University of Plymouth

PEARL **https://pearl.plymouth.ac.uk**

04 University of Plymouth Research Theses 01 Research Theses Main Collection

2004

Advanced user authentification for mobile devices

Clarke, Nathan Luke

http://hdl.handle.net/10026.1/598

http://dx.doi.org/10.24382/4527
University of Plymouth

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.

store

ADVANCED USER AUTHENTICATION FOR MOBILE DEVICES

N. L. CLARKE

Ph.D. 2004

90 0618019 1

LIBRARY STORE

REFERENCE ONLY

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.

Advanced User Authentication for Mobile Devices

by

NATHAN LUKE CLARKE

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

DOCTOR OF PHILOSOPHY

School of Computing, Communication & Electronics

In collaboration with

Orange Personal Communication Services Ltd.

November 2004

University of Plymouth
Library
Item No. 9006180191
Shelfmark THESIS 621.382 CLA

Abstract

Advanced User Authentication for Mobile Devices

Nathan Luke Clarke
BEng (Hons)

Recent years have witnessed widespread adoption of mobile devices. Whereas initial popularity was driven by voice telephony services, capabilities are now broadening to allow an increasing range of data orientated services. Such services serve to extend the range of sensitive data accessible through such devices and will in turn increase the requirement for reliable authentication of users.

This thesis considers the authentication requirements of mobile devices and proposes novel mechanisms to improve upon the current state of the art. The investigation begins with an examination of existing authentication techniques, and illustrates a wide range of drawbacks. A survey of end-users reveals that current methods are frequently misused and considered inconvenient, and that enhanced methods of security are consequently required. To this end, biometric approaches are identified as a potential means of overcoming the perceived constraints, offering an opportunity for security to be maintained beyond point-of-entry, in a continuous and transparent fashion.

The research considers the applicability of different biometric approaches for mobile device implementation, and identifies keystroke analysis as a technique that can offer significant potential within mobile telephony. Experimental evaluations reveal the potential of the technique when applied to a Personal Identification Number (PIN), telephone number and text message, with best case equal error rates (EER) of 9%, 8% and 18% respectively. In spite of the success of keystroke analysis for many users, the results demonstrate the technique is not uniformly successful across the whole of a given population. Further investigation suggests that the same will be true for other biometrics, and therefore that no single authentication technique could be relied upon to account for all the users in all interaction scenarios. As such, a novel authentication architecture is specified, which is capable of utilising the particular hardware configurations and computational capabilities of devices to provide a robust, modular and composite authentication mechanism. The approach, known as IAMS (Intelligent Authentication Management System), is capable of utilising a broad range of biometric and secret knowledge based approaches to provide a continuous confidence measure in the identity of the user. With a high confidence, users are given immediate access to sensitive services and information, whereas with lower levels of confidence, restrictions can be placed upon access to sensitive services, until subsequent reassurance of a user's identity.

The novel architecture is validated through a proof-of-concept prototype. A series of test scenarios are used to illustrate how IAMS would behave, given authorised and impostor authentication attempts. The results support the use of a composite authentication approach to enable the non-intrusive authentication of users on mobile devices.

Contents

List of Figures

List of Tables

Acknowledgements

The research programme was made possible due to funding from the Engineering and Physical Sciences Research Council (EPSRC), and Orange Personal Communication Services Ltd. I wish to thank both organisations for their support.

I also wish to thank Imagis Technologies, and particularly John Lyotier, for providing the facial recognition software which subsequently enabled its incorporation within IAMS. Without the facial recognition software it would have not been possible to develop such an interesting prototype.

The work, and indeed this PhD, would not have been possible without the help and support of my Director of Studies, Dr. Steven Furnell. Thanks go to him for his tireless effort in steering me through the PhD process, from publishing papers to presenting at international conferences. His professionalism and experience has been invaluable, and I owe much of my success to his guidance.

Thanks must also go to my other supervisors, Prof. Paul Reynolds and Dr. Benn Lines, who have spent a lot time proof reading papers and my thesis, in addition to providing helpful experience and guidance throughout my studies.

Finally, I wish to thank my friends and family for their support over the past three years. In particular, I wish to thank my parents, who I'm sure never thought my student life would end.

Authors Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award.

This study was financed with the aid of a studentship form the Engineering and Physical Sciences Research Council, and carried out in collaboration with Orange Personal Communication Services Ltd.

Relevant seminars and conferences were regularly attended at which work was often presented and several papers prepared for publication.

Signed .....

Date 18/11/04

1 Introduction & Overview

The research presents a novel approach to authentication for mobile devices, enabling continuous identity verification of the user, whilst minimising intrusive authentication requests that would require explicit interaction. With the growing number and complexity of devices, and their future ability to access a prolific range of services, this composite authentication architecture solves the problems of weak and intrusive point-of-entry authentication techniques and typically requires nothing more than the user interacting with the mobile device in a normal manner.

1.1 Introduction

The ability to communicate and work whilst on the move has given rise to a significant growth in mobile devices. The term mobile device describes three principal computing devices, the mobile handset (or cellular handset), the Personal Desktop Assistant (PDA) and the laptop[1]. The growth of mobile devices has primarily come out of mobile handset related technologies with worldwide subscribers now in excess of a billion (UMTS Forum, 2003). In addition, both the use of PDAs and laptop computers has been growing in popularity (Smith, 2004a; Lemon, 2003): behind this growth are wireless technologies such as cellular networks and wireless LANs, which enable mobile devices to access a range of data-centric services. For instance, future cellular devices will be able to pay for products using micro-payments and digital money, surf the Internet, buy and sell stocks, transfer money and manage bank accounts, and wireless LAN enabled devices with their high bandwidth connections are capable of providing fast access to corporate networks and financial information.

In order to enable delivery of such services, mobile devices have become increasingly powerful: mobile handsets in particular have evolved from relatively basic terminals, that would handle analogue telephony communications, to digital handsets capable of providing a host of data-centric services, turning the handset into a multimedia, multi-purpose, mobile communications tool, providing much of the functionality of today's PDAs. In fact, a convergence can be seen between mobile handsets and PDAs, with the only significant difference at present being the access technology to the wireless network – with PDAs typically utilising wireless LAN and handsets using one of many cellular

[1] The term mobile device will be utilised throughout this thesis to describe all three types of mobile device. Specific reference to individual devices will be made as and where necessary.

standards that exist. In parallel with this increase in functionality is the ability for devices to store information, with many accepting solid-state memory such as Compact Flash and Secure Digital (SD), which are capable of providing storage in excess of 512MB. Laptop computers fall somewhat outside of this definition due to their far superior processing and storage capability, more similar to desktop computers than the remaining mobile devices. Nevertheless, this storage capability enables mobile devices to store large quantities of information – much of which may be personally, financially or corporately sensitive.

Given the widespread popularity, increased functionality and storage, the need to protect the mobile device becomes paramount in order to stop misuse. In 2001, 700,000 mobile handsets were stolen in the UK (Harrington & Mayhew, 2001), leading the government to set-up a National Mobile Phone Crime Unit to specifically target the problem (Best, 2003). It can be conjectured that the advanced capabilities of future mobile devices will make them even more desirable targets.

Currently, the most popular access security to date takes the form of the password or PIN, a secret knowledge approach that relies heavily upon the user to ensure continued validity. For example, the user should not use the default factory settings, tell other people, or write it down. However, the poor use of passwords and PINs has been widely documented, with many laptop owners using simple passwords that dictionary attacks can crack in seconds (Denning, 1999) and with many mobile handset and PDA users not even using the security which is available (Lemos, 2002). In addition, mobile handsets only request the PIN at switch on, with the device remaining on for large periods of the day with no protection from misuse. Although this has not been a big issue, as the number of mobile devices capable of advanced services and the availability of some wireless networks is limited, this will not hold true in the future where the majority of mobile devices will be capable of, and

have access to, an extensive range of services. The financial loss to the user in this case would not only be the theft of the device itself, but the services accessed before network access is denied and the personal data stored upon the device.

The aim of this research is to establish an advanced authentication architecture capable of providing the increased security required for mobile devices, and extending protection beyond point-of-entry as to ensure the identity of the user on a continual basis. In order to achieve this continuous authentication, a second aim, that of providing transparent or non-intrusive authentication, is deemed imperative in order to minimise user inconvenience and increase subsequent user acceptance. By being able to authenticate a user without their knowledge, the integrity of the system can be automatically maintained and monitored without the user's explicit interaction, until such time as the system deems an impostor is accessing the system.

1.2 Aims & Objectives

The aim of this research is to define, design and validate an advanced non-intrusive user authentication security architecture suited to mobile devices. This has been achieved by focussing upon the technology and functionality of mobile devices to evaluate approaches that would enable transparent and continuous authentication.

In order to achieve this, the research can be divided into five distinct phases.

- To assess the requirement for new and advanced authentication techniques and mechanisms for mobile devices.

- To investigate the applicability of advanced authentication techniques, for deployment on a mobile device.

- To design and evaluate a new biometric technique for mobile devices, with the aim of increasing the transparent authentication capability available to the device.

- To design an architecture to support the aims of continuous and transparent authentication on mobile devices thereby ensuring security is maintained.

- To implement and test a prototype of the system to demonstrate its practical effectiveness.

The first phase provides a comprehensive review and discussion of the need for authentication. Through an understanding of the development of mobile devices, and where the direction the technology is taking, this phase of the research provides the comprehensive arguments and basis for the need for additional authentication. This identified the second phase proceeds with a literature review and evaluation of current authentication approaches; giving an insight into current authentication techniques with a particular focus upon their deployment within a mobile device context. The outcome of this phase is to identity a number of authentication approaches that would lend themselves towards a mobile device.

In order to achieve the objective of transparent and continuous authentication it was imperative to be able to increase the transparent authentication capability of mobile devices. From the identified approaches, one particular technique fulfilled this objective

across a wide range of mobile devices. The ability to authenticate a person based upon their typing patterns, known as keystroke analysis, would permit all mobile devices with a keypad the capacity, in principal, to authenticate users based upon entering a telephone number or text message, scheduling a task or composing an email. However, although the technology had been proven with a good degree of success on standard keyboards, it was unproven on keypads, where the tactile and typing differences might have proven the technique infeasible. Therefore, the third phase of the research sought to evaluate the feasibility of a keystroke analysis technique upon a keypad.

However successful keystroke analysis proved to be, it would not be suited to all mobile devices. A small number do not have keypads or thumb-sized keyboards making the technique obsolete. In addition, it was clear from initial studies of keystroke analysis, the performance of the technique would not have proven conclusive enough to be deployed in its own right. As a result the fourth phase of the research sought to design an authentication architecture flexible enough to encompass all mobile devices, utilising a composite number of authentication techniques that draw upon the different hardware components of a mobile device. The completion of the final phase was to design and evaluate a prototype of the authentication architecture.

1.3 Thesis Structure

The thesis addresses the aforementioned objectives in order and is comprised of the following chapters.

Chapter 2 discusses the need for user authentication, focussing upon the proliferation of wireless communication networks, and the growing popularity of mobile devices, illustrating from a technological perspective the need to protect mobile devices from misuse. The chapter continues, describing the mechanisms currently deployed on mobile devices to ensure identity verification, and provides substantial evidence of the weaknesses of such approaches. The chapter concludes by analysing results from a survey into the attitudes and opinions of subscribers towards security for their mobile handset, determining how users currently use their handset and their perceptions of the current authentication mechanism.

Having firmly established the need for authentication, chapter 3 is dedicated to a review of biometrics. Having discussed the process behind biometrics, what they are, and the factors that affect them, the chapter proceeds to describe a number of biometric techniques that lend themselves to application on a mobile device, ensuring the aims of continuous and transparent authentication are met. The use of biometrics is supported by the findings from the aforementioned survey of subscribers. Finally, considerations into the practical use of biometrics are discussed, with particular emphasis upon keystroke analysis.

Chapter 4 introduces the first of two studies into the feasibility of keystroke analysis on a mobile device. The studies have been based upon identifying particular user-handset

interactions with which to authenticate the user, in particular, the manner in which users enter telephone numbers, enter PINs and compose text messages. Chapter 4 utilises a particular keystroke characteristic to classify users based upon the entry of telephone numbers and PINs. The chapter compares and contrasts the application of a number of pattern classification algorithms based upon statistical and artificial intelligence techniques. The chapter concludes with an evaluation of the technique.

Chapter 5 builds on the successes and knowledge of chapter 4 to evaluate the viability of authenticating users based upon a second keystroke characteristic, applied to the composition of text messages.

Chapter 6 presents a mechanism for composite authentication. Through the use of multiple authentication techniques, the ability to correctly verify the identity of a user becomes stronger, as the weaknesses of one technique, are overcome by the strengths of others. In addition, the use of a composite authentication approach permits a more transparent means of authentication. Keystroke analysis permits the authentication of users during certain handset interactions such as entering a telephone number, but not others. By using different techniques in varying handset scenarios it is possible to non-intrusively authenticate the user during a wider range of handset interactions. The architecture has been designed in a flexible, modular and scalable manner in order to meet the differing hardware and network variations that reside with mobile devices. The chapter describes the various components required in the framework and the processes developed to ensure that the system integrity is maintained.

Chapter 7 proposes an Intelligent Authentication Management System (IAMS) architecture which incorporates the aforementioned composite authentication framework. The chapter

proceeds to discuss the development IAMS along with keystroke analysis and a commercial biometric into a functional prototype. The chapter describes the process of realising the specification within a proof-of-concept prototype, highlighting three key system components:

- The Console Manager, as the administrative tool for controlling, adding and monitoring mobile devices;
- IAMS Manager, as the real-time authentication controller and
- Client-Side software, providing the end-user interface and biometric capturing.

Chapter 8 presents an evaluation of IAMS. The chapter details the theoretical performance IAMS can achieved under a number of different hardware scenarios and compares this against a number of alternative authentication techniques. The chapter concludes by providing a practical validation of the IAMS prototype.

Finally, chapter 9 presents the main conclusions arising from the research, highlighting the key achievements and limitations. The chapter contains a discussion on areas for future research and development. The thesis also provides a number of appendices in support of the main discussion, including experimental procedures and code listings. The appendices also contain a number of published papers arising from the research programme.

2 Review of Authentication on Mobile Devices

This chapter investigates and discusses the need for authentication on mobile devices, by highlighting the predominant wireless technologies and the services which they enable – illustrating their popularity and potential dangers. The chapter proceeds to discuss the types of mobile device which utilise these wireless networks and the user authentication mechanisms that reside within them – focussing upon the weaknesses and drawbacks of current approaches. Finally, the chapter presents further evidence in the form of an end-user survey of subscribers, which assessed their attitudes and opinions towards security for their mobile handset.

2.1 Introduction

The purpose of authentication is to ensure that access is only given to an authorised person or persons. However, the authentication mechanism itself can vary both in complexity and in cost, and the level of authentication required is inherently tied to the application within which it is deployed. The level of authentication provided by mobile devices to date is arguably commensurate with the level of protection required against misuse, when considering the financial cost of device misuse, due to the limited services and data that can be accessed, versus the cost of implementing an authentication mechanism.

However, with the popularity of mobile devices, increasing functionality and access to personally and financially sensitive information, the requirement for additional and/or advanced authentication mechanisms is argued to be essential. Much of this authentication need has come about due to the success of wireless networking technologies that have given devices access to services and information whilst on the move, beyond what is stored within the device itself. As such a secret-knowledge, point-of-entry technique, such as the PIN-based authentication that is currently implemented on all but a few mobile devices, will no longer be sufficient.

2.2 Mobile Devices & Wireless Networks

Mobile devices have evolved from two contrasting directions. The first is from telephony devices that have always had a wireless network connection, but until recently minimal computational and storage capability, and so were unable to provide the user with many services beyond voice telephony. The second is from devices with reasonable computing power but no (simple) method by which they were able to connect to a network outside of the office environment. Today, however, with the advancement of mobile handsets and wireless networking, mobile devices have both the network access and computing capacity to provide users with a diverse range of services. This can be supported by a strong market growth in mobile devices, up 62% in 2004 on the previous year (Smith, 2004b), and with forecasts predicting wireless revenues being worth up to $126bn by 2008 (ARC Group, 2003).

The single most successful wireless technology to date has evolved device technology from pure telephony handsets into multimedia multi-functional mobile communication tools. The mobile telecommunications industry has experienced a number of revolutionary and evolutionary steps during its relatively short existence, with a current subscription based of 1.3 billion users worldwide (Cellular Online, 2004a). Table 2.1 illustrates the evolution of the mobile handset from the GSM (Global System for Mobile Communications) perspective – the most popular cellular standard (GSM World, 2003).

	Mobile Phone Evolution					
	1G	2G		2.5G	3G	4G
Technical						
Network Type	TACS	GSM	HSCSD	GPRS	UMTS	Internet
Transmission Type	Analogue	Digital	Digital	Digital	Digital	Digital
Data Bandwidth (bits/sec)		9.6K	57.4K*1	114K*1	2M*1	>100M
Frequency	900M	900 & 1800M	1800M	900 & 1800M	2G	40/60G
Switching	Circuit	Circuit	Circuit	Packet	Packet	Packet
Services						
Voice	✓	✓	✓	✓	✓	✓
SMS		✓	✓	✓	✓	✓
Internet		✓(WAP)	✓(WAP)	✓(WAP)	✓	✓
MMS				✓	✓	✓
Miscellaneous						
Availability	1983	1992	2000	2001	2002	2010

*1 Theoretical maximum bandwidth

Table 2.1: Evolution of the Mobile Phone

Within the UK, the four principal network operators are still running 2.5G networks. However Vodafone, T-Mobile and Orange are in the process of enabling data communications across their 3G network (Sherriff, 2004). Only Hutchison 3G have a working 3G network for public use to date (Hutchison 3G, 2004a).

The investment made by cellular operators into 3G networks stands as a testament to the potential revenue opportunity 3G networks are perceived to present, with UK operators alone having cumulatively invested over £22 billion in spectrum licensing (Wakefield, 2000). This ignores the additional investments required in network infrastructure to upgrade the network to 3G. Table 2.2 illustrates several categories of service application that have been defined for 3G (Giussani, 2001) and Figure 2.1 illustrates projected revenue forecasts for 3G services (UMTS Forum, 2003).

provider in Japan, however, has already gone beyond Europe in its deployment of data services and serves as an (additional) example of the popularity and potential revenue source data services can be. NTT DoCoMo is Japan's largest mobile network provider with over 48 million subscribers (NTT DoCoMo, 2004b). In 1999 DoCoMo introduced iMode, a wireless internet service that permits the user to receive news, email, entertainment channels and stock news amongst other information (Dubendorf, 2003). This service has experienced unprecedented success with over 41 million subscribers (NTT DoCoMo, 2004c). Since the introduction of iMode, DoCoMo has rolled out third generation networks, the first commercial network in the world, with over 3 million subscribers (NTT DoCoMo, 2004d).

Another increasingly predominant wireless networking technology is wireless LAN (also known as WiMax or Wi-Fi). A recent study noted organisations with over 100 employees were reporting they had experienced saving of $164,000 annually on cabling costs and labour (Reynolds, 2003), through the deployment of wireless networks. However, of particular interest is the growing number of public Wi-Fi locations, known as "hotspots", that are appearing, giving the general public access to broadband connections for their Wi-Fi enabled mobile devices. For instance, by the summer of 2004, BT Openzone, just one of many Wi-Fi providers in the UK, plans to boost its current 1,700 public hotspots to 4,000 (Twist, 2004). It has been predicted that by 2006, 100 million users worldwide will be using Wi-Fi (Reynolds, 2003).

The terms Wi-Fi and WiMax describe a family of networking standards created by the 802 Local and Metropolitan Area Networks Standards Committee (LMSC) of the IEEE computer Society (IEEE Computer Society, 2001). Work began in 1990, when the LMSC formed the 802.11 workgroup to develop a wireless networking standard. The output from

this body was to establish a number of standards, which vary in their data capacity and operating frequencies (Maxium & Pollino, 2002). A recent report looking into Wi-Fi in North America and Europe forecasts Wi-Fi services to be worth $18 billion by 2008 (Smith, 2003). The wide bandwidth provided by Wi-Fi further expands the range of services that can be provided to mobile devices. With these new range of services and the financial and personal costs incurred should the device be misused, the need to ensure the correct identity of the user becomes far more important than when the number and cost of services was limited.

Much discussion has taken place regarding the role mobile (cellular) networks and Wi-Fi have and whether this role is competitive or complementary (Vaughan-Nichols, 2003; 3G.co.uk, 2003). With trade-offs between mobile networks providing more comprehensive service coverage and Wi-Fi having cheaper network infrastructure and faster transmission speeds (Reynolds, 2003). Again, it is not the intention of the author to argue the advantages and disadvantages of each access technology, but to highlight their existence, level of industry support and service capability. It is likely however, due in part to large industry backing and financial support that both technologies will co-exist as complementary services in the near term. 3GPP (Third Generation Project Partnership), a group of interest parties governing the application of UMTS, has already taken the initiative to develop a cellular-WLAN internetworking architecture as an add-on to the 3GPP mobile system specifications (Ahmavaara, 2003). In any event, high-speed wireless communications are here to stay.

2.3 Authentication on Mobile Devices

Wireless networks provide the opportunity for a user to access a wide variety of services, from email, bank accounts and share dealing, to location-based services and infotainment (UMTS Forum, 2003). But what devices can access these services and what ensures the person using the device is the authorised user?

The majority of mobile devices can be described to fall broadly within three categories:

- Cellular, Mobile Handset or Smart Phone
- Personal Desktop Assistant
- Laptop Computer

The process of authentication in general is based upon three fundamental approaches (Wood, 1977): something the user knows, i.e. passwords and PINs; something the user has, i.e. tokens and/or something the user is, i.e. biometrics. This section will examine the user authentication mechanisms deployed upon these devices, focussing upon their strengths and weaknesses.

2.3.1 Mobile Handset

Recent statistics from the UK Home Office has highlighted the issue of mobile handset theft, with over 700,000 handsets stolen in 2001 (Harrington & Mayhew, 2001), although unofficial reports have put this figure in the region of 1.3 million (Leyden, 2002). It should be noted that, not all handset thefts led to handset misuse, in terms of accessing

The SIM card is a removable token containing the authentication keys required for network authentication, allowing in principle for a degree of personal mobility. For example, a subscriber could place their SIM card into another handset and use it in the same manner as they would use their own phone with calls being charged to their account. However, the majority of mobile handsets are typically locked to individual networks, and although the SIM card is in essence an authentication token, in practice the card remains within the mobile handset throughout the life of the handset – removing any additional security that might be provided by a token-based authentication technique.

The purpose of the IMSI and TMSI are to authenticate the SIM card itself on the network, and they do not ensure that the person using the phone is actually the registered subscriber. This is only achieved (typically) at switch on using the PIN, although some manufacturers also have the PIN mechanism when you take the mobile out of a stand-by mode. As such, a weakness of Point-of-Entry systems is that, after the handset is switched on, the device is vulnerable to misuse should it be left unattended or stolen. No continuous authentication mechanism resides on second generation mobile handsets in order to ensure that the user is the registered subscriber throughout the duration the handset remains powered on.

In addition, the PIN is a secret-knowledge authentication approach, and thus relies upon some knowledge that the authorised user has. Unfortunately, secret-knowledge based techniques have been found to be inherently insecure, due in many cases to the authorised users themselves (Lemos, 2002; Morris & Thompson, 1979). Reasons for insecurity can include noting the PIN on paper and telling it to friends. One implementation of the PIN on mobile handsets that does curb attacks is by allowing the user to enter the PIN a limited number of times (typically three) and thus removing the possibility of brute force attacks (entering every possible combination of PIN input).

More recently, a few handset operators and manufacturers have identified the need to provide more secure authentication mechanisms. For instance, Sagem (2002) developed a handset with fingerprint reader showcasing future product functionality and Atrua Technologies have developed a directional menu pad (similar in appearance to a mouse-pad contained on a laptop) that also provides fingerprint recognition (Atrua, 2004). To date however, only one commercial handset exists that provides alternative point-of-entry authentication to the PIN, and that has been developed for Japan's NTT DoCoMo network operator. The F505i handset comes equipped with a built-in fingerprint sensor, providing biometric authentication of the user (NTT DoCoMo, 2004a). Although fingerprint technology increases the level of security available to the handset, the implementation of this mechanism has increased handset cost, and even then the technique remains point-of-entry only and intrusive to the subscriber.

However, given the introduction of third generation mobile networks, it can be argued that handsets will represent an even greater enticement for criminals:

1. More technologically advanced mobile handsets – 3G handsets will be far more advanced than current mobile phones with many having much of the functionality of PDAs. As such 3G handsets will be more expensive and subsequently attractive to theft, resulting in a financial loss to the subscriber.
2. Availability of data services – 3G networks will provide the user with the ability to download and purchase a whole range of data services and products that would be charged to the subscribers account. Additionally 3G networks will provide access to bank accounts, share trading and making micro-payments. Theft and misuse of the handset would result in financial loss for the subscriber.

3. Personal Information – 3G handsets will be able to store much more information than current handsets. Contact lists will not only include name and number but addresses, dates of birth and other personal information. 3G handsets may also be able to access personal medical records and home intranets and their misuse would result in a personal and financial loss for the subscriber.

To combat these security issues, the 3GPP has drawn up standards concerning security on 3G handsets. In a document called "3G – Security Threats and Requirements" (3GPP, 1999) the requirements for authentication are outlined, stating:

> *"It shall be possible for service providers to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorised access to 3G services by masquerade or misuse of priorities"*

The important consequence of this standard is to authenticate subscribers during service delivery, an extension of the 2G point-of-entry authentication, which requires continuous monitoring and authentication. This could be best achieved through a non-intrusive or transparent technique so users would not be aware that authentication is taking place, avoiding the user having to stop a call in order to re-enter a PIN for instance. However, network operators, on the whole, have done little (with the previous DoCoMo exception noted) to improve authentication security, let alone provide a mechanism for making it continuous.

level of protection, the authentication mechanism on PDAs is determined by the operating system. To date, both the main operating systems have deployed password or PIN based authentication, with the occasional high end model containing a fingerprint sensor, as illustrated by the HP iPAQ. The additional security provided by this IPAQ really is the exception rather than the rule, as only one particular model of iPAQ (incidentally the most expensive) contains the sensor, with the remaining models relying upon a password or PIN. None of the Palm-based PDAs contain any authentication security beyond secret-knowledge based approaches as standard. A number of companies are beginning to provide authentication mechanisms for PDAs. Romsey Associates has developed a signature recognition approach for use on Palm and Windows based PDAs (PDALok, 2004a), and Domain Dynamics, a company specialising in authenticating a person by their voice (known as Voice Verification) has designed software compatible with PDAs, although to the authors best knowledge, no commercial PDAs have deployed the technique to date (Domain Dynamics, 2004). Although, as with NTT DoCoMo's handset with fingerprint sensor, this additional security mechanism does not provide any additional security beyond point-of-entry.

Similarly to mobile handsets, the use of any authentication approach on a PDA is optional, with a user having (where applicable) the choice of which technique to use, a PIN or a password. However, due to the lack of education and a perception that PDAs are not as susceptible to misuse and attack as normal desktop computers a large number of users do not utilise any technique. A survey has found one in four corporate respondents do not protect their device, with two out of three firms having no PDA guidelines on security (Kelly, 2002). Although this argument or approach may well have been appropriate with older PDAs with reduced functionality and importantly no wireless access technology, this is no longer true today. With PDA's able to access the internet and corporate networks

independently of their desktop computer through technologies such as Wi-Fi, corporate networks once thought to be secure are finding their networks open to attack due to the weaknesses PDAs introduce (Moore, 2001). Conversely, however, a recent survey of 230 business professionals found that 81% felt that the information on the PDA was either somewhat or extremely valuable and 70% were interested in having a security system for their PDA, with 69% willing to pay more for a PDA with security than one without (Shaw, 2004), clearly demonstrating a need for more secure authentication on PDAs.

