as details of the duration of each session as descried in the previous chapter five (5.5). In addition, results of the responses to the pre-test and post-test questionnaires were also collected. Only the research investigator and the participant were allowed in the lab, to avoid any possible disruption and to enable the researcher to observe any usability or security issues during the experiment and record

the participant's comments. Nevertheless, attention was paid to the task duration, in which the participants were urged to remain focused on the experiment and discourage any side conversations during the trials, unless participants chose to talk.

Below is the series of tasks the users were required to perform at each session.

A. Initialisation session – Day one

The first session started with a brief introductory overview of the procedure, participants' rights as well as an explanation about the system functionalities and the process of enrolment and authentication. Instruction manuals 'guide booklets' and 'video demos' that practically describe the registration and login sequential steps were made available for the participants as training materials. As shown in Table 6-3, nearly two-thirds of the users benefited from the booklet guides and a quarter of them used the video materials to explore the new system. A few participants liked to experience both materials mainly by using one material for the registration process and the other for the authentication. However, in reality users are not always expected to read a guide but it is assumed that they may look for some guides whenever they could not understand the scheme's process from the on screen tips or explanations.

User guide material	Number of users
Guide booklets	51
Guide videos	20
Both videos & booklets	10

Table 6-3: User preferences of information guide materials

After gaining the required understanding of the system and how it works, participants started the registration phase to create their own accounts.

Once the users were registered, they were requested to fill out a short online pre-test questionnaire on demographic and authentication experience. This acted as a separator

role between phases to distract the user's attention away from the registration process to aid a better evaluation of memorability during the next phase. This is similar to the Mental Rotation Tests (MRTs) procedure used in (Chiasson, Biddle & van Oorschot, 2007), which aims to clear the participants' working memory.

The final task of the first session was the login phase, where participants were asked to login (maximum 10 total attempts) under the following conditions:

- Total of five correct authentication attempts = successfully completed this session.
- Total of five incorrect attempts = receive the guide booklets or play the video demos, then try again.

The decision on the appropriate number of attempts to be allowed for the participants in this study was made by visiting previous studies within this domain (Table 6-2). The study found that the required successful authentication attempts varied between 3 and 10. However, some other studies requested the participants to login for 10 successful times as well, but that had a negative impact on some participants who found it too repetitive (Wiedenbeck *et al.*, 2006). Thus, to avoid the participants' boredom and at the same time allow the study to attain sufficient analytical login data, a similar method to that used in (Citty & Hutchings, 2010) was adopted with some modifications to keep the required balance. The maximum number of allowed login attempts was limited to 10 while users can accomplish their task whenever they achieve 5 correct attempts.

Since the proposed system was new to the participants, they were instructed to avoid clicking on the pass-images, instead they were encouraged to mentally locate the pass-images and map them to the right axis to obtain the correct OTP codes.

B. Follow-up session (short-term memorability experiment) – One week later

After a week of non-use, participants returned to the lab where they were requested to repeat the login task using the same procedures and conditions.

By completing the login task, the security experiment takes place which will be explained in more details in the next chapter.

C. Final session (long-term memorability experiment) – One month later

The third and final session took place one month after the first session. The first task was again to login using the created account with the same rules and conditions as the first and second sessions.

Lastly, each participant received an online post-test questionnaire to assess their impression of the GOTPass system, as well as finding out more about their opinion towards such a new system.

Given the longitudinal nature of the study, and the necessity for those involved to remain available for each stage of the work, the participants were sourced from the local university staff/student, and recruited via several methods: including word-of-mouth, student portals, emails and posters. Participation did not require any specific level of computing ability. Each participant received reasonable compensation (£15) for their participation, payable upon the completion of the study at the end of the third session. As for the session duration, the allocated time for each session never exceeded 30 minutes.

The experiment was conducted over five weeks and involved 81 participants (63 males, 18 females) who attended all three separate sessions. Participants had a mix of educational levels ranging from undergraduate and postgraduate. Most participants were aged between 18 and 39 years. Fifty percent of the participants reported an intermediate level

of computer experience, yet 17% indicated a basic level. Almost all participants have used various types of one-time password and many of whom were satisfied with such technology. The majority of the participants indicated that they knew about at least one type of graphical technique. Draw-based graphical password was the most familiar type to the users, followed by recognition-based passwords, whereas only a few respondents had prior knowledge of the click-based technique. Many participants demonstrated several insecure behaviours associated with the way to manage their multiple passwords. Top rated methods were reusing the same password and saving in the browser or mobile phone note. In regard to the techniques they follow while creating their password, the responses were varied but the most frequent ones included choosing similar ones to other current passwords and easy to remember passwords.

Beautement and Sasse (2010) highlighted two main points that may affect the generalisation of the results to other users' performance. One is the small sample size of 40 participants or less and the second is the over-reliance on students as participants. Thus, an effort was spent to avoid these points in this research by recruiting larger sample (nearly double the number) for the lab study and relatively mixed participants between students and staff.

6.4   Study results and explanations

As defined by the ISO 9241-11 (International Organization for Standardization, 1998), effectiveness, efficiency and satisfaction are the main components of usability in a particular context. However, according to Bangor, Kortum and Miller (2008), there are no absolute measures of usability. Nevertheless, major usability features from the ISO and previous studies (Table 6-2) were extracted to build usability evaluation criteria for the new graphical password system including efficiency, effectiveness, memorability, and

user satisfaction. This section reports the quantitative results for all usability components except user satisfaction, which reports qualitative results from the surveys regarding the user perceptions.

6.4.1 Efficiency

Usability element	Measurements	Assessment type	Assessment method
Average entry time for registration/ authentication	$Av\ (R) = \dfrac{\text{Sum (successful\_registration\_times)}}{\text{number\_of\_successful\_registrations}}$ $Av\ (L) = \dfrac{\text{Sum (successful\_login\_times)}}{\text{number\_of\_successful\_logins}}$	Objective/ quantitative	Experiment/ user trial

Table 6-4: Efficiency evaluation elements

Table 6-4 descries the details of the measurements used to calculate the efficiency of the proposed scheme. As anticipated, creating a GOTPass account took longer than some other authentication forms, such as the traditional textual password and other types of graphical password schemes. The total amount of time taken to register for GOTPass included typing a username, drawing an unlock pattern, clicking the 'Register Pattern' button, initial thinking time (image viewing), selecting four pass-images, confirming the selection of images, choosing the security level and, finally, clicking the 'Submit' button. As shown in Table 6-5, the average registration time was 134 seconds. It can also be inferred that the time deference between the minimum and maximum time taken was massive (more than four folds).

	Total attempts	Total time	Average	SD	Minimum	Maximum
Registration	81	10,833	134	36.5	59	254

Table 6-5: Registration entry time details (in seconds)

The analysis of the breakdown of the registration entry time (Table 6-6) showed that the last step of the registration process (GOTPass input format) consumed slightly more time than the image selection step. Interestingly, unlock pattern step took only less than 5% of the total time taken for registration, which confirms being a user-friendly scheme even in a web-based form using computer mouse.

	Username	Pattern	Image selection	GOTPass	Total time
Registration	2,317	488	3,866	4,162	10,833
	21.4%	4.5%	35.7%	38.4%	

Table 6-6: Breakdown of the registration entry time (in seconds)

It is worth mentioning that participants were totally new to the system and, while they were creating their accounts, spent quite a lot of time talking and asking questions about the prototype, trying to start discussions about several aspects, such as the potential advantages and disadvantages of the system and the way it was implemented which might justify the differences between the minimum and maximum time as shown in Table 6-5. Although the registration time was relatively high, it was considered generally acceptable for most participants, as indicated later in the post-test questionnaire result, where 80% of the users stated that they managed to complete the required tasks quickly. In contrast, only one participant disagreed with this statement.

In the analysis of the time taken to enter the correct submission, the average was 24.5 seconds, as presented in Table 6-7. The long input time was also expected in the login phase, since the login task involves a number of keystroke and mouse activities. There was a slight variation in the average login time taken in each trial: 23.6, 25.5 and 24.3 seconds respectively.

	Total attempts	Success	Total time	Average	SD	Minimum	Maximum
Login	1,302	1,215	29,754	24.5	11	8	83

Table 6-7: Entry time details for successful authentication (in seconds)

Additionally, the time taken to mentally locate the correct pass-images and their associated codes is also considered to be a significant factor that increased the login time which consumed more than half of the total time (Table 6-8).

	Username	Pattern	Image recognition & GOTPass	Total time
Login	9,887	2,530	17,337	29,754
	33.2%	8.5%	58.3%	

Table 6-8: Breakdown of the authentication entry time (in seconds)

6.4.2 Effectiveness

Usability element	Measurements	Assessment type	Assessment method
Login success rate	$SR(L) = \dfrac{number\_of\_successful\_logins}{number\_of\_total\_logins}$	Objective/ quantitative	Experiment/ user trial

Table 6-9: Effectiveness evaluation elements

The details of the measurements used to calculate the effectiveness of the proposed scheme can be seen in Table 6-9. The study looked at the proportion of all successful login attempts across all trials to calculate the overall success rate of the proposed system. In total, data from 1,302 login attempts carried out by all participants were analysed. Table 6-10 provides details of the success and failure rates for the authentication phase over the three trial sessions. The results showed a relatively high success rate, as over than 93% of the attempts were successful. Although the first trial was preceded by MRTs, to distract the users after the registration task and free up their working memory, this did not seem to have any clear impact on the success rate of the first trial in particular. In the final session (Trial 3), there seems to be some associations of the GOTPass credentials in

the participants' memory, as the number of incorrect inputs was lower than that in Trial 2. Moreover, it appears that there is a slight fluctuation in the login success rate between trials where the success rate decreased from Trial 1 to Trial 2 and then increased again in Trial 3. According to Catuogno and Galdi (2014), a justification of such behaviour can be the confidence that the users gained in the first session that they were able to use and remember credentials easily. Such feeling reduces the level of attention and, thus, increases the user tendency to errors. As a result, they make some improper responses in the second session. Nevertheless, those errors trigger their attention and increase the success rates during the final session.

	Total attempts	Successful		Failed	
Trial 1	429	405	94.4%	24	5.6%
Trial 2	438	405	92.5%	33	7.5%
Trial 3	435	405	93.1%	30	6.9%
Total	1,302	1,215	93.3%	87	6.7%

Table 6-10: Login success and failure rates

Interestingly, the study showed that none of the users were completely unable to login within the given number of attempts. Approximately 40% of the participants managed to complete their login tasks without error. Moreover, since many systems limit the number of consecutive incorrect attempts a user is allowed to make, this measure was enabled to determine the highest number of repeated failed attempts. The results showed that only one user failed to login within three consecutive incorrect login attempts, and seven others failed for two logins. In addition, only one participant was responsible for the maximum non-consecutive failed attempts by a user (five attempts), as shown in Chart 6-1 below.
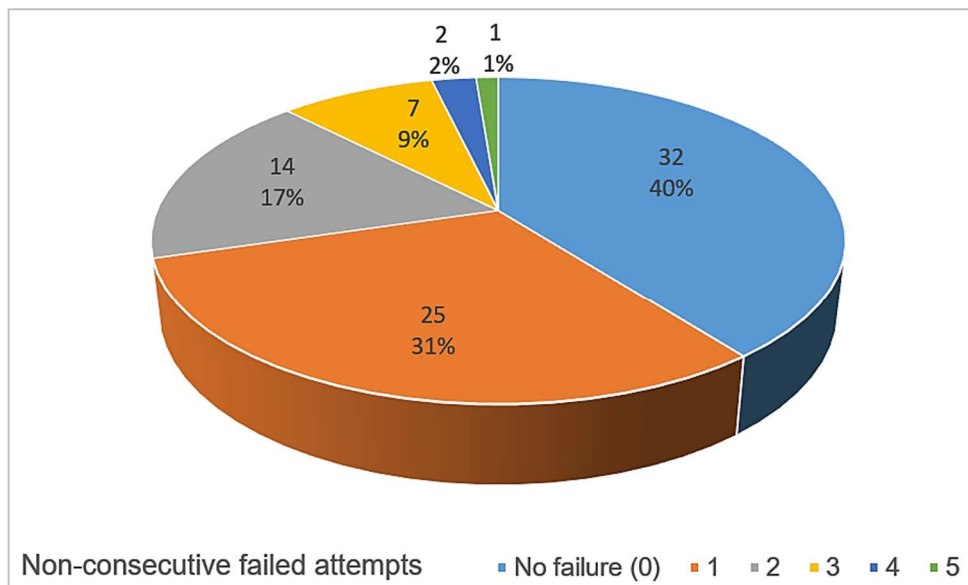
Chart 6-1: Number of users and their non-consecutive failed attempts

One of the observations from the trials highlighted that almost all failures occurred within the recognition part of the authentication process, more precisely the wrong codes or inputting codes in the wrong order, since the majority of the participants claimed that they were sure about recognising their pass-images correctly but might have entered the codes in an incorrect order or made a typographical mistake.

6.4.3 Memorability

Usability element	Measurements	Assessment type	Assessment method
Memorability over time intervals Short (one week), Extended (one month)	Matched at first attempt Matched within three login attempts	Objective/ quantitative	Experiment/ user trial

Table 6-11: Memorability evaluation elements

The above Table 6-11 shows the details of the measurements used to calculate the memorability of the proposed scheme. Participants carried out a memorability experiment twice. The first took place after one week of non-use (Trial 2) and the second was one month later (Trial 3). The results showed that all users (100%) managed to login

168

successfully to their GOTPass accounts, but the number of attempts to do so varied. There was no lockout event since all consecutive incorrect attempts were three or less.

	Trial 2						Trial 3					
Attempt sequence	1st	2nd	3rd	4th	5th	6th	1st	2nd	3rd	4th	5th	6th
Failure frequency	12	6	6	4	3	2	15	3	5	4	2	1
Total	33						30					

Table 6-12: Details of the frequency of the failed attempts based on trials and attempts

Table 6-12 illustrates the number of failed login attempts in each sequence. It can be inferred from the table that 85% of the participants in Trial 2 managed to login successfully on their first attempt. In addition, the number of failed attempts seems to reduce over time. One month later, in Trial 3, when participants tried to re-enter their GOTPass secrets, only 19% were unable to correctly login at the first attempt. However, during all trials almost all users logged in successfully within three attempts, which shows an encouraging outcome from a password recall perspective.

According to Renaud (2004), the frequency of use is an important factor of memorability which means how often the user will access the system. The categorisation of usage can be either high (daily), medium (once a week) or low (once a month). The more frequent the system is used the more easier the credentials become to remember, since the repeated use can ease the credentials memorability for users. On the other hand, when the system is used less frequently it is even more essential for the secrets to be easily memorable. Therefore, GOTPass scheme can suit systems in any of the three usage categories as it showed a relatively high memorability level over time.

6.4.4 User satisfaction

Usability element	Measurements	Assessment type	Assessment method
Overall satisfaction (simplicity, ease of use, understandability and perception of using GOTPass)	- Satisfied - Neutral - Unsatisfied (7-point Likert scale/ multiple choice)	Subjective/ qualitative	Questionnaire/ attitude scale

Table 6-13: User satisfaction evaluation elements

The details of the measurements used to analyse the level of user satisfaction of the proposed scheme is shown in Table 6-13. User satisfaction was measured through a post-test questionnaire, which was given to the users at the end of their final session of the study. The aim was to discover the users' feelings towards the perceived aspects of usability and security of the proposed system.

The survey was carried out online and consisted of 35 questions in 5 main sections organised as follows: (1) Training/Instruction - ask about the effectiveness of the way the study was presented, (2) Usability aspects - analysis of the user experience of various usability factors, (3) Security aspects - investigate how secure the system is from the respondents' viewpoints, (4) Design aspects - analysing respondents' experience of the system's design, and finally (5) Overall opinions - analysis of the overall users' satisfaction level of the proposed authentication mechanism.

The survey questions were mainly derived from IBM Computer Usability Satisfaction Questionnaires – The post-study usability questionnaire 'PSSUQ' (Lewis, 1995). However, there are some other valuable evaluation tools such as the System Usability Scale 'SUS' (Brooke, 1996) but it was not used in this research because it produces a single scoring number representing the overall usability measure. None of the

similar/competitor schemes to GOTPass has used SUS to measure the usability which made it difficult to compare the outcome of compared schemes.

Most measurements were carried out using a 7-point Likert scale, ranging from 1 (strongly agree) to 7 (strongly disagree), whereas some others used multiple-choice measurements. All 81 participants of the user study took part in the survey. The results indicated that 86% of the respondents agreed that learning how to use the system and how to create a GOTPass account was simple, with the remaining 14% showing an average response. Almost 91% of the participants stated that this authentication method would become easier and quicker to use with practice. The vast majority of the participants (98.7%) stated that they would be confident using the GOTPass system. Ninety-four percent of the participants thought that the GOTPass system could be used for sensitive web authentication. The overall level of user satisfaction with the GOTPass system was very high, as 98% were in support of the idea. Note that the results of all responses were mostly in the positive half of the scale, which, in turn, reflects positive outcomes towards a prospective solution.

6.4.5 Other usability-related questionnaire results

Beside the above reported results from the post-test questionnaire, this section continues to present results of other aspects of usability that were covered in the questionnaire. For an easier presentation of the result data, the average value of each survey statement was used and arranged into tables based on its related section.

In the first section (Table 6-14), the majority of the participants showed that the provided guide materials were useful and helpful which made the learning task easier.

Section (A) - Training/Instructions *(1) Strongly disagree – (7) Strongly agree*	Average	%
Learning how to use this system was simple	6.25	89.2
Support information was clear and understandable	6.47	92.4
Support information was effective in helping me complete the tasks	6.54	93.5

Table 6-14: Questionnaire results: Training/Instructions

Section (B) was concerned about various usability features that ensure the suitability of the proposed scheme for use from the participants' viewpoints. The results in Table 6-15 show that the creation and authentication processes using GOTPass was simple and quick for most participants. In addition, they agreed that this authentication method would become easier and quicker to use after gaining experience with practice. In regard to memorability, a question was asked about the ability to remember GOTPass after a few weeks of non-use, 88% of the participants were confident that they will remember their password correctly. The responses about the introduction of the keyboard as an input means with graphical password scheme were mostly positive. Also the utilisation of the unlock pattern technique on the web was supported by a high number of participants. Finally, users were asked to rate each part of their GOTPass based on what they think might cause the remembrance/recall difficulty. The results showed a moderate impact was caused by the input format and pass-images respectively.

Section (B) - About the usability aspects *(1) Strongly disagree – (7) Strongly agree*	Average	%
It was easy to create my GOTPass account	6.44	92.1
Logging in using GOTPass was easy	6.36	90.8
I was able to complete the required tasks quickly	6.15	87.8
This authentication method would become easier and quicker to use after gaining experience (practice).	6.58	94.0
It was difficult to enter my GOTPass even though I thought I remembered it	2.12	30.3

If I didn't login to my account for a few weeks, I would still remember my password		6.16	88.0
Using keyboard as an input means with graphical password scheme seems:	(Convenient)	6.06	86.6
	(Practical)	6.26	89.4
	(Secure)	6.64	94.9
Using unlock pattern on the web was:	(Convenient)	6.36	90.8
	(Practical)	6.43	91.9
	(Secure)	6.27	89.6
Rate each part of your GOTPass based on what you think might cause the remembrance/recall difficulty? *(1) No impact – (6) High impact*	(Username)	1.73	28.8
	(Unlock pattern)	2.09	34.8
	(Pass-images)	2.7	45.1
	(Input format)	2.81	46.9

Table 6-15: Questionnaire results: usability aspects

In respect to the design aspects, section (D) reported users' views about different system characteristics. Table 6-16 shows that the majority of responses pointed out that the number of images and themes used by the system were adequate.

Section (D) - About the design aspects	High %	Adequate %	Low %
The number of pattern nodes (16) on a matrix of size (4×4) was:	6.2	92.6	1.2
The number of images within each theme (30/theme) in the registration page was:	17.3	80.2	2.5
The number of images (16) on a matrix size (4×4) in the login page was:	3.7	93.8	2.5
The number of pass-images (4 images) that users need to remember was:	1.2	96.3	2.5

Table 6-16: Questionnaire results: design aspects

Furthermore, almost half of the participants found that randomising (shuffling) images locations on the grid has a slight effect on performance (causing longer time to identify pass-images) and one-third of the users said it had no effect. The convenience level of assigning the image themes by the system was about 89%. As for the partial assigning of the GOTPass input format (code location) by the system, the convenience level was around 90%. As part of the design aspects questions, the participants were asked about

their views regarding the generated codes where 84% of them thought that generating alphanumerical codes would provide more security while 83% stated that the current numerical codes would be more usable. In regard to the length of the GOTPass code (8 characters long), the majority of the participants (90%) found it adequate.

Section (E) - Overall opinion *(1) Strongly disagree – (7) Strongly agree*	Average	%
This system has the functions and capabilities I expect it to have	6.53	93.3
Using GOTPass system was convenient	6.52	93.1
I would use GOTPass confidently	6.75	96.5
I think GOTPass can be used for sensitive web authentication	6.54	93.5
Overall, I am satisfied with GOTPass system	6.75	96.5

Table 6-17: Questionnaire results: overall opinion

The last section of the post-test questionnaire was about the overall opinion to find out how satisfied the participants were with various parts of the system. As shown in Table 6-17, the overall satisfaction throughout was considerably high.

6.4.6   Prototype analysis results

This section analyses some of the result data of the conducted user trials and reports general observations in respect to the usage behaviour.

A. Unlock pattern

The chosen unlock patterns by users were examined against bias selection. Table 6-18 presents the repeated pattern shapes that were chosen by several users. It can be inferred that most frequent shapes were formed by English letters (i.e. L, N, Z) with some variations in orientation. Although the results revealed that the bias selection does exist, but the ratio of its occurrence is relatively low which did not exceed 9% by maximum.

174
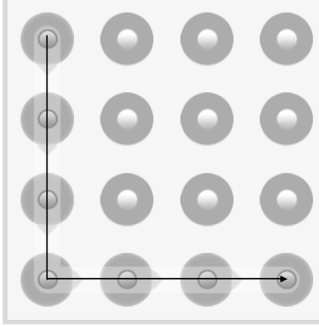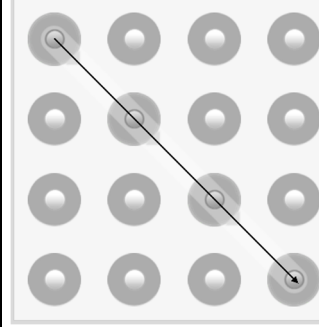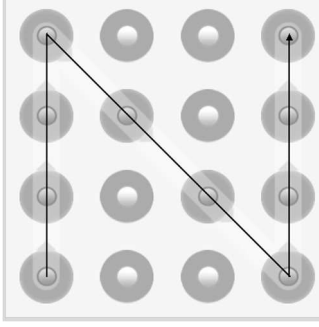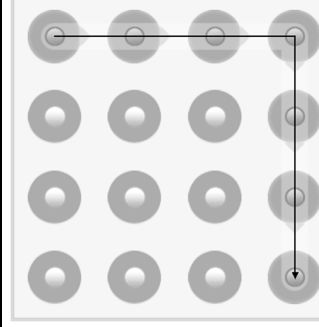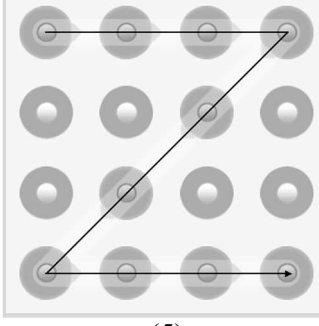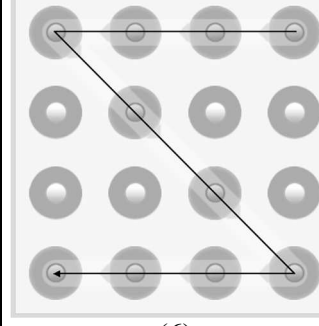
Selection frequency	Pattern shapes	
7 8.6%	 (1)	 (2)
4 4.9%	 (3)	 (4)
3 3.7%	 (5)	 (6)

Table 6-18: Frequently chosen patterns

In this prototype implementation, the restriction policy on the minimum number of nodes that the user must select was not activated, which is supposed to be 5 as previously mentioned in Chapter five (5.3.1). The reason behind that was to investigate the normal unrestricted users' preferences towards the length of the pattern. For instance, the pattern shape (2) that appears in Table 6-18 was formed in a straight line connecting 4 nodes only.

The following Table 6-19 presents the different pattern lengths and the number of users chosen the same length regardless of the similarity of shapes. It can be depicted that the

majority of participants (89%) complied with the policy that limits the minimum number of nodes without enforcement. More than 60% of the users chose their patterns with 7, 10, 5 points long respectively.

Pattern length	Frequency	%
7	24	29.6
10	16	19.8
5	10	12.4
4	9	11.1
6	7	8.6
8	5	6.2
13	4	4.9
9	4	4.9
12	1	1.2
16	1	1.2

Table 6-19: The frequancy of the chosen pattern length

B. Themes

Since GOTPass scheme introduced a new way to reduce the bias selection through the use of system-assigned themes and user-selected images approach, this part of the study analysed the distribution of the themes and its effectiveness.

	Theme name	Frequency	%
1	Computer	33	10.2
2	Transportation	29	9.0
3	House	29	9.0
4	Sport	28	8.6
5	Stationery	27	8.3
6	Sign	27	8.3
7	Clock	26	8.0
8	Flag	26	8.0
9	Earth	26	8.0
10	Paint	25	7.7
11	Food	24	7.4
12	Animal	24	7.4

Table 6-20: The frequancy of the assigned theme

Table 6-20 demonstrates the frequency of assigning each theme to the users. As each user is assigned four themes, the distribution ratios are considered close.

One of the interesting findings in this regard was to realise that there were four sets of duplicated themes assigned to different users regardless of their sequence. However, the chosen pass-images by users were different as the records showed no duplication in the pass-images portfolios for all users. This is a significant sign that support the effectiveness of such approach in reducing the chance of having the same pass-image portfolios for several users.

C. Images

This subsection collected data about images chosen 4 times or more by different participants. The goal was somewhat related to that discussed earlier in the theme analysis. Finding out whether particular images were chosen more than others raises the alert of having hot-images that may lead to security issues such as easy to guess images.

Table 6-21 illustrates the number of times each pass-image was chosen by users. There was a total of 23 pass-images each of which was chosen by 4 users or more. It can be inferred that the amount of images selected repeatedly more than 4 times constitutes approximately 7% of the entire selected pass-images (324 images). The most frequent pass-image was selected 10 times, that is just 2.5% of the total available images while the 4 time-selected pass-images were only 1% each. Generally, these percentages seem very low to help attackers determine or even guess the correct pass-images of other users.

	Images	Theme name	FRQ	Overall %		Images	Theme name	FRQ	Overall %
1		House	10	2.5	13		Computer	5	1.3
2		Clock	8	2.0	14		Transportation	5	1.3
3		Sign	8	2.0	15		Stationery	4	1.0
4		Flag	7	1.8	16		Animal	4	1.0
5		Computer	6	1.5	17		Earth	4	1.0
6		Sport	6	1.5	18		Transportation	4	1.0
7		Animal	6	1.5	19		House	4	1.0
8		Flag	6	1.5	20		Earth	4	1.0
9		Computer	5	1.3	21		Stationery	4	1.0
10		Sport	5	1.3	22		Sign	4	1.0
11		Flag	5	1.3	23		Paint	4	1.0
12		Food	5	1.3	**Overall %** = percentage of chosen image based on the total available images (400 images)			

Table 6-21: The repeatedly selected pass-images

D. General trials observations

During the experiments time, participants were observed in order to realise any unexpected usage behaviour. From the results presented in Table 6-22, it appears that some users tried to click directly on their pass-images instead of looking for the associated random codes. Others just pointed at either the pass-images or their related codes. Both behaviours make the system vulnerable to observation attacks. It was also noticed that some users were practicing insecure activities even with the new system, such as writing down login information. Not only that but also some users were found dragging and dropping their random codes into the designated field instead of writing them, which indeed reveal part of their login information for any peepers.

Observed behaviours	FRQ	Notes
Clicking on images to select	15	Usually in the first attempt
Pointing at images or codes (by mouse or finger)	4	
Thinking that pass-images will be displayed in rounds	2	
Trying to write down information	2	
Using laptop touchpad for drawing	2	Found hard
Copy & past username, drag & drop codes	5	

Table 6-22: Observed user behaviours

6.5 Discussion

At first glance, many users thought that using GOTPass scheme might be too complex; however, learning and practising the system created an opposite impression, as the majority found it easy to use and adoptable. Longer account creation time is a disadvantage of the system, but, at the same time, it is worth mentioning that GOTPass is a multi-layer authentication approach which employs several graphical password techniques into a single robust mechanism. That, in turn, might justify the longer time

taken to create user accounts or login to the system. In order to register or login, users need to complete multiple steps which have an obvious impact on the complexity of the registration and authentication process. That is specifically clear when compared to the traditional textual password which takes 25 second to create a new password and 24 second to login after one week (Dhamija & Perrig, 2000). However, although GOTPass scheme seems complex and takes longer time, the user study showed that, overall, users were satisfied – there were no complaints about the duration of the registration process or the level of difficulty. Furthermore, it is worth spending an extra little time using GOTPass scheme to be protected against various common security attacks, which is one of the primary objectives of this system.

In a study by Beautement and Sasse reported that many users encounter difficulties recalling their credentials correctly with infrequent authentication (once a week or less). In that case, the ability to correctly recall the credential is more important for performance than fast execution. Whereas in the frequent authentication (once a day or more), fast execution becomes a priority as recalling the credential becomes automatic for most users (Beautement & Sasse, 2010). This implies that GOTPass would best serve within the first category of infrequent authentication. However, that does not necessarily mean that GOTPass scheme is inappropriate for the frequent authentication but rather suggests further investigation on its suitability for such type of authentication.

Although the combination of several security methods may yield a higher level of security, it may also affect the usability of the system. However, that is not the case with the GOTPass scheme, as it aims to keep a reasonable balance between security and usability and avoid any trade-off. According to the results of the user study, there is no evidence of a negative impact on usability as a result of combining multiple security methods. Additionally, reporting a high success rate even after a period of time, as well

as the users' positive perception regarding the simplicity of the system, prove that multi-security layers do not hamper the usability of GOTPass.

Comparing the login time of the GOTPass scheme to other graphical schemes that are similar in nature, such as (Khot, Kumaraguru & Srinathan, 2012) (Komanduri & Hutchings, 2008) (Gao *et al.*, 2009b), GOTPass showed that the login time still appears to be sensible (see Chart 6-2). As mentioned earlier, a significant reason that influences the performance time of an authentication scheme is the involvement of multiple steps, which also justifies the longer time taken to register and login using GOTPass scheme. However, GOTPass is still comparable to other two-step authentication approaches, and is even superior within its category (three-step).
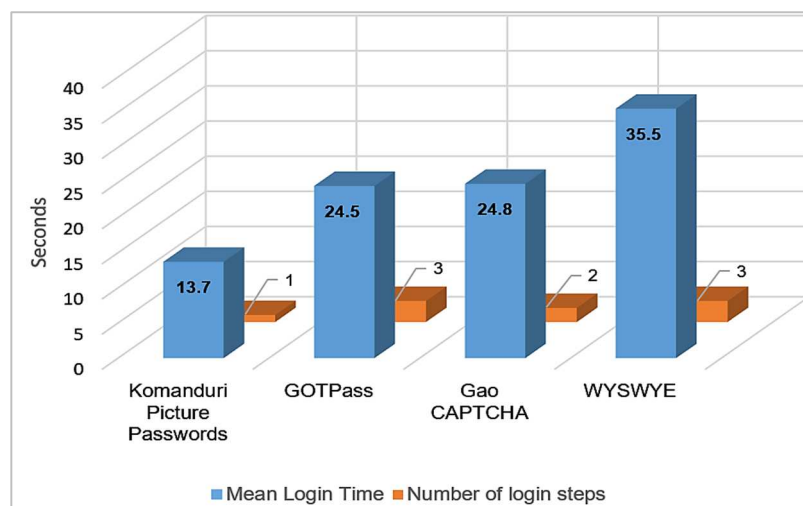
Chart 6-2: Comparison of the mean login time and steps to login

In terms of comparing GOTPass with its closest scheme, GOTP, a direct comparison is not straightforward, given that the evaluation data for GOTP are limited to post-test survey responses and not experimental data (Ku *et al.*, 2012). Nonetheless, a brief comparison between the two schemes is presented next. The data of the survey had to be adjusted from a 7-point Likert scale to a 5-point Likert scale to enable a direct comparison. In order to gain comparable results, the response values of the relevant questions were converted using the following method (IBM Support, 2010):

1. L_i = Multiply the response value by its frequency (e.g. 7-point Likert scale × number of selected times).

2. S = Sum, the total of all points (L_7 + … + L_1).

3. P = Divide S by the number of participants (S ÷ 81) [the mean value in a 7-point Likert scale].

4. Q = Divide P by 7 (P ÷ 7) [the value should be in the range between 0 and 1].

5. R = Multiply Q by the new Likert point number (Q × 5) [the mean value in a 5-point Likert scale], the value of R represents the original result but using a 5-point Likert scale.

	Convenience level	Creation time	Memorability	Login time	Simplicity of procedure	Convenience of authentication process
GOTPass (7-point)	6.52	6.15	6.16	6.15	6.44	6.36
GOTPass (5-point)	4.65	4.4	4.4	4.4	4.6	4.55
GOTP	4	3.5	3.67	4.17	3.67	3.67
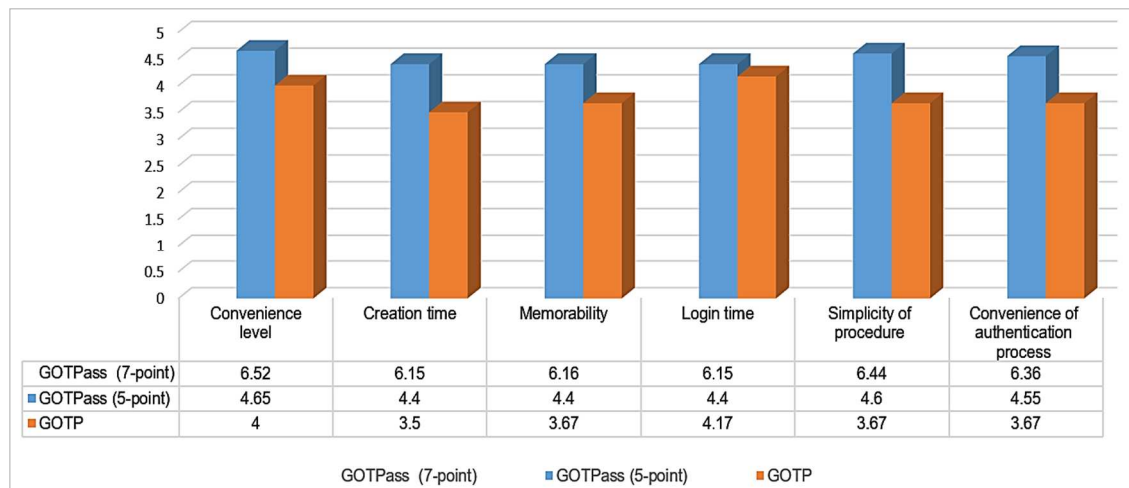
Chart 6-3: Comparison summary of GOTP and GOTPass

Chart 6-3 highlights the differences between the compared schemes based on the available evaluation data of the GOTP scheme. Although GOTP scored highly regarding the level of memorability, GOTPass showed even better results, which satisfies one of the main requirements of any prospective alternative authentication system. In relation to that, ease of use is another important feature, and GOTPass achieved a higher result than that of GOTP. However, across all comparison parameters GOTPass has performed very well, with over than four out of five in all aspects. A major advantage of GOTPass was the larger number of participants, which increases the accuracy and reliability of the result.

In addition, GOTP scheme requires the user to memorise four alphanumeric codes obtained by identifying the pass-images over four rounds. That, in turn, would require memory recall from the user, posing possible usability issues. In contrast, the GOTPass scheme does not involve codes memorisation, since they are visible on a single screen. In addition, GOTP is designed for smartphone platform that can be used as an out-of-band channel authentication, which is usually carried out away from the browser, whereas GOTPass utilises an in-session/in-band authentication system using the existing browser. In other words, there is no need for additional devices, such as a token or mobile phone, to use the GOTPass scheme. Regarding the length of the OTP code, GOTP submits a four-character-long code while GOTPass offers an eight-character code. Themes and images used in GOTP are static and unchangeable, but in GOTPass they are dynamic and shuffling.

Figure 6-1: A screenshot of the GOTP login screen

The letters and numbers in the top corner of each GOTP image are barely readable on a mobile phone screen (Figure 6-1), which can be considered to be a major usability drawback of the system. In this respect, I must acknowledge the authors of the GOTP

scheme (especially Okkyung Choi) for their cooperation and making the GOTP application available for me to test and have a real experience with it.

In a quick comparison to the most common authentication techniques utilising OTP in online banking, the login time and number of steps needed for login were compared. All these accounts involved in this test belong to the researcher who carried out each test individually. The first step involved noting down each and every step throughout the login process. Secondly, a stop watch of a smartphone was used to record the time taken from the beginning of the login till the end. However, it was ensured that all login prerequisites such as the tokens and mobile phones were present before the start. Therefore, the consumed time does not include searching/bringing in a token or mobile phone.

E-banking	HSBC	SAMBA	SAMBA	GOTPass
OTP method	Soft-token	Hard-token	SMS	Graphical
No. of steps	8	8	7	4
Steps details	Username/ID, select login method, enter memorable question, move to soft-token, enter security key, generate OTP, go back to bank website, enter OTP	Username, password, select OTP method, move to hard-token, enter PIN, generate OTP, go back to bank website, enter OTP	Username, password, select OTP method, move to mobile phone, receive SMS message, go back to bank website, enter OTP	Username, pattern, recognise pass-images, enter OTP
Average login time 3 logins (seconds)	74, 58.9, 51.9 **61.6**	32.6, 31.2, 30.4 **31.4**	50.24, 34.21, 37.23 **40.56**	18.7, 21.6, 16.1 **18.8**

Table 6-23: Login process of GOTPass versus common online banking authentications

Table 6-23 shows the results of the comparison between GOTPass scheme and various OTP techniques provided by some online banking systems. Overall, GOTPass scheme

required nearly half of the steps needed for login by other compared techniques. As far as the login time is concerned, GOTPass performed well among others demonstrating the shortest duration time. However, a factor of these approaches is not just how long they take to perform the task but how friendly they feel in process. Apart from the GOTPass scheme, all compared schemes required some instant disruption while logging in since the user needs to be diverted away to pick the authentication device (token or mobile) to obtain the OTP code.

6.6 Summary

This chapter presented the results of the experiments conducted to evaluate the usability of the system. The results indicated that the GOTPass scheme has achieved a high level of effectiveness and user satisfaction as well as an acceptable level of efficiency. Moreover, the impact of being a multi-layer authentication approach on the duration time taken for registration or login was obvious but did not affect the overall level of user satisfaction. The study showed that GOTPass has the potential to succeed and contribute towards the adoption of graphical password technologies. In respect to the analysis of the prototype data, the results showed that the approach of system-assigned theme with user-chosen images was effective and reduced the personalised selection of images. Furthermore, there was a few repetitions in the theme assigning process but nevertheless, that did not cause any duplicates in the image portfolios among all users. In connection to that, the number of pass-images that were selected repeatedly by several users was reasonably low which fortify the system against guessing attack by decreasing the image probability.

In conclusion, the study indicated that most of the main usability characteristics that the proposed scheme aimed to satisfy in the first place as mentioned at the beginning of this

chapter were achieved. Overall, the GOTPass was uncomplicated multi-step scheme, simple to recall, easy to use, acceptably efficient in terms of registration and authentication time duration, and does not require any additional devices to carry. However, the last requirement was the ease of recovery, but was not included in the study since it was assumed that implementing one of the existing techniques (i.e. email the login reset procedure to the registered email address) would satisfy such requirement.

As this chapter discussed the usability aspects of the GOTPass scheme in details, the security aspects need to be investigated with more elaboration as well. Thus, the next chapter will be dedicated for the security-related experiments and analysis.

Chapter Seven

Security Evaluation of the GOTPass System

7.1 Introduction

The primary goal of an authentication system must be to provide sufficient security for a target environment. The satisfaction of security requirements of any proposed system should be evaluated against common security attacks. Focusing on one particular security strength and leave the system vulnerable to other types of attacks would not fulfil the security requirements adequately. For security systems, it is essential to assess the design of the system in a controlled lab prior to any deployment plan for field study or in the wild. That should enable observation of any potential security issues that can be easier to control and amend in lab but would be difficult if occurred in a field study.

The strength of the GOTPass scheme is mainly derived from the incorporation of several security characteristics including the protection layer of unlock pattern, dynamic pass-images portfolio, pre-determined input format, and codes randomness. This chapter addresses the security capabilities of the GOTPass scheme based on a user study conducted to assess the potential of the scheme to withstand common security threats. Attack-alike simulations were designed, including guessing, intersection, and shoulder-surfing attacks, to enable a proper security evaluation and to measure the system reaction against various attacks. An in-depth analysis of the security evaluation is reported which shows a high resistance capability of GOTPass scheme against common graphical password attacks. Other essential security measures were also included such as the theoretical security assessment and the full size of password space. Participants of all experiment types were requested to use the same test machine to try compromising the system using different attack methods. Towards the end of this chapter, the results of the complementary study is presented which applies a minor modification to the design of the system that resulted in a valuable security enhancement without affecting the system usability nor the user experience.

In this research, attacks exploiting software flaws for entire bypassing the authentication technique are out of scope which limit the discussion to those common attacks seeking direct obtainment of user's credentials.

7.2 Security concerns and threats to Graphical authentication

The security of an authentication system is mainly related to the difficulty of cracking the secret key. There are several threats that attackers may exploit to break the authentication system and gain an unauthorised access. According to De Angeli et al. (2005), the three basic security dimensions considered for the security evaluation were guessability, observability and recordability. A brief overview of the common attacks against graphical authentication systems to obtain user's credentials is provided next:

7.2.1 Guessability

Guessability is a measure of how simple it is for an attacker to guess the authentication secret of a legitimate user. In recognition-based authentication, "Prioritised guessing attacks" aims to increase the probability of selecting the correct image through the prioritisation of the most commonly selected images (English & Poet, 2011a).

7.2.2 Observability:

7.2.2.1 Shoulder-surfing

When authenticating in public places, shoulder-surfing attack is of real concern since it enables an attacker to capture an individual's password by direct observation or by recording the entire authentication session (Lashkari et al., 2009). A general goal of resisting shoulder-surfing attack should be to harden the attacker's task of learning enough key images that lead to a successful future replay attack (Dunphy, Heiner & Asokan, 2010). According to Wu *et al.* (2014), shoulder-surfing attacks can be classified into two types; (1) Weak shoulder-surfing that does not utilise any video equipment and

(2) Strong shoulder-surfing that make use of video equipment to capture the entire login process including keystrokes and the mouse clicks. However, several conditions like the required shooting angle and lighting have showed that video shoulder-surfing seems less practical than expected (Schaub *et al.*, 2013).

7.2.2.2　Intersection attack

Intersection attack is possible when the role of an image as either a pass-image or a decoy can be determined by the frequency of its appearance at each login. That in turn allows the attacker to use the most frequently viewed images to pass the challenge screen and gain access (English & Poet, 2012). In addition, a source intersection attack is an attack that possibly occur when pass-images and decoys are each drawn from distinguishable image sources such as personal images and drawings (Dunphy, Heiner & Asokan, 2010).

7.2.3　Recordability:

7.2.3.1　Replay attack through eavesdropping

Intercepting the communication between authentication client and server can enable attackers to capture the transmitted image portfolios and the user selection. Afterwards, the copied login data can be replayed again to the server to potentially obtain a false positive access (English & Poet, 2011b) (van Oorschot & Wan, 2009).

A different form of such attack can be carried out using nearby high-quality smartphone camera that aim to capture sensitive data from devices in the vicinity (Marquardt *et al.*, 2011).

7.2.3.2　Phishing

Phishing attack is based on tricking users into submitting their login information at a fraudulent website that records users' input. The need for presenting a correct set of images to the user prior to password entry makes this type of attack difficult with recognition-based systems. In schemes with variant responses, multiple server probes

would be necessary since only a portion of the user's secret is exposed on each login attempt (Biddle, Chiasson & van Oorschot, 2012).

7.2.3.3 Spyware

7.2.3.3.1 Keystroke-loggers

Some graphical password schemes utilise the keyboard to input login information. By this means, user's input can be captured using keystroke-loggers unless the input's content is varied at each login time (Gao *et al.*, 2013).

7.2.3.3.2 Screen-scrapers

Screen-scrapers install software on a computer to record the user's operational activities. Under normal circumstances, the difficulty of installing spyware on a user's computer without being noticed makes screen-scrapers a less serious threat (Gao *et al.*, 2013).

7.2.3.3.3 Other spyware

Combining keystroke-loggers and screen-scrapers is a method of attack that can obtain both the screen content with the keyboard input information. It is clear that this type of threat can be of an increased risk to the development of graphical password security (Gao *et al.*, 2013).

7.2.4 Dictionary attack

The idea of the dictionary attack is based on trying all possible passwords from a relatively short pre-assembled list (dictionary) of high probability candidate password collected from experimental data or assumptions about user behaviour (Biddle, Chiasson & van Oorschot, 2009).

7.3 GOTPass security features

In this scheme, users must enter the correct OTP provided through the recognition-based graphical password. In addition, a number of advantages are offered to strengthen the proposed technique such as providing dynamic secrets with no reliance on static password nor pass-images, implicit authentication feedback in which the scheme does not reveal any indication about the status of the login session. However, the inability to spot the correct pass-images by the legitimate users is a type of alert that something went wrong with that login attempt which require the user to go back to make the necessary correction.

As far as the security of the proposed system is concerned, GOTPass aims to be equipped with high security features without sacrificing the usability of the system. Table 7-1 contains a list of these security features with a brief description of the anticipated advantages of each feature.

Security Features	Advantage
Shuffling images	Reduce the risk of observation attack, which observes several login sessions to look for unchanged pass-images if always located in the same position.
Online verification	Utilising the unlock pattern technique as a proactive check to act as a first line of protection.
System assigned themes	Decrease guessing chances caused by hot-images or known personal image preferences. However, user will have the chance to select the preferable images from among the assigned themes to avoid affecting the usability by keeping good memorability level.
Pass-image portfolio	The system randomly presents a subset of the user's pass-images (2 out of 4) in each authentication session. That should mitigate the observation, phishing, and replay attacks.
Distractor-images portfolio	Ensure that recording multiple challenge screens to figure out the high frequent images is ineffective through maintaining constant distractor-images for each given pass-image.

Account lockout	Limit the number of consecutive incorrect attempts and apply a delay between login attempts to prevent excessive guessing tries and dictionary attack.
Implicit authentication feedback	The status of the login session is not revealed until after the final submission. Attacker will have no indication of which part of the scheme went wrong. That should resist guessing and trial & error attacks.
One-Time-Password	Resist eavesdropping attacks and credential theft.
Shoulder-surfing resistant	The use of multi-layer authentication makes it hard to record multiple login techniques. The transparency level of the unlock pattern drawing disguises the correct pattern shape and thus makes it harder to capture. No indicator of image selection, so onlooker cannot identify password images.
Difficult to guess	Guessing various login techniques is made hard by implementing a multi-layer authentication. OTP is changeable every time. Authentication feedback is only given at the end of the login session. That is also called implicit feedback which should only be recognisable and useful for the legitimate user.
Dictionary attacks resistant	The use of multi-layer authentication makes it hard to conduct an online dictionary attack on multiple login techniques, e.g. unlock pattern should protect the primary authentication method (image recognition). On top of that, the use of OTP should mitigate this type of attack.
Safe against Spywares	Both keystroke logger and screen recording are needed to gain enough knowledge of the secret components, which is mostly time, effort, and cost overhead for attackers.
Anti-phishing and replay attack	The need for presenting a correct set of images to the user prior to password entry makes such attacks difficult. The implementation of variant responses reveals only a portion of the user's secret on each login attempt.

Table 7-1: GOTPass security features

7.4 Security evaluation

Various general evaluation criteria have been proposed to assess different aspects of the authentication system's security. Among these proposals, De Angeli *et al.* (2005) have considered three basic dimensions for security evaluation. Guessability which measures the impostor's ability to guess the password, Observability that measures the impostor's ability to monitor the password while it is being entered by the user, and Recordability which measures the impostor's ability to record/capture the user's password. Moreover, Gao *et al.* (2013) discussed spyware as an additional password capturing-based attack.

Furthermore, English and Poet (2011b) have taken advantage of the same categorisation with further expansion that result in 4-tuple evaluation metric. Potential attacks against recognition-based graphical password were classified under one of the main related threat categories which are presented in Table 7-2. The security evaluation criterion is determined by whether the identified countermeasure/security benefit is provided by the scheme or not. Eventually, the scheme can present the overall level of resistance against particular types of attack by the number of applied countermeasures.

In this section, the security evaluation of GOTPass scheme is discussed including two types of the evaluations; the first is 'theoretical' based on assessment criteria and the second is 'empirical' where several attacks were simulated and tested.

7.5 Preliminary 'theoretical' security evaluation

The main security threats of recognition-based graphical authentication have been gathered alongside the suggested countermeasures to form a scoring table. By adopting a similar evaluation approach as that proposed by English and Poet (2011b), the scoring procedure can be slightly enhanced to suit a hybrid scheme like GOTPass. Appropriate

weights for the countermeasures are provided by a 4-point scoring method motivated by the ranking framework of Bonneau *et al.* (2012). The scoring technique is adapted to present the overall level of resistance against particular types of attack based on whether the countermeasure is being implemented or not using the following scale points [No (0), Partially (1), Almost (2), Yes (3)].

The result of the 'theoretical' security evaluation is shown in Table 7-2, which contains the threats alongside a list of the countermeasures and their scores.

Category	Security concern	Threat	Countermeasure	Score
Password Capture-based	Observability	Shoulder-surfing	Show no or disguised indicator of selection	3
			Greater pass-images number than that of challenge screens	3
			Variable response	3
			Indirect input	3
		Intersection analysis	Constant display of distractors and pass-images, <u>or</u> Present a small constant subset of distractors for each given pass-image	3
			Display distractors only in subsequent challenge screens following any incorrect attempt	3
			Limit the number of attempts for unsuccessful authentication	3
			No pass-image portfolio implementation, <u>or</u> Implement pass-image portfolio + distractor portfolio	3
			Pass-images and distractors are not drawn from distinct sources	3
	Recordability	Replay attack	Random image location	3
			Submit different value each time	3

			Implement pass-image portfolio	3
		Phishing attack	SSL implementation	1
			Protect images database (without knowledge of user's images beforehand, it would be difficult to present correct images to extract user's graphical password)	2
	Spyware	Keystroke-loggers	Varied input's content at each login time	3
		Screen-Scrapers	Use shielded input characters	3
			No indication of selection	3
Password Space-based	Guessability	Guessing attack	Disallow user choice of images	2
			Select distractors from random categories	3
			Wide range of image categories	3
			Display images from same categories	3
			Provide implicit feedback for incorrect input	3
	Online dictionary attack		Limiting the number of incorrect attempts	3
			Increase the delay between any 2 consecutive error logins	3
			Total	**68**

Table 7-2: The result of the 'theoretical' security evaluation

The GOTPass scheme has scored 68 points out of 72 (94%), which seems encouraging result but also needs to be supported by an empirical proof that reflects the same high security level. Among all the countermeasures listed in Table 7-2, GOTPass scheme scored the maximum except three of them. First was 'Disallow user choice of images', as mentioned previously this issue was avoided by assigning random themes to the users and allow them to choose from the images inside each theme which should somewhat restrict user choices. Second was 'SSL implementation', it can be assumed that the connection is secured by an SSL implementation but since there was no actual implementation of that countermeasure in the prototype, it was given one score only. Third was 'Protect images

database', securing the database was taken into consideration while implementing the system, however, there is a chance for security improvement by storing images directly into the database in the form of BLOBs data type then try to apply appropriate encryption. In fact, that might have an effect on the performance of the image retrieval which requires further investigation and testing.

7.6 Password space and entropy

In this section of the chapter, the password space of each part of the GOTPass scheme is discussed.

i. Unlock Pattern:

In order to approximate the full password space of a draw-based scheme, Tao and Adams (2008) used a method based on the observation that a new password with the length (L + 1) could be derived from connecting an additional node to any password with length of L or extending the last stroke by one unit in each available direction (the least 3 and the most 8).

With the consideration of the grid size of the GOTPass scheme (4×4) the lower bound (the minimum number of neighbours for a node is 5 as shown in Figure 7-1) of the full password space will be:

$$\sum_{i=1}^{L\max} G^2 \times (G^2 + 5)^{i-1}$$
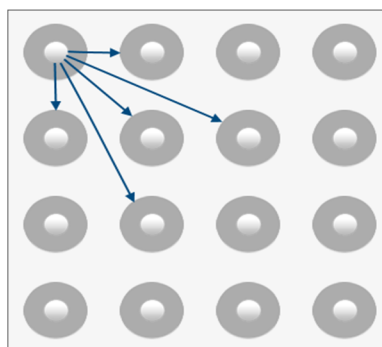
Figure 7-1: Lower bound: minimum number of node's neighbours

The upper bound (the maximum number of neighbours for a node is 12 as shown in Figure 7-2) will be:

$$\sum_{i=1}^{Lmax} G^2 \times (G^2 + 12)^{i-1}$$
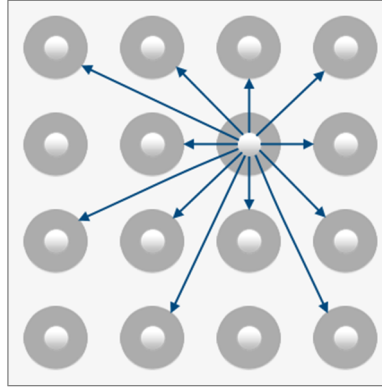
Figure 7-2: Upper bound: maximum number of node's neighbours

The lower bound of the password space was used to approximate the actual password space since there was no significant difference between the lower bound and the upper bound.

In case of GOTPass and to calculate the password space for the unlock pattern using the lower bound equation when Lmax = 5 (number of connected nodes) and grid size is 4×4 (G=4):

$$\text{Password space (Unlock pattern)} = \sum_{i=1}^{5} 4^2 \times (4^2 + 5)^{i-1} = 3{,}267{,}280$$

$$\text{Password Entropy (Unlock pattern)} = \log_2 (3{,}267{,}280) \approx 22 \text{ bits}$$

Another possible way to calculate the theoretical password space for the pattern-based graphical authentication is presented by Schneegass *et al.* (2014). For a pattern lock of minimum nodes of 5 chosen from a grid of total size of 16, the password entropy is calculated as follows:

$$\text{The minimum} = \log_2 (16 \times 15 \times 14 \times 13 \times 12) \approx 19 \text{ bits}$$

$$\text{The maximum} = \log_2 (16!) \approx 44 \text{ bits}$$

ii.   Image choice:

In a study by Vorster and van Heerden (2015) to analyse the key-space of graphical passwords, they suggested that the password space is not N^k as assumed by most researchers, but rather close to N!/(N-k)!. In the same way, van Oorschot and Wan (2009) calculated the password entropy of the recognition-based graphical scheme using the following equation when the order of the image selection is necessary:

$$r \text{ (number of rounds)} \times \log_2 \left[\frac{n \ (displayed \ images)!}{\big(n \ (displayed \ images) - k \ (passimages)\big)!} \right]$$

For the GOTPass scheme, r = 1, n = 16, k = 2, which means there is one round of verification and 2 images need to be selected in the correct order from an image panel of size 16.

$$1 \times \log_2 \left[\frac{(16)!}{(14)!} \right]$$

Password Entropy (Image choice) = $1 \times \log_2[240] \approx 8$ bits

iii.   GOTPass input format:

One-time password can be randomly guessed from the code cells above or aside the image panel since the user can select any 2 cells from the top or left axis of the challenge set. To find the password space for this part of the scheme, the method of Khot, Kumaraguru and Srinathan (2012) to compute the guessing success probability was applied.

$$r \text{ (number of rounds)} \times \log_2 \left[\frac{n \ (code \ cells)!}{\big(n \ (code \ cells) - k \ (required \ code \ cells)\big)!} \right]$$

The parameters above, r = 1, n = 8, k = 2, mean that there is one round of verification and 2 code cells need to be selected in the correct order from the edges of the image panel of size 8.

$$1 \times \log_2 \left[\frac{(8)!}{(6)!} \right]$$

Password Entropy (GOTPass input format) = $1 \times \log_2[56] \approx 6$ bits

Parameters	Range of available selections	Length of password entry	Password Entropy (Bits)
Pattern: 4×4 grid size	16 nodes	5 connected nodes	22
Image choosing: 4×4 images panel	16 images / 1 round	2 images	8
GOTPass input format	4 combination options	1 combination	6
	8 cells of code	2 cells of code	
		Total Entropy	**36**

Table 7-3: GOTPass password entropy

Table 7-3 highlights the size of the password entropy of GOTPass authentication mechanism, considering a number of parameter settings and details. GOTPass scheme has approximately 36 bits of password entropy, which also represents 2^{36} possible values (password space). The probability of successfully guessing random chosen GOTPass secrets by an attacker with no prior knowledge of the secrets except the username of the target account is $\frac{1}{2^{36}}$ (1 in 68,719,476,736). However, guessing the image-based step separately would not be securely sufficient since it would only need $\frac{1}{2^8}$ (1 in 256) chances to succeed. Although the password space size is not long enough, as most schemes of the recognition-based are, compared with that of the conventional textual password (Suo, Zhu & Owen, 2005), but GOTPass scheme leverages of multi-layer authentication which should complicate any potential attack that may exploit the password space size. Furthermore, Florêncio, Herley and Coskun (2007) found that adding login rules such as account lock-out to a relatively weak passwords of 20 bits or so is considered sufficient

protection against relevant attacks. According to van Oorschot and Wan (2009), security can be increased by choosing different parameters, yet that also affects usability.

7.7   Security empirical evaluation

Experiments to evaluate the security of the GOTPass approach were conducted in a controlled lab environment since the physical attendance for all users was required. Due to the difficulty of hiring expert testers to undertake the attacks on the proposed system, ordinary participants were recruited and asked to take part in this security experiment. For that reason, the activities of the study were simplified to suit typical users, who do not necessarily require hacking tools or special experience. The same 81 participants who took part in the usability experiment were recruited to participate in the security experiment as well. An advantage of recruiting those participants was that they were already familiar with the new scheme with a prior experience gained from their participation in the usability experiment.

Three security attacks were planned and simulated (guessing, intersection, and shoulder-surfing) to evaluate the capability of the proposed system to withstand these types of attacks. Participants were asked to devote attention to the task of each given attack and act as attackers to try to break into the system. In all security experiments, there was no direct interaction between the actual victim and the attacker (participant) since the victim was simulated in a form of recorded videos. The security experiment trials were conducted using the same GOTPass prototype application but using a different database instance to avoid interfering and affecting the data of another parallel experiment focusing on usability aspects of the approach. All participants used the same computer to perform the study tasks. Only the research investigator and the participant were allowed in the lab to avoid any possible disruption and to observe any security issues as well as noting participants' comments.

During the experiment and while the participants performing their tasks, the experimenter used to have a special form for each experiment and for every user to allow following up with the participants and record important information about each part of the experiment.

The study collected a total of 690 login attempts carried out by 81 participants. These were divided into 3 groups based on the assigned security attack experiment, as shown in Table 7-4.

Attack Type	Number of users	Number of attempts
Guessing	27	235
Shoulder-surfing	27	210
Intersection	27	245
Total	81	690

Table 7-4: Number of users & attempts in each experiment

7.7.1 Guessing attack

In this type of attack, attackers try to guess the authentication secrets of a legitimate user. In order to successfully guess GOTPass credentials, the attacker must guess 3 combined steps: unlock pattern shape, 2 pass-images, and finally the input format of GOTPass code combination, which is computationally hard.

A group of 27 participants, who were already familiar with the system, took part in this trial. Their task was to act as attackers to guess a particular account credentials. An additional account was created for this purpose, and some general information about that account was documented and revealed to help attackers guess it correctly. The given information was the username, the shape of the pattern, and the selected security level of that account. The details of the created account and the information revealed was as follows:

- **Username:** guesscscan (given)

- **Pattern:** shape of number '2'

    (Partially given – only the shape was revealed, then after 5 attempts the exact pattern was given)
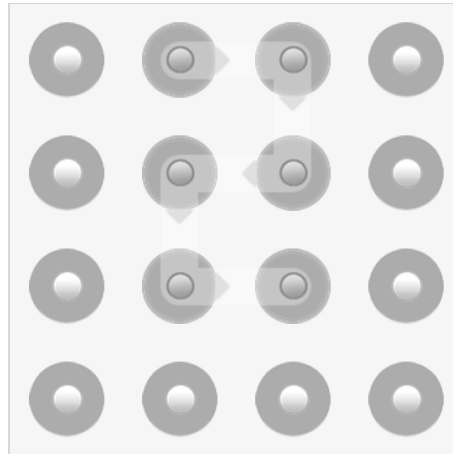
Figure 7-3: The shape of the correct unlock pattern to guess (shape of number 2)

- **Pass-images:** Chosen from the following themes: flag, stationery, computer, and paint

    (Partially given – only the themes that pass-images belong to were revealed)

Figure 7-4: The pass-images portfolio for the 'guessing attack' account

- **Input format (Code location):** Basic security level: First pass-image from TOP, Second pass-image from TOP

    (Partially given – only the security level was revealed but not the exact option)

In order to validate participants' guesses, they were given the chance to use the GOTPass system and try to login with the information they managed to gather. Each user was allowed maximum of 10 attempts unless they decide to give up after their fifth attempt.

That in turn allowed further investigation of two points:

- The level of difficulty to guess user credentials.

- The effectiveness of revealing GOTPass secrets to others.

Participants	Attempts	Success	Coincident	Total	Success with aid
27	235	2	4	6	6
		0.9%	1.7%	2.6%	100%

Table 7-5: Details about the guessing attack trial

The total number of break-in attempts in this attack trial was 235 (Table 7-5). Only 2 attempts were successful which is considered less than 1% whereas, 4 other attempts were deemed as coincidence due to part of the correct credentials being incorrect but succeed by chance (i.e. missing one of the pass-images but submit the correct associated codes). According to Wiedenbeck *et al.* (2006), the accidental login (i.e. an attacker select the correct codes by chance) in challenge-response authentication is always possible. However, all of these successful guessing attempts occurred within the last 5 attempts in which the participants gained some help from the experimenter. The aid was in a form of solving the unlock pattern in order to facilitate the guessing task for the remaining parts that include the pass-images and the input format. Users who failed to make any successful login during the first 5 attempts were offered this type of help.

Correct pattern without aid	Correct pattern with aid	Correct single pass-image	Correct 2 pass-images	Correct input format
4	100	47	7	123
1.7%	42.6%	20%	3%	52.3%

Table 7-6: Breakdown of each correct part of the guessing attempts

It is worth mentioning that within the first 5 attempts for all users (135 attempts), only 4 attempts (3%) succeeded on guessing the correct unlock pattern (Table 7-6). However, those successful pattern guesses were followed by unsuccessful ones since users were

uncertain about the correctness of their guesses due to the implementation of the implicit feedback. After the first 5 attempts, the experimenter helped the users by solving the unlock pattern for them. Thus, a significant finding can be inferred that implementing the unlock pattern in the scheme is effective since it proves its ability to act as a first line of defence to protect the main recognition-based graphical password. In addition, in about less than a quarter of the total attempts, participants managed to correctly guess only one pass-image but failed to do so for the second pass-image. In very few occasions (3%), participants guessed the two pass-images correctly but that does not necessarily mean that they managed to complete their login successfully as they still need to enter the correct associated GOTPass codes in the correct order. In regard to the input format, participants were able to guess the correct input format for more than half of the attempts. Although this guessing percentage appears high but it should be noted that there are only two options for the user to choose from as the security level was given.

Another investigated point was the effectiveness of revealing GOTPass secrets to others. The analysis of this attack experiment showed that passing account secrets (unlock pattern, pass-images, input format) to another person was not easy and thus ineffective. At first, users could not manage to guess the correct pattern which was given as a shape of number 2. Due to the high number of variations of that shape, it was clearly hard to determine the correct pattern. One of the possible additions to ease this part was to provide the starting point of the shape and the size (how many points) to the attacker, which needs further investigation to ensure its validity. With regard to the pass-images, since the system might display images from the same category or even similar images with different colours, that should complicate the accuracy of the information revealed as well as increase the uncertainty. Revealing the security level whether Basic or Advanced would also require the user to choose from the two available sub options. Thus, passing the exact input format

(e.g. the code of the 1st pass-image from Top & 2nd from Left) should be more useful than knowing the security level. In addition, users were asked in the post-test questionnaire about what they think about the simplicity of passing their account information to friends and their ability to use this information to login on their behalf. Over than 70% of the participants thought that their friends would still have difficulty logging in correctly using the given information about the GOTPass secrets.

Pass-image					Total
FRQ	23	18	11	9	61

Figure 7-5: Frequency of identified pass-images in the guessing attack experiment

The analysis of the frequency of identifying pass-images during the guessing attack experiment showed that some images were identified more often than others (Figure 7-5). However, the use of distractor-images in association with each pass-image was effective in obscuring the correct pass-images that led attackers to select distractor-images instead.

7.7.2 Observability – Shoulder-surfing attack (SSA)

Assuming that the attackers managed to pass the first defence technique (unlock pattern), they will still be confronted by another security barrier that is the image recognition and its associated OTP technique. Selecting pass-images is done only mentally which means that there is no need for clicking on the required images. Determining the pass-images is only used to find the respective code positions that the user needs to enter in the OTP text field. Consequently, the attacker who tries to peep over the shoulder or record with hidden cameras could only manage to capture random numbers being entered. However, observing multiple login sessions where the entered codes are also visible might enable the attacker to discover the pass-images based on the intersection and correlation among the observations.

In this part of the experiment, the system resistance against the shoulder-surfing attack was examined. This simulation involves the experimenter acting as a victim with an arrangement for the participants to watch multiple login trials to gain as much information as possible to try using it to gain an unauthorised access. An additional account was created then used to login to the system for 3 times. During that time, the scene of the experiment machine was being filmed (the camera was intentionally placed at a location less immediately adjacent to the user entering the login data). A different group consisting of 27 users participated in this study in which they were displayed the captured video of the login attempts for two times and were allowed to take notes while watching the video to help them gather information about the user account that they need to break into. The details of the target account to be captured was as follows:

- **Username:** sscscan (shown)
- **Pattern:** shape of number '2' (shown)
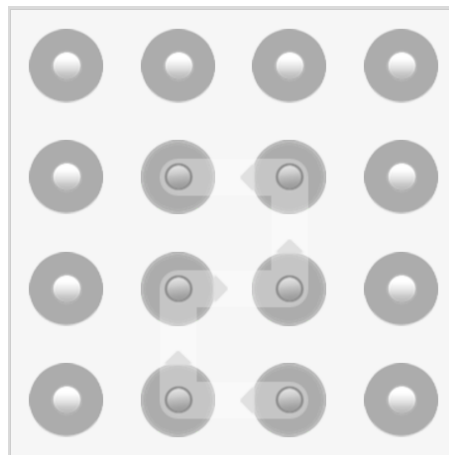
Figure 7-6: The shape of the unlock pattern to be captured (shape of number 2 in reverse)

- **Pass-images:** (Required)
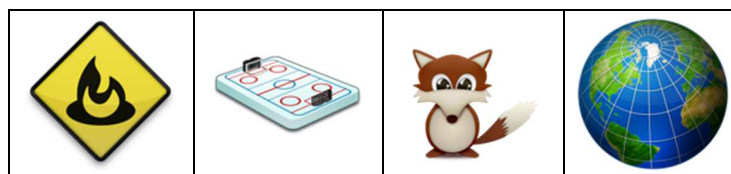
Figure 7-7: The pass-images portfolio for the shoulder-surfing account

- **Input format (Code location):** (Required – can be extracted by analysing the keyboard captured data during entry)

In order to validate the captured information, users were given the chance to use the GOTPass system and try to login with the information they managed to collect. The allowed login attempts were limited to 10, however, in case users want to give up earlier they have the right to stop after completing the fifth attempt.
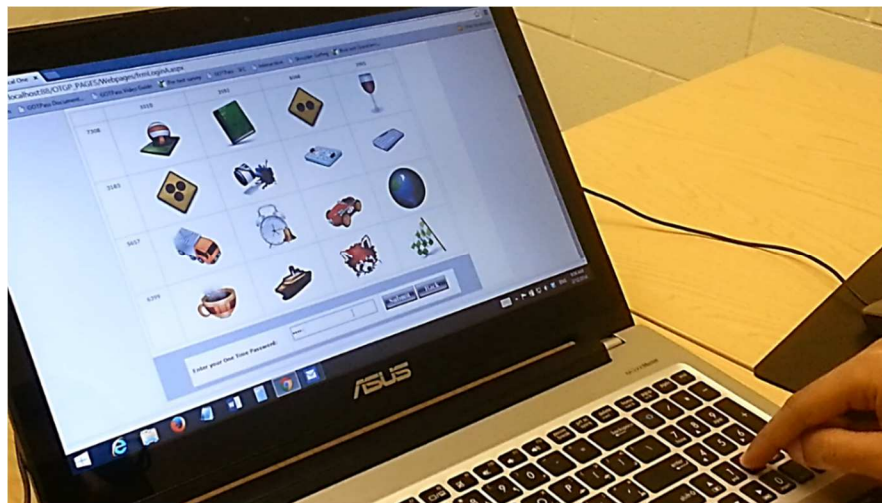
Figure 7-8: A screenshot from the shoulder-surfing attack simulation video

In this experiment, users carried out 210 attempts in total. As shown in Table 7-7, users managed to gain correct access 6 times (equivalents to 3%) and 5 other attempts were reported as coincidence. Although the rate of break-in using shoulder-surfing attack was about 5% but that might be due to the nature of filming the scene for the attack simulation, which involved the screen and keyboard as shown in Figure 7-8. That, in turn, allowed easier capturing for the needed information since the challenge set data and the entered codes via the keyboard were all available. In addition, the majority of the successful attempts (82%) occurred within the last 5 attempts which might mean that users started to build their knowledge by combining some of the gathered information from the captured video and the analysis of the real data of each login session.

Participants	Attempts	Success	Coincident	Total	Success within last 5 attempts
27	210	6	5	11	9
		2.9%	2.4%	5.2%	4.3%

Table 7-7: Details about the shoulder-surfing attack trial

Drawing the unlock pattern was designed to be less visible (semi-transparent) for peepers but visible enough for the close legitimate user as illustrated in Figure 7-6. The data shown in Table 7-8 supported such implementation since some participants failed to capture the correct pattern shape even after playing the captured video multiple times which resulted in 12.4% incorrect attempts. Moreover, identifying one single correct pass-image was successful in about 38% of the attempts whereas recognising the two pass-images together was achieved in approximately 4% of the attempts. As for the input format, participants identified the correct input format of over than 50% of the attempts. However, this type of attack seems less complicated than others as the attackers can gain more information that might facilitate the break-in task and with some intensive analysis, the attempt might succeed.

Correct username	Correct pattern	Correct single pass-image	Correct 2 pass-images	Correct input format
200	184	79	9	109
95.2%	87.6%	37.6%	4.3%	51.9%

Table 7-8: Breakdown of each correct part of the shoulder-surfing attempts

Analysing the frequency of identifying pass-images during the shoulder-surfing attack experiment indicated that pass-images were identified almost evenly (Figure 7-9). However, the uncertainty about the correct combination of pass-images and the input format beside the use of distractor-images played a vital role in confusing the attackers.

Pass-image					Total
FRQ	26	25	25	21	97

Figure 7-9: Frequency of identified pass-images in shoulder-surfing attack

7.7.3 Observability – Intersection attack (ISA)

Using intersection analysis by its own will not reveal much information as portfolios for both pass-image and distractor-image are implemented. An attacker would face difficulties distinguishing between pass-images that are valid to locate the code positions and the distractor-images that are linked to each pass-image. However, in case the attackers succeeded in finding the correct pass-images they will still need to guess the correct input format (code location) correctly.

Another security experiment task was to inspect the system resistance against intersection attack. Simulating this attack used similar approach as that described previously in the shoulder-surfing attack subsection (7.7.2). An additional account was used and a set of 27 participants were displayed a video of screen capturing the login attempts of that specific account for 3 times (Figure 7-10). Watching the video was repeated two times for each user. Note taking was allowed and then participants were given 10 login attempts at maximum, where they need to identify the pass-images of that account at first then guess the correct input format.

Figure 7-10: A screenshot from the intersection attack simulation video

The details of the target account to be captured was as follows:

- **Username:** iscscan (shown)

- **Pattern:** shape of number '2' (shown)
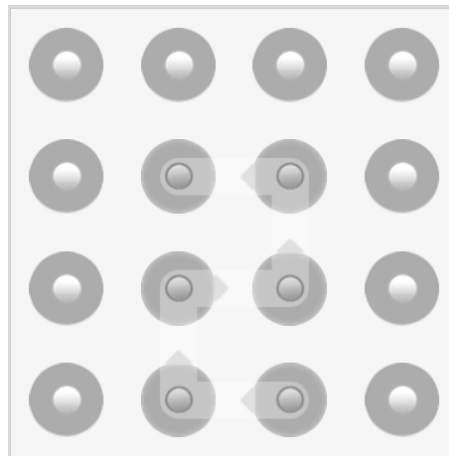
Figure 7-11: The shape of the unlock pattern to be captured (shape of number 2 in reverse)

- **Pass-images:** (Required)

Figure 7-12: The pass-images portfolio for the intersection account

- **Input format (Code location):** (Required – totally hidden by shielding the entered data)

211

Despite the fact that the screen capturing of all login components were clearly visible and easy to note down except the entered data, which was shielded, none of the 245 attempts to break into the system using intersection attack was successful apart from 6 attempts that succeeded accidentally (Table 7-9). It can be inferred from this result that carrying out a successful attack would need information from both the challenge set as well as the keyboard which proves the effectiveness of separating the challenge mean and the data entry mean to mitigate such attacks. That corresponds to the findings of the study by Tari, Ozok and Holden (2006), which indicated that replacing regular mouse click by a keyboard for data entry was very effective in reducing the threat of shoulder-surfing attack. The implementation of a keypad entry adds an extra challenge before an attacker which requires capturing information from two distinct sources; keystroke-logger and screen scraping.

Participants	Attempts	Success	Coincident	Total	Success within last 5 attempts
27	245	0	6	6	3
		0	2.4%	2.4%	1.2%

Table 7-9: Details about the intersection attack trial

The data in Table 7-10 shows that all attackers succeeded in capturing the correct pattern shape which implies that direct recording of the login screen by some types of spyware can unveil the pattern very clearly. Moreover, participants managed to identify one single correct pass-image of nearly half of the attempts, however, they failed to recognise the two pass-images together, except for a few times of about 3%. Additionally, choosing the correct input format was successful in less than one quarter of the attempts. Overall, intersection attack seems to be a complex attack as a significant part of the information needed to complete the attack is always absent which is the input format. Without the knowledge of the input format (code location) the attacker can only randomly guess one of the four available options that lead to the correct code combination.

Correct username	Correct pattern	Correct single pass-image	Correct 2 pass-images	Correct input format
244	245	105	7	58
99.6%	100%	42.9%	2.9%	23.7%

Table 7-10: Breakdown of each correct part of the intersection attempts

By examining the result of the frequency of identifying pass-images during the intersection attack experiment, Figure 7-13 showed that the number of identified pass-images was relatively high and there was a variation in the number of times each image was identified. However, that might indicate that viewing a captured video of the login screen is somewhat useful for partial recognition of the pass-images but nevertheless that is not enough to break-in successfully since the input format is still unknown.

Pass-image					Total
FRQ	52	35	20	12	119

Figure 7-13: Frequency of identified pass-images in intersection attack

7.8 Experiment results and discussion

Table 7-11 shows a summary of the experiment results where the total number of the successful break-in attempts was only 8 out of 690, which represents only 1.2%. When considering the coincident attempts, the total number of break-in attempts was raised to 23 that is only 3.3%. This rate is relatively low and the results are encouraging since attack simulations were deliberately designed to facilitate misuse. In reality, it seems very difficult to capture several login sessions from a close distance as in the conducted simulations which means an attack in a real environment should be more complicated than that in the lab. In addition, almost all attackers used the "Trial and Error" method to solve the break-in tasks.

	Success	Coincident	Total	Percentage
Guessing	2	4	6	6/235×100 = **2.6**
Intersection	0	6	6	6/245×100 = **2.4**
Shoulder-surfing	6	5	11	11/210×100 = **5.2**
Total	8	15	23	23/690×100 = **3.3**
Percentage	8/690×100 = **1.2**	15/690×100 = **2.2**	23/690×100 = **3.3**	

Table 7-11: Number of successful break-in attempts in all security experiments

The number of the successful attempts of the shoulder-surfing attack trial was higher than that of the other attacks. The success rate for shoulder-surfing attack occupies about half of the total successful attempts whereas the other half is divided nearly equally between guessing and intersection attacks. One reason behind the high break-in rate in the shoulder-surfing attack is the availability of the main authentication components of this scheme; username, unlock patter, pass-images, and random codes. Capturing and analysing the entered codes would lead to discovering the rows and columns of the pass-images which reduces the image options and therefore increases the probabilities of identifying the correct pass-images.

A few observations about exceptional incidents were reported. Table 7-12 contains interesting results that summarise the exceptional incidents that resulted in unexpected outcomes or the so-called coincident attempts. In general, the results indicated that similar incidents were performed by attackers in spite of the type of the attack. Mainly, there were 4 incident types in which the first one has its users successfully identified two correct pass-images as well as the correct input format (code locations) but the codes were entered in the wrong order which ended up as incorrect attempt. In the second incident, the attackers recognised two correct pass-images but could not identify the correct input format (code locations), at the end, the attempt was unsuccessful. In the third incident, the user managed to identify only 1 correct pass-image and correct input format (code

location). The second chosen image was wrong but located on the same axis where the correct pass-image was residing which luckily resulted in entering the right codes. In the last incident, the attacker did not manage to identify any correct pass-images but managed to identify the correct input format (code location). Luckily, the chosen images were located on the same axes where the correct pass-images were residing which luckily resulted in entering the right codes for that particular attempt.

It can be inferred from Table 7-12 that choosing the pass-images and their associated codes in the correct order can be considered a security feature that adds strength to the system. With regard to guessing attack, although coincident success is possible, but still did not exceed 1.7% of the carried out attempts which is deemed very low and unlikely to threaten the security of the GOTPass scheme.

	Pass-image1	Pass-image2	Input format (Code location)	Code order	Login status	Attack	FRQ.	Total
Incident 1	✓	✓	✓	✗	✗	Guessing	5	6
						SSA	1	
Incident 2	✓	✓	✗	-	✗	ISA	7	7
Incident 3	✓	✗	✓	✓	✓	Guessing	2	9
						SSA	4	
						ISA	3	
Incident 4	✗	✗	✓	✓	✓	Guessing	2	6
						SSA	1	
						ISA	3	

Table 7-12: Breakdown of the login status for the exceptional incidents in the security attacks

Other general observations were also noted, one of which was the capture of only the random codes from the displayed video by a few participants who thought that they would be asked to enter the exact codes for the experiment while some others used the intersection strategy to guess the pass-images while performing different type of attack. It was also noticed that attackers tried to choose images from the same axis which is incorrect by design while some others tried to choose images from the same theme which is obviously impossible.

Focusing more on one of the chained steps and neglecting the others by choosing weak passwords should not be a major issue, as the success of breaking one of the authentication steps will not compromise the entire credentials. In addition, the employment of the implicit feedback technique plays an important role in hiding which step is actually incorrect. In this way, it is difficult for an attacker to find out whether the stronger or weaker step went wrong. In other words, GOTPass works as a package where each part or feature complements the other. Another important factor is the implementation of the challenge-response (or dynamic pass-images portfolio) which keep challenging the user with a subset of the pass-images portfolio at each login time.

At the end of each security trial, participants were interviewed and asked a few questions regarding the trial they just undertook. Mainly, they were asked to determine which part of the GOTPass scheme has made the system difficult to break into. A request was made for the users to sort their answers in descending order based on the difficulty level. In the guessing attack experiment, the answers were almost close but pattern-related factors were selected more. The majority of users admitted that it is a chain of factors and looking at each one aside makes you think it is causing more difficulty than others.

There are two important factors that may influence the quality of the user performance in such specialised experiments that are the expertise and the personal interest. Thus, in an attempt to measure the user's interest to conduct these types of security experiments, they were asked whether they have the interest to take part in a similar activity in the future or not. Over than 80% of the respondents were positive and keen to participate again which gives an indication that they were motivated and enjoying their attacking tasks.

7.9 Results of user perception and questionnaire

The security-related data of this section was derived from the same data source of the usability study. Away from the security attacks, the idea was to find out about the user attitudes towards security while using the scheme. During the registration phase, users were asked to select their preferable security level at the final step. Table 7-13 shows that nearly two-thirds of the participants selected the basic security level. That might be due to either less concern about security or maybe the caution of using a new scheme. Still, choosing the advanced level by more than the third of the participants for a newly introduced authentication system is considered good sign of user attitude towards security. In respect to the input format, the random assigning of the various input formats by the system seems fair for the basic level but uneven for the advanced level.

Security level	Input format option	FRQ.	Percentage
Basic	Option 1 (Top-Top)	24	29.6%
	Option 2 (Left-Left)	25	30.9%
Total		49	60.5%
Advanced	Option 3 (Top-Left)	22	27.2%
	Option 4 (Left-Top)	10	12.3%
Total		32	39.5%

Table 7-13: The frequency of the chosen security level & the assigned option

A complete section of the post-test questionnaire was dedicated for the security aspects of the scheme. A major part of this questionnaire was discussed earlier in chapter 6 especially sections related to usability and design aspects of the system. As far as the GOTPass security is concerned, participants were asked some questions regarding how they feel about several security points of the system as highlighted in Table 7-14. At first and as the main purpose of such authentication system is to secure the users accounts, participants were asked whether they would trust GOTPass scheme to do so or not. The result showed that most of the responses were positive in that matter. Meaningful

passwords can be easily linked to a particular user and thus easy to guess but that is not the case with GOTPass, as 91% of the participants stated that their GOTPass secret is unlikely to be meaningful to others. In regard to the ability to guess the GOTPass, only less than quarter of the responses thought that this scheme would be easy to guess by attacker. Another issue of passwords is the ease of revealing secrets to others, but over than 80% of the responses thought that disclosing the secrets would not allow their friends to reproduce the GOTPass secrets correctly. One important security feature was the ambiguity of the feedback in which the user is not informed when making mistakes during password entry until after the final login submission. Although implementing such technique can possibly confuse legitimate users, but conversely the majority of participants considered it as a good security practice. Participants were asked to rate the impact level of each part of their GOTPass on increasing the security. The result showed that pass-images and their associated input format formed the highest security impact whereas unlock pattern scored above average.

Section (C) - About the security aspects *(1) Strongly disagree – (7) Strongly agree*		Average	%
I would trust GOTPass system to secure my accounts		6.68	95.4
My GOTPass is unlikely to have any meaning to other people		6.37	91.0
This type of authentication would be easy for attackers to guess		1.58	22.6
If I briefly explain to my partner/close friend what my GOTPass secrets are, I think they will still have difficulty reproducing my GOTPass correctly		5.85	83.6
I think that the ambiguity of the feedback, when a wrong username or pattern is entered, is a good security practice.		6.75	96.5
Rate the impact level of each part of your GOTPass on increasing the security: *(1) No impact – (6) High impact*	(Username)	2.73	45.5
	(Unlock pattern)	4.65	77.6
	(Pass-images)	5.62	93.6
	(GOTPass input format - Code location)	5.60	93.4

Table 7-14: The results of the security section of the post-test questionnaire

Participants were asked some additional questions in relation to security such as how they feel about the implementation of variable response through pass-images portfolio. Two-thirds of the participants felt that this technique has added security to the system while quarter of them felt that it has added both security and complexity. Despite the fact that many participants thought that using mouse click to select pass-images can provide convenience to users, only a few of them of less than 5% thought that it can provide more security. That means that they feel that the use of mouse click is insecure and instead using keyboard can be better option to enhance the security. A large number of users thought that it would be more secure if the system generates alphanumerical codes as an alternative to the numerical codes. Finally, the majority of participants agreed to use GOTPass for sensitive web authentication.

7.10 The protection against other attacks

There are other attacks that can threaten the graphical password schemes such as spyware, phishing, replay and dictionary attacks. The effect of such attacks can be theoretically analysed as follows. In order for a spyware attack to succeed, enough information about the password components must be gained. Installing a keystroke logger to collect the entered data may help in revealing the username and possibly the unlock pattern, but it is practically useless beyond that. The reason is that the image recognition step of the GOTPass scheme is carried out mentally without the need for clicking on the pass-images, besides the use of OTP which is changeable at every login time. The other type of spying is through the screen recording in which all visual information is made available for the attacker. This attack is able to disclose login information about username, unlock pattern, and the challenge set images with their random codes but fails to catch the entered codes since the GOTPass scheme uses shielded input characters. Thus, using any type of the aforementioned spywares in its own would not compromise the system. However,

utilising both techniques; keystroke logger and screen recording would be needed to gather enough knowledge of the different authentication steps, which is mostly time, effort, and cost overhead for attackers.

Phishing and replay attack against GOTPass scheme would require a prior acquisition of the system images as well as the victim pass-images in particular. This is needed in order to display the correct set of images that the user can recognise and then make the right selection. However, this is infeasible since the original purpose of such attack is to discover the victim's pass-images and once it is known then there is no point of carrying out the attack in the first place. In addition, the system is designed to use assorted responses approach (pass-image portfolio) which ensures that only a subset of the user's secret is exposed on each login attempt not the whole secret.

Dictionary attacks on a multi-layer authentication system like GOTPass is hard due to the difficulty of conducting an online dictionary attack on multiple login techniques, e.g. unlock pattern should protect the primary authentication method (image recognition). Building such a dictionary is even more difficult since it presumably involves a combination of several distinct techniques. There is no way to verify the correct or wrong step of the submitted login information. Moreover, the use of OTP should mitigate this type of attack. Another effective protection technique is the implementation of the system lockout which limit the number of incorrect attempts before the system suspend the account for a particular period of time. Besides, increasing the delay before reactivating the account would add extra security as well as usability since it ensures that the legitimate user is not permanently locked out in case several incorrect attempts were made.

7.11 Additional security study

This supplementary study is initially concerned about the intersection attack mitigation. Although the result of the primary security experiment of this attack was encouraging, but the analysis of the result led to a design enhancement that may potentially increase the resistance against intersection attack in particular and other attacks in general.

The idea was to increase the number of the distractor-images linked to each pass-image from 3 to 7. In this case the challenge grid will contain 2 pass-images and 14 distractor-images which eliminate the use of decoy images. The prospective advantage of this modification was to prevent the attacker from analysing the login screens seeking to identify the images that appear more frequently. In other words, the displayed images in the grid would be constant across all login sessions depending on the system selected set of pass-images from the user portfolio. That, in turn, should decrease the guessing probability of combining two correct pass-images.

7.11.1 Study procedure

This study was conducted offline where the physical attendance of the participants is not required, taking part in this study can be done at the participant's end at anytime and anywhere. It was intended for those who already participated in the GOTPass user trials and were familiar with the system. The study was prepared in a document and sent to participants by email with an invitation letter describing the required task and the approach to complete and submit the answers. Initially, the study involved only the image recognition and the input format determination steps. Thus, the study assumed that the username and unlock pattern were successful and focused only on the remaining steps. In order to have an appropriate experiment setup, four images were selected randomly as pass-images for the given account beside a random input format as highlighted in Figure 7-14. The study document was organised in a way that the 10 login sessions were simulated to cover all possible pass-images combinations.

Pass-images	
Input format	1st pass-image (LEFT) + 2nd pass-image (TOP)

Figure 7-14: Details of the experimental account for break-in

Participants were given two weeks to answer and respond to the study. In order to motivate participants to take part in this additional experiment and to encourage them to spend more effort to find the right answers, a prize of £20 cash was allocated for one lucky winner under the following conditions:

1. The break-in is considered successful when both pass-images and the associated codes are all correct.

2. To enter the prize draw, at least one successful attempt is required out of the total 10 attempts.

3. Successful participants will enter the prize draw and the winner will be chosen randomly to earn the prize.

Participants were presented with screenshots of 10 login attempts for a single GOTPass account (see Figure 7-15). The task was to identify the most frequently appeared images that likely to be the correct pass-images for the given account in each login session. They were also reminded that the total pass-images for this account is 4, but the system displays only 2 random correct pass-images in each challenge grid. After identifying the pass-images, they must determine the codes associated with each pass-image – top or left.

Underneath each challenge grid there is a table in which the participant needs to fill-in by specifying the pass-image number and the code from top axis or left axis of each image. Once all answers of the 10 login sessions were completed, the user was requested to save the study document in his/her name and send it back to the experimenter email address or alternatively it can be printed out and hand in a hard copy.

Figure 7-15: Sample of the login session of the additional security experiment

7.11.2 Results and analysis

By the end of the allowed period of study that last for two weeks, 22 responses from the participants were received that forms a total of 220 attempts. The result showed that none of the participants managed to break-in successfully. Thus, there was no winner, but still the prize was randomly awarded to one participants amongst all.

The results in Table 7-15 indicated that some participants managed to identify one single correct pass-image in almost one quarter of the attempts. In 16% of the attempts, they successfully selected a single correct code. Three participants managed to submit the correct codes for the login session which is equivalent to only 1.4% of the total attempts. However, these successful attempts were not completely correct but coincident since the selected pass-images were wrong. Lastly, the input format was chosen correctly in less

than 10% of the attempts. From the above results, having a full set of distractor-images alongside the subset of the pass-images has proved its value in mitigating the intersection attack and consequently the shoulder-surfing attack which sometimes utilise intersection technique to complete the attack.

	Correct single pass-image	Correct both pass-images	Correct single code	Correct both codes	Correct input format (code location)
FRQ.	53	0	36	3	21
%	24.1	0	16.4	1.4	9.5

Table 7-15: The outcome details of the additional security trial

For broader investigation about the validity of the initial results obtained above, the study reanalysed the received answers based on different scenarios of input format options. In this part of the study, the data was revisited again several times but with the assumption that another input format option was in place each time instead of the one originally assigned when this additional study was initiated. Table 7-16 presents the outcomes of the study in cases where other input formats were used. It can be inferred that there were more correct elements than that in the primary setup but that does not mean a complete correct attempt. Among these cases, the highest rate (30%) of identifying a single pass-image was reached when using the other input format option of the advanced security level. The most successful attempts in submitting the correct codes was with the first basic security level. Only 4% of the total attempts entered the correct codes which is almost three times the rate in the primary setup, but even though, it is still considered low. The correct input format was successfully guessed in more than one third of the attempts when applying the second basic security level.

Security level	Input format	Correct single code	Correct both codes	Correct input format (code location)
Advanced 1	1st pass-image - top / 2nd pass-image - left	66 (30%)	7 (3.2%)	69 (31.4%)
Basic 1	1st pass-image - left / 2nd pass-image - left	49 (22.3%)	9 (4.1%)	45 (20.5%)
Basic 2	1st pass-image - top / 2nd pass-image - top	56 (25.5%)	5 (2.3%)	77 (35%)

Table 7-16: The outcome details for the other input formats

7.11.3 The original GOTPass design versus modified design

Despite the fact that there was no significant pattern found in the additional study to distinguish between the security levels or even the input formats, but there was an added security value. Comparing the results of the intersection attack experiments in the original design of GOTPass and the modified one showed a substantial advantage gained by the implementation of a constant set of distractor-images. Adopting the 7 distractor-images approach improved the security of the GOTPass scheme as highlighted in Table 7-17 where participants of the original design managed to identify almost twice as many 'single pass-image' as the participants of the modified design did. Not only that but also participants of the modified design were unable to identify any combination of the two pass-images.

	Correct single pass-image	Correct both pass-images
Original GOTPass implementation 3 distractor-images	47.3%	2.9%
Modified GOTPass implementation 7 distractor-images	24%	0%

Table 7-17: Results comparison between the original and modified GOTPass design

7.12 Summary

To conclude, this chapter has demonstrated how secure the GOTPass scheme is in resisting guessing and observation attacks. The security evaluation provided deep insight on the resistance level of different types of attacks including guessing attack, intersection attack, and shoulder-surfing attack. The GOTPass scheme underwent two types of security evaluation: theoretical and empirical. The security experiment involved three different attack simulations designed for the participants to carry out. One of the important evaluation factors to increase the result's accuracy was the large sample size of participants for such a security experiment. The empirical study included 690 break-in attempts divided into three different attacks trials. The results were encouraging as they showed only 3.3% of the total conducted attempts were successful which is considered a relatively low rate. The overall solution was therefore found to be both secure and usable. In addition, another supplementary study was conducted concerning mainly about intersection attack. This study involved changing a fundamental attribute of the system that is increasing the number of the distractor-images and eliminating the use of decoys. The results were encouraging as none of the participants succeeded to identify the required set of pass-images which proves its effectiveness. Furthermore, other types of possible attacks including spyware, phishing, replay, and dictionary attacks were discussed. The analysis of the outcome showed that the GOTPass scheme has the necessary defence techniques in place to mitigate the threats of such attacks. Overall, this system has shown a considerable potential and capability to contribute in enhancing current usable security.

Chapter Eight

Conclusions and Future Work

This chapter concludes the work of this thesis by presenting an outline of the research contributions, followed by a summary of the thesis and the research limitations. Finally, several potential future works are discussed.

8.1. Research contributions and achievements

This thesis has made several original contributions to the research in regard to the usable security of graphical password authentication as follows:

- A new data-entry classification within the field of graphical authentication was suggested. This classification utilises keyboard-typing entry as a way to submit the secret information. In addition, the study also suggested adding some distinguishing details for better clarification which involved several design aspects, such as the input approach (draw, click, choice, keyboard-typing entry) and the display style (grid, image, icon).

- Developing a hybrid multi-layer authentication system (GOTPass) which combines multiple graphical password methods (draw-based and recognition-based) along with the one-time password technique (OTP). The new composite scheme provides an in-browser/in-band OTP which is totally independent of any additional devices. Moreover, GOTPass scheme showed significant usability and security capabilities that fulfil the need for a secure usable alternative authentication scheme.

- Employing a dynamic one-time password combination obtained through a multi-layer graphical password. That enables the production of a number of one-time codes, but requires an additional step to realise the correct ones. Knowing the correct graphical password components along with the input format (code location) leads to the right combination of codes.

- Implementing a web-based unlock pattern showed an effective proactive protection. The level of safeguarding provided by the integration of the unlock pattern into the other steps of the scheme was very high.

- Adopting a new approach to reduce the selection of hot-images by using system-assigned themes with user-chosen images. This approach distributes the selection of pass-images by assigning users with random themes which restrict the direct selection of preferable images that are likely to become hot-images.

- Evaluating the security of a hybrid graphical authentication using two methods. The first method is 'theoretical', based on assessment criteria, while the second is 'empirical', in which several attacks were simulated and examined. The results of the two evaluations were both supportive and positive.

The research aims were achieved through satisfying the following research objectives:

Objective 1: Review the common user-authentication mechanisms to highlight their strengths and weaknesses, and then conduct a comprehensive review of graphical password schemes in order to explore their characteristics and try to find an opportunity for enhancement.

Reviewing the main user-authentication mechanisms in Chapter 2 helped to recognise the drawbacks that need to be overcome while proposing a new authentication technique.

Chapter 2 managed to answer the following questions:

- Having identified the core problems related to the conventional text-based passwords, what are the alternatives? Do the alternatives offer a better solution?

- Is there still need for a new alternative authentication?

- What are the requirements of such an alternative?

In terms of graphical password authentication, reviewing the related literature has resulted in comprehensive comparisons between different aspects of the existing schemes. The advantages and limitations of each category were addressed in Chapter 3.

A number of key features to be included into the new proposal were derived from the conducted reviews. These features are summarised below:

- Generating an OTP using detour (indirect input) techniques, where the knowledge of the actual password is used for login while the actual password remains hidden to increase the security level.

- Spyware and observation problems can be overcome by separating the challenge operation from the response operation.

- Avoiding any visual clicking or selection (none, deception, or transparent entry) in the authentication process is effective mitigation against observation attacks.

Chapter 3 managed to answer the following questions:

- Are there any significant strengths within the graphical password that can be leveraged to produce an enhanced secure/usable authentication method?

- What are the challenges that face the current graphical password techniques?

Objective 2: Assess the authentication mechanisms offered by online banking systems by exploring the authentication limitations. Investigate the users' perception of the idea of carrying around multiple authentication tokens and how they perceive the adoption of the graphical password method as an alternative authentication method to protect their accounts.

Having investigated the existing online authentication methods currently in use by some leading financial firms, Chapter 4 confirmed that the majority of the online banking

systems do not offer a secure alternative authentication if the main authentication method cannot be satisfied. In addition, this chapter presented the results of the online user survey, which sought the views of users regarding carrying around multiple authentication tokens and what they thought about graphical passwords as a possible alternative. The results demonstrated that approximately two-thirds of the participants had experienced failure in fulfilling the login requirements for various reasons – more than half were related to the unavailability of the authentication devices. A large number of the participants stated that carrying around multiple tokens is inconvenient, and almost half of them supported the use of graphical passwords as an alternative means of authentication.

Chapter 4 managed to answer the following questions:

- Do online banking systems offer secure alternative ways for authentication in situations where the main authentication method cannot be satisfied due to the unavailability of the security token?
- Is carrying around multiple security tokens convenient for online banking clients?
- Would users accept the idea of having graphical passwords in place for authentication when their security tokens are unavailable?

Objective 3: Design and develop a novel authentication scheme and then empirically evaluate its security and usability.

The aim of the thesis was to fill the research gap to enable users secure access to their accounts in situations where the use of an authentication device is not possible. In doing so, the thesis introduced a novel authentication scheme called Graphical One-Time Password (GOTPass), which combines two types of graphical passwords, namely draw-based and recognition-based methods along with the utilisation of the one-time password technique. This was presented in Chapter 5, which described the registration and

authentication procedures, with an emphasis on the significant characteristics of the new scheme.

Chapter 5 managed to answer the following questions:

- Does the proposed system have the capability to work independently of any devices?
- Can the proposed system work with an online banking system or similar?

Initially this scheme underwent two main evaluations related to usability and security to ensure its suitability for critical systems. Chapter 6 presented the outcome of the empirical usability evaluation which involved 81 participants over a 5-week time period. Participants carried out a total of 1,302 login attempts with a 93% success rate and an average login time of 24.5 seconds. Overall, the new scheme showed an acceptable level of efficiency as well as a relatively high level of effectiveness and user satisfaction. Furthermore, memorability was also evaluated where all participants managed to remember their new credentials and login successfully within three login attempts after one month of non-use.

Chapter 6 managed to answer the following question:

- Does the new scheme provide the main usability characteristics, in terms of effectiveness, efficiency, memorability and user satisfaction?
- How effective is the system-assigned themes with user-chosen images approach in reducing the bias selection and hot-images?

The security evaluations were discussed in Chapter 7, which presented the initial theoretical evaluation followed by the simulation of three types of attacks: guessing, shoulder-surfing and intersection. The theoretical assessment revealed that most of the

countermeasures to protect against common attacks were taken into account by the proposed system. The outcomes of the empirical evaluations demonstrated that the new scheme managed to mitigate both guessing and observation attacks. The experiments included 690 break-in attempts divided into three different attack trials. Only 3.3% of the total conducted attempts were successful which is considered to be a relatively low rate. Looking at the overall results from both experiments (usability and security), they qualify the new scheme and show that it can contribute to enhancing the current state of usable security.

Chapter 7 managed to answer the following questions:

- Does the new scheme offer the main security characteristics?
- Is the new scheme capable of withstanding the major types of attacks?

Objective 4: Investigate the users' perception of the security and usability aspects of the new proposed authentication scheme.

Measuring the users' satisfaction of the new scheme, including security, usability and design aspects, was discussed in Chapter 6 and Chapter 7. The qualitative results of the post-test questionnaire were used to assess the overall level of user satisfaction which was very high, as 98% of the participants supported the idea of the new scheme.

Chapter 6 and 7 managed to answer the following question:

- Would end users find the new scheme acceptably usable and capable of protecting their accounts?

8.2. Research limitations

The thesis has reported some research/approach limitations as enumerated below.

- Users with certain sight disabilities are out of the scope of this study, as it is mainly based on visual elements, which is considered to be an approach limitation.

- The use of the unlock pattern technique may add a practical constraint to this approach, due to the fact that it has been patented by Google.

- The difficulty of hiring expert testers to undertake the security attacks on the proposed system led to the task being carried out by ordinary participants.

  To mitigate this obstacle, the empirical security evaluations were designed to be simple that help non-expert participants to break into the system. In other words, the experiments did not require any hacking skills or specific tools.

- The recording of the activity logs for the GOTPass input format in particular, was not as effective as expected. The details of the input format selection made by the user were not recorded sufficiently, and thus no further analysis was possible. In a typical case, each part of the entered code (four-digits) should be logged first and then checked to ensure it matches any of the displayed codes on the edges of the challenge grid. That, in turn, would also allow the identification of the combination option of the GOTPass input format. If no match was found, that would mean that the entered codes were mistyped.

  Although this point has imposed some data analysis limitations, it apparently has no significant impact on the main findings of the research. However, implementing this modification would result in better outcomes for more accurate analysis.

In spite of the limitations described above, the work is still considered to be valid, as shown in the results of the evaluations in the earlier chapters.

8.3. Future work

The thesis has contributed to the literature of usable security in general and graphical passwords in particular. However, during the work of this thesis, new research directions have also arisen. This section highlights a number of potential future research opportunities.

8.3.1. GOTPass design improvements

Depending on the desirable balance of security and usability for users or organisations, there are several ways in which the GOTPass scheme could be further modified to provide various improvements (i.e. a number of design alterations are possible to boost either side of the system, namely security or usability, after examining their viability). Some suggestions are outlined below:

- Further investigation into combining several graphical password categories (i.e. recognition, draw, and click) is suggested. This could be achieved by adding one more system-assigned image to the GOTPass challenge and requesting the user to create click points on the image. In the login phase, during image selection step, the system will display two random pass-images, as usual, as well as the click-based image. Users will then need to click on the image's secret points, then identify their pass-images, and finally, enter the corresponding GOTPass codes.

- Assigning the GOTPass input format (final registration step) automatically by the system might be worthy of exploration. This aims to bring several benefits to the system, such as reducing the registration time and, more importantly, reducing the impact of the process of partially assigning the input format. During the post-test questionnaire, this was rated by the users as having a high impact on causing recall difficulty.

- There is also the opportunity to increase the number of code options. Currently, only two edges are utilised (top and left), but this could be extended to use the four edges surrounding the challenge grid (top, bottom, right, and left). This, in turn, should increase the password space and, therefore, the system security; however, the usability (memorability) of the system might be affected, and this should be carefully examined.

- Attempting to improve the registration and authentication times of the current GOTPass design is an essential step. Removing several unnecessary clicks in the current design, such as moving directly to the next step immediately after the pen-up at the end of the pattern drawing in both phases the registration and authentication should be effective. Also eliminating the confirmation screens in the registration phase should significantly reduce the time spent creating a password.

- Studying the feasibility of other interface designs. This research was established using a single interface design. Therefore, a variety of other interface designs could be investigated taking into account the possible effect on security and usability. For example, the impact of the dynamic display layout (i.e. 4×4, 6×6, 8×8) could be investigated, which can increase the password space and complicate the task for the attackers, since different users may have different-sized grids which adds an additional step in front of the attackers, who need to discover further information to undertake a successful attack.

- Another interesting design improvement can be through offering different system configurations related to the generated OTP, such as the use of numeric/ alphabetic/ alphanumeric codes and the length of the password (4, 8 or 12 characters long).

- Merging the unlock pattern and the image-recognition panels into one embedded screen can be a significant design enhancement that can enable the system to work with different platforms, such as a smartphone. In other words, the unlock pattern screen should be superimposed over the image-based screen.

- By adopting the modified design described in the additional security experiment (Chapter seven – 7.10) which showed positive results, it might be worth investigating the optional deployment of GOTPass scheme without the unlock pattern step or even replace it by some other frontline approaches in cases where the multi-step technique is less important. That should reduce the time taken for login, however the security of the system should be ensured and not to be affected by this modification.

8.3.2. Security improvements

- Instead of implementing a distractor-images portfolio for each pass-image, implementing it based on a user's account would confuse the attacker, meaning that the attacker would be unable to determine the correct pass-images. In this way, each account will have a distractor-images portfolio that should appear each time the user tries to login. For example, for each login attempt there should be 14 distractor-images derived from the account's portfolio of distractors, which is typically a slightly larger set of distractor-images.

- Another interesting variation of the proposed solution can be the implementation of an Out-of-Band technique. In this version, the user does not need to select the input format during the enrolment phase, but instead it will be sent to the registered mobile number or email address of the user, prompting them to enter one of the available input format options – for instance, the code of the 1st pass-image from the top axis & the code of the 2nd pass-image from the left-hand axis.

Adopting such a technique would have advantages for security as well as usability, since it eliminates the final step of the registration process. As a result, users will need to remember less information related to their credentials. On the other hand, one drawback of such a system would be the dependency on devices (mobile phone) and service providers (network operation), unless the email option is used instead.

- The impact of the image and code ordering on the security and usability of the GOTPass scheme is another aspect that needs further investigation.

- Investigate the security impact of adding a new system attribute that allows the GOTPass codes to be entered in different pre-determined directions. In other words, the codes can be entered in two ways (forward ordering – left to right or backward ordering – right to left), aiming to further complicate the attacker.

- Study the feasibility of utilising the background colour feature to make it easier for users to spot their pass-images and the likelihood of increasing the password space of the system.

8.3.3. General improvements

- Enlarging the sample of participants and running the user study for an extended period of time are suggestions that will allow a more conclusive analysis of the data.

- One of the recommendations of this research is to arrange to conduct a field study in an actual environment where the proposed scheme can constitute part of the security requirements in that organisation. That should help to gather more representative results and feedback for further assessment and enhancement.

- It is also suggested to investigate the compatibility and effectiveness of the current design on different platforms, especially handheld devices.

- Examining the memory interference of multiple GOTPass passwords is one of the factors that may affect the future deployment of this scheme.

- Enhance the recording of the experimental data to include the input data (any typed-in data) and the pass-images on that row or column, if possible, for better analysis and to enable a more precise investigation towards the cause of the failed attempts, which also lead to an automated way to identify the coincident successful attempt.

8.4. Discussion

Although GOTPass scheme has been demonstrated to be a valid secure/usable alternative authentication system; but, nonetheless, it has not been given the chance to be evaluated and examined in a critical environment such as online banking. Preliminary evaluations findings from the evaluations presented in chapter 6 and 7 showed that the GOTPass scheme would need further usability and security improvements to suit sensitive systems. For instance, the usability assessment in (Chapter six – 6.4.2) indicated that only 40% of the users completed the authentication tasks without error and the time consumption nature of the mechanism was reasonably high; both aspects would not be sufficient enough for such systems. From the security prospective, the assessment in (Chapter seven – 7.8) showed that successful break-in rate was (3.3%) which is deemed high specially for financial systems. In addition, the conducted experiment to evaluate the user perception of this new technique was not ecologically valid because participants were not asked to access a system they cared about or await a certain service in return such as authenticating for the purpose of accessing module materials, timetables or marks. In regards to the prototype design, the images used in this prototype might be suboptimal

because of the similarity between some of them which was due to the difficulty of acquiring suitable images for the authentication purposes.