An additional problem found with PDAs is that they tend to be used as a store for passwords that can be used for other computer systems, such as their office computer (Protocom, 2003). A typical reason for this is due to network administrators who are aware of the weaknesses of password based authentication mechanisms, requesting their employees to regularly change their password. Moreover, network administrators also place conditions on the selection of passwords, such as they must contain a mixture of upper, lower case characters and numbers, and exceed 8 characters, which places an extra burden upon the employee to remember their password (Federal Information Processing Standards, 1985). Some companies go as far as generating random passwords to be used by employees. To remember such passwords, employees have traditionally tended to write them down and place the post-it-note on the under side of the keyboard or under the mouse pad (Smith, 2002); however more recently PDAs are being used. However, as PDA's themselves quite frequently have no authentication security, the subsequent misuse of the PDA would provide the impostor not only with the information stored upon the PDA, but with the means of accessing a number of additional computing systems.

In all, PDAs in general suffer the same authentication weaknesses as their handset counterparts, but have the additional problem that misuse of the PDA does not only

compromise the data stored upon the device and the services which can subsequently be accessed by the device, but the PDA can also compromise corporate network security and act as a loophole for impostors to access what (perhaps) were secure networking infrastructures. The importance therefore to continually ensure user identity becomes even more paramount for corporate businesses.

2.3.3 Laptop Computer

The laptop computer, comparable to traditional desktop computing in terms of computational and storage capacity than other mobile devices, represents the largest of the mobile devices. The authentication mechanisms deployed on a laptop can therefore be quite diverse and mimic those deployed on standard PCs. This section focuses upon the traditional and widely adopted method of authentication. Unsurprisingly, this method has been password based. Although, as previously mentioned, network administrators and operating systems can be configured to accept passwords that are more difficult to hack and attack, the weakness of password based techniques on PCs and laptops has been well documented over the years. A noted book by Denning (1999), describes a number of techniques used to attack passwords, such as brute force attacks, packet sniffing, the use of malware (malicious software, i.e. Trojan horses) and social engineering, to name a few of the principal approaches.

These weaknesses of secret knowledge based techniques have been identified and addressed by a number of companies that have required high level security protection for their laptop. Typically, this protection has taken the form of either an integrated or add-on fingerprint sensor, such as Acer's Travelmate 740 (Lemon, 2001). The UK government has

Example	Number of Permutations	Average Attack Space
4-digit number based upon a date	512 (336 not rounded)	9 bits
Random 4 digit number	16,384 (10,000 not rounded)	14 bits
Random 10-letter English text	65,536	16 bits
Average Attack Space = $\log_2(m^n)$ Where m = number of random characters; n = number of digits		

Table 2.3: Average Attack Space of Secret-Knowledge Approaches

From Table 2.3 it can be seen how the Average Attack Space is significantly reduced from 14 bits to 9 bits when the password or PIN is not chosen randomly, reiterating the importance of choosing random passwords.

Although theoretically the foundations of secret knowledge approaches can be strong, they also have many weaknesses. These are typically based upon technological weaknesses and in appropriate use by the end-user. Taking a broader look at the deployment of secret knowledge approaches within a more mature computing environment such as desktop PCs, the password from a technical perspective has repeatedly been shown to be lacking, with applications developed to hack, capture and circumvent passwords. Although many of theses techniques have not currently be found on PDAs and mobile handsets, the increasing functionality and popularity of these devices will undoubtedly make them targets in the future. From a usability perspective, Kevin Mitnick, a leading figure in IT security and infamous former computer hacker has argued how the end-user is the weakest link in the security chain (Temple & Regnault, 2002). Using authentication techniques that rely on the user for their validity would therefore inherently make secret-knowledge based techniques insecure, as previous studies have highlighted (Protocom, 2003; Morris & Thompson, 1979).

In addition, Microsoft's Chief Architect and co-founder Bill Gates has recently been quoted as saying "passwords are dead" (Kotadia, 2004), citing numerous weaknesses and deficiencies that password based techniques experience. Unfortunately for mobile devices, the authentication technique Mr. Gates recommends is the deployment of token based authentication and/or one-time passwords. As previously explained within the context of a mobile handset, token based authentication was originally envisaged to be provided by the SIM card itself. However, due to the mobile nature of the device, both the device and the authentication token in its traditional from would tend to be left together removing any security the token may have provided. This does not however discount token-based approaches altogether. Through utilising proximity sensors it would be possible to develop tokens that could be worn, such as jewellery, but authenticate wirelessly without any physical connection. The range of the sensor can be carefully controlled to ensure neither the device or the person is too far away without locking the device.

Although this technique is feasible, and arguably increases user convenience over traditional approaches, as no interaction is required, the use of the token-based approach still requires the user to remember to wear the token, relying on the primary weakness of security, the user. A second potential weakness, depending on the form the token takes, is from theft. If a person is able to steal the mobile device they could also arguably have the opportunity of taking the token, allowing authentication free misuse. Finally, the cost of manufacturing and deploying this technique must be considered. Both software and hardware would need to be developed and deployed across a large number of mobile devices. In addition, mechanisms must also be present to replace lost and broken tokens, increasing the customer service cost of providing the mechanism.

2.4 A Survey of Subscriber Attitudes

The previous sections have described the authentication mechanisms deployed on mobile devices, giving technological arguments to their weaknesses. The introduction and success of any new product or technology, however, will rely heavily upon customer perceptions. If a customer perceives a product or service to be unreliable, even though it perhaps is not, then the product or service is likely to encounter poor adoption. Mobile devices and authentication are by no means an exception to this rule so a survey was commissioned to evaluate subscribers' attitudes and opinions towards security. Given the wider adoption of mobile handsets over other mobile devices, this survey was focussed directly at the users of mobile handsets in particular. The survey was designed to evaluate:

- current and future handset and service requirements,
- current and future attitudes towards authentication.

The survey ran for a period of two years, and a total of 297 respondents completed the online questionnaire. A copy of this questionnaire, along with the raw results can be found in appendix A.

2.4.1 Demography

The survey was distributed online with a single stipulation, the respondent had to be a current or past user of a mobile handset. Due to the natural distribution of the survey, amongst a majority of engineering and computing students, it was found a large proportion of respondents were male in the 17-24 age bracket. In all, 86% of the respondents are male

and 71% of the respondent's population fall into the 17-24 age bracket. Although this is likely to skew the results from an age dependent analysis, the magnitude of this variation is not as large as it might initially appear, as the 15-24 year age bracket has been shown to have the largest mobile phone penetration of all age groups, with an 86% penetration (Competitive Commission, 2003). In addition, a recent study performed by the international research group NOP, found there were no large differences in the willingness to spend more for mobile services between men and women (Cellular Online, 2004b).

An analysis of the respondents' service providers choice as illustrated in Table 2.4 shows a variation in overall market share in comparison to the actual UK figures, with 38% of the respondents connected to Orange compared to a national figure of 28%. Although the reasons why this percentage difference occurred are unknown, it can be argued that with a mobile handset population of 45 million in the UK (Competition Commission, 2003) operator variations will arise with such a small sample population such as this survey. The nature of this difference should not affect the results of the survey with respect to service and authentication as all network operators currently have very similar service offerings and an identical authentication mechanism.

Company	UK Market Share in 2001 (%)*	Network Share of Surveyed Users (%)
Orange	28	38
O_2	25	8
T-Mobile	23	22
Virgin	(included within T-Mobile)	2
Vodafone	25	25
Other	-	*5*

* Source: Competition Commission, 2003

Table 2.4: Network Operators Market Share

The mobile manufacturer Nokia has a 54% share of respondents handsets with the nearest competitor Motorola having 8%, followed by Samsung and Siemens, This is also reflected with global handset sales in Q3 of 2003 with Nokia, Motorola, Samsung and Siemens having 50%, 15%, 11% and 5% (Cellular Online, 2003). So customer preferences towards a particular brand of handset and features should be adequately reflected within the respondent population.

2.4.2 Handset Purchasing Considerations

With many key mobile markets becoming saturated, with over 70% of Europeans using a mobile (3G, 2003), mobile handset manufacturers and network operators are looking to generate revenue from current subscribers upgrading their existing handset to a newer and more advanced handset. It was decided to gauge the relative importance of numerous factors subscribers placed upon deciding which network operator and handset to purchase, looking in particular how security was viewed within this context.

Table 2.5 illustrates what factors customers take into account when considering which network operator to subscribe to. The most important factor is the price of the handset deal, which is not unsurprising as cost tends always to be a key deciding factor. Network coverage and reliability came next, which again are fundamental to the operation of the handset. Security features along with operator loyalty came last. This could be due to the fact that currently all network operators provide an identical mechanism for authentication of the user, so the subscriber has no means of differentiating between operators, or alternatively could be an indication that users do not feel security to be a particularly big issue.

Consideration	Rank (%)		
	Low	Medium	High
Choice of Handset	12	40	48
Network Coverage	2	27	71
Operator Loyalty	21	51	28
Prices, Deals etc	4	19	77
Reliability	3	28	70
Security Features	26	51	23

Table 2.5: Considerations when Choosing your Network Operator

However, when respondents where asked to rank the factors affecting their choice of mobile handset, security features came second to battery life suggesting customers are indeed security conscious, but perceive the issue to be a handset dependent rather than network operator one. Functionality such as personalising your handset through swappable features, games and accessories are low on the list of customer's priorities.

Consideration	Rank (%)		
	Low	Medium	High
Accessories	39	44	17
Battery Life	5	33	61
Brand Loyalty	32	42	26
Games	57	33	10
Infra-Red/Bluetooth	37	35	28
Security Features	27	50	23
Swappable Fascias	62	32	6

Table 2.6: Considerations when Choosing your Mobile Handset

2.4.3 Present & Future Mobile Handset Usage

The need for advanced authentication mechanisms has been argued to have come about due to the more advanced features and functionality of mobile devices, in addition to the relative weakness of secret knowledge based authentication approaches. However, the level of authentication security must be commensurate with the cost incurred with its misuse, otherwise the solution would be both costly and inconvenient. If subscribers only wish to use their handset for telephony, then the argument for more advanced

authentication mechanisms has been somewhat diminished. This section will analyse current and future handset usage in order to gauge from a customer perspective the need for security.

The need to be accessible via a mobile handset is apparent from how long respondents leave their handset switched on for. 85% of those questioned said they kept their handset on for more than 10 hours a day, with only 2% leaving the handset on for less than one hour. This tends towards a couple of implications:

- The need to leave the handset on comes in part from the need to stay in touch. So is the mobile handset the users' principal means of achieving this? Those switching on for less than one hour are likely to be users who only switch on when they wish to use the handset, thus either not wishing to be kept in contact with or they have another principal means of communication such as a landline telephone. Those users leaving their handset on for a long period of time are likely to consider their handset to be their major means of contact, illustrating both the reliance users place in their mobile and a long-term commitment to the technology.
- As a large proportion of respondents are leaving their handset on for long periods of the day, an issue of security arises particularly for those users with no standby PIN protection – this particular approach requests the user to enter the PIN in order to take the handset out of standby mode. However, this tends to be a very intrusive authentication approach, and this is reflected by many of the manufacturers not implementing this function. From the survey, 82% of respondents do not use any form of secondary PIN protection. This results in a significant number of handsets being unlocked and unprotected for long periods of the day, introducing the possibility of authentication free masquerade attacks.

2.4.4 Current Authentication Approaches

As previously discussed, the primary method of security for a mobile handset is the PIN. 66% of respondents reported to use PIN authentication at switch on, with 18% of users also utilising the secondary standby mode authentication. If this figure were to be extrapolated to the global population of mobile users, the 34% of users not using the PIN could currently represent some 438 million subscribers with no authentication security (Cellular News, 2004). Almost a third of respondents (30%) consider the PIN to be an inconvenient approach to security, with only 25% being confident or very confident in the protection it provided. It is worth noting however, that the largest proportion of respondents (42%) believed the PIN to provide an adequate level of security (which given the limited storage capacity and functionality of current handsets is understandable).

Identifying potential weaknesses of the PIN, it can be seen from Figure 2.7, that 45% of respondents have never changed their code. The reasons for this are likely to be a combination of users who have never used the PIN and those who have enabled the facility, but never changed the number from the default factory setting. In addition, a further 42% of respondents have only ever changed the PIN once, after initially purchasing the handset. Only 13% of respondents have ever changed their PIN number more than once.

The incorrect entry of the PIN three times results in the handset locking down and requires a PIN Unlock Code (PUK) to be obtained from the network operator. Whilst the handset is locked no access is given to the device, with the exception of emergency service calls. Over a third of respondents (38%) have had to unlock their phone using the PUK code at some point, a task which is both intrusive and time consuming. This highlights another undesirable effect of secret knowledge based approaches. It is not only inconvenient to the subscriber but an additional undesirable expense for the network operator having to provide the additional customer service support.

With mobile handset technology progressing and subscribers being given access to additional services, as already outlined in this chapter, it was encouraging that 85% of respondents were in favour of additional handset security. Only 2% thought it was a bad idea (the remaining were indifferent). An important distinction should be made between the need for improving security due to the advancements in services provided and the subsequent risks they pose and the need for improving security for current handsets. This result seems to suggest that respondents are aware of the need for security with respect to their current handsets, negating the technological arguments due to future advancements.

2.5 Conclusion

The growth and popularity of mobile devices and wireless networking technologies has increased the need to ensure the validity of the user. Information stored and accessed by these devices is no longer limited to names and numbers, but can hold a wide variety of personally and commercially sensitive information. This trend of increasing services and mobile computing is only set to continue, as users integrate technology within their lives

and unlock themselves from the desktop computer. However, research from the Gartner Group, suggests around 90% of mobile devices to date are lacking the security to prevent hackers from gaining access (Gold, 2004).

This chapter has discussed the relative merits of a secret knowledge based approach using PINs and found them some what lacking in the necessary authentication security required for mobile devices. These weaknesses were then subsequently reinforced through an end-user survey, which found that a large number of users are not using the PIN. Of those that did, many had infrequently (or never) changed the PIN code, and almost a third had experience handset theft or misuse in some form. Using a token authentication approach, where the token and device have to be physically connected, does not lend itself particularly well in this situation either. For example, many users will leave the token within the mobile handset for convenience, citing subscriber use of the SIM card, which was designed as a token. Token based approaches, similarly to secret knowledge based techniques, fundamentally rely on the user to remember something to ensure security, whether this is to remember the password or PIN, or to remember to pick up the token along with the handset. The third approach to authentication, "something the user is", known generally as biometrics, does not rely on the user to remember anything, just on being themselves.

On the basis of these findings, it is evident that alternative and stronger authentication approaches are required for mobile devices. These techniques must be capable of securing access to sensitive services and information throughout the duration of a session, in a user-friendly and convenient fashion. Possible foundations for such an approach are considered in the next chapter.

3 Biometric Authentication

Having established the need for advanced authentication mechanisms for mobile devices, this chapter presents and discusses the use of biometrics to solve this problem. The chapter begins by describing a generic biometric model and the factors that affect the system. An overview of biometric techniques is presented, focussing and exemplifying a number of approaches for their specific applicability within a mobile device.

3.1 Introduction

The use of biometrics, or specifically unique human characteristics, has existed for hundreds of years in one form or another, whether it is a physical description of a person or perhaps more recently a photograph. Consider for a moment what it is that actually allows you to recognise a friend in the street, or allows you to recognise a family member over the phone. Typically this would be their face and voice respectively, both of which are biometric characteristics. However, the definition of biometrics within the IT community is somewhat broader than just requiring a unique human characteristic(s) and describes the process as an automated method of determining or verifying the identity of a person (Nanavati et al., 2002).

The deployment and application of biometric systems, although currently small in comparison to password based approaches, is becoming more widespread. Some mobile devices introduced in chapter 2 included a fingerprint sensor for additional security. In addition, the CSI/FBI Computer Crime and Security Survey has shown an increase in biometric deployment from 8% to 11% over 2000-2004 (Richardson, 2003; Gordon et al., 2004), illustrating that the field of biometrics is beginning to become more mainstream.

3.2 A Generic Biometric System

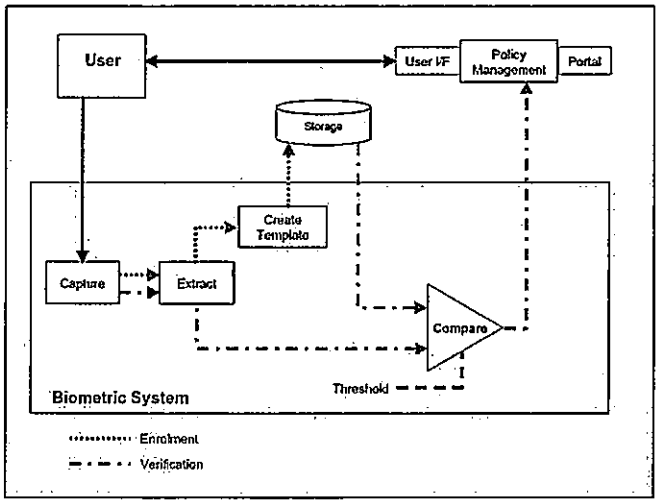
Many commercial biometric techniques exist, with new approaches continually being developed in research laboratories. The underlying process, however, remains identical. Biometric systems can be used in two distinct modes, dependent upon whether the system wishes to *determine* or *verify* the identity of a person.

- Verification – determining whether a person is who they claim to be.
- Identification – determining who the person is.

The particular choice of biometric will greatly depend upon which of these two methods is required, as performance, usability, privacy and cost will vary. Verification, from a classification perspective, is the simpler of the two methods, as it requires a one-to-one comparison between a recently captured sample and reference sample, known as a template, of the claimed person. Identification requires a sample to be compared against every reference sample, a one-to-many comparison, contained within a database, in order to find if a match exists. Therefore the unique characteristics used in discriminating people need to be more distinct or unique for identification than for verification. The majority of biometrics are not based upon completely unique characteristics. Instead a compromise exists between the level of security required and thus more discriminating characteristics and the complexity, intrusiveness and cost of the system to deploy. It is unlikely however, in the majority of situations that a choice would exist between which method to implement. Instead, different applications or scenarios tend to lend themselves to a particular method. For instance, PC login access is typically a verification task, as the user will select their username. However, when it comes to a scenario such as claiming benefits, an

identification system is necessary to ensure that the person has not previously claimed benefits under a pseudonym.

A generic biometric system is illustrated in Figure 3.1, showing both of the key processes involved in biometric systems: enrolment and authentication. Enrolment describes the process by which a user's biometric sample is initially taken and used to create a reference template for use in subsequent authentication. As such, it is imperative that the sample taken during enrolment is from the authorised user and not an impostor, and that the quality of the sample is good. The actual number of samples required to generate an enrolment template will vary according to the technique and the user. Typically, the enrolment stage will include a quality check to ensure the template is of sufficient quality to be used. In cases where it is not, the user is requested to re-enrol onto the system.



Source: CESG, 2004.

Figure 3.1: A Generic Biometric System

Authentication is the process that describes the comparison of an input sample against one or more reference samples – one in the context of a verification system, many with an identification system. The process begins with the capture of a biometric sample, often

from a specialised sensor. The biometric or discriminatory information is extracted from the sample, removing the erroneous data. The sample is then compared against the reference template. This comparison performs a correlation between the two samples and generates a measure or probability of similarity. The threshold level controls the decision as to whether the sample is valid or not, by determining the required level of correlation between the samples. This is an important consideration in the design of a biometric, as even with strong biometric techniques, a poorly selected threshold level can compromise the security provided. Finally, the decision is typically passed to a policy management system, which has control over a user's access privileges.

3.3 Authentication Approaches

Biometric approaches are typically subdivided into two categories, physiological and behavioural. Physiological biometrics are based upon classifying a person according to some physical attribute, such as their fingerprints, their face or hand. Conversely, behavioural biometrics utilise some unique behaviour of the person such as, their voice or the way in which they write their signature. It is often argued that many biometrics could fit into both categories, for instance, although fingerprints are physiological biometrics, the way in which a user presents a finger to the sensor, and the subsequent image that is captured, is dependent upon behaviour. However, it is common to select the category based upon the principal underlying discriminative characteristic – in this particular example the fingerprint itself.

The following section will briefly introduce a number of different biometric approaches that currently exist within both commercial and research arenas.

3.3.1 Physiological Biometrics

The majority of core biometric techniques commercially available are physiologically based and tend to have a more mature and proven technology. In addition, physiological biometrics typically have more discriminative and characteristic invariant features, and as such are often utilised in both verification and identification systems (Woodward et al., 2003).

- Ear Geometry

  This approach looks at the shape and the ridges of an ear to perform authentication. The uniqueness of the ear is currently untested, with various governments currently accepting and rejecting its admissibility within criminal courts (BBC News, 1999; Morgan, 1999). Although no commercial implementations of this technique currently exist, the robustness of the discriminating features suggests this is a technology with potential (Woodward et al., 2003).

- Facial Recognition

  Utilising the distinctive features of a face, facial recognition has found increasing popularity in both computer/access security and crowd surveillance applications, due in part to the increasing performance of the more recent algorithms and its transparent nature (i.e. authentication of the user can happen without their explicit interaction with a device or sensor). The actual features utilised tend to change between proprietary algorithms but include measurements that tend not to change over time, such as the distance between the eyes and nose, areas around cheekbones and the sides of the mouth (Nanavati et al., 2002). A number of commercial

products are currently on the market such as Imagis Technologies ID-2000 (2004) and Identix Face IT (2004), with newer products based upon three-dimensional facial recognition (Biovisec, 2004).

- Facial Thermogram

  A non-commercialised biometric, facial thermogram utilises an infra-red camera to capture the heat pattern of a face caused by the blood flow under the skin. The uniqueness is present through the vein and tissue structure of a user's face. However studies to date have not quantified its reliability within an identification system (Woodward et al., 2003). Recent studies have shown the external factors such as surrounding temperature play an important role in the performance of the recognition (Socolinsky & Selinger, 2004). This technique has significant potential as recognition can be provided transparently, night or day and if implemented within a facial recognition system (as a multi-modal biometric[2]) would improve overall authentication performance.

- Fingerprint Recognition

  The most popular biometric to date, fingerprint recognition, can utilise a number of approaches to classification including minutiae-based (irregularities within fingerprint ridges) and correlation-based to authenticate a person (Maltoni et al., 2003). The image capture process does require specialised hardware, based upon one of four core techniques: capacitive, optical, thermal and ultrasound, with each device producing an image of the fingerprint. Fingerprint recognition is a mature and proven technology with very solid and time invariant discriminative features

[2] The combination of two or more biometric samples or techniques to constructively improve system performance (Maltoni et al., 2003).

suitable for identification systems. Although the uniqueness of fingerprints is not in question, fingerprint systems do suffer from problems such as fingerprint placement, dirt and small cuts on the finger, and are inherently an intrusive authentication approach, as the user is required to physically interact with the sensor. To date fingerprint recognition has been deployed in a wide variety of scenarios from access security to computer security on laptops, mobile phones and PDA's.

- Hand Geometry

  The second most widely deployed biometric is hand geometry. The technique involves the use of a specialist scanner which takes a number of measurements such as length, width, thickness and surface area of the fingers and hand (Smith, 2002). Different proprietary systems take differing numbers of measurements but all the systems are loosely based on the same set of characteristics. Unfortunately, these characteristics do not tend to be unique enough for large-scale identification systems, but are often used for time and attendance systems (Ashbourn, 2000). The sensor and hardware required to capture the image tends to be relatively large (IR Recognition Systems, 2004) and arguably not suitable for many applications such as computer-based login.

- Iris Recognition

  The iris is the coloured tissue surrounding the pupil of the eye and is composed of intricate patterns with many furrows and ridges. The iris is an ideal biometric in terms of both its uniqueness and stability (variation with time), with extremely fast and accurate results (Daugman, 1998). Traditionally systems required a very short focal length for capturing the image (e.g. physical access systems), increasing the

intrusiveness of the approach. However, newer desktop based systems for logical access are acquiring images at distances up to 18 inches (Nanavati et al., 2003). Cameras are still however sensitive to eye alignment causing inconvenience to users.

- Retina Scanning

  Retina scanning utilises the distinctive characteristics of the retina and can be deployed in both identification and verification modes. An infra-red camera is used to take a picture of the retina highlighting the unique pattern of veins at the back of the eye. Similarly to iris recognition, this technique suffers from the problems of user inconvenience, intrusiveness and limited application as the person is required to carefully present their eyes to the camera at very close proximity. As such, the technique tends to be most often deployed within physical access solutions with very high security requirements (Nanavati et al., 2002).

Additional physiological biometrics have been proposed such as odour, vein and fingernail bed recognition, with the research continuing to identify body parts and other areas with possible biometric applications (Woodward et al., 2003).

3.3.2 Behavioural Biometrics

Behavioural biometrics classify a person on some unique behaviour. However, as behaviours tend to change over time due for instance, to environmental, societal and health variations, the discriminating characteristics used in recognition also change. This is not necessarily a major issue if the behavioural biometric has built-in countermeasures that

constantly monitor the reference template and new samples to ensure its continued validity over time without compromising the security of the technique. In general, behavioural biometrics tend to be more transparent and user convenient than their physiological counterparts, however, at the expense of a lower authentication performance.

- Keystroke Analysis

  The way in which a person types on a keyboard has been shown to demonstrate some unique properties (Spillane, 1975). The process of authenticating a person from their typing characteristic is known as Keystroke Analysis (or Dynamics). The particular characteristics used to differentiate between people can vary, but often includes the time between successive keystrokes, also known as the inter-key latency and the hold time of a key press. The unique factors of keystroke analysis are not discriminative enough for use within an identification system, but can be used within a verification system. Authentication itself can be performed in both *static* (text dependent) and *dynamic* (text independent) modes. However, although much research has been undertaken in this field due to its potential use for computer security, only one commercial product to date has been deployed and is based on the former (and simpler) method of static verification. BioPassword (2004) performs authentication based upon a person's username and password. A major downside to keystroke analysis is the time and effort required to generate the reference template. As a person's typing characteristics are more variable than say a fingerprint, the number of samples required to create the template is greater, requiring the user to repetitively enter a username and password until a satisfactory quality level is obtained.

- Service Utilisation Profiling

  Service Utilisation describes the process of authenticating a person based upon their specific interactions with applications and or services (Furnell et al., 2001). For instance, within a PC, service utilisation would determine the authenticity of the person dependent upon which applications they used, when and for how long, in addition to also utilising other factors. Although the variance experienced within a user's reference template could be far larger than with other biometrics, it is suggested that sufficient discriminative traits exist within our day to day interactions to authenticate a person. Although not unique and distinct enough to be used within an identification system, this technique is non-intrusive and can be used to continuously monitor the identity of users whilst they work on their computer system. However, this very advantage also has a disadvantage with regard to users' privacy, as their actions will be continually monitored, and such information has the potential to be misused (e.g. the capturing of passwords). Although no authentication mechanisms exist utilising this technique, a number of companies are utilising service utilisation as a means of fraud protection (Graham-Rowe, 2001; Rogers, 2001).