8.5. Final words

GOTPass has received a positive media coverage that was started by the Press Office of Plymouth University, where an interview was held at the Centre for Security, Communications and Network Research. The media & communications officer (Mr Alan Williams) led the interview, where he was explained, in detail, how the GOTPass system works and then discussed some of the research outcomes (Williams, 2015). Following the press release, the coverage has expanded to reach several types of media*. In addition, the GOTPass system has been overwhelmed by the techrepublic.com report that included GOTPass in "10 of the latest security products that can help you fight the bad guys" (Forrest, 2016). However, despite the encouragement triggered by the media interest, overall, the message does not claim that GOTPass is the best solution.

Efforts to find alternative authentication mechanisms for electronic banking are continuing. Recently, some financial services providers, such as HSBC and First Direct, are investing in using voice and fingerprint biometrics as part of their mobile banking systems. The launch of these biometrics aims to make accessing bank accounts even quicker and easier for customers (HSBC News and Media, 2016). However, such technology would only be available for some customers, since it is only enabled on mobile banking apps with touch ID on Apple devices, which limits the expected wide/universal use of the services.

---

*
http://www.eurekalert.org/pub_releases/2015-12/uop-iac122215.php
www.techrepublic.com/article/good-bye-weak-passwords-hello-gotpass-graphical-authentication/
https://twitter.com/search?&q=GOTPass
https://www.youtube.com/watch?v=s37_H7y1nAc

Furthermore, MasterCard has announced that online payments would accept selfies and fingerprints to authenticate customers instead of passwords and codes. A specific app needs to be installed on the customer's PC, tablet or smartphone. The verification of the customer's identity will take place whenever further authentication is required, by looking at the phone's camera or using the fingerprint sensor of the phone. While taking the selfie, the user will be asked to blink into the camera, to ensure that the presented user is a real and not a photo (Kennedy, 2016). The use of such integrated biometrics on user's devices for authentication is tying down the authentication to the mobile device which, for some users, can be considered a downside of such a mechanism. However, this type of news shows that the authentication trend of online financial services is not confined to hardware tokens or similar, but it is appealing to other alternative authentication mechanisms that can not only provide security but are also usable. Therefore, utilising a diverse range of techniques within such critical systems motivates the research domain of graphical authentication to find its respected position within the field of secure authentication technology.

References

Adams, A. & Sasse, M. A. (1999). 'USERS ARE NOT THE ENEMY'. *Communications of the ACM*, 42 (12). pp 40-46.

Akula, S. & Devisetty, V. (2004). 'Image based registration and authentication system', *Proceedings of Midwest Instruction and Computing Symposium*.

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S. & Reich, C. (2015). 'The Current Use of Authentication Technologies: An Investigative Review', *Proceedings of the IEEE 2015 International Conference on Cloud Computing (ICCC15)*. Riyadh, Saudi Arabia, pp. 239-246.

Alexander, C. (2008). 'Two Factor Authentication That Doesn't Use Chips'. *Card Technology Today*, 20 (5). pp 9.

Anderson, J. R. & Bower, G. H. (1972). 'Recognition and retrieval processes in free recall'. *Psychological Review*, 79 (2). pp 97.

Anderson, R. J. (2010a). 'Access Control'. *Security Engineering: A guide to building dependable distributed systems*. 2nd edn.: Wiley, 4, pp 93-127.

Anderson, R. J. (2010b). 'Usability and Psychology'. *Security Engineering: A guide to building dependable distributed systems*. 2nd edn.: Wiley, 2, pp 17-61.

Andriotis, P., Tryfonas, T. & Oikonomou, G. (2014). 'Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method', *Human Aspects of Information Security, Privacy, and Trust*. Springer, pp. 115-126.

Andriotis, P., Tryfonas, T., Oikonomou, G. & Yildiz, C. (2013). 'A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks', *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, pp. 1-6.

AuthenticationWorld.com (2012). 'Password Authentication'. [Online]. Available at: http://authenticationworld.com/Password-Authentication/index.html (Accessed: Feb 2015).

AuthShield (2015). 'AuthShield One Click'. [Online]. Available at: http://auth-shield.com/one-click/ (Accessed: March 2016).

Aviv, A. J., Gibson, K., Mossop, E., Blaze, M. & Smith, J. M. (2010). 'Smudge Attacks on Smartphone Touch Screens'. *The 4th USENIX Workshop on Offensive Technologies (WOOT'10).* pp 1-7.

Balfanz, D., Chow, R., Eisen, O., Jakobsson, M., Kirsch, S., Matsumoto, S., Molina, J. & van Oorschot, P. (2012). 'The Future of Authentication'. *IEEE symposium on Security & Privacy*, 10 (1). pp 22-27.

Bangor, A., Kortum, P. T. & Miller, J. T. (2008). 'An Empirical Evaluation of the System Usability Scale'. *Intl. Journal of Human–Computer Interaction*, 24 (6). pp 574-594.

BBC (2016). 'MWC 2016: Clay digit fools smartphone fingerprint sensors'. [Online]. Available at: http://www.bbc.co.uk/news/technology-35642747 (Accessed: March 2016).

Beautement, A. & Sasse, A. (2010). 'Gathering Realistic Authentication Performance Data Through Field Trials', *The sixth Symposium On Usability Privacy and Security (SOUPS)*. Redmond, WA, USA.

Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H. & Bhogle, P. (2015). 'Comparison of Graphical Password Authentication Techniques'. *International Journal of Computer Applications*, 116 (1). pp 11-14.

Bianchi, A., Oakley, I. & Kwon, D.-S. (2011). 'Obfuscating authentication through haptics, sound and light'. *CHI '11 Extended Abstracts on Human Factors in Computing Systems*. Vancouver, BC, Canada: ACM. pp 1105-1110.

Bicakci, K., Atalay, N. B., Yuceel, M., Gurbaslar, H. & Erdeniz, B. (2009). 'Towards Usable Solutions to Graphical Password Hotspot Problem', *Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, COMPSAC'09*. pp 318-323.

Biddle, R., Chiasson, S. & Van Oorschot, P. (2012). 'Graphical Passwords: Learning From the First Twelve Years'. *ACM Computing Surveys (CSUR)*, 44 (4). pp 1-41.

Biddle, R., Chiasson, S. & Van Oorschot, P. C. (2009). 'Graphical Passwords: Learning from the First Generation'. *Technical report TR-09-09,* School of Computer Science, Carleton University. Available at: https://www.scs.carleton.ca/sites/default/files/tr/TR-09-09.pdf (Accessed: March 2016).

Birget, J. C., Dawei, H. & Memon, N. (2006). 'Graphical Passwords Based on Robust Discretization'. *IEEE Transactions on Information Forensics and Security,* 1 (3). pp 395-399.

Birget, J. C., Hong, D. & Memon, N. (2003). 'Robust discretization, with an application to graphical passwords'. *Cryptology ePrint Archive: Report 2003/168*. Available at: https://eprint.iacr.org/2003/168 (Accessed: March 2016).

Blair, S. (2007). 'Gris expectations'. *Engineering & Technology*, 2 (12). pp 28-29.

Blonder, G. E. (1996). *'Graphical password'*. US5559961A. Available at: http://www.google.co.uk/patents/US5559961

Bond, M. (2008). *'Comments on GrIDsure Authentication'*. Available at: http://www.cl.cam.ac.uk/~mkb23/research/GridsureComments.pdf (Accessed: March 2016).

Bonneau, J., Herley, C., Van Oorschot, P. C. & Stajano, F. (2012). 'The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes', *2012 IEEE Symposium on Security and Privacy (SP)*, pp 553-567.

Borgohain, T., Borgohain, A., Kumar, U. & Sanyal, S. (2015). 'Authentication Systems in Internet of Things'. *International Journal of Advanced Networking and Applications*, 6 (4). pp 2422-2426.

Braz, C. & Robert, J.-M. (2006). 'Security and usability: the case of the user authentication methods'. *Proceedings of the 18th Conference on l'Interaction Homme-Machine*. Montreal, Canada: ACM, pp 199-203.

Brooke, J. (1996). 'SUS - A Quick and Dirty Usability Scale'. *Usability evaluation in industry*. London: Taylor & Francis, pp 189-194.

Brostoff, S., Inglesant, P. & Sasse, M. A. (2010). 'Evaluating the Usability and Security of a Graphical One-Time PIN System'. *Proceedings of the 24th BCS Interaction Specialist Group Conference*. Dundee, UK: British Computer Society, pp 88-97.

Brostoff, S. & Sasse, M. A. (2000) 'Are Passfaces More Usable Than Passwords? A Field Trial Investigation'. in McDonald, S., Waern, Y. and Cockton, G. (eds.) *People and Computers XIV — Usability or Else!: Proceedings of HCI 2000.* London: Springer London, pp 405-424.

Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S. & Nabbus, E. A. (2013). 'Electronic Authentication Guideline—NIST Special Publication 800-63-2'. *US Department of Commerce, National Institute of Standards and Technology*.

Catuogno, L. & Galdi, C. (2014). 'Analysis of a two-factor graphical password scheme'. *International Journal of Information Security*, 13 (5). pp 421-437.

Chakrabarti, S., Landon, G. V. & Singhal, M. (2007). 'Graphical Passwords: Drawing a Secret with Rotation as a New Degree of Freedom', *The Fourth IASTED Asian Conference on Communication Systems and Networks (AsiaCSN 2007)*.

Bicakci, K., Atalay, N. B., Yuceel, M., Gurbaslar, H. & Erdeniz, B. (2009). 'Towards Usable Solutions to Graphical Password Hotspot Problem', *Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, COMPSAC'09*. pp 318-323.

Biddle, R., Chiasson, S. & Van Oorschot, P. (2012). 'Graphical Passwords: Learning From the First Twelve Years'. *ACM Computing Surveys (CSUR)*, 44 (4). pp 1-41.

Biddle, R., Chiasson, S. & Van Oorschot, P. C. (2009). 'Graphical Passwords: Learning from the First Generation'. *Technical report TR-09-09,* School of Computer Science, Carleton University. Available at: https://www.scs.carleton.ca/sites/default/files/tr/TR-09-09.pdf (Accessed: March 2016).

Birget, J. C., Dawei, H. & Memon, N. (2006). 'Graphical Passwords Based on Robust Discretization'. *IEEE Transactions on Information Forensics and Security,* 1 (3). pp 395-399.

Birget, J. C., Hong, D. & Memon, N. (2003). 'Robust discretization, with an application to graphical passwords'. *Cryptology ePrint Archive: Report 2003/168*. Available at: https://eprint.iacr.org/2003/168 (Accessed: March 2016).

Blair, S. (2007). 'Gris expectations'. *Engineering & Technology*, 2 (12). pp 28-29.

Blonder, G. E. (1996). *'Graphical password'*. US5559961A. Available at: http://www.google.co.uk/patents/US5559961

Bond, M. (2008). *'Comments on GrIDsure Authentication'*. Available at: http://www.cl.cam.ac.uk/~mkb23/research/GridsureComments.pdf (Accessed: March 2016).

Bonneau, J., Herley, C., Van Oorschot, P. C. & Stajano, F. (2012). 'The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes', *2012 IEEE Symposium on Security and Privacy (SP)*, pp 553-567.

Borgohain, T., Borgohain, A., Kumar, U. & Sanyal, S. (2015). 'Authentication Systems in Internet of Things'. *International Journal of Advanced Networking and Applications*, 6 (4). pp 2422-2426.

Braz, C. & Robert, J.-M. (2006). 'Security and usability: the case of the user authentication methods'. *Proceedings of the 18th Conference on l'Interaction Homme-Machine*. Montreal, Canada: ACM, pp 199-203.

Brooke, J. (1996). 'SUS - A Quick and Dirty Usability Scale'. *Usability evaluation in industry*. London: Taylor & Francis, pp 189-194.

Brostoff, S., Inglesant, P. & Sasse, M. A. (2010). 'Evaluating the Usability and Security of a Graphical One-Time PIN System'. *Proceedings of the 24th BCS Interaction Specialist Group Conference*. Dundee, UK: British Computer Society, pp 88-97.

Brostoff, S. & Sasse, M. A. (2000) 'Are Passfaces More Usable Than Passwords? A Field Trial Investigation'. in McDonald, S., Waern, Y. and Cockton, G. (eds.) *People and Computers XIV — Usability or Else!: Proceedings of HCI 2000.* London: Springer London, pp 405-424.

Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S. & Nabbus, E. A. (2013). 'Electronic Authentication Guideline—NIST Special Publication 800-63-2'. *US Department of Commerce, National Institute of Standards and Technology*.

Catuogno, L. & Galdi, C. (2014). 'Analysis of a two-factor graphical password scheme'. *International Journal of Information Security*, 13 (5). pp 421-437.

Chakrabarti, S., Landon, G. V. & Singhal, M. (2007). 'Graphical Passwords: Drawing a Secret with Rotation as a New Degree of Freedom', *The Fourth IASTED Asian Conference on Communication Systems and Networks (AsiaCSN 2007)*.

Chakrabarti, S. & Singbal, M. (2007) 'Password-Based Authentication: Preventing Dictionary Attacks'. *Computer*, 40 (6). pp 68-74.

Chalkias, K., Alexiadis, A. & Stephanides, G. (2006). 'A Multi-Grid Graphical Password Scheme'. *Proceedings of the 6th International Conference on Artificial Intelligence and Digital Communications (AIDC)*. Thessaloniki, Greece. pp 80-90.

Charruau, D. (2004). '*Assessing the Viability of Alternative Authentication Methods'*. MSc Thesis. University of Plymouth.

Charruau, D., Furnell, S. & Dowland, P. (2005). 'PassImages: An Alternative Method of User Authentication'. *Proceedings of the 4th Annual ISOneWorld Conference and Convention*. Las Vegas, USA.

Chiang, H.-Y. & Chiasson, S. (2013). 'Improving User Authentication on Mobile Devices: A Touchscreen Graphical Password', *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*. ACM, pp. 251-260.

Chiasson, S., Biddle, R. & van Oorschot, P. C. (2007). 'A second look at the usability of click-based graphical passwords'. *Proceedings of the 3rd symposium on Usable privacy and security SOUPS'07*. Pittsburgh, USA. ACM, pp 1-12.

Chiasson, S., Forget, A., Biddle, R. & van Oorschot, P. C. (2008). 'Influencing Users Towards Better Passwords: Persuasive Cued Click-Points'. *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction BCS-HCI'08*. Liverpool, UK. British Computer Society, pp 121-130.

Chiasson, S., van Oorschot, P. C. & Biddle, R. (2007). 'Graphical Password Authentication Using Cued Click Points'. In: Biskup, J. and López, J. (eds.), *Computer Security – ESORICS 2007: 12th European Symposium On Research In Computer Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp 359-374.

Citty, J. & Hutchings, D. R. (2010). *TAPI: Touch-screen Authentication using Partitioned Images*. Elon University Technical Report 2010-1. Available at: http://facstaff.elon.edu/dhutchings/papers/citty2010tapi.pdf.

ConfidentTech (2012). 'One-Time Passwords Using Images'. [Online]. Available at: http://www.confidenttechnologies.com/content/when-passwords-arent-enough (Accessed: March 2016).

Crawford, H., Renaud, K. & Storer, T. (2013). 'A framework for continuous, transparent mobile device authentication'. *Computers & Security*, 39, Part B pp 127-136.

CRYPTOCard Inc (2010a). 'Cryptocard Acquires GrIDsure Tokenless Authentication IP'. [Online]. Available at: http://www.safenet-inc.com/news/2012/cryptocard-acquires-GrIDsure-tokenless-authentication-IP/ (Accessed: March 2016).

CRYPTOCard Inc (2010b). 'GrIDsure Token Guide for BlackShield ID'. [Online]. Available at: http://www2.safenet-inc.com/cryptocard/implementation-guides/Tokens/GrIDsure%20Token%20Guide.pdf (Accessed: March 2016).

Davis, D., Monrose, F. & Reiter, M. K. (2004). 'On User Choice in Graphical Password Schemes'. *Proceedings of the 13th USENIX Security Symposium*. San Diego, pp 151-164.

De Angeli, A., Coutts, M., Coventry, L., Johnson, G. I., Cameron, D. & Fischer, M. H. (2002). 'VIP: A Visual Approach to User Authentication'. *Proceedings of the Working Conference on Advanced Visual Interfaces AVI'02*. Trento, Italy. ACM, pp 316-323.

De Angeli, A., Coventry, L., Johnson, G. & Coutts, M. (2003). 'Usability and user authentication: Pictorial passwords vs. pin'. In: Paul T. McCabe (ed.), *Contemporary Ergonomics 2003*. London: Taylor & Francis, pp 240-245.

De Angeli, A., Coventry, L., Johnson, G. & Renaud, K. (2005). 'Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems'. *International Journal of Human-Computer Studies*, 63 (1–2). pp 128-152.

Deshmukh, S. & Devale P. R. (2013). 'Implementation of an Efficient Mechanism for Secure Authentication'. *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)*, 3 (5). pp 103-112.

Devlin, M., Nurse, J. C., Hodges, D., Goldsmith, M. & Creese, S. (2015). 'Predicting Graphical Passwords'. In: Tryfonas, T. and Askoxylakis, I. (eds.), *Human Aspects of Information Security, Privacy, and Trust.* Los Angeles, USA: Springer International Publishing, pp 23-35.

Dhamija, R. & Perrig, A. (2000). 'Déjà vu: A User Study Using Images for Authentication', *Proceedings of the 9th Conference on USENIX Security Symposium.* (9), pp 45-58.

Dimitropoulos, L. K. (2011). '*GrIDsure: Effects of background images on pattern choice, usability and memorability*'. MSc Thesis. University College London.

Dube, D. & Gulati, V. P. (2005). 'Information System Audit and Assurance'. New Delhi: Tata McGraw-Hill Education, pp 594-608.

Dunphy, P., Fitch, A. & Olivier, P. (2008). 'Gaze-contingent passwords at the ATM'. *Proceedings of the 4th Conference on Communication by Gaze Interaction (COGAIN)*. Prague, Czech Republic. pp 59-62.

Dunphy, P., Heiner, A. P. & Asokan, N. (2010). 'A Closer Look at Recognition-based Graphical Passwords on Mobile Devices'. *Proceedings of the Sixth Symposium on Usable Privacy and Security SOUPS'10*. Redmond, USA: ACM, pp 1-12.

Dunphy, P., Nicholson, J. & Olivier, P. (2008). 'Securing Passfaces for Description'. *Proceedings of the 4th symposium on Usable privacy and security SOUPS'08*. Pittsburgh, USA: ACM, pp 24-35.

Dunphy, P. & Yan, J. (2007). 'Do Background Images Improve "Draw A Secret" Graphical Passwords?'. *Proceedings of the 14th ACM conference on Computer and communications security CCS'07*. Alexandria, Virginia, USA: ACM, pp 36-47.

Elftmann, P. (2006). 'Secure Alternatives to Password-based Authentication Mechanisms'. Diploma Thesis. *Laboratory for Dependable Distributed Systems, RWTH Aachen University*.

EMC (2015). 'RSA SecurID Software Tokens Data Sheet'. [Online]. Available at: http://www.emc.com/collateral/data-sheet/h13819-ds-rsa-securid-software-tokens.pdf (Accessed: March 2016).

ENCAP (2012). 'Securing Enterprise Applications in the Post-PC era'. [Online]. Available at: https://www.encapsecurity.com/encap-launches-white-paper-on-enterprise-authentication-in-the-post-pc-era/ (Accessed: Feb 2013).

English, R. & Poet, R. (2011a). 'Measuring the Revised Guessability of Graphical Passwords'. *5th International Conference on Network and System Security (NSS)*. Milan: IEEE, pp 364-368.

English, R. & Poet, R. (2011b). 'Towards a metric for recognition-based graphical password security'. *5th International Conference on Network and System Security (NSS)*. Milan: IEEE, pp 239-243.

English, R. & Poet, R. (2012). 'The Effectiveness of Intersection Attack Countermeasures for Graphical Passwords'. *11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. Liverpool: IEEE, pp 1-8.

European Central Bank "ECB" (2013). 'RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS'. [Online]. Available at: https://www.ecb.europa.eu/ (Accessed: March 2016).

Everitt, K. M., Bragin, T., Fogarty, J. & Kohno, T. (2009). 'A Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords'. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems CHI'09*. Boston, USA: ACM, pp 889-898.

Federal Financial Institutions Examination Council 'FFIEC' (2001). 'Authentication in an Internet Banking Environment'. [Online]. Available at: https://www.ffiec.gov/pdf/authentication_guidance.pdf (Accessed: March 2016).

Federal Financial Institutions Examination Council 'FFIEC' (2003). 'FFIEC E-Banking Booklet'. [Online]. Available at: http://www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/GroupDocuments/e_banking.pdf (Accessed: March 2016).

Federal Financial Institutions Examination Council 'FFIEC' (2006). 'IT Examination Handbook: information security Booklet'. *USA: FFIEC Publishers.*

Florêncio, D., Herley, C. & Coskun, B. (2007). 'Do Strong Web Passwords Accomplish Anything?'. *Proceedings of the 2nd USENIX workshop on Hot Topics in Security HotSec'07*, pp 1-6.

Forrest, C. (2016). '10 of the latest security products that can help you fight the bad guys'. [Online]. Available at: http://www.techrepublic.com/pictures/10-of-the-latest-security-products-that-can-help-you-fight-the-bad-guys/2/?ftag=TRE684d531&bhid=23139800868270451999291043424733 (Accessed: March 2016).

Fu, K., Sit, E., Smith, K. & Feamster, N. (2001). 'Dos and Don'ts of Client Authentication on The Web', *Proceedings of the 10th USENIX Security Symposium*. Washington, USA: USENIX Association, pp 251-268.

Furnell, S. (2005). 'Authenticating Ourselves: Will We Ever Escape the Password?'. *Network Security*, 2005 (3). pp 8-13.

Furnell, S. & Zekri, L. (2006). 'Replacing Passwords: In Search of the Secret Remedy'. *Network Security*, 2006 (1). pp 4-8.

Gani, A. (2010). 'A New Algorithm on Graphical User Authentication (GUA) based on Multi-Line Grids'. *Scientific Research and Essays*, 5 (4). pp 3865-3875.

Gao, H., Jia, W., Ye, F. & Ma, L. (2013). 'A Survey on the Use of Graphical Passwords in Security'. *Journal of Software*, 8 (7). pp 1678-1698.

Gao, H., Liu, X., Dai, R., Wang, S. & Chang, X. (2009a). 'Analysis and Evaluation of the ColorLogin Graphical Password Scheme', *Fifth International Conference on Image and Graphics, ICIG'09.* Xi'an, China: IEEE, pp 722-727.

Gao, H., Liu, X., Wang, S. & Dai, R. (2009b). 'A New Graphical Password Scheme Against Spyware by Using CAPTCHA'. *Proceedings of the 5th symposium on Usable Privacy and Security SOUPS'09*. Mountain View, USA: ACM.

Gao, H., Liu, X., Wang, S., Liu, H. & Dai, R. (2009c). 'Design and Analysis of a Graphical Password Scheme'. *Fourth International Conference on Innovative Computing, Information and Control (ICICIC)*. Kaohsiung, Taiwan: IEEE, pp 675-678.

Gao, H., Ren, Z., Chang, X., Liu, X. & U., A. (2010). 'A New Graphical Password Scheme Resistant to Shoulder-Surfing', *International Conference on Cyberworlds (CW)*. Singapore: IEEE, pp 194-199.

Gemalto (2015). 'BREACH LEVEL INDEX—First Half Review'. [Online]. Available at: http://breachlevelindex.com/pdf/Breach-Level-Index-Report-H12015.pdf (Accessed: March 2016).

Gibson, R. (2011). 'BIOMETRIC ACCESS CONTROL SYSTEMS'. [Online]. Available at: http://iwatchsystems.com/technical/2011/03/03/biometric-access-control-systems/ (Accessed: March 2016).

Goldberg, J., Hagman, J. & Sazawal, V. (2002). 'Doodling our way to better authentication'. *Proceedings of CHI'02 Extended Abstracts on Human Factors in Computing Systems*. Minneapolis, USA: ACM, pp 868-869.

Golle, P. & Wagner, D. (2007). 'Cryptanalysis of a Cognitive Authentication Scheme (Extended Abstract)', *IEEE Symposium on Security and Privacy (SP'07)*. Berkeley: IEEE, pp 66-70.

Goode, A. (2014). 'Bring your own finger–how mobile is bringing biometrics to consumers'. *Biometric Technology Today*, 2014 (5). pp 5-9.

Google (2015). '2-Step Verification – Google Authenticator'. [Online]. Available at: https://www.google.com/intl/en/landing/2step/ (Accessed: March 2016).

Gołofit, K. (2007). 'Picture Passwords Superiority and Picture Passwords Dictionary Attacks'. *Proceedings of the International Multiconference on Computer Science and Information Technology*. pp 681-690.

Gordon, S. (2005). 'Fighting Spyware and Adware in the Enterprise'. *Information systems security*, 14 (3). pp 14-17.

Grand, J. (2001). 'Authentication tokens: balancing the security risks with business requirements'. [Online]. Available at: http://grandideastudio.com/wp-content/uploads/authentokens_paper.pdf (Accessed: March 2016).

Gupta, S., Sabbu, P., Varma, S. & Gangashetty, S. V. (2011). 'Passblot: A Usable Way of Authentication Scheme to Generate One Time Passwords'. In: Wyld, D.C., Wozniak, M., Chaki, N., Meghanathan, N. and Nagamalai, D. (eds.), *Advances in Network Security and Applications.* Springer Berlin Heidelberg, pp 374-382.

Gupta, S., Sahni, S., Sabbu, P., Varma, S. & Gangashetty, S. V. (2012). 'Passblot: A Highly Scalable Graphical one Time Password System'. *International Journal of Network Security & Its Applications (IJNSA)*, 4 (2). pp 201-216.

Gyorffy, J. C., Tappenden, A. F. & Miller, J. (2011). 'Token-based Graphical Password Authentication'. *International Journal of Information Security*, pp 1-16.

Haichang, G., Xiyang, L., Ruyi, D., Sidong, W. & Xiuling, C. (2009). 'Analysis and Evaluation of the ColorLogin Graphical Password Scheme'. *Fifth International Conference on Image and Graphics, ICIG'09.* Xi'an, China: IEEE, pp 722-727.

Haichang, G., Xuewu, G., Xiaoping, C., Liming, W. & Xiyang, L. (2008). 'YAGP: Yet Another Graphical Password Strategy'. *Annual Computer Security Applications Conference, ACSAC 2008.* Anaheim, USA: IEEE, pp 121-129.

Herley, C. & Van Oorschot, P. (2012). 'A Research Agenda Acknowledging the Persistence of Passwords'. *IEEE Security & Privacy,* 10 (1). pp 28-36.

Hochheiser, H., Feng, J. & Lazar, J. (2008). 'Challenges in universally usable privacy and security'. *Symposium On Accessible Privacy and Security (SOAPS'08)*. Pittsburgh, USA.

Hollingworth, H. L. (1913). 'Characteristic Differences between Recall and Recognition'. *The American Journal of Psychology*, 24 (4). pp 532-544.

Home Office and The Rt Hon Theresa May MP (2014). 'Mobile phone theft paper highlights models targeted by thieves'. [Online]. Available at: https://www.gov.uk/government/news/mobile-phone-theft-paper-highlights-models-targeted-by-thieves (Accessed: March 2016).

Hong, D., Man, S., Hawes, B. & Mathews, M. (2004). 'A graphical password scheme strongly resistant to spyware', *Proceedings of the International conference on security and management.* Las Vergas, USA: CSREA Press, pp 94-100.

HSBC News and Media (2016). 'HSBC and first direct bring biometric banking to the mainstream'. [Online]. Available at: http://www.about.hsbc.co.uk/~/media/uk/en/news-and-media/rbwm/160219-first-direct-and-hsbc-bring-biometric-banking-to-the-mainstream.pdf (Accessed: March 2016).

IBM Support (2010). 'Transforming different Likert scales to a common scale'. [Online]. Available at: http://www-01.ibm.com/support/docview.wss?uid=swg21482329 (Accessed: March 2016).

International Organization for Standardization—ISO 9241-11 (1998). 'Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) — Part 11: Guidance on Usability'.

Jain, A., Ross, A. A. & Nandakumar, K. (2011). *Introduction to biometrics.* New York, USA: Springer Science & Business Media.

Jain, A. K., Ross, A. & Prabhakar, S. (2004). 'An introduction to biometric recognition'. *IEEE Transactions on Circuits and Systems for Video Technology*, 14 (1). pp 4-20.

Jali, M. Z. (2011). *'A Study of Graphical Alternatives for User Authentication'*. PhD Thesis. Plymouth University.

Jali, M. Z., Furnell, S. M. & Dowland, P. S. (2011). 'Multifactor Graphical Passwords: An Assessment of End-User Performance'. *7th International Conference on Information Assurance and Security (IAS)*. Melaka, Malaysia: IEEE, pp 7-12.

Jansen, W. A., Gavrila, S., Korolev, V., Ayers, R. & Swanstrom, R. (2003). 'Picture Password: A Visual Login Technique for Mobile Devices—NISTIR 7030'. *US Department of Commerce, National Institute of Standards and Technology*. Available at: http://csrc.nist.gov/publications/nistir/nistir-7030.pdf.

Jebriel, S. & Poet, R. (2011). 'Preventing shoulder-surfing when selecting pass-images in challenge set'. *International Conference on Innovations in Information Technology (IIT)*. Abu Dhabi, UAE: IEEE, pp 437-442.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K. & Rubin, A. D. (1999). 'The design and analysis of graphical passwords'. *Proceedings of the 8th USENIX Security Symposium*. Washington, USA, pp 1-14.

Jhawar, R., Inglesant, P., Courtois, N. & Sasse, M. A. (2011). 'Make mine a quadruple: Strengthening the security of graphical one-time pin authentication'. *5th International Conference on Network and System Security (NSS)*. Milan, Italy: IEEE, pp 81-88.

Just, M. & Aspinall, D. (2012). 'On the Security and Usability of Dual Credential Authentication in UK Online Banking'. *International Conference for Internet Technology And Secured Transactions*. London, UK: IEEE, pp 259-264.

Kennedy, J. (2016). 'MasterCard will soon accept selfies to process online payments'. [Online]. Available at: www.siliconrepublic.com/gear/2016/02/23/mastercard-selfies-mwc-16 (Accessed: March 2016).

Kessler, G. C. (1996). 'Passwords—strengths and weaknesses'. [Online]. Available at: http://www.garykessler.net/library/password.html Accessed: October 2016).

Khot, R. A., Kumaraguru, P. & Srinathan, K. (2012). 'WYSWYE: shoulder surfing defense for recognition based graphical passwords'. *Proceedings of the 24th Australian Computer-Human Interaction Conference*. Melbourne, Australia: ACM, pp 285-294.

Komanduri, S. & Hutchings, D. R. (2008). 'Order and Entropy in Picture Passwords'. *Proceedings of Graphics Interface 2008*. Ontario, Canada: Canadian Information Processing Society, pp 115-122.

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H. & Kim, J.-H. (2012). 'Extended OTP Mechanism Based on Graphical Password Method'. In: J. Park, J., Leung, C.M.V., Wang, C.-L. and Shon, T. (eds.), *Future Information Technology, Application, and Service: FutureTech 2012 Volume 1*. Dordrecht: Springer Netherlands, pp 203-212.

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H. & Kim, J.-H. (2013). 'Two-factor Authentication System Based on Extended OTP Mechanism'. *International Journal of Computer Mathematics*, 90 (12). pp 2515-2529.

Kuseler, T. & Lami, I. A. (2012). 'Using Geographical Location as an Authentication Factor to Enhance mCommerce Applications on Smartphones'. *International Journal of Computer Science and Security (IJCSS)*, 6 (4). pp 277-287.

Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O. & Saleh, D. (2009). 'Shoulder Surfing Attack in Graphical Password Authentication'. *International Journal of Computer Science and Information Security (IJCSIS)*, 6 (2). pp 145-154.

Levy, C. (2011). 'Authentication Options-Today's Trends Are Moving Well Beyond Passwords'. 33 (4).

Lewis, I. (2014). 'Ever had your fingerprints taken? Meeting the challenges of 21st Century access control'. *Biometric Technology Today*, 2014 (5). pp 9-11.

Lewis, J. R. (1995). 'IBM computer usability satisfaction questionnaires: psychometric evaluation and instructions for use'. *International Journal of Human-Computer Interaction*, 7 (1). pp 57-78.

Lin, D., Dunphy, P., Olivier, P. & Yan, J. (2007). 'Graphical passwords & qualitative spatial relations'. *Proceedings of the 3rd symposium on Usable privacy and security (SOUPS'07)*. Pittsburgh, USA: ACM, pp 161-162.

Liu, X., Qiu, J., Ma, L., Gao, H. & Ren, Z. (2011). 'A Novel Cued-recall Graphical Password Scheme'. *Sixth International Conference on Image and Graphics (ICIG)*. Hefei, China: IEEE, pp 949-956.

Luo, X. R., Brody, R., Seazzu, A. & Burd, S. (2011). 'Social Engineering: The Neglected Human Factor for Information Security Management'. *Information Resources Management Journal (IRMJ)*, 24 (3). pp 1-8.

Malempati, S. & Mogalla, S. (2011). 'A Well Known Tool Based Graphical Authentication Technique'. *First International Conference on Computer Science, Engineering and Applications (CCSEA)*. Chennai, India: AIRCC, pp 97-104.

Man, S., Hong, D. & Matthews, M. (2003). 'A shoulder-surfing resistant graphical password scheme-WIW'. *Proceedings of International conference on security and management (SAM'03)*. Las Vegas, USA: CSREA Press, pp 105-111.

Marquardt, P., Verma, A., Carter, H. & Traynor, P. (2011). '(sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers'. *Proceedings of the 18th ACM conference on Computer and communications security*. Chicago, Illinois, USA: ACM, pp 551-562.

McDonald, D. L., Atkinson, R. J. & Metz, C. (1995). 'One Time Passwords in Everything (OPIE): Experiences with Building and Using Stronger Authentication'. *Proceedings of the 5th USENIX UNIX Security Symposium*. Salt Lake City, USA.

Meyer, R. (2007). 'Secure Authentication on the Internet'. *SANS Institute—InfoSec Reading Room*.

Minne, P., Wells, J., Hutchinson, D. & Pierce, J. (2007). 'An investigation into the usability of graphical authentication using AuthentiGraph'. *5th Australian Information Security Management Conference*. Perth Western, Australia: Edith Cowan University, pp 175-186.

Mohammed, R., Bindu, C. S., Reddy, P. C. & Satyanarayana, B. (2008). 'A Novel Cognition Based Graphical Authentication Scheme which is Resistant to Shoulder-Surfing Attack'. *Proceedings of 2nd International conference on information Processing, ICIP*. Bangalore, India.

Monrose, F. & Reiter, M. (2005). 'Graphical passwords'. *Security and Usability.* O'Reilly, ch.9, pp 147-164.

Nali, D. & Thorpe, J. (2004). 'Analyzing user choice in graphical passwords', Tech. Rep. TR-04-01. *School of Computer Science, Carleton University, Ottawa, Canada.*

Nelson, D. L., Reed, V. S. & Walling, J. R. (1976). 'Pictorial superiority effect'. *Journal of Experimental Psychology: Human Learning and Memory*, 2 (5). pp 523-528.

Nickerson, R. S. (1968). 'A note on long-term recognition memory for pictorial material'. *Psychonomic Science*, 11 (2). pp 58-58.

O'Gorman, L. (2003). 'Comparing Passwords, Tokens, and Biometrics for User Authentication'. *Proceedings of the IEEE*, 91 (12). pp 2021-2040.

Office for National Statistics (2015). 'Focus on property crime: 2014 to 2015 — Mobile phone ownership and theft'. [Online]. Available at: http://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/focusonpropertycrime/2014to2015 (Accessed: March 2016).

Ortiz, S. J. (2007) 'One-Time Password Technology'. *Processor,* 29 (15). (Accessed: March 2016)

Paivio, A. (1986). 'A dual-coding approach'. *Mental representations.* Oxford Psychology Series 9, New York: Oxford University Press.

Paivio, A. & Csapo, K. (1973). 'Picture Superiority in Free Recall: Imagery or Dual Coding?'. *Cognitive psychology*, 5 (2). pp 176-206.

Paivio, A., Rogers, T. B. & Smythe, P. (1968). 'Why are pictures easier to recall than words?'. *Psychonomic Science*, 11 (4). pp 137-138.

Passfaces Corporation (2015a). 'The Science Behind Passfaces'. *White Paper*, [Online]. Available at: http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf (Accessed: March 2016).

Passfaces Corporation (2015b). 'Passfaces: Two Factor Authentication for the Enterprise'. [Online]. Available at: www.passfaces.com (Accessed: March 2016).

Pierce, J. D., Wells, J. G., Warren, M. J. & Mackay, D. R. (2003). 'A conceptual model for graphical authentication'. *1st Australian Information Security Management Conference*. Perth,Western Australia, (24), pp 347-351.

Pinkas, B. & Sander, T. (2002). 'Securing Passwords Against Dictionary Attacks'. *Proceedings of the 9th ACM conference on Computer and communications security*. Washington, USA: ACM, pp 161-170.

Por, L., Lim, X. & Kianoush, F. (2008). 'Background Pass-Go (BPG), a New Approach for GPS'. *Proceedings of the 12th WSEAS international conference on Computers*. Heraklion, Greece: World Scientific and Engineering Academy and Society (WSEAS), pp 369-374.

Por, L., Lim, X., Li, Q., Chen, S. & Xu, A. (2008). 'Issues, Threats and Future Trend for GSP'. *Proceedings of the 7th WSEAS international conference on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS'08)*. Hangzhou, China: World Scientific and Engineering Academy and Society (WSEAS), pp 627-638.

Por, L. & Lin, X. (2008). 'Multi-Grid Background Pass-Go'. *WSEAS Transactions on Information Science and Applications*, 5 (7). pp 1137-1148.

Ramakrishnan, G. (2001). 'Risk Management for Internet Banking'. *Information Systems Control Journal*, (6), pp 48-51. Available at: https://www.academia.edu/1269394/Risk_Management_for_Internet_Banking (Accessed: March 2016).

Ratha, N. K., Connell, J. H. & Bolle, R. M. (2001). 'Enhancing security and privacy in biometrics-based authentication systems'. *IBM systems Journal*, 40 (3). pp 614-634.

Ray, P. P. (2012). 'Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices'. *International Journal of Computer Trends and Technology (IJCTT)*, 3 (2). pp 235-241.

relbanks.com (2015). 'Banks Around the World'. [Online]. Available at: http://www.relbanks.com/ (Accessed: March 2016).

Renaud, K. (2004). 'Quantifying the Quality of Web Authentication Mechanisms: A Usability Perspective'. *Journal of Web Engineering*, 3 (2). pp 95-123.

Renaud, K. (2009). 'On user involvement in production of images used in visual authentication'. *Journal of Visual Languages & Computing*, 20 (1). pp 1-15.

Renaud, K. & De Angeli, A. (2004). 'My password is here! An investigation into visuo-spatial authentication mechanisms'. *Interacting with computers*, 16 (6). pp 1017-1041.

Renaud, K. & De Angeli, A. (2009). 'Visual Passwords: Cure-All or Snake-Oil?'. *Communications of the ACM*, 52 (12). pp 135-140.

Renaud, K., Mayer, P., Volkamer, M. & Maguire, J. (2013). 'Are Graphical Authentication Mechanisms as Strong as Passwords?'. *The 2013 Federated Conference on Computer Science and Information Systems (FedCSIS)*. Kraków, Poland: IEEE, pp 837-844.

Renaud, K. & Olsen, E. S. (2007). 'DynaHand: Observation-resistant recognition-based web authentication'. *IEEE Technology and Society Magazine*, 26 (2). pp 22-31.

Rescorla, E. & Lebovitz, G. (2010). 'A Survey of Authentication Mechanisms'. [Online]. Available at: http://tools.ietf.org/html/draft-iab-auth-mech-07.

Rittenhouse, R. G., Chaudry, J. A. & Lee, M. (2013). 'Security in Graphical Authentication'. *International Journal of Security and Its Applications*, 7 (3). pp 347-356.

Ritter, D., Schaub, F., Walch, M. & Weber, M. (2013). 'MIBA: Multitouch Image-Based Authentication on Smartphones'. *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. Paris, France: ACM, pp 787-792.

Roman Yudkin - Confident Technologies® (2011). 'How to Strengthen Online Authentication while Balancing Security, Usability and Cost', *White Paper*. [Online]. Available at: http://ctidev.confidenttechnologies.com/files/Romanwhitepaper.pdf (Accessed: March 2016).

Rouse, M. (2014). 'out-of-band authentication'. [Online]. Available at: http://searchsecurity.techtarget.com/definition/out-of-band-authentication (Accessed: March 2016).

Rubin, A. D. (1996). 'Independent one-time passwords'. *computing Systems*, 9 (1). pp 15-27.

Sabzevar, A. P. & Stavrou, A. (2008). 'Universal Multi-Factor Authentication Using Graphical Passwords', *IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS'08)*. Bali, Indonesia: IEEE, pp 625-632.

SafeNet (2015). 'GrIDsure Authentication Token'. [Online]. Available at: http://www.safenet-inc.com/resources/product-brief/data-protection/GrIDsure_Authentication_-_Product_Brief/ (Accessed: March 2016).

Schaub, F., Walch, M., Könings, B. & Weber, M. (2013). 'Exploring the Design Space of Graphical Passwords on Smartphones'. *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS'13)*. Newcastle, UK: ACM, pp 1-14.

Schneegass, S., Steimle, F., Bulling, A., Alt, F. & Schmidt, A. (2014). 'SmudgeSafe: Geometric Image Transformations for Smudge-resistant User Authentication'. *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. Seattle, USA: ACM, pp 775-786.

Schultz, E. E., Proctor, R. W., Lien, M.-C. & Salvendy, G. (2001). 'Usability and security an appraisal of usability issues in information security methods'. *Computers & Security*, 20 (7). pp 620-634.

SecurEnvoy (2013a). 'What is 2FA?'. [Online]. Available at: http://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm (Accessed: March 2016).

SecurEnvoy (2013b). 'Hardware Tokens vs Tokenless'. [Online]. Available at: http://www.securenvoy.com/two-factor-authentication/hardware-tokens-vs-tokenless.shtm (Accessed: March 2016).

Shepard, R. N. (1967). 'Recognition memory for words, sentences, and pictures'. *Journal of verbal Learning and verbal Behavior*, 6 (1). pp 156-163.

Siadati, H., Gupta, P., Smith, S., Memon, N. & Ahamad, M. (2015). 'Fortifying Android Patterns using Persuasive Security Framework'. *The Ninth International Conference on Mobile Ubiquitous Computing , Systems, Services and Technologies (UBICOMM 2015)*. Nice, France, pp 68-75.

Smetters, D. & Jacobson, V. (2009). 'Securing network content'. *Technical report, PARC*. Citeseer. pp 1-7.

Snodgrass, J. G. & Asiaghi, A. (1977). 'The Pictorial Superiority Effect in Recognition Memory'. *Bulletin of the Psychonomic Society*, 10 (1). pp 1-4.

Sobrado, L. & Birget, J.-C. (2002). 'Graphical passwords'. in The *Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*. Vol 4. [Online]. Available at: http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm (Accessed: March 2016).

Sollie, R. S. (2005). 'Security and usability assessment of several authentication technologies'. Master Thesis. *Gjøvik University College*.

Song, Y., Cho, G., Oh, S., Kim, H. & Huh, J. H. (2015). 'On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks'. *Proceedings of the 33rd*

Annual ACM Conference on Human Factors in Computing Systems. Seoul, Republic of Korea: ACM, pp 2343-2352.

Stamp, M. (2011). 'Authentication'. *Information security: principles and practice.* 2nd edn., 7 7. New Jersey: John Wiley & Sons. pp 229-254.

Standing, L. (1973). 'Learning 10000 pictures'. *The Quarterly journal of experimental psychology*, 25 (2). pp 207-222.

Standing, L., Conezio, J. & Haber, R. N. (1970). 'Perception and memory for pictures: Single-trial learning of 2500 visual stimuli'. *Psychonomic Science*, 19 (2). pp 73-74.

StrikeForce Technologies Inc. (2015). 'ProtectID® White Paper'. [Online]. Available at: http://www.strikeforcetech.com/PID/img/ProtectID_White_Paper.pdf (Accessed: March 2016).

Stubblefield, A. & Simon, D. (2004). 'Inkblot Authentication'. *Microsoft Technical Report MSR-TR-2004-85*, pp 1-16.

Sule, D. (2013). 'Man in the Browser—A Threat to Online Banking'. *ISACA JOURNAL, (4)*. pp 16-18. Available at: http://www.isaca.org/Journal/archives/2013/Volume-4/Documents/13v4-Man-in-the-Browser.pdf (Accessed: March 2016).

Suo, X., Zhu, Y. & Owen, G. (2006). 'Analysis and Design of Graphical Password Techniques'. *Advances in Visual Computing*, (4292). pp 741-749.

Suo, X., Zhu, Y. & Owen, G. (2005). 'Graphical Passwords: A Survey'. *21st Annual Computer Security Applications Conference (ACSAC'05)*. Tucson, USA: IEEE.10 pp.-472.

Swivel Secure (2014). 'Mobile app based authentication - Data Sheet'. [Online]. Available at: http://hosteu.msgapp.com/uploads/96495/Documents/Data%20Sheets/1411_DS_Mobile_App_EN.pdf (Accessed: March 2016).

Syukri, A., Okamoto, E. & Mambo, M. (1998). 'A User Identification System Using Signature Written with Mouse'. In: Boyd, C. and Dawson, E. (eds.), *Information Security and Privacy.* Springer Berlin Heidelberg, (1438), pp 403-414.

Tao, H. & Adams, C. (2008). 'Pass-Go: A Proposal to Improve the Usability of Graphical Passwords'. *International Journal of Network Security*, 7 (2). pp 273-292.

Tari, F., Ozok, A. & Holden, S. H. (2006). 'A Comparison of Perceived and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords'. *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS'06)*. Pittsburgh, USA: ACM, pp 56-66.

The BBA (2015). 'Mobile phone apps become the UK's number one way to bank'. [Online]. Available at: https://www.bba.org.uk/news/press-releases/mobile-phone-apps-become-the-uks-number-one-way-to-bank/ (Accessed: March 2016).

The Defence Signals Directorate (DSD) (2014). 'Multi-factor authentication'. [Online]. Available at: http://www.asd.gov.au/publications/protect/Multi_Factor_Authentication.pdf (Accessed: March 2016).

The Royal Bank of Scotland © (2014). 'Will I be charged for any mobile phone text alert messages I may get?—Ask a Question - RBS'. [Online]. Available at: http://supportcentre-rbs.custhelp.com/app/answers/detail/a_id/745/kw/network%20operator (Accessed: March 2016).

Thorpe, J. & van Oorschot, P. C. (2004). 'Towards secure design choices for implementing graphical passwords'. *20th Annual Computer Security Applications Conference*. pp 50-60.

Thorpe, J. & van Oorschot, P. C. (2007). 'Human-seeded attacks and exploiting hot-spots in graphical passwords', *Proceedings of 16th USENIX Security Symposium (SS'07)*. Boston, USA: USENIX Association Berkeley, pp 103-118.

Uellenbeck, S., Dürmuth, M., Wolf, C. & Holz, T. (2013). 'Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns'. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. Berlin, Germany: ACM, pp 161-172.

Van Oorschot, P. C. & Wan, T. (2009). 'TwoStep: An Authentication Method Combining Text and Graphical Passwords'. In: Babin, G., Kropf, P. and Weiss, M. (eds.), *E-Technologies: Innovation in an Open World.* Springer Berlin Heidelberg, (26) pp 233-239.

Von Zezschwitz, E., Dunphy, P. & De Luca, A. (2013). 'Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices'. *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*. Munich, Germany: ACM, pp 261-270.

Vorster, J. & van Heerden, R. (2015). 'Graphical Passwords: A Qualitative Study of Password Patterns'. *Iccws 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security*. Reading, UK: Academic Conferences and Publication Limited, pp 375-383.

Wang, L., Chang, X., Ren, Z., Gao, H., Liu, X. & Aickelin, U. (2010). 'Against Spyware Using CAPTCHA in Graphical Password Scheme'. *24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*. Perth, Australia: IEEE, pp 760-767.

Weinshall, D. (2004). 'Secure Authentication Schemes Suitable for an Associative Memory'. *Hebrew University, Leibniz Center for Research in Computer Science. Technical Report TR-*2004-30.

Weinshall, D. (2006). 'Cognitive Authentication Schemes Safe Against Spyware'. *Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06)*. Berkeley, USA: IEEE. pp 6 pp.-300.

Weir, C. S., Douglas, G., Richardson, T. & Jack, M. (2010). 'Usable Security: User Preferences for Authentication Methods in eBanking and the Effects of Experience'. *Interacting with Computers*, 22 (3). pp 153-164.

Weiss, R. & Luca, A. D. (2008). 'PassShapes: Utilizing Stroke Based Authentication to Increase Password Memorability'. *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*. Lund, Sweden: ACM, pp 383-392.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. & Memon, N. (2005a). 'Authentication using graphical passwords: effects of tolerance and image choice'. *Proceedings of the 2005 symposium on Usable privacy and security* (*SOUPS'05)*. Pittsburgh, USA: ACM, pp 1-12.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. & Memon, N. (2005b). 'Authentication using graphical passwords: Basic results'. *Human-Computer Interaction International (HCII 2005)*. Las Vegas, USA.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. & Memon, N. (2005c). 'PassPoints: Design and Longitudinal Evaluation of a Graphical Password System'. *International Journal of Human-Computer Studies*, 63 (1). pp 102-127.

Wiedenbeck, S., Waters, J., Sobrado, L. & Birget, J.-C. (2006). 'Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme'. *Proceedings of the working conference on Advanced visual interfaces*. Venezia, Italy: ACM, pp 177-184.

Williams, A. (2015). 'Images and codes provide alternative to multiple device password systems'. [Online]. Available at: https://www.plymouth.ac.uk/news/images-and-codes-could-provide-secure-alternative-to-multiple-device-password-systems-study-suggests (Accessed: March 2016).

Williamson, G. D. (2006). 'Enhanced Authentication in online Banking'. *Journal of Economic Crime Management*, 4 (2) Available at:

http://www.utica.edu/academic/institutes/ecii/publications/articles/51D6D996-90F2-F468-AC09C4E8071575AE.pdf (Accessed: March 2016).

Wu, T.-S., Lee, M.-L., Lin, H.-Y. & Wang, C.-Y. (2014). 'Shoulder-surfing-proof graphical password authentication scheme'. *International journal of information security*, 13 (3). pp 245-254.

Xiaoyuan, S., Ying, Z. & Owen, G. S. (2005). 'Graphical Passwords: A Survey'. *21st Annual Computer Security Applications Conference (ACSAC'05)*. Tucson, USA: IEEE. pp. 10 pp.-472.

Xue, M., Hitt, L. M. & Chen, P.-y. (2011). 'Determinants and Outcomes of Internet Banking Adoption'. *Management Science*, 57 (2). pp 291-307.

Yesseyeva, E., Yesseyev, K., Abdulrazaq, M., Lashkari, A. & Sadeghi, M. (2014). 'Tri-Pass: A New Graphical User Authentication Scheme'. *International Journal of Circuits, Systems and Signal Processing*. (8) pp 61-67.

Zangooei, T., Mansoori, M. & Welch, I. (2012). 'A Hybrid Recognition and Recall Based Approach in Graphical Passwords', *Proceedings of the 24th Australian Computer-Human Interaction Conference*. Melbourne, Australia: ACM, pp 665-673.

Zezschwitz, E. v., Luca, A. D., Janssen, P. & Hussmann, H. (2015). 'Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)lock Patterns'. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Seoul, Republic of Korea: ACM, pp 2339-2342.

Zheng, Z., Liu, X., Yin, L. & Liu, Z. (2010). 'A Hybrid password Authentication Scheme Based on Shape and Text'. *Journal of Computers*, 5 (5). pp 765-772.

Zippy, E. & Moshe, Z. (2009). 'Authentication Methods for Computer Systems Security'. *Encyclopedia of Information Science and Technology, Second Edition.* Hershey, USA: IGI Global, pp 288-293.

Appendices

Appendix A Review of additional graphical password schemes

Appendix B Images licences

Appendix C List of invitation letters & Ethical approvals

Appendix D List of questionnaires

Appendix E Experiments task sheets

Appendix F Implementations of GOTPass prototype

Appendix G Published papers & Press release

Appendix A Review of additional graphical password schemes and list of scheme names with references

i. Graphical password schemes names and references

A list of all graphical password schemes that have been discussed in this thesis along with their bibliography for easy reference.