- Signature Recognition

  As the name implies, signature recognition systems attempt to authenticate a person based upon their signature. Although signatures have been used for decades as a means of verifying the identity of a person on paper, their use as a biometric is more recent (Woodward et al., 2003). Authentication of the signature can be performed statically or/and dynamically. Static authentication involves utilising the actual features of a signature, whereas dynamic authentication also uses information regarding how the signature was produced, such as the speed and

pressure. Numerous commercial applications exist, including for use within computer access and point-of-sale verification (PDALok, 2004b; CIC, 2004). However, due to the behavioural aspect of the technique and the variability between signatures, it is not recommended for use within an identification system.

- Voice Verification (or Speaker Recognition)

  A natural biometric, and arguably the strongest behavioural option, voice verification utilises many physical aspects of the month, nose, and throat, but is considered a behavioural biometric as the pronunciation and manner of speech is inherently behavioural (Woodward et al., 2003). Although similar, it is important not to confuse voice verification with voice recognition, as both systems perform a distinctly different task. Voice recognition is the process of recognising *what* a persons says, whereas voice verification is recognising *who* is saying it. Voice verification, similarly to keystroke analysis, can be performed in static (text dependent) and dynamic modes (text independent), again with the former being a simpler task than the latter. Numerous companies exist providing various applications and systems that utilise voice verification, for instance Nuance (2004) provide static authentication for call centres, and Anovea (2004a) who provide static authentication for logical access solutions. To the author's best knowledge no true commercial dynamic-based approaches exist, based upon anything a user might say. Pseudo-dynamic approaches do exist, which request the user to say a random two numbers which have not been particularly trained for during enrolment (VeriVoice, 2004). But as the user is told what two numbers to repeat, the technique cannot be truly dynamic.

The list of biometrics provided should not be considered exhaustive as new techniques and measurable characteristics are constantly being identified. It does, however, outline the main biometric approaches to date with an insight into the newer techniques. For further updates on new biometric techniques refer to the International Biometrics Group (2004) and Biometrics Catalogue (2004).

3.4 Factors Affecting a Biometric System

As previously explained, all biometrics work on the basis of comparing a biometric sample against a known template, which is securely acquired from the user when they are initially enrolled on the system. However, this template matching process gives rise to a characteristic performance plot between the two main errors governing biometrics: the False Acceptance Rate (FAR), or rate at which an impostor is accepted by the system, and the False Rejection Rate (FRR), or rate at which the authorised user is rejected from the system. The error rates share a mutually exclusive relationship – as one error rate decreases, the other tends to increase, giving rise to a situation where neither of the error rates are typically both at zero percent (Cope, 1990). Figure 3.2 illustrates an example of this relationship. This mutually exclusive relationship translates into a trade off for the system designer between high security and low user convenience (tight threshold setting) or low security and high user convenience (slack threshold setting). Typically, a threshold setting that meets the joint requirements of security and user convenience is usually set. A third error rate, the Equal Error Rate (EER), equates to the point at which the FAR and FRR meet and is typically used as a means of comparing the performance of different biometric techniques. These performance rates when presented are the averaged results across a test population, therefore presenting the typical performance a user might expect

to achieve[3]. Individual performances will tend to fluctuate dependent upon the uniqueness of the particular sample.

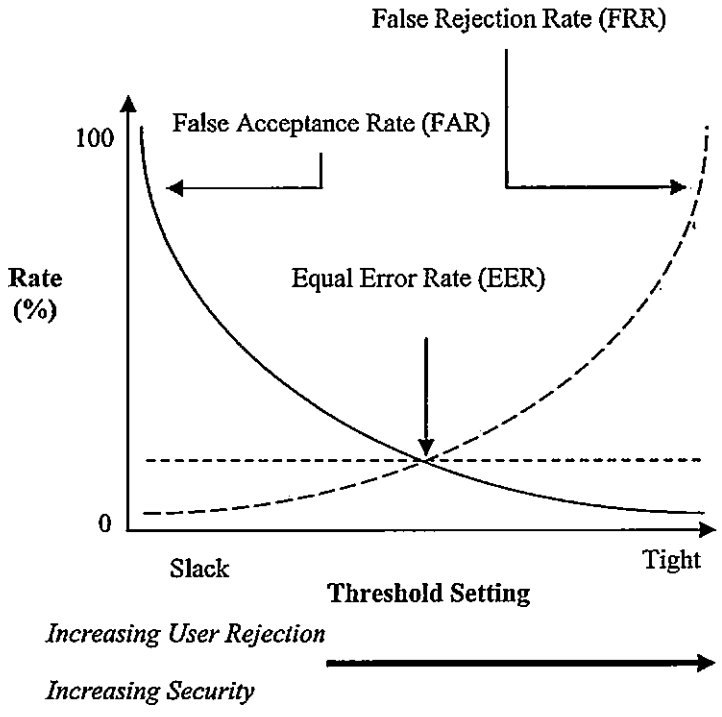


Figure 3.2: Mutually Exclusive Relationship between the FA & FR Rate

The actual performance of different biometric techniques varies considerably with the uniqueness and sophistication of the pattern classification engine. In addition, published performances from companies often portray a better performance than typically achieved given the tightly controlled conditions in which they perform their test. The National Physical Laboratory (2001) on behalf of the Communications Electronics Security Group (CESG) conducted an independent evaluation of a number of biometric systems, giving a more realistic perspective upon the performance that can be achieved. The results from this study are illustrated in Table 3.1.

[3] The performance rates presented in this thesis will be the averaged performance for the complete system, unless otherwise indicated by superscript "i" for individual.

Biometric Technique	EER (%)	Company
Hand Geometry	1.5	Recognition Systems HandKey II
Facial Recognition*	2.5	Identix FaceIT
Voice Verification	3.5	OTG SecurPBX
Fingerprint (chip)*	4.5	Infineon VeriTouch
Fingerprint (chip)*	6	Infineon VeriTouch
Facial Recognition*	7	Identix FaceIT
Fingerprint (optical)	9	*Company name not disclosed*
Vein	9	Neusciences Biometrics Veincheck Prototype

*Alternative enrolment and verification algorithms were provided

Table 3.1 A Comparison of Biometric Performance Rates

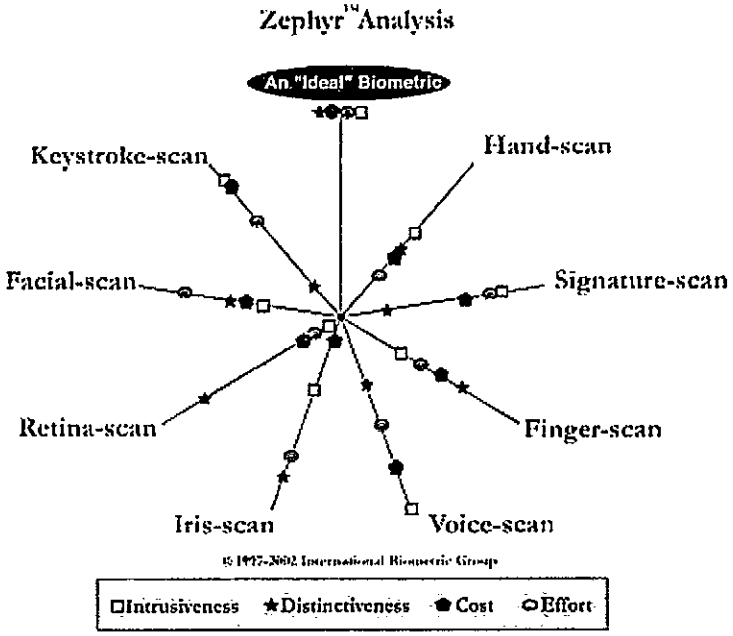
However, it is important to realise no single biometric exists that would satisfactorily suit every application, because although security is a key factor in any decision, other considerations play an intrinsic role in the choice of biometric for any given authentication application. As such it is difficult to quantify what level of performance is needed for successful deployment. It can be noted however, all the biometric systems illustrated in Table 3.1, with the exception of the VeinCheck Prototype, are commercially available[4].

The International Biometric Group (IBG) considers four factors to be important in the choice of biometric, shown in Table 3.2 and has produced a Zephyr diagram to plot these factors for a number of key biometrics, as illustrated in Figure 3.3.

User Criteria	Technology Criteria
Effort – How much time and effort is required on the part of the user.	Cost – Cost of hardware capture device
Intrusiveness – How intrusive the users perceives the system to be	Distinctiveness – How well the system identifies individuals

Table 3.2: Factors Affecting the Choice of Biometric

[4] Subsequent performance comparisons within this thesis will therefore be made against these figures.



Source: International Biometric Group, 2004.

Figure 3.3: Zephyr Analysis of Biometrics

The Zephyr diagram illustrates the comparative strengths and weaknesses of a number of biometrics, ranked from (outside) better to (inside) worse using the four major factors. Taking an example from the figure, some techniques perform better in some areas than in others, for instance, keystroke analysis performs relatively well with both cost and intrusiveness factors, principally because the solution requires no additional hardware (the keyboard is usually already present) and thus is a software only solution and authentication is achieved by monitoring natural typing patterns. The effort required for keystroke analysis is relatively small, although successful systems to date do require the user to type in a specific keyword such as a username and/or password rather than dynamically authenticating the user by a previously unknown character string. The major disadvantage with keystroke analysis systems to date is their accuracy, with fairly substantial false acceptance and false rejection rates.

open the potential for voice verification, and the keypad would allow a keystroke analysis technique to be applied. For handsets or PDAs without a keypad, a touch sensitive screen is usually provided as the human-computer interface, where signature recognition could subsequently be utilised.

The use of biometrics on mobile devices can be supported by further results from the survey introduced in chapter 2. In all, 83% of respondents thought biometric authentication to be a good idea. Asking respondents which authentication techniques they are aware of and would use resulted in some both predictable and surprising outcomes, as illustrated in Figure 3.5. Predictable were the favoured biometrics of fingerprint and voiceprint recognition, which were also most known about through the respondent population. 99% of the respondents aware of fingerprinting were also happy to use the technique on a mobile handset. Surprising results were iris scanning, a technique often felt to be quite intrusive, being more popular and more familiar to those questioned than the less intrusive facial recognition technique. In absolute terms, keystroke analysis proved least favourable. However, as a percentage of respondents aware of the technique and who were willing to use the approach, facial recognition was least popular. An analysis of the results shows that the popularity of a biometric is intrinsically linked to the awareness of the approach – as a user is unlikely to use a technique about which they have no knowledge. With the exception of facial recognition, all of the techniques achieved over 60% of respondents who have knowledge of the technique would also use it. It could therefore be hypothesised that a user's willingness to adopt a particular technique is high and could well be increased through a degree of education.

device is challenged. For all biometric techniques this information, known as a profile or template, will be person dependent and represent that person's unique biometric. The final objective of the survey was to establish where respondents would prefer this biometric signature to be stored, i.e. on the handset or within the network. There are relative advantages and disadvantages of both approaches, such as storing the template within the network would remove the majority of computer processing away from the handset improving memory and battery life. It would also permit a greater degree of personal mobility, as users would be able to use any handset and have their usage billed to their own personal account. Conversely, information on the handset will remove any network traffic caused by the authentication requests, and remove the need for any personal information to leave the mobile device. The respondents were in favour of a handset centric model with 50% of the vote, with 34% in favour of a network centric model (the remainder were indifferent). This is not an unusual result, in that respondents would tend to be thinking of factors affecting them personally, such as the loss of their biometric signature, rather than factors such as increasing personal mobility and network traffic, and as such would consider having personal control over their biometric profile to be the safest option.

From a subscriber's perspective, it can be suggested that the use of biometric techniques would be an acceptable method of authentication, with a majority of users willing to utilise this authentication in a continuous and transparent manner. However, when considering which biometrics to implement within a mobile device, one must consider all the factors; of cost, accuracy, intrusiveness and effort, in addition to user preference. Table 3.3 illustrates how these key factors vary for different biometric techniques with a specific focus on their applicability within a mobile device. Given the already high cost of hardware, the cost factor has been converted into whether a device would already normally or potentially contain the hardware required to capture the biometric sample – based upon

products currently on the market. Information on whether the hardware used to capture the biometric sample is reusable is also included. Hardware that can be utilised for a multitude of applications is arguably a far better use of resources and is more likely to be included within the device on a wider scale. A (subjective) accuracy category has been assigned to each of the biometrics. Given techniques with no empirical data on performance, a performance indication is included based upon the potential uniqueness of the technique. Also, each of the techniques have been assigned to either an intrusive or non-intrusive category. This factor is slightly different to the definition applied in the previous section and describes the practical intrusiveness and subsequent effort required in using the biometric. A non-intrusive label is assigned to a technique which has at least the potential to be implemented within a mobile device where the capture and subsequent authentication of the user can be performed without the knowledge of it occurring, for example, the use of facial recognition whilst the user is in a video conference. This would remove any effort required by the user to authenticate themself. It does not consider how intrusive the technique is perceived to be by the user. Conversely, an intrusive technique is one where a user is explicitly asked or required to present a sample.

Biometric Technique	Mobile Handset Hardware	PDA Hardware	Laptop Hardware	Hardware Reusable	Accuracy	Intrusive/ Non-Intrusive
Ear Recognition	Maybe	No	No	No	Very Good*1	Non-Intrusive
Facial Recognition	Yes	Maybe	No	Yes	Very Good	Non-Intrusive
Facial Thermogram	No	No	No	No	Good*1	Non-Intrusive
Fingerprint Recognition	Maybe	Maybe	Maybe	No	Excellent	Intrusive
Iris Recognition	Maybe	Maybe	No	No	Excellent	Intrusive
Keystroke Analysis	Yes	Yes	Yes	Yes	Good	Non-Intrusive
Retina Scanning	No	No	No	No	Excellent	Intrusive
Service Utilisation	Yes	Yes	Yes	Yes	Okay*1	Non-Intrusive
Signature Recognition	No	Yes	No	Yes	Good	Non-Intrusive
Voice Verification	Yes	Yes	Yes	Yes	Very Good	Non-Intrusive

*1 *Accuracy (Subjective)*

Table 3.3: Compatible Biometric Techniques for Mobile Devices

Given the apparent disparity identified in chapter 2, between users wanting more authentication security, but not currently using what is available, and the relatively high inconvenience factor experienced by users, the use of transparent authentication using biometrics would solve both the technological requirement for a more secure authentication mechanism and the user's need to remove any inconvenience from the authentication process. Unfortunately, biometric approaches with excellent accuracy are also the intrusive techniques. A compromise between the level of security provided by a technique and the inconvenience to the user is required. This pattern can be seen to continue, with techniques such as service utilisation and keystroke analysis having very good non-intrusive potential but with lower accuracy rates. However, a number of techniques can be identified as appropriate for deployment on mobile devices in general:

- Facial Recognition,
- Keystroke Analysis,

- Signature Recognition,
- Speaker Recognition and
- Service Utilisation.

This selection is based upon the hardware available on mobile devices and the possible non-intrusiveness of its application. It does not take into account other factors, such as the computational and storage requirements of the techniques. The reason for this is two-fold. Mobile devices are increasing in their computing power and storage capacity on an almost yearly basis, with devices of today already being comparable to basic desktop computers of three or four years ago. Therefore, in all likelihood, mobile devices of the future will not have problems processing the data required for enrolment and authentication. In the short-term, the widespread use of wireless networking technologies would permit the use of a client-server topology for authentication – where the server is given responsibility for the computationally intensive tasks and storage of biometric templates.

Further analysis illustrates their potential for use within mobile devices under different circumstances. As previously described, facial recognition can be used on mobile handsets, however, with the proviso of a front-facing camera, PDAs and laptop computers could also utilise this technique. Keystroke Analysis could be deployed on all three categories of device to perform transparent authentication whilst the user is entering text messages, scheduling a meeting, or typing a document. Signature recognition could be used as a user is entering words using the transcriber function of PDA or the notepad function of a tablet PC. Speaker recognition has the potential to be deployed on all three devices with the presence of a microphone. However, its greatest application would be in telephony, where dynamic authentication of the user can take place during a normal telephone call. Service

utilisation also has the potential to monitor behavioural patterns on all three categories of device, flagging possible misuse when the user deviates from their typical routine.

In practice however, many of these techniques do not currently have the functionality to be deployed in this manner. In fact, only facial recognition could be used *"as-is"*, with all the remaining techniques requiring varying degrees of modification or development. Keystroke analysis, although commercially available for static-based authentication on PC keyboards, currently has no dynamic-based approach – although this technique has been thoroughly researched (Leggett, 1991; Napier et al., 1995). Of more concern is the applicability of keystroke analysis on a mobile handset or PDA, where the keypad or thumb sized keyboard represents a different tactile environment with which the user must interact. The feasibility of authenticating a user based upon a keypad is currently undocumented. Signature recognition has been developed commercially to provide intrusive authentication of the user based upon a signature, but not on general words signed through transcriber. Speaker verification has also been developed for static (and pseudo-dynamic) authentication, but does not currently perform dynamic authentication of the user. Finally, although service utilisation techniques have been applied within fraud detection scenarios, their use as a real-time authentication technique is also unproven. It is clear therefore, that the majority of techniques require at least adaptation, if not a complete feasibility study before practical implementation of the technique can occur.

Of all the applicable techniques, keystroke analysis represents the most favourable technique due to the transparent nature of authentication and its possible deployment across all three categories of mobile device (with the proviso of a keypad or keyboard being present). This next section presents a brief overview of the research performed in keystroke analysis.

3.6 Literature Study of Keystroke Analysis

A number of studies have been performed in the area of keystroke analysis since its conception in 1975 (Spillane, 1975). Although the studies tend to vary in approach from what keystroke information they utilise to the pattern classification techniques they employ, all have attempted to solve the problem of providing a robust and inexpensive authentication mechanism. Table 3.4 illustrates a summary of the main research studies performed to date. All, with the exception of Ord and Furnell (2000), were based upon classifying users on full keyboards, with Ord and Furnell utilising only the numerical part of the keyboard.

Study	Static/ Dynamic	Keystroke Metrics		Classification Technique	# of Participants	FAR (%)	FRR (%)
		Inter-Key	Hold-Time				
Joyce & Gupta 1990	Static	✓		Statistical	33	0.3	16.4
Leggett et al. 1991	Dynamic	✓		Statistical	36	12.8	11.1
Brown & Rogers 1993	Static	✓	✓	Neural Network	25	0	12.0
Napier et al 1995	Dynamic	✓	✓	Statistical	24	3.8% (combined)	
Obaidat & Macchairolo 1997	Static	✓	✓	Statistical	15	0.7	1.9
				Neural Network		0	0
Monrose & Rubin 1999	Static	✓		Statistical	63	7.9 (combined)	
Cho et al. 2000	Static	✓	✓	Neural Network	25	0	1
Ord & Furnell 2000	Static	✓		Neural Network	14	9.9	30

Table 3.4: Summary of Keystroke Analysis Studies

At first glance, it would appear both of the dynamic based studies have performed well against static based approaches, given the more difficult task of classification, however, these results were obtained with users having to type up to a hundred characters before successful authentication. Its applicability to a mobile device in this instance is therefore limited. However, all of the studies have illustrated the potential of the technique, with Obaidat and Macchairolo (1997) performing the best with a FAR and FRR of 0% using a neural network classification algorithm. In general, neural network based algorithms can be seen to outperform the more traditional statistical methods, and have become more popular in later studies. Notably, the original idea of keystroke analysis proposed that a

person's typing rhythm is distinctive and all the original studies focussed upon the keystroke latency (the time between two successive keystrokes); however, more recent studies have identified the hold time (the time between pressing and releasing a single key) as being as discriminative. The most successful networks implemented a combination of both inter key and hold time measures, illustrating that the use of both measures has a cumulative and constructive effect upon performance.

It is very difficult to directly compare and contrast many of these studies in terms of their verification system and performance, as their method for evaluating (and calculating) the error rates differ depending upon the aim of the study. For example, while some were static-based verifiers, others were dynamic-based with varying character lengths. For a detailed description and analysis of these studies refer to Appendix B.

A point identified in a number of studies is the failure of keystroke analysis to perform successfully for a minority cross section of users. These users tend to have high inter-sample variances and have few distinctive typing rhythms. As such, any authentication system that implements a keystroke analysis technique would also have to consider the small number of users that will exhibit too high an error rate in order to ensure both the security and user convenience factors required by the overall system are met.

3.7 Conclusion

Given the three categories of authentication, authenticating a person based upon their unique characteristics represents the only plausible approach that results in improving the level of security provided, without further increasing any user inconvenience. It has been identified that, through the intelligent application of biometric techniques, authentication of the user can (in theory) take place transparently enabling them to be authenticated numerous times without inconvenience, as samples are captured during a users normal interaction with the device.

The principal weakness surrounding biometrics is the accuracy of the approaches, with techniques varying in strength from very strong techniques, such as retina scanning, to weak options, such as service utilisation. However, no matter how strong a technique is, the effectiveness of discriminating between users is determined by the threshold level. A poorly selected threshold level in retina scanning could degrade its performance below a well selected threshold level in service utilisation. It is imperative therefore to ensure threshold levels are chosen correctly for individual techniques and possibly even on a per user basis.

The survey has clearly demonstrated users' willingness to adopt biometric authentication and a number of biometric approaches have been identified for use within one or more types of mobile device. Facial recognition in particular has been shown to be useful, with little or no modification required to the technique. The remaining biometrics identified require some level of development. Other particularly useful biometrics include speaker verification, keystroke analysis and signature recognition. Both speaker verification and

signature recognition have some level of development continuing with respect to their application within mobile devices. However, the use of keystroke analysis on a keypad represents an intriguing proposal given that keypads are present on the majority of handsets, and because it also represents the simplest and most transparent authentication technique – as users can be authenticated as they enter general data on the keypad. As such, the next two chapters proceed to give some further focus to the feasibility of the technique within a mobile handset.

4 Verification of Identity through Numeric Input Data

The previous chapter discussed biometrics in general, with subsequent focus upon techniques that lend themselves to a mobile device. The inexpensive and transparent nature of keystroke analysis makes the technique an ideal authentication mechanism. However, the viability of the approach, due to the differing tactile qualities of keypads, has not been documented to date. This chapter presents a study into authenticating users based upon numerical entry utilising the inter-keystroke latency. The chapter compares and contrasts a number of statistical and neural network based pattern classification techniques in order to evaluate overall system performance.

4.1 Introduction

Given the large number of mobile handsets that have keypads and indeed a growing number of PDAs with thumb size keyboards (such as Palm Tungsten W/C and Sharp Zaurus) – more similar to keypads than to full-size keyboards in practicality, keystroke analysis has the potential to enable authentication of users in a cost effective and efficient manner. If authentication of users were possible during their normal interaction with the handset (such as entering telephone numbers) then authentication could be performed non-intrusively and potentially continuously throughout the duration of usage.

In order to provide a robust evaluation of keystroke analysis on a mobile handset, both keystroke characteristics introduced in section 3.6 were tested across two typical handset interactions:

- Authentication of users based upon their entry of telephone numbers, using the inter-keystroke latency metric,
- Authentication of users based upon typing text messages, using the hold time of the most recurrent characters.

These characteristics were chosen due to the degree of discriminatory information they bring to the pattern classification problem. Previous studies had identified their potential (see Appendix B), whereas it is anticipated that other measurable characteristics such as, the mean typing speed and mean error rate would not offer the same capability. The inter-keystroke latency represents the traditional approach to keystroke analysis and performs classification on the time between key presses. The hold-time is the time taken to press and

release a key for a particular character. This chapter will focus upon the first of these two handset interactions with the following chapter detailing the second.

4.2 Data Collection

The purpose of this investigation is to determine the feasibility of identifying a user by the way in which they enter numbers on a mobile handset keypad. To this end, three input scenarios were developed to encompass the different input scenarios a user might experience.

1. Entry of a fixed four-digit number, analogous to the PINs used on many current mobile handsets.
2. Entry of a fixed eleven-digit number, analogous to the telephone numbers that you would enter on a handset.
3. Entry of a varying eleven-digit number, again analogous to the telephone numbers that you would enter on a handset.

The first and second input scenarios represent *static* keystroke analysis, in that they attempt to authenticate a person from the way in which they enter a specific number. However, in the telephone number scenario it would be unlikely the user would repeatedly enter an identical number – as the more common numbers would be stored in the phonebook, so the classifier would have to be able to classify users on unknown telephone numbers. This type of authentication is known as *dynamic* authentication, and forms the basis for the third input scenario. From the three scenarios several objectives can be achieved. The four-digit input will firstly help determine how successful a small input vector can be in classification

as compared to the longer 11-digit, and secondly whether the PIN code currently used on mobile handsets could be hardened with a keystroke analysis biometric producing a two-factor authentication technique (Monrose et al., 1999). The varying 11-digit input will indicate how well a keystroke analysis technique works based upon real input data, using the static 11-digit input as a basis for comparison – the 11-digit static input will represent the upper performance boundary for inputting numerical telephone numbers, as static authentication approaches have performed significantly better than their dynamic counterparts (Umphress & Williams, 1985; Joyce & Gupta, 1990).

A total of thirty two test subjects were asked to enter the data for the three input scenarios. The number of input samples chosen for each study, thirty samples for the first and second input scenarios and fifty for the third, was based upon the requirement to keep the number of samples to a minimum. In a practical system it would not be plausible for the user to input an excessive number of samples before authentication could subsequently take place. The actual number were based on a successful study by Ord and Furnell (2000), with the sample size of the varying 11-digit input scenario increased to allow for the larger variations in input characteristic, as would be expected by a dynamic authentication approach. The break-down of the input data is illustrated in Figure 4.1. Two thirds of the dataset was utilised in the generation of the reference template or profile, with the remaining third used as validation samples. The pattern classification tests were performed with one user acting as the valid authorised user, whilst all the other users were acting as impostors.

From the literature survey a number of pattern classification techniques were introduced that performed well in studies. These algorithms broadly fall into two categories:

- Statistically based, and
- Neural Network based.

As such, a number of algorithms from both categories were applied in order to determine the most optimal level of system performance. Figure 4.4 illustrates an overview of keystroke analysis system. For detailed information on what these algorithms are and how they were deployed refer to the background information in Appendix C. In addition specific page references to the appendix are made as and where necessary throughout this section.

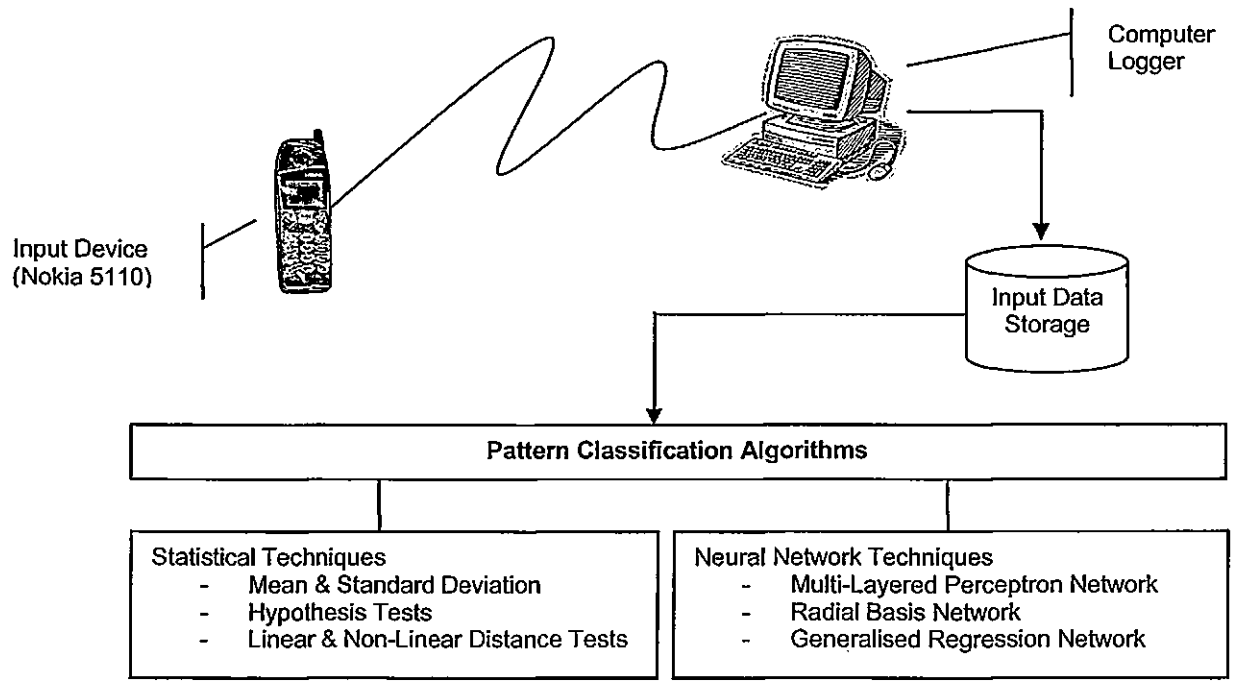


Figure 4.4: Keystroke Analysis System Overview

In order to investigate the classifiers, a number of program scripts were generated to perform various tasks, such as manipulation of the input data, generation of neural networks and the subsequent evaluation of the performance. Several of these function scripts were utilised in each of the classification algorithms and form the following common components:

- Data Extraction Function – Extracts user's data from a number of text files, providing error checking and returns the input data for each of the thirty two users.

- Outlier Removal Function – Removes outliers from the input data based upon 'individual users' mean and standard deviation. An outlier being defined as an input whose value lies outside three standard deviations of a users mean. The figure of three standard deviations is based upon a Gaussian or Normal distribution where 99% of a user's samples should theoretically reside within three standard deviations of the user's mean.

- Dataset Split Function – Splits the data into the required training and validation datasets based upon approximately 2/3 of the data contributing towards the training dataset and 1/3 towards the validation dataset, evenly extracted throughout the complete dataset.

The parent-child function scripts utilised in the statistical recognition techniques are illustrated in Figure 4.5 with each of the parent scripts calling the child scripts in order from right to left. The application and evaluation of each statistical technique is performed by the respective parent script.

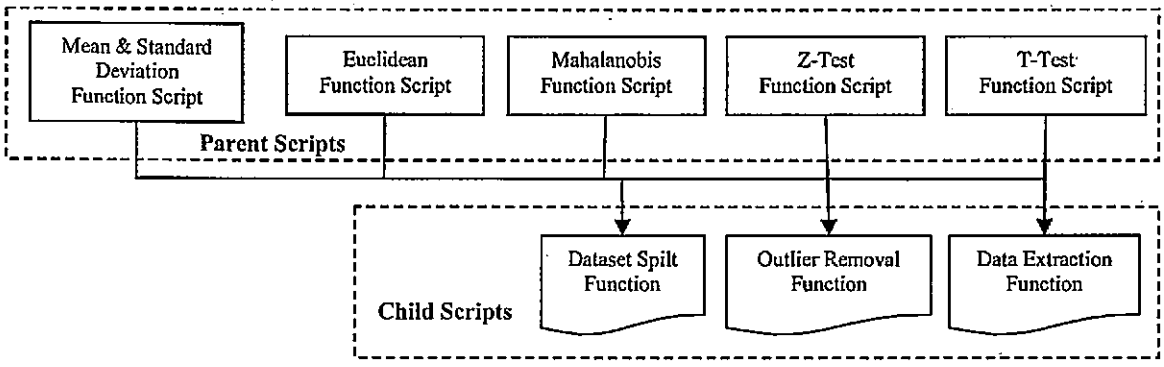


Figure 4.5: Statistical Recognition Program Function Tree

Similarly, Figure 4.6 illustrates the neural network series of parent and child function scripts. The neural network series of scripts includes two further child scripts, a network script (of which there are two versions, one for each parent script, which create and train the neural networks) and an evaluating script which completes the error rate calculations and generates the overall system performance. Each of the neural network control scripts define the network parameters and performs the iterative tests required to optimise network configurations.

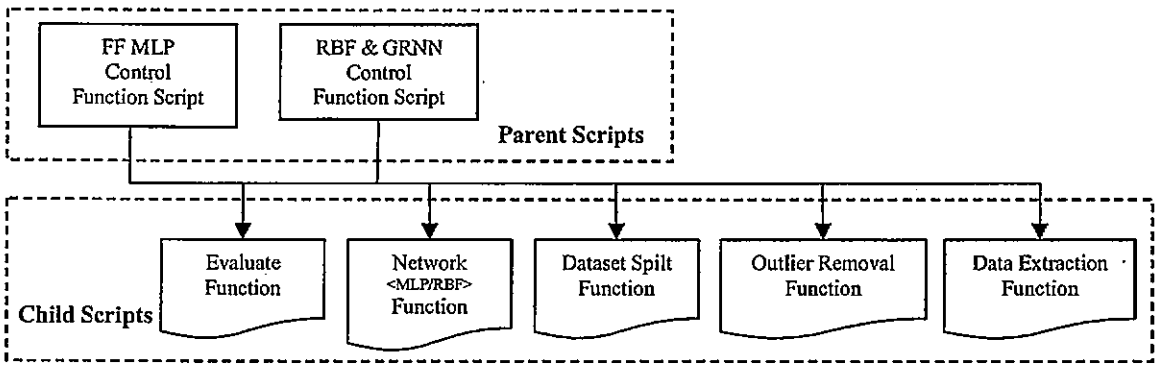


Figure 4.6: Neural Network Program Function Tree

A copy of all these scripts can be found within Appendix D, along with detailed descriptions of their operation.

4.4 Results

The results from the classification of numeric input vectors are divided into the classification algorithms. However, the first section describes (from a descriptive statistics perspective) the difficulties any classification algorithm will encounter with the input data.

Many of the classification algorithms (in particular the neural network based approaches) have performed many iterations, changing the various network parameters in order to optimise the performance of the classifier. Over 1200 tests have been completed in total. With such a large number of tests, the results section focuses in detail upon the most successful algorithm configurations, detailing where applicable the differences in performance with respect to particular algorithm parameters. A complete set of results with all combinations can be found within appendix D.

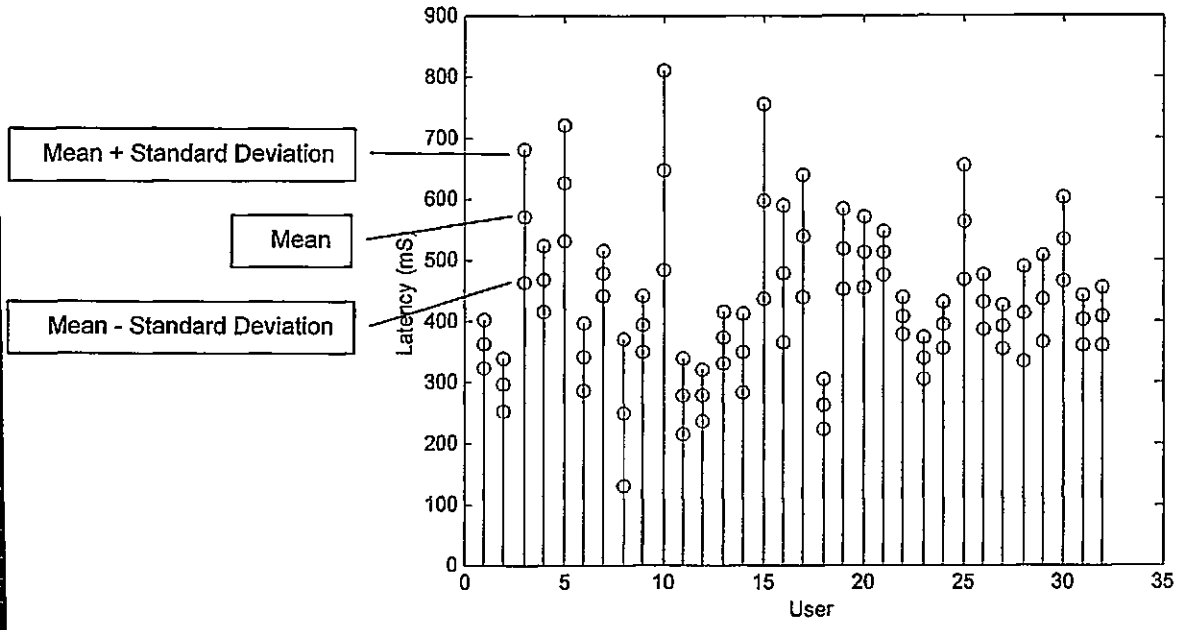
4.4.1 Descriptive Statistics

Analysis of the input data permits an insight into the complexities of successfully discriminating between the users. The problem is that latency vectors observed from a single user may incorporate a fairly large spread of values. This spread, otherwise known as variance, is likely to encompass input vectors that closely match other users. Because user's latency vectors do not exist on clearly definable discriminative regions, the problem is made much more complex for the classification algorithms.

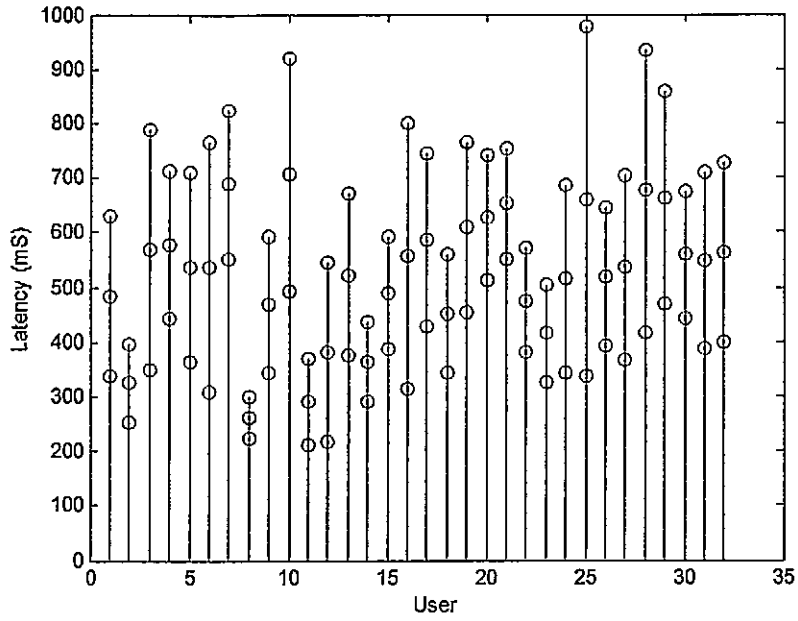
Two types of variance can be extracted from the latency data:

- Inter-sample variance, which ideally would be zero, so that every sample a user inputs would be identical and therefore easier to classify.
- Inter-user variance, a measure of the spread of the input samples between users, which would be ideally as large as possible in order to widen the boundaries between users.

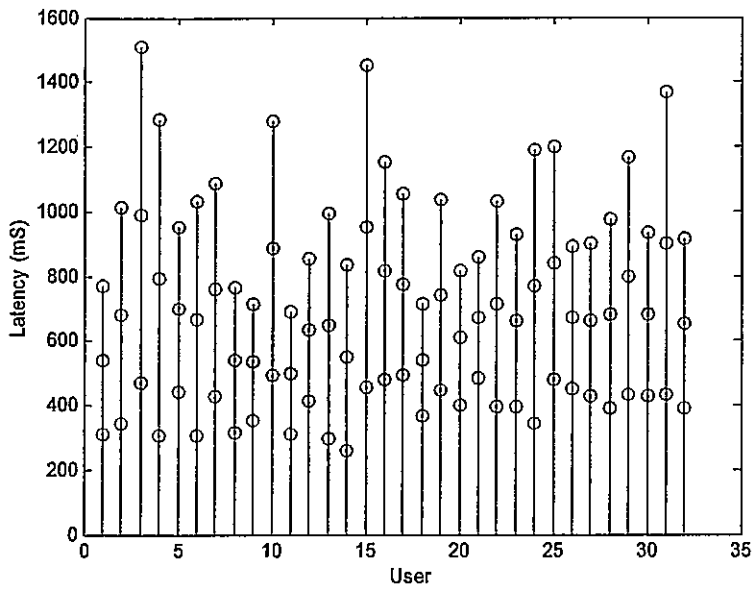
For illustration purposes, the figure below shows a mean and standard deviation plot of users' input data across the three input scenarios. The figure presents each users mean latency value and also the variance of users input values by calculating the standard deviation, giving an estimate to the inter-sample variance for a user.



(a) 4-Digit Input



(b) 11-Digit Input



(c) Varying 11-Digit Input

Figure 4.7: Latency Mean & Standard Deviation for each User

Although, an initial analysis of the inter-sample variance indicates that they are not ideal, however, some users obviously have smaller inter-sample variances than others. Significant differences can be noted between the three input scenarios, such as generally

smaller standard deviations and the lower average latency for the 11-digit input compared to those from the varying 11-digit input scenario. This is expected, in the sense that users would become used to entering the fixed 11-digit number, and therefore the inter-sample variation would progressively decrease. However, it is the 4-digit input that shows the lowest inter-sample variance, possibly indicating strong classifiable regions.

Notable in all three input scenarios is the large number of users that have latency spreads that coincide with a number of others, illustrating that they have very low inter-user variance. The latency spread being defined as the range of a users input vectors that reside between lower (mean minus a standard deviation) and upper (mean plus a standard deviation) latencies. This will make classification more difficult as users input vectors are more likely to be similar, or within similar boundaries as other users.

Through an analysis of the inter-user variance it is possible to construct a table describing which users have the largest inter-user variance; with a view to indicating which users input data would be most successfully classified. Table 4.1 illustrates the top four users with the largest inter-user variance for the 4-digit and 11-digit input scenarios – the varying 11-digit input was omitted due to the lack of discernable features because of the relative similarity in the user's inter-user variance. This table identifies *Users 5, 8, 10 and 11* with the 4-digit input and *Users 6, 7, 8 and 28* with the 11-digit input. According to the hypothesis regarding the inter-user variance (i.e. the larger the variance the more classifiable a user will become) these users should achieve good classification results. However, this technique can at best only identify a couple of networks and certainly cannot be exclusively used as a means of illustrating the relative complexity of users input data.

4.4.2 Mean & Standard Deviation Algorithm

The results from the mean and standard deviation technique are, due to the more rudimentary algorithm employed, fairly poor. Refer to page 4 of Appendix C for an explanation of the technique. However, for the 11-digit input scenario, this technique did prove to be the most successful statistical pattern recognition technique, with an EER of 18%. A number of variables exist within the algorithm that permits the designer to optimise the performance. These include:

- Number of valid latencies within any individual input vector – how many of the latencies in a single input vector are required to fall within the mean and standard deviation boundary?
- Number of standard deviations – how large should the conditional boundary be?
- Minimum number of repeated digraphs (for varying 11-digit input only) – to ensure only those digraphs that have been repeated at least the minimum number of times are used in the classification algorithm.

For the 11-digit input scenario, the optimum conditions were obtained with the standard deviation set to 1.2 and the number of valid latencies within a input vector set to 8 (8/11= 73% of the input vector). The optimum conditions for the 4-digit input scenario was with the standard deviation set to 1.4, with the number of valid latencies set to 3 (3/4=75%), giving rise to an EER of 18%. The optimum conditions for the varying 11-digit input scenario were unusually somewhat smaller, with the standard deviation boundary set to a very small 0.5 but with the number of valid latencies set to 1 far lower than other scenarios (1/11=9%). The reason for this is likely to reside with the large standard deviations of users

4.4.3 Linear Minimum Distance Algorithm

The minimum distance algorithm comprised of the Euclidean technique. In order to achieve optimal results the algorithm utilises the classification distance (the distance at which a user is deemed to be authentic or an impostor). This process is performed on an individual basis for each user, thereby further reducing the error rates. For information on this technique refer to page 5 of Appendix C.

The 4-digit input scenario using a Euclidean classifier was the most successful, with an EER of 18%. The results for the minimum distance algorithm are illustrated in Table 4.3. However, as with any biometric, these performance rates are determined by defining a threshold value – a trade off between security and user convenience, which is illustrated in Figure 4.13, with an EER residing at a Euclidean distance of 280.

	Euclidean (%)		
	FAR	FRR	EER
4-Digit	18	18	18
11-Digit	22	22	22
Varying 11-Digit	36	36	36

Table 4.3: Minimum Distance Algorithm Results

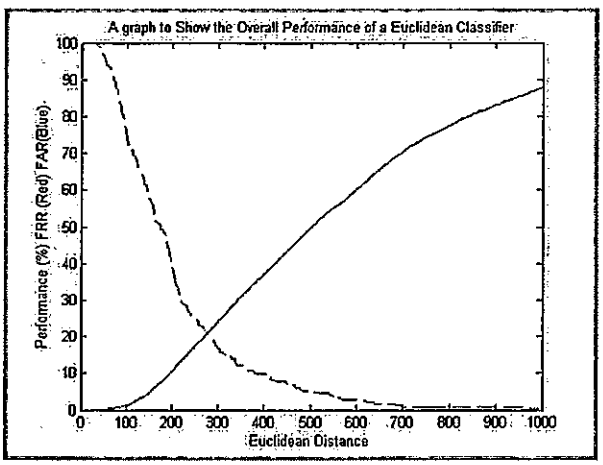


Figure 4.13: FA & FR Variations in the 4-Digit Euclidean Technique

An analysis of individual user's performances has identified *Users 8* performing the best, with the lowest EER^i of 0% achieved with the 11-digit input. The worst individual result was obtained by *User 6*, with an EER^i of 58% with the varying 11-digit input. The best and worst individual classifier performances for the minimum distance technique, across the three input scenarios are illustrated in Table 4.4.

	Euclidean (User/EER' %)	
	Worst	Best
4-Digit	17/35	11/8
11-Digit	25/56	8/0
Varying 11-Digit	6/58	21/15

Table 4.4: Best & Worst Users Utilising the Minimum Distance Algorithm

4.4.4 Hypothesis Test

The hypothesis test utilised in this study was the t-test. Information on how to implement this technique can be found on page 7 of Appendix C. The level of significance, α, was varied in order to optimise algorithm performance. The most optimal level of α was determined for each individual user thereby further improving the performance rates. Figure 4.14 illustrates how the average FAR and FRR vary dependent upon the level of significance applied to the test.

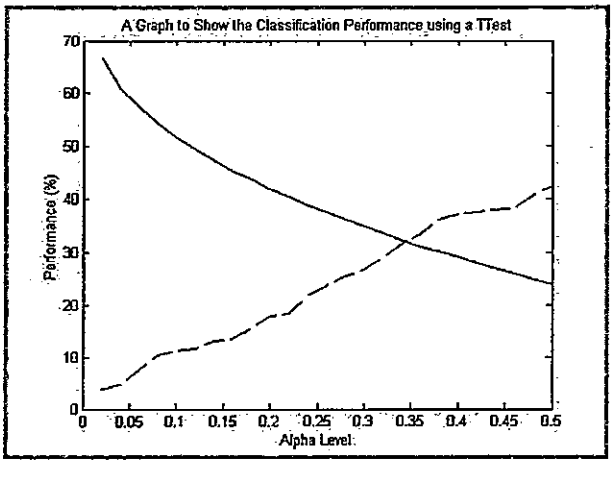


Figure 4.14: FA & FR Variations in the 4-Digit T-Test

The results, as illustrated in Table 4.5, indicate that the minimum distance algorithm previously presented outperformed the t-test in all three input scenarios. The best result the t-test achieved was an EER of 23% with the 4-digit input scenario.

	T-Test (%)		
	FAR	FRR	EER
4-Digit	24	22	23
11-Digit	32	30	31
Varying 11-Digit	38	37	38

Table 4.5: Hypothesis Test Results

Analysing the individual performances shows a broad range of results, as illustrated in Table 4.6 with the worst EER^i of 56% with the varying 11-digit input scenario. Conversely, the best EER^i of 2% was experienced in the 11-digit input scenario. Again, this table illustrates the variability in the performances achieved by users.

	T-Test (User/EER^i %)	
	Worst	Best
4-Digit	16/34	8/5
11-Digit	3/43	8/2
Varying 11-Digit	12/56	3/17

Table 4.6: Best & Worst Users Utilising the Hypothesis Tests

4.4.5 Feed-Forward Multi-Layered Perceptron

The feed-forward MLP networks are amongst the most user configurable neural network topologies. A detailed explanation of neural networks and their application can be found on page 9 of Appendix C. Unfortunately, due to the lack of design techniques governing the value of the parameters, a large number of iterative tests are required in order to achieve an optimal performance. From previous research (Clarke, 2001) two design variables listed below were identified as performing well to the classification problem:

- Transfer Function – Hyperbolic tangent sigmoid function
- Training Algorithm – Gradient descent with momentum and adaptive learning rate

The following network parameters were varied in order to gauge network performance variations, with the view of achieving the most optimal performance rates:

- Number of network layers – varied between 2 and 3 hidden layers
- Number of neurons per layer – varied between 1 and 35
- Number of training epochs – varied between 1000 and 9000

As each user creates an individual neural network and therefore respective FA, FR and EE rates, the results illustrated are an average of all the users' EERs. The most successful FF MLP networks are illustrated in Table 4.7, with the 11-digit input scenario achieving the lowest equal error rate of 13%.This was achieved utilising a two-layer neural network with 11 input nodes, 31 neurons in the hidden layer and 1 neuron in the output layer, having been trained with 7000 epochs. It was noticeable the most complex input scenario (the varying 11-digit input) achieved its best results using the simplest of all three networks with 15 hidden neurons and 7000 training epochs. This would seem to suggest that the (FF MLP) neural networks are unable to generate the discriminative boundaries required and subsequently the most successful networks are those capable of generating more general decision boundaries.

	Network Description		FAR (%)	FRR (%)	EER (%)
	Structure	Epochs			
4-Digit	31 9 1	5000	17	14	16
11-Digit	31 1	7000	15	11	13
Varying 11-Digit	15 1	7000	27	25	26

Table 4.7: Most Successful Feed-Forward MLP Networks

The results also show that the 4-digit input scenario requires a network configuration very similar to the 11-digit input, even though there is a 7-digit difference in the two input vectors. Based upon this, it could be conjectured that the 11-digit results might improve further given larger network configurations. Unfortunately, due to processing constraints, it is not possible to increase the number of neurons in a hidden layer beyond 35 in order to test for any further improvements to be gained in network performance, although this would seem doubtful as the network performance is tending not to increase above 30 neurons.

Monitoring the individual error rates, the EER varies considerably between users. For example, using the most successful networks as depicted in Table 4.7, Table 4.8 illustrates the best and worst performing user networks with their corresponding EER. Both the 4-digit and 11-digit input scenarios achieved $EERs^{i}$ of below 1%, with up to seven participants using a number of the network configurations with $EERs^{i}$ below 10%. However a number of users, such as *Users 16 and 17*, continually perform poorly, to such an extent that an argument could be made about the lack of applicability a keystroke analysis technique has with these particular users using this particular classification technique.

	Best		Worst	
	User	EER^{i} (%)	User	EER^{i} (%)
4-Digit	2	0	17	30
11-Digit	8	0	16	33
Varying 11-Digit	3	3	4	40

Table 4.8: Best & Worst Individual EER's (FF MLP)

4.4.6 Radial Basis Function Networks

RBF networks in comparison to FF MLP networks are far more easily configurable, with only two network variables – the performance goal and spread. In order to optimise the networks both variables were changed independent of each other with the performance goal starting at a value of 0.1 and finishing at 20, and the spread was varied between 0.1 and 1.0. A description of the neural network can be located on page 16 of Appendix C.

The most successful RBF networks are illustrated in Table 4.9, where the 11-digit input scenario again outperforms the 4-digit input, with an EER of 14%. All three input scenario results are worse overall than their FF MLP counterparts, with the worst increase in the varying 11-digit input scenarios EER from 26% in the MLP configuration to 29% in the RBF configuration.

	Performance Goal	Spread	FAR (%)	FRR (%)	EER (%)
4-Digit	12	0.2	15	19	17
11-Digit	8	0.6	14	13	14
Varying 11-Digit	16	0.9	28	29	29

Table 4.9: Most Successful RBF Networks

An analysis of the individual network performances gives rise to a large spread of results with the 11-digit input scenario, achieving an EER^i of 1% for *User 14* and a worst result of 42% for *User 25*. These results were obtained through individual analysis of the most successful networks, as depicted in Table 4.9 and the complete set of results is illustrated in Table 4.10.

	Best		Worst	
	User	EER' (%)	User	EER' (%)
4-Digit	2	0	17	40
11-Digit	14	1	25	42
Varying 11-Digit	14	4	7	50

Table 4.10: Best & Worst Individual EER's (RBF)

4.4.7 Generalised Regression Neural Networks

GRNN's are, in terms of implementation, the simplest of neural network configurations, with only a single network parameter to define. Using the (user-defined) spread value GRNN's can be quite successful. For more information regarding this approach refer to page 19 of Appendix C. Typically values for the spread range from 0.01 through to 1.0. The most successful GRNN's are illustrated in Table 4.11. The 4-digit input scenario achieved an EER of 13%, the most successful result across all the neural network and pattern recognition techniques. The varying 11-digit input marginally improved its EER in comparison to the RBF networks achieving an EER of 28%. However, this is still 2% greater than the FF MLP.

	Spread	FAR (%)	FRR (%)	EER (%)
4-Digit	0.1	14	12	**13**
11-Digit	0.2	11	17	**14**
Varying 11-Digit	0.4	23	32	**28**

Table 4.11: Most Successful Generalised Regression Networks

Bearing in mind the simplicity and speed of implementation, the GRNN initially appears to be a successful network configuration. Although it is relatively successful, care needs to be taken as small changes in the spread can cause large changes in the resultant EER. So unlike both FF MLP and RBF networks, GRNNs are very sensitive to network changes which from a practical standpoint could prove troublesome.

An analysis of the individual network performances, as illustrated in Table 4.12, highlights the differences in the EER between individual network performances, with some users performing better than others. For instance both the 4-digit and 11-digit input scenarios achieved worst EERs greater than both the FF MLP and RBF networks, but equally achieved 0% ERR^i with *User 7* in the fixed 11-digit input scenario.

	Best		Worst	
	User	EER^i (%)	User	EER^i (%)
4-Digit	11	0	17	35
11-Digit	7	0	3	49
Varying 11-Digit	14	9	5	48

Table 4.12: Best & Worst Individual EER's (GRNN)

From an analysis of all the results from the GRNN investigation, the results from the 11-digit input scenario proved most interesting, with a number of users experiencing low $EERs^i$. For instance, across all the spread settings *Users 7 and 8* both have $EERs^i$ of 0%, with 8 further users with $EERs^i$ below 5%.

4.4.8 Extension to the Neural Network Investigations

The results obtained by the neural network based classification techniques have proved promising, and have therefore given rise to three extended investigations:

1. Best Case Neural Network – combining the best individual network performances from the various network configurations.
2. Gradual training FF MLP – ensuring each individual network is utilising the most optimal number of training epochs.
3. Area Code Input Scenario – authentication of users based on the area code of a telephone number.