Recall-based scheme	Reference
Syukri Algorithm – (draw a signature)	Syukri, Okamoto and Mambo (1998)
Draw-A-Secret (DAS)	Jermyn *et al.* (1999)
Grid Selection	Thorpe & van Oorschot (2004)
Multi-Grid DAS (MGDAS)	Chalkias, Alexiadis & Stephanides (2006)
Qualitative Draw-A-Secret (QDAS)	Lin et al. (2007)
Background Draw-A-Secret (BDAS)	Dunphy & Yan (2007)
DAS with Rotation (R-DAS)	Chakrabarti, Landon & Singhal (2007)
Pass-Go	Tao and Adams (2008)
Background Pass-Go (BPG)	Por, Lim & Kianoush (2008)
Multi-Grid Background Pass-Go (MGBPG)	Por & Lin (2008)
Yet another Graphical Password (YAGP)	Haichang et al. (2008)
Blonder Scheme	Blonder (1996)
PassPoints	Wiedenbeck *et al.* (2005)
Cued Click Points (CCP)	Chiasson, van Oorschot and Biddle (2007)
Persuasive Cued Click-Points (PCCP)	Chiasson et al. (2008)
Click Buttons according to Figures in Grids (CBFG)	Liu et al. (2011)
Multi-Factor Graphical Authentication	Sabzevar & Stavrou (2008)
Multitouch Image-Based Authentication on Smartphones (MIBA)	Ritter et al. (2013)
Tri-Pass	Yesseyeva et al. (2014)
Inkblot Authentication	Stubblefield and Simon (2004)
Zheng (Shape & Text)	Zheng et al. (2010)

Recognition-based scheme	Reference
PassFaces	Passfaces Corporation, (2015)
Déjà vu	Dhamija and Perrig (2000)
Triangle scheme, Moveable frame scheme, Other special geometric configurations	Sobrado and Birget (2002)
Visual Identification Protocol (VIP)	De Angeli et al. (2002)
Picture Password	Jansen et al. (2003)
Story	Davis, Monrose and Reiter (2004)
PassImages	Charruau, Furnell & Dowland (2005)
Colorlogin	Gao et al. (2009)
Graphical Password with Icons (GPI) & Graphical Password with Icons suggested by the System (GPIS)	Bicakci et al. (2009)
CDS	Gao et al. (2010)
Where You See is What You Enter (WYSWYE)	Khot, Kumaraguru and Srinathan (2012)
AuthentiGraph	Pierce et al. (2003)
Cognitive Authentication	Weinshall (2006)
Mohd's Scheme	Mohammed et al. (2008)
Komanduri & Hutchings Picture Password	Komanduri and Hutchings (2008)
Gaze-Contingent	Dunphy, Fitch & Olivier (2008)
Image Based Registration and Authentication System (IBRAS)	Akula & Devisetty (2004)
Convex Hull Click scheme (CHC)	Wiedenbeck et al. (2006)
Shoulder-Surfing-Proof (SSP)	Wu et al. (2014)
Weinshall approach	Weinshall (2004)
DynaHand	Renaud & Olsen (2007)

Hybrid schemes	References
Hong scheme	Man, Hong & Matthews (2003)
Recall-a-Formation (RAF)	Suo, Zhu and Owen (2006)
TwoStep	van Oorschot and Wan (2009)
Touch-screen Authentication using Partitioned Images (TAPI)	Citty and Hutchings (2010)
Enhanced Graphical Authentication System (EGAS)	Jali, Furnell and Dowland (2011)
Deshmukh's scheme	Deshmukh and Devale (2013)

Graphical OTP schemes	References
GrIDsure	(Blair, 2007)
Enhanced-GrIDsure with Background	Dimitropoulos (2011)
GrIDsure with 4 Patterns (GS4)	Jhawar et al. (2011)
Gao CAPTCHA	Gao et al. (2009b)
Passblot	Gupta et al. (2011)
ImageShield	Roman Yudkin - Confident Technologies® (2011)
Graphical One Time Password (GOTP)	Ku et al. (2012)
Zangooei Hybrid approach	Zangooei, Mansoori and Welch (2012)

a. Draw-based schemes

(Weiss & Luca, 2008) came up with a novel idea for authenticating users with stroke-based drawings called "PassShapes". The simple geometric shapes of this system are composed of a different combination of eight diverse strokes. A PassShape may possibly be comprised of several stroke sequences, each of which consists of several strokes drawn sequentially without lifting the pen. An alphanumeric string representation is utilised as an output of the PassShape password for the internal processing. A character representation is assigned for each stroke, where the directions of the stroke are indicated by the letters (e.g. 'U' means Up, 'D' means Down, etc.), whereas the numbers represent the direction equivalent to the position of the number on a standard number pad (i.e. '3' refers to 'lower right'). Two stroke sequences can be separated by a pen-up event marked with an 'X'. However, an exact redrawing of a PassShape in the same size or position is not required since only the strokes and their order are calculated. Since PassShape contains only straight lines, reproducing the password should be easy and effortless even for non-artistic users.
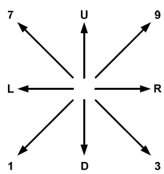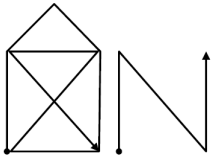
PassShapes: eight different possible strokes	The internal representation of PassShape: U93DL9L3XU3U

Figure 1: "PassShape" design (Weiss & Luca, 2008)

Another user-drawn scheme called "Touchscreen Multi-layered Drawing" (TMD) was designed by (Chiang & Chiasson, 2013). The aim was to encourage more complex passwords through the use of multiple layers of grids with large detached cells. Beside the commonly used types of "cells": Unselected and Selected cells, there is a new type called Warp cells. The way to display the next layer is by touching any of the four Wrap

cells which allows users to draw longer secrets across several layers. The usability of TMD on mobile devices was assessed by a user study that involved 90 users. After one week of the password creation, the TMD showed superior result with login success rate of 86% within the first attempt and 15-18 seconds of average login time.
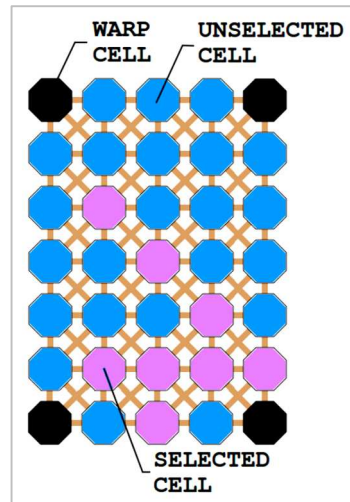
Figure 2: "**TMD**" interface

- **Studies related to Android Unlock Pattern:**

An attempt to mitigate the Smudge attack was conducted by (Schneegass et al., 2014) who introduced "SmudgeSafe" system that depends on geometrical transformations of the image. The transformations may include translation, rotation, scaling, shearing, or flipping. The password security is significantly improved as the images appear differently in each login time. Hence, smudge traces are overlapped which makes guessing or inferring the original password very difficult. The proposed method was made available through Google Play store for evaluation. Over five months, the application was downloaded by 374 users and 130,000 logins were collected. The result of the study showed that the SmudgeSafe performed best and provided more security in comparison with PINs and original lock patterns.

In a field study across 3 weeks, (Von Zezschwitz, Dunphy & De Luca, 2013) compared the performance of personal identification numbers (PIN) and pattern locks. The study

designed two Android-based prototypes to be installed on the participants' smartphones. Participation was divided into two groups; the pattern group which consisted of 29 users and the second PIN group with 24 users. Participants were requested to use the respective prototype to login once every day and were allowed a maximum of 3 attempts each time. The study analysed 504 PIN entries and 609 pattern entries. The result showed a significant difference in the overall error rate between the PIN group (0.08%) and pattern group (16.3%). However, according to the relevant questionnaire answers, users of the pattern system were not irritated by the failure rate but conversely they appeared to have a strong preference for the pattern lock approach. An additional task was assigned to the participants after 14 days of non-use to rate the memorability of the given system. In this recall test, users needed to recall their PIN or pattern using printed copy of the prototypes. The result indicated that both approaches performed fairly equally with 92% successful recall in the PIN group and 90% in pattern group. One interesting finding was that assigning secure complex patterns did not affect the memorability of the drawings.

The security of Android unlock pattern was also studied by (Uellenbeck et al., 2013). Instead of the theoretical password spaces, they measured the actual user choices of patterns. It was found that the process of the pattern selection is not a bias free. To improve the security of such scheme, some changes to the points' arrangement were proposed that should increase the space of the passwords actually in use. The first alteration was the 'Leftout Small Pattern', which reduces the bias by omitting the upper left point. The second alteration was the 'Leftout Large Pattern' where the overall point count is increased by adding two points to the bottom row. The third alteration was the 'Circle Pattern' which removes corner points. The final alteration was the 'Random Pattern' in which the points are arranged randomly. A user study was conducted that involved 366 participants over several weeks. The result indicated that the Circle Pattern

approach was better in performance and security as well, in contrast to the Random Pattern approach which was hard to use. The study concluded that the implementation of different approaches for different smartphones might reduce the risk of building an attack dictionary.

(Andriotis et al., 2013) conducted another study on user practices when creating a pattern lock and to find out about users' perceptions towards producing a secure pattern. As a result, a behaviour-based attack and physical attack methods were established aiming to retrieve full or part of a pattern by reducing the search space of possible combinations. The best ways to produce quality results while performing physical attacks turned out to be through optical cameras or microscopes. In 2014, (Andriotis, Tryfonas & Oikonomou, 2014) introduced an enhancement to Pattern-Lock graphical authentication method. They found that users of this method were not informed about the strength of their chosen pattern. Thus, they proposed displaying a feedback to emphasize the lack of security of the user's initial choice which allow users to revise their pattern to make it stronger. The result of the research showed that users selected fewer 'Weak' passwords after propounding the feedback. Informing the users about their password strength resulted in changing the choice of patterns for almost quarter of the participants.

(Song et al., 2015), came up with a new strength meter to indicate how strong a user's pattern lock is in the face of shoulder-surfing or guessing attacks. In order to design an effective meter, different factors were carefully considered to measure the strength of a pattern lock. These factors include the length of a pattern lock, the number of connected points, and the number of lines connecting point-to-point. The meter is designed visually as a slider located on the top of the screen which shows real time pattern strength while

users create their patterns. There are three scales to represent the strength; weak, medium, or strong.

The correctness and accuracy of the designed meter was evaluated through a user study that involved 101 participants. Users were presented with pattern locks categorised as weak, medium, or strong using the meter and were asked to perform shoulder-surfing attacks on them. The study tested 606 pattern locks, among which nearly 71% were successfully compromised patterns. However, the result showed that compromising pattern locks that were indicated as strong by the meter were harder than those indicated as medium or weak.

A second experiment was conducted through a field study to investigate how effective the meter is in assisting users to select stronger pattern locks. The experiment made use of an Android application called "EnCloud" which was equipped with the proposed meter and made available via Android Play store. To use the application, users need to create a pattern lock for authentication, some of whom were offered with the strength meter. The analysis of the collected data confirmed that the meter assistance was beneficial for the majority of the users which resulted in generating more secure pattern locks.
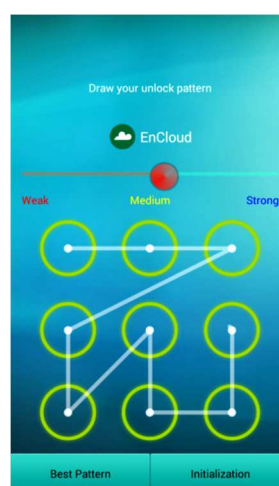
Figure 3: Pattern Lock Strength Meter (Song *et al.*, 2015)

In another research by (Zezschwitz et al., 2015), a systematic evaluation to quantify the susceptibility of unlock patterns against shoulder surfing was presented. Various

influencing parameters on observation resistance were examined including: length of patterns, visibility of lines, knight moves, overlaps and intersections. In order to weigh the impact of a single parameter, an online study was conducted that used an algorithm to generate patterns and simulate the human behaviour to unlock those patterns. During the experiment, the display of the device is perfectly located within the sight of the attacker who can view the authentication attempt once. Afterwards, the attacker gets hold of the device in which he needs to redraw the captured pattern for verification. The study involved 5960 patterns of different lengths and strengths, which were attacked by 298 participants. The results revealed that attackers managed to correctly shoulder surf 51.7% of the patterns, out of which 57.9% had visible lines. The length of the successfully attacked patterns was shorter (M=5.7) than the unsuccessful ones. The influence of all parameters was highly significant, however the line visibility and pattern length were of particular importance. The observation risk was reduced by 67% when lines were invisible. The observers' chance was decreased by 45% when increasing the pattern length by one. The addition of other parameters like knight move brought the risk down by 32%, overlaps 20%, and intersections 12%. The study concluded that attacking Android patterns is easy even when observed once. However, it suggested using this prediction model as a proactive security checker that estimates the risk of a given pattern to help users to avoid weak patterns.

(Siadati et al., 2015) presented two persuasive methods that should expand the effective password space by urging users to select stronger patterns. The first mechanism is called "BLINK", which suggests the starting point of the pattern for the user without enforcement. As a result, the bias selection of starting points should be significantly reduced and be less predictable. During registration, BLINK will recommend a random point out of the 9 points by adding an extra circle around it and blink until the user starts

drawing a pattern. The second mechanism is called "EPSM": Embedded pattern strength meter, where users receive continuous feedback about the strength of their patterns during the creation process. The system provides feedback to help users adjusting their weak patterns by updating the pattern's colour according to the strength level. A weak pattern appears in red colour, moderate pattern in yellow, and a strong pattern in green.

A user study to evaluate security and usability of the proposed designs was conducted on 270 participants. Each participant was randomly appointed to one of the three different user interfaces: (NORMAL) the traditional Android Patterns, the BLINK, and the EPSM. The task involved creating a new pattern and confirming it then complete a survey. The result indicated that choosing strong patterns was increased to 60% when using BLINK and 77% when EPSM is used. The use of BLINK managed to eliminate the bias selection of starting point by distributing the selections almost evenly. The suggested points by the system was accepted by 85% of the users. In addition, the study confirmed that the created patterns using EPSM and BLINK are more secure than NORMAL. In regards to the accuracy of the pattern recall, the result showed no significant difference in the recall rates between either NORMAL and BLINK or NORMAL and EPSM.
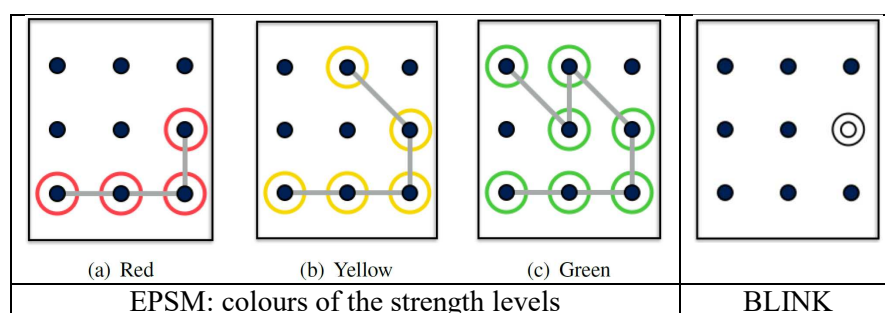
Figure 4: "EPSM" & "BLINK" interfaces (Siadati *et al.*, 2015)

b. Click-based techniques

(Sabzevar & Stavrou, 2008) proposed a new multi-factor authentication scheme based on a graphical password. To that end, the user's own handheld device is utilised as a decoder

for the password and a second factor for authentication process. Authentication is based upon two images (Password Image and Key Image). The user is firstly challenged with an image password sent to their terminal by a service provider. Next, a corresponding key image containing some hint information is transmitted to the user's handheld device to enable an appropriate determination of the required click points and the correct ordering. The approach takes advantage of the increased popularity of handheld devices, such as cell phones, so there is no more need for memorising different passwords or carrying different hardware tokens. The proposed method is capable of protecting against a diverse range of threats, such as key-loggers, brute-force and shoulder-surfing. Unfortunately, evaluation experiment was not conducted and no data was published that prove the scheme's performance and security in practice.

| Password Image | Corresponding Key Image (Handheld) |
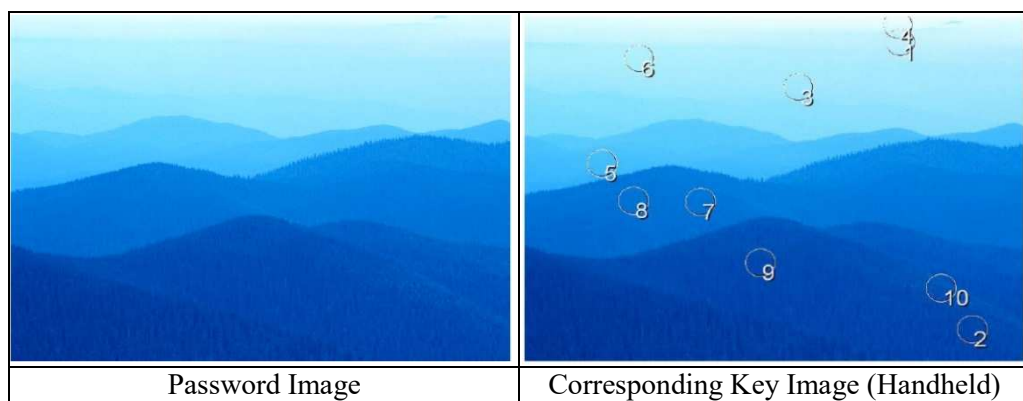
Figure 95: Multi-Factor Graphical Authentication (Sabzevar & Stavrou, 2008)

(Ritter et al., 2013) took advantage of the multiple fingers used for password entry to enhance the security of their proposed technique. The new scheme is called "Multitouch Image-Based Authentication on Smartphones" (MIBA). In each login round, the user is allowed to mark multiple points on an image which thwarts the password observation by an adversary. The background images are used as cues and the next round's image is determined depending on the user's input in the recent round. A semi-transparent grid of potential click points overlays the background image to help in placing fingers correctly. Clicking on any potential click point turns it into fully transparent. In addition, a shift

function was further introduced to increase the theoretical password space. The shift function extends the entropy of a round by providing an additional entry mode that is difficult for an observer to distinguish from a normal round. A shift round is activated by a slightly longer press which vibrates the phone as an indication of the shift function activation. MIBA is able to produce 14.7 bit of theoretical password space per round. An initial lab experiment was performed to evaluate the required entry time as well as user perception of MIBA usability. 75% of all password entry attempts carried out by 30 participants took less than 10 seconds. As for the usability, initial difficulties when using multiple fingers for input were reported by some participants. Nevertheless, the user experience of MIBA was overall satisfactory and participants considered it useful.

Figure 6: Selecting click points with multiple fingers in "MIBA" (Ritter *et al.*, 2013)

(Yesseyeva et al., 2014) proposed a new scheme called "Tri-Pass" that was adopted from two earlier techniques named PassPoint and Triangle. The registration starts by choosing an image from a set of pictures and then click on any three points on the image as "password points". The authentication process is based on clicking on any three points that will form a triangle around each password point. It means that inside each area of the invisible triangles there is one password point. To login, there should be three clicks per password point, that is a total of nine clicks for the entire three password points. The sequence of inputting points is a condition for successful authentication. The usability of the Tri-Pass method was evaluated by survey. Over 60% of the responses viewed the method as reliable and trustworthy and more than 70% of the users considered the system

as simple to use, register and login. However, only half of the respondents found the system easy to memorize and learn. As for the time efficiency, registration time was satisfactory whereas login time took much longer compared with textual password.

Figure 7: "Tri-Pass" algorithm: Login phase (Yesseyeva *et al.*, 2014)

c. Choice-based techniques

In 2008, (Dunphy, Fitch & Olivier, 2008) introduced a new joint method between PassFaces (as the main graphical authentication scheme) and eye tracker (as the input means) to resist shoulder-surfing. The system was deployed over a simulated ATM machine. Despite the known limitations of the eye trackers technique such as failing to enrol errors, the study showed good initial results in regards to user performance and skill improvement in using the eye tracker technique.
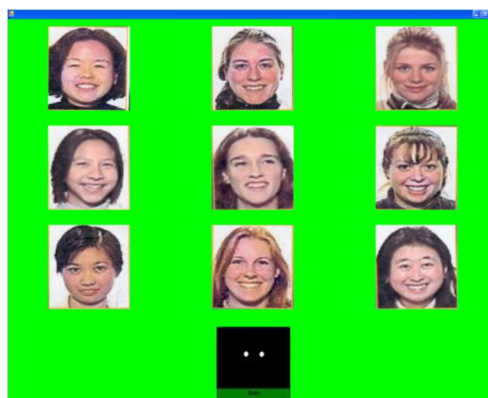
Figure 8: "Gaze-Contingent" login challenge (Dunphy, Fitch & Olivier, 2008)

(Akula & Devisetty, 2004) proposed a similar technique to Déjà vu named "Image Based Registration and Authentication System" (IBRAS). In this technique the registration

process starts by selecting an image which is user's choice followed by displaying the selected image on the window for user verification. The system requires the users to carry the secret image with them for future use. The user is requested to submit a combination of the unique user ID and the secret image chosen earlier as credentials to the system. The authentication request is approved when the image matches with the one already stored in the system. Interestingly, only the hashed value of the image is stored in the system not the image itself. Moreover, the images are hashed using a secure hashing function SHA-1which does not seem to have an impact on the system's memory since it produces only 20 byte secure output.

In a similar way to the Triangle scheme (Sobrado & Birget, 2002) which was mentioned earlier, (Wiedenbeck et al., 2006) proposed their Convex Hull Click scheme "CHC" which is a multi-rounds challenge-response authentication. In this scheme, creating a password requires the user to choose and remember some icons (pass-icons) from a larger set of icons. At login time, the system challenges the user by displaying a number of randomly arranged icons, a few of which are pass-icons. The user is required to recognise three or more of the corresponding password icons and then use those pass-icons to virtually create a convex hull, which is the area in between the edges that join several pass-icons. Responding to the challenge is done by clicking anywhere within the convex hull. However, the window's size and the user's ability to identify the pass-icons among many other icons are considered two practical limits.

A usability study was carried out by fifteen participants in two sessions, a first day session and a week later follow-up session. In the initial session, the task for the participants was to login for ten successful logins. The result indicated that 90.35% of the password inputs were correct with an average time of 71.66 seconds. The follow-up session involved showing the participants a printed list of 112 randomly ordered icons and were requested to spot the five pass-icons. The result of this session showed a high level of memorability

as 14 participants managed to identify the five pass-icons correctly whereas the remaining participant failed to remember only one of the pass-icons. However, looking for the pass-icons in the screen requires more scanning and can be even confusable if icons are small and look similar. Another weak aspect of CHC is the longer time taken for password entry.

Two probabilistic attacks against the CHC scheme were reported later in 2013 by Asghar et al. (Asghar et al., 2013). The attacks statistics addressed some weaknesses in the convex hull protocol against a passive eavesdropping attack. The result of the observation of a few authentication sessions in those attacks simulations revealed a high probability of obtaining secret icons. Thus, impersonating other users is simple once some secret icons are obtained.
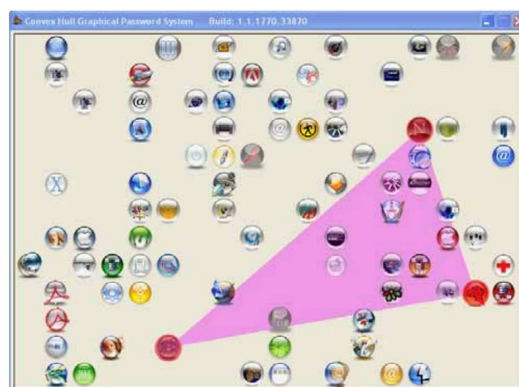
Figure 9: "CHC" login interface (Wiedenbeck *et al.*, 2006)

Later in 2014, (Wu et al., 2014) proposed a new graphical password authentication system called "Shoulder-Surfing-Proof" (SSP). The new proposal improved the Triangle scheme (Sobrado & Birget, 2002) and CHC scheme (Wiedenbeck *et al.*, 2006) by using a number of colour balls moving on the screen instead of clicking on a fixed region. At registration, users need to remember password icons and their colours. In SSP, the way to enter passwords is changed. To authenticate, the user just presses the space key to confirm when one matching ball is moving into the authentication region. The addition of dynamic moving colour balls to the screen complicates the chosen locations. That will make

comparing and analysing the screen snaps of an entire captured authentication process to find out password icons even more difficult. Attackers cannot distinguish the correct colour and icons even when recording the location of each moving ball while a user presses the space key.

The experiment included attack simulations of login attempts using the mouse-clicking approach and SSP approach. The results of the comparison showed that the success probability of guessing the correct passwords for both approaches was almost similar due to the use of the same convex-hull algorithm. As far as the feasibility of SSP scheme is concerned, fifteen users participated in the trial where each individual was requested to register with the system by selecting one colour five icons. During the authentication performance, the user spent an average of 25.71 seconds to find out the convex hull formed with the pre-selected icons, while completing the authentication process consumed 35.29 seconds in average.
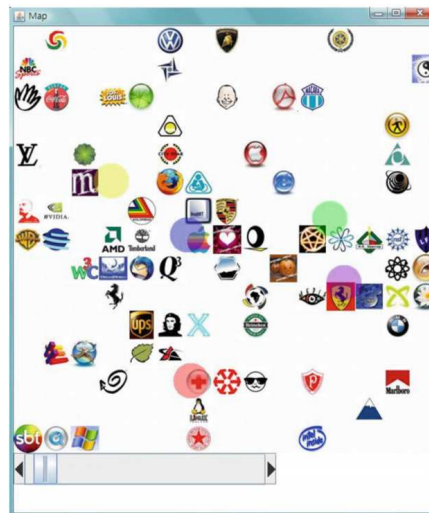
Figure 10: Login interface of **"SSP"** scheme (Wu *et al.*, 2014)

(Weinshall, 2004) introduced a protocol based on the human ability to recognise pictures. This protocol aims to ensure secure authentication even in cases where eavesdroppers manage to overhear some of the successful authentication sessions. The system is composed of two sets of pictures: 240 pictures of public set B and a secret subset F of 60

familiar pictures selected for each user. The protocol was designed as a 4x5 grid presenting a random selection of 20 pictures from set B. Next to each picture there is an assigned random bit (0 or 1). There are two possible methods to identify the users. In the first variant, users are required to recognise the first and last familiar pictures from subset F and compare the associated bits, determining whether they are equal or not. In the second variant, the first, second and last familiar pictures from subset F must be identified by the user and then their 3 associated bits are compared to check whether their majority is 0 or 1.

A user study, that involved 20 queries to answer, was carried out on small scale of three users and over various time periods. The result showed a high success rate and suggested that this protocol has the chance to practically authenticate users.

Figure 11: "Weinshall approach" An example of one query panel (Weinshall, 2004)

(Renaud & Olsen, 2007), proposed their authentication approach "DynaHand" utilising graphical mechanism and relying on the ability of the users to recognise random five-digit numeral strings of their own handwriting. The system involves three rounds that are required to complete the authentication process each of which displays nine images while randomising the sequence of its five-digit content. That means that remembering the PIN is no longer required where users only need to recognise their own handwritten numbers.

A successful authentication is achieved through a correct identification of the handwritten numerals for all three sequential stages.
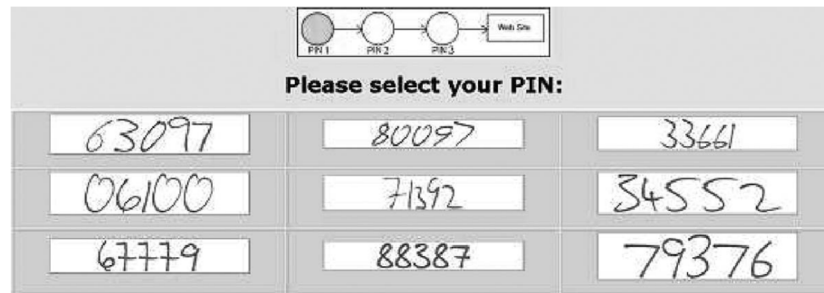
Figure 12: "DynaHand" authentication system (Renaud & Olsen, 2007)

(Bicakci et al., 2009) proposed a solution to overcome the hotspot problem through two novel recognition-based graphical password methods. Graphical Password with Icons "GPI" and Graphical Password with Icons suggested by the System "GPIS" are the proposed systems that utilize icons as points of click on the graphical password interface. In the first system GPI, the common idea of clicking on particular locations on a background image to form a graphical password is replaced by clicking on a number of displayed icons. The second system GPIS uses the same concept except that the set of password icons are generated randomly and assigned by the system to the user who can accept that given icons or reject them by requesting a new set. Both schemes contain 150 icons selected from 15 categories. Each line presents icons from the same category and each user receives random display of categories and their instances. Users of these schemes need to select their passwords by clicking on six icons in sequence. However, a different kind of hotspot can be also generated when using icons (hot-icons) since some can draw users' attention. To overcome this issue, GPIS scheme should be selected as it uses system assigned icons instead.

The usability and security of GPI and GPIS were compared with a conventional click-based graphical password scheme (PassPoints) through a lab experiment. Sixty-nine participants took part in this study which divided them into three groups. The result

revealed that the registration time for GPI was longer than that of PassPoints. Approximately 20% of the users of all groups forgot their password which means that there is no significant difference in the memorability level between the compared schemes. Although users of GPIS scheme were assigned the icons by the system, but that had no substantial impact on the usability and memorability. As far as the entry time is concerned, the proposed schemes performed slower than PassPoints scheme.

| GPI interface | GPIS interface |
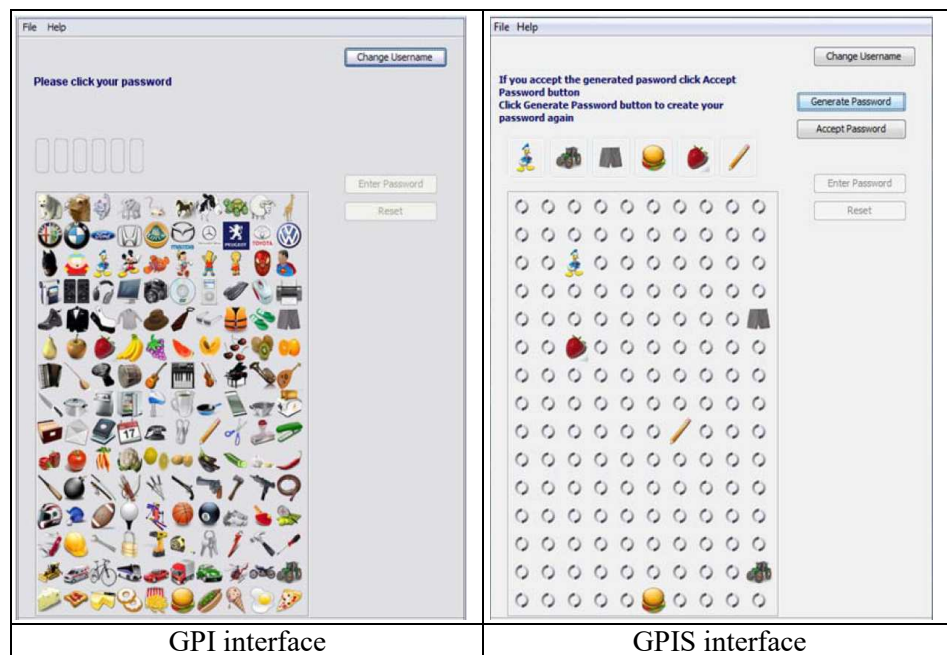
Figure 13: "GPI" & "GPIS" interfaces

References

Akula, S. & Devisetty, V. (2004) 'Image based registration and authentication system', *Proceedings of Midwest Instruction and Computing Symposium*.

Andriotis, P., Tryfonas, T. & Oikonomou, G. (2014) 'Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method', *Human Aspects of Information Security, Privacy, and Trust*. Springer, pp. 115-126.

Andriotis, P., Tryfonas, T., Oikonomou, G. & Yildiz, C. (2013) 'A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks', *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, pp. 1-6.

Asghar, H., Li, S., Pieprzyk, J. & Wang, H. (2013) 'Cryptanalysis of the Convex Hull Click Human Identification Protocol'. *International Journal of Information Security*, 12 (2). pp 83-96.

Bicakci, K., Atalay, N. B., Yuceel, M., Gurbaslar, H. & Erdeniz, B. (2009) 'Towards Usable Solutions to Graphical Password Hotspot Problem', *Computer Software and Applications*

Conference, 2009. COMPSAC '09. 33rd Annual IEEE International. 20-24 July 2009. pp. 318-323.

Chiang, H.-Y. & Chiasson, S. (2013) 'Improving User Authentication on Mobile Devices: A Touchscreen Graphical Password', *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services.* ACM, pp. 251-260.

Dunphy, P., Fitch, A. & Olivier, P. (2008) 'Gaze-contingent passwords at the ATM', *4th Conference on Communication by Gaze Interaction (COGAIN).*

Renaud, K. & Olsen, E. S. (2007) 'DynaHand: Observation-resistant recognition-based web authentication'. *Technology and Society Magazine, IEEE,* 26 (2). pp 22-31.

Ritter, D., Schaub, F., Walch, M. & Weber, M. (2013) 'MIBA: Multitouch Image-Based Authentication on Smartphones', *CHI'13 Extended Abstracts on Human Factors in Computing Systems.* ACM, pp. 787-792.

Sabzevar, A. P. & Stavrou, A. (2008) 'Universal Multi-Factor Authentication Using Graphical Passwords', *SITIS '08, IEEE International Conference on Signal Image Technology and Internet Based Systems.* Nov. 30 2008-Dec. 3 2008. pp. 625-632.

Schneegass, S., Steimle, F., Bulling, A., Alt, F. & Schmidt, A. (2014) 'SmudgeSafe: Geometric Image Transformations for Smudge-resistant User Authentication', *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing.* ACM, pp. 775-786.

Siadati, H., Gupta, P., Smith, S., Memon, N. & Ahamad, M. (2015) 'Fortifying Android Patterns using Persuasive Security Framework'. *The Ninth International Conference on Mobile Ubiquitous Computing (UBICOMM 2015).* Nice, France, pp 68-75.

Sobrado, L. & Birget, J.-C. (2002) 'Graphical passwords'.[in The *Rutgers Scholar, An Electronic Bulletin* for. *Undergraduate Research.* 4. Available at: http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm (Accessed:Sobrado, L. & Birget, J.-C.

Song, Y., Cho, G., Oh, S., Kim, H. & Huh, J. H. (2015) 'On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks', *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.* ACM, pp. 2343-2352.

Uellenbeck, S., Dürmuth, M., Wolf, C. & Holz, T. (2013) 'Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns', *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security.* ACM, pp. 161-172.

Von Zezschwitz, E., Dunphy, P. & De Luca, A. (2013) 'Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices', *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services.* ACM, pp. 261-270.

Weinshall, D. (2004) 'Secure Authentication Schemes Suitable for an Associative Memory'. *Hebrew University, Leibniz Center for Research in Computer Science. Technical Report TR,* 30

Weiss, R. & Luca, A. D. (2008) 'PassShapes: Utilizing Stroke Based Authentication to Increase Password Memorability'. *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges.* Lund, Sweden: ACM, pp 383-392.

Wiedenbeck, S., Waters, J., Sobrado, L. & Birget, J.-C. (2006) 'Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme', *Proceedings of the working conference on Advanced visual interfaces.* ACM, pp. 177-184.

Wu, T.-S., Lee, M.-L., Lin, H.-Y. & Wang, C.-Y. (2014) 'Shoulder-surfing-proof graphical password authentication scheme'. *International journal of information security*, 13 (3). pp 245-254.

Yesseyeva, E., Yesseyev, K., Abdulrazaq, M., Lashkari, A. & Sadeghi, M. (2014) 'Tri-Pass: A New Graphical User Authentication Scheme'. *International Journal of Circuits, Systems and Signal Processing*, 8 pp 61-67.

Zezschwitz, E. v., Luca, A. D., Janssen, P. & Hussmann, H. (2015) 'Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)lock Patterns'. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Seoul, Republic of Korea: ACM, pp 2339-2342.

Appendix B Images licences

Image License Note

All images displayed on this web site are the property of their respective owners. For security purposes we have summarized and grouped the images based on their license type to avoid any possible disclosure of the images used in this prototype for further protection from various types of security attacks such as 'phishing attack'.

Image Qty	License Type	BY
136	Free for personal use	Iconshock - http://www.iconshock.com
		Icons Land - http://www.icons-land.com
		Jesper Andersson - http://www.sortitoutsi.net
		Custom Icon Design - http://www.customicondesign.com
		Andrea Austoni **-** http://www.cutelittlefactory.com/
		Eighty8four **-** http://eighty8four.com
		TPDK design - http://blog.tpdkdesign.net/
		Artua - http://www.artua.com/
		Turbomilk - http://www.turbomilk.com
		Kyo Tux - http://kyo-tux.deviantart.com
		Bart Kowalski - http://bartkowalski.com/
		Icebabee - http://icebabee.deviantart.com/
		Artdesigner.lv - http://www.artdesigner.lv
		Babasse - http://babasse.deviantart.com
		Gakuseisean - http://gakuseisean.deviantart.com/
		Harwen Zhang - http://harwen.net/
		Jonas Rask - http://jonasraskdesign.com
		Itzik Gur - http://itzikgur.deviantart.com
		http://mebaze.com
		Everaldo Coelho - http://www.everaldo.com/
		Reynaldo Ramos - http://xenturion.deviantart.com/
		Google - http://www.google.com
		MayoSoft - http://mayosoft.deviantart.com
		Mike Beecham - http://mikebeecham.deviantart.com/
		Fasticon - http://www.fasticon.com/
		Ramotion - http://www.ramotion.com

		Tatice - http://tatice.deviantart.com/
109	**Free for commercial use**	Mysitemyway Design Team - http://icons.mysitemyway.com
		Icons Land - http://www.icons-land.com
		IconEden - http://www.iconeden.com
		Nishan Sothilingam
		I love colors - http://www.ilovecolors.com.ar/
		Sebastien Durel - http://www.crystalxp.net/galerie/en.id.3751-bagg-a-png.htm
		Aha-Soft
		Aleksandra Wolska - http://www.olawolska.com
		Dellustrations - http://dellustrations.com/work_icons.html
		Icojam - http://www.icojam.com
		Cyberella - http://www.cybertronical.com
		PC Unleashed - http://pcunleashed.com/
		Artdesigner.lv - http://www.artdesigner.lv
		Zen Nikki - http://zen-nikki.deviantart.com/
		IFA
		Rimshotdesign - http://rimshotdesign.com
		Media Design - http://mediadesign.deviantart.com
		IconBlock - http://www.iconblock.com/
		Bharathp666 - http://bharathp666.deviantart.com/
		Navdeep Raj - http://dezinerfolio.com
		Double-J designs - http://www.doublejdesign.co.uk/
		Ozturk - http://www.hadibe.com
		MazeNL77 - http://mazenl77.deviantart.com/
		Vlademareous - http://vlademareous.deviantart.com/
		Denis Sazhin
		Morcha - http://morcha.blogbus.com/logs/30886671.html
		Webdesigner Depot - http://www.webdesignerdepot.com
		LazyCrazy - http://lazycrazy.deviantart.com/
		DryIcons - http://dryicons.com

56	Creative Commons	Oxygen Team - http://www.oxygen-icons.org/
		Kidaubis Design - http://www.kidcomic.net
		IconFinder - http://www.iconfinder.net
		Mathieu - http://www.mat-u.com/
		Aha-Soft
		Kyo Tux - http://kyo-tux.deviantart.com
		VistaICO.com - http://www.vistaico.com
		Double-J designs - http://www.doublejdesign.co.uk/
		Limpa (Björn Lindberg) - http://www.limpa.net
		PCconsultants.co.uk - http://www.pcconsultants.co.uk
		Milanioom - http://milanioom.deviantart.com
		Wallpaper FX
		Kendra Schaefer - http://www.kendraschaefer.com
		Kyle Van Essen - http://kylevanessen.com/
		Pack Yuuyake - http://dunedhel.deviantart.com/art/Pack-Yuuyake-96029071
		Dunedhel - http://dunedhel.deviantart.com/
		Raadius - http://raadius.deviantart.com/
		Javier Aroche - http://www.javier-aroche.com/
		Neurovit - http://neurovit.deviantart.com
		r3dlink13 - http://r3dlink13.deviantart.com/
		Ahmad Hania
		Maja Bencic - http://www.fritula.hr
		Eray Zesen
		Omercetin - http://omercetin.deviantart.com/
		Interactivemania - http://www.interactivemania.com
		Svengraph - http://svengraph.deviantart.com
		Wwalczyszyn - http://wwalczyszyn.deviantart.com/
		Visual Pharm - http://icons8.com/
		Cyberchaos05 - http://cyberchaos05.deviantart.com
		BlueMalboro - http://bluemalboro.deviantart.com/art/Micro-Icon-Set-42295693
		Kidaubis - http://kidaubis.deviantart.com/
		Delacro - http://delacro.deviantart.com/
		Pica-ae - http://pica-ae.deviantart.com/
		Arrioch - http://arrioch.deviantart.com

41	Free for non commercial use	Oliver Scholtz (and others) - http://linux.softpedia.com/developer/Oliver-Scholtz-93.html
		Babasse - http://babasse.deviantart.com
		Aha-soft - http://www.aha-soft.com
		Louis Harboe - http://graphicpeel.com
		Susumu Yoshida - http://www.mcdodesign.com/
		Everaldo Coelho - http://www.everaldo.com/
		Tuziibanez - http://tuziibanez.deviantart.com
		Capital18 - http://capital18.deviantart.com
		Jommans - http://jommans.deviantart.com/
		Custom Icon Design - http://www.customicondesign.com
		Blackblurrr - http://blackblurrr.deviantart.com
		Seanau - http://www.seanau.com
		Nikolay Verin - http://ncrow.deviantart.com/
		Dan Wiersema - http://danwiersema.com
		PixelPirate - http://pixelpirate.deviantart.com
		Benbackman - http://benbackman.deviantart.com/
		Panoramix - http://panoramix-.deviantart.com/art/Xi4Dox-36612582
32	GPL	Alessandro Rei - http://www.kde-look.org/usermanager/search.php?username=mentalrey
		Sergio Sánchez López - http://www.kde-look.org/usermanager/search.php?username=Sephiroth6779
		Pavel InFeRnODeMoN - http://www.kde-look.org/usermanager/search.php?username=InFeRnODeMoN
		Lothar Grimme - http://www.grafixport.org
		Alexandre Moore - http://sa-ki.deviantart.com/
		New Mooon - http://code.google.com/u/newmooon/
		Walrick - http://walrick.deviantART.com
23	LGPL	Everaldo Coelho - http://www.everaldo.com/
		Alexandre Moore - http://sa-ki.deviantart.com/
		David Vignoni - http://www.icon-king.com/
		Marco Martin

Legal consultation about the licencing of using free images

Hi Hussain,

Yes, I did talk to him and he agreed with me that on the following conditions:

- This work was not on a public server, but only on an internal Plymouth Uni server
- It was being made as part of your personal research work within your education here at the university
- Was not being used in any commercial context
- That you gave credits to all providers of images within the appendices explaining that specific link could not be given due to security worries
- That you offered to remove any image, if the owner wished

There is no reason at all why you shouldn't continue to use the images in this way.

I look forwards to seeing it all working.

Good luck

Best wishes

EIB

****
Ed I Bremner
Digital Learning Environment Advocate
Associate Lecturer – Photography
e: ed.bremner@plymouth.ac.uk
m: 07973 335509
s: ed.bremner

If you are emailing about the DLE, send direct to dle.ah@plymouth.ac.uk
****

Appendix C List of invitation letters & Ethical approvals

1) Invitation letters
- **Online survey**

Subject: Invitation to participate in a survey

Dear,

You have been invited to participate in a survey.

The survey is titled:
"Survey of Authentication Mechanisms for Online Banking"

"The research is focused on the usable security within the field of user authentication in critical systems like financial institutes. These systems offer a variety of authentication mechanisms. Thus, the research aims to investigate the user experience with various types of user authentication methods in general and with online banking in particular besides understanding the attitudes of the users towards these authentication techniques."

To participate, please click on the following link:
https://www.cscan.org/surveys/index.php?sid=52849&lang=en

Sincerely,

Hussain Alsaiari (hussain.alsaiari@plymouth.ac.uk)

- **GOTPass experiment (User trials)**

<div style="border:1px solid black">

Invitation letter

Dear,

You have been invited to participate in a user trial as part of my PhD research "Graphical One-Time-Password authentication".

You will be kindly asked to come for **three** separate sessions at regular intervals as described below:

Session 1	Session 2	Session 3
Initial date	1 week later	1 month later

The trial will require you to use a graphical authentication system in 3 sessions for the duration of approximately 30 minutes in each session. The task involves registering with the system to create a new user account, and then using that account to login to the system for several times.

As part of the study, you will be asked to fill out online pre-test and post-test questionnaires that are used to investigate your views of the system in terms of security and usability. If you would like to participate, please sign up for your first session (please select one time slot only). Subsequent sessions will be on the same time slot in one week and one month time.

Participation is open to anyone aged 18 years or older with any level of computing abilities. Each participant will receive £5 for each 30 minutes of participation (3 sessions = **£15** in total) that is payable upon the completion of the study (end of session3).

To participate, please use the following link to sign up for the time slot as convenient:

http://www.signupgenius.com/go/10c0a4baaac2aabfc1-onetimegraphical

 LOCATION: Plymouth University | 3rd Floor Portland Square Building

</div>

- **Tear off flyer**

Earn £15

You are invited to participate in a user trial as part of a PhD research "Graphical One-Time-Password authentication".

You will be kindly asked to come for **three** separate sessions at regular intervals as described below:

Session 1	Session 2	Session 3
Initial date	1 week later	1 month later

Participation is open to anyone aged 18 years or older with any level of computing abilities. Each participant will receive £5 for each 30 minutes of participation (3 sessions = **£15** in total) that is payable upon the completion of the study (end of session3).

For more information and to participate, please use the following link or scan the QR code to sign up for the time slot as convenient:

http://qrs.ly/794hh5t

LOCATION: Plymouth University | Rolle 203

Sincerely,

Hussain Alsaiari | Principal Investigator

The Centre for Security, Communications and Network Research (CSCAN)

Plymouth University | Room A304 Portland Square Building

Office: +44 (0)1752 586287 | Email: hussain.alsaiari@plymouth.ac.uk

http://qrs.ly/794hh5t Email: hussain.alsaiari@plymouth.ac.uk	http://qrs.ly/794hh5t Email: hussain.alsaiari@plymouth.ac.uk	http://qrs.ly/794hh5t Email: hussain.alsaiari@plymouth.ac.uk	http://qrs.ly/794hh5t Email: hussain.alsaiari@plymouth.ac.uk	http://qrs.ly/794hh5t Email: hussain.alsaiari@plymouth.ac.uk	http://qrs.ly/794hh5t Email: hussain.alsaiari@plymouth.ac.uk	http://qrs.ly/794hh5t Email: hussain.alsaiari@plymouth.ac.uk	http://qrs.ly/794hh5t Email: hussain.alsaiari@plymouth.ac.uk	http://qrs.ly/794hh5t Email: hussain.alsaiari@plymouth.ac.uk

- **Supplementary Security experiment**

Dear Participant*,

I would like to invite you again to this additional GOTPass security experiment. This time, your physical attendance is not required; taking part in this study can be done at your end anywhere anytime.

The experiment is about a security attack called "Intersection Attack" which utilises the most frequently viewed images to determine the correct pass-images.

Your task: The attached file contains screenshots of 10 login attempts for a single GOTPass account. You are kindly requested to identify the most frequent images that are likely to be the correct pass-images in each login attempt. Note that the total pass-images for this account are 4, but the system displays only 2 random correct pass-images in each challenge grid. After identifying the pass-images, you will need also to determine the codes associated with each pass-image – TOP or LEFT.

Please write your answers on the tables below each challenge grid by specifying the image number and the code from top axis or left axis of each image. Once you complete your answers, please save your document in your name and send it back

to hussain.alsaiari@plymouth.co.uk or alternatively you can print a copy and fill it by hand and submit it in person to Hussain Alsaiari (PSQ - A304)

Wining conditions:

1. The break-in is considered successful when both pass-images and the associated codes are all correct.

2. To enter the prize draw, at least one successful attempt is required out of the total 10 attempts.

3. Successful participants will enter the prize draw and the winner will take the prize of £20 cash.

Submission Deadline: Midnight of Sunday 22 February 2015

Winner announcement: Tuesday 24 February 2015

Best Regards,

Hussain Alsaiari

* This participation is intended for those who already participated in the GOTPass user trials and are familiar with the system.

2) Ethical approvals

Faculty of Science and Technology

Smeaton 009, Plymouth

To:	Hussain Alsaiari	From:	Paula Simson
cc:	Dr Paul Dowland, Dr Maria Papadaki	Secretary to Human Ethics Committee	
Your Ref:		Our Ref:	scitech:\x:\human ethics:
Date:	13 May 2013	Phone Ext:	84503

<u>Application for Ethical Approval</u>

Thank you for submitting the ethical approval form and details concerning your project:

'Graphical One-Time-Password'

I am pleased to inform you that this has been approved.

Kind regards

Pᐧ imˢⁿ

Paula Simson

RESEARCH WITH PLYMOUTH UNIVERSITY

5 November 2014

CONFIDENTIAL
Hussain Alsairi
School of Computing and Mathematics

Dear Hussain

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

'Graphical One-Time-Password Authentication'

I am pleased to inform you that this has been approved.

Kind regards

Simson

Paula Simson
Secretary to Faculty Research Ethics Committee

cc. Dr Maria Papadaki

Appendix D List of questionnaires

1) User authentication experience online survey

Survey of Authentication Mechanisms for Online Banking

INFOSECURITY WITH PLYMOUTH UNIVERSITY

Centre for Security, Communications and Network Research (CSCAN)

This survey is being conducted for PhD research on "Authentication Mechanisms for Online Banking" at Plymouth University, United Kingdom. The survey aims to investigate the user experience with various types of user authentication methods in general and with online banking in particular. There are 5 main sections organized as follows:

1. Background/demographic - Overview of respondents' background, consisting of age, gender, education background, employment status, and computing skills.
2. Experience with user authentication - Analysis of experience of user authentication schemes and security-related techniques.
3. Participant's banking usage - Background information about respondents' banking activities.
4. Online banking experience - Analysing respondents' experience of authenticating to online banking system.
5. Opinions of alternative authentication - Analysis of users' acceptance level of the alternative authentication mechanisms.

Researcher details:
Hussain Alsaiari
Centre for Security, Communications and Network Research (CSCAN)
School of Computing and Mathematics
Plymouth University
Plymouth, PL4 8AA
United Kingdom
E-mail: hussain.alsaiari@plymouth.ac.uk

Project Supervisors:
Dr Maria Papadaki
Dr Paul Dowland
Prof. Steven Furnell

There are 29 questions in this survey.

A note on privacy
This survey is anonymous.
The record kept of your survey responses does not contain any identifying information about you unless a specific question in the survey has clearly asked for this. If you have responded to a survey that used an identifying token to allow you to access the survey, you can rest assured that the identifying token is not kept with your responses. It is managed in a separate database, and will only be updated to indicate that you have (or haven't) completed this survey. There is no way of matching identification tokens with survey responses in this survey.

There are 29 questions in this survey

Consent Form

Dear participants,

This survey is designed for adult participation. If you are UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY. Anyone 18 years old and above can take part in the survey and has the right to withdraw up until the final submission of their responses.
All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data. Should you have any questions about the study or you wish to receive a copy of the results, please contact the researcher Hussain Alsaiari via email or address below:

Researcher details:
Hussain Alsaiari
Centre for Security, Communications and Network Research (CSCAN)
School of Computing and Mathematics
Plymouth University
Plymouth, PL4 8AA
United Kingdom
Mail to: hussain.alsaiari@plymouth.ac.uk

If you have any concerns regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Technology Ethics Committee:
Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Technology
Plymouth University
Plymouth, PL4 8AA
United Kingdom
Phone:+44 (0)1752584503
Mail to: paula.simson@plymouth.ac.uk

** Only answer this questionnaire if you are 18 years old and above. If NOT, please quit the survey.**
Are you 18 years old and above?
*

Please choose **only one** of the following:

○ Yes

I understand that I am free to withdraw up until the point of submission of my responses and I confirm that I have read and understand the information given and agree to take part in the study? *

Only answer this question if the following conditions are met:
Answer was 'Yes' at question '1 [D1]' (Dear participants,   This survey is designed for adult participation. If you are UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY. Anyone 18 years old and above can take part in the survey and has the right to withdraw up until the final submission of their responses. All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data. Should you have any questions about the study or you wish to receive a copy of the results, please contact the researcher Hussain Alsaiari via email or address below: Researcher details: Hussain Alsaiari Centre for Security, Communications and Network Research (CSCAN) School of Computing and Mathematics Plymouth University Plymouth, PL4 8AA United Kingdom Mail to: hussain.alsaiari@plymouth.ac.uk If you have any concerns regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Technology Ethics Committee: Paula Simson 009, Smeaton, Drake Circus Faculty of Science and Technology Plymouth University Plymouth, PL4 8AA United Kingdom Phone:+44 (0)1752584503 Mail to: paula.simson@plymouth.ac.uk   ** Only answer this questionnaire if you are 18 years old and above. If NOT, please quit the survey.**   Are you 18 years old and above?)

Please choose **only one** of the following:

○ Agree

Section (1) - Demographic details about you

What is your age group (in years)? *

Only answer this question if the following conditions are met:
Answer was 'Agree' at question '2 [D2]' (I understand that I am free to withdraw up until the point of submission of my responses and I confirm that I have read and understand the information given and agree to take part in the study?)

Please choose **only one** of the following:

○ 18-29
○ 30-39
○ 40-49
○ 50-59
○ 60+

What is your gender? *

Please choose **only one** of the following:

○ Male
○ Female

What is your country of residence? *

Please choose **only one** of the following:

○ Drop-down country list
○ Other [   ]

What is your highest educational level? *

Please choose **only one** of the following:

○ Postgraduate (e.g Masters, PhD)
○ Higher education (e.g Bachelor Degree, HND, Diploma)
○ Further education (e.g Certificates, A-Levels, GNVQ)
○ Other [   ]

What is your employment status? *

Please choose **only one** of the following:

○ Employed
○ Self-employed
○ Student
○ Other [   ]

What is the level of your computer experience/knowledge? *

Please choose **only one** of the following:

○ Basic (beginner with limited skills)
○ Intermediate (broad range of skills covering a multitude of basic areas)
○ Advanced (specialist with a broad range of skills in a multitude of areas)

Section (2) - About your experience of user authentication

What type of 'alternative' authentication methods other than the traditional text-based password have you used?