From an implementation perspective, iterating through several hundred network configurations in order to determine the most optimal configuration for each user would be far too time consuming and computationally intensive. However, what these results have shown is the ability of neural networks to correctly discriminate users dependent upon how they type numbers, and additionally, identified a series of network configurations that perform particularly well. Therefore future implementations would either need to iterate through a small number of network configurations and choose the best configuration, or develop an algorithm that can (from an analysis of the input data) determine the most appropriate network configuration for each user.

4.4.8.2 Gradual Training Method

The "Gradual Training Method" sought to compensate for the possible lack of generalisation. One technique employed to combat the issue of generalisation is "early stopping", where the data set is split into three – a training set, a validation set, and a test set. Both the training and validation datasets are used in the creation and training of the network, with the network being trained using the training dataset, but after each epoch the network error is calculated using the validation dataset. When the network error increases for a specified number of iterations, the training is stopped and the test dataset is utilised to gauge the network performance. Unfortunately, due to the relatively small size of the dataset it would be unrealistic to divide the dataset into three. As such, a gradual training investigation was sought where the dataset was split into the usual two, training and test datasets and the network performance was calculated at defined intervals in the number of epochs. This differs from "early stopping" as the training dataset is not used to prematurely

looks into simulating dynamic authentication by utilising the more static components for a telephone number, i.e. the area code. It could be hypothesised that a typical user might dial telephone numbers that come from a limited number of areas. As such, the investigation utilises the data obtained from the static 11-digit input scenario having removed the latter 6 latencies from each input vector to leave just the latencies corresponding to the dialled area code.

The results, as illustrated in Table 4.13, are promising with an overall EER of 11%. The gradual training technique was utilised with a FF MLP network configuration. Both configuration 1 and configuration 2 in the table represent the results obtained from a single network configuration, with the combined network results representing the overall result obtained from the individual results. The results are obviously worse than the static 11-digit input scenario as the input vector has been reduced from 11 latencies to 5, but are an improvement over the varying 11-digit input scenario.

	FAR (%)	FRR (%)	EER (%)
Configuration 1	17	19	18
Configuration 2	18	18	18
Combined Net	13	9	11

Table 4.13: Network Performance Utilising the Area Code of the 11-Digit Input

So authentication on varying telephone numbers can be achieved through a two stage approach. If a user enters a varying telephone number where a network exists to authenticate the person by the area code, then a static approach can be used, otherwise, a dynamic authentication network could be utilised.

4.5 Conclusion

The investigations have shown the ability for classification algorithms to correctly discriminate between users with a relatively good degree of success, with neural network approaches performing significantly better than their pattern recognition counterparts. The general performance of the 4-digit input vector (analogous to the PIN) suggests that the entry of the PIN on a mobile handset has a quite unique dialling pattern, perhaps due to user's previous experience of having to enter such short sequences on a regular basis, and could form a good basis for a hardened password approach as suggest by Monrose et al. (1999). Classification algorithms typically find classification simpler when the input vector is large, as it would arguably contain more discriminative information. Overall, this was found to be the case, with the 11-digit input generally outperforming the 4-digit input, but not always by a large margin.

The inter-user variances generated in the descriptive statistics section, illustrated in Table 4.1, highlighted a number of possible users who it was hypothesised would (due to their large inter-user variance) perform well in classification. A comparison of these users with the results from the combined neural network investigation shows all 8 users from both 4 and 11 digit input scenarios achieving some of the lowest $EERs^i$ with all of them having achieved an EER^i of below 10%. This supports the argument for the inter-user variance being used as a soft indicator towards possible classification success.

The degree to which varying network configurations effects the overall network performance is somewhat negligible, with the optimal network configurations only improving the EER by 2-3% over the original results. However, the different network

configurations do appear to have a large effect on individual performance rates, as illustrated by the performance of the "best case" neural network results in Figure 4.15, Figure 4.16 and Figure 4.17. Performance comparisons of all the classification techniques for the 4-digit and 11-digit input scenarios are illustrated in Figure 4.20 and Figure 4.21.

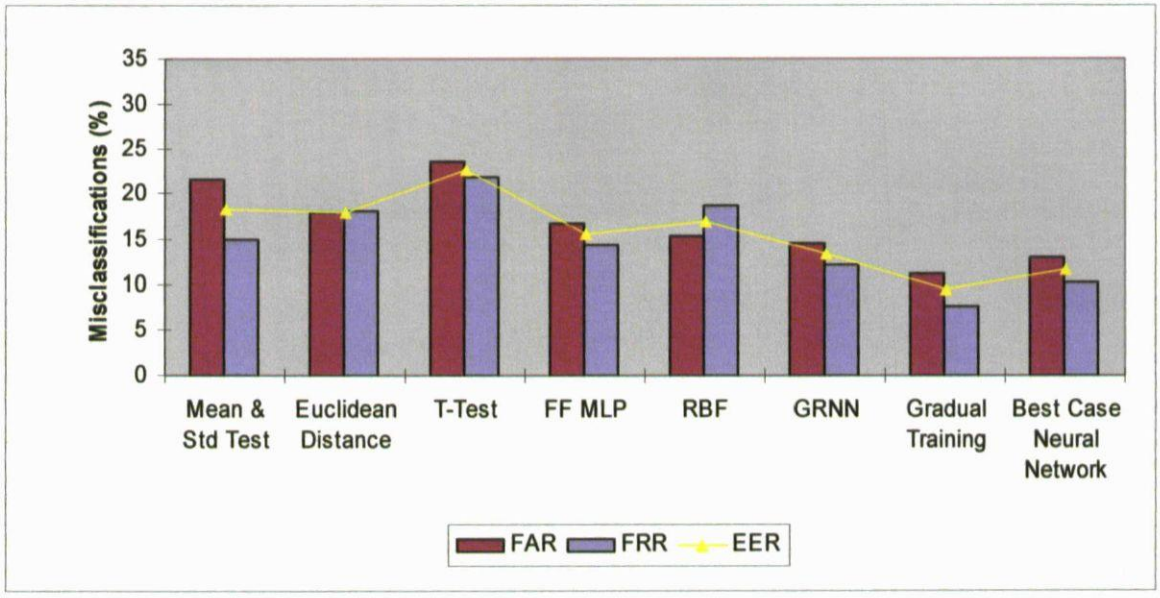


Figure 4.20: Overall Classification Results for the 4-Digit Input

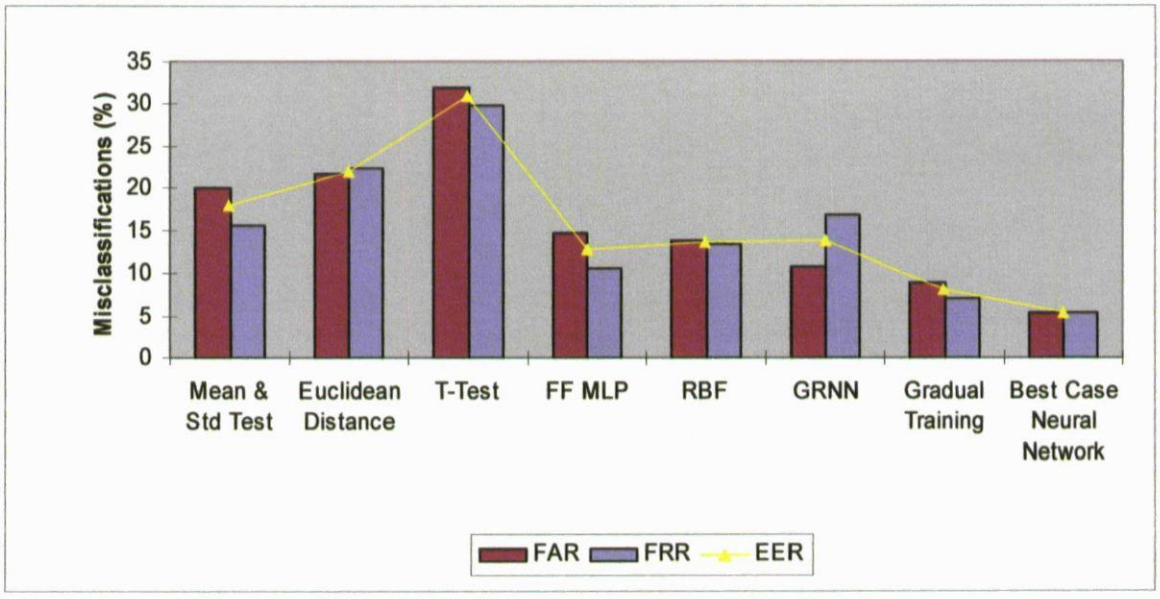


Figure 4.21: Overall Classification Results for the 11-Digit Input

From an analysis of the classification algorithms, it is clear that some of the individual network performances experienced 40%+ false acceptance and false rejection rates. This would indicate one of two problems. The first problem is that, a user's input varies too much from input to input for even a static keystroke analysis technique to prove useful. The second is that, the classifier may not be sensitive enough to the user's data. Both of these problems could be counteracted as the user enters more and more data to the classification engine. Currently, however, this error rate would be completely unsatisfactory, and any keystroke analysis algorithm developed will need to monitor a user's individual error rates and determine the level of security provided given the current input data. Conversely, a number of classifiers (particularly the neural network based techniques) experienced a number of users achieving a FAR^i and FRR^i of 0%, reiterating the ability for users' keypad interactions to be discriminative.

Although classifiers were relatively successful based upon static inputs, to work effectively any practical implementation of keystroke analysis would depend on the ability to provide classification of dynamic inputs in order to provide non-intrusive, ad hoc authentication. Although the results for dynamic input classification have been poor in comparison with a static approach they are nevertheless encouraging, especially considering the small datasets with which the classifier was trained and validated. It may also be possible to improve dynamic authentication performance by utilising the more static elements of a varying input. For example the area code of a telephone number – this resulted in an EER of 11% using the area code of the 11-digit input scenario.

Having established a successful method of authenticating users based upon numerical data, the next chapter will evaluate the feasibility of character-based classification, using a different keystroke characteristic.

5 Verification of Identity through Alphabetic Input Data

Chapter 4 sought to evaluate the ability to verify subscribers by the way in which they typed numerical inputs. A second popular handset interaction, due primarily to the popularity of SMS messaging, is the composition of text messages. Therefore, this chapter has focussed upon on the ability to verify users by the way in which they type alphabetic characters on a mobile handset. Building upon the findings of Chapter 4, the classification algorithms utilised in this study are based on feed-forward MLP neural network configurations. The chapter will conclude with a comprehensive discussion on the viability of keystroke analysis on a mobile handset.

5.1 Introduction

The numerical input investigation utilised the inter-keystroke latency or time between two successive keystrokes as the discriminatory characteristic for classifying a user's input vectors. This study looked into discriminating users by utilising another characteristic typing trait identified during the literature study, that of the time taken to press and release a single key, otherwise known as key hold time. This was chosen for two reasons; firstly and predominately in order to evaluate the feasibility of another keystroke characteristic, and secondly due to the increased number of digraph pairs (different permutations of two keys) character-based authentication introduces. In a numeric input scenario, the number of digraph pairs is 100, as there are 10 numbers. In a character-based input scenario where there are 26 characters, the resultant number of possible digraph pairs increases to 676. Many of the digraph pairs will not naturally appear in the English language reducing this number, and although it would also be possible to develop classification algorithms based on a small number of the most recurrent digraphs, a user could not be guaranteed to enter those digraph pairs in any one situation.

Through utilising the hold-time of a key, the number of possible combinations is reduced from over 600 to just 26, making classification both simpler and more likely to occur in any one given text message. The hold time in this particular investigation is somewhat different from the traditional definition of the word, as keypad keys have to be pressed several times in order to type many of the characters (e.g. the letter 'b' requires the number 2 button to be pressed twice). The hold time in this study is therefore defined as the time taken from when the first key depression event has occurred to the final key press release. As described by the calculation of the hold time, this study utilises the traditional text

message entry method where users have to repeatedly press a key to enter some characters. It was decided not to utilise a predictive texting input method for two reasons:

1. A key would only need to be pressed once for each character, thereby arguably reducing the discriminatory information contained within the hold time.
2. As each key is only required to be pressed once, the number of digraph pair combinations reduces back to 100, therefore permitting the inter-keystroke characteristic to be implemented, as presented in Chapter 4.

Although the initial classification concept for this investigation is to perform dynamic keystroke analysis on the text messages – due to the very large number of character combinations, a normal static approach where individual networks are developed for each word or even sentence is impractical. However, from Chapter 4 it is evident that static based approaches perform substantially better than their dynamic counterparts. As such, it was decided that by utilising the more static components of the text message, classification can be achieved statically. Therefore, by designing neural networks whose inputs to the network are based upon the most recurrent characters, classification can be obtained statically on text messages independent of the actual word(s) or sentence being composed.

5.2 Data Collection

The data collection stage of this investigation required new subscriber interaction data to be obtained. As such, thirty participants were obtained and they entered a total of thirty text messages each, ten text messages over three sessions, where each session was separated by a least a week. By using multiple sessions it was hoped to obtain more robust

and user-indicative input data – an improvement based upon reviewing the numerical input investigation procedure. The text messages themselves were a collection of quotes, lines from movies and typical SMS messages, where the only proviso was to ensure enough of the characters were repeated to enable classification – a list of the messages can be found in Table 5.1. No importance was placed on achieving a particular distribution of character repetitions as in a practical implementation the algorithm would dynamically adapt to the most recurrent characters within an individual users captured dataset.

#	Text Message
1	the quick brown fox jumped over the lazy cow
2	a lie gets halfway around the world before the truth has a chance to get its pants on
3	hi john can not make lunch will phone you later
4	love cures people both the ones who give it and the ones who receive it
5	in a meeting at present will conference call you later
6	everything is funny as long as it is happening to somebody else
7	lack of will power has caused more failure than lack of intelligence or ability
8	fancy a couple of drinks tonight down the local
9	it is a rock tommy it does not have any vulnerable spots
10	i will meet you in town by the bus station at one
11	i love the smell of napalm in the morning
12	master yoda says i should be mindful of the future
13	a father is a guy who has snapshots in his wallet where his money used to be
14	a man knows when he is growing old because he begins to look like his father
15	all that stands between the graduate and the top of the ladder is the ladder
16	if computers get too powerful we can organise them into committees
17	a diplomat is a man who always remembers a womens birthday but never remembers her age
18	i refuse to admit that i am more than fifty two even if that makes my children illegitimate
19	all of lifes great lessons present themselves again and again until mastered
20	do you want the job done right or do you want it done fast
21	a good marriage would be between a blind wife and a deaf husband
22	A man is a success if he gets up in the morning and gets to bed at night and in between he does what he wants to do
23	to educate a man in mind and not in morals is too educate a menace to society
24	advice is what we ask for when we already know the answer but wish we did not
25	immaturity is the incapacity to use ones intelligence without the guidance of another
26	a positive attitude may not solve all your problems but it will annoy enough people to make it worth the effort
27	a great obstacle to happiness is expecting too much happiness
28	consistency requires you to be as ignorant today as you were a year ago
29	adults are just children who earn money
30	children are natural mimics who act like their parents despite every effort to teach them good manners

Table 5.1 Text Message Dataset

Table 5.2 illustrates the break-down of character repetitions from the input dataset. Based upon the numerical input investigation, those characters with repetitions of thirty or greater could be utilised in the classification process if necessary.

The modified mobile handset developed for the numeric-based investigation in Chapter 4 was re-used in this investigation in order to keep the same tactile qualities.

5.3 Procedure

The investigation required the generation of a series of new function scripts that had the ability to handle character-based input data – the format of which differed greatly from the numeric input data, although the overall procedure of data extraction, outlier removal and dataset splitting remained the same. The parent-child function scripts utilised in this investigation are illustrated in Figure 5.3 (please refer to section 4.3 for function script descriptions). Due to the larger number of reoccurrences within this set of input data, it was possible to perform an additional test on the feed-forward MLP paradigm that would improve the generalisation of the network. The technique known as "early stopping" performs a similar function to the gradual training test performed in the first investigation. However, unlike the gradual training scheme (where the system designer decides the epoch levels), early stopping will stop the number of epochs on an individual user basis and within a single epoch, thereby theoretically optimising the neural networks further. In order to achieve this test it was therefore necessary to create a specialist control and network function script capable of handling the modified function calls (not illustrated in Figure 5.3).

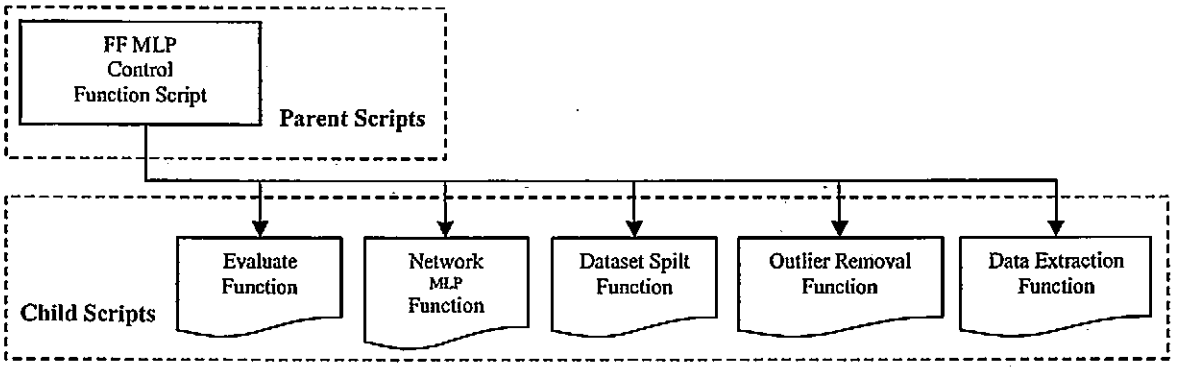


Figure 5.3: Character Verification Program Function Tree

The investigation itself utilised only one of the neural network paradigms, Feed-Forward MLPs. The RBF networks were removed, as they were the worst performers in the previous investigation. Due to the one-to-one mapping of input vectors to neurons that GRNN networks require, and the larger the input dataset (up to 94 input vectors per person[5]), the network was deemed inappropriate in this investigation as they would require several hundred neurons plus in order to provide classification (94 multiplied by number of users). Such a number of neurons would be both impractical and too computationally complex.

By manipulation of the MLP network parameters the investigation has sought to minimise classification performance error. In addition to varying the network parameters as defined in the first investigation, this investigation has also varied the number of inputs to a neural network in order to establish the optimal number of input characters required to successfully authenticate a subscriber. A trade-off exists between utilising a longer input vector (thereby improving classification but to the detriment of increasing network complexity), and leaving the input vector with *null* values – since there are no guarantees

[5] 94 input vectors are generated after outliers had been removed from the dataset.

that a text message may contain the characters you require to make up the input vector. Table 5.3 illustrates the number of the input vectors being investigated, along with the characters being utilised in the construction of the vector itself.

Number of Inputs	Characters in Input Vector
2	ET
3	ETA
4	ETAO
5	ETAON
6	ETAONI

Table 5.3: Input Vector Construction

5.4 Results

The results from the verification of character-based input vectors are split into the classification algorithms. However, the first section outlines the descriptive statistics of the input data with respect to the thirty participants, allowing for an intuitive overview of the classification problem.

Similarly to the first investigation, a large number of iterations were necessary in order to optimise the performance, and the following results illustrate the most successful network configurations. However, a complete listing of all the results can be found in Appendix D.

5.4.1 Descriptive Statistics

The descriptive statistics stage is an important aspect in the designing of a classification system as it permits an insight into the relationships that occur within the data. By performing mean and standard deviation examinations it is possible to establish the degree

Figure 5.4 illustrates these relationships with each users' mean and standard deviations plotted, for the four most recurrent characters; 'e', 't', 'a' and 'o'. It can be seen that many of the users share a similar mean and standard deviation plot, e.g. *Users 2 and 4* with character 'e' and *Users 19 and 21* with character 't' (far more so than in the first investigation), thereby giving rise to poor network performance due to the networks inability to discriminate between them. However, this is not necessarily the case, as the similarity in mean and variance does not continue throughout all characters (as indicated in the figure), and since the input vector to the neural network is constructed from a number of characters it is hoped this should provide the sufficient disparities required in input data for the network to discriminate against users correctly.

An analysis of the inter-user variance has presented a number of users that continually reappear with large inter-user variances when compared to the remaining users, as illustrated in Table 5.4. Using this technique assists in predicting which users would be expected to perform well in classification if the argument of inter-user variance stands true.

Rank	User
1	23
2	11
3	10
4	17

Table 5.4 Participants with Largest Inter-User Variance

In order to appreciate the difficulties involved in discriminating between users successfully, Figure 5.5 illustrates 2D plots of the input data. Figure 5.5(a) illustrates a 2 character input vector (characters 'e' and 't') for a single user, with a fairly large spread of values, and Figure 5.5(b) illustrates the same 2 character input vector with all users' input data included. This problem is compounded when larger input vectors are introduced,

discrete stages in the input data should still be sufficient to generate the correct classifiable boundaries.

5.4.2 Feed-Forward Multi-Layered Perceptron

The feed-forward MLP network is the most suitable neural paradigm given this type of classification problem. Unlike the numerical input investigation, this study has significantly more input data with which to train the networks. Unfortunately, the resultant effect of this is that many of the network paradigms considered suitable in Chapter 4 are not suitable here due to the one-to-one mapping of input vectors to neurons. Feed-forward MLPs, due to the complex mesh of inter-connections between neurons, do not require this same level of input neuron mapping.

The most successful FF MLP networks are illustrated in Table 5.5, with the 5-digit input scenario achieving the lowest EER of 20%. Although at first glance these results seem a little high, it must be remembered that the neural networks only utilising the hold-time of up to six characters for classification. These results were achieved utilising a network configuration of 28 neurons in the first hidden layer and a single output neuron as usual, with 100 epochs using the Levenberg-Marquardt training algorithm[6]. It would be expected that the larger input vector neural networks would outperform their smaller counterparts, as they would typically contain more discriminative information. A possible reason for this disparity is that the extra character in the 5 and 6 input neural networks does not contain any additional positive discriminative information, but contains no discriminative or even

[6] The Levenberg-Marquardt algorithm was utilised in this study as the traditional Gradient Descent algorithm was, given the larger datasets to process, very time consuming. Although the Levenberg-Marquardt algorithm is quicker in providing training, a trade-off exists, as the Gradient Descent algorithm provide more stable results (Demuth & Beale, 2001).

negative discriminative information. Alternatively, these larger input vector neural networks, due to the additional information contained within the vector, might require a larger and more complex neural network to compensate for the increased dimensionality of the problem.

# of Inputs	FAR (%)	FRR (%)	EER (%)
2	26	28	27
3	23	26	24
4	21	23	22
5	20	20	20
6	23	18	21

Table 5.5: Most Successful Feed-Forward MLP Networks

Monitoring the individual error rates taken from the best performing network configurations previously presented in Table 5.5, the EER can be seen to vary considerably, as illustrated in Table 5.6. Of most concern is the 6-digit input scenario, where the worst case result was with *User 26* being unclassifiable - a situation where the FAR^i is equal to 100% with the FRR^i equal to 0% or vice versa. It is worth noting, however, that *User 26* is not unclassifiable with all 6-digit input network configurations. In this circumstance, with this network configuration, the classification algorithm is unable to discriminate between the authorised user and the impostor. Having said this, $EERs^i$ of 33% and greater as illustrated in Table 5.6 are in any practical sense also unacceptable.

# of Inputs	Best		Worst	
	User	EER (%)	User	EER (%)
2	17	12	22	47
3	7	12	22	41
4	23	10	22	36
5	13	9	22	33
6	10	5	26	UNCLASSIFIABLE

Table 5.6: Best & Worst Individual EER's (MLP)

The practicalities of such a result would mean the user would currently be unable to use this particular network in a character-based keystroke analysis technique to authenticate themselves. There are two possible solutions to this issue. The first would be to obtain more discriminative input samples and retrain the network, or indeed try another network configuration. Alternatively, and more simply, the classifier would utilise one of the remaining neural networks residing with the other input scenarios. Through utilising the network that performed the best, user authentication can be made possible for all users (within of course certain performance boundaries).

5.4.3 Gradual Training Multi-Layered Perceptron

The gradual training MLP algorithm was developed in the first investigation as a means of improving generalisation and subsequent network performance, since traditional techniques such as early stopping could not be used due to the very small nature of the input data. This is not the case for the second study where "early stopping" can be utilised. However, the use of a gradual training scheme is not lost in this investigation, as it enables the network designer to closely monitor the changes in network performance as the number of epochs varies. Also, in a practical sense this could also be utilised as an authentication system to authenticate a user using a small dataset for training, very much like in the first investigation.

The network configuration utilised in this algorithm consisted of 22 neurons in the first hidden layer, 5 in the second and 1 output neuron. The training epochs were varied by 15 between the lower boundary of 15 epochs to the upper boundary of 150 epochs. The EERs for each of the input scenarios across each of the participants are illustrated in Figure 5.6.

increases so does the complexity of the neural network required to solve the problem, and perhaps this is one reason why no real improvement was gained between the 5-digit and 6-digit input scenarios when utilising an identical network configuration.

5.4.4 Early Stopping Multi-Layered Perceptron

"Early stopping" is a traditional technique for preventing poor generalisation – the problem where networks are either over or under trained resulting in poor network performance. Despite similarity in approach to gradual training, "early stopping" has distinct differences, which were explained previously.

As the number of training epochs was relatively low in this test (5-100), it was possible to utilise a much larger neural network than would otherwise be possible due to computational complexity and subsequent time to train. The network utilised varied with the most successful consisting of 18 neurons in the first hidden layer, 18 in the second and the usual 1 output neuron, and although the number of training epochs was arbitrarily capped at 5000 none of the networks passed 125 epochs.

From the results, illustrated in Table 5.7, on average the 6-digit input scenario proved the most successful in terms of network performance, achieving an EER of 21%. The results also show the EER improving as the size of the input vector was increased from 2-digits through to 6, which given the increased size of the neural network, would substantiate the argument that more discriminatory information is held within the longer input vectors given a large enough neural network capable of constructing more complex discriminatory

boundaries. However, it is important to note these EERs are still higher than those achieved previously.

# of Inputs	FAR (%)	FRR (%)	EER (%)
2	25	29	27
3	27	24	26
4	22	25	24
5	22	22	22
6	20	22	21

Table 5.7: Most Successful Early Stopping Networks

An analysis of the individual network performances gives rise to a large spread of values, with the best EER^i being achieved by *User 17* in the 6-digit input scenario of 8%. The worst result was an EER^i of 43%, by *User 22* in the 2-digit input scenario.

# of Inputs	Best		Worst	
	User	EER (%)	User	EER (%)
2	17	13	22	43
3	17	13	8	42
4	23	10	22	43
5	17	10	8	37
6	17	8	15	43

Table 5.8: Best & Worst Individual EER's (Early Stopping)

It would be expected that the "early stopping" algorithm, due to the one epoch resolution and larger network size, would outperform the gradual training algorithm; however this was not the case. The most probable reason for such a result is due to the difference in dataset splits. The dataset split in the gradual training algorithm may have given rise to a training dataset that is a true representation of the test data set whereas the dataset split with early stopping might have given rise to the data in the training and validation datasets being representational to each other but not completely representational of the test dataset, giving rise to artificially poorer network performance. This error arises purely as a product of having to split the input data into datasets in order to evaluate network performance, and

could therefore be removed in any practical situation by further training with the validation and test datasets.