Examples of some alternative authentication methods:

	Biometrics		Hardware-based
Fingerprint recognition	**Facial recognition**	**ATM Card (Chip & PIN)**	**One-Time-Password token**

*

Please choose **all** that apply:

☐ None - never used any alternative authentication methods

☐ Fingerprint recognition

☐ Facial recognition

☐ ATM Card (Chip & PIN)

☐ One-Time-Password token

☐ N/A - I do not want to share this information

☐ Other: _____

How important is using multiple layers of authentication to ensure better security?

iii	One-Time-Password (Dynamic password for each login attempt)
ii	Personal Verification Questions (mother's maiden name, favourite author)
i	Secret Knowledge (Username & Password)

*

Please choose **only one** of the following:

○ Very Important

○ Important

○ Moderately Important

○ Of Little Importance

○ Unimportant

○ Not sure

Why do you not prefer using multiple layers of authentication? *

Only answer this question if the following conditions are met:
Answer was at question '10 [B5]' (How important is using multiple layers of authentication to ensure better security?   )

Please choose the appropriate response for each item:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Complicated	○	○	○	○	○
Impractical	○	○	○	○	○
I see no value in using it	○	○	○	○	○

What do you think about carrying around several security devices like tokens for multiple accounts authentication?

Example:
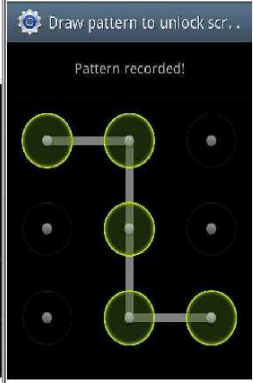
*

Please choose the appropriate response for each item:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Not Sure
I think it is convenient	○	○	○	○	○	○
I think it is necessary	○	○	○	○	○	○
I think it is acceptable on balance	○	○	○	○	○	○

Images/pictures/drawings have been used as a form of user authentication approach, which form have you ever heard of or know about?

* Graphics-based authentication comes in different forms:

- _Recognition-based:_ where a set of images is displayed to the user who needs to identify the pre-chosen pass-images (pictorial password) from among other decoy images.	- _Draw-based:_ user needs to reproduce the previously drawn picture/shape password.	- _Click-based:_ user is presented with images and asked to click on certain (pre-set) images click points.

*

Please choose **all** that apply:

☐ Never heard of these techniques

☐ Recognition-based

☐ Draw-based

☐ Click-based

Section (3) – About your banking usage

Which answer best reflects the number of online banking accounts you are using?

Example of online banking login screen:

Log on to Personal Internet Banking

Please enter your user ID eg IB1234567890 or John123

[ ] **Continue**

☐ Remember my user ID ⑦ Forgotten your user ID?

*

Please choose **only one** of the following:

○ None - I do not use online banking

○ One

○ 2-5

○ 6-9

○ 10+

○ N/A - I do not wish to share this information

Why do you not use online banking? *

Only answer this question if the following conditions are met:
Answer was 'None - I do not use online banking' at question '14 [C20]' (Which answer best reflects the number of online banking accounts you are using? Example of online banking login screen:)

Please choose **all** that apply:

☐ I don not have a bank account

☐ My bank does not offer online banking

☐ Lack of familiarity with the technology

☐ Concerns over the security provided online

☐ Lack of trust in online banking

☐ Inconvenience/usability issues with the technology

☐ Prefer to conduct financial transactions in person

☐ Other: [   ]

How often do you use your online banking system? *

Only answer this question if the following conditions are met:
Answer was 'One' *or* '2-5' *or* '6-9' *or* '10+' at question '14 [C20]' (Which answer best reflects the number of online banking accounts you are using? Example of online banking login screen:)

Please choose **only one** of the following:

○ Regularly (e.g daily, weekly)

○ Occasionally (e.g couple of times a month)

○ Rarely (e.g every few months)

○ Not sure

○ Other [   ]

For what purposes do you use online banking services? *

Please choose **all** that apply:

- ☐ Checking bank account information/transaction
- ☐ Updating personal information (address, contacts)
- ☐ Performing some non-transactional tasks (order cheque books, notify of lost cards)
- ☐ Utilizing a variety of online payment services (bills, fund transfer, credit card)
- ☐ Other: _____

Section (4) - About your online banking experience

Does your online banking system require multi-factor authentication?

* A multi-factor authentication is a composite authentication mechanism of more than one form of identity verification such as
Something you know + Something you have (Textual password + Token)
or Something you are + Something you know (Fingerprint + PIN)

Example:
Customer ID & Password (something you know) + One-Time-Password (something you have).

*

Only answer this question if the following conditions are met:
Answer was NOT 'None - I do not use online banking' at question '14 [C20]' (Which answer best reflects the number of online banking accounts you are using? Example of online banking login screen:)

Please choose **only one** of the following:

○ Yes

○ No

What types of One-Time-Password authentication are offered by your online banking system?

* A One-Time-Password (OTP) is a randomly generated password valid for a single use, producing a unique password for each login session or transaction. That means that the user will end up using different dynamic passwords for each and every login attempt. It can be delivered by either a security token, SMS text message, or soft token (software application).

Examples of One-Time-Password (OTP) types:

Security OTP token (Hardware)	OTP SMS text message	OTP soft token (Software)

*

Only answer this question if the following conditions are met:
Answer was NOT 'None - I do not use online banking' at question '14 [C20]' (Which answer best reflects the number of online banking accounts you are using? Example of online banking login screen:)

Please choose **all** that apply:

☐ None - the online banking system does not facilitate a One-Time-Password

☐ Security token device (Hardware)

☐ SMS text message

☐ Soft token (Software)

☐ Other: _____

How do you rate your experience of using a One-Time-Password? *

Please choose **only one** of the following:

○ Very Satisfied

○ Satisfied

○ Neutral

○ Dissatisfied

○ Very Dissatisfied

How many times have you failed to login using multi-factor or One-Time-Password authentication since you started using it? *

Please choose **only one** of the following:

○ Never

○ Rarely

○ Sometimes

○ Frequently

What was the cause of the failure? *

Please choose **all** that apply:

☐ Mistyped the code

☐ Lost token/Mobile

☐ Forgotten token/Mobile

☐ Lack of mobile service (i.e. no mobile signal coverage for SMS text message)

☐ Token/Software failure issues

☐ Other: _____

In your opinion, what is likely to be the biggest potential problem that might prevent a successful multi-factor or One-Time-Password login attempt? *

Please choose **all** that apply:

☐ Mistyped the code

☐ lost token/Mobile

☐ Forgotten token/Mobile

☐ Lack of mobile service (i.e. no mobile signal coverage for SMS text message)

☐ Token/Software failure issues

☐ Other: _____

Section (5) - Your opinions of alternative authentication mechanisms

Some online banking systems have started to implement a visual secret image technique as an assurance for their customers that they are accessing a legitimate online banking website.
With a visual secret image, the user verifies the legitimacy of the visited website through the observation of the correct self-selected image presented by the website.

Example:

Your Image:

Your Phrase:
End of day time!!!

NOTE:
If you do not recognize your security image and personal phrase, do not proceed to access your account.

Do you agree that utilizing images in this manner can enhance system security?

*

Please choose **only one** of the following:

○ Strongly Agree
○ Agree
○ Neutral
○ Disagree
○ Strongly Disagree

Do you like/accept the idea of replacing or supplementing the existing one-time-password methods with a *one-time graphical password* to avoid the need to carry around an additional security device or to help in situations where the security token is unavailable?

* For illustration, one-time graphical password can be simply described in the following model where users recognise their pre-chosen images and obtain the one-time-password associated with each image:

9543	1109	3443
6501	9954	3217
7429	5478	8432

Authentication steps:

1. Pre-chosen password images are displayed among other decoys.
2. Random One-Time-Code is associated with every image.
3. Recognise/Identify password images.
4. Obtain the associated codes.
5. Enter the obtained code in the verification field.

*

Please choose **only one** of the following:

○ Strongly Accept
○ Accept
○ Neutral
○ Reject
○ Strongly Reject

Would you be confident to use the alternative graphical authentication method in online banking? *

Please choose **only one** of the following:

○ Very Confident

○ Confident

○ Neutral

○ Un-confident

○ Very Un-confident

Why would you not feel confident using the alternative graphical authentication method in online banking? *

Only answer this question if the following conditions are met:
Answer was 'Very Un-confident' *or* 'Un-confident' at question '26 [D2]' (Would you be confident to use the alternative graphical authentication method in online banking?)

Please choose **all** that apply:

☐ Insecure

☐ Impractical

☐ Unfamiliar

☐ Not a widely adopted method

☐ Other: _____

Will fixing the issues you identified above help in changing your mind to accept and use the proposed alternative graphical authentication method? *

Only answer this question if the following conditions are met:
Answer was 'Very Un-confident' *or* 'Un-confident' at question '26 [D2]' (Would you be confident to use the alternative graphical authentication method in online banking?)

Please choose **only one** of the following:

○ Yes

○ No

○ Not sure

○ Other _____

How would you prefer to use the proposed alternative *one-time graphical password authentication* beside the secret knowledge (text-based password) in online banking system? *

Only answer this question if the following conditions are met:

-------- Scenario 1 --------

Answer was 'Neutral' *or* 'Confident' *or* 'Very Confident' at question '26 [D2]' (Would you be confident to use the alternative graphical authentication method in online banking?)

-------- or Scenario 2 --------

Answer was 'Yes' at question '28 [D4]' (Will fixing the issues you identified above help in changing your mind to accept and use the proposed alternative graphical authentication method?)

Please choose **only one** of the following:

○ as a replacement for the existing (primary) one-time-password authentication (token, SMS, Soft token)

○ as a secondary (supplementary) one-time-password authentication to be used only when needed (e.g. primary one-time-password method is unavailable)

○ Not sure

○ Other _____

Thank you for completing this questionnaire.

Your participation is highly appreciated and your responses are valuable to us.

Submit your survey.
Thank you for completing this survey.

2) GOTPass Pre-test questionnaire

Pre-test Questionnaire: Graphical One-Time-Password Authentication

Centre for Security, Communications and Network Research (CSCAN)

This survey is being conducted for PhD research on "Graphical One-Time-Password Authentication" at Plymouth University, United Kingdom.

The survey aims to investigate the user experience and behaviour with various types of user authentication methods. There are 2 main sections organized as follows:

1. Background/demographic - Overview of respondents' background consisting of age, gender, education background, employment status.
2. Experience with user authentication - Analysis of respondents' computing experience, password-related behaviours, and authentication schemes.

Principal investigator details:
Hussain Alsaiari
Centre for Security, Communications and Network Research (CSCAN)
School of Computing and Mathematics
Plymouth University
Plymouth, PL4 8AA
United Kingdom
E-mail: hussain.alsaiari@plymouth.ac.uk

Project Supervisors:
Dr Maria Papadaki
Dr Paul Dowland
Prof. Steven Furnell

There are 12 questions in this survey.

A note on privacy
This survey is anonymous.
The record kept of your survey responses does not contain any identifying information about you.

There are 13 questions in this survey

Consent Form

Dear participants,

You can kindly take part in the survey and has the right to withdrawat anytime. All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Data will be presented in such a way that your identity cannot be connected with specific published data. Should you have any questions about the study or you wish to receive a copy of the results, please contact the principal investigator Hussain Alsaiari via email or address below:

Principal Investigator details:
Hussain Alsaiari
Centre for Security, Communications and Network Research (CSCAN)
School of Computing and Mathematics
Plymouth University
Plymouth, PL4 8AA
United Kingdom
Email to: hussain.alsaiari@plymouth.ac.uk

If you have any concerns regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Eenvironment Ethics Committee:

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Technology
Plymouth University
Plymouth, PL4 8AA
United Kingdom
Phone:+44 (0)1752584503
Email to: paula.simson@plymouth.ac.uk

I confirm that I am 18 years old or above and I understand that I am free to withdraw at anytime?
*

Please choose **only one** of the following:

○ Yes

Section (1) - Demographic details about you

What is your age group (in years)? *

Please choose **only one** of the following:

○ 18-29
○ 30-39
○ 40-49
○ 50-59
○ 60+

What is your gender? *

Please choose **only one** of the following:

○ Male
○ Female

What is your country of residence? *

Please choose **only one** of the following:

○ Drop-down country list
○ Other [   ]

What is your highest educational level? *

Please choose **only one** of the following:

○ Postgraduate (e.g Masters, PhD)
○ Higher education (e.g Bachelor Degree, HND, Diploma)
○ Further education (e.g Certificates, A-Levels, GNVQ)
○ Other [   ]

What is your employment status? *

Please choose **only one** of the following:

○ Employed
○ Self-employed
○ Student
○ Other [   ]

Section (2) - About your experience of user authentication

What is the level of your computer experience/knowledge? *

Please choose **only one** of the following:

○ Basic (beginner with limited skills)

○ Intermediate (broad range of skills covering a multitude of basic areas)

○ Advanced (specialist with a broad range of skills in a multitude of areas)

How many passwords do you have to remember? *

Please choose **only one** of the following:

○ 1 - 5

○ 6 - 10

○ 11 - 15

○ 16 or more

○ Not sure

How do you manage multiple passwords?

(Examples: Reuse the same password for multiple accounts, Use a significant dates, such as a birth date, Writing passwords down, Save passwords in text note on my computer or mobile phone, Save passwords in browsers, Use password manager software, Include the website name in each password, etc.)

*

Please write your answer here:

Which techniques do you usually use when creating your password?

(Examples: Easy to remember, Difficult for others to guess, The same as another password I currently have, etc.)

*

Please write your answer here:

307

What types of One-Time-Password authentication have you ever used?

* A One-Time-Password (OTP) is a randomly generated password valid for a single use, producing a unique password for each login session or transaction. That means that the user will end up using different dynamic passwords for each and every login attempt. It can be delivered by either a security token, SMS text message, or soft token (software application).

Examples of One-Time-Password (OTP) types:

Security OTP token (Hardware)	OTP SMS text message	OTP soft token (Software)

*

Please choose **all** that apply:

☐ None - never used One-Time-Password

☐ Security token device (Hardware)

☐ SMS text message

☐ Soft token (Software)

☐ Other: _____

How do you rate your experience of using a One-Time-Password? *
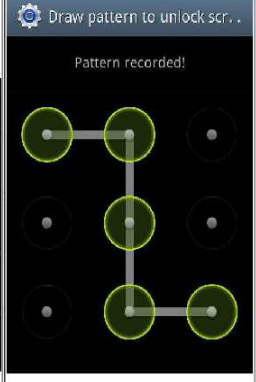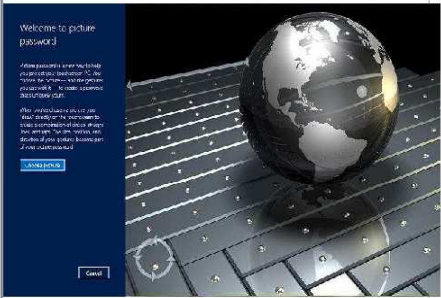
Only answer this question if the following conditions are met:
Answer was at question '11 [B3]' (What types of One-Time-Password authentication have you ever used? * A One-Time-Password (OTP) is a randomly generated password valid for a single use, producing a unique password for each login session or transaction. That means that the user will end up using different dynamic passwords for each and every login attempt. It can be delivered by either a security token, SMS text message, or soft token (software application). Examples of One-Time-Password (OTP) types: Security OTP token (Hardware) OTP SMS text message OTP soft token (Software)   )

Please choose **only one** of the following:

○ Very Satisfied

○ Satisfied

○ Neutral

○ Dissatisfied

○ Very Dissatisfied

Images/pictures/drawings have been used as a form of user authentication approach, which form have you ever heard of or know about?

* Graphics-based authentication comes in different forms:

- _Recognition-based:_ where a set of images is displayed to the user who needs to identify the pre-chosen pass-images (pictorial password) from among other decoy images.	- _Draw-based:_ user needs to reproduce the previously drawn picture/shape password.	- _Click-based:_ user is presented with images and asked to click on certain (pre-set) images click points.

*

Please choose **all** that apply:

☐ Never heard of these techniques

☐ Recognition-based

☐ Draw-based

☐ Click-based

Thank you for completing this questionnaire.

Your participation is highly appreciated and your responses are valuable to us.

Submit your survey.
Thank you for completing this survey.

3) GOTPass Post-test questionnaire

Post-test Questionnaire: Graphical One-Time-Password Authentication

INFOSECURITY WITH PLYMOUTH UNIVERSITY

Centre for Security, Communications and Network Research (CSCAN)

This survey is being conducted for PhD research on "Graphical One-Time-Password Authentication" at Plymouth University, United Kingdom.

The survey aims to investigate the user acceptance of the new proposed authentication system from both aspects of secuirty and usability. There are 5 main sections organized as follows:

1. Training/Instruction - Ask about the effectiveness of the way the study was presented.
2. Usability aspects - Analysis of the user experience of various usability factors.
3. Security aspects- Investigate how secure the system is from the respondents' view points.
4. Design aspects - Analyse respondents' experience of the system's design.
5. Overall opinions - Analysis of the overall users' acceptance level of the proposed authentication mechanism.

Principal investigator details:
Hussain Alsaiari
Centre for Security, Communications and Network Research (CSCAN)
School of Computing and Mathematics
Plymouth University
Plymouth, PL4 8AA
United Kingdom
E-mail: hussain.alsaiari@plymouth.ac.uk

Project Supervisors:
Dr Maria Papadaki
Dr Paul Dowland
Prof. Steven Furnell

There are 35 questions in this survey.

A note on privacy
This survey is anonymous.
The record kept of your survey responses does not contain any identifying information about you.

There are 36 questions in this survey

Consent Form

Dear participants,

You can kindly take part in the survey and has the right to withdrawat anytime. All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Data will be presented in such a way that your identity cannot be connected with specific published data. Should you have any questions about the study or you wish to receive a copy of the results, please contact the principal investigator Hussain Alsaiari via email or address below:

<div align="center">

Principal Investigator details:
Hussain Alsaiari
Centre for Security, Communications and Network Research (CSCAN)
School of Computing and Mathematics
Plymouth University
Plymouth, PL4 8AA
United Kingdom
Email to: hussain.alsaiari@plymouth.ac.uk

</div>

If you have any concerns regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Eenvironment Ethics Committee:

<div align="center">

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Technology
Plymouth University
Plymouth, PL4 8AA
United Kingdom
Phone:+44 (0)1752584503
Email to: paula.simson@plymouth.ac.uk

</div>

I confirm that I am 18 years old or above and I understand that I am free to withdraw at anytime?
*

Please choose **only one** of the following:

◯ Yes

Section (A) - Training/Instructions

Learning how to use this system was simple.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

The support information (such as guide book, on-screen messages and other documentation) provided with this system was clear and understandable. *

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

The support information was effective in helping me completing the tasks (Registration & Login). *

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

Section (B) - About the usability aspects

It was easy to create my GOTPass account (Registration phase).
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

Logging in using GOTPass was easy.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

I was able to complete the required tasks quickly.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

It was difficult to enter my GOTPass even though I thought I remembered it.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

If I didn't login to my account for a few weeks, I would still remember my password.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

Rate each part of your GOTPass based on what you think might cause the remembrance/recall difficulty?

('0' is No impact and '5' is the highest impact on memorability)

*

Please choose the appropriate response for each item:

	(0) No Impact	(1) Low Impact	(2)	(3) Average Impact	(4)	(5) High Impact
Username	○	○	○	○	○	○
Unlock pattern	○	○	○	○	○	○
Pass-images	○	○	○	○	○	○
GOTPass input format (Code location)	○	○	○	○	○	○

This authentication method would become easier and quicker to use after gaining experience (practice).
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

Using keyboard as an input means with graphical password scheme seems:
*

Please choose the appropriate response for each item:

	(1) Strongly Agree	(2)	(3)	(4) Neutral	(5)	(6)	(7) Strongly Disagree
Convenient	○	○	○	○	○	○	○
Practical	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○

Using unlock pattern on the web was:
*

Please choose the appropriate response for each item:

	(1) Strongly Agree	(2)	(3)	(4) Neutral	(5)	(6)	(7) Strongly Disagree
Convenient	○	○	○	○	○	○	○
Practical	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○

Section (C) - About the security aspects

I would trust GOTPass system to secure my accounts.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

My GOTPass is unlikely to have any meaning to other people.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

This type of authentication would be easy for attackers to guess.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

If I briefly explain to my partner/close friend what my GOTPass secrets are, I think they will still have difficulty reproducing my GOTPass correctly.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

I think that the ambiguity of the feedback, when a wrong username or pattern is entered, is a good security practice.

(The system gives no indication during entering login information whether it is correct or wrong until after the final submission when the system shows the final result (successful or failed) login attempt without specifying where was the mistake if there was any.)

*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

Rate the impact level of each part of your GOTPass on increasing the security:

('0' is No impact and '5' is high)

*

Please choose the appropriate response for each item:

	(0) No Impact	(1) Low Impact	(2)	(3) Average Impact	(4)	(5) High Impact
Username	○	○	○	○	○	○
Unlock pattern	○	○	○	○	○	○
Pass-images	○	○	○	○	○	○
GOTPass input format (Code location)	○	○	○	○	○	○

Section (D) - About the design aspects

The number of pattern nodes (16) on a matrix of size (4x4) was:
*

Please choose **only one** of the following:

○ High

○ Adequate

○ Low

The number of images within each theme (30/theme) in the registration page was:
*

Please choose **only one** of the following:

○ High

○ Adequate

○ Low

The number of images (16) on a matrix size (4x4) in the login page was:
*

Please choose **only one** of the following:

○ High

○ Adequate

○ Low

The number of pass-images (4 images) that users need to remeber was:
*

Please choose **only one** of the following:

○ High

○ Adequate

○ Low

I think randomizing (shuffling) images locations on the grid has (……………….) on performance (longer time to identify pass-images) *

Please choose **only one** of the following:

○ Slight effect

○ No effect

○ Major effect

I feel that the implementation of variable response through pass-images portfolio (register 4 images as full pass-image bundle and use only 2 of them randomly in each authentication session) has added:
***

Please choose **only one** of the following:

○ Security

○ Complexity

○ Both Security & Complexity

○ Not Sure

Assigning the image themes by the system was:
***

Please choose **only one** of the following:

○ Convenient

○ No effect

○ Inconvenient

Partial assigning of the GOTPass input format (code location) by the system was:

(Based on the user selection of the security level, the system assigns the user with one of the two options available in each security level randomly)

***

Please choose **only one** of the following:

○ Convenient

○ No effect

○ Inconvenient

I think using mouse click to select pass-images can provide more: *

Please choose **only one** of the following:

○ Security

○ Convenience

○ Both Security & Convenience

○ Not Sure

**I think it would be more <u>secure </u>if the system generates
***

Please choose **only one** of the following:

○ Numeric codes

○ Alphabetic codes

○ Alphanumeric codes

**I think it would be more <u>usable </u>if the system generates
***

Please choose **only one** of the following:

○ Numeric codes

○ Alphabetic codes

○ Alphanumeric codes

**The length of the GOTPass code (8 characters long) was:
***

Please choose **only one** of the following:

○ Short

○ Adequate

○ Long

322

Section (E) - Your overall opinion

This system has the functions and capabilities I expect it to have.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

Using GOTPass system was convenient.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

I would use GOTPass confidently.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

I think GOTPass can be used for sensitive web authentication.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

Overall, I am satisfied with GOTPass system.
*

Please choose **only one** of the following:

○ (1) Strongly Agree

○ (2)

○ (3)

○ (4) Neutral

○ (5)

○ (6)

○ (7) Strongly Disagree

Thank you for completing this questionnaire.

Your participation is highly appreciated and your responses are valuable to us.

Submit your survey.
Thank you for completing this survey.

1) Briefing document for the user experiment

Graphical One-Time-Password (GOTPass)
Briefing document for potential participants in user trial
Hussain Alsaiari
hussain.alsaiari@plymouth.ac.uk
Centre for Security, Communications and Network Research (CSCAN),
School of Computing and Mathematics,
Plymouth University

About the research:

The main objective of this research is to investigate the usability and security of a graphical authentication method, which provides possible alternatives to traditional username/password authentication.

What you are required to do?

In this trial, you are kindly requested to use a graphical authentication system by simply creating a new user account and then use it to sign back into the system. The authentication task will involve entering a username, redrawing the unlock pattern, remembering the images that you chose within the given themes, and finally entering the OTP code in the correct pre-chosen format. The study involves three separate sessions distributed on first day, one week later, and after one month.

Below is the series of the main tasks you need to perform on each session:

D. Initialization session (Day 1)

1) Register and confirm your username, unlock pattern, pass-images, OTP input format. (web application)

2) Answer a pre-test questionnaire. (online survey)

3) Login using your GOTPass credential. (web application)

E. Follow-up session (Week later)

    1) Login using your GOTPass credential. (web application)

F. Final session (Month later)

    1) Login using your GOTPass credential. (web application)

    2) Answer a post-test questionnaire. (online survey)

The process flow of the required tasks is as follows:

For the **registration task**, you are required to create a new account by entering a unique username, drawing an unlock pattern shape, selecting 4 password images from 4 different system assigned themes, and lastly choosing one option of 4 available OTP input format. This authentication approach does not require you to remember the sequence of your password images. Please be noted that writing your password components down is unsecure practice.

Before proceeding to the Login task, you need to **answer a pre-test questionnaire**. The purpose of doing this activity is to provide you with a divider time between the registration and the login task.

During the **Login task**, you are requested to login by providing the correct username, redraw the unlock pattern, then the system will display a 4x4 grid that contains random 2 password images out of your 4 previously chosen images, which you will need to identify and enter the associated OTP axis code as per the registration.

The login conditions will be as follows:

- 5 consecutive correct authentication tries > Successfully completed this session
- 5 total incorrect attempts > receive the guide booklet or play the video demo, then restart again

Finally, at the end of last session you will receive a **post-test questionnaire** (Impression & Opinion).

Notes:

- You are recommended to go through the training (guide booklet/ video demo) before starting your trial as it will provide a clearer idea on how the new method works.
- Please avoid clicking on the pass-images, just mentally locate them and map them to the right pre-chosen axis of the OTP code.

How long will it take?

The total amount of time will depend upon your experiences with the new method, but on average each trial session requires no more than 40 minutes.

What will the results of the study be used for?

The result of this trial will contribute towards PhD research that proposes an alternative authentication method, with the ultimate aim to enhance any current problems.

All results from this trial will be used and reported anonymously in the ongoing research. You will be given an opportunity to find out the results of this trial by asking for a copy of the findings to be emailed to you after the full study has been conducted and analysed.

Any further enquiries about how the study has been conducted, do not hesitate to contact the Secretary, Faculty of Science and Environment Research Ethics Committee, **Mrs Paula Simson** at **paula.simson@plymouth.ac.uk**

Thank you very much indeed for your time and kind participation.

2) **Task sheet for Guessing attack study**

Guessing attack

In this type of attack, attackers will try to guess the authentication secret of a legitimate user. In recognition-based authentication, "Prioritised guessing attacks" aims to increase the probability of selecting the correct image through the prioritisation of the more commonly selected images.

Task: You will be provided some information about the user account that you will be required to guess the password of that account.

In order to validate your guessing, you will be given the chance to use the GOTPass system and try to login with the information you managed to guess. The allowed attempts will be limited to 5 unless you think that you can manage to succeed if you were given more chances.

Account information:

Username:	**guesscscan**
Pattern:	**shape of number 2**

Pass-images themes:	**flag, stationery, computer, paint**
Input format:	**Basic security level** (both numeric codes are form same axis – Top/Left)

Guessing attack experiment (observation form)

Date	Time	

Attempt # 1		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 2		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 3		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 4		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 5		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

What do you think might made GOTPass hard to guess?

Pattern shape		Pattern start point & direction		
image shuffling		dynamic pass-images		
input format		other		

Do you have any interest in breaking in this system (for further research)?

3) Task sheet for Intersection attack study

Intersection attack

Intersection attack is possible when the role of an image as either a pass-image or a distractor can be determined by the frequency of its appearance at login. That in turn allow the attacker to use the most frequently viewed images to pass the challenge screen and gain access.

Task: You will be displayed a video of screen capturing the login attempts for 3 times. You are allowed to take notes while watching the video to help you gather information about the user account that you will be required to login with the information of that account.

In order to validate your captured information, you will be given the chance to use the GOTPass system and try to login with the information you managed to gather. The allowed attempts will be limited to 5 unless you think that you can manage to succeed if you were given more chances.

Intersection attack experiment (observation form)

Date	Time	

Attempt # 1

Username		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 2

Username		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 3

Username		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 4

Username		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 5

Username		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

What do you think might made GOTPass hard to capture?

image shuffling		input format	
dynamic pass-images		other	

Do you have any interest in breaking in this system (for further research)?

4) Task sheet for Shoulder-surfing attack study

Shoulder-Surfing attack

When authenticating in public places, shoulder surfing become of special concern since it enables attacker to capture individual's password by direct observation or by recording the entire authentication session.

Task: You will be displayed a video of login attempts being captured while an individual was entering authentication information for 3 times. You are allowed to take notes while watching the video to help you gather information about the user account that you will be required to login with the information of that account.

In order to validate your captured information, you will be given the chance to use the GOTPass system and try to login with the information you managed to gather. The allowed attempts will be limited to 5 unless you think that you can manage to succeed if you were given more chances.

Shoulder-Surfing attack experiment (observation form)

Date	Time	

Attempt # 1

Username		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 2

Username		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 3

Username		
Pattern		
1st pass-image		
2nd pass-image		
1st code		
2nd code		

Attempt # 4		
Username		
Pattern		
1ˢᵗ pass-image		
2ⁿᵈ pass-image		
1ˢᵗ code		
2ⁿᵈ code		

Attempt # 5		
Username		
Pattern		
1ˢᵗ pass-image		
2ⁿᵈ pass-image		
1ˢᵗ code		
2ⁿᵈ code		

What do you think might made GOTPass hard to capture?

image shuffling		input format		
dynamic pass-images		other		

Do you have any interest in breaking in this system (for further research)?

Intersection Attack Experiment #2

Introduction: Intersection attack is possible when the role of an image as either a pass-image or a distractor can be determined by the frequency of its appearance at login. That in turn allow the attacker to use the most frequently viewed images to pass the challenge screen and gain access.

Task: You will be presented with screenshots of 10 login attempts for a single GOTPass account. You are kindly requested to identify the most frequent images likely to be the correct pass-images in each login attempt. Note that the total pass-images for this account is 4, but the system displays only 2 random correct pass-images in each challenge grid. After identifying the pass-images, you will need also to determine the codes associated with each pass-image – TOP or LEFT, as per the following options:

    Option one: 1st pass-image (TOP) + 2nd pass-image (TOP)

    Option two: 1st pass-image (LEFT) + 2nd pass-image (LEFT)

    Option three: 1st pass-image (TOP) + 2nd pass-image (LEFT)

    Option four: 1st pass-image (LEFT) + 2nd pass-image (TOP)

Please write your answers on the tables below each challenge grid by specifying the image number and the code from top axis or left axis of each image. Once you complete your answers, please save your document in your name and send it to hussain.alsaiari@plymouth.ac.uk or alternatively you can print a copy and fill it by hand and submit it in person to Hussain Alsaiari (PSQ - A304)

Login Session #1

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

1. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Login Session #2

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

2. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Login Session #3

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

3. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Login Session #4

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

4. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Login Session #5

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

5. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Login Session #6

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

6. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Login Session #7

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

7. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Login Session #8

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

8. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Login Session #9

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

9. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Login Session #10

	1111	2222	3333	4444
5555	1	2	3	4
6666	5	6	7	8
7777	9	10	11	12
8888	13	14	15	16

10. What are the pass-images and their codes?			
Pass-image #1		Code #1	
Pass-image #2		Code #2	

Appendix F Implementations of GOTPass prototype

1) **GOTPass Registration & Login user guides**

   A. Registration guide

Graphical One Time Password System

GOTPass

Type in your full name

Registration: Step 1 - Username Selection , Step 2 - Pattern Drawing

Full Name
Enter your name

Test Guide Account

User Name
Choose a user name

test_acc

Type in your username that will identify your account

Pattern Unlock: Draw a pattern of your choice then click on "Register Pattern" button

Draw an unlock pattern shape by connecting nodes together

Back   **Register Pattern**
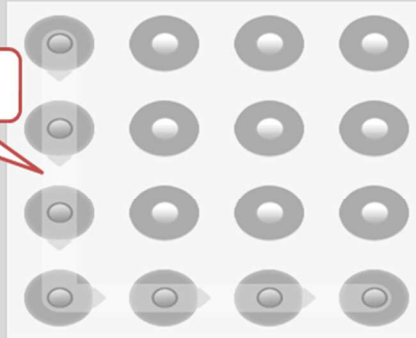
Once you complete the required fields, click on register pattern button

If you need to clear everything in the page and start over, click on reset button

Reset

Registration - Image Selection - Step 3

The random selected theme is : **Animal**

This is the 1st theme assigned to you randomly by the system

Please select one preferable image from each theme by clicking on it.

Back

Choose & click on one image from the displayed images

Registration - Image Selection - Step 3

The random selected theme is : **Sport**

Please select one preferable image from each theme by clicking on it.

This is to confirm the image you have selected as your 2nd password image

This image has been selected to be one of your password images. Would you like to add it to your images portfolio?

Yes, select next password image   Cancel

If you like the image then click on this button, otherwise click cancel

You have already added **1 image**. Please select next image for your password images portfolio
* Total number of password images required is 4 images

Back

Registration - Image Selection - Step 3

The random selected theme is : **Clock**

This is the 3rd theme assigned to you randomly by the system

Please select one preferable image from each theme by clicking on it.

Choose & click on one image from the displayed images

You have already added **2 image**. Please select next image for your password images portfolio
* Total number of password images required is 4 images

Back

Registration - Image Selection - Step 3

The random selected theme is : Food

Please select one preferable image from each theme by clicking on it.

This is to confirm the image you have selected as your 4th and final password image

This image has been selected to be one of your password images. Would you like to add it to your images portfolio?

Yes, Go to next step   Cancel

If you like the image then click on this button to move to the next step, otherwise click cancel

You have already added 3 images. Please select next image for your password images portfolio
* Total number of password images required is 4 images

Back

Registration - GOTPass Input Format - Step 4

Instructions:
- The position of your pass-images in the grid will be used to indicate a code that you need to enter using the keypad/keyboard.
- The GOTPass codes are located on Top or Left axis of each of your pass-images.
- There are 2 security levels options which you can choose from.

There are two security levels to choose from: Basic or Advance

○ Basic Security Level   ○ Advanced Security Level

Numeric codes for both images are taken from the same axis.   Numeric codes are taken from a different axis for each image.

Your assigned input format & an example for illustration:

Option one: Type the 4-digit code for your 1st pass-image from the TOP axis and the code for your 2nd pass-image from the TOP axis

(2) 6501   3217   1109 (1)   2357

Identify your pass-images by navigating through the grid from LEFT to RIGHT (→) starting from TOP LEFT image down to the BOTTOM (↓).

This displays the input format that was assigned to you based on your selection of the security level options

Your selected pass-images are:

This displays the password images you selected in the previous section

Click on submit button to create your account

Back   Submit

B. Login guide

2) GOTPass Database

Database Design Document

Introduction

This document describes the database design, data model, and database interfaces. The scope of this document covers the database objects involved in registration and login of users based on GOTPass principles.

System Information

System Overview	Details
System name	Graphical One Time Password System
System type	User authentication prototype
Operational status	Research experiment
Environment / Special conditions	Can be integrated with any web application that requires authentication

Acronyms and Abbreviations

Acronym / Abbreviation	Meaning
GOTPass	Graphical One Time Password System
GOTPassDB	Graphical One Time Password Database

System Overview:

Database Management System Configuration

Vendor	Hardware	Version	Comments
Microsoft SQL Server	Processor type → Intel® Core™ i7 3537U @2.00 GHz 2.50 GHz System Type → 64-bit Operating system Memory → 8 GB	SQL Server 2012	SQL Server Management Studio V.11

Support Software

Product	Version	Purpose
.NET Framework	4.5	
Internet Information Services (IIS)	8.5	

Data Stores

Data store for GOTPass system is a database named "GOTPassDB" which is a repository of a set of integrated objects as defined below.

	Object Name	Object Description	Utilisation
1	User Information	Keeps basic information of user who wants to register to the system. The component consists of user full name, username and drawn password pattern.	Registration/Login
2	User Images	Stores registered/selected images used for login into the system database. This object saves information about the user images, whether pass-images selected by user or their associated distractor-images.	Registration/Login
3	User Axis Order (input format)	User select X (Top) or Y (Left) axis of each image to enter the combination code as a final password.	Registration/Login
4	Themes	A library of themes. Every theme has its own list of related images.	Registration/Login
5	Registration Log	Records time details of the user's activity during the process of registeration to the system.	Registration
6	Login Logs	Records time details of the user's activity of each login session. Moreover, this object is used also to lock users out when exceeding a number of wrong attempts.	Login
7	Lookup Information	Contains multiple lookup information that is used to support application processes.	Registration/Login
8	Exception	Various types of system and user exception are recorded by this object.	

Database administrative functions:

Naming Conventions

Type	Guideline
Style	Example: Use lowercase characters
Table names	% NAME-ABBREVIATION%_%MAJOR %_%MINOR % Example: UM_USER_MASTER Use singular names. Never plural
Field/Column names	%TABLENAME-ABBREVIATION%_%FIELD-SCOPE-NAME% Example: UM_USER_MASTER If column is primary key %TABLENAME-ABBREVIATION%_%FIELD-SCOPE-NAME%_ID Example: UM_USER_ID If Name Foreign key fields the same name as the primary key to which they refer
Stored Procedure / Function	%MAJOR %%ACTIVITY_NAME% Activity Name is Get/Insert/Update Example: UserImageGet

Database Design

The main logical components of GOTPassDB database are tables, stored procedures, and views. There are four major designs which are described as follows:

a) **Theme Lookup:**

Theme lookup was designed to contain theme library. This library is used in random selection of theme during registration process. Every theme has multiple images. Theme library and associated images are designed and mapped once and is used in user registration. Note: There is no application interface for adding themes or images into the database. The design is as follows:
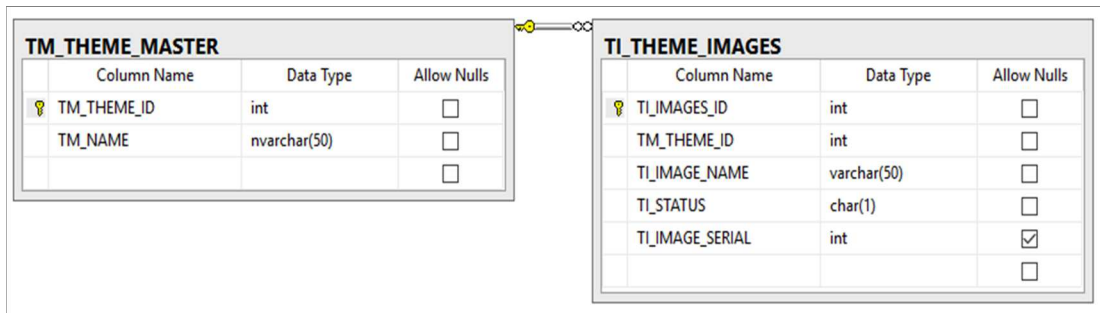
[1] TM_THEME_MASTER	
Field Name	**Description**
TM_THEME_ID	Numeric unique ID
TM_NAME	Name of the theme

[2] TI_THEME_IMAGES	
Field Name	**Description**
TI_IMAGES_ID	Numeric unique ID
TM_THEME_ID	Numeric ID linked to TM_THEME_MASTER
TI_IMAGE_NAME	Name of the image on file
TI_STATUS	Image status is used to enable or disable images. Initially same number of images for each theme was entered but due to variation in the number of images inside each theme, image status was used to indicate whether the image does exist (value=1) otherwise (value=0) to avoid displaying empty images in registration pages. (This is used only if the number of images of a spacific theme is less than 30 which is the number needed to fill in the matrix of images).
TI_IMAGE_SERIAL	Serial number of the image within its relevant theme

b) User Registration:

This design contains all the tables involved in the GOTPass registration process. User is registered into the system once the data is inserted successfully into the designated tables.

TI_THEME_IMAGES

Column Name	Data Type	Allow Nulls
TI_IMAGES_ID	int	☐
TM_THEME_ID	int	☐
TI_IMAGE_NAME	varchar(50)	☐
TI_STATUS	char(1)	☐
TI_IMAGE_SERIAL	int	☑
		☐

TM_THEME_MASTER

Column Name	Data Type	Allow Nulls
TM_THEME_ID	int	☐
TM_NAME	nvarchar(50)	☐
		☐

UI_USER_IMAGE

Column Name	Data Type	Allow Nulls
UI_IMAGE_ID	int	☐
UM_USER_ID	int	☐
TI_IMAGES_ID	int	☐
LKDCODE_TYPE	char(7)	☐
UI_PARENT_IMAGE_ID	int	☑
		☐

UM_USER_MASTER

Column Name	Data Type	Allow Nulls
UM_USER_ID	int	☐
UM_FULL_NAME	nvarchar(MAX)	☐
UM_USERNAME	varchar(50)	☐
UM_PATTERN_STR	varchar(100)	☐
		☐

UAO_USER_AXIS_ORDER

Column Name	Data Type	Allow Nulls
UM_USER_ID	int	☐
UAO_IMG_SHOW_ORD	int	☐
UAO_AXIS	char(1)	☐
		☐

[3] UM_USER_MASTER	
Field Name	**Description**
UM_USER_ID	Numeric unique ID
UM_FULL_NAME	Full name of the user
UM_USERNAME	Unique username
UM_PATTERN_STR	Pattern underlying code

[4] UI_USER_IMAGE	
Field Name	**Description**
UI_IMAGE_ID	Numeric unique ID
UM_USER_ID	Registered user ID linked to UM_USER_MASTER
TI_IMAGES_ID	Numeric ID linked to TI_THEME_IMAGES
LKDCODE_TYPE	Lookup code to indicate image type (PASSIMG = pass-image, MASKIMG = distractor-image)
UI_PARENT_IMAGE_ID	Numeric ID referring to the associated parent pass-image (number of distractors to each pass-image)

[5] UAO_USER_AXIS_ORDER	
Field Name	**Description**
UM_USER_ID	Registered user ID linked to UM_USER_MASTER

| UAO_IMG_SHOW_ORD | The numeric order (1=first, 2=second) |
| UAO_AXIS | Associated axis (X, Y) |

c) System Lookup:

System lookup design contains tables that are required to maintain setup information of the system. These tables contain multiple lookup information including image types, timeout for the login attempts, and number of failed attempts before lockout, and time duration for denying access etc.

LKM_LOOKUP_MASTER

Column Name	Data Type	Allow Nulls
LKM_ID	int	☐
LKM_NAME	varchar(50)	☐
LKM_DESC	nvarchar(50)	☑
		☐

LKD_LOOKUP_DETAIL

Column Name	Data Type	Allow Nulls
LKD_CODE	varchar(50)	☐
LKM_ID	int	☐
LKD_NAME	nvarchar(200)	☐
LKD_DESC	nvarchar(200)	☑
		☐
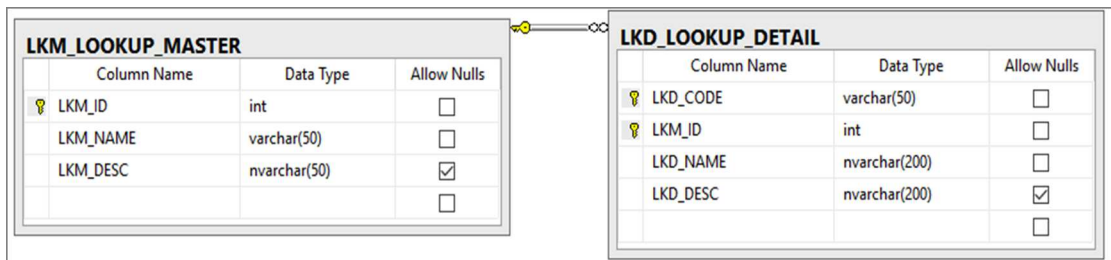
[6] LKM_LOOKUP_MASTER	
Field Name	**Description**
LKM_ID	Numeric unique ID
LKM_NAME	Name of lookup field
LKM_DESC	Description of lookup field

[7] LKD_LOOKUP_DETAIL	
Field Name	**Description**
LKD_CODE	Unique Code
LKM_ID	Numeric ID linked to LKM_LOOKUP_MASTER
LKD_NAME	The name of lookup data
LKD_DESC	Detailed description of lookup field – This is optional field to understand the purpose of lookup data. This is normally required by developer in future to remember the purpose of that data.

d) Activity Logs:

The design ensures logging every user activity in GOTPass system including each stage of registration as well as each login event. Similarly, in case of system error and exception, system logs full inner exception thrown by the system and its timestamp. Following tables are included in this design:

363

UM_USER_MASTER

	Column Name	Data Type	Allow Nulls
🔑	UM_USER_ID	int	☐
	UM_FULL_NAME	nvarchar(MAX)	☐
	UM_USERNAME	varchar(50)	☐
	UM_PATTERN_STR	varchar(100)	☐
			☐

RT_REGISTRATION_TRACE

	Column Name	Data Type	Allow Nulls
🔑	RT_REG_ATTEMPT_ID	int	☐
	UM_USER_ID	int	☐
	RT_USER_BEGIN	char(8)	☑
	RT_USER_END	char(8)	☑
	RT_PATTERN_BEGIN	char(8)	☑
	RT_PATTERN_END	char(8)	☑
	RT_IMAGE_BEGIN	char(8)	☑
	RT_IMAGE_END	char(8)	☑
	RT_OTP_BEGIN	char(8)	☑
	RT_OTP_END	char(8)	☑
			☐

ULL_USER_LOGIN_LOGS

	Column Name	Data Type	Allow Nulls
🔑	ULL_ID	int	☐
🔑	ULL_USERNAME	varchar(50)	☐
	ULL_AUTHEN_STATUS	varchar(20)	☐
	ULL_TIME_ATTEMPT	datetime	☐
	UM_USER_ID	int	☑
	ULL_USER_BEGIN	char(8)	☑
	ULL_USER_END	char(8)	☑
	ULL_USER_SUCCESS	bit	☑
	ULL_PATTERN_BEGIN	char(8)	☑
	ULL_PATTERN_END	char(8)	☑
	ULL_PATTERN_SUCCESS	bit	☑
	ULL_OTP_BEGIN	char(8)	☑
	ULL_OTP_END	char(8)	☑
	ULL_OTP_SUCCESS	bit	☑
	ULL_Trial_Num	smallint	☑
			☐

CM_EL_EXCEPTION_LOG

	Column Name	Data Type	Allow Nulls
🔑	CEL_ID	int	☐
	CEL_TIMESTAMP	datetime	☐
	CEL_TYPE	nvarchar(50)	☐
	CEL_MESSAGE	nvarchar(500)	☐
	CEL_STACKTRACE	nvarchar(4000)	☑
			☐

[8] RT_REGISTRATION_TRACE	
Field Name	**Description**
RT_REG_ATTEMPT_ID	Numeric unique ID
UM_USER_ID	Registered user ID linked to UM_USER_MASTER
RT_USER_BEGIN	Start time of registering username
RT_USER_END	End time of registering username
RT_PATTERN_BEGIN	Start time of registering pattern
RT_PATTERN_END	End time of registering pattern
RT_IMAGE_BEGIN	Start time of registering images
RT_IMAGE_END	End time of registering images
RT_OTP_BEGIN	Start time of registering OTP input format
RT_OTP_END	End time of registering OTP input format

[9] ULL_USER_LOGIN_LOGS	
Field Name	**Description**
ULL_ID	Numeric unique ID
ULL_USERNAME	The username used for login (either correct or wrong)
ULL_AUTHEN_STATUS	Authentication status (Success/Failure)
ULL_TIME_ATTEMPT	Date/time of the login attempt
UM_USER_ID	Numeric ID for correct/existing username linked to UM_USER_MASTER
ULL_USER_BEGIN	Start time of login username

ULL_USER_END	End time of login username
ULL_USER_SUCCESS	Username success status (1 OK, 0 No)
ULL_PATTERN_BEGIN	Start time of login pattern
ULL_PATTERN_END	End time of login pattern
ULL_PATTERN_SUCCESS	Pattern success status (1 OK, 0 No)
ULL_OTP_BEGIN	Start time of login OTP input format
ULL_OTP_END	End time of login OTP input format
ULL_OTP_SUCCESS	OTP input format success status (1 OK, 0 No)

[10] CM_EL_EXCEPTION_LOG	
Field Name	**Description**
CEL_ID	Numeric unique ID
CEL_TIMESTAMP	Date/time of the event log
CEL_TYPE	Error message type that shows the title of error
CEL_MESSAGE	Error message text that shows .NET inner exception
CEL_STACKTRACE	Error details that shows complete stack of error from class/methods; that means error is thrown back from many methods

Details of stored procedures are described as follows:

S. #	Stored Procedure Name	Parameters	Purpose
1	TRG_THEME_RANDOM_GET	@EXCLUDE_THEMEID_STR	To get a random theme for image selection. This procedure is used in registration process for system theme selection.
2	ImagesRandomByThemeGet	@ThemeID	To fetch random images for system selected themes in registration process.
3	UserMaskImageInsert	@UserID @UserImageXml	To insert random distractor-images (mask) with each user selected pass-image as associated distractor-images.
4	UserLoginTraceInsert	@UM_USER_ID @RT_USER_BEGIN @RT_USER_END @RT_PATTERN_BEGIN @RT_PATTERN_END @RT_IMAGE_BEGIN @RT_IMAGE_END @RT_OTP_BEGIN	To insert the registration activity logs of the user into database.

S. #	Stored Procedure Name	Parameters	Purpose
		@RT_OTP_END	
5	UserLogsForLockingGet	@UserName @RecordCount @Interval	To get the log of the user's previous attempts.
6	UserInsert	@fullname @username @pattern @userid out	To create new user in the registration stage, insert the details of the user information.
7	UserImageInsert	@UserID @ImageID @UserImageID out	To insert the user selected images (pass-images). This procedure is part of registration.
8	UserAxisOrderInsert	@UserID @ImageShowOrder @Axis	To insert the system selected axis order of images based on the user selected security level; basic or advanced. This process is part of registration.
9	UserLoginLogsInsert	@ULL_USERNAME @ULL_AUTHEN_STATUS @UM_USER_ID @ULL_USER_BEGIN @ULL_USER_END @ULL_USER_SUCCESS @ULL_PATTERN_BEGIN @ULL_PATTERN_END @ULL_PATTERN_SUCCESS @ULL_OTP_BEGIN @ULL_OTP_END @ULL_OTP_SUCCESS	To record the activities of each login step and then insert the complete log of the login attempt into the database.
10	UserInformationGet	@UserName	To fetch user information.
11	UserImageGet	@UserID	To get the images of the registered users. This procedure is part of login process.
12	MaskImageGet	@UserImageID	To get distractor-images associated with each pass-image during login process.
13	ImagesRandomByThemeGetForLogin	@ThemeID @UserID @top	To get the pass-images of a registered user along with distractor-images and other random images. This

S. #	Stored Procedure Name	Parameters	Purpose
			procedure is used in login process.
14	UserAxisOrderGet	@UserID	To get image axis order to place the generated random password. This procedure is part of login procedure.
15	SetupDataGet	@SetupId	To get lookup data (e.g. number of failed attempts, lockout time, timeout). This procedure is generic procedure created for generic table of lookup.
16	CM_EI_EXCEPTION LOG_INSERT	@CEL_TYPE @CEL_MESSAGE @CEL_STACKTRACE @CEL_ID OUTPUT	To record and insert error /exception that occur when running the system. This procedure is called by system unnoticeably whenever the user experience irregular behaviour when using the system.

Dependencies

Table and column in [application] schema	Schema the table/ column refers to	Table
TM_THEME_MASTER/ TM_THEME_ID	TM_THEME_ID	TI_THEME_IMAGES
TI_THEME_IMAGES/ TI_IMAGES_ID	TI_IMAGES_ID	UI_USER_IMAGES
UM_USER_MASTER/ UM_USER_ID	UM_USER_ID	UAO_USER_AXIS_ORDER
		UI_USER_IMAGE
UI_USER_IMAGE/ UI_IMAGE_ID	UI_PARENT_ IMAGE_ID	UI_USER_IMAGE
	UI_IMAGE_ID	UIO_USER_IMAGE_ORDER
LKM_LOOKUP_MASTER/ LKM_ID	LKM_PARENT_LKMID	LKM_LOOKUP_MASTER
	LKM_ID	LKD_LOOKUP_DETAIL
LKD_LOOKUP_DETAIL/ LKD_CODE	LKD_PARENT_LKDCODE	LKD_LOOKUP_DETAIL
LKD_LOOKUP_DETAIL/ LKM_ID	LKD_PARENT_LKMID	

3) GOTPass application components

A. Application pages

1) FrmHomePage.aspx

1.1 Identification
   Hierarchy: OTGP_ PAGES→Webpages
   Namespace: OTGP_PAGES.Webpages

1.2 Definition
   The purpose of this page is to provide user choices either to register (create a new user) or to login into the system if he/she is a returning user.

1.3 Methods and Events
Page Events
1.3.1 **Page_Load**: This event checks the user session which is sent to this webpage. If the session is expired the system shows the message to user that your session has been expired.

1.3.2 **IbRegister_Click:** This event is related to the 'Register' *image* click. In this event, the system redirects the user to the registration step number 1.

1.3.3 **LbRegister_Click:** This event is for the 'Register' *link* click. In this event, the system redirects the user to the registration step number 1.

1.3.4 **IbLogin_Click:** This event is for the 'Login' *image* click. In this event, the system redirects the user to the login step number 1.

1.3.5 **LbLogin_Click:** This event is for 'Login' *link* click. In this event, the system redirects the user to the login step number 1.

2) FrmRegisterA.aspx

2.1. Identification
   Hierarchy: System.Object → OTGP_ PAGES
   Namespace: OTGP_PAGES

2.2 Definition
   This page starts the Registration Step 1. This webpage takes two inputs; the user full Name and username as inputs. In addition, user registers the graphical unlock pattern on this page. This username and unlock pattern will be used as part of the credentials for user to login into the system.

2.3 Methods and Events
Internal page method:

2.3.1 **ChkUserName:** This method checks the duplication of the entered username from database. It does not let the registration steps to continue and prompts the user with an error message stating that the chosen username is already registered.

2.3.2 **IbRegisterPattern_Click:** This method first checks the username is not duplicated and Pattern lock is drawn then proceed to register the user.

3) FrmRegisterC.aspx

3.1 Identifications
　　　Hierarchy:　System.Object → OTGP_PAGES
　　　Namespace: OTGP_PAGES

3.2 Definition
This page is for step 2 of registration process. In this step system randomly selects 4 themes for the user and each selected theme contains many images. Each user has to select 4 images to continue the registration process.

3.3 Methods and Events:
Internal page event:

3.3.1 **Page Load:** In this page load event, the system checks the username and pattern is inserted by the user or not. In case the username or pattern was unfound, the system will redirect the user back to Registration step 1.

This event calls two internal page methods GetSelectedRandomTheme and BindSelectedRandomThemeImages which are explained next.

3.3.2 **GetSelectedRandomTheme:** This method takes the input of already selected theme ID in order to make the logic for not repeating the selected theme ID again. For the first time it takes the ID to 0. This method calls the database process to get the random themes to present them in the system.

3.3.3 **BindSelectedRandomThemeImages:** This method sets the interface of the page as we get the images of the randomly selected theme. This method binds the images of the selected theme within the grid on the page to display the images to user.

3.3.4 **ImageButton_Click:** This is the control event which is bounded with all the images on the page and it just records the image selection starting time and changes the background of selected image and popup a larger version of the selected image. The popup screen contains two buttons; one to confirm the image selection, and the second button to cancel it.

3.3.5 **btnOk_Click:** This control event is bounded with the popup decision button1 which states to add the selected image and continue with a new theme. In this event the logic is implemented to check whether the user has selected four images or less. If that selection is the fourth image, then the system redirects the user to the next Registration step.

3.3.6 **btnCancel_Click:** This control event is bounded with the popup decision button2 which states to cancel the selected image and go back to the same theme grid to add a new image.

4) FrmRegisterationD.aspx

4.1 Identifications
Hierarchy: System.Object → OTGP_PAGES
Namespace: OTGP_PAGES

4.2 Definition
This page is the last step of Registration process. In this step the user will select the input format (the axis locations for the codes). This page contains two security levels. Initially, the system selects one of them for the user randomly, however, users can change the assigned security level as they wish. Inside each security level there are two options that determine the exact location of codes where the user needs to look for after identifying the pass-images. These options cannot be changed once they are selected by the system since the system, at the page load, will select one of the two options of each security level and link it with security level for that session. In this page, the system also displays all the selected images for the user.

4.3 Methods and Events:
Internal page event:

4.3.1 **Page Load:** In this event, the user session is checked; if the session is expired the system displays the session expiration message. In this event, the system binds the user selected images to show the interface and also the system selects a random security level.

4.3.2 **rdoBasicSecurity_CheckedChanged:** This is the control event which is bound with the Radio Button control on page to select the basic security level. User can change the security level as desired.

4.3.3 **rdoAdvanceSecurity_CheckedChanged:** This is the control event which is bound with the Radio Button control on page to select the advanced security level. User can change the security level as desired.

4.3.4 **InsertUserRegistration:** This method takes the user's input data to the middle layer that communicates with the database to register the user into the system by saving the details into the database. In this method system

also note the time of every transaction taken by the user in details to complete the registration.

5) FrmLoginA.aspx

5.1 Identifications
   Hierarchy: System.Object → OTGP_PAGES
   Namespace: OTGP_PAGES

5.2 Definition

This page is for the login process. It shows empty table without images in the background and a popup screen where the user needs to enter the username and draw the unlock pattern. Based on the provided (entered) credentials, the system checks the data; if correct then returns a set of images including user's pass-images, but if the user inputs the wrong credentials the system shows a set of random images. This page also locks out the user if the maximum number of allowed failed attempts are met which is also configurable through the database.

5.3 Methods and Events:
  Internal page event:

  5.3.1 IbLoginPattern_Click: This method takes user credentials as input and on validation it shows the random images for user verification.

  5.3.2 ImagebtnLogin_Click: This is the control event which is bound with Button control on page to login into the system. This method first checks if the user is not blocked. If the user is blocked, then it returns the control and shows the random images but without performing the login. On the other hand, if the user is not blocked it performs the validation with the random codes which are generated by Random numbers and placed on the pre-determined axis based on the correct pass-images. If the user is validated, the system displays the success page and maintains the log of the failure and success attempts in the database.

B. Application classes

1) clsTheme Class

1.1. Identification
 Hierarchy: System.Object → OTGP_OBJECTS.BLL.clsTheme
 Namespace: OTGP_OBJECTS.BLL

1.2. Definition

The purpose of this class is to provide properties and methods for Theme objects to implement business processes. Theme object also contains images to link Themes and Images.

1.3. Properties

Theme properties are as follows:-

1.3.1. lstThemeImage

Holds a collection of images in .NET list object i.e. registration image selected by user etc.

1.3.2. ThemeImageID

Holds a single image.

1.3.3. MaskImageCount

Configures number of distractor-images for each pass-image.

1.3.4. RandomImageForLoginCount

Configures the total number of images that the system will show to user in login page. Users will select their pass-images from among these images.

1.4. Methods

Theme objects use the following methods:-

1.4.1. GetRandomTheme

a. Parameters:

strExcludeThemeID – This is the input parameter of string type to exclude the themes that the system should not fetch.

Return – Method returns DataTable of themes.

b. Method definition:

This method is used in registration process to get random themes from the pool of lookup provided themes. Method have strExcludeThemeID parameter to exclude those themes that are already shown and user have selected image from it. strExcludeThemeID is comma separated string that keeps on including the theme that has been shown to user.

1.4.2. GetRandomImageByTheme

a. Parameters:

Return – Method returns DataTable of images for a given Theme.

b. Method Definition:

This method is used to retrieve random images of the provided Theme. The method receives ThemeID by class property. It is used in registration process to display images of a particular Theme.

1.4.3. GetRandomImagesForLogin

a. Parameters:

intUserID – an input parameter of integer type. It carries registered user id.
intTop – an input parameter of integer type used to show number of images in login. This number includes the pass-images and distractor-images.
Return – Method returns DataTable of images.

b. Method Definition:

This method is used in the user login process. The method fetches random images from random themes to display against GOTPass codes. The method does not fetch real pass-images and its corresponding distractor-images.

1.4.4. GetUserImages

a. Parameters:

intUserID – an input parameter of integer type. It carries registered user id.
Return – Method returns DataTable of user pre-chosen pass-images.

b. Method Definition:

This method fetches user pass-images that user has selected during registration.

1.4.5. GetMaskImages

a. Parameters:

intUserImageID – holds the value of the user image that has been selected in registration.
Return – Method returns DataTable of distractor-images against particular user pass-image.

b. Method Definition:

This method retrieves distractor-images for a given user pass-images.

2) clsThemeT Class

2.1. Identification
Hierarchy: System.Object → OTGP_OBJECTS.BLL.clsThemeT
Namespace: OTGP_OBJECTS.BLL

2.2. Definition
The purpose of this class is to provide properties and methods for Theme objects to access database objects. This class is associated with clsTheme class as it provides all type of data access interfaces to clsTheme. clsTheme purely implements business processes of GOTPass system without having any database interface. However, clsThemeT exposes database interfaces for clsTheme to save and retrieve information. This class implements transaction and other common methods that are required for database operations.

3) clsUser Class

3.1. Identification
Hierarchy: System.Object → OTGP_OBJECTS.BLL.clsUser
Namespace: OTGP_OBJECTS.BLL

3.2. Definition
The purpose of this class is to provide properties and methods for User objects to implement business processes of GOTPass.

3.3. Properties
User class properties are as follows:

3.3.1. UserID
An integer datatype to hold the UserId of a registered user.

3.3.2. FullName
Holds the full name of a registered user. This property saves values of string type.

3.3.3. UserName
Holds the UserName for a registered user. The property uses string datatype.

3.3.4. Pattern
Holds the value of the unlock pattern which is a set of integer numbers, selected by the user during registration.

3.3.5. UserImageOrderCode
Contains the order value of user pass-images. This carries string value.

3.3.6. objTheme
Carries complete Theme object. User class have a relation with Theme object.

3.3.7. UserImageID

Contains registered user image id. It can also hold values of user selected image id before the creation of user account.

3.3.8. UserImageAxis

Holds registered user image axis. This property can also contain axis values in registration process before the creation of account.

3.3.9. lstUser

Carries a list of users in .NET list objects.

3.3.10. AuthenticationStatus

Holds authentication status of user attempt whether the login is correct or not.

3.3.11. UserLoginAttempts

Holds maximum value for user login attempts. Whenever this limit is reached in login screen, system will lock the account. This carries integer data types.

3.3.12. UserLoginInterval

This integer property carries the time duration in which the user is locked out when s/he failed to login for a particular number of times.

3.3.13. UserNameBeginTime

This property is used to log registration/login start time for typing in username and full name. It contains hours, minutes and second in string format.

3.3.14. UserNameEndTime

This property is used to log registration/login end time for typing in username and full name. It contains hours, minutes and second in string format.

3.3.15. UserPatternBeginTime

This property is used to log registration/login pattern drawing start time. It contains hours, minutes and second in string format.

3.3.16. UserPatternEndTime

This property is used to log registration/login pattern drawing end time. It contains hours, minutes and second in string format.

3.3.17. UserImageBeginTime

This property is used to log registration/login start time to select pass-images. It contains hours, minutes and second in string format.

3.3.18. UserImageEndTime

This property is used to log registration/login start time to select pass-images. It contains hours, minutes and second in string format.

3.3.19. UserOTGPBeginTime

This property is used to log registration/login start time to input GOTPass code. It contains hours, minutes and second in string format.

3.3.20. UserOTGPEndTime

This property is used to log registration/login start time to input GOTPass code. It contains hours, minutes and second in string format.

3.3.21. IsUserCredentialsValid

It is a Boolean property to validate the user credentials whether correct or not.

3.3.22. IsUserCredentialsPatternValid

It is a Boolean property to validate the unlock pattern credential whether correct or not.

3.3.23. IsUserNameValid

It is a Boolean property to validate the username whether correct or not.

3.3.24. IsUserPatternValid

It is a Boolean property to validate the unlock pattern whether correct or not.

3.3.25. IsUserOTPValid

It is a Boolean property to validate GOTPass code whether correct or not.

3.4. Methods
User objects have following methods:-

3.4.1. InsertUser

This method creates a new user in the database by inserting username, fullname and unlock pattern details.

3.4.2. InsertUserImage

This method inserts the user selected pass-images during registration process.

3.4.3. InsertMaskImage

This method is triggered after inserting user pass-images. This method saves distractor-images for each pass-image. The system saves 3 distractor-images with each password-image.

3.4.4. InsertImageOrder

This method inserts the required order of the selected pass-images.

3.4.5. GetUserInformation

The method is used to get the information of a registered user.

3.4.6. InsertUserLoginLogs

This method is called for tracing. It saves information of user login attempt.

3.4.7. InsertUserAxisOrder

This method is used to save the GOTPass axis order to generate OTP password during login.

3.4.8. GetUserLogInformation

This method is used to retrieve and verify user credentials. It is used in login process.

3.4.9. RegisterUser

This is the main method to register a user into the system. There are multiple methods that are called by this method.

3.4.10. GetImagesForLogin

This method retrieves pass-images from the database. The method is used in login process to present pass-images to the user and generate OTP password.

3.4.11. GetUserImageInsertPosition

This is a middle method to implement logic of inserting pass-images mixed with decoy-images.

3.4.12. GetMaskImageInsertPosition

This method inserts distractor-images into the grid with other pass-images and decoy-images.

3.4.13. CreateImageTableForLogin

This method is the main method to create table/grid of images for user login. This table/grid contains pass-images, decoy-images and distractor-images.

3.4.14. GetUserRegisteredImageOrder

This method is used for generating a random code in the right order based on pass-images and the pre-determined input format.

3.4.15. LoginUserHandler

This is top middle method to handle full login process. There are hierarchy of methods called from this method to implement logic of login processes.

3.4.16. ReplaceRandomNumberInDatTable

This method assigns 4-digits random number to the images (pass-images, decoy-images and distractor-images) on x-axis and y-axis.

3.4.17. GenerateUserRegisteredImageOrderCode

This method generates string of password by getting 4-digits random code along with user selected x-axis and y-axis information of the selected pass-image.

3.4.18. GenerateOTGP

This is the main method that handles the random code generation process.

3.4.19. CheckUserCredentials

This method validates the unlock pattern of user during login process.

3.4.20. InsertUserTrace

This method inserts trace information of the user who is registering into the system.

4) clsUserT Class

4.1. Identification
Hierarchy: System.Object → OTGP_OBJECTS.BLL.clsUserT
Namespace: OTGP_OBJECTS.BLL

4.2. Definition
This class is associated with clsUser class as it provides all type of data access interfaces to clsUser. clsUser purely implements business processes of GOTPass system without having any database interface. However, clsUserT exposes database interfaces for clsUser to save and retrieve information. This class implements transaction and other common methods that are required for database operations. The methods in this class do database communication and work as a middle layer of business and database access layers.

Appendix G Published papers & Press release

1) H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell, "Alternative Graphical Authentication for Online Banking Environments,". In *HAISA,* 2014, pp. 122-136.

Alternative Graphical Authentication for Online Banking Environments

H. Alsaiari[1], M. Papadaki[1], P.S. Dowland[1] and S.M. Furnell[1,2]

[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, United Kingdom
[2]Security Research Institute, Edith Cowan University, Perth, Western Australia
e-mail: info@cscan.org

Abstract

Many financial institutes tend to implement a secure authentication mechanism through the utilization of the One-Time-Password (OTP) technique. The use of a hardware security token to generate the required OTP has been widespread. Despite the fact that this method provides a fairly high level of security, many systems have not taken into consideration the need for a secure alternative login method whenever the hardware token is unavailable. This paper discusses the authentication issues associated with current e-banking login implementations when the hardware security token is unavailable. The study was supported by a user survey to realize the constraints confronting the user while logging in to their online banking system. The result showed that many online banking users had multiple accounts and found carrying around several security tokens is inconvenient. Moreover, high proportion of the users had confidently accepted the concept of one-time graphical password as an alternative means of authentication. Therefore, a potential solution has been introduced along with a conceptual discussion. The proposal aims to consolidate several authentication mechanisms to unite their various advantages into one robust authentication system with consideration of usability. The composite mechanism comprises of a One-Time-Password combined with graphic-based authentication techniques.

Keywords

Alternative authentication, User authentication security, Online banking authentication, Graphical password, One-Time-Password

1. Introduction

Online banking, also known as Internet banking, is a means of delivering banking services electronically to customers. Online banking services include accessing account information, the transfer of funds between different accounts and making electronic payments and settlements (Dube & Gulati, 2005; FFIEC, 2003). The popularity of online banking is growing, but it is now faced with major challenges, one of which is the high risk of data compromise. Thus, in order to minimize the threats to online banking and at the same time increase customer security, confidence and acceptance of this electronic service channel, the online accounts of customers must be securely protected via enhancing user authentication without adversely impacting upon the users' experience (Williamson & Money–America's, 2006).

122

As reported by Verizon (2013), 37% of breaches in 2013 affected financial organizations, which increased by about 10% compared with the previous year's report. Crime against the finance industry involved various type of common attacks such as tampering (physical), brute force (hacking), and spyware (malware). The target of such breaches was mostly payment cards, credentials, and bank account info. Basically, gaining unauthorized access in an easy and less-detectable way is possible through leveraging other's authorization access. Moreover, an earlier report (2012) showed that about four of every five breaches involving hacking was factored by authentication-based attacks (guessing, cracking, or reusing valid credentials). Authentication credentials theft presented a high value of loss as a result of espionage-related breaches. About 80% of these attacks can be forced to adapt or die whenever the idea of a suitable authentication replacement is collectively accepted.

The critical importance of securing the wide range of banking services being deployed over the Internet is a major concern for both service providers and customers. Thus, extreme caution is always paid to safeguarding the e-banking system as well as customer information. The first line of defence is protecting the authentication system from fraud and identity theft. Currently, the traditional text-based password is the foremost knowledge-based authentication and the primary form of user authentication (De Angeli et al., 2005; Fu et al., 2001) and while there are many techniques to secure passwords (Pinkas & Sander, 2002), most are insufficient in the face of attackers' tools (Chakrabarti & Singbal, 2007; AuthenticationWorld.com, 2012). The deficiencies of the textual password is well-known and affects both aspects of usability and security (Dhamija & Perrig, 2000; Suo, Zhu & Owen, 2005). Therefore, the need for alternative methods has emerged where various alternative knowledge-based techniques have been proposed, such as graphic-based passwords (recognising graphical elements – e.g. images, iconography, grids) (Gyorffy, Tappenden & Miller, 2011; Kuber & Yu, 2010) or associative/cognitive questions (Zhao, Dong & Wang, 2006; Alexander, 2008). Each approach has different aspects of strengths and weaknesses.

In crucial systems such as in financial organizations, robust security is constantly demanded. One of the solutions to meet that goal is the One-Time-Password approach. The idea of OTPs is to encode the password for a single use only; producing a unique password for each login session or transaction. In other words, the user will end up using different dynamic password for each login. Illegitimately obtaining an OTP should be useless and helpless for attackers to generate any further encoded passwords. Thus, managing to record or steal a used OTP would be totally unusable for further login attempts since an OTP loses its validity (expire and discard) after first use. This means that OTP systems are protected against replay attacks (Yampolskiy, 2007; McDonald, Atkinson & Metz, 1995).

This paper aims to point out limitations in some authentication cases within the online banking system and propose a potential solution to securely fill-in this gap using the same web browser without the need for any additional devices. The remainder of the paper proceeds with a brief review of some authentication features provided by leading financial institutes. Section 3 then discusses the authentication

problems in online banking. Section 4 presents the preliminary survey results that investigate the authentication issues in online banking and gauge perceptions towards alternative authentication methods. Section 5 gives a general introduction to our proposed prototype of OTGP and conclusions and future work are addressed in Section 6.

2. The provided authentication by leading banking institutes

We conducted a review of the authentication approaches offered by banking services providers. We assessed the practices of the top four banks as ranked by relbanks.com (relbanks.com, 2012) in the UK and Saudi Arabia on the basis that respondents from these countries would form the basis for later survey data collection. The purpose was to gain tangible results from a field review that investigate and compare different authentication experiences within the electronic banking domain.

The comparison data was collected by visiting each online banking service of these banks to explore the provided authentication features. The services were compared on the basis of the following factors:

- **Authentication options**: when more than one authentication method is available for the user to choose from (e.g. OTP hardware-token or subset digits of textual password). Combining more than one form of authentication mechanism is called **Two-factor authentication**.
- **Static password**: The conventional password approach.
- **Subset digits of password**: challenges the user by requesting to submit different digit locations of the full password (e.g. 2nd, 4th, 7th digit of your password).
- **Memorable information**: a type of personal questions that can be easy and short to answer by legitimate user.
- **OTP (SMS)**: a One Time Password sent to mobile phones through carrier short messages.
- **OTP (Soft-Token)**: a type of One Time Password that is generated by software application usually installed on smart phones.
- **OTP (Hard-Token)**: a special hardware device that directly generates a One Time Password.
- **PIN-dependent token**: an additional feature to the hard-token device where a PIN is needed to generate One Time Password.
- **Card-dependent token**: Another additional feature to the hard-token device where a smart-card is required to generate One Time Password.
- **Authorization site image**: a feature that allows the selection of a picture that will indicate a correct access to the official online banking website at every login time (and not a phishing website).
- **Authorization personal image**: allows uploading a personal picture that will be shown at every login to ensure accessing the official online banking website.

- **Designation of safe computer**: a computer that typically being used to access online banking accounts can be designated to be recognised as a Trusted Computer, any access from any other PCs will be denied.

	Bank	Authentication options	Two-factor authentication	Static password	Subset digits of password	Memorable information	OTP (SMS)	OTP (Soft-Token)	OTP (Hard-Token)	Token needs PIN	Token needs Card	Other
UK Banks	HSBC	✗	✓	✗	✗	✓	✗	✗	✓	✓	✗	
	Barclays	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	
	Royal Bank of Scotland	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	
	Lloyds	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	
Saudi Arabian Banks	National Commercial Bank	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	-Authorization Site Image
	Al-Rajhi Bank	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	
	Samba Financial	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗	-Authorization personal Image -Designation of safe computer
	Riyad Bank	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	

Table 1: Authentication technologies used by leading banking institutes

The comparative Table 1 reveals that various authentication techniques to secure access to the systems have been applied. The text-based password is still the most common method used, appearing in different forms, such as static password, subset digits or memorable information. Usually, text passwords are used in conjunction with other authentication methods such as One-Time-Password (OTP) which also forms a two-factor authentication. In addition, the majority of banking systems have fortified their systems by implementing two-factor authentication instead of relying on a single factor. A number of banking systems have offered a variety of One-Time-Password (OTP) implementation methods using hardware tokens, short messages (SMS) or software tokens with the support of some additional security features.

Furthermore, it can be inferred that some authentication features are applied in one country but not the other. For instance, while some UK online banking systems utilise subset digits of password and memorable information, Saudi Arabian banks mostly do not. Whereas, soft-token OTP is implemented in Saudi Arabia but not commonly used in the UK. Notably, this part of the study was focused solely on the login authentication service which means that it does not cover any further authentication like transaction-based authentication or adding a new payee.

3. Limitations of online banking authentication

Giving the option for the user to choose the appropriate authentication method is a fundamental usability feature that adds flexibility to the system. Despite the fact that this feature does exist in some current systems, it is realized that the available options depend mainly on phone banking services providing the required access or on giving the customer the choice of selecting between the use of a hardware token or SMS. That means that there is still potential for encountering some of the usability problems, such as that of being reliant on hardware devices like mobile phones or OTP tokens, which are vulnerable to theft and loss or in the case of mobile phones may suffer an interruption in the service coverage (Weir et al., 2010). In addition, other systems may offer the traditional passcode option or allow authentication via a series of Q&A challenges in case the user is unwilling/unable to use the recommended secure authentication options which potentially fall back into the weaknesses of the traditional textual password. However, none of the discussed authentication options other than the text-based password offer in-session authentication which uses the web browser to process any extra login task. That in turn emphasizes the dependence on an additional out-of-band means (e.g. token/mobile) to secure the authentication task.

More recently, many banks have adopted OTP authentication using hardware tokens that are supplied to each client as part of a multi-factor authentication scheme. Although this method is effective, it has a fundamental downside due to the reliance of the applied OTP authentication being mostly on a single OTP delivery method. Thus, many online banking systems are not equipped with a supplementary authentication method to back up the primary hardware-based OTP authentication. In other words, lost/stolen/forgotten/damaged hardware tokens will prevent clients from gaining access to the online banking system due to the absence of an operative alternative means of logging in under such critical circumstances. However, some online banking systems utilize an out-of-band method, such as mobile SMS messaging, as a parallel means of obtaining the OTP. Still, this service can encounter several problems, such as message delivery delay, weak signalling, roaming availability and charges (Weir et al., 2010; RBS, 2014). Therefore, the need for a secure, usable secondary authentication method to play an alternative role alongside the primary hardware-based OTP scheme has emerged in cases where the hardware token is unavailable.

Graphic-based authentication is among the promising alternative proposals, which occupies an important position within user authentication research area (Ray, 2012).

126

According to classic cognitive science experiments, humans have a vast, almost limitless memory especially for pictures (Dhamija & Perrig, 2000). Thus, authentication types that depends on graphics are likely to tackle the memorability problems that negatively affect text-based authentication since remembering complex passwords as well as multiple passwords for different systems are claimed to be a difficult task (Furnell, 2005; Furnell & Zekri, 2006), while at the same time, humans find it easier to recognise images even after a period of time (Anderson, 2001).

4. Research survey

A structured online questionnaire was designed and delivered to investigate the authentication issues associated with online banking in addition to gauging the participants' perceptions and attitudes towards alternative authentication methods for online banking. The main purpose of the survey was to find answers for some research-related questions such as whether users manage multiple online accounts, are using security tokens for that purpose, the user perception regarding carrying around several tokens, have they ever encountered login problems when using these tokens, and finally their acceptance of alternative authentication methods. The survey was comprised of a total of twenty nine questions encompassing demographic information, experiences of user authentication schemes and security-related techniques, usage of the banking system, experiences of authentication within the online banking system and lastly the users' opinions and acceptance level of the alternative authentication mechanisms.

4.1. Results interpretation and analysis

A total of 250 respondents participated in this online survey over a period of 3 weeks. All participants were volunteers, participants were recruited from students and staff in the authors' university, and colleagues/friends of the author who were invited via email and text messages. Two thirds of the respondents were males and the remaining third were females. The age group between 30 and 39 years comprised the majority of the sample and represented 43% of the total number of participants. The residential location shows that almost 90% of the respondents resided either in the UK (46%) or Saudi Arabia (44%). Regarding the educational background, the highest percentage of participants (44%) had studied at Higher education level, while 39% were Postgraduates. As for the employment status, the highest percentage of participants (67%) were employed followed by 24% being students. Regarding the level of computer experience, most participants (48%) considered themselves to be at advanced level followed closely by 47% at intermediate level with only a small percent (4%) having a basic level of computer skills.

The results revealed that 57% of the participants have used OTP as an alternative authentication method. Regarding the importance of multiple levels of authentication where various authentication approaches from the same category (usually knowledge-based) are combined, 90% of the participants were supportive of this kind of technique, agreeing that it was important.

127

An important question was asked aiming to measure the users' opinions on carrying around multiple security devices to fulfil the authentication requirements of multiple online accounts. Table 2 demonstrates that most respondents opposed the idea with 69% feeling that carrying multiple tokens is not convenient and 38% thinking it is unnecessary. However, 38% of the participants said it is acceptable on balance.

	Convenient		Necessary		Acceptable	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Agree	44	17.6	90	36.0	96	38.4
Neutral	34	13.6	64	25.6	71	28.4
Disagree	172	68.8	96	38.4	83	33.2

Table 2: Participants' opinion about carrying multiple tokens

The participants were also asked some banking-related questions. As per the survey results shown in Figure 1, the vast majority of respondents (93%) were online banking users. Amongst these, 65% were managing more than one online account with 56% having between 2 and 5 online accounts. Noticeably, 9% of the respondents had more than five online accounts, while approximately a quarter of the participants had only a single online account. Around two thirds of the online banking respondents stated that they access their online banking accounts on a regular basis, while nearly a quarter of the respondents accessed their accounts occasionally. The final part of this section investigated the purpose of using online banking services. The results shows that 40% of the participants were utilizing this service to conduct a variety of online payment services, such as paying bills or transferring funds, while 36% of them used the service for checking bank account information/transactions.
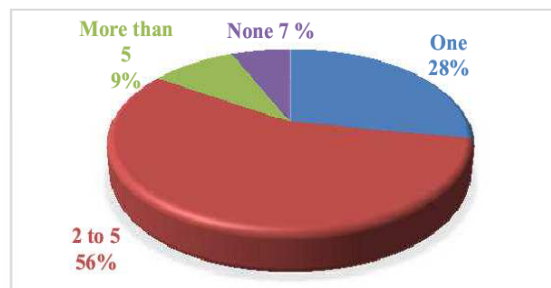
Figure 1: Number of online banking accounts

With regards to the online banking experience, more than 85% of the participants' online banking systems require multi-factor authentication. Remarkably, OTP authentication was offered by the banks of 90% of the participants, as shown in Table 3. Furthermore, since most of the participants were from the UK and Saudi Arabia, a further analysis was carried out to assess the popularity of certain types of OTP techniques in these countries. The findings indicated that the most used

128

technique in the UK was the security token device whereas SMS text messages were the most common in Saudi Arabia. It should be noted here that the responses to some questions were open to multiple choices which explain why the responses count in Table 3 exceeded the number of participants.

Type of OTP	Count	Responses %
None - the online banking system does not facilitate a One-Time-Password	32	10.4%
SMS text message	136	44.2%
Security token device (Hardware)	114	37.0%
Soft token (Software)	26	8.4%

Table 3: The offered types of One-Time-Password

Table 4 illustrates that 76% of the responses indicated that they were satisfied with the use of One-Time-Password authentication, while in contrast a very small portion were dissatisfied with this type of technique.

OTP experience	Frequency	Percent
Satisfied	160	76.2
Neutral	38	18.1
Dissatisfied	12	5.7

Table 4: Participants experience with OTP technique

As part of multi-factor and OTP authentication, the participants were asked if they had failed to login using these methods before. The result shows that 64% had experienced failure in fulfilling the login requirements for several reasons (Figure 2), such as mistyping the code which comes first with (48%), the lack of mobile services (21%) and lost token/mobile (9%). However, 43% of these incidents occurred only rarely, while less than 3% happened frequently.
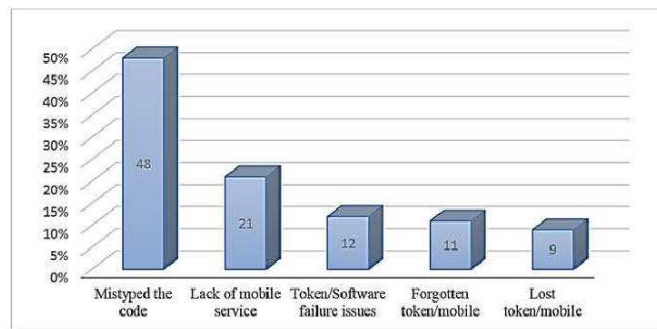
Figure 2: Reasons of experienced login failure

Table 5 shows that 73% of the participants who had login problems were still expressing themselves to be 'satisfied' overall when using one-time-password. However, only less than 5% of the participants with multiple online accounts had dissatisfaction experience using one-time-password and approximately 18% of the responses were 'neutral' as presented in Table 6.

		Frequency of login failure using multi-factor or One-Time-Password authentication			
		Rarely	Sometimes	Frequently	Percentage%
Experience of using One-Time-Password	Satisfied	103	22	4	73
	Neutral	31	10	2	22
	Dissatisfied	7	4	0	5
Percentage %		70.2	25.5	4.3	

Table 5: Satisfaction of the participants who experienced login failure

		Multiple online banking accounts %
Experience of using One-Time-Password	Satisfied	77.7
	Neutral	17.6
	Dissatisfied	4.7

Table 6: Satisfaction of the participants with multiple accounts

The last section presented a conceptual model (Figure 3) about the prospective solution with a concern about participants' opinions towards alternative authentication mechanisms. In terms of accepting the idea of replacing or supplementing the existing one-time-password method with a one-time graphical password technique, responses showed that almost half of the participants (49%) accepted the idea, while in contrast, less than a quarter (23%) rejected it. Another question in this regard was about the participants' confidence in the alternative graphical authentication method for online banking. 49% of the participants responded with "confident" and 26% with "un-confident".

130

Figure 3: One-time graphical password conceptual model

4.2. Discussion of research survey

The collected data showed diversity in the participants' experiences and knowledge of authentication and online banking. It appears that plenty of the participants had a reasonable understanding of authentication enhancement in the online banking environment; nevertheless, a small percentage of participants had little knowledge of online banking authentication. The positive record of participants' computer experiences indicates the development of users' computing skills and their competency to perform more complex computer tasks.

As per the survey results, it was found that a high percentage of respondents hold and manage several online banking accounts. This demonstrates a trend towards the utilization of the online channel to simplify performing banking transactions as well as other account management tasks. Moreover, the results also emphasize the difficulty of using multiple security tokens to manage these accounts; many participants disagreed with the idea of carrying around multiple devices for login purposes, describing it as inconvenient and unnecessary. Additionally, the survey showed that a high proportion of the total sample number access their accounts on a daily or weekly basis, which obviously proves the increasing popularity of and demand for online banking services.

One of the interesting results of the survey was the high percentage of responses indicating that the online systems of the participants' banks require multi-factor authentication. Furthermore, many of those systems make use of the OTP authentication method. More than half of the participants had already been using One-Time-Password as an alternative method of authentication. That in turn reveals the importance and feasibility of both techniques for the online banking environment. Interestingly, the result shows that the majority of respondents have had satisfactory experiences using OTP techniques. In spite of this positive statistic, the survey recorded a relatively high ratio of failing to satisfy the login requirements for multi-

factor or OTP authentication but these failures were not frequent. By excluding half of the incidents (experienced failures) caused by mistyping the code, which is a common human mistake, it can be inferred that a lack of mobile services is the cause of many login failures. However, a number of participants have different views on this, believing that the main reason for login failure is forgetting or losing a token/mobile.

Although user satisfaction with the existing OTP methods is reasonable, that does not negate the need to consolidate the overall authentication mechanism for such a crucial system. In other words, the current system is to some extent able to fulfil the needs of a large number of customers and match the functional expectations of many customers and providers of online banking services; however, at times customers find themselves unable to access their accounts because of the inability to fulfil the login requirements of the primary authentication method and at the same time the lack of alternative authentication methods. As a result of this, the demand for further investigation and consideration of this issue has emerged. The authentication system should cover most possible login scenarios to ensure high availability and less restriction.

The aim of the final section of the survey was to determine participants' views towards alternative authentication mechanisms. Specific questions were asked about graphics utilisation for authentication purposes, which were positively answered with acceptance to such technique's implementation. In addition, the participants were asked about how acceptable it would be to replace or supplement the existing one-time-password system with one-time graphical password system. The result presented that a large number (nearly half) of participants were open to the idea of using such graphical authentication in the context of online banking system with confidence.

5. Overview of the proposed solution

The conducted review of the current state of graphical techniques along with the outcome of the survey study has pointed to the need for an enhanced authentication method to fulfil the security and usability requirements. This research aims to contribute in overcoming the major issues in the existing graphical schemes to obtain an enhanced scheme that can be utilised for filling-in the authentication shortage in the online banking systems. Therefore, a hybrid secure solution is proposed – a One-Time-Graphical-Password "OTGP" which intends to leverage a multi-level authentication to ensure a robust and secure authentication. For which purpose, a combination of multiple authentication mechanisms will be employed which are a One-Time-Password along with a Graphical password. In addition, various graphical password methods have been merged to form a new mixture of Recall and Recognition-based techniques. The final component of this integrated authentication system will involve a determination task of OTP input formats. More precisely, the method will be established by solving the lock-pattern (Draw-based), followed by identifying password images (Image-recognition) and last step will be entering the corresponding OTP code according to the pre-chosen format (Knowledge-based).

132

Table 7 illustrates a breakdown of the hybrid scheme characteristics. For better clarification, this study suggests the addition of some distinguishing details in a manner that involves several design aspects. Firstly, the input approach, for instance, is what the user needs to submit as the login information for the authentication session. This input approach includes the following: Draw, Click, Choice or Typing. The second aspect is the display style, which means the presentation mode that forms the password challenge, such as: Grid, Image, Icon.

		Category	Approach	Style
1	**Pattern unlock**	Recall	Draw	Grid
2	**Image recognition**	Recognition	Choice	Multi-images
3	**OTP formation**	Recall	Typing Entry	Keyboard

Table 7: Categorisation and characteristic breakdown

The main expected technical advantages of the proposed scheme are summarised as follows:

- Combination of multiple authentication mechanisms (Graphical password and One-Time-Password).
- Combination of multiple graphical password categories (Recall-based [Draw] and Recognition-based [Choice]).
- System assigned themes with user chosen images.
- Various OTP formats.

The proposed scheme involves two phases; enrolment and authentication. The steps of the process flow for these phases are shown in more detail in Table 8.

133

General Process Flow	Enrolment Phase	Authentication Phase
Secret Knowledge (Username)	Select a unique username	Enter correct username
Pattern Unlock Graphical Password (Recall-based, Draw-based)	A 4x4 Pattern grid will be displayed. The user needs to draw a pattern as minimum of 4 points (strokes)	Unlock pattern grid by redrawing the pre-chosen pattern
Image Recognition Graphical Password (Recognition-based, Choice-based)	The system will assign 4 random themes for the user. A panel of images from each of the assigned themes will be presented for the user to make his/her own selection	The system displays a 4x4 panel of images containing (2 random pass-images out of the 4 previously chosen pass-images + 14 other decoy images). The user needs to identify the two pass-images
One-Time-Password Formation of the final password entry	Since the edge side of each row and column of the panel will be assigned 4 random digits, user can choose from a number of different OTP format combinations such as: (1st pass-image = Top axis code + 2nd pass-image = Left axis code)	Enter the associated OTP with each image in the same OTP format chosen previously
Confirmation / Authentication	Confirming the entire password process (Pattern redrawing, choosing pass-images, OTP format selection	Access is granted when all provided information is correct

Table 8: Process flow for the enrolment and authentication phases

6. Conclusion and Future Work

An overview of various authentication features provided by some of the leading banks has been presented and discussed. It was found that the adoption of multi-factor authentication using hardware token OTPs has increased. However, the study has shown that there are some failures in fulfilling the login requirement using the OTP method, even though the user experience with such a technique has been found to be satisfactory. Furthermore, carrying around multiple security tokens to manage several online accounts has been described as inconvenient and unnecessary. In this paper, the issue of the absence of an alternative authentication method when the main hardware OTP token is not present has been discussed. To overcome this issue, a general conceptual structure of the proposed solution has been introduced involving several authentication mechanisms such as graphic-based and One-Time-Password that aim to meet the main objective of having a usable secure authentication mechanism that is available anytime and anywhere without the need for additional devices. The initial features and advantages of the OTGP scheme were briefly presented. The next phase will look at system implementation with initial user trials

134

and lab experiments. Statistical data such as time, security level, and password memorability over time intervals will be some of the outputs of the experiment. Upon the assumption of positive results from the initial trials, the final phase of the OTGP project will then expand the study through a field experiment to obtain a wider range of participants for more accurate results.

7. References

Alexander, C. (2008) 'Two Factor Authentication That Doesn't Use Chips'. *Card Technology Today*, 20 (5). pp 9.

Anderson, R. J. (2001) 'Access Control'. *Security Engineering: A guide to building dependable distributed systems.* 1st edn.: Wiley, pp 51-71.

AuthenticationWorld.com (2012) *Password Authentication*. Available at: http://authenticationworld.com/Password-Authentication/index.html (Accessed: 02/04/2014).

Chakrabarti, S. & Singbal, M. (2007) 'Password-Based Authentication: Preventing Dictionary Attacks'. *Computer*, 40 (6). pp 68-74.

De Angeli, A., Coventry, L., Johnson, G. & Renaud, K. (2005) 'Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems'. *International Journal of Human-Computer Studies*, 63 (1–2). pp 128-152.

Dhamija, R. & Perrig, A. (2000) 'Déjà vu: A User Study Using Images for Authentication', *the 9th USENIX Security Symposium*. pp. 45-58.

Dube, D. & Gulati, V. P. (2005) 'Information System Audit and Assurance'. (Appendix B). pp 594.

FFIEC (2003) 'FFIEC E-Banking Booklet'. [Online]. Federal Financial Institutions Examination Council. Available at: http://www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/GroupDocuments/e_banking.pdf (Accessed: 02/04/2014).

Fu, K., Sit, E., Smith, K. & Feamster, N. (2001) 'Dos and Don'ts of Client Authentication on The Web', *Proceedings of the 10th conference on USENIX Security Symposium*. Washington, D.C. USENIX Association, pp. 19-19.

Furnell, S. (2005) 'Authenticating Ourselves: Will We Ever Escape the Password?'. *Network Security*, 2005 (3). pp 8-13.

Furnell, S. & Zekri, L. (2006) 'Replacing Passwords: In Search of the Secret Remedy'. *Network Security*, 2006 (1). pp 4-8.

Gyorffy, J. C., Tappenden, A. F. & Miller, J. (2011) 'Token-based Graphical Password Authentication'. *International Journal of Information Security*, pp 1-16.

Kuber, R. & Yu, W. (2010) 'Feasibility Study of Tactile-based Authentication'. *International Journal of Human-Computer Studies*, 68 (3). pp 158-181.

McDonald, D. L., Atkinson, R. J. & Metz, C. (1995) 'One Time Passwords in Everything (OPIE): Experiences with Building and Using Stronger Authentication', *the Proceedings of the 5th USENIX Security Symposium*. Salt Lake City, Utah.

Pinkas, B. & Sander, T. (2002) 'Securing Passwords Against Dictionary Attacks', *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, pp. 161-170.

Ray, P. P. (2012) 'Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices'. *Journal of Information Engineering and Applications*, 2 (2). pp 1-11.

relbanks.com (2012) *Banks Around the World*. Available at: http://www.relbanks.com (Accessed: 02/4/2014).

RBS (2014) Will I be charged for any mobile phone text alert messages I may get? - Ask a Question. The Royal Bank of Scotland ©. Available at: http://supportcentre-rbs.custhelp.com/app/answers/detail/a_id/745/kw/network%20operator (Accessed: 12/4/2014).

Suo, X., Zhu, Y. & Owen, G. S. (2005) 'Graphical Passwords: A Survey', *Computer Security Applications Conference, 21st Annual*. 5-9 Dec. 2005. pp. 10 pp.-472.

Verizon (2013) *2013 Data Breach Investigations Report*. Verizon Enterprise Security Solutions. Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf (Accessed: 02/04/2014).

Weir, C. S., Douglas, G., Richardson, T. & Jack, M. (2010) 'Usable Security: User Preferences for Authentication Methods in eBanking and the Effects of Experience'. *Interacting with Computers*, 22 (3). pp 153-164.

Williamson, G. D. & Money–America's, G. (2006) 'Enhanced Authentication in online Banking'. *Journal of Economic Crime Management*, 4 (2).

Yampolskiy, R. V. (2007) 'User Authentication via Behavior Based Passwords', *Systems, Applications and Technology Conference, 2007. LISAT 2007. IEEE Long Island*. 4-4 May 2007. pp. 1-8.

Zhao, Z., Dong, Z. & Wang, Y. (2006) 'Security Analysis of a Password-based Authentication Protocol Proposed to IEEE 1363'. *Theoretical Computer Science*, 352 (1–3). pp 280-287.

136

2) H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell, "Secure Graphical One Time Password (GOTPass): An Empirical Study," Information Security Journal: A Global Perspective, vol. 24, pp. 207-220, 2015/12/31 2015.

Secure Graphical One Time Password (GOTPass): An Empirical Study

H. Alsaiari, M. Papadaki, P. Dowland & S. Furnell

Taylor & Francis
Taylor & Francis Group

Secure Graphical One Time Password (GOTPass): An Empirical Study

H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell
Centre for Security Communication and Network Research, School of Computing Electronics and Mathematics, Plymouth University, Plymouth, United Kingdom

ABSTRACT The traditional text-based password has been the default security medium for years; however, the difficulty of memorizing secure strong passwords often leads to insecure practices. A possible alternative solution is graphical authentication, which is motivated by the fact that the capability of humans' memory for images is superior to text, which helps to improve password usability and security. Recently, some implementations of graphical authentication techniques have been deployed in practice. This paper introduces a new hybrid graphical authentication, "GOTPass," that authenticates by means of a one-time numerical code that needs to be typed in based on a sequence of secret images and a prechosen input format. An important focus for this paper was the security aspects of the graphical password scheme. This paper reports an in-depth analysis of the security evaluation and shows a high resistance capability of GOTPass against common graphical password attacks. Three attacks were simulated (Guessing, Intersection, and Shoulder-surfing), and the results showed that nearly 98% of the 690 attempts failed to compromise the system.

KEYWORDS authentication, graphical passwords, knowledge-based one-time password, usable security

Address correspondence to H. Alsaiari, Centre for Security Communication and Network Research, School of Computing Electronics and Mathematics, Plymouth University, Drake Circus, Plymouth, PL4 8AA, United Kingdom.
E-mail: hussain.alsaiari@plymouth.ac.uk

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/uiss.

1. INTRODUCTION

The conventional text-based password is the most convenient and commonly used approach to authenticate users. However, this method has well-known defects and deficiencies in practice (Xiaoyuan, Ying, & Owen, 2005). Users may tend to select easy-to-guess passwords or, when choosing complex passwords, usually find it difficult to remember the paswords, which may lead to other insecure behaviors such as writing passwords down or using the same password repeatedly for multiple accounts (Dhamija & Perrig, 2000). Thus, the need for substitutes for traditional authentication methods has emerged to achieve secure and reliable authentication.

Graphical authentication is one of the proposed alternatives to text-based schemes. Instead of remembering long set of characters, a user can be authenticated by recognising predefined images or recreating graphical drawings (Rittenhouse, Chaudry, & Lee, 2013). The idea of using images instead of text or numbers was motivated by the assumption that presenting items as pictures is easier to remember than presenting items as words (Snodgrass & Asiaghi, 1977). Thus, the pictures superiority

207

effect appears to substantially increase memorability. According to Renaud and De Angeli (2009), "humans have a vast, almost limitless memory for pictures which they remember far better and for longer than words" (p. 135–140). In addition, pictorial passwords include other possible advantages, such as enlarging the passwords space, reducing choosing trivial passwords, and making it difficult to share and write down passwords (Gołofit, 2007). Since the mid-1990s, many graphical password schemes have been proposed aimed at enhancing the password memorability and strengthening security. More recently, graphical password approaches have started to gain popularity inline with the revolution of online services and mobile devices that demand friendlier alternatives to traditional methods. However, graphical passwords are not vulnerability-free since the authentication interface is exposed which allow direct observation or recording for the authentication session so attackers can capture the input screen along with the entered password (Gao, Jia, Ye, & Ma, 2013). Graphical passwords are susceptible to various types of attacks such as guessing, shoulder-surfing, and intersection (Biddle, Chiasson, & Van Oorschot, 2012).

This paper addresses the security capabilities of a new graphical mechanism based on a user study conducted to assess the potential of the GOTPass scheme to withstand common security threats. Attack-alike simulations were designed to enable a proper security evaluation and to measure the system reaction against various attacks. Participants of all experiment types were requested to use the same test machine to try compromising the system using different attack methods.

The rest of the paper is structured as follows: Section 2 presents the security concerns and threats on graphical authentication and covers part of the security-related work on graphical authentication. Section 3 explains the design and process of the new GOTPass scheme. Section 4 highlights the GOTPass security aspects, and section 5 reports the experiments and the evaluation results. Section 6 presents an overview of the usability study results. Section 7 provides an overall discussion, and section 8 concludes.

2. SECURITY CONCERNS AND THREATS

2.1. Guessability

Guessability is a measure of how simple it is for an attacker to guess the authentication secret of a legitimate user. In recognition-based authentication, prioritized guessing attacks try to increase the probability of selecting the correct image through the prioritization of the more commonly selected images (English & Poet, 2011a).

2.2. Observability

2.2.1. Shoulder-Surfing

When authenticating in public places, shoulder surfing is of real concern since it enables an attacker to capture an individual's password by direct observation or by recording the entire authentication session (Lashkari, Farmand, Zakaria, Bin, & Saleh, 2009). A general goal of resisting shoulder surfing attack should be to harden the attacker's task of learning enough key images that lead to a successful future replay attack (Dunphy, Heiner, & Asokan, 2010). However, several conditions like the required shooting angle and lighting have shown that video shoulder surfing seems less practical than expected (Schaub, Walch, Könings, & Weber, 2013).

2.2.2. Intersection Attack

Intersection attack is possible when the role of an image as either a pass-image or a distractor can be determined by the frequency of its appearance at login. That in turn allows the attacker to use the most frequently viewed images to pass the challenge screen and gain access (English & Poet, 2012). In addition, a *source intersection attack* is an attack that possibly occur when pass-images and distractors are each drawn from unlike image sources such as personal images and drawings (Dunphy et al., 2010).

2.3. Recordability

2.3.1. Replay Attack through Eavesdropping

Intercepting the communication between authentication client and server can enable attackers to capture the transmitted image portfolios and the user selection. Afterwards, the copied login data can be replayed again to the server to potentially obtain a false positive access (English & Poet, 2011b) (Van Oorschot & Wan, 2009).

2.3.2. Phishing

A phishing attack is based on tricking users into submitting their login information at a fraudulent website that records users' input. The need for presenting a correct set of images to the user prior to password entry makes this type of attack difficult with recognition-based systems.

H. Alsaiari et al.

In schemes with variant responses, multiple server probes would be necessary since only a portion of the user's secret is exposed on each login attempt (Biddle et al., 2012).

2.3.3. Spyware

2.3.3.1. Keystroke-loggers

Some graphical password schemes utilise the keyboard to input login information. By this means, user's input can be captured using keystroke-loggers unless the input's content is varied at each login time (Gao et al., 2013).

2.3.3.2. Screen-scrapers

Screen-scrapers install software on a computer to record the user's operating activities. Under normal circumstances, the difficulty of installing spyware on a user's computer without being noticed makes screen-scrapers a less serious threat (Gao et al., 2013).

2.3.3.3. Other Spyware

Combining keystroke-loggers and screen-scrapers is a method of attack that can obtain both the screen content and the keyboard input information. It is clear that this type of threat can be of an increased risk to the development of graphical password security (Gao et al., 2013).

2.4. Dictionary Attack

The idea of the dictionary attack is based on trying all possible passwords from a relatively short preassembled list (dictionary) of high probability candidate password collected from experimental data or assumptions about user behavior (Biddle, Chiasson, & Van Oorschot, 2009).

2.5. Safeguarding Graphical Passwords

An important security measure is to protect graphical authentication information against malicious observations that steal credential information. Observation threats come in different forms, either direct observation by an adversary such as shoulder-surfing attack or indirect such as camera recordings. Therefore, it is necessary to protect the authentication scheme from such attack. Authentication information should not be exposed during the data entry phase or should complicate the extraction of secret authentication data in case the input process is being viewed by others.

Many graphical password methods have been proposed, but with different aims, leading to several limitations. Gao, Liu, Wang, and Dai (2009) and Wang et al. (2010) developed an anti-spyware solution based on a challenge-response protocol to enhance the security by using CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart). The new authentication scheme is a combination of graphical password and textual CAPTCHA.

Van Oorschot and Tao Wan (2009) came up with a new scheme called "TwoStep." This scheme is a hybrid user authentication approach that uses traditional text passwords and recognition-based graphical passwords. In the first step, users will still use a text password. The second step involves entering a graphical password. Since text passwords are vulnerable to phishing attacks as well as keylogger attacks, this scheme aims to overcome such security issues by complementing the text password with the graphical password. A successful attack of this type will need prior knowledge of users' images, which is usually not possible.

Shoulder-surfing resistant techniques were proposed to protect recognition-based graphical passwords. Khot, Kumaraguru, and Srinathan (2012) proposed the WYSWYE (Where You See is What You Enter) scheme. In this technique, users are not required to select their password images by clicking on them. Instead, they are only used to locate the associated positions to be marked in the response grid. So looking over a user's shoulder could only allow the capture of random clicked positions on the response grid. Thus, a shoulder-surfing attack is ineffective since it is hard to correlate the marked positions back to the password images in the challenge grid. In addition, randomly guessing the password through brute force is not feasible since it produces a one-time password that is valid only for one session. This scheme can also resist the intersection attack since all login sessions will use the same set of images.

3. THE GOTPASS APPROACH

Graphical **O**ne **T**ime **Pass**word, or GOTPass, is a hybrid secure solution that leverage a multilevel authentication to ensure a robust secure authentication. A combination of multiple authentication mechanisms are employed using a graphical password along with a one-time password. Moreover, an integration of various graphical password methods has been implemented to form a new mixture of recall and recognition-based techniques. The

TABLE 1   Categorization and characteristic breakdown of GOTPass scheme

		Category	Approach	Style
1	Pattern unlock	Recall	Draw	Grid
2	Image recognition	Recognition	Choice	Multi-images
3	OTP input format	Recall	Typing entry	Keyboard

final component of this authentication system involves a determination task of GOTPass input formats, that is, the location of the associated codes. More precisely, the method will be established by solving the lock-pattern (draw-based) similar to that of an Android unlock pattern (Biddle et al., 2012), followed by identifying pass-images (image-recognition). The final step will be entering the corresponding one-time code according to the prechosen format (knowledge-based). Table 1 illustrates the characteristics of the hybrid scheme and shows a breakdown of these classifications for each technique separately.

The main technical advantages of the proposed scheme include the combination of multiple authentication mechanisms (graphical password and one-time password), combining multiple graphical password categories (recall-based [draw] and recognition-based [choice]), system assigned themes with user chosen images, and the implementation of various GOTPass input formats (code locations).

3.1. Enrollment

The registration involves three main phases. First, users need to choose a unique username and draw any shape on a 4x4 unlock pattern panel. Second, the system will automatically assign four random themes for each user, one after another. In each theme selection round, 30 images will be displayed for the user to select one pass-image from each of the given themes (total four all together). This is the pass-images portfolio that will provide a dynamic

pass-images pool without burdening the user memory. Finally, the position of the pass-images in the grid will be used to indicate a code that needs to be entered using the keypad/keyboard that is referred to as the GOTPass input formats. These codes are located on top or left axis of each pass-image. There are two security level options for the user to choose from either basic or advanced. In the basic security level, the numeric codes for both pass-images are taken from the same axis whereas the numeric codes in the advanced level are taken from different axis for each pass-image. Inside each option, there are further code combination options for the system to randomly assign to the user. The assigned input format is clearly presented to the user with an illustration example (e.g., top axis for first pass-image + left axis for second pass-image). GOTPass input format is implemented to complex the observation attack in such a way that each pass-image can have more than combination code options. Table 2 shows details of the GOTPass input format combination options.

3.2. Authentication

The system will prompt the registered user for the username and display an on-screen pattern lock (Figure 1), which requires the user to redraw the predefined unlock pattern shape by reconnecting nodes to reform the correct pattern shape.