5.5 Conclusion

The study has shown the ability for classification algorithms to correctly discriminate between users with a relatively good degree of accuracy based on a user's hold-time of a key. Although network performance has been consistently poorer than the static approaches presented in the numeric input study, these results do compare well if not better on the whole to the dynamic verification approach performed previously, illustrating that in terms of performance the hold time characteristic resides in between static and dynamic based authentication using the inter-keystroke latency characteristic. The ability for an authentication system to provide authentication independent of what the user is typing is important if continuous and non-intrusive authentication is to be achieved.

A comparison of the inter-user variance predictions of good classifiable users again proved correct, with *Users 10, 11, 17 and 23* all achieving EERs[i] of below 10% (see Figure 5.6 for a comparison). The inter-user variance measure could also have a second use in selecting a small number of users with which to train each user network. Currently training of each user is performed with one user acting as the authorised user with the remaining users acting as impostors. In a practical situation, with many thousands of users, it would not be practical or desirable for a network to be trained with so many users. Instead the inter-user variance measure could be used to determine those users with the most similarity in their input data to the authorised user and for the network to only use a number of those users. For instance, by using only the users with small inter-user variances in comparison to the

Although this technique for character-based authentication is word independent and would, under the majority of circumstances, meet the requirement of continuous and non-intrusive authentication, implementing a static approach on commonly reoccurring text message words might provide the discriminative information required to authenticate users with a greater degree of accuracy, in particular those who currently cannot be discriminated using this pseudo-dynamic approach.

Chapters 4 and 5 have thoroughly investigated the feasibility of authenticating users based upon their typing characteristics on a mobile handset – showing both the keystroke latency and hold-time as viable discriminative characteristics. In particular, this study has shown in general the ability of neural networks to more successfully discriminate between users over traditional statistical techniques. The overall process of discrimination would arguably be improved if both typing characteristics could be used in conjunction with each other, which could be implemented for numerical-based authentication. However, the process of continuous and non-intrusive authentication does not easily permit this technique for character-based authentication due to the large number of digraph pairs that exist.

From the results from this study, keystroke analysis has shown promise when compared against commercial biometrics, as illustrated in Table 3.1. Although, the ability for classification algorithms to correctly discriminate between users very successfully is low, the majority of users are experiencing a fair to good performance. However, as with all biometrics, a number of users remain that are unable to be correctly authenticated to a reasonable degree. Therefore, any practical implementation of keystroke analysis would require a flexible framework, ensuring that even those users for whom keystroke analysis is not a viable approach are still provided with a adequate level of security (but equally

ensuring that the majority of users that are classifiable using keystroke analysis benefit from the higher level of protection provided by the technique).

The results presented however, must be considered in context. Two feasibility studies were performed in controlled conditions, with users entering data repeatedly. Within a practical environment, the variability of the users' input data is likely to be larger, as users may be walking whilst typing, consuming alcohol or performing other tasks, making the process of authentication more difficult. Therefore, it would not be viable to use this technique, where a user is accepted or rejected based upon a single keystroke analysis result. However, due to its transparent nature, it would be possible to use an unsuccessful authentication request as a trigger for a heightened level of monitoring on the device. Therefore keystroke analysis is capable of increasing the transparent authentication capability of devices with keypads.

Chapter 3 identified a number of additional biometric techniques capable of increasing the transparent authentication ability of a device. However, given the varying hardware configurations of devices, in addition to the performance of the techniques, it is clear that no single technique would suffice. On this basis, it is proposed that a mechanism is required that is adaptable to the differing hardware configurations, and capable of utilising an array of authentication tools to maintain the integrity of the system. The next chapter proceeds to describe such a composite authentication mechanism and the processes required to maintain security.

6 A Novel Mechanism for Composite Authentication

This thesis has described many types of authentication technique. Secret-knowledge based approaches have been generally found lacking, and individual biometric techniques only go so far in solving the problem. Chapters 4 and 5 have demonstrated that the use of keystroke analysis will increase the level of transparent authentication provided by a device, but does not provide sufficient performance to be deployed as the only authentication mechanism. As such, this chapter will describe the processes and algorithms required to provide a novel composite authentication mechanism capable of utilising a suite of authentication techniques both biometric and secret-knowledge based in order to provide a robust and dynamic authentication mechanism.

6.1 Introduction

It is envisaged that a successful authentication mechanism for mobile devices must meet a number of objectives:

- to increase the authentication security beyond secret-knowledge based approaches;
- to provide transparent authentication of the user (within limits) to remove the inconvenience factor from authentication;
- to provide continuous or periodic authentication of the user, so that the confidence in the identity of the user can be maintained throughout the life of the device;
- to provide an architecture that would function (to one extent or another) across the complete range of mobile devices, taking into account the differing hardware configurations, processing capabilities and network connectivity.

This has been achieved through utilising a combination of secret knowledge and biometric-based techniques within an appropriately flexible framework. The framework operates by initially providing a baseline level of security, using secret knowledge approaches, which progressively increases as the user interacts with their device and biometric samples are captured. Although user authentication will begin rather intrusively (e.g. when the device is switched on for the first time), with the user having to re-authenticate periodically, the system will however quickly adapt, and as it does so the reliance upon secret knowledge techniques is replaced by a reliance upon biometrics – where the user will be continuously and non-intrusively authenticated. The result is a highly modular framework that can utilise a wide-range of standardised biometrics, and which is able to take advantage of the different hardware configurations of mobile devices – where a combination of cameras,

microphones, keypads etc can be found. The proceeding sections will describe the components and processes of the composite authentication mechanism.

6.2 Process Engines

The computational backbone of this framework, from template generation to file synchronisation is provided by four process engines:

- Data Collection Engine
- Biometric Profile Engine
- Authentication Engine
- Communications Engine

6.2.1 Data Collection Engine

The Data Collection Engine is required to provide the capturing of a user's input interactions. The actual samples to be captured by the engine will be dependent upon the hardware contained within the device - as the hardware configuration of devices can vary considerably, with a mixture of cameras, microphones, keypads and even fingerprint sensors on some devices. However, as an example, the typical hardware configurations on a third generation mobile handset, will permit the framework to capture the following types of input sample:

- Keystroke latencies from a keypad whilst the user is typing – including entering telephone numbers and the typing of text messages.
- Images from a camera whilst the user is interacting with the device

be required to capture static input samples from the user device. The control of this is achieved through the Authentication Manager and a lookup table which contains the master list of compatible biometrics for a particular user, referred to as the Authentication Assets, which will be described in section 6.3.2.

Once the software interfaces have captured a user's interactions, the next stage of the Data Collection Engine is to pre-process this data into a biometric sample – thereby removing any erroneous data from the sample, leaving only the information which is required for the authentication. This stage is optional in the client-server topology, but recommended to minimise the size of the template file that has to be sent across the network – thereby reducing network traffic. The task of pre-processing (and other biometric specific operations such as template generation and authentication) is dependent upon the individual biometric technique – each one will pre-process the input data in a different way. For instance, pre-processing of keypad input data to be used by keystroke analysis involves the calculation and scaling of timing vectors, whereas the pre-processing of a sound file for use by a Voice Verification technique would involve the extraction of key sound characteristics.

In order to achieve modularity – so that the framework can utilise one or more biometric techniques in any given device – the system must be compatible with a wide-range of different biometric techniques from a number of biometric vendors. Although all the algorithms associated with a biometric technique are proprietary, a standard programming API exists for biometrics called BioAPI (BioAPI Consortium, 2003). Through BioAPI, the framework is able to make standard function calls to whichever proprietary algorithms are necessary, requesting for sample pre-processing, template generation and authentication –

thereby negating the requirement for any custom software development of biometric algorithms.

After the pre-processing the Data Collection Controller will proceed to send a control message to the Authentication Manager, informing it what input data has been captured. This enables the manager to utilise the most appropriate input sample in a given situation. It will also send the biometric sample to the Input Cache for temporary storage and possible subsequent use in authenticating the user.

The actual run-time content of the Input Cache is dependent upon the type of input data being collected, which is in turn dependent on the hardware configuration of the device – identified by the Authentication Assets. However, the general structure of the Input Cache consists of a table (per user) containing date, time, technique, sub-category and file location information on the biometric sample (and also secret knowledge techniques). Table 6.1 illustrates the table format using facial recognition, keystroke analysis, voice verification and intrusive responses as an example.

ID	Date	Time	Technique	Sub-Category	File Location
1	19/05/04	09:32	Facial Recognition	None	\\input_cache\Face001
2	19/05/04	14:48	Keystroke Analysis	Text	\\input_cache\Keystroke_Telep002
3	19/05/04	15:03	Keystroke Analysis	Telephone Dynamic	\\input_cache\Keystroke_Text067
4	19/05/04	15.15	Voice Verification	Phrase 2	\\input_cache\Voice003
5	19/05/04	15.16	Intrusion	Face	\\input_cache\Intrusive_Face011
6	19/05/04	15.18	Intrusion	Cognitive Response	\\input_cache\Intrusive_Cognitive002
:	:	:	:	:	:

Table 6.1: Input Cache Database

As a number of the biometric approaches have several algorithms that enable the technique to classify users due to the different types of input, such as static and dynamic samples, the sub-category entry is included within the input cache tables to identify which algorithm to use. It also identifies in the case of an intrusive response which technique has been utilised. The File Location entry acts as a pointer to the biometric sample, for voice and facial verification this means a sound and image file (dependent on pre-processing).

Once the input data has been used to authenticate the user, the subsequent result will also indicate whether it is believed the data belongs to the authorised user or an impostor. If the data is found to be valid then the sample can be passed on to the Profile storage element for use in calibrating future classification algorithms. If the data is found to be from an impostor then the sample is removed and deleted from memory.

6.2.2 Biometric Profile Engine

The Biometric Profile Engine's primary role is to generate the biometric templates that enable subsequent classification by the Authentication Engine. This is achieved through a series of template generation algorithms, which take the biometric sample (pre-processing it if necessary) and output a unique biometric template. The contents of this biometric template will differ between biometric techniques – the facial recognition template might consist of a number of distance measurements between key features of a face, the voice template might consist of amplitude measurements at discrete moments in time, and the keystroke analysis template might consist of a number of weight values corresponding to a trained neural network for the authorised user. The Biometric Profile Controller, as illustrated in Figure 6.2, then takes both the biometric sample and biometric template and

which initially provides no security beyond what is currently available on cellular, mobile devices (i.e. secret-knowledge approaches such as the PIN or password) and for the biometric security to gradually increase as the user naturally interacts with their device. Apart from initially setting the PIN code and cognitive question(s), this will remove any requirement to generate any templates, which given the number of input scenarios, could take a significant period of time to setup, with the secondary and subsequent effect of ensuring the input data is truly representative of the natural users device interaction. However, it is likely that some biometric templates maybe generated during device registration, such as facial recognition. If the device has the hardware available, several images of the user can be taken whilst the user is setting the cognitive responses and can be subsequently used to generate the template.

The nature and storage of the user's input data within the Profile storage element is illustrated in the tables below. The Profile storage element contains two types of information. The first is a Biometric Template database containing a list of biometric templates that have been generated, including re-train dates and file location of the template. It is this table which both the Biometric Profile Engine and Authentication Engine will utilise in order to re-train algorithms and perform authentication requests.

ID	Date	Retrain Date	Technique	Technique Sub-Category	Threshold Scale	Template Storage
1	10/06/04	24/11/02	Keystroke	Static: 4	1	\\profile\template\keystroke_4
2	15/06/04	N/A	Keystroke	Cognitive	1	\\profile\template\keystroke_cog
3	19/06/04	N/A	Keystroke	Static: 5	1	\\profile\template\keystroke_5
4	19/06/04	N/A	Voice	Static: 2	1	\\profile\template\voice_static_1
5	21/06/04	N/A	Keystroke	Static: 11	1	\\profile\template\keystroke_11
6	23/06/04	25/11/03	Facial		1	\\profile\template\face
7	25/06/04	N/A	Voice	Static: 4	1	\\profile\template\voice_static_4
:	:	:	:	:	:	:

Table 6.2: Biometric Template Database

The second type of information consists of a series of tables which contain the raw input data from the authorised user. One master table is present for each biometric technique that exists on the device, containing the file location of the raw data. For keystroke analysis this means another database containing each of the various sub-categories of technique, as illustrated in Table 6.3. For facial and voice verification, the file locations pin-point the original (pre-processed) image and sound files, as illustrated in Table 6.4 and Table 6.5 respectively. In addition to the biometric tables, a cognitive response table is also required to store a users' cognitive questions and answers, from which samples can be subsequently compared.

ID	Date	Time	Sub-Category	File Location
2	20/11/03	14:48	Static: 4	\\profile\keystroke\keydata.mdb - PIN Table
3	22/11/03	10.03	Dynamic	\\profile\keystroke\keydata.mdb - Tele Table
4	23/11/03	13:01	Character	\\profile\keystroke\keydata.mdb - Char Table
:	:	:	:	:

Table 6.3: Profile Storage: Keystroke Dynamics

ID	Date	Time	File Location
1	19/11/03	09:32	\\profile\face\raw1.jpeg
2	20/11/03	14:48	\\profile\face\raw2.jpeg
3	22/11/03	10.03	\\profile\face\raw3.jpeg
:	:	:	:

Table 6.4: Profile Storage: Facial Recognition

ID	Date	Time	Sub-Category	File Location
1	19/11/03	09:32	Static: 10	\\profile\voice\raw1.wav
2	20/11/03	14:48	Static: 4	\\profile\voice\raw2.wav
3	22/11/03	10.03	Dynamic	\\profile\voice\raw3.wav
:	:	:	:	:

Table 6.5: Profile Storage: Voice Verification

ID	Date	Time	Cognitive Question	Cognitive Response	Keystroke Enabled	Template Generated
1	19/11/03	09:32	Date of Birth	19/05/78	True	12/06/04
2	20/11/03	14:48	PIN	354621	False	
3	22/11/03	10.03	Mothers Maiden Name	Kent	True	14/06/04
:	:	:	:	:	:	:

Table 6.6: Profile Storage: Cognitive Response

A user's input data is stored even after template generation, so that the biometric algorithms can perform re-training in order to achieve a better performance rate. However, a limit will exist on how much data the system wishes to store and for how long – as user's characteristics will change over time and early input samples may not still be suitable. As such the system administrator will need to define a period of storage – which in a standalone scenario is likely to be largely dependent upon the storage capabilities of device.

The biometric template database also contains a column referred to as the "Threshold Scale". This is a numerical scale which permits the framework a level of flexibility with regard to the threshold setting of the numerous biometric techniques. The threshold level, as discussed in detail in Chapter 3, determines the level of security provided by a biometric approach versus inconvenience – as too higher a security level would result in the authorised user being falsely rejected more often. In practice, the setting of this threshold tends to prove problematic. Setting a threshold level of 0.8 might work well for one user but not another, and neither does this value translate into a meaningful performance level. In principle, the main method of setting the threshold level is determined by the security setting for an individual, whether it is set to high, medium or low. It is suggested that these threshold settings are calculated based upon:

$$Medium = Average\_Output\_Level\_Of\_Samples = \frac{\sum Ouput\_Level\_Of\_Sample}{No\_Of\_Samples}$$

With the low and high level settings based upon the average +/- the difference between the average output level and the highest output level achieved divided by two.

The authentication samples will vary in nature dependent upon the biometric techniques available to a particular mobile device. Within a third generation mobile handset, it is envisaged this data will include facial images, timing vectors and voice waveforms, in addition to cognitive responses or password based data. If the client-server topology is defined, where some or all of the authentication techniques are performed locally, then it is imperative the Communications Engine performs biometric template synchronisation to ensure the most up to date and relevant template is being employed. Authentication Response and System/Client parameters allow server and client to know what mode of operation they are working in, which side performs authentication and for which authentication techniques. For instance, it would be plausible to perform the less computational complex functions, such as password/cognitive response verification, on the mobile device, reducing network overhead, but leave the server to perform the more complex biometric verifications. Although not defined by this mechanism it is assumed the communication and storage of the biometric samples are performed securely to ensure no manipulation of the templates can occur. The Communications Engine also enables the server to provide feedback to the user, either through requesting they intrusively authenticate themselves or via a Security Status – a mechanism that enables the user to monitor the protection provided to the device.

6.3 System Components

This section addresses the various remaining components of the framework (with the exception of the Authentication Manager), which helps to provide the system parameters and define the authentication techniques. This section is split into the following:

- Security Status
- Intrusion Interface
- Authentication Assets
- System Parameters & Administration
- Authentication Response Assignment

6.3.1 Security Status & Intrusion Interface

The Security Status and Intrusion Interface components represent the two output processes of the framework. The Security Status simply provides information to the end-user regarding the level of security currently provided by the device, the success or failure of previous authentication requests and the System Integrity. Although it is perceived that the majority of users will have no interest in viewing this, it is included as an informational guide to the user.

Each mobile device must be able to establish the level of security with which it can provide. This is achieved by determining which authentication techniques are currently enabled (i.e. have a template generated or/and password enabled). As the performance of biometric techniques varies (as identified in Chapter 3) a process is required to ensure weaker authentication techniques do not compromise the level of security. To this end, each of the authentication techniques is given a confidence level depending on the error rate. As illustrated in Table 6.7, the confidence levels are separated into two types, those concerned with biometric techniques and those based on secret knowledge techniques. The biometric techniques are categorised on their published false acceptance rate for the

system[7], with the system having more confidence the lower the FAR. The secret knowledge techniques are split into two levels, P0, which represents PIN, password or cognitive based responses, and P2 which represents the administrator password or the PUK code in cellular network terms.

Biometric		Secret Knowledge	
Confidence Level	FAR Level	Confidence Level	Input Required
B0	10-20%	P0	PIN/Cognitive
B1	5-10%	P1	PUK (Operator)/ Administrator Password
B2	2-5%		
B3	0-2%		

Table 6.7: Confidence Level Definitions

These confidence values are also used in determining what level of the security the device is able to provide. As illustrated Table 6.8, a security level of 'excellent' is given to the device if the device is capable of providing a biometric authentication with a confidence level of B3. The PIN Only security level is used as an indication of secret knowledge level security only – it does not mean it has a lower security level than B0, but just that only PIN/password security is available.

Security Level	Confidence Level
Excellent	B3
High	B2
Medium	B1
Low	B0
PIN Only	P0

Table 6.8: Security Level of Mobile Device

The security level is only an indication of the potential security the device is able obtain and not of what the current security level is – this is achieved through the use of a System Integrity measure. The security level of a device could be used by manufacturers and/or

[7] Not on individual performances

network operators as a selling point. The System Integrity is one of two key processes working at the core of the framework to maintain security. It is a sliding numerical value between -5 and +5[8], with -5 indicating a low security, 0 a normal 'device switch-on' level and +5 indicating a high security level. The System Integrity changes depending upon the result of authentication requests and the time that has elapsed between them. Each of the confidence levels are given a number which is added or subtracted from the System Integrity dependent upon whether the technique has passed or failed the input sample, up to a defined maximum level. This System Integrity level is a continuous measure increasing and decreasing over the time of a user's session. Table 6.9 illustrates by how much the System Integrity level is to be increased or decreased for each of the confidence levels. The maximum System Integrity level is included to ensure a user is unable to achieve the higher integrity levels by utilising techniques with relatively high false acceptance rates (i.e. those with lower confidence levels – B1, B0). This ensures a user with a System Integrity Level of 5 has not only had consistent successful authentication requests during their session, but has also recently been authenticated by a biometric technique with a confidence value of B3.

Confidence Level	Increment/Decrement Value	Maximum System Integrity Level
P1	None – System Integrity set to 0	NA
P0	NA	NA
B3	2	5
B2	1.5	4
B1	1	3
B0	0.5	2

Table 6.9: System Integrity Changes

[8] The boundaries defined on the numerical scale are only provided as a suggestion. Practical evaluation might result in a redefining of these limits.

The secret knowledge confidence levels have a somewhat different role. P1 has the effect of resetting the System Integrity level – since in a client-server topology, P1 represents the network administrators overriding the password (or PUK code in cellular terms). In a standalone topology, typing P1 would either unlock the device or give access to the host administrative settings. The P0 level is only required in two scenarios – if no biometric approaches are available for use (in which case the Authentication Manager will resort to providing a basic level of security through the use of the PIN, password or cognitive response), and secondly as a means of providing two-factor authentication – the PIN or password is used in conjunction with keystroke analysis to verify the authenticity of the user. In this special situation, whatever the confidence value of the respective keystroke analysis technique, if successful, the level is increased by 1 (up to the maximum of B3) – as this represents a multi-modal approach, referred to specifically as a hardened password.

The period of time that has elapsed between authentication requests also affects the System Integrity level. In order to ensure that devices remaining unused for a period do not continue to have a high integrity level, which could be subsequently misused by an impostor to access more sensitive information and expensive services, the integrity level begins to decrease overtime. The actual period is to be configurable on a per user basis through the administrative settings – frequent users could benefit from a lower period (such as 30 minutes) and infrequent users with a slightly longer period (such as 50 minutes). After each defined period of misuse the System Integrity level decreases until the normal security level of 0 is reached. In practical terms this means a mobile device with a period of 30 minutes set and the highest integrity level of 5 will take 2 hours 30 minutes to decrease down to a normal integrity level. Negative System Integrity values however remain until a subsequent authentication request changes it (for the better or worse) or the P1 level code is entered.

The Intrusion Interface is required on the occasions when the identity of the user needs to be verified before continuation of services. Although the framework is designed to operate in a non-intrusive manner, there are occasions when the user will be required to authenticate themselves, typically when the system has already non-intrusively and unsuccessfully attempted to authenticate the user several times – see section 6.4 for an explanation as to when these occasions arise. The interface itself, and how it operates, will vary between devices and operating systems depending how complex the system is and what resources are available to it – e.g. whether the device has the ability to control file accesses. On simple devices it might just remove the option of going into a specific sub menu with a subsequent message advising of the reason why. On more complex devices, where the underlying operating system is more complex, a more comprehensive interface will be required to lock out the necessary controls.

6.3.2 Authentication Assets

The Authentication Assets are a detailed breakdown of the authentication mechanisms available to the Authentication Manager for a particular mobile device, and include both biometric and secret knowledge based approaches. The information contained within the Authentication Assets is used by the Authentication Manager to determine which techniques are supported, and in particular, which techniques have templates generated and what the corresponding confidence levels are for the technique. This enables the Manager to decide upon which technique, given the contents of the Input Cache, would be most appropriate for use in subsequent authentication. Within the client-server topology the Authentication Assets for a client are stored within the Client Database.

As a wide range of mobile devices exist, which differ in terms of their hardware configuration and operating system, it becomes implausible to design an authentication mechanism that will automatically work on all devices. The difficulty is enabling the framework to plug-in to the different operating systems, particularly the software interfaces of the Data Collection Engine and the Intrusion Interface. Although the framework is system- and device-independent in its approach to authentication security, the practical nature of utilising different operating systems would require both OS and hardware vendors to co-operate on implementing the framework in the first instance. The Authentication Assets would represent a list of compatible authentication techniques for a mobile device, as illustrated in Table 6.10. The Authentication Assets table is populated as biometric samples are collected and templates created.

ID	Technique	Technique Sub-Category	Topology	Device/Network Compatibility	Template Gen Date	Confidence Level	Intrusive
1	Cognitive	Phrase #	Both	True	-	B2	True
2	EAR		-	-	-	B0	True
3	Face		-	-	-	B1	True
4	Finger		-	-	-	B0	True
5	Keystroke	Static #	Both	True	-	B2	False
6		Dynamic	Both	True	18/07/2003	B3	False
7	PIN		Both	True	12/07/2003	P0	True
8	Signature		-	-	-	B2	False
9	Voice	Static #	Server	True	15/07/2003	B2	False
10		Dynamic	Server	False	-	B3	True
:	:	:	:		:	:	:

Table 6.10: Default Authentication Assets: Compatibility Table

The Technique and Sub-Category columns of the table define all the BioAPI compatible devices along with the secret-knowledge approaches – although the Technique column is fixed by the number of BioAPI compatible devices. This list is able to grow in terms of the Sub-Category, as the framework captures more static input data. The Topology column determines where the authentication techniques are enabled (i.e. standalone, server, both) and are defined by the hardware vendor (as the OS is an integrated part of the device). The

Device/Network compatibility column enables the administrator (particularly in a client-server topology) to disable any of the techniques that are enabled by the Hardware Compatibility – this may be desirable for a user who has difficulty in using a particular technique or for network related reasons – the technique can then be disabled in order to improve user convenience. The remaining columns in the Compatibility table indicate whether a valid template has been generated, what the corresponding confidence levels are for the biometric techniques, and whether that technique can be utilised in an intrusive authentication request.

The second table within the Authentication Assets is an Algorithm Location table, as illustrated in Table 6.11. The ID value within the Compatibility table corresponds to the ID value in the Algorithm Location table, which details the file location of each of the authentication techniques library file. It is these library files which contain the procedures for pre-processing, template generation and authentication.

ID	Server DLL Location	Client DLL Location
1	\\server\library\secret.dll	\\client\library\secret.dll
2	\\server\library\ear.dll	\\client\library\ear.dll
3	\\server\library\face.dll	\\client\library\face.dll
4	\\server\library\finger.dll	\\client\library\finger.dll
5	\\server\library\secret.dll \\server\library\keystroke.dll	\\client\library\secret.dll \\client\library\keystroke.dll
:	:	:

Table 6.11: Authentication Assets: Algorithm Location Table

In a standalone topology the above tables are all that are required to provide the hardware dependent information to the framework. However, in a client-server topology, a network is very likely to consist of a varied number of different mobile devices to which the framework will have to adapt, ensuring a high level of security given any combination of hardware. To this end a Hardware Compatibility Database (HCD), as illustrated in Table

6.12, is included in the server architecture to provide a list of all compatible devices, along with specific information about which authentication techniques are available.

ID	Manufacturer	Device Model	Part #	Sever-Side						
				Cognitive	EAR	Facial	Finger	Keystroke	Password	Voice
1	HP	3867	C5647A	Enable	Disabled	Enabled	Enabled	Disabled	Enabled	Enabled
2	Nokia	6210	543897	Disabled	Enabled	Enabled	Disabled	Enabled	Enabled	Enabled
:	:	:	:	:	:	:	:	:	:	:

Client-Side						
Cognitive	EAR	Facial	Finger	Keystroke	Password	Voice
Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled
Disabled	Disabled	Enabled	Disabled	Enabled	Enabled	Enabled
:	:	:	:	:	:	:

Table 6.12: Hardware Compatibility Database

This will enable the framework to create an Authentication Asset tables on an individual basis, where each class of device will have an independent table, which the administrator is able to customise.

6.3.3 System Administration & Authentication Response

In order to achieve a commensurate level of security versus user convenience, for a given mobile device, the framework allows a device administrator to define a number of system parameters. These include:

- enabling or disabling IAMS (per device or per user);
- individual enabling/disabling of authentication techniques;
- determining the processing split between client and server (in the network version only);
- Input Cache raw data period;

- profile storage of raw data period;
- System Integrity period;
- manual template generation/re-training;
- monitoring Authentication Requests;
- monitoring System Integrity Levels;
- security level – high, medium, low (has an effect on the threshold values chosen for the biometric techniques);
- topology – standalone or client-server.

In addition to the above parameters, the device administrator is also permitted to define the Authentication Response table. The table, as illustrated in Table 6.13, defines a number of key services that the device can access, including bank accounts, share dealing, micro-payments and expensive video calls with a corresponding System Integrity, Confidence Level and (where applicable) Location Access. In order for a user to access any of the services listed they must have a System Integrity level greater or equal to that specified. If not, the user will be subsequently required to authenticate themselves using an authentication technique with the corresponding Confidence Level in order to proceed with the service. If they are unable to obtain the required Confidence Level, the service will remain inaccessible to the user.