Despite the supplied information being correct or not, the next step of the authentication will display a fresh

TABLE 2   GOTPass input format combination options

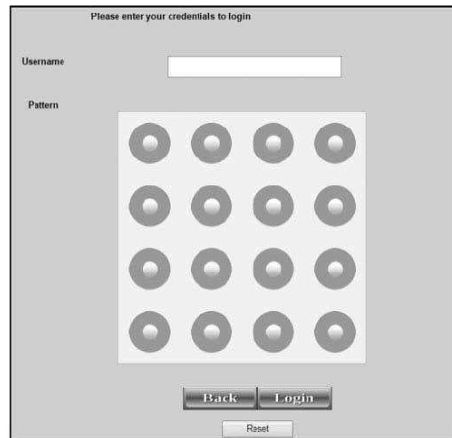| User choice	Random system assigning		
Security level	Option	Pass-image	Code
Basic	Option 1	1st pass-image	from **TOP** axis
		2nd pass-image	from **TOP** axis
	Option 2	1st pass-image	from **LEFT** axis
		2nd pass-image	from **LEFT** axis
Advanced	Option 3	1st pass-image	from **TOP** axis
		2nd pass-image	from **LEFT** axis
	Option 4	1st pass-image	from **LEFT** axis
		2nd pass-image	from **TOP** axis

H. Alsaiari et al.

398

FIGURE 1 "GOTPass" unlock pattern step.

(4x4) image panel, as illustrated in Figure 2, containing dummy images when the information of the previous step is incorrect. Otherwise the panel will contain two random pass-images out of the four previously chosen pass-images, six distractor images that are associated with the pass-images (three distractors for each pass-image), and eight random decoy images. The system generates new OTP codes and fills the panel edges (axis) of each row and column (only the occupied locations by the correct pass-images will contain the correct GOTPass codes). To complete the authentication process, the user must first identify the password images among others in the panel. From the grid top and left axis, the user needs to locate and enter the codes associated with each pass-image (the code should be entered in the correct format as previously assigned and shown in the registration phase). The search navigation for the pass-images should be carried out on a row basis starting from the top left corner down to the bottom of the panel. That makes it necessary to select the pass-images and thereafter the associated codes in the right order depending on which pass-image appears first. Once the system ensures that all provided information is correct then the user is successfully authenticated and granted access.

From a developmental prospective, the system was simply designed to save the application images on the webserver and store their unique IDs into the database. During authentication, the login grid is filled with pass-images and decoy images. The system then generates two sets of random numeric codes and place them on the designated boxes corresponding to the correct pass-images whereas the remaining boxes are filled in with other arbitrary codes. Hence, a successful login attempt requires identifying the pass-images and entering their associated one time codes.

FIGURE 2 "GOTPass" image recognition and OTP code entry.
Assuming security level option 3 is in use (Top axis for 1st pass-image + Left axis for 2nd pass-image).

Secure Graphical One Time Password (GOTPass) 211

4. GOTPASS SECURITY

In this scheme, users must enter the correct OTP provided through the recognition-based graphical password. In addition, a number of advantages are offered to strengthen the proposed technique, such as providing dynamic secrets with no reliance on static password or pass-images or implicit authentication feedback in which the scheme does not reveal any indication about the status of the login session. However, the inability to spot the correct pass-images by the legitimate users is a type of alert that something is wrong with that login attempt which must be corrected.

As pointed out by Biddle et al. (2012), allowing users to choose their own passwords can enable a personalized attack where the probability of guessing the user's password by a person who knows the user might be higher than other attackers. However, system assigned images lead to usability issues derived mainly from the difficulty of remembering random images (Chiasson, Forget, Biddle, & Van Oorschot, 2008). Due to these conflicting problems, a new balanced approach has been adopted that benefits from the advantages of both techniques. The idea is to have themes assigned by the system and then allow the user to select the preferable images among each assigned theme. This can reduce the likelihood of bias choice, hot-images, and personal preference images, but at the same time should keep the task simple for users to remember the images they selected.

As far as the security of the proposed system is concerned, GOTPass aims to be equipped with high security features without sacrificing the usability of the system. Table 3 contains a list of these security features with a brief description of the anticipated advantages of each feature. However, the expected size of the password space is not long enough, which can be a disadvantage. Most of the recognition-based schemes suffer from the low password space compared with the conventional text-based password (Xiaoyuan et al., 2005), but GOTPass leverages multilevel authentication, which should complicate any potential attack that may exploit the password space size.

5. SECURITY EVALUATION

Various general evaluation criteria have been proposed to assess different aspects of the authentication system's security. Among these proposals, De Angeli, Coventry, Johnson, and Renaud (2005) have considered three basic dimensions for security evaluation: guessability, which

measures the impostor's ability to guess the password; observability, which measures the impostor's ability to monitor the password while it is being entered by the user; and recordability, which measures the impostor's ability to record/capture the user's password. Moreover, Gao et al. (2013) discussed spyware as an additional password-capturing-based attack.

Furthermore, English and Poet (2011b) have taken advantage of the same categorization with further expansion that results in four-tuple evaluation metric. Potential attacks against recognition-based graphical password were classified under one of the main related threat categories that are presented in Table 4. The security evaluation criterion is determined by whether the identified countermeasure/security benefit is provided by the scheme or not. Eventually, the scheme can present the overall level of resistance against particular types of attack by the number of applied countermeasures.

In this section, two types of the security evaluation are discussed: theoretical based on assessment criteria and empirical, where several attacks were simulated and tested.

5.1. Preliminary Theoretical Security Evaluation

The main security threats of recognition-based graphical authentication have been gathered alongside the suggested countermeasures to form a scoring table. By adopting a similar evaluation approach as that proposed by English and Poet (2011b), the scoring procedure can be slightly enhanced to suit a hybrid scheme such as GOTPass. Appropriate weights for the countermeasures are provided by a four-point scoring method motivated by the ranking framework of Bonneau, Herley, Van Oorschot, and Stajano (2012). The scoring technique is adapted to present the overall level of resistance against particular types of attack based on whether the countermeasure is being implemented or not using the following scale points [No (0), Partially (1), Almost (2), Yes (3)].

The result of the 'theoretical' security evaluation is shown in Table 4, which contains the threats alongside a list of the countermeasures and their scores.

The GOTPass scheme has scored 68 points out of 72, which seems encouraging but also needs to be supported by an empirical proof that reflects the same high security level. Among all the countermeasures listed in Table 4, GOTPass scheme scored the maximum in all but three of them. First

TABLE 3 GOTPass security features

Security features	Advantage
Shuffling images	Reduce the risk of observation attack, which observes several login sessions to look for unchanged pass-images if always located in the same position.
Online verification	Utilising the unlock pattern technique as a proactive check to act as a first line of protection.
System assigned themes	Decrease guessing chances caused by hot-images or known personal image preferences. However, user will have the chance to select the preferable images from among the assigned themes to avoid affecting the usability by keeping good memorability level.
Pass-image portfolio	System will randomly present a subset of the users' pass-images (2 out of 4) in each authentication session. That should mitigate the observation, phishing, and reply attacks.
Distractor images portfolio	Ensure that recording multiple challenge screens to figure out the high frequency images is ineffective through maintaining constant distractors for a given pass-image.
Account lockout	Limit the number of consecutive incorrect attempts and apply a delay between login attempts to prevent excessive guessing tries and dictionary attack.
Implicit authentication feedback	The status of the login session is not revealed until after the final submission. Attacker will have no indication of which part of the scheme went wrong. That should resist guessing attack.
One-time password	Resist eavesdropping attacks and credential theft.
Shoulder-surfing resistant	The use of multilevel authentication makes it hard to record multiple login techniques. The transparency of the unlock pattern drawing disguises the correct pattern shape and thus makes it hard to capture. No indicator of image selection, so onlooker cannot identify password images.
Difficult to guess	Guessing various login techniques is made hard by implementing a multi-level authentication. OTP is changeable every time. Authentication feedback is only given at the end of the login session. That is also called implicit feedback which should only be recognisable and useful for the legitimate user.
Dictionary attacks resistant	The use of multilevel authentication makes it hard to conduct an online dictionary attack on multiple login techniques, e.g., unlock pattern should protect the primary authentication method (image recognition). On top of that, the use of OTP should mitigate this type of attack.
Safe against spywares	Both keystroke logger and screen recording are needed to gain enough knowledge of the password components, which is mostly time, effort, and cost overhead for attackers.
Anti-phishing and replay attack	Presenting a correct set of images to the user prior to password entry makes it difficult. The implementation of variant responses exposes only a portion of the user's secret on each login attempt.

is "Disallow user choice of images;" as mentioned previously, this issue was avoided by assigning random themes to the users and allowing them to choose form the images inside each theme, which should restrict user choices. Second is "SSL implementation;" it can be assumed that the connection is secured by an SSL implementation, but since there was no actual implementation of that countermeasure in the prototype, it was given 1 score only. Third is "Protect images database;" securing the database was taken into consideration while implementing the system. However, there is a chance for security improvement by storing images directly into the database in the form of BLOBs data type then apply appropriate encryption. In fact, that might have an effect on the performance of

401

TABLE 4   The result of the 'theoretical' security evaluation

Category	Security concern	Threat	Countermeasure	Score
Password Capture-based	Guessability	Guessing attack	Disallow user choice of images	2
			Select distractors from random categories	3
			Wide range of image categories	3
			Display images from same categories	3
			Provide implicit feedback for incorrect input	3
	Observability	Shoulder surfing	Show no or disguised indicator of selection	3
			Greater pass-images number than that of challenge screens	3
			Variable response	3
			Indirect input	3
		Intersection analysis	Constant display of distractors and pass-images, or	
			Present a small constant subset of distractors for each given pass-image	3
			Display distractors only in subsequent challenge screens following any incorrect attempt	3
			Limit the number of attempts for unsuccessful authentication	3
			No pass-image portfolio implementation, or	
			Implement pass-image portfolio + Distractor portfolio	3
			Pass-images and distractors are not drawn from distinct sources	3
	Recordability	Replay attack	Random image location	3
			Submit different value each time	3
			Implement pass-image portfolio	3
		Phishing attack	SSL implementation	1
			Protect images database (without knowledge of user's images beforehand, it would be difficult to present images to extract user's graphical password)	2
	Spyware	Keystroke-loggers	Varied input's content at each login time	3
		Screen-scrapers	Use shielded input characters	3
			No indication of selection	3
Password space-based	Online dictionary attack		Limiting the number of incorrect attempts	3
			Increase the delay between any 2 consecutive error logins	3
Total				**68**

the image retrieval which requires further investigation and testing.

5.2. Security Experimental Evaluation

The GOTPass prototype was developed as a web-based application using Microsoft Visual Studio 2013—C#, and SQL Server 2012 as the database management system. The prototype application was hosted on a laptop with 15.6" screen display set at a resolution of 1366 x 768 pixels and running windows 8.1. As the main purpose of the prototype development was to prove the concept of the proposed solution, there are some limitations in the current state of the implementation that can be carried out in the future work such as the lack of encryption and secure SSL connection.

Experiments to evaluate the security of the GOTPass approach were conducted in a controlled lab environment since the physical attendance for all users was required. Due to the difficulty of hiring expert testers to undertake the attacks on the proposed system, ordinary participants were recruited and asked to take part in this security experiment. For that reason, the activities of the study were simplified to suit typical users who may not require

H. Alsaiari et al.

hacking tools or special experience. All participants used the same computer to perform the study tasks. Only the research investigator and the participant were allowed in the lab to avoid any possible disruption and to observe any usability or security issues as well as record participants' comments.

The security experiment involved 81 participants (63 male, 18 female). Participants were recruited via several invitations using staff, student portals, emails, and posters. Thus, most participants were university staff and students, with a mixture of educational levels between undergraduate and postgraduate. Most participants were 18–39 years old. Thirty-three percent of them reported an advanced level of computer experience, yet 50% indicated an intermediate level. Almost all participants pointed out that they knew about at least one type of the graphical password techniques.

Three security attacks were planned and simulated (guessing, intersection, and shoulder-surfing) to evaluate the capability of the proposed system to withstand these types of attacks. Participants were asked to devote attention to the task of each given attack and act as attackers to try to break-in. In all security experiments, there was no direct interaction between the actual victim and the attacker (participant) since the victim was simulated in a form of recorded videos. The security experiment trials were conducted using the same GOTPass prototype application but using a different database to avoid interfering and affecting the data of another parallel experiment focusing on usability aspects of the approach.

The study collected a total of 690 login attempts carried out by 81 participants. These were divided into three groups based on the assigned security attack experiment, as shown in Table 5.

5.2.1. Guessing Attack

In this type of attack, attackers try to guess the authentication secrets of a legitimate user. In order to successfully guess GOTPass credentials, the attacker must guess three combined steps: unlock pattern shape, two pass-images,

TABLE 5 Number of users & attempts in each experiment

Attack type	Number of users	Number of attempts
Guessing	27	235
Shoulder-surfing	27	210
Intersection	27	245
Total	81	690

and finally the input format of OTP code combination, which is computationally hard.

A group of 27 participants who were already familiar with the system took part in this trial. Their task was to act as attackers to guess a particular account credentials. An additional account was created for this purpose, and some general information about that account was revealed to help attackers guess it correctly. The given information was the username, the shape of the pattern, and the selected security level of that account. In order to validate participants' guesses, they were given the chance to use the GOTPass system and try to login with the information they managed to gather. Each user was allowed maximum of 10 attempts unless they decide to give up after their fifth attempt.

That in turn allowed further investigation of two points:

• The level of difficulty to guess user credentials and
• The effectiveness of revealing GOTPass secrets to others.

The total number of break-in attempts in this attack trial was 235 (Table 6). Only two attempts were successful which considered less than 1%, whereas four attempts were recorded as coincident due in part to the correct credentials being incorrect but succeed. They succeeded by chance, missing one of the pass-images but submitting the correct associated codes. It is worth mentioning that within the first five attempts for all users, only four attempts (3%) succeeded on guessing the correct unlock pattern (Figure 3). However, those successful pattern guesses were followed by unsuccessful ones since users were uncertain about the correctness of their guesses due to the implementation of the implicit feedback. After the first five attempts, the experimenter helped the users by solving the unlock pattern for them and giving them the chance to guess the remaining part that included the pass-images and the input format for five more times. Thus, a significant finding can be inferred that implementing the unlock pattern in the prototype is effective since it proves its ability to act as a first line of defense to protect the main recognition-based graphical password.

Another investigated point was the effectiveness of revealing GOTPass secrets to others. The analysis of this attack experiment shows that passing account secrets (unlock pattern, passimages, input format) to another person was not easy and thus ineffective. At first, users could not manage to guess the correct pattern which was given as a shape of number 2. Due to the high number of

Secure Graphical One Time Password (GOTPass)   215

TABLE 6   Details about the guessing attack trial

Participants	Attempts	Success	Coincident	Total	Success with aid
27	235	2	4	6	6
33%	34.1%	0.9%	1.7%	2.6%	100%
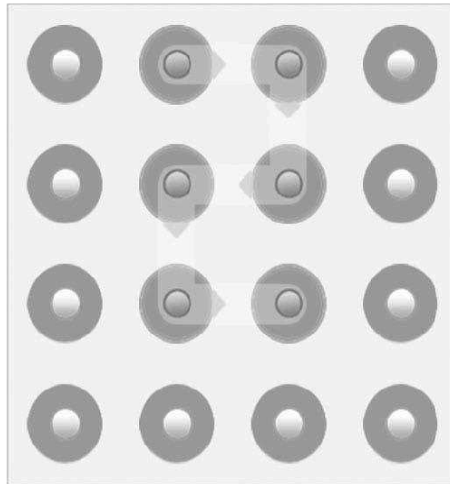
FIGURE 3   The shape of the correct unlock pattern to guess (shape of number 2).

variations of that shape, it was clearly hard to determine the correct pattern. One of the possible additions to ease this part was to provide the starting point of the shape and the size (how many points) to the attacker, which needs further investigation to ensure its validity. With regards to the pass-images, since the system might display images from the same category or even similar images with different colours, that should complicate the accuracy of the information revealed as well as increase the uncertainty. Revealing the security level helped determine whether basic or advanced would also require the user to choose from the two available suboptions. Thus, passing the exact input format (e.g., the code of the first pass-image from top and second from left) should be more useful than knowing the security level. In addition, users were asked in the posttest questionnaire about what they think about the simplicity of passing their account information to friends and their ability to use this information to login on their behalf. More than 70% of the participants thought that

their friends would still have difficulty logging in correctly using the information gained about the GOTPass secrets.

5.2.2. Observability—Shoulder Surfing Attack

Assuming that the attackers managed to pass the first defence technique (unlock pattern), they will still be confronted by another security barrier that is the image recognition and its associated OTP technique. Selecting pass-images is done only mentally, which means there is no need for selecting or clicking on the required images. Determining the pass-images is only used to find the respective code positions that the user needs to enter in the OTP field. Consequently, the attacker who tries to peep over the shoulder or record with hidden cameras could only manage to capture random numbers being entered. However, observing multiple login sessions where the entered codes are also visible might enable the attacker to discover the pass-images based on the intersection and correlation among the observations.

In this part of the experiment, the system resistance against the shoulder surfing attack was examined. This simulation involves the experimenter acting as a victim with arrangement for the participants to watch the login trials to gain as much information as possible to try using it to gain an unauthorised access. An additional account was created and used for logging for three times. During that time, the scene of the experiment machine was being filmed (the camera was intentionally placed at a location less immediately adjacent to the user entering the login data). A different group consisting of 27 users participated in this study in which they were displayed the captured video of the login attempts for two times and were allowed to take notes while watching the video to help them gather information about the user account that they need to break. In order to validate the captured information, users were given the chance to use the GOTPass system and try to login with the information they managed to collect. The allowed login attempts were limited to 10; however, in case users want to give up earlier, they have the right to stop after completing the fifth attempt.

216

H. Alsaiari et al.

TABLE 7 Details about the shoulder-surfing attack trial

Participants	Attempts	Success	Coincident	Total	Success within last 5 attempts
27	210	6	5	11	9
33%	30.4%	2.9%	2.4%	5.2%	81.8%

FIGURE 4 A screenshot from the shoulder-surfing attack simulation video.

In this experiment, users carried out 210 attempts in total. As shown in Table 7, users managed to gain correct access six times (equivalents to 3%) and five other attempts were reported coincident. Although the rate of break-in using shoulder surfing attack was about 5%, that might be due to the nature of filming the scene for the attack simulation, which involved the screen and keyboard as shown in Figure 4. That in turn allows easier capturing for the needed information since the challenge set data and the entered code via the keyboard are all provided. In addition, drawing the pattern unlock was designed to be less visible (semi-transparent) for peepers but visible enough for the close legitimate user as shown in Figure 3. However, this type of attack seems less complicated than others as the attackers can gain information that might facilitate the break-in task and with some intensive analysis, the attempt might succeed.

5.2.3. Observability—Intersection Attack

Using intersection by its own will not reveal much information as pass-image and distractor portfolios are implemented. An attacker would face difficulties distinguishing between pass-images that are valid to locate the code positions and the distractors that are linked to each pass-image. In addition, in case users succeeded in finding
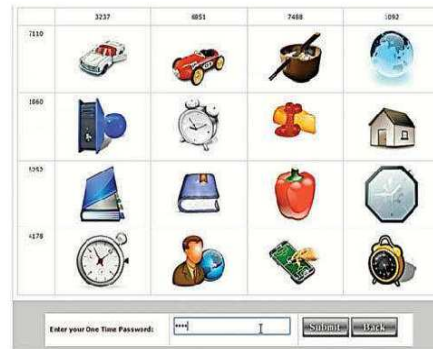
FIGURE 5 A screenshot from the intersection attack simulation video.

the correct pass-images, they will still need to correctly guess the correct input format (code location).

Another security experiment task was to inspect the system resistance to intersection attack. Simulating the attack used similar approach as described previously in the shoulder surfing attack subsection. An additional account was used, and 27 participants were displayed a video of screen capturing the login attempts of that specific account three times (Figure 5). Watching the video was repeated two times for each user. Note taking was allowed and then participants were given 10 login attempts as a maximum, where they needed to identify the pass-images of that account at first then guess the correct input format.

Despite the fact that the screen capturing of all login components were clearly visible and easy to note down except the entered data, which was shielded, none of the 245 attempts to break-in using intersection attack was successful, except for the six attempts that succeeded coincidently (Table 8). It can be inferred from this result that conducting a successful attack would need both information from the challenge set as well as the keyboard, which proves the effectiveness of separating the challenge mean and the data entry mean to mitigate such attacks.

Secure Graphical One Time Password (GOTPass) 217

TABLE 8 Details about the intersection attack trial

Participants	Attempts	Success	Coincident	Total	Success within last 5 attempts
27	245	0	6	6	3
33%	35.5%	0	2.4%	2.4%	50%

6. USABILITY EVALUATION

A successful authentication system should keep a balance between usability and security. System usability is an essential design aspect that should not be compromised for security (and vice versa). A parallel work (to be published separately) was also conducted to evaluate the usability aspects of the approach. However, in the interest of clarity, the key points from the preliminary results are also presented in this paper.

The usability user study included three separate user trial sessions on the first day of the study, one week later, and after one month. The experiment was conducted over five weeks and involved 81 participants who attended all three sessions. The study reported quantitative results for usability components (effectiveness, efficiency, and memorability) as well as qualitative results for the user satisfaction collected from the surveys of user perceptions.

The average time for GOTPass registration was 134 seconds. Although the registration time was relatively high, it was considered generally acceptable for most participants as indicated in the post-test questionnaire result where 80% of the users stated that they managed to complete the required tasks quickly. As for the login phase, data from 1,302 login attempts carried out by all participants were analyzed. The average login time was 24.5 seconds. The long input time was expected since the login task involved a number of keystrokes and mouse activities. A significant reason influencing the performance time of an authentication scheme is the involvement of multiple steps, which justifies the longer time taken by GOTPass to register and login as well. However, GOTPass is still comparable to other two-step approaches and even superior within its category (three-step).

The result shows a relatively high success rate of over 93% of the attempts were successful. Interestingly, the study showed that none of the users was completely unable to login within the given attempts. Furthermore, participants carried out a memorability experiment twice. The first took place after one week of nonuse in trial 2 and second was a month later in trial 3. The results showed that all users managed to login successfully using their GOTPass accounts within three tries and with no lockout event.

7. DISCUSSION

Table 9 shows a summary of the experiment results where the total number of the successful break-in attempts was 23 out of 690, which represents only 3.3%. This rate is relatively low, and the results are encouraging since attack simulations were deliberately designed to facilitate misuse. In reality, it seems difficult to capture several login sessions from a close distance as in the simulations, which means an attack in a real environment should be more complicated than that in the lab. In addition, almost all participants used the "trial and error" method to solve the break-in tasks.

The number of the successful attempts of the shoulder-surfing attack trial was higher than that of the other attacks. The success rate for shoulder surfing attack occupy about half of the total successful attempts whereas the other half is divided nearly equally between guessing and intersection attacks.

A few observations about exceptional incidents were reported. Table 10 contains interesting results that explain the exceptional incidents that resulted in unexpected outcomes or the so-called coincident attempts. Mainly, there

TABLE 9 Number of successful break-in attempts

	Success	Coincident	Total	Percent
Guessing	2	4	6	6/235*100 = **2.6**
Intersection	0	6	6	6/245*100 = **2.4**
Shoulder-surfing	6	5	11	11/210*100 = **5.2**
Total	8	15	23	23/690*100 = **3.3**
%	8/690*100 = **1.2**	15/690*100 = **2.2**	23/690*100 = **3.3**	

H. Alsaiari et al.

TABLE 10 Breakdown of the exceptional incidents

Pass-image 1	Pass-image 2	Input format (code location)	Code order	Final result	Attack	FRQ	Total
✓	✓	✓	×	×	Guessing	5	6
					SSA	1	
✓	✓	×	−	×	IS	7	7
✓	×	✓	✓	✓	Guessing	2	9
					SSA	4	
					IS	3	
×	×	✓	✓	✓	Guessing	2	6
					SSA	1	
					IS	3	

were four incident types. In the first one, users successfully identified two correct pass-images and correct input format (code locations), but the codes were entered in the wrong order which ended up as incorrect attempt. In the second incident, the user recognized two correct pass-images but could not identify the correct input format (code locations); at the end the attempt was unsuccessful. In the third incident, the user managed to identify only one correct pass-image and correct input format (code location). The second chosen image was wrong but located on the same axis as the correct one, which resulted in a correct attempt. In the last incident, the user did not manage to identify any pass-images but managed to identify the correct input format (code location). Both pass-images were located on the same axes as the correct pass-images, which finalized the attempt as successful.

8. CONCLUSIONS

This paper has demonstrated a new secure scheme that resist guessing and observation attacks. The security evaluation provided deep insight on the resistance level of different types of attacks including guessing attack, intersection attack, and shoulder-surfing attack. The security of the GOTPass scheme has been evaluated theoretically and empirically. The security experiment involved three different attack simulations designed for the participants to carry out. One of the important evaluation factors to increase the result's accuracy was the large sample size of participants for such a security experiment. The experiments included 690 break-in attempts divided into three different attacks trials. The results were encouraging and showed only 3.3% of the conducted attempts were successful, a relatively low rate. The overall solution was therefore found to be both secure and usable. Thus, this system has considerable potential and will contribute in enhancing

current usable security. However, more conclusive analysis is required through conducting a field study in an actual environment with larger participant sample. Moreover, the impact of the image and code ordering on the security and usability is another aspect that needs investigation.

REFERENCES

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2009). *Graphical passwords: Learning from the first generation* (Technical report TR-09-09). Ottawa, Canada: School of Computer Science, Carleton University.

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys, 44*(4), 1–41. doi:10.1145/2333112

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). *The quest to replace passwords: A framework for comparative evaluation of web authentication schemes*. Paper presented at IEEE Symposium on Security and Privacy (SP), San Francisco, California, USA.

Chiasson, S., Forget, A., Biddle, R., & Van Oorschot, P. C. (2008). Influencing users towards better passwords: Persuasive cued click-points. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1* (pp. 121–130). Swinton, UK: British Computer Society.

De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies, 63*(1–2), 128–152. doi:10.1016/j.ijhcs.2005.04.020

Dhamija, R., & Perrig, A. (2000). *Déjà vu: A user study using images for authentication*. Paper presented at Proceedings of the 9th USENIX Security Symposium, Denver, Colorado, USA.

Dunphy, P., Heiner, A. P., & Asokan, N. (2010). *A closer look at recognition-based graphical passwords on mobile devices*. Paper presented at Proceedings of the Sixth Symposium on Usable Privacy and Security, New York, NY, USA.

English, R., & Poet, R. (2011a). Measuring the revised guessability of graphical passwords. In *5th International Conference on Network and System Security (NSS)* (pp. 364–368). Milan, Italy: IEEE.

English, R., & Poet, R. (2011b). Towards a metric for recognition-based graphical password security. In *5th International Conference on Network and System Security (NSS)* (pp. 239–243). Milan, Italy: IEEE.

English, R., & Poet, R. (2012). The effectiveness of intersection attack countermeasures for graphical passwords. In *11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 1–8). Liverpool, United Kingdom: IEEE.

Secure Graphical One Time Password (GOTPass)

219

Gao, H., Jia, W., Ye, F., & Ma, L. (2013). A survey on the use of graphical passwords in security. *Journal of Software*, *8*(7), 1678–1698. doi:10.4304/jsw.8.7.1678-1698

Gao, H., Liu, X., Wang, S., & Dai, R. (2009). *A new graphical password scheme against spyware by using CAPTCHA*. Paper presented at Symposium on Usable Privacy and Security (SOUPS), Mountain View, CA, USA.

Gołofit, K. (2007). Picture passwords superiority and picture passwords dictionary attacks. In *Proceedings of the International Multiconference on Computer Science and Information Technology* (pp. 681–669). Wisła, Poland: IEEE.

Khot, R. A., Kumaraguru, P., & Srinathan, K. (2012). *WYSWYE: Shoulder surfing defense for recognition based graphical passwords*. Paper presented at Proceedings of the 24th Australian Computer-Human Interaction Conference, Melbourne, VIC, Australia.

Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder surfing attack in graphical password authentication. *International Journal of Computer Science and Information Security (IJCSIS)*, *6*(2), 145–154.

Renaud, K., & De Angeli, A. (2009). Visual passwords: Cure-all or snake-oil? *Communications of the ACM*, *52*(12), 135–140. doi:10.1145/1610252

Rittenhouse, R. G., Chaudry, J. A., & Lee, M. (2013). Security in graphical authentication. *International Journal of Security & Its Applications*, *7*(3), 347–356.

Schaub, F., Walch, M., Königs, B., & Weber, M. (2013). *Exploring the design space of graphical passwords on smartphones*. Paper presented at Proceedings of the Ninth Symposium on Usable Privacy and Security, New York, NY, USA.

Snodgrass, J. G., & Asiaghi, A. (1977). The pictorial superiority effect in recognition memory. *Bulletin of the Psychonomic Society*, *10*(1), 1–4. doi:10.3758/BF03333530

Van Oorschot, P. C., & Wan, T. (2009). TwoStep: An authentication method combining text and graphical passwords. In G. Babin, P. Kropf, & M. Weiss (Eds.), *E-technologies: Innovation in an open world* (Vol. 26, pp. 233–239). Berlin Heidelberg, Germany: Springer.

Wang, L., Chang, X., Ren, Z., Gao, H., Liu, X., & Aickelin, U. (2010). *Against spyware using CAPTCHA in graphical password scheme*. Paper presented at 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), Perth, Australia.

Xiaoyuan, S., Ying, Z., & Owen, G. S. (2005). *Graphical passwords: A survey*. Paper presented at Computer Security Applications Conference, 21st Annual, Tucson, Arizona, USA.

BIOGRAPHIES

Hussain Alsaiari received a bachelor's degree in computer science from King Abdulaziz University, Saudi Arabia, in 2000. He was awarded his MSc with distinction in Internet, computer and system security from the University of Bradford, United Kingdom, in 2006. He is currently a PhD candidate in the Centre for Security, Communications and Network Research at Plymouth University, United Kingdom. His research interests reside in the area of authentication, usable security, and human aspects of security.

Dr. Maria Papadaki received her PhD in 2004 from University of Plymouth. Prior to joining academia in 2006, she worked as a security analyst for Symantec EMEA. Her research interests include incident response, insider threat, intrusion prevention and detection, security information and event management, security assessment, social engineering, security usability, and security education. Her research outputs include 19 journal and 30 international peer-reviewed conference papers. Dr. Papadaki holds GCIA, GPEN, and CEH certifications and is a member of the GIAC Advisory Board, as well as the BCS, IISP, and ISACA. Further details can be found at www.cscan.org/papadaki/

Dr. Paul Dowland is a member of the Centre for Security, Communications & Network Research and manages the teaching of computer security and networking within the School of Computing, Electronics and Mathematics at Plymouth University in the United Kingdom. His interests include network and system security, user authentication, and security education. Dr. Dowland is the secretary to the International Federation for Information Processing (IFIP) working group 11.1 (Information Security Management) and a Fellow of the BCS. He is the author of more than 50 papers in refereed international journals and conference proceedings, has edited 24 books, and is the co-author of *E-Mail Security: A Pocket Guide* (2010). Further details can be found at the CSCAN website (www.cscan.org/pdowland). He can also be followed on Twitter (@pdowland).

Prof. Steven Furnell is the head of the Centre for Security, Communications & Network Research at Plymouth University (UK), an adjunct professor with Edith Cowan University (Western Australia), and an honorary professor with Nelson Mandela Metropolitan University (South Africa). His interests include mobile device security, cyber crime, user authentication, and security usability. Prof. Furnell is the author of more than 260 papers in refereed international journals and conference proceedings, as well as books including *Cybercrime: Vandalizing the Information Society* (2001) and *Computer Insecurity: Risking the System* (2005). He is also the editor-in-chief of *Information & Computer Security* and co-chair of the Human Aspects of Information Security & Assurance (HAISA) symposium (www.haisa.org). He is active in a variety of professional bodies and is a fellow of the BCS, a senior member of the IEEE, and a board member of the IISP. Further details can be found at www.plymouth.ac.uk/cscan.

H. Alsaiari et al.

3) H. Alsaiari, M. Papadaki, P. S. Dowland, and S. M. Furnell, "A Review of Graphical Authentication Utilising a Keypad Input Method," in Proceedings of the Eighth Saudi Students Conference in the UK, ed: IMPERIAL COLLEGE PRESS, 2015, pp. 359-374.

A Review of Graphical Authentication utilising a Keypad Input Method

H. Alsaiari, M. Papadaki, P.S. Dowland
Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK
S.M. Furnell
Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK, and Security Research Institute, Edith Cowan University, Perth, Australia

Abstract

The traditional password has long been the most widely used authentication mechanism in spite of its well-known flaws. In order to address these flaws, researchers have utilised images or drawings as a potential alternative. In this paper, we consider the attributes of several graphic-based techniques. As a result, the study suggests a new data-entry classification within the field of graphical authentication. Several related graphical password schemes that share the characteristic of keypad typing entry are reviewed here. In addition, various illustrative summaries are provided in accordance with the related category, which also shows the fundamental design aspects associated with each category. This work aims to benefit researchers in the field of authentication security with an interest in alternative authentication methods.

Keywords: graphical password; alternative authentication; authentication security.

1. Introduction

User authentication plays a vital role in the field of information security since it is a means of identifying the user and verifying that the user is permitted to access a system such as a computer (Stamp, 2011). A key method for granting access to systems is knowledge-based authentication, which can be simply formulated as 'something users know'. The traditional text-based password is the foremost knowledge-based authentication method and the primary form of user

authentication to date (De Angeli *et al.*, 2005; Fu *et al.*, 2001). While many techniques are used to secure passwords (Pinkas and Sander, 2002), most are insufficient in the face of attackers' tools (Chakrabarti and Singbal, 2007; AuthenticationWorld.com, 2012). The text-based password system is widely used despite its well-recognised deficiencies, which affect both usability and security (Dhamija and Perrig, 2000; Xiaoyuan, Ying and Owen, 2005). The difficulty of remembering strong, complex passwords is one of the fundamental problems that users encounter, leading them to choose weaker passwords or to adopt insecure behaviours (Por *et al.*, 2008; Xiaoyuan, Ying and Owen, 2005; Dhamija and Perrig, 2000). Another major issue with textual password authentication is its susceptibility to credential theft (Balfanz *et al.*, 2012).

Due to the aforementioned shortcomings of the traditional textual authentication method, the need for alternatives has emerged. Various knowledge-based techniques have been proposed, such as graphical passwords (recognising graphical elements, e.g. images, iconography, grids) (Gyorffy, Tappenden and Miller, 2011; Kuber and Yu, 2010) or associative/cognitive questions (Zhao, Dong and Wang, 2006; Alexander, 2008). Each approach has its strengths and weaknesses. Graphic-based authentication is among the most promising alternative proposals and occupies an important position within user authentication research (Ray, 2012). Therefore, our research interest is entirely focused upon the use of graphical passwords to satisfy the security and usability requirements for authentication systems.

As a first step towards that direction, the aim of this paper is to review available literature and consider the security and usability requirements of existing systems. One interesting feature to be introduced in this paper is the use of the keyboard/keypad as an input mechanism instead of using the mouse, which is the method commonly used with graphical passwords.

2. Graphical Authentication Mechanisms

According to classic cognitive science experiments, humans possess a vast memory for pictures (Standing, Conezio and Haber, 1970). Thus, authentication methods that depend on graphics are less likely to encounter the memorability problems that text-based authentication methods do. Remembering complex passwords as well as multiple passwords for different systems is difficult (Furnell, 2005; Furnell and Zekri, 2006), while humans find recognising images, even after a period of time, far easier (Anderson, 2001).

2.1. Categorisation of graphical authentication

Researchers have mainly categorised graphical password authentication based on the cognitive tasks used to remember or retrieve the password. Monrose and Reiter (2005) divided graphical authentication into three main types: image recognition, tapping or drawing and image interpretation. Whereas Suo *et al.* (Suo, Zhu and Owen, 2005) classified it into two categories: recognition-based and recall-based approaches. As for Wiedenbeck *et al.* (2005), they expanded the aforementioned categories to include recognition, cued recall and pure recall. This latter type of grouping is the one this research has found most appropriate to adopt throughout the rest of the work. However, combining any of these categories is also a feasible option. Furthermore, for better clarification, one of the contributions of this study is the suggestion of adding some distinguishing details in a manner that involves several design aspects, as illustrated in Fig. 1. Firstly, the input approach, for instance, is what the user needs to submit as the login information for the authentication session. This input approach includes the following: draw, click, choice or typing. The second aspect is the display style, which means the presentation mode that forms the password challenge, such as grid, image and icon.

In this paper, attention is paid exclusively to those schemes that utilise graphics as an authentication means in addition to the use of keystrokes as an entry approach to submit the

necessary access data. According to the study conducted by Tari, Ozok and Holden (2006), replacing the regular use of a mouse for data entry in many graphical password schemes with a keypad is effective in terms of reducing the risk of a shoulder-surfing attack. In other words, this makes it more difficult to gain enough information about the password since both keystroke logger and screen scraping are required.
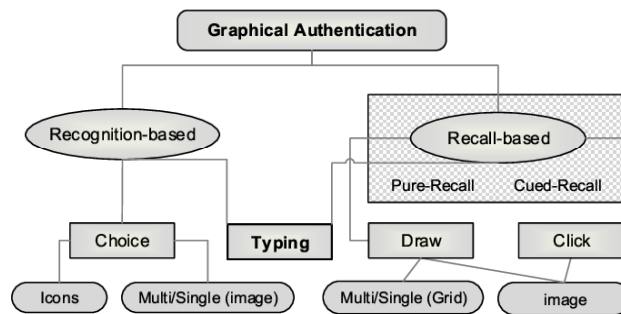

Figure 1. **Categorisation of graphic-based authentication**.

2.2. Recall-based schemes

The recall-based technique is a type of authentication where access is granted by reproducing a secret (e.g. drawing or clicking on image locations) that was previously created or chosen during the registration phase. The recall-based category can be further divided into pure recall and cued recall. Pure recall is difficult in practical terms due to its reliance on the user's ability to remember and access the information directly without cues, whereas cued recall helps users to remember their passwords by providing the necessary associated cues that trigger the memory (Malempati and Mogalla, 2011). As far as the password space is concerned, many recall-based schemes offer a large password space compared to that of textual passwords.

Stubblefield and Simon (2004) outlined a simple cued-recall scheme called 'inkblot authentication'. This scheme works as an aid for the user in creating and memorising strong textual passwords by generating and displaying a series of inkblots. During password registration, the user is asked to associate each of the ten displayed inkblots with a memorable word. The final password is derived from concatenating these words in a certain manner (e.g. the first and last

letters of each word). This scheme protects users from shoulder-surfing, since an attacker cannot obtain the password by only watching the inkblots without knowing the word associations. However, apart from the longer time required for authentication, this scheme received a positive user experience, especially the memorability aspect.

Figure 2. Inkblot authentication login screen (Stubblefield and Simon, 2004).

Gupta *et al.* (2011; 2012) implemented an authentication technique based on inkblots' mnemonics called 'passblot'. This scheme uses a set of inkblots unique to each user to generate pseudo-random, one-time passwords (OTP). Passblot makes use of only ten random inkblot-like images. During the first use of the system, users are required to assign a description to each inkblot. The final association with the inkblot is formed by the first and last letters of the description. In the authentication phase, four out of the ten inkblots are shown to the users, and they enter the corresponding associations. While most users appreciated the security enhancement provided by the system and felt that they understood its working process, many found difficulties in describing their inkblots and retaining their description.
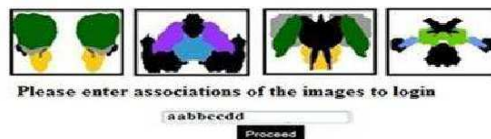

Figure 3. Login screen of passblot (Gupta *et al.*, 2012).

In 2005, Craymer and Howes invented a secure authentication methodology called 'GrIDsure', which was acquired in 2010 by CRYPTOCard Inc. (CRYPTOCard Inc, 2010; Safenet Inc, 2010) to be re-launched in a commercial form. The GrIDsure scheme generates a dynamic OTP. For registration, a five-by-five grid of cells containing random characters is presented to the user, who selects a favourite personal identification pattern (PIP), which is composed of four cells of any shape in any order. In each authentication attempt, the grid cells will be filled in with a random set of characters. Users are required to use a keyboard to input the corresponding characters occupying their PIP cells. In the user experiment conducted by Brostoff, Inglesant and Sasse (2010), the result showed that learning the GrIDsure system was easy and recalling patterns was acceptably reliable. However, the effective pattern space was small.
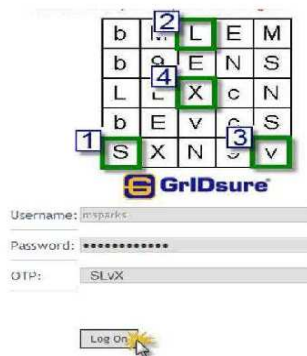

Figure 4. Authentication stage of GrIDsure (CRYPTOCard Inc, 2010).

Dimitropoulos (2011) proposed an enhanced version of GrIDsure using background images in an attempt to persuade users to choose more complicated patterns and hence stronger passwords. The same technique as the original GrIDsure was used, but with the help of a background image. According to the experiment result, using GrIDsure with background images has led more users to choose complicated passwords, while maintaining good memorability. Moreover, as the users got more familiar with the mechanism, the login time was reduced, in contrast to the longer time taken in registration.
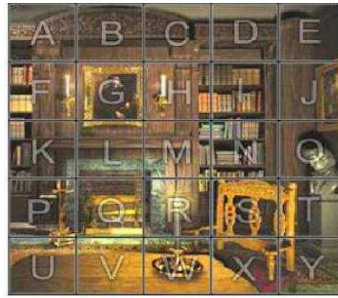
414

Figure 5. Enhanced-GrIDsure with a background image (Dimitropoulos, 2011).

Table 1 highlights and compares the major attributes of the recall-based schemes. It also reveals an important finding in that two of the main design aspects of this category (draw, click) are not implemented with the discussed feature that uses a keystroke to enter password information.

Table 1. Comparative summary of recall-based attributes.

	Graphical password system	Category		Approach			Style	
		Recall	Cued recall	Draw	Click	Typing entry	Grid	Image
1	Inkblot authentication		✓			✓		✓M
2	GrIDsure	✓		PATTERN		✓	✓	
3	Enhanced-GrIDsure with background		✓	PATTERN		✓	✓	✓
4	Passblot		✓			✓		✓M
							M = multi	

2.3. Recognition-based schemes

Image-recognition schemes have been proposed as a replacement for precise-password recall to minimise the burden on the users' cognitive memory, reduce the amount of user mistakes and improve the usability experience (Dhamija and Perrig, 2000). In most cases, there are two stages involved in such techniques. The first is the registration stage, where a set of images are presented to users from which they should form their password by selecting some of the images within the displayed set. The second is the authentication stage, which involves recognising and identifying

the pre-defined images, usually from among other decoy images. With regard to the password space, generally it is of a limited size and thus it is recommended that these schemes are accompanied by an online reference-validation mechanism to prevent any automated search (Monrose and Reiter, 2005).

Man, Hong and Matthews (2003) developed a scheme called 'where is Waldo' (WIW), which deals with shoulder-surfing attacks. The system displays a few well-ordered images, each of which contains many objects. Some of these are pre-chosen pass-objects that form part of the user's password. The appearance and location of these pass-objects spell a letter. The spelled letter is varied dynamically, since with each login attempt the location of the pass-objects is randomly changed.

Later, Hong et al. (2004) further enhanced the WIW technique by adding a flexibility feature as a way of assigning each pass-object a variant with the user's own codes. Simply, password creation is achieved by choosing four pass-icons from an icon library containing a total of 121 objects. Each icon consists of four variations. The user is required to assign a corresponding string to every variation. Login access is granted when the user successfully identifies the pre-chosen pass-icons from the grid and enters the pre-determined string corresponding to each pass-icon variation. The study reported that login using this system took a little bit longer time than a textual password system.

Figure 6. Hong authentication technique (Hong et al., 2004).

Komanduri and Hutchings (2008) implemented a picture-password system with the ability to produce a memorable, high-entropy password. Their system attempts to avoid the easy-to-guess-password problem by assigning users with a composed random password. The proposed system consists of 80 unrepeated pictures, each of which is labelled with a character. Each participant is assigned with a unique arrangement of eight items known as the 'home grid', which they need to recognise to fulfil the future authentication requirements. Pictures are always placed in a fixed location within the home grid with the same corresponding keyboard key. Based on a small sample size for the study, it showed that picture passwords were slightly more memorable than character passwords.
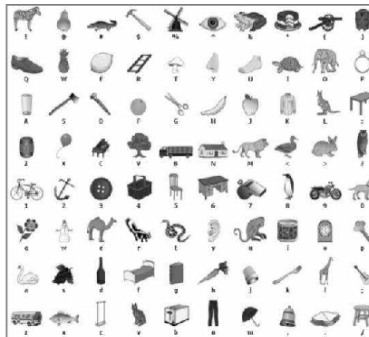

Figure 7. Picture password (Komanduri and Hutchings, 2008).

Gao *et al.* (2009) (see also Wang *et al.*, 2010) innovated a solution based on a challenge-response protocol to enhance security via protecting the graphical passwords against spyware attacks by utilising the CAPTCHA (completely automated public Turing tests to tell computers and humans apart) technique. The basic scheme assigns and embeds a CAPTCHA instance into each displayed image. To register, users need to choose and remember pass-images as their password. In order to authenticate, users are required to pass two tests. First is image recognition, where they need to look for their pass-images among other decoy images. This is followed by solving and typing the assigned CAPTCHA string that appears below each pass-image. The scheme takes a longer time to login compared to text-based schemes, whereas it takes a shorter time when compared to other graphical password schemes.

Figure 8. Gao's CAPTCHA scheme (Gao *et al.*, 2009).

Confident Technologies® (2011) has introduced a new approach that provides an image-based, OTP named 'Confident ImageShield™'. In this technique, the registration phase involves selecting a few easy-to-remember categories. Each authentication attempt displays a grid full of random images overlaid by alphanumeric characters. The user is then prompted to identify the images that match the pre-selected themes. Finally, the user needs to type in the alphanumeric characters associated with the password images. A feature of this scheme is the changeable location of the pictures and their characters. As a result, a unique OTP or PIN is submitted in each login attempt.
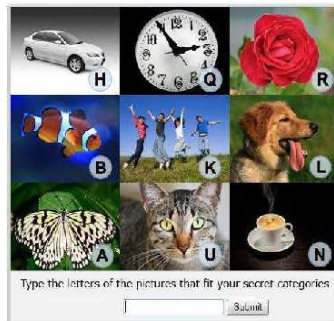

Figure 9. Confident ImageShield scheme.

Ku *et al.* (2012; 2013) proposed a solution to generate a graphical OTP (GOTP) for financial services using smartphones. The password creation is based on selecting an image portfolio that consists of four rounds that should form a story to act as a recall assistant. Each authentication

round displays images on a four-by-nine grid frame in the correct order. The respective alphanumeric OTP code is shown on the top-left corner of the screen, and the user needs to memorise this for the next round. The final, fifth round is the password-input step, which contains a random layout display of 12 buttons to allow entering the memorised four OTP texts matching the image portfolio. The result of the study showed that the average registration time was quite fast. Moreover, a considerably high result was gained from the user study which evaluated the password recall convenience, recall interference, authentication time and recall convenience of OTP text and security level.

Figure 10. Authentication process of GOTP scheme (Ku *et al.*, 2012, 2013).

Table 2 below shows the result of the conducted comparison. It can be inferred that graphical authentication schemes that depend on recognition mostly utilise multiple images or icons to allow users to identify and choose password images from among other decoy images. However, the recognition-based technique is fundamentally associated with a choice-based approach, in some cases with the additional support of the keypad-typing-entry approach. Plenty of recognition-based techniques have benefited from the keypad-typing-entry approach, which seems more viable with choice-based schemes than others.

Table 2. Comparative summary of recognition-based attributes.

| | Graphical password system | Category: recognition | | | | |
| | | Approach | | | Style | |
		Click	Choice	Typing entry	Image	Icon
1	WIW		✔	✔		✔ M
2	Hong scheme		✔	✔		✔ M
3	Komanduri and Hutchings picture password		✔	✔		✔ M
4	Gao CAPTCHA		✔	✔	✔ M	
5	Confident ImageShield		✔	✔	✔ M	
6	GOTP		✔	✔	✔ M	
						M = multi

3. Security Outlines

Various graphical password systems have been proposed to deal with different types of threats. For instance, many have tried to tackle shoulder-surfing attacks and some others have attempted to prevent the use of spyware and so on. A comparison has been conducted based on some major security features and vulnerabilities covered in the existing literature (Hafiz *et al.*, 2008; Rittenhouse, Chaudry and Lee, 2013). This aims to give some indication of the degree of security of the systems. The security features were compared on the basis of the following factors:

1. Shuffling images: dynamic image locations, always changeable.
2. System-assigned images: users cannot select their images; instead the system will assign images for them, which can help to avoid vulnerabilities such as choice of predictable images.
3. Multiple rounds: pass-images are distributed over multiple screens (one image in each page).
4. OTP: a password that is valid for a single use then expires.
5. Hash function: a type of cryptography that allows encrypting data in a way that it is difficult to invert.

Whereas the comparison of vulnerability features was based on the susceptibility to various types of attack such as:

420

1. Shoulder-surfing: the use of direct observation techniques to obtain victims' passwords, PINs or other security information.

2. Guessing: the ability to guess another user's password.

3. Dictionary attack: a dictionary of common words is used to identify the password of a legitimate user.

4. Spyware: a hidden software component that gathers information about users without their knowledge.

Table 3 summarises the results of the comparison of the graphical schemes that make use of the keystroke in an attempt to address those security issues and vulnerabilities. However, since this work is based on the available literature, it should be noted here that there is insufficient information about some schemes, which might prevent a fair comparison being made. The reason could be the different aims and objectives of the proposed schemes.

Table 3. Summary of security attributes comparison.

| | Graphical password system | Security features and vulnerabilities | | | | | | | | | Other features and limitations |
		Images/objects shuffling	System-assigned images	Multiple rounds	OTP	Hash function	Shoulder-surfing resistant	Difficult to guess	Dictionary attacks resistant	Safe against spyware	
1	Inkblot authentication	✓	-	-	-	-	✓	-	-	-	Uses a small set of static blots
2	GrIDsure	-	-	-	✓	x	x	-	-	x	Vulnerable to eavesdropping
3	Enhanced-GrIDsure with background	-	-	-	✓	-	-	-	✓	-	Safe against hotspots
4	Passblot	-	-	-	✓	-	✓	-	✓	✓	Resist social engineering
5	WIW	✓	-	-	-	-	✓	-	-	-	
6	Hong scheme	✓	-	✓	-	-	-	-	-	✓	Memorability difficulty
7	Komanduri and Hutchings picture password	x	✓	-	-	-	-	✓	-	-	
8	Gao CAPTCHA	-	x	x	-	-	-	✓	-	✓	CAPTCHA
9	Confident ImageShield	✓	x	x	✓	-	-	-	-	-	
10	GOTP	✓	x	✓	✓	-	✓	-	-	-	
	✓ Yes, x No, - Not mentioned										

As Table 3 depicts, different schemes with the typing-entry feature have various interesting strength points; however, some other security features had little attention. That in turn indicates that an enhanced technique is needed to consolidate as many features as possible to produce a robust, usable authentication system. Thus, we are currently conducting implementation and evaluation work towards a composite mechanism that involves an OTP combined with graphic-based authentication techniques.

4. Conclusion

There is a growing interest in replacing traditional text-based passwords with graphical techniques. In this paper, we have tried to describe in detail the categories of graphic-based authentication and suggest an enhanced way of classification as well as introduce typing as a new input approach. Interestingly, this work reviewed solely the schemes that make use of keypad typing as a means of password entry. From a security prospective, the diversity between the authentication challenge and the data-entry method can mitigate some common security attacks such as shoulder-surfing. The final part highlighted a comparative summary of the schemes of this category that involved some major security features and vulnerabilities, aiming to indicate the strengths and weaknesses of each scheme.

References

Alexander, C. (2008). Two Factor Authentication That Doesn't Use Chips, *Card Technology Today*, **20**, 9.

Anderson, R.J. (2001). *Security Engineering: a Guide to Building Dependable Distributed Systems*, 1st ed., John Wiley & Sons, New Jersey, USA, 51–71.

AuthenticationWorld.com. 2012. *Password Authentication*. [Online]. Available at: http://authenticationworld.com/Password-Authentication/index.html [Accessed 2 February 2015].

Balfanz, D., Chow, R., Eisen, O., Jakobsson, M., Kirsch, S., Matsumoto, S., Molina, J. and Van Oorschot, P. (2012). The Future of Authentication, *Security and Privacy, IEEE*, **10**, 22–27.

Brostoff, S., Inglesant, P. and Sasse, M.A. (2010). Evaluating the Usability and Security of a Graphical One-Time PIN System, *Proceedings of the 24th BCS Interaction Specialist Group Conference*, British Computer Society, Edinburgh Napier University, Edinburgh, Scotland, UK, 88–97.

Chakrabarti, S. and Singbal, M. (2007). Password-Based Authentication: Preventing Dictionary Attacks, *Computer*, **40**, 68–74.

Confident Technologies®. 2011. *When Passwords Aren't Enough*. [Online]. Available at: http://confidenttechnologies.com/content/when-passwords-arent-enough [Accessed 2 February 2015].

CRYPTOCard Inc. 2010. *GrIDsure Token Guide for BlackShield ID*. [Online]. Available at: http://www2.safenet-inc.com/cryptocard/implementation-guides/Tokens/GrIDsure%20Token%20Guide.pdf [Accessed 2 February 2015].

De Angeli, A., Coventry, L., Johnson, G. and Renaud, K. (2005). Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems, *International Journal of Human-Computer Studies*, **63**, 128–152.

Dhamija, R. and Perrig, A. (2000). *Déjà Vu: a User Study Using Images for Authentication*, Ninth USENIX Security Symposium, Denver, Colorado, USA, 45–58.