The purpose of the Authentication Response table is to ensure key services and file locations are protected with a higher level of security than less private information or cheaper services. For example, it is unlikely you would require the same level of security for preventing a user sending a text message than accessing their bank account details. Determining which service or what information the user is accessing at any particular

moment is achieved by the Authentication Manager, via the System Monitor in the Data Collection Engine.

Service	System Integrity Level	Confidence Level	Location Access (if applicable)
Bank Account Access	=>4	B3	http://hsbc.co.uk
Downloading Media Content	=>3	B2	
Media Message	=>1	B1	
Micropayments	=>4	B3	
Share Dealing	=>4	B3	http://sharedeal.com
Text Message	=>-1	B0	
Video Call (International)	=>2	B2	
Video Call (National)	=>1	B1	
Video Call (Other Cellular Networks)	=>2	B2	
Voice Call (International)	=>2	B2	
Voice Call (National)	=>0	B0	
Voice Call (Other Cellular Networks)	=>1	B1	
:	:	:	:

Table 6.13: Authentication Response Table

For mobile devices without a B3 level of security, the administrator is left with two possibilities:

1. To lower the System Integrity levels within the Authentication Response table appropriately, although this is not recommended as it would lower the security of the device.
2. To intrusively request the user to authenticate themselves each time they wish to use the most sensitive services, using a cognitive response and keystroke analysis approach (otherwise known as a hardened password).

In a standalone topology, access to the administrative settings and Authentication Response table require the highest security setting, as unauthorised access would invalidate the integrity of the system and permit the impostor to set low security setting for sensitive and expensive services. As such, the user is required to pass either a technique with a B3

confidence level or a two-factor authentication mechanism, as previously described, in order to access this information.

In a client-server topology, the administrative settings and authentication response table will be defined by the network administrator – thereby removing any chance of impostor misuse – optionally the client will still be able to view (in read only format) a number of security settings through the Security Status interface.

6.4 Authentication Manager

The Authentication Manager is the central controlling element of the framework, with control over the process engines and intrusion interface. The role of the Authentication Manager includes:

- determining the topology and administrative setting;
- generating and maintaining the System Integrity level;
- requesting profile generation and retraining;
- making authentication requests, both intrusive and non-intrusive;
- determining what subsequent action should be taken, given the authentication result;
- determining whether a user has the required System Integrity level;
- requesting removal and lock down of services and file locations;
- use and maintenance of the Authentication Assets.

However, the principal task of the Authentication Manager is to determine when to make an authentication request and decide on what subsequent action to take. The type of request is based upon two factors; what input samples have been captured recently – which the Authentication Manager knows via the Data Collection Engine, and which authentication mechanism would be best to use – this is determined from the Authentication Assets. The decision will be essentially based upon the most recent input sample with the best performance rate, with "recent" being defined administratively but suggestively in the region of 2-4 minutes – obviously a window of compromise exists between a technique with a higher confidence level and whose sample was taken earlier than a technique with a lower confidence level. This is solved by the Authentication Manager Process Algorithm, which also determines what action to take after the authentication request, as illustrated in Figure 6.5.

The Process Algorithm is the second of the key security process working at the core of this framework (the System Integrity level being the other). The Process algorithm has four stages of authentication security (depicted in Table 6.14, and dependent upon the result of authentication responses) with the level of authentication security being increased until the device is locked (requiring an administrative password or PUK code from a cellular network provider). The number of stages was determined by a compromising between requiring a good level of user convenience and better security. Through mixing transparent and intrusive authentication requests into a single algorithm it is expected that the majority of authorised users will only experience the transparent stages of the Process algorithm. The intrusive stages of the algorithm are required to ensure the validity of the user utilising the stronger authentication tools before finally locking the device from use. The difference between intrusive and transparent authentication requests is identified in the algorithm. The

intrusive authentication requests require the user to provide a biometric sample of confidence value B3 or B2 (whichever is available and higher).

Authentication Security Level	Description of Alert
1	Normal
2	Authenticate on Users Next Input
3	Request Entry of a B3/B2 Level or PIN/Cognitive Question
4	Lock Handset – Requires Unlock code from Network Operator

Table 6.14: Authentication Security Level Descriptions

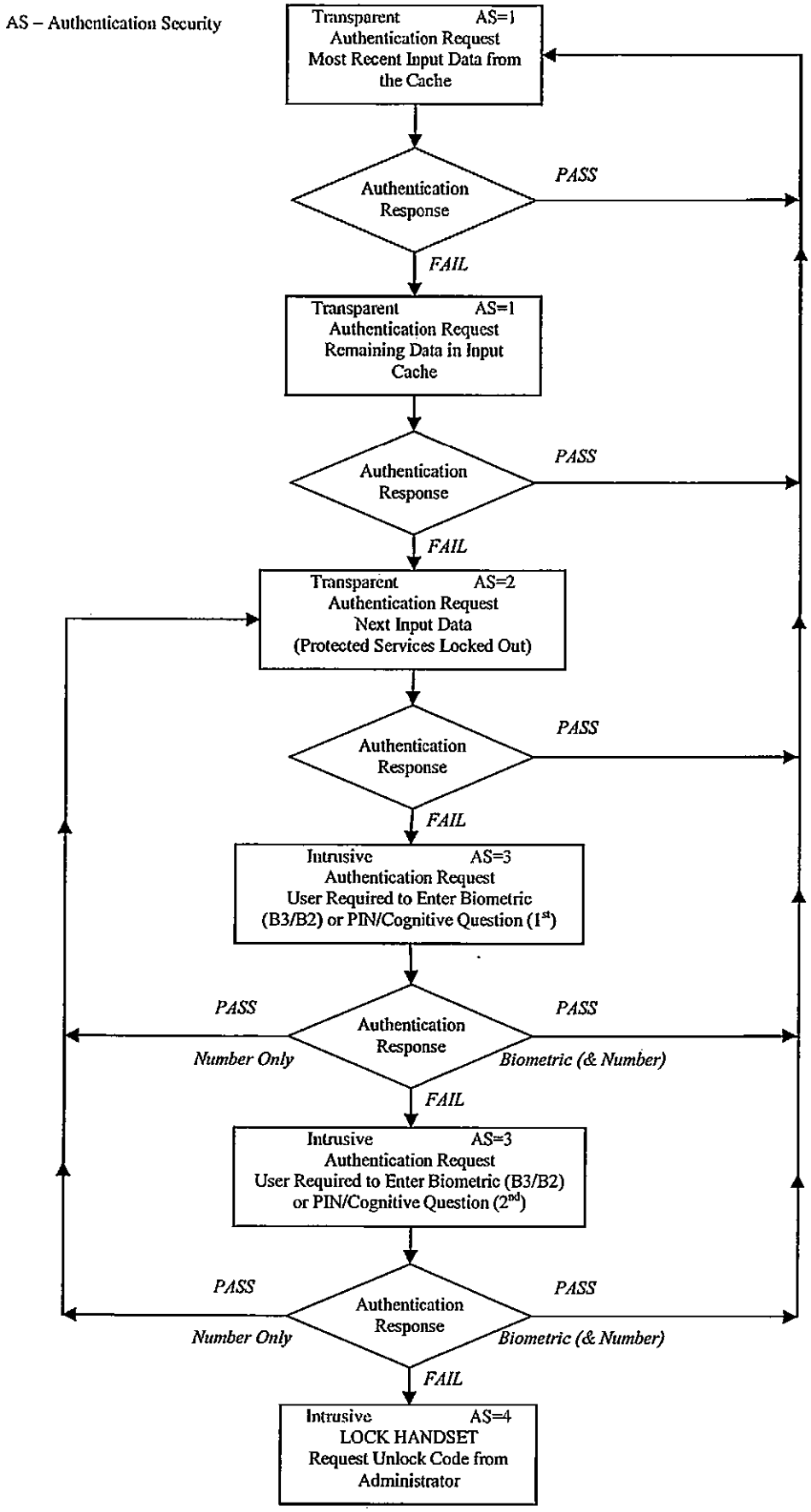


Figure 6.5: Authentication Manager: Process Algorithm

The general operation of the Authentication Manager is to periodically send an authentication request to the Authentication Engine, where periodically is definable administratively, but would by typically in the range of 10-25 minutes, and in practice also a function of usage. The Authentication Engine will subsequently retrieve the last and highest (in terms of confidence value) set of user's inputs (i.e. a camera image from a video conference call or a sound file from voice dialling) from the last *x* minutes (where x is also definable administratively, but would typically be in the region of 2 minutes). If the Authentication Engine passes the input, the Authentication Manager goes back into a monitoring mode. If not, then the Authentication Manager performs an authentication request again, but using the remaining data from the Input Cache from the last *y* minutes (where y is definable administratively, but would typically be in the region of 5 minutes) – using the highest confidence level technique. If no additional data is present or the response is a fail, the Authentication Manager increases the security level and will request authentication on the next input sample to the device – the user would now not be able to use any of the protected services until this stage had been completed. If the user passes this, or any of the previous stages, then the Authentication Manager goes back into a monitoring/collection mode. If the Authentication Engine responds with a fail then the Authentication Manager will request the user to authenticate themselves – the first intrusive authentication request. The Authentication Manager, via the Intrusion Interface, will use a biometric technique with a confidence value of B3 or B2 (whichever is higher) in order to minimise the risk of a false acceptance. If no biometric techniques or templates exist with a confidence value of B3 or B2, then the user will be requested to enter their PIN, password or answer a cognitive question. If they pass this, and the PIN or password has a corresponding keystroke analysis template, then this will also be utilised in order to provide a two-factor authentication mechanism. If the keystroke analysis template exists, and the user passes the biometric authentication, then the system will revert back to a

monitoring mode. If the biometric fails, or the template does not exist, then the technique will remain at a heighten security level of 2 – where the Authentication Manager will request authentication on the next available input sample. If an intrusive authentication request is passed, the previous biometric samples that were failed are deemed to be in fact from the authorised user and incorrectly failed. As such, these samples are added to the Profile database for subsequent re-training and are not deleted.

The Process algorithm is inherently biased toward the authorised user as they are given three non-intrusive chances to authenticate correctly, with two subsequent additional intrusive chances. This enables the system to minimise any user inconvenience from the authorised user aspect. However, due to the trade-off between the error rates, this has a detrimental effect on the false acceptance rate, increasing the probability of wrongfully accepting an impostor every time an authentication request is sent. With the Process algorithm in mind, for an impostor to be locked out of the device they must have their authentication request rejected a maximum of 5 consecutive times. However, this is where the System Integrity has a significant role. The probability of an impostor continually being accepted by the framework becomes very small as the number of authentication requests increase. This would indicate that the impostor will be identified correctly more often that not (even if not consecutively as required by the Process Algorithm), reducing the System Integrity value to a level where the majority if not all of the services and file access permissions have been removed – essentially locking the device from any practical use.

The System Integrity comes into operation when a user attempts to access a protected service or file location. If they do not have the required integrity level, the Authentication Manager will intrusively request the user to authenticate themself using an authentication

technique with the required confidence value to permit access to the file or service – which is dependent upon the Authentication Response table. In this case, should the security level of the Process algorithm reside at 1 or 2, the authentication request can be used as the next authentication request in the Process algorithm. Should the request succeed then the user is given access to the information or service they require. However, should the request fail, the user will be blocked from using the file or service and the Process Algorithm will proceed to the next stage. The trade-off existing within this architecture is between user convenience and device misuse. Although an impostor will not be rejected from the system immediately under this process, the degree of misuse has been limited by the presence of the System Integrity. In a practical situation, it is likely an impostor will be able to make a telephone call or send a text message before the system locks down (the actual range of services available to the impostor will largely depend upon the Authentication Response table). However, all of the key sensitive and expensive services will be locked out of use. By permitting this limited misuse of the device, it is possible to achieve a much higher level of user convenience at minimal expense to the security.

The remaining duties of the Authentication Manager are mainly concerned with control, such as sending a template generation and retraining request to the Biometric Profile Engine (during computational non-intensive periods in a standalone topology) to update the biometric profiles and subsequently updating the Authentication Assets as a result. The client side Authentication Manager will also monitor (via the Communications Engine) the network connectivity to the server – should connection be lost at any stage, the client-side will revert into a standalone configuration, thereby achieving autonomous operation. This could be useful in a number of situations, such as a poor network signal, network failure and when roaming on other networks – which might not have the framework implemented.

6.5 Conclusion

The framework has been designed in a modular and robust manner to enable network administrators the flexibility and convenience of configuring a composite authentication mechanism to meet their specific requirements.

The mechanism has been designed on the principle that no single authentication approach is 100% reliable, whether it is because of technical issues or even lack of use due to user inconvenience. Through adding a level of intelligence to the authentication process, it is no longer a matter of providing a pass or fail response to the identity of a user, but a probability level indicating the confidence the system has in the identity of the user, with the system's behaviour dependent upon the result. With a low probability, the system removes automatic access to key services and information and increases the level of monitoring of the user. With a high confidence level, the user has the ability to interact and access the complete range of services and applications provided by the mobile device without hindrance.

The next chapter discusses a possible architecture for this composite authentication mechanism and proceeds to describe the implementation, design and evaluation of a functional prototype based upon this architecture.

7 IAMS Architecture & Prototype

The Intelligent Authentication Management System (IAMS) is a comprehensive, robust and scalable user authentication architecture for mobile devices. Based upon the framework presented in Chapter 6, the architecture solves the problem of weak, insecure and inconvenient user authentication that typically resides on such devices by incorporating transparent biometric authentication of the user. This chapter discusses the architectural specification of the composite authentication mechanism, and proceeds to present a functional prototype of the system.

7.1 Introduction

The focus of this thesis has been towards the development of a more secure authentication mechanism for mobile devices, capable of surpassing the hardware limitations imposed by such devices, to provide a flexible, transparent and continuous authentication approach. The sections that follow introduce a possible architecture for this framework and discuss the design and development of a functional prototype.

7.2 IAMS Topology

The architecture can operate in two topologies. It can operate as a client-server and as a standalone system, enabling IAMS to operate completely autonomously. As a client to the server, the device provides the input sample capturing and intrusion response interface (e.g. locking down a device in the presence of a suspected impostor) with all the computational power and control provided by the server. In a standalone mode, the device performs all of the IAMS operations by itself, with no network connection. The two topologies allow IAMS to be useful for both wireless and non-wireless devices, with the ability to dynamically switch between the two client modes. This permits wireless networks, such as cellular networks, to control authentication security by operating in a client-server mode, but also allow individual mobile users and cellular users with no network coverage the advantage of increased authentication security[9].

[9] The security of the topology, in terms of being able to circumvent and by-pass this architecture will not be discussed. It is assumed that the architecture will be deployed in an environment that prevents this; for instance, through the encryption of biometric samples and correct integration of IAMS in the mobile devices own security architecture.

From an architectural perspective there are few differences between the two topologies, with the server-client configuration splitting the computational and control overhead from the client onto the server. However, it is worth noting that the standalone configuration is unlikely to support the same number of authentication techniques as the server-client due to the reduction in computing power. The degree of split in computation is dependent upon the implementation – with the network administrator determining how much processing gets done at the server and the client.

7.2.1 IAMS Server Architecture

The architecture, illustrated in Figure 7.1, outlines the functional components of the server topology. All of these components and their operation have been drawn directly from the composite authentication framework. The Authentication Manager has overall control of the authentication system, determining both when authentication should take place and what the current state of security is. The process engines provide the computational power of the system, with an Authentication Engine to authenticate users, a Biometric Profile Engine to generate and train the relevant biometric templates required for subsequent classification, and a Communications Engine to communicate and synchronise data with the client device. To supplement these process engines, a number of storage elements are utilised. As the OS and hardware on mobile devices tend to vary considerably, devices will not automatically be supported. The Hardware Compatibility database contains information about which mobile devices are configured to work with the architecture, along with a list of supported biometrics. The system administrator will utilise this information, in addition to a number of system parameters to generate a client profile, which is stored in the Client database. This database holds a master list of clients enabled,

The device topology does however introduce a number of additional components that provide the input and output functions of the system. The fourth process engine in the form of the Data Collection Engine is included on the device topology and provides the input mechanism, which collects and processes users' device interactions. The output components consist of an Intrusion Interface and Security Status. The former as described in Chapter 6 provides the IAMS to OS connection for restricting user access and provides user information as and when required, and the latter provides an overview to the system integrity and security of the device.

Depending on which topology the device is in, the architecture will slightly differ with a number of the architectural components not required. For instance, in a standalone topology the device has no use for the Communications Engine – as no network exists to which it can connect. In a client-server topology the components not required will vary depending upon the processing split between the server and client. There are numerous reasons why a network administrator may wish to split the processing and control of IAMS differently, such as network bandwidth and availability, centralised biometric template storage and processing, and memory requirements of the mobile device. For example, in order to minimise network traffic, the network administrator may require the host device to perform the authentication process of user samples locally on the device, or conversely, the administrator may wish the device to only perform pre-processing of input samples and allow the server to perform the authentication, thus removing the majority of the computational overhead from the device, but still reducing the sample size before transmitting across the network. Figure 7.3 illustrates the device topology for the latter example, with the Biometric Profile Engine, Authentication Engine, both storage elements and the Authentication Assets not in use on the device architecture.

7.3 IAMS Prototype Implementation

Given the flexibility of the aforementioned architecture, a number of decisions had to be made concerning which topology to use and what mobile devices to develop the architecture for. It was decided to utilise a client-server topology and simulate a mobile handset environment within a mobile device. This decision was based upon:

- Mobile handsets represent the largest segment of the mobile device market.
- Discussions with Orange PCS, a leading mobile operator and industrial partner of the project, revealed clear preferences towards keeping the intelligence and administrative control within the network rather than the handset. The reason for this decision is based upon wanting to retain control and security over the network.
- The aforementioned biometric approaches currently do not operate within a mobile device. Although IAMS is able to operate without biometrics, the inclusion of them would provide an illustration to the capability and transparency of IAMS. Without biometrics, IAMS can only provide authentication through cognitive responses.

The prototype development of IAMS was divided into three constituent parts:

1. Authentication Manger – providing the entire server-side operational functionality, including, biometric profiling, authentication and data synchronisation.
2. Administrative Console – containing all the administrative and system settings.
3. Client-Side Interface – providing the simulated mobile handset functionality, data capture and intrusion control.

In terms of hardware connectivity, the Authentication Manager runs on a standard PC, with the Administrative Console also able to run on the same PC or on any remote computer. It is an independent application that only requires connection to the IAMS databases. Figure 7.4 illustrates the hardware configuration.

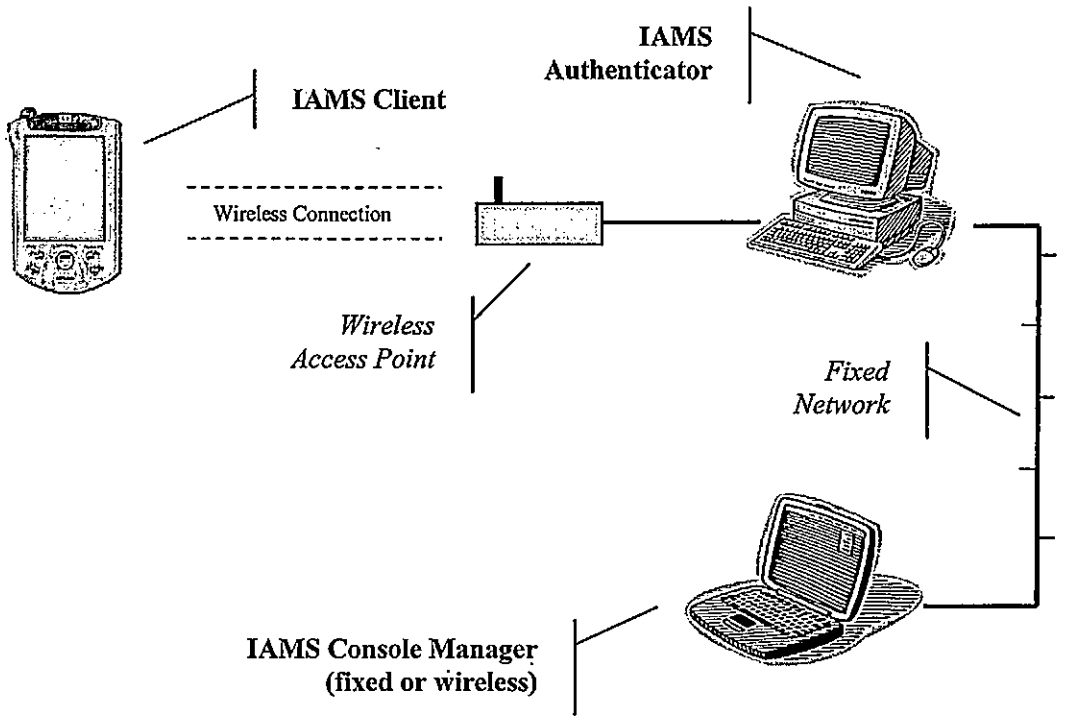


Figure 7.4: IAMS Hardware Configuration

The client has been designed to operate on a HP iPAQ (H5450), with an additional camera and keyboard added to the device to permit facial recognition and keystroke analysis. This configuration was chosen primarily due to the stable development platform and the lack of applicable mobile handsets (or smart phones in particular). The iPAQ was chosen over other PDAs (with built in keypads and cameras) due to availability of the necessary camera Software Development Kit (SDK) that enables control of the camera.

From a topology perspective, the client was developed based upon the topology as illustrated in Figure 7.3. The server-side applications are separated into two distinct

C++. The proceeding sections will illustrate the completed prototype. A copy of the application code can be found in Appendix E.

7.3.1 Authentication Manager

The Authentication Manager represents the largest element of development. Key development milestones included:

- Database creation – IAMS Client, Biometric Profile & Input Cache,
- Data synchronisation and biometric sample analysis – synchronising data and biometric samples. This stage also analysed the biometric samples in order to evaluate the specific type of sample,
- Authentication Process – the connection of a number of data sources to ensure the correct decisions are made,
- File manipulation and database entry and update,
- Incorporation of biometric approaches – enrolment and authentication.

The prototype has integrated two biometric techniques, keystroke analysis and facial recognition. The latter was generously provided by Imagis Technologies in the form of an SDK. Little effort was required in incorporating either technique within IAMS, as standard enrolment and authentication functions were utilised. However, as keystroke analysis on a keypad had not been developed previous to this research study, the technique had to be designed and developed from scratch, before inclusion within IAMS. MatLab was retained as the computational engine behind the technique, with a number of scripts generated to enrol and authenticate a user based upon:

7.3.2 Administrative Management Console

The Administrative Console provides the system level monitoring and configuration of IAMS. The functionality of console can be split into:

- Defining and adding authentication techniques;
- Defining and adding compatible hardware devices;
- Defining and adding client devices;
- Monitoring and parameter settings of current clients.

The application begins by giving an overview of IAMS clients, with information on System Integrity, Authentication Level and current connection status, as illustrated in Figure 7.8.

7.4 Conclusion

The development of IAMS from architecture to development has addressed the requirement of an advanced authentication mechanism. The use of a composite authentication approach provides a robust, transparent method of increasing authentication security beyond traditional point-of-entry systems. The level of authentication security is, however, dependent upon the device and the authentication techniques that can be deployed within it.

From a comprehensive analysis of authentication mechanisms currently available, such as SecureSuite (I/O Software, 2004), AccessMaster (Evidian, 2004), SAFSolution (SafLink, 2004) and BNX's Idenitity Management Suite (2004), IAMS is the only mechanism capable of providing a continuous and often transparent confidence measure for the identity of the user. Although the aforementioned techniques are capable of utilising a number of authentication techniques under a wider authentication mechanism, none are designed for use on mobile devices, and more importantly none are capable of dynamically adjusting to the wide range of techniques across the diverse range of hardware devices.

Having established and developed a composite authentication mechanism, the proceeding chapter will address the validation and evaluation, comparing and contrasting its performance against a number of commercial available authentication techniques.

8 IAMS Evaluation

The chapter evaluates the architecture both theoretically and practically, providing illustrations of typical system behaviour and performance. The chapter concludes by discussing the advantages of IAMS over existing biometric authentication techniques.

8.1 Introduction

Unfortunately, due to the limitations on the prototype development, it was not possible to provide a thorough evaluation of the authentication architecture. In particular, it was not possible to practically deploy and evaluate the mechanism, as the client-side prototype only mimicked the functionality of a mobile handset, so it would not be possible to obtain a user's true interaction with the device, which would subsequently affect the System Integrity level and behaviour of the mechanism. In addition, the lack of available PDAs and restricted network coverage would make a practical deployment difficult and arguably artificial.

The validation of IAMS was therefore achieved by two approaches:

1. The performance of IAMS was evaluated theoretically given predefined performance rates of a number of typical biometric approaches that could be found on mobile devices. A cross section of devices was chosen and the probability of an authorised user and an impostor being rejected and accepted is calculated at a number of key stages in the authentication mechanism.
2. The authentication processes were validated by putting the prototype through a number of prescribed scenarios. Through manually controlling the success or failure of authentication requests, it was possible to validate the underlying security processes working within IAMS.

The proceeding two sections will present the findings of these two processes.

8.2 Theoretical System Performance

IAMS has been designed to operate on a wide variety of mobile devices with differing hardware configurations, subsequently requiring it to utilise a number of different authentication techniques. Some devices will support a multitude of biometric techniques, whereas others will have a limited number of techniques available to IAMS. The varied nature of the authentication techniques on different devices gives rise to IAMS achieving differing levels of non-intrusive and intrusive security. This section describes a number of scenarios involving different hardware configurations in order to demonstrate what levels of authentication security can be expected from IAMS. The hardware configurations chosen are based upon broad examples of mobile device available today, and include a typical 2.5G cellular handset and two PDAs with quite differing hardware features.

In order to make a fair comparison between hardware scenarios, the FAR and FRR will be fixed across the devices, with typical values, as illustrated in Table 8.1, for each of the biometric techniques. The figures for the keystroke analysis techniques were obtained from the results of Chapters 4 and 5, with the remaining results taken from the National Physical Laboratory Biometric Test Report (2001). The number of compatible biometrics was increased beyond the two techniques included within this practical prototype in order to give a clearer illustration of system behaviour and performance.

Biometric Technique	Sub-Category	FAR (%)	FRR (%)
Facial Recognition	-	0.2	7
Fingerprint	-	0.1	6
Keystroke Dynamics	PIN/Cognitive	3	40
Keystroke Dynamics	Text	15	28
Keystroke Dynamics	Telephone	18	29
Voice Verification	-	0.7	4

Table 8.1: Typical Biometric Performance Rates

The analysis will be broken down into two constituent parts – the probability of an authorised user and an impostor reaching the end of the non-intrusive and phone lock stages of the Process algorithm, as indicated by Authentication Levels 2 and 4 respectively in Figure 6.5; and the probabilities involved with the authorised and unauthorised access on the System Integrity measure.

8.2.1 Sony Ericsson T68 Mobile Handset

The hardware found on the T68, as illustrated in Figure 8.1, will permit IAMS to use the following biometric techniques:

- Keystroke Analysis – PIN/Cognitive, Telephone[#], Text[#]
- Voice Verification[#]

[#]*Non-Intrusive Techniques*

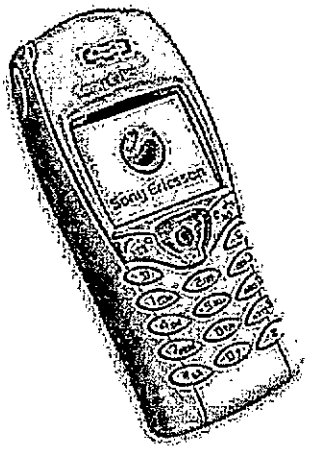


Figure 8.1 Sony Ericsson T68i Mobile Handset

All biometric techniques can perform authentication intrusively. However, those indicated with a *hash* can also perform non-intrusive authentication – which will be required for the early stage of the Process algorithm. For instance, in this particular example the only intrusive technique is the keystroke analysis technique with PIN/Cognitive entry.

The analysis of the non-intrusive stage of the process algorithm, up to Authentication level 2, is illustrated in Table 8.1, with the three scenarios showing a best case; with the probabilities of a user being rejected three consecutive times using the biometric technique with the lowest FAR; a worst case, utilising the biometric technique with the highest FAR, and an intermediate scenario, demonstrating a more practical level of device usage and subsequent probabilities. An example of how these calculations are achieved is given below. These probabilities reduce further after the intrusive stage of the Process algorithm to give a 0.05% probability of an authorised user rejection and 65% probability of an impostor rejection, as illustrated in Table 8.3.

Probability Calculations – Worked Example:

(Intermediate Mode)

Authentication Techniques: *Tele – FAR=18%, FRR=29%*
Text – FAR=15%, FRR=28%
Voice – FAR=0.7%, FRR=4%
PIN – FAR=3%, FRR=40%

Authorised User Being Rejected at AS 2

Probability = *Tele FRR x Text FRR x Voice FRR*
= *0.29 x 0.28 x 0.04*
= *0.0032*
= ***0.3%***

Impostor User Being Rejected at AS 2

Probability = *(1-Tele FAR) x (1- Text FAR) x (1-Voice FAR)*
= *(1-0.18) x (1-0.15) x (1-0.007)*
= *0.6921*
= ***69%***

Authorised User Being Rejected at AS 4

Probability = *Tele FRR x Text FRR x Voice FRR x PIN FRR x PIN FRR*
= *0.29 x 0.28 x 0.04 x 0.4 x 0.4*
= *0.00052*
= ***0.05%***

Impostor User Being Rejected at AS 4

Probability = *(1-Tele FAR) x (1-Text FAR) x (1-Voice FAR) x (1-PIN FAR) x (1-PIN FAR)*
= *(1-0.18) x (1-0.15) x (1-0.007) x (1-0.03) x (1-0.03)*
= *0.6512*
=*65%*

Taking the intermediate scenario, it can be seen the probability of an authorised user being rejected from the system is 0.3% and the probability of an unauthorised user being correctly rejected by the system three consecutive times is 69%.

Scenario	Series of Biometric Techniques	Probability (%)	
		Authorised User Being Rejected at AS 2	Impostor User Being Rejected at AS 2
Best	Voice, Voice, Voice	0.006	98
Intermediate	Tele, Text, Voice	0.3	69
Worst	Tele, Tele, Tele	2	55

Table 8.2: Performance Probabilities of Non-Intrusive Stage of Process Algorithm

Scenario	Series of Biometric Techniques	Probability (%)	
		Authorised User Being Rejected at AS 4	Impostor User Being Rejected at AS 4
Best	Voice, Voice, Voice, PIN, PIN	0.001	92
Intermediate	Tele, Text, Voice, PIN, PIN	0.05	65
Worst	Tele, Tele, Tele, PIN, PIN	0.4	52

Table 8.3: Performance Probabilities of Complete Process Algorithm

The effect of the Process algorithm is to ensure authorised users are not rejected from their own mobile device, however at the detriment of increasing the subsequent false acceptance rate. The probability of an impostor being rejected decreases as they need to be correctly identified five times. However, this is offset by the interaction of the System Integrity monitor. IAMS will only permit access to file locations and services upon certain System Integrity levels – which are only obtainable with a number of consecutively successful authentication requests. Table 8.4 and Table 8.5 illustrate the probabilities of an impostor

obtaining various System Integrity levels given a series of authentication requests by certain biometrics.

Table 8.4 illustrates an impostor's best chance of being accepted and obtaining a +5 integrity level. This is achieved through three voice verifications and a PIN authentication and has a corresponding probability of 0.000001%, or a 1 in 100 million chance. So 99.999999% of impostors will be rejected by the system by that stage – making unauthorised access to a +5 level a highly unlikely event. The probabilities also demonstrate the likelihood of an impostor being continually rejected by the system, with an 95% chance that the impostor will reach an integrity level of -5 – essentially locking the device down. These probabilities also do not take into account the secret knowledge aspect of the PIN authentication; in that the user must have knowledge of the PIN/Cognitive before keystroke analysis is enabled, to provide the two-factor authentication, and thus would further improve the probabilities in practice.

Biometric Technique	Impostor Accepted			Impostor Rejected		
	System Integrity		Probability (%)	System Integrity		Probability (%)
	Before	After		Before	After	
Voice	0	+1.5	0.7	0	-1.5	99
Voice	+1.5	+3	0.005	-1.5	-3	99
Voice	+3	+4	0.00003	-3	-4	98
PIN	+4	+5	**0.000001**	-4	-5	95

Table 8.4: System Integrity Probabilities: Easiest Impostor Scenario

Biometric Technique	Impostor Accepted			Impostor Rejected		
	System Integrity		Probability (%)	System Integrity		Probability (%)
	Before	After		Before	After	
Tele	0	+0.5	18	0	-0.5	82
Text	+0.5	+1	2.7	-0.5	-1	70
Text	+1	+1.5	0.4	-1	-2.5	60
Tele	+1.5	+2	0.07	-2.5	-3	49
Voice	+2	+3.5	0.0005	-3	-4	48
PIN	+3.5	+5	**0.00002**	-4	-5	47

Table 8.5: System Integrity Probabilities: Hardest Impostor Scenario

Biometric techniques with higher FARs can enable an impostor to obtain the lower positive integrity levels, where they can misuse some services for a short period.

In addition to the Process algorithm and System Integrity measure, should an impostor request a service or file location that the integrity level is too low to allow, the user will be immediately requested to authenticate themselves. Upon failure of this request, the service or file location will be refused, the integrity level decreases and the process algorithm will be invoked.

8.2.2 HP IPAQ H5550 PDA

The hardware found on the HP iPAQ (model H5555), as illustrated in Figure 8.2, with additional camera and cellular network access will permit IAMS to utilise the following biometric techniques:

- Facial Recognition[#]
- Voice Verification[#]
- Fingerprint Recognition

[#] *Non-Intrusive Techniques*

Scenario	Series of Biometric Techniques	Probability (%)	
		Authorised User Being Rejected at AS 4	Impostor User Being Rejected at AS 4
Best	Face, Face, Face, Finger, Finger	0.0001	99
Intermediate	Face, Voice, Face, Face, Finger	0.00008	99
Worst	Voice, Voice, Voice, Face, Face	0.00003	98

Table 8.7: Performance Probabilities of Complete Process Algorithm

As the stronger biometric techniques have higher confidence levels, the number of authentication requests required for an impostor to reach a +5 integrity level has decreased, with the subsequent effect of increasing the probability of an impostor reaching the higher +5 level (in relation to the previous cellular handset example). Conversely however, the higher confidence levels lower the probability of an impostor reaching the lower integrity levels, and significantly increase the probability of negative integrity values – with a 99% probability of a -5 System Integrity value, which would lock the device from use.

Biometric Technique	Impostor Accepted			Impostor Rejected		
	System Integrity		Probability (%)	System Integrity		Probability (%)
	Before	After		Before	After	
Face	0	+2	0.2	0	-2	100
Face	+2	+4	0.0004	-2	-4	100
Face	+4	+5	**0.0000008**	-4	-5	99

Table 8.8: System Integrity Probabilities: Easiest Impostor Scenario

Biometric Technique	Impostor Accepted			Impostor Rejected		
	System Integrity		Probability (%)	System Integrity		Probability (%)
	Before	After		Before	After	
Voice	0	+1.5	0.7	0	-1.5	99
Voice	+1.5	+3	0.005	-1.5	-3	99
Voice	+3	+4	0.00003	-3	-4	98
Face	+4	+5	**0.00000007**	-4	-5	98

Table 8.9: System Integrity Probabilities: Hardest Impostor Scenario

With this particular device IAMS is able to utilise very strong authentication techniques giving rise to excellent false rejection and false acceptance probabilities. However, a down-side to a device such as this is the inability for IAMS to obtain the necessary samples non-intrusively – thereby possibly increasing the user inconvenience aspect.

This device fits somewhere in between the two previous examples in terms of the authentication techniques available to IAMS. In its best case scenarios the device can achieve the same non-intrusive results as the HP iPAQ, but with a worst case scenario identical to the cellular handset. This device does, however, offer more combinations of non-intrusive technique, as indicated previously, with three techniques (4 algorithms) available for use. As such, a couple of intermediate scenarios have been included so that a more comprehensive result can be shown. The two intermediate scenarios illustrate a difference in probabilities that can be obtained non-intrusively, depending upon what input samples are available, with an authorised user rejection probability ranging from of 0.06% to 0.08%, and an impostor rejection probability ranging from 70% to 81%. With the addition of the intrusive stage of authentication these probabilities reduce to 0.0002-0.02% and 81-67% respectively. These intermediate results are better than the results from the cellular handset and are achievable in a larger number of non-intrusive approaches, suggesting the more techniques available to IAMS the better level of security it is able to provide for a given level of user inconvenience.

Scenario	Series of Biometric Techniques	Probability (%)	
		Authorised User Being Rejected at AS 2	Impostor User Being Rejected at AS 2
Best	Face, Face, Face	0.03	99
Intermediate 1	Tele, Voice, Face	0.08	81
Intermediate 2	Tele, Text, Face	0.06	70
Worst	Tele, Tele, Tele	2	55

Table 8.10: Performance Probabilities of Non-Intrusive Stage of Process Algorithm

Scenario	Series of Biometric Techniques	Probability (%)	
		Authorised User Being Rejected at AS 4	Impostor User Being Rejected at AS 4
Best	Face, Face, Face, Face, Face	0.0002	99
Intermediate 1	Tele, Voice, Face, Face, Voice	0.0002	81
Intermediate 2	Tele, Text, Face, Face, PIN	0.02	67
Worst	Tele, Tele, Tele, PIN, PIN	0.4	52

Table 8.11: Performance Probabilities of Complete Process Algorithm

The probabilities associated with the System Integrity level are identical to results in previous devices, with the easiest impostor scenario obtaining a +5 level identical to the HP iPAQ (refer to Table 8.8), and the hardest impostor scenario achieving a +5 level identical to the cellular handset example (refer to Table 8.5). The best result showing a probability of 0.0000008% (1 in 125 million) of achieving a +5 integrity level and a 99% of chance of achieving the opposite -5 level, thus the ability for an impostor to obtain a system integrity level at which significant harm could be experienced is theoretically small.

An analysis of the probabilities across all three hardware configurations raises the question regarding how much an impostor can misuse a device using only the lower System Integrity levels – since as previously discussed, the lower the confidence value associated with a biometric technique, the higher the probability an impostor is able to achieve the lower integrity levels. The amount of misuse is solely dependent upon the Authentication Response table, which describes what integrity level is required to access a particular service and or file location.

It has been demonstrated, that although the Authentication Process algorithm has the effect of minimising the inconvenience factor from authentication of the authorised user, it has the subsequent effect of increasing the false acceptance rate. The use of a System Integrity measure in addition to the Authentication Response table will assist in minimising the amount of unauthorised access before the system effectively shuts the user out. Having theoretically illustrated the operation of these security mechanisms, the next stage is to ensure their correct deployment within the prototype.

8.3 Practical Validation of Prototype

The validation of the prototype involves ensuring both the security mechanisms operating within IAMS are functioning as specified. Unfortunately, given the flexibility of IAMS and the numerous combinations of intrusive and transparent authentication requests and different authentication tools, it would not be plausible to test every configuration. The particular mechanisms tested are:

- the Authentication Process, and
- the System Integrity level.

To validate these processes, IAMS was put through four predefined procedures to ensure the system performed as expected. The procedures were designed to test the extremities of the security mechanisms. The first three were used to monitor the behaviour of both processes, with a fourth aimed at specifically monitoring the system integrity measure. These procedures are defined below:

1. Repeatedly dial a telephone number, passing all authentication requests. This procedure was re-run with every authentication request failing. This test represented a typical telephony interaction, where under the IAMS architecture the System Integrity measure would not be permitted to obtain the higher values due to the lower confidence level assigned to the keystroke analysis technique.
2. Repeatedly initiate a video conference call, passing all authentication requests. This procedure was re-run with every authentication request failing. This test permitted

the validation of the facial recognition technique and its affects upon the System Integrity level and Authentication level.

3. Perform a series of handset interactions, passing all authentication requests. This procedure was re-run with every authentication request failing.
    a. Dial a telephone number
    b. Check your bank balance
    c. Compose a text message and send by dialling a number
    d. Make a video conference call

    This procedure represented a series of typical handset interactions that would validate the intrusive authentication process (the user will not have the appropriate System Integrity level to access their bank balance without intrusively authenticating themselves).
4. Repeat procedure 3, failing all non-intrusive authentication requests but passing the intrusive requests. This test represented a user having difficult with the transparent authentication process and ensured the intrusive authentication process was operational.

An example of the output generated by IAMS, given the first procedure, is illustrated below.

Any non-essential output, such as the database connections and initialisation of the biometric modules has been removed. The authentication process has, for debug purposes, been set to 20 seconds. This permits the procedures to be executed rapidly and accounts for a large number of authentication requests present. The system starts with the Authentication Level set to 1 and a System Integrity of 0.

```
System Integrity Level: 0

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2
```

Authentication request – but no sample present to authenticate, so the authentication level is set to 2

```
System Integrity Level: 0

Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated
```

A keystroke analysis sample has been captured. Defined as a dynamic telephone entry, the sample is moved into the input cache for subsequent classification.

```
Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

System Integrity Level: 0.5
Authentication Level: 1
```

The authentication request has taken the telephone sample and passed the sample (this procedure will pass all samples). The system integrity is increased by 0.5 – the correct amount assigned by the B0 confidence level. The authentication level is reset to 1.

```
Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2
```

The authentication process initiates, but as no samples are present, the authentication level is set to 2 again.

```
System Integrity Level: 0.5

Biometric Technique: Keystroke Analysis Sub Category:
Telephone_01248618453
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

System Integrity Level: 1.5
Authentication Level: 1
```

A static telephone number sample has been captured. Subsequent classification passed the sample and the system integrity is increased to 1.5. The increase of 1 is due to the higher confidence level assigned to static telephone numbers over dynamic. The authentication level is set back to 1.

```
Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 1.5

Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

System Integrity Level: 2
Authentication Level: 1
```

Again, a dynamic telephone number is entered and subsequent classification increases the system integrity level by 0.5 to 2.

```
Processing Biometric Input Sample...
Authentication Request...
```

```
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 2

Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

System Integrity Level: 2
Authentication Level: 1
```

Once more a dynamic telephone number is entered and passed. The authentication level is set back to 1, however the system integrity level does not increase. This is due to the upper limit placed on each confidence level. The user is unable to achieve the higher system integrity levels using a dynamic telephone number – as correctly defined by the specification. The complete output script for this procedure, in addition to the remaining procedures can be found in Appendix E.

As illustrated by Table 8.12 all of the procedures functioned as specified by the architecture.

Procedure #	Authentication Request	Authentication Level	System Integrity Level	Procedure Successful
1	Pass	1	2	✓
1	Fail	4	-4.5	✓
2	Pass	1	5	✓
2	Fail	4	-5	✓
3	Pass	1	5	✓
3	Fail	4	-4.5	✓
4	NA	1	4	✓

Table 8.12: IAMS Validation Results

8.4 Conclusion

The results from the theoretical system performance have illustrated how difficult obtaining access to sensitive services (with System Integrity levels of +5) is for unauthorised users, with a false acceptance probability in the range of 0.00000007-0.000001% compared with the best FAR of 0.1% using a fingerprint technique. The false rejection probability has also shown an improvement with a worst case probability of incorrectly rejecting an authorised user of 0.4% and a best case of 0.00003%. Although it is difficult to directly compare the performance of IAMS against individual techniques as the probability of successfully authenticating a person depends on various stages of the security algorithms, a comparison of these results against individual results, as presented in Table 8.1, illustrates the improvement in performance IAMS experiences.

It is clear from these results, that system performance is largely dependent upon the authentication tools available to IAMS. Devices with stronger authentication tools are more capable of successfully detecting an authorised and unauthorised user than their counterparts. However, even those devices, such as the cellular handset, with limited authentication tools, the levels of FAR and FRR achieved are sill stronger than many individual authentication techniques, with a (worst case) probability of an authorised user incorrectly being rejected of 0.4% (equivalent FRR) and a (worst case) probability of an unauthorised user gaining entry to the most sensitive services of 0.00002% (equivalent FAR).

The results from the practical validation of the prototype have demonstrated IAMS is operating as defined by the architecture, with the System Integrity level and Process algorithm requesting intrusive authentication request as and when necessary.

IAMS has successfully achieved the objectives of providing an advanced authentication mechanism which increases the level of authentication security but without increasing the level of user inconvenience. Through utilising a suite of authentication tools within an intelligent framework, the weaknesses of one technique are overcome by the strengths of others.

9 Conclusions & Future Work

This chapter concludes the thesis by summarising the achievements of the research programme. The chapter proceeds to discuss the limitations of the research, and considers areas for further refinement.

9.1 Achievements of the Research

The growth and popularity of mobile devices and wireless networking technologies has increased the need to ensure the validity of the user. Chapter 2 illustrated that this trend of increasing services and mobile computing is set to continue as users integrate technology within their lives and unlock themselves from the desktop computer. However it was identified that current secret-knowledge based approaches were lacking in the necessary authentication security. This was subsequently reinforced through an end-user survey, which found that a large number of users are not using the PIN and almost a third had experienced handset theft or misuse.

On the basis of these findings, it is evident that alternative and stronger authentication approaches are required for mobile devices. Of the remaining approaches, biometrics was identified as the only approach that does not reply upon the user remembering something, but just on who they are. It was acknowledged that this technique must be capable of securing access to sensitive services and information throughout the duration of a session, in a user-friendly and convenient fashion.

Through the intelligent application of biometric techniques, Chapter 3 identified that authentication of the user can take place transparently enabling users to be authenticated numerous times without inconvenience, as biometric samples are captured during a user's normal interaction with the mobile device. The deployment of biometrics to mobile devices was supported by the end-user survey, with 83% in favour. However, in order to achieve transparent and subsequent convenient authentication, only a subset of biometric techniques were found to be suitable. Of those available, keystroke analysis represented the

most intriguing proposal given the wide availability of keypads and keyboards on mobile devices and the transparent fashion of obtaining the biometric samples.

Although the application of keystroke analysis had been established for keyboards, its deployment to a mobile device with fewer, smaller keys and a different tactile environment had until this research not been documented. Chapters 4 and 5 sought to evaluate the novel application of keystroke analysis to a mobile handset, utilising the two main keystroke characteristics of keystroke latency and hold-time. Both studies concluded successfully with promising results when compared to typical results achieved by other biometric techniques. This technique would permit transparent authentication of users whilst they enter telephone numbers, PINs and compose text messages. Although the performance of keystroke analysis was not as good when compared to some physiological biometrics such as fingerprints, its transparent nature would permit an increase in the level of authentication security that could be provided by a mobile device.

However, the results from the feasibility study must be considered in context. Both studies were performed in controlled conditions, with users entering data repeatedly. Within a practical environment, the variability of the users' input data is likely to be larger, as users may be walking whilst typing, consuming alcohol or performing other tasks, making the process of authentication more difficult. Therefore, it would not be viable to use this technique, where a user is accepted or rejected based upon a single keystroke analysis result. However, due to its transparent nature, it would be possible to use an unsuccessful authentication request as a trigger for a heightened level of monitoring on the device. In addition, from an analysis of the expected performances of biometric techniques in conjunction with the weaknesses of other approaches and the differing hardware configurations of mobile devices it was evident that no single authentication technique

would suffice. What was evident however was the availability of a suite of authentication techniques, both biometric and secret-knowledge based that could be utilised together.

An appropriate framework was therefore required to adapt to the differing hardware configurations of mobile devices providing authentication techniques which adjusted to the available hardware and the level of security required. To this end, a composite authentication mechanism was specified in Chapter 6, along with the security processes required to maintain security and system integrity. The mechanism was designed in a modular and robust manner to enable network administrators the flexibility and convenience of configuring a composite authentication mechanism to meet their specific requirements.

Through adding a level of intelligence to the authentication process, it is no longer a matter of providing a pass or fail response to the identity of a user, but a probability level indicating the confidence the system has in the identity of the user, with the system's behaviour dependent upon the result. With a low probability, the system removes automatic access to key services and information and increases the level of monitoring of the user. With a high confidence level, the user has the ability to interact and access the complete range of services and applications provided by the mobile device without hindrance.

Chapters 7 proposed an architecture for the composite authentication mechanism, known as IAMS and proceeded to develop a functional prototype based upon the specification, illustrating its functionality and transparency of operation. A comparison of commercially available authentication mechanisms found IAMS to be the only mechanism capable of providing a continuous and transparent confidence measure for the identity of the user.

Although many of the commercial approaches are capable of utilising a number of authentication techniques under a wider authentication mechanism, none are designed for use on mobile devices and more importantly none are capable of dynamically adjusting to the available authentication techniques across the diverse range of hardware devices.

Chapter 8 subsequently evaluated the mechanism both theoretically and practically. System performance was calculated theoretically and found to be largely dependent upon which authentication techniques were available to IAMS. It was found that IAMS was capable of protecting and securing services and information beyond what a single authentication technique was able to achieve, for instance, the FAR of a user obtaining a System Integrity level of +5 (a level at which users can access all services and information) is in the range of 0.00000007-0.000001% against a one-off FAR of 0.1% for a fingerprint technique. The FRR has also improved with a worst case of 0.4% and a best case 0.00003% across the range of mobile devices evaluated.

The research has met all of the objectives originally outlined in chapter 1 and has resulted in the design and development of an advanced authentication architecture for mobile devices. In addition, a number of papers relating to the research programme have been published in internationally recognised journals and presented at refereed conferences. In particular, the author has been awarded a best paper prize at the 3rd Australian Information Warfare and Security Conference, and a best student poster prize at the 5th World Conference and Exhibition on the Practical Application of Biometrics. Aspects of the project have also led to commercial prototyping and development for Orange PCS.

9.2 Limitations of the Research

Although the objectives of the research programme have been met, a number of decisions had to be made which imposed limitations upon the work. These decisions were typically either practically based or due to financial restrictions. The key limitations of the research are summarised below.

1. A number of practical limitations exist with the keystroke analysis study. The limited number of participants and input data hindered a more thorough evaluation of the technique. In particular, the controlled environment in which user's input data was captured may not have simulated the real variations in input data that might be seen in practice. Having said this, the option of monitoring user's real handset interactions is only now becoming more plausible due to the introduction of smart phones, which are programmable. Previously, handsets utilised propriety operating systems requiring collaboration from handset manufacturers.

2. Insufficient time and resources were available to further assess the applicability of keystroke analysis to thumb-sized keyboards – an interface similar in size to keypads but with full keyboard functionality. This interface does represent a different tactile environment from the previous two mentioned earlier, although not completely dissimilar to keypads. Given the successful study of keystroke analysis on keypads, in addition to the previous work performed on keyboards, it was considered that the technique would arguably be functional on thumb-sized keyboards as well.

3. The development of IAMS was only performed using a simulated mobile handset interface on a PDA. Due to the lack of programmable handsets, and the immaturity of the technology, it was decide that a more stable platform would be suitable.

4. IAMS was only able to utilise two biometrics in the final prototype. Unfortunately, voice verification, a technique that would lend itself to a mobile handset, was not incorporated in to the prototype due to financial restrictions.

5. The lack of a practical evaluation of IAMS with real participants. This would have enabled a comprehensive analysis of system performance in real time. Unfortunately, the lack of available handsets, and the subsequent cost had the handsets existed, meant system evaluation could only be performed theoretically.

Despite these limitations, the research programme has made valid contributions to knowledge and provided sufficient proof of concept for the ideas proposed.

9.3 Suggestions & Scope for Future Work

This research programme has advanced the field of authentication for mobile devices. However, a number of areas of scope for future work exist, specifically related to this research and more generally within the area of authentication on mobile devices. These suggestions are detailed below:

1. A wider and practical deployment of keystroke analysis capturing software. This would permit a comprehensive and thorough evaluation of the technique with real handset interactions.

2. Further resource could be spent into optimising the neural network configurations and training stages. In particular, reducing the computational requirements of classification for deployment on mobile devices. One key development would be the creation of artificial impostor data to successfully train against the authorised users' data. In a standalone topology the mobile device will have no access to other user's data, to use as impostor data – as was the procedure in this research study. Successful training of a network will therefore depend upon the creation of artificial impostor data that is able to successfully create decision boundaries around an authorised user's input samples. Some work has already been performed in this area by an MSc project supervised by the author (Lecomte et al. 2003).

3. Further research and development is required into providing biometric techniques applicable to a mobile device. In particular, developing dynamic voice verification techniques for use in telephony applications, and signature recognition for mobile devices with no keypad or keyboard present – capable of authenticating a person based upon words rather than a signature. An additional technique of interest, if the transparency issues were overcome, is fingerprint recognition as the technique is not only popular with users but is one of the more secure biometric approaches.

4. One of the more controversial sides to this research is with regard to the use and storage of biometric templates and samples. For wide adoption of biometrics and IAMS, it is imperative that network administrators consider the opinions of end-

users, since the wide scale implementation of biometric solutions to date has proved to be an emotive issue for the public (BBC News, 2004).

5. A comprehensive evaluation of IAMS is required from both a system security performance perspective, but also considering the practicalities of implementation in client-server and standalone topologies. What are the computational requirements of the system on a per user basis, and can this be scaled successfully across all users on a mobile network? What effect will this have upon network bandwidth, and what degree of personal mobility exists for the user?

6. Research and software development is required on the operating systems of mobile devices, in order to capture and process the biometric samples. It will be necessary to embed IAMS monitoring software within the device to transparently capture this information without any significant degradation of system performance.

9.4 The Future of Authentication for Mobile Devices

Wireless mobile computing is here to stay, with people beginning to utilise a wide range of services to assist their everyday lives, from email to video conferencing. This is set to continue as new services become available providing information at our finger tips. Future services have the potential to become more sensitive as access, for example, to medical records and home intranets becomes available. However, this increase in functionality and storage capacity of mobile devices has the subsequent effect of increasing the financial and personal cost incurred should the device be misused. It can be argued at this stage that identity authentication no longer becomes an option but a necessity.

Although many mechanisms currently exist for authenticating users, this research has highlighted the need to provide increased security, in a continuous and user friendly fashion. The research programme has, through a comprehensive analysis, designed and developed an authentication architecture capable of providing transparent and continuous authentication of the user, independent of the hardware or network configuration. Authentication is no longer a one-off process but a continual confidence based measure, capable of utilising a wide range of authentication techniques to maintain system integrity.

In conclusion, authentication on mobile devices will become an increasingly important consideration for users, as the cost and functionality of devices make them desirable targets for misuse. The ability to perform authentication continuously and conveniently will be fundamental to the successful deployment of future mechanisms.

References

1 3G. (2003). "European Mobile