Dimitropoulos, L.K. (2011). *GrIDsure: Effects of Background Images on Pattern Choice, Usability and Memorability*, University College London, London, UK.

Fu, K., Sit, E., Smith, K. and Feamster, N. (2001). Dos and Don'ts of Client Authentication on The Web, *Proceedings of the 10th Conference on USENIX Security Symposium*, USENIX Association, Washington, DC, USA.

Furnell, S. (2005). Authenticating Ourselves: Will We Ever Escape the Password?, *Network Security*, 2005, 8–13.

Furnell, S. and Zekri, L. (2006). Replacing Passwords: in Search of the Secret Remedy, *Network Security*, 2006, 4–8.

Gao, H., Liu, X., Wang, S. and Dai, R. (2009). A New Graphical Password Scheme against Spyware by Using CAPTCHA, *Proceedings of the Fifth Symposium On Usable Privacy and Security*, SOUPS, Mountain View, California, USA, 15–17.

Gupta, S., Sabbu, P., Varma, S. and Gangashetty, S.V. (2011). 'Passblot: a Usable Way of Authentication Scheme to Generate One Time Passwords', in Wyld, D.C., Wozniak, M., Chaki, N., Meghanathan, N. and Nagamalai, D. (eds), *Advances in Network Security and Applications*, Springer, Berlin and Heidelberg, Germany, pp. 374–382.

Gupta, S., Sahni, S., Sabbu, P., Varma, S. and Gangashetty, S.V. (2012). Passblot: a Highly Scalable Graphical One-Time Password System, *International Journal of Network Security and its Applications*, **4**.

Gyorffy, J.C., Tappenden, A.F. and Miller, J. (2011). Token-Based Graphical Password Authentication, *International Journal of Information Security*, **10**, 1–16.

Hafiz, M.D., Abdullah, A.H., Ithnin, N. and Mammi, H.K. (2008). *Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique*, Second Asia International Conference on Modeling and Simulation, IEEE, Kuala Lumpur, Malaysia, 13–15 May 2008, 396–403.

Hong, D., Man, S., Hawes, B. and Mathews, M. (2004). A Graphical Password Scheme Strongly Resistant to Spyware, *Proceedings of the International Conference on Security and Management*, Las Vegas, Nevada, USA.

Komanduri, S. and Hutchings, D.R. (2008). *Order and Entropy in Picture Passwords*, Graphics Interface Conference, Canadian Information Processing Society, Ontario, Canada, 115–122.

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H. and Kim, J-H. (2012). Extended OTP Mechanism Based on Graphical Password Method, *Future Information Technology, Application, and Service*, **1**, 203–212.

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H. and Kim, J-H. (2013). Two-Factor Authentication System Based on Extended OTP Mechanism, *International Journal of Computer Mathematics*, **90**, 1–15.

Kuber, R. and Yu, W. (2010). Feasibility Study of Tactile-Based Authentication, *International Journal of Human-Computer Studies*, **68**, 158–181.

Malempati, S. and Mogalla, S. (2011). *A Well-Known Tool Based Graphical Authentication Technique*, First International Conference on Computer Science, Engineering and Applications, Chennai, India, 97–104.

Man, S., Hong, D. and Matthews, M. (2003). A Shoulder-Surfing Resistant Graphical Password Scheme-WIW, *Proceedings of the International Conference on Security and Management*, Las Vegas, Nevada, USA, 105–111.

Monrose, F. and Reiter, M. (2005). Graphical Passwords, *Security and Usability*, 147–164.

Pinkas, B. and Sander, T. (2002). Securing Passwords against Dictionary Attacks, *Proceedings of the Ninth ACM Conference on Computer and Communications Security*, ACM, Washington, DC, USA, 161–170.

Por, L., Lim, X., Li, Q., Chen, S. and Xu, A. (2008). *Issues, Threats and Future Trend for GSP*, Seventh WSEAS International Conference on Applied Computer and Applied Computational Science, World Scientific and Engineering Academy and Society, China.

Ray, P.P. (2012). Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices, *Journal of Information Engineering and Applications*, **2**, 1–11.

Rittenhouse, R.G., Chaudry, J.A. and Lee, M. (2013). Security in Graphical Authentication, *International Journal of Security and its Applications*, **7**.

Safenet Inc. 2010. *Cryptocard Acquires GrIDsure Tokenless Authentication IP*. [Online]. Available at: http://www.safenet-inc.com/news/2012/cryptocard-acquires-gridsure-tokenless-authentication-ip/ [Accessed 2 February 2015].

Stamp, M. (2011). *Information Security: Principles and Practice*, 2d ed., Wiley-Blackwell, New Jersey, USA, 229–254.

Standing, L., Conezio, J. and Haber, R.N. (1970). Perception and Memory for Pictures: Single-Trial Learning of 2,500 Visual Stimuli, *Psychonomic Science*, **19**, 73–74.

Stubblefield, A. and Simon, D. (2004). *Inkblot Authentication: Technical Report MSR-TR-2004-85*, Microsoft Research, Redmond, Washington, USA, 1–16.

Suo, X., Zhu, Y., and Owen, G.S. (2005). Graphical Passwords: a Survey, 21st Annual Computer Security Applications Conference, Tuscon, Arizona, USA, 5–9 December 2005.

Tari, F., Ozok, A. and Holden, S.H. (2006). A Comparison of Perceived and Real Shoulder-Surfing Risks between Alphanumeric and Graphical Passwords, *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS, Pittsburgh, Pennsylvania, USA, 56–66.

Wang, L., Chang, X., Ren, Z., Gao, H., Liu, X. and Aickelin, U. (2010). *Against Spyware using CAPTCHA in Graphical Password Scheme*, 24th IEEE International Conference on Advanced Information Networking and Applications, IEEE, Perth, Australia, 760–767.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005). PassPoints: Design and Longitudinal Evaluation of a Graphical Password System, *International Journal of Human-Computer Studies*, **63**, 102–127.

Zhao, Z., Dong, Z. and Wang, Y. (2006). Security Analysis of a Password-Based Authentication Protocol Proposed to IEEE 1363, *Theoretical Computer Science*, **352**, 280–287.

4) H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell, "Graphical One-Time Password (GOTPass): A Usability Evaluation," Information Security Journal: A Global Perspective, pp. 1-15, 2016/05/18, 2016.

Graphical One-Time Password (GOTPass): A usability evaluation

Hussain Alsaiari, Maria Papadaki, Paul Dowland & Steven Furnell

Taylor & Francis
Taylor & Francis Group

Graphical One-Time Password (GOTPass): A usability evaluation

Hussain Alsaiari, Maria Papadaki, Paul Dowland, and Steven Furnell

Centre for Security Communication and Network Research, School of Computing Electronics and Mathematics, Plymouth University, Plymouth, United Kingdom

ABSTRACT

Complying with a security policy often requires users to create long and complex passwords to protect their accounts. However, remembering such passwords is difficult for many and may lead to insecure practices, such as choosing weak passwords or writing them down. In addition, they are vulnerable to various types of attacks, such as shoulder surfing, replay, and keylogger attacks (Gupta, Sahni, Sabbu, Varma, & Gangashetty, 2012) One-Time Passwords (OTPs) aim to overcome such problems (Gupta et al., 2012); however, most implemented OTP techniques require special hardware, which not only adds cost, but there are also issues regarding its availability (Brostoff, Inglesant, & Sasse, 2010). In contrast, the use of graphical passwords is an alternative authentication mechanism designed to aid memorability and ease of use, often forming part of a multifactor authentication process. This article is complementary to the earlier work that introduced and evaluated the security of the new hybrid user-authentication approach: Graphical One-Time Password (GOTPass) (Alsaiari et al., 2015). The scheme aims to combine the usability of recognition-based and draw-based graphical passwords with the security of OTP. The article presents the results of an empirical user study that investigates the usability features of the proposed approach, as well as pretest and posttest questionnaires. The experiment was conducted during three separate sessions, which took place over five weeks, to measure the efficiency, effectiveness, memorability, and user satisfaction of the new scheme. The results showed that users were able to easily create and enter their credentials as well as remember them over time. Participants carried out a total of 1,302 login attempts with a 93% success rate and an average login time of 24.5 s.

1. Introduction

In general, the task of recognizing a displayed item has been demonstrated to be easier for people than relying on their memory to recall the same information without any assistance (Nielsen, 1994). Furthermore, a classic cognitive science experiment showed that humans have a strong memory ability for images (Standing, Conezio, & Haber, 1970). Thus, recognition-based techniques are an interesting branch of graphical passwords, which involve identifying a set of user-selected images among other, decoy images. This technique has been proposed as a usable alternative to textual passwords, since it includes many useful features, such as ease of memorization, simple use, as well as providing a reasonable security level (Khot, Kumaraguru, & Srinathan, 2012). With respect to security, the password space is an important factor for a robust authentication scheme. Generally, most recognition-based schemes suffer from a small password space, whereas many recall-based schemes can offer a much larger password space. Therefore, the proposed scheme employs both techniques to gain the best of each. An Android unlock pattern (a recall-based [draw-based] technique) is implemented as a point-of-entry defence for the main recognition-based (choice-based) technique.

One of the authentication mechanisms to withstand many of the traditional textual password security issues is the One-Time Password (OTP). The nature of this technique makes it appropriate to secure various financial services and online payments, since OTP generates a password that is valid for a single use and then expires. Thus, this article proposes an authentication scheme that makes use of a graphical password to generate an

CONTACT Hussain Alsaiari ✉ info@cscan.org 🖳 Centre for Security Communication and Network Research, School of Computing Electronics and Mathematics, Plymouth University, Drake Circus, Plymouth, PL4 8AA, United Kingdom.

OTP. It is envisaged that the proposed mechanism could form a lower-cost and more readily available alternative to token reader devices that are often used in online banking.

The rest of this article is organized as follows: The next section briefly introduces relevant existing schemes. Then, the GOTPass approach is described. The following section provides a detailed usability evaluation, as well as an overview of the security evaluation. After that, we discuss the outcomes of the scheme's evaluation, followed by our conclusions.

2. Related work

Komanduri and Hutchings (2008) implemented a picture password system with the ability to produce a memorable, high-entropy password. The proposed system consists of 80 unrepeated pictures, and each one is labeled with a character. Each participant is assigned a unique arrangement of eight items known as the "home grid," which must be recognized to fulfill future authentication requirements. Pictures are always placed in a fixed location within the home grid, with the same corresponding keyboard key. In this system, a dual input ability is enabled by using either the keyboard or an on-screen mouse cursor. Furthermore, another initiative was launched to accept an unordered input, thus allowing the selection of the correct images in any order. According to the study, a successful authentication system could benefit from this unordered recall.

Gao, Liu, Wang, and Dai (2009) and Wang et al. (2010) innovated a solution based on a challenge–response protocol to protect graphical passwords against spyware attacks by utilizing a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA). The new authentication scheme is a combination of graphical password and a textual CAPTCHA that is assigned and embedded into each displayed image. To register, users need to choose and remember a number of pass-images as their password. In order to authenticate, users are required to pass two steps. First is the image recognition step, where they need to look for their pass-images among other, decoy images. The second step involves solving and typing in the assigned CAPTCHA string that appears below each pass-image in a certain way. The improved technique of this scheme uses a predefined random length as an alternative to the usual uniform length. As such, the user predetermines the position and the number of characters. Consequently, users need to select and memorize the letter positions (pass-positions) of each pass-image (e.g., the letters in the first, third, and seventh positions).

De Angeli et al. (2002) and De Angeli, Coventry, Johnson, and Coutts (2003) presented an innovative concept for user authentication called Visual Identification Protocol (VIP), which is based on the idea of replacing conventional PIN numbers with pictures. An authentication attempt is successful when users correctly select the images that are part of their portfolio among other decoys within the display panel. There are three variations of the VIP scheme, one of which is the advanced scheme (VIP3), which assigns a portfolio of eight pictures to each user. At every login attempt, a 4×4 challenge set is presented to the user, containing four random portfolio pictures together with an additional 12 distractors. To authenticate, users have to identify their preset images among the 16 images shown on the interface in any sequence.

(Van Oorschot & Wan, 2009) came up with a new scheme called TwoStep. The new scheme is a hybrid user-authentication scheme that utilizes traditional text passwords and recognition-based graphical passwords. In the first step, users provide a text-based password as usual, but the second step involves entering a graphical password. Users need to register a number of images as their graphical password components, which are set over a particular number of rounds. Once this has been done, an index number is assigned to each image. The login screen will display, at random, the images along with their index numbers. A selection panel is located at the lower part of the screen, which contains all of the index numbers in ascending order. To authenticate, the user needs to identify the image and select the corresponding index number from the selection panel. TwoStep has the advantage of the user being able to enter the graphical password part by clicking a mouse, which reduces the possibility of keylogging attacks.

427

In Where You See is What You Enter (WYSWYE) (a scheme proposed by (Khot et al., 2012)), two variations of the proposed approach were implemented: Horizontal Reduce (HR) and Dual Reduce (DR). Although they are different in terms of the challenge grid size and the process of identifying and mapping the image pattern, the underlying strategy is the same.

In the registration stage of the DR scheme, users are presented with a set of 28 images and required to create a password containing four images. During the login time, the scheme generates two side-by-side grids; the challenge grid contains random images, four of which correspond to the password. The user is expected to interact only with the second grid, the response grid, which is smaller in size; it is initially empty and is used for input entry purposes. To map between the different size grids, the user must reduce the bigger challenge grid to the size of the response grid. This is done by a mental elimination of the rows and columns that do not contain any of the password images from the challenge grid. Login is achieved by locating the password image positions inside the reduced challenge grid and by subsequently using the response grid to map them accurately.

Ku et al. (2012) and Ku et al. (2013) proposed a solution to generate a graphical one-time password (GOTP) for financial services using smartphones. The password creation is based on selecting an image portfolio that consists of four rounds that form a story—to act as a recall assistant. Each authentication round displays images on a 4×9 grid frame in the correct order. The respective alphanumeric OTP code is shown at the top-left corner of the screen, and the user needs to memorize this for the next round. The final (fifth) round is the password input step, which contains a random layout display of 12 buttons to allow the user to enter the memorizsed four OTP texts that match the image portfolio. The study showed that the average registration time was quite fast, with positive results that evaluated the recall interference, authentication time, and recall convenience.

However, the GOTP approach still requires the user to memorize an alphanumeric code obtained by identifying the pass-images over several rounds and then entering the code in the final round. That, in turn, may require memory recall from

the user, resulting in usability issues. In addition, GOTP is designed for smartphone platforms that can be used as an out-of-band channel for authentication, which is carried out away from the browser. In other words, there is a need for an additional device (smartphone) to be present in order to use the GOTP scheme; however, this is not always an issue for many users nowadays. Furthermore, the length of the OTP code generated by GOTP is short compared to other similar schemes, which provide twice as long OTP codes (e.g., Picture Password and Gao's CAPTCHA). Therefore, the demand for an enhanced authentication mechanism that utilizes the advantages of such schemes (e.g., one-time password and the use of separate means for data entry) and overcomes their limitations (e.g., the need for extra devices, burdening memory with codes to remember, short codes, and static pass-images) has emerged.

3. The GOTPass scheme

Having considered the contributions of the prior works, this section proposes the basis of an alternative approach that seeks to address the perceived shortcomings. As described by (Alsaiari, Papadaki, Dowland, & Furnell, 2015), the proposed scheme is a hybrid multilevel authentication mechanism called Graphical One-Time Password (GOTPass). The overall objectives of the proposed scheme are presented next, followed by details of the operational approach.

3.1. Objectives

The objective of this scheme is to enhance the usability features of the existing graphical authentication system by developing a new multigraphical password technique that fulfills most of the usability requirements. The main usability characteristics that the GOTPass authentication system aims to satisfy can be highlighted as follows.

The first requirement is the ability to create a new password using a simple process and a minimal number of steps. Second, the password should be easy to remember, so users are not overwhelmed by a raft of complex secrets that they have to memorize. Third, it should be a simple-to-use scheme that is reliable (an unreliable system

may result in denial of access). Fourth, it should be efficient to use, and the registration and login time should be acceptably short. Fifth, there should be nothing to carry, which means that a user should not rely on auxiliary devices (e.g., tokens) to perform the authentication task, excluding devices that users usually carry around at all times, such as mobile phones. Finally, it should be easy to recover, allowing users to regain the ability to login in case the authentication credentials are forgotten.

The key technical advantages of the proposed scheme are considered to be

- Combination of multiple authentication mechanisms (graphical password and OTP)
- Combination of multiple graphical password categories (recall-based [draw] and recognition-based [choice])
- System-assigned themes with user-chosen images
- Various GOTPass input formats (code locations)

One of the significant features of an image-based authentication technique is the ease of recall, which is something that a conventional text-based password lacks. Thus, this has motivated us to investigate and develop an enhanced graphical authentication mechanism. However, most recognition-based graphical password schemes are vulnerable to observation attacks (e.g., shoulder surfing), due to their very nature of being visible to surrounding people. Therefore, we employed a user-friendly graphical technique (unlock pattern) that acts as a front-line defender before the recognition-based technique. This is in line with the results of an earlier field study carried out over 21 days, which confirmed that users were in favor of the pattern mechanism despite the repeated errors they made (Von Zezschwitz, Dunphy, & De Luca, 2013). According to (Chiang & Chiasson, 2013), the Android screen unlock technique is the most well-known deployed graphical password. Finally, the system's security is strengthened by the implementation of the OTP technique. Table 1 summarizes the rationale behind the selection of these various authentication techniques.

3.2. Approach

GOTPass scheme combines graphical and one-time passwords. In addition, various graphical password methods have been merged to form a new mix of recall- and recognition-based techniques. The final component of GOTPass involves the determination of input formats, or, in other words, the location of the associated codes. More precisely, the method will be established by solving the lock pattern (draw-based), followed by identifying pass-images (image recognition), and the last step will be to enter the corresponding OTP code according to the prechosen format (knowledge-based).

The process flow for the enrollment and authentication phases is summarized in Table 2, which defines the requirements and procedures for each phase as well as showing the authentication classifications of each part.

3.3. Enrollment

The registration stage involves three main phases. First, the user needs to choose a unique username and draw any shape on a 4×4 unlock pattern. Second, the system will automatically assign four random themes for each user, one after another. The user needs to select one pass-image from each of the given themes (four altogether). Finally, the position of the pass-images in the grid will be used to indicate a code that needs to be entered using the keypad/keyboard, which is referred to as the GOTPass input format. These codes are located on the top or left-hand axis of each pass-image. There are two security-level options for the user to choose from: basic or advanced. At the basic security level, the numeric codes for both pass-images are taken from the same axis, whereas the numeric codes at the advanced level are taken from a different axis for each pass-image. The system-assigned input format is clearly presented to the user with an illustrative example (e.g., top axis for the first pass-image + left-hand axis for the second pass-image).
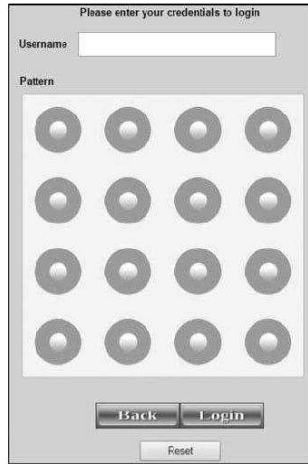
Figure 1. GOTPass unlock pattern step.

3.4. Authentication

The system will prompt the registered user for his or her username and display an on-screen pattern lock (Figure 1), which requires the user to redraw the predefined unlock pattern shape by connecting nodes to re-form the correct pattern shape.

If the preceding step is correct, the system will display a fresh (4×4) image panel, as illustrated in Figure 2, containing two random pass-images out of the four previously chosen pass-images, six distractor images that are associated with the pass-images (three for each), and another eight random decoy images. The system generates new OTP codes and fills the panel edges (axis) of each row and column (only the locations that are occupied by the correct pass-images will contain the correct GOTPass codes). To complete the authentication process, the user must first identify the password images among others in the panel (this is done mentally; there is no need to touch/click on the images). From the grid axis, the user needs to locate and enter the codes associated with each pass-image (these should be entered in the correct format, as previously assigned and shown in the registration phase). It is necessary to select the pass-images and, thereafter, the associated codes in the correct order depending on which pass-image appears first. Once the system ensures that all of the information that has been provided is

Figure 2. GOTPass image recognition and OTP code entry – Assuming security-level option 3 is in use (top axis for the first pass-image + left axis for the second pass-image).

430

correct, then the user is successfully authenticated and granted access.

4. Evaluation

The study conducted by (Biddle, Chiasson, & Van Oorschot, 2011) stated that the consistency of the published research within the domain of graphical authentication is almost absent, which complicates the task of reproducing results or comparing schemes. Many graphical password system proposals have an inadequate evaluation of either security or usability, or even both. The lack of an accepted usability standard in this area of research is a result of the missing coordination work between researchers, which led to the use of different evaluation criteria for nearly every system proposal. Furthermore, (Bonneau, Herley, Van Oorschot, & Stajano, 2012) realized that the original publications on such schemes included optimistic and incomplete ratings. Therefore, standard evaluation methods and measurements are required to carry out a reasonable comparison against other works.

A proper framework is required to evaluate the design of a successful authentication mechanism against several aspects of security and usability (De Angeli, Coventry, Johnson, & Renaud, 2005). Hence, a collection of evaluation criteria and guidelines has been carefully identified by exploring the characteristics and methods of the existing graphical authentication schemes alongside the review of the available evaluation studies. However, it should be noted that fulfilling all the requirements of security and usability in a single authentication scheme is unlikely to be achievable (Schaub, Walch, Könings, & Weber, 2013).

To prepare an appropriate evaluation plan, a review of studies carried out by similar graphical password techniques was conducted. As Table 3

Table 1. Rationale behind the selection of various authentication techniques.

	Authentication technique	Rationale of selection
1	Pattern unlock	Protect the main image-based scheme User-friendly and familiar
2	Image recognition	Easy to remember Easy to use
3	OTP input format	Provide robust security

illustrates, almost all schemes carried out in-lab studies. Most schemes were performed over several sessions with various time intervals. The maximum number of sessions used was three and the minimum number was one. With regard to the number of trials, two schemes allowed 10 authentication attempts. The number of participants ranged between 10 and 61. Essential evaluation elements, such as effectiveness, efficiency, memorability, and user satisfaction, were the components of most of the conducted studies. In addition, at the end of the table, a summary of the GOTPass scheme study is included to enable an easy basis for comparison.

4.1. GOTPass usability

A successful authentication system should maintain a balance between usability and security. System usability is an essential design aspect that should not be compromised for security (and vice versa). The GOTPass proposal contains some interesting usability design features (Table 4), such as the use of image themes that prompt users to remember password images. Although the system prohibits users from using their own images, to protect against a guessing attack by a familiar person and help reduce the impact of users' tendency to choose predictable images, they are allowed to choose preferred images from a specified theme, which adds flexibility to the system as well as freedom of choice for the user. One of the GOTPass goals is to have a reasonable level of memorability so users manage to remember their pass-images easily. However, there is no use of mnemonics to assist users in remembering their passwords, since the proposed scheme uses multiple authentication mechanisms that make applying such a feature on each mechanism both difficult and pointless.

4.1.1. Experiment design and implementation

The GOTPass prototype was developed as a web-based application using Microsoft Visual Studio 2013—C# and SQL Server 2012 as the Database Management System. The prototype application was hosted on a laptop with a 15.6-in. screen display set at a resolution of 1366×768 pixels and running Windows 8.1.

Table 2. Process flow for the enrollment and authentication phases.

General process flow	Registration phase	Authentication phase
Secret knowledge (username)	Select a unique username	Enter the correct username
Pattern unlock Graphical password (recall-based, draw-based)	- 4×4 pattern grid will be displayed - The user needs to draw a pattern in any preferred shape	Unlock the pattern grid by redrawing the prechosen pattern
Image recognition	- The system will assign four random themes for the user	The system displays a 4×4 panel of images containing two random pass-images out of the four previously chosen pass-images, plus 14 other decoy images
Graphical password (recognition-based, choice-based)	- A panel of images from each of the assigned themes will be presented and the user will make his or her own selection	The user needs to identify the two pass-images
One-Time Password Formation of the final password entry	- Since the edge side of each row and column of the panel will be assigned four random digits, the user can choose from two available security-level options: basic or advanced. Each level has two different GOTPass input format combinations, and the system will randomly assign one to the user	Enter the associated GOTPass code with each image in the same previously chosen format and in the correct order

A user study was conducted that involved three separate trial sessions on the first day of the study, one week later, and after one month. A within-subjects design method was used in which the same users participated in all experimental tasks—that is, repeated measures were taken from the same people. Participants performed two main assignments: first, to enroll and authenticate several times over specific time intervals; and second, to act as observers to try and capture the experimenter's login password using various attacking techniques. This study was a longitudinal testing method, since several observations of the same subjects were conducted over a period of time.

Experiments to evaluate the usability and security of the GOTPass approach were conducted in a controlled laboratory environment, as all users were required to be physically present and use the same computer to perform the study tasks. For study purposes, the implemented scheme generated some significant activity logs in such a way that it stored timestamps, login status (successful, failed), as well as details of the duration of each session. In addition, results of the responses to the pretest and posttest questionnaires were also collected. Only the research investigator and the participant were allowed in the lab, to avoid any possible disruption and observe any usability or security issues, as well as record the participant's comments. Nevertheless, attention was paid to the session duration, in which we tried to remain focused on the experiment and discouraged any side conversations during the trials, unless participants chose to talk.

Given the longitudinal nature of the study, and the necessity for those involved to remain available for each stage of the work, the participants were sourced from the local staff/student community at the authors' university, and recruited via several methods, including word of mouth, student portals, emails, and posters. Participation did not require any specific level of computing ability. Participants received reasonable compensation for their participation, payable upon the completion of the study at the end of the third session. As for the session duration, the allocated time for each session never exceeded 30 min.

The experiment was conducted over five weeks and involved 81 participants (63 male, 18 female) who attended all three separate sessions. Most participants were university staff and students, with a mix of educational levels ranging from undergraduate and postgraduate. Most participants were aged between 18 and 39 years. Fifty percent of participants reported an intermediate level of computer experience, yet 17% indicated a basic level. Almost all participants indicated that they knew about at least one type of graphical technique. Draw-based graphical passwords were most familiar to the users, followed by recognition-based passwords, whereas only a few respondents had prior knowledge of the click-based technique.

4.1.2. User study procedure

Following is the series of tasks the users were required to perform at each session.

4.1.2.1. Initialization session—day one. The first session started with a brief introductory overview of the procedure, participants' rights, as well as an explanation about the system functionalities and the process of enrollment and authentication. An instruction manual "guide booklet" and video demo that described the registration and login sequential steps were made available as training materials.

After gaining the required understanding of the system and how it works, participants started the registration phase, where they created a new account.

Once the users were registered, they filled out a short online pretest questionnaire on demographic and authentication experience. This acted as a separator role between phases to distract the user's attention away from the registration process, to aid a better evaluation of memorability during the next phase. This is similar to the Mental Rotation Tasks (MRTs) procedure, which aims to clear the participants' working memory.

The final task of the first session was the login phase, where participants were required to login (maximum 10 total attempts) under the following conditions:

- Total of five correct authentication attempts > successfully completed this session.
- Total of five incorrect attempts > receive the guide booklet or play the video demo, then try again.

Participants were instructed to avoid clicking on the pass-images; instead, they were encouraged to mentally locate the images and map them to the right axis of the OTP code.

4.1.2.2. Follow-up session (short-term memorability experiment)—one week later. After a week of nonuse, participants returned to the lab, where they were asked to repeat the login task.

4.1.2.3. Final session (long-term memorability experiment)—one month later. The third and final session took place one month after the first session. The first task was again to login using the created account, with the same rules and conditions as the first and second trials.

Table 3. Summary of the graphical password technique studies.

Scheme	Type of study	Sessions	Trials	Participants	Evaluation elements
Komanduri Picture Passwords (Komanduri et al., 2008)	In-lab and any location	- Day 1 in-lab - Day 2 any location - Day 9 in-lab	Eight complete correct inputs	- 23 participants - Only 15 participants received picture-based passwords	Effectiveness, efficiency, and memorability
TwoStep (van Oorschot & Wan, 2009)	No user study	Future work: lab/field studies	—	—	—
WYSWYE Dual-Reduce (DR) (Khot et al., 2012)	Controlled lab	One login session	Three login attempts	- 24 participants. - None of them knew about GP	Accuracy, efficiency, learnability, and user satisfaction
VIP (De Angeli et al., 2002)	Controlled lab	Two login sessions: first day and after one week	10 authentication attempts—with three incorrect attempts	61 participants	Effectiveness, efficiency, and user satisfaction
GOTP (Ku et al., 2012)	In-lab	—	—	10–20 participants with prior knowledge of use	Password creation time, login time, recall convenience and recall disturbance
Gao CAPTCHA (Wang et al., 2010)	In-lab	Three login sessions: day one, one week later, and one month later	- Test 1 (day 1): 10 times, - Test 2 (one week) - Test 3 (one month): three times	36 participants unfamiliar with the scheme	Login success percent, login time, and memorability
GOTPass	In-lab	Three login sessions: day one, one week later, and one month later	Allowed: maximum10 login attempts for each session Required: only 5 correct logins	81 participants	Effectiveness, efficiency, user satisfaction, and memorability

433

Finally, participants received an online posttest questionnaire to assess their impression of the GOTPass system, as well as find out their opinion on it.

4.1.3. Usability study results

As defined by ISO 9241-11 (International Organization for Standardization, 1998), effectiveness, efficiency, and satisfaction are the main components of usability in a particular context. However, there are no absolute measures of usability (Bangor et al., 2008). Nevertheless, major usability features from ISO and previous studies were extracted to build a usability evaluation criteria for the new graphical password system. This article reports the quantitative results for all usability components except user satisfaction, which reports qualitative results from the surveys regarding the user perceptions.

4.1.3.1. Efficiency. Table 5 describes the details of the measurements used to calculate the efficiency of the proposed scheme. As anticipated, creating a GOTPass account took a relatively long time, since registering for GOTPass includes typing a username, drawing a pattern, clicking the "Register Pattern" button, initial thinking time (image viewing), selecting four pass-images, choosing the security level, and, finally, clicking the "Submit" button. As shown in Table 6, the average registration time was 134 s. It is worth mentioning that participants were totally new to the system and, while they created their accounts, spent quite a lot of time talking and asking questions about the prototype, trying to start discussions about several aspects, such as the potential advantages and disadvantages of the system and the way it was implemented. Although the registration time was relatively high, it was considered generally acceptable for most participants, as indicated in the posttest questionnaire result, where 80% of the users stated that they managed to complete the

required tasks quickly. In contrast, only one participant disagreed with this statement.

In the analysis of the time it took to enter the correct submission, the average was 24.5 s, as presented in Table 7. The long input time was also expected in the login phase, since the login task involves a number of keystroke and mouse activities. In addition, the time taken to mentally locate the correct pass-images and their associated codes is also considered to be a significant factor that increased the login time. There was a slight variation in the average login time between trials: 23.6, 25.5, and 24.3 s, respectively.

4.1.3.2. Effectiveness. The details of the measurements used to calculate the effectiveness of the proposed scheme can be seen in Table 8. The study looked at the proportion of all successful login attempts across all trials to calculate the success rate of the proposed system. In total, data from 1,302 login attempts carried out by all participants were analyzed. Table 9 provides details of the success and failure rates for the authentication phase over the three trial sessions. The results show a relatively high success rate, as over 93% of the attempts were successful. Although the first trial was preceded by MRTs, to distract the users after the registration task and free up their working memory, this did not have any clear impact on the success rate of the first trial in particular. In the final session (Trial 3), there seemed to be some associations of the GOTPass in the participants' memory, as the number of incorrect inputs was lower than in Trial 2.

Interestingly, the study showed that none of the users was completely unable to login within the given number of attempts. Approximately 40% of the participants managed to complete their login tasks without error. Moreover, since many systems limit the number of consecutive incorrect attempts a user is allowed to make, we introduced this measure to determine the highest number of repeated failed attempts. The results show that only one user failed to login, with three consecutive incorrect login attempts, and seven others failed for two logins. In addition, only one participant was responsible for the maximum nonconsecutive failed attempts by a user (five attempts), as shown in Figure 3.

Table 4. GOTPass usability features.

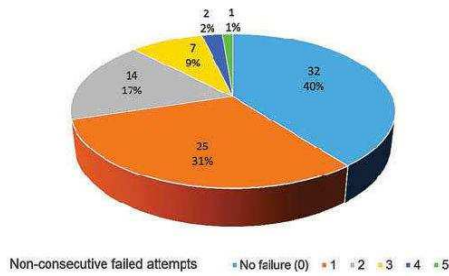|	Usability features				
	System-assigned themes	User-provided images	User-selected images	Memorability	Mnemonic
GOTPass	✓	✓	✓	✓	✓

Figure 3. Number of users and their non-consecutive failed attempts.

One of the observations from the trials highlighted that almost all failures occurred within the recognition part of the authentication process—more precisely, the wrong codes or inputting codes in the wrong order—since the majority of the participants claimed that they were sure they recognized their pass-images correctly but might have entered them in the incorrect order or made a typographical mistake.

4.1.3.3. Memorability.
Table 10 shows the details of the measurements used to calculate the memorability of the proposed scheme. Participants carried out a memorability experiment twice. The first took place after one week of nonuse (Trial 2), and the second was one month later (Trial 3). The results showed that all users managed to login successfully to their GOTPass accounts, but the number of attempts to do so varied. There was no lockout event, since all consecutive incorrect attempts were three or fewer.

Table 11 illustrates the number of failed login attempts in each sequence. It can be inferred from the table that 85% of the participants in Trial 2 managed to login successfully on their first attempt. In addition, the number of failed attempts seemed to reduce over time. One month later, in Trial 3, when participants tried to re-enter their GOTPass secrets, only 19% were unable to login correctly at the first attempt. However, during all trials, almost all users logged in successfully within three attempts, which shows an encouraging outcome from a password recall perspective.

4.1.3.4. User satisfaction.
The details of the measurements used to analyze the level of user satisfaction of the proposed scheme is shown in Table 12. User satisfaction was measured through a posttest questionnaire, which was given to the users at the end of their final study session. The aim was to discover the users' feelings toward the perceived aspects of usability and security of the proposed system. Most measurements were carried out using a 7-point Likert scale, ranging from 1 (strongly agree) to 7 (strongly disagree), whereas some others used multiple-choice measurements. All 81 participants of the user study took part in the survey. The results indicate that 86% of the respondents agreed that learning how to use the system and how to create a GOTPass account was simple, with the remaining 14% showing an average response. Almost 91% of the participants stated that this authentication method would become easier and quicker to use with practice. The vast majority of the participants (98.7%) stated that they would be confident using the GOTPass system. Ninety-four percent of the participants thought that the GOTPass system could be used for sensitive web authentication. The overall level of user satisfaction with the GOTPass system was very high, as 98% were in support of the idea. Note that the results of all responses were mostly in the positive half of the scale, which, in turn, reflects positive outcomes toward a prospective solution.

4.2. GOTPass security

Of particular interest to our work is the security aspect, which was evaluated in detail in a parallel work (Alsaiari et al., 2015). In brief, the key points from the preliminary results are also presented in this article. Two types of security evaluation were conducted, the first, "theoretical,", was based on assessment criteria, and the second, "empirical,", was where several attacks were simulated and tested.

The security experiment involved 81 participants, who were divided into three groups based on the assigned security attack experiment. Simulations of three security attacks were prepared (guessing, intersection, and shoulder-surfing attacks) to evaluate the proposed system's capability to resist such attacks. Participants were asked to

435

Table 5. Efficiency evaluation elements.

Usability elements	Measurements	Assessment type	Assessment method
Average entry time for registration/authentication	$Av(R) = \dfrac{Sum(successful\_registration\_times)}{number\_of\_successful\_registrations}$ $Av(L) = \dfrac{Sum(successful\_login\_times)}{number\_of\_successful\_logins}$	Objective/quantitative	Experiment/user trial

Table 6. Registration entry time details (in seconds).

	Total attempts	Total time	Average	SD	Minimum	Maximum
Registration	81	10,833	134	36.5	59	254

act as attackers to try and steal a victim's credentials. Overall, the analysis of the security evaluation showed that GOTPass had a high resistance against common graphical password attacks. The results showed that only 3.3% of the 690 login attempts succeeded in compromising the system.

5. Discussion

Compared with other graphical password techniques that are similar in nature, such as (Khot et al., 2012; Komanduri & Hutchings, 2008; Gao et al., 2009), GOTPass has both advantages and disadvantages. At first glance, many users thought it might be too complex; however, learning and practicing the system created an opposite impression, as the majority found it easy to use and adoptable.

The long account creation time is a disadvantage of the system, but, at the same time, it is worth mentioning that GOTPass is a multilevel authentication approach that employs several graphical password techniques into a single robust mechanism. That, in turn, might justify the extended time taken to create user accounts. In order to register, users need to complete multiple steps: username selection, unlock pattern drawing,

multiround pass-images selection, and, finally, choosing the security level along with the input format. In addition, these factors have an obvious impact on the complexity of the registration process. However, although it seems complex and takes time, the user study shows that, overall, users were satisfied—there were no complaints about the duration of the registration process or the level of difficulty. Furthermore, the GOTPass scheme provides strong resistance against various common security attacks, which is one of the primary objectives of this system.

Although the combination of several security methods may yield a higher level of security, it may also affect the usability of the system. However, that is not the case with the GOTPass scheme, as it aims to keep a reasonable balance between security and usability and avoid any trade-off. According to the results of the user study, there is no evidence of a negative impact on usability as a result of combining multiple security methods. Additionally, reporting a high success rate even after a period of time, as well as the users' positive perception regarding the simplicity of the system, prove that multiple security levels do not hamper the usability of GOTPass.

Focusing more on one of the chained steps and neglecting the others by choosing weak passwords should not be a major issue, as the success of breaking one of the authentication steps will not compromise the entire credentials. In addition, the

Table 7. Entry time details for successful authentication (in seconds).

	Total attempts	Success	Total time	Average	SD	Minimum	Maximum
Login	1,302	1,215	29,754	24.5	11	8	83

Table 8. Effectiveness evaluation elements.

Usability elements	Measurements	Assessment type	Assessment method
Login success rate	$SR(L) = \dfrac{number\_of\_successful\_logins}{number\_of\_total\_logins}$	Objective/quantitative	Experiment/user trial

Table 9. Login success and failure rates.

	Total attempts	Successful		Failed	
Trial 1	429	405	94.4%	24	5.6%
Trial 2	438	405	92.5%	33	7.5%
Trial 3	435	405	93.1%	30	6.9%
Total	1,302	1,215	93.3%	87	6.7%

Table 10. Memorability evaluation elements.

Usability elements	Measurements	Assessment type	Assessment method
Memorability over time intervals Short (one week), Extended (one month)	Matched at first attempt Matched within three login attempts	Objective/ quantitative	Experiment/ user trial

Table 11. Details of the frequency of the failed attempts based on trials and attempts.

	Trial 2						Trial 3					
Attempt sequence	1st	2nd	3rd	4th	5th	6th	1st	2nd	3rd	4th	5th	6th
Failure frequency	12	6	6	4	3	2	15	3	5	4	2	1
Total	33						30					

employment of the implicit feedback technique plays an important role in hiding which step is actually incorrect. In this way, it is difficult for an attacker to find out whether the strong or the weak step is wrong. In other words, GOTPass works as a package in which each part or feature complements the other.

Comparing the login time of GOTPass to other graphical schemes (see Figure 4) shows that the login time still appears to be sensible. As mentioned earlier, a significant reason that influences the performance time of an authentication scheme is the inclusion of multiple steps, which also justifies the longer time taken to register and login to GOTPass. However, GOTPass is still comparable to other two-step approaches, and is even superior within its category (three-step).

In terms of comparing GOTPass with its closest scheme, GOTP, a direct comparison is not straightforward, given that the evaluation data for GOTP are limited to posttest survey responses and not experimental data (Ku et al., 2012).
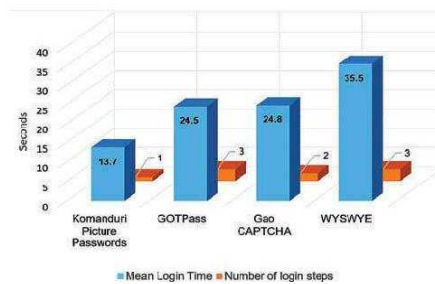
Nonetheless, a brief comparison between the two schemes is presented next. The data of our survey had to be adjusted from a 7-point Likert scale to a 5-point Likert scale to enable a direct comparison. To gain comparable results, the response values of the relevant questions were converted using the following method (IBM Support, 2015):

(1) L_i = Multiply the response value by its frequency (e.g., 7-point Likert scale × number of selected times).
(2) S = Sum, the total of all points ($L_7 + \ldots + L_1$).
(3) P = Divide S by the number of participants (S ÷ 81) [the mean value in a 7-point Likert scale].
(4) Q = Divide P by 7 (P ÷ 7) [the value in the range between 0 and 1].
(5) R = Multiply Q by the new Likert point number (Q × 5) [the mean value in a 5-point Likert scale], where the value of R represents the original result but using a 5-point Likert scale.

Figure 5 highlights the differences based on the available evaluation data of the GOTP scheme. It demonstrates that GOTPass has a major advantage of having a larger number of participants, which
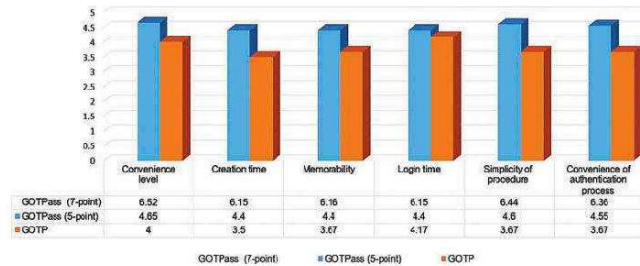

Figure 4. Comparison of the mean login time and number of steps to login.

Table 12. User satisfaction evaluation elements.

Usability elements	Measurements	Assessment type	Assessment method
Overall satisfaction (simplicity, ease of use, understandability, and perception of using GOTPass)	Satisfied Neutral Unsatisfied (7-point Likert scale/multiple choice)	Subjective/ qualitative	Questionnaire/ attitude scale

437

Figure 5. Comparison summary of GOTP and GOTPass.

increases the accuracy and reliability of the result. Although GOTP scored highly regarding the level of memorability, GOTPass showed even better results, which satisfies one of the main requirements of any prospective alternative authentication system. In relation to that, ease of use is another important feature, and GOTPass achieved a higher result than that of GOTP. However, across all comparison parameters, GOTPass performed very well, with over four out of five in all aspects.

In addition, the GOTP scheme requires the user to memorize four alphanumeric codes obtained by identifying the pass-images over four rounds. That, in turn, would require memory recall from the user, posing possible usability issues. In contrast, the GOTPass scheme does not involve the memorization of codes, since they are visible on a single screen. In addition, GOTP is designed for a smartphone platform that can be used as an out-of-band channel authentication, which is usually carried out away from the browser, whereas GOTPass utilises an in-session authentication system using the existing browser. In other words, there is no need for additional devices, such as a token or mobile phone, to use the GOTPass scheme. Regarding the length of the OTP code, GOTP submits a four-character-long code, whereas GOTPass requires an eight-character code. Themes and images used in GOTP are static and unchangeable, but in GOTPass they are dynamic and shuffling. The letters and numbers in the top corner of each GOTP image are barely readable on a mobile phone screen (Figure 6), which can be considered to be a major usability drawback of the system.

6. Conclusions and future research

This article has presented a usable mechanism to help authenticate users by using combined graphical password techniques along with an OTP. The main contribution is the introduction of draw-based and recognition-based graphical methods with the employment of an OTP to resist many of the common security threats without sacrificing ease of use. Initially, the results of the experiments indicated that the scheme has an acceptable level of efficiency and effectiveness as well as a high level of user satisfaction. Moreover, the study showed that GOTPass has the potential to succeed and contribute toward the adoption of graphical password technologies. Further research is recommended that should concentrate on conducting a field study and improving registration and login times. Enlarging the sample of participants and running the user study for an extended period of time are suggested to allow more conclusive analysis of the data. It is also suggested to investigate the compatibility and effectiveness of the current design on different platforms, especially handheld devices. In terms of security, the resilience of the proposed scheme has been investigated in parallel with this study. In fact, the results of the earlier security experiment, involving three different attack simulations against GOTPass, were encouraging and complementary to this work.

References

Alsaiari, H., Papadaki, M., Dowland, P., & Furnell, S. (2015). Secure graphical one time password (GOTPass): An Empirical study. *Information Security Journal: A Global Perspective, 24*(4–6), 207–220.

Figure 6. A screenshot of the GOTP login screen.

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *International Journal of Human-Computer Interaction, 24*(6), 574–594. doi:10.1080/10447310802205776

Biddle, R., Chiasson, S., & Van Oorschot, P. (2011). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys, 44*, 4.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy (SP)* (pp. 553–567). IEEE.

Brostoff, S., Inglesant, P., & Sasse, M. A. (2010). Evaluating the usability and security of a graphical one-time PIN system. In *Proceedings of the 24th BCS Interaction Specialist Group Conference* (pp. 88–97). British Computer Society.

Chiang, H.-Y., & Chiasson, S. (2013). Improving user authentication on mobile devices: A touchscreen graphical password. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 251–260). ACM.

De Angeli, A., Coutts, M., Coventry, L., Johnson, G. I., Cameron, D., & Fischer, M. H. (2002). VIP: A visual approach to user authentication. In *AVI '02 Proceedings of the Working Conference on Advanced Visual Interfaces* (pp. 316–323). New York, NY: ACM.

De Angeli, A., Coventry, L., Johnson, G. I., & Coutts, M. (2003). Usability and user authentication: Pictorial passwords vs. pin. In P. T. McCabe (Ed.), *Contemporary ergonomics* (pp. 253–258). London, UK: Taylor & Francis.

De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies, 63*(1–2), 128–152. doi:10.1016/j.ijhcs.2005.04.020

Gao, H., Liu, X., Wang, S., & Dai, R. (2009). A new graphical password scheme against spyware by using CAPTCHA. In *Proc. Symposium On Usable Privacy and Security (SOUPS)* (pp. 15–17).

Gupta, S., Sahni, S., Sabbu, P., Varma, S., & Gangashetty, S. V. (2012). Passblot: A highly scalable graphical one time password system. *International Journal of Network Security & Its Applications (IJNSA), 4*, 2.

IBM Support. (2015). *Transforming different Likert scales to a common scale*. Retrieved from http://www-01.ibm.com/support/docview.wss?uid=swg21482329

International Organization for Standardization. (1998). *ISO 9241-11: Ergonomic requirements for office work with visual display terminals (VDTs): Part 11: Guidance on usability.*

Khot, R. A., Kumaraguru, P., & Srinathan, K. (2012). WYSWYE: Shoulder surfing defense for recognition based graphical passwords. In *Proceedings of the 24th Australian Computer-Human Interaction Conference* (pp. 285–294). ACM.

Komanduri, S., & Hutchings, D. R. (2008). Order and entropy in picture passwords. In *Graphics Interface Conference 2008* (pp. 115–122). Ontario, Canada: Canadian Information Processing Society.

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J.-H. (2012). Extended otp mechanism based on graphical password method. In *Future Information Technology, Application, and Service*, Vol. 1 (pp. 203–212). Netherlands: Springer.

Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J.-H. (2013). Two-factor authentication system based on extended otp mechanism. *International Journal of Computer Mathematics*, 90(12), 2515–2529.

Nielsen, J. (1994). Usability heuristics. In J. Nielsen (Ed.), *Usability Engineering* (pp. 129–130). London, UK: AP Professional.

Schaub, F., Walch, M., Könings, B., & Weber, M. (2013). Exploring the design space of graphical passwords on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (p. 11). ACM.

Standing, L., Conezio, J., & Haber, R. N. (1970). Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. *Psychonomic Science*, 19(2), 73–74. doi:10.3758/BF03337426

Van Oorschot, P. C., & Wan, T. (2009). TwoStep: An authentication method combining text and graphical passwords. In G. Babin, P. Kropf, & M. Weiss (Eds.), *E-technologies: innovation in an open world* (Vol. 26, pp. 233–239). Berlin Heidelberg: Springer.

Von Zezschwitz, E., Dunphy, P., & De Luca, A. (2013). Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 261–270). ACM.

Wang, L., Chang, X., Ren, Z., Gao, H., Liu, X., & Aickelin, U. (2010). Against spyware Using CAPTCHA in Graphical password scheme. In *24th IEEE International Conference on Advanced Information Networking and Applications (AINA)* (pp. 760–767). IEEE.

Biographies

Hussain Alsaiari received a Bachelor's Degree in Computer Science from King Abdulaziz University, Saudi Arabia, in 2000. He was awarded his MSc with distinction in Internet, Computer and System Security from the University of Bradford, UK, in 2006. He is currently a PhD candidate in the Centre for Security, Communications and Network Research at Plymouth University, UK. His research interests reside in the area of authentication, usable security, and human aspects of security.

Dr. Maria Papadaki received her PhD in 2004 from University of Plymouth. Prior to joining academia in 2006, she worked as a security analyst for Symantec EMEA. Her research interests include incident response, insider threats, intrusion prevention and detection, security information and event management, security assessment, social engineering, security usability, and security education. Her research output includes 19 journal and 30 international peer-reviewed conference papers. Dr. Papadaki holds GCIA, GPEN, and CEH certifications and is a member of the GIAC Advisory Board, as well as the BCS, IISP, and ISACA. Further details can be found at www.cscan.org/papadaki.

Dr. Paul Dowland is a member of the Centre for Security, Communications & Network Research and manages the teaching of computer security and networking within the School of Computing, Electronics and Mathematics at Plymouth University in the United Kingdom. His interests include network and system security, user authentication, and security education. Dr. Dowland is the secretary to the International Federation for Information Processing (IFIP) Working Group 11.1 (Information Security Management) and a Fellow of the BCS. He is the author of over 50 articles in refereed international journals and conference proceedings, has edited 24 books, and co-authored *E-Mail Security: A Pocket Guide* (IT Governance Pub., 2010). Further details can be found at the CSCAN website (www.cscan.org/pdowland). Paul can also be followed on Twitter (@pdowland).

Prof. Steven Furnell is the head of the Centre for Security, Communications & Network Research at Plymouth University (UK), an Adjunct Professor with Edith Cowan University (Western Australia), and an Honorary Professor with Nelson Mandela Metropolitan University (South Africa). His interests include mobile device security, cyber crime, user authentication, and security usability. Prof. Furnell is the author of over 260 articles in refereed international journals and conference proceedings, as well as books including *Cybercrime: Vandalizing the Information Society* (Addison-Wesley, 2002) and *Computer Insecurity: Risking the System* (Springer Science & Business Media, 2005). He is also the editor-in-chief of *Information & Computer Security*, and the co-chair of the Human Aspects of Information Security & Assurance (HAISA) symposium (www.haisa.org). Steve is active in a variety of professional bodies, and is a Fellow of the BCS, a Senior Member of the IEEE, and a Board Member of the IISP. Further details can be found at www.plymouth.ac.uk/cscan.

440

- **Press Release**

SUCCEED
WITH
PLYMOUTH
UNIVERSITY

/ Home / Press office / Images and codes provide alternative to multiple device password systems

Images and codes provide alternative to multiple device password systems

Researchers from the Centre for Security Communication and Network Research believe GOTPass could be effective in protecting against hackers

Mr Alan Williams

Media & Communications Officer

Communication Services (External Relations)

23 December 2015

A system using images and a one-time numerical code could provide a secure and easy to use alternative to multi-factor methods dependent on hardware or software and one-time passwords, a study by Plymouth University suggests.

Researchers from the Centre for Security Communication and Network Research (CSCAN) believe their new multi-level authentication system GOTPass could be effective in protecting personal online information from hackers.

It could also be easier for users to remember, and be less expensive for providers to implement since it would not require the deployment of potentially costly hardware systems.

Writing in Information Security Journal: A Global Perspective, researchers say the system would be applicable for online banking and other such services, where users with several accounts would struggle to carry around multiple devices, to gain access.

They also publish the results of a series of security tests, demonstrating that out of 690 hacking attempts – using a range of guesswork and more targeted methods – there were just 23 successful break-ins.

PhD student Hussain Alsaiari, who led the study, said:

> "Traditional passwords are undoubtedly very usable but regardless of how safe people might feel their information is, the password's vulnerability is well known. There are alternative systems out there, but they are either very costly or have deployment constraints which mean they can be difficult to integrate with existing systems while maintaining user consensus. The GOTPass system is easy to use and implement, while at the same time offering users confidence that their information is being held securely."

To set up the GOTPass system, users would have to choose a unique username and draw any shape on a 4x4 unlock pattern, similar to that already used on mobile devices. They will then be assigned four random themes, being prompted to select one image from 30 in each.

When they subsequently log in to their account, the user would enter their username and draw the pattern lock, with the next screen containing a series of 16 images, among which are two of their selected images, six associated distractors and eight random decoys.

Correctly identifying the two images would lead to the generated eight-digit random code located on the top or left edges of the login panel which the user would then need to type in to gain access to their information.

Initial tests have shown the system to be easy to remember for users, while security analysis showed just eight of the 690 attempted hackings were genuinely successful, with a further 15 achieved through coincidence.

Dr Maria Papadaki, Lecturer in Network Security at Plymouth University and director of the PhD research study, said:

> "In order for online security to be strong it needs to be difficult to hack, and we have demonstrated that using a combination of graphics and one-time password can achieve that. This also provides a low cost alternative to existing token-based multi-factor systems, which require the development and distribution of expensive hardware devices. We are now planning further tests to assess the long-term effectiveness of the GOTPass system, and more detailed aspects of usability."

The research paper – Secure Graphical One Time Password (GOTPass): An Empirical Study by Alsaiari, Papadaki, Dowland and Furnell – is published in Information Security Journal: A Global Perspective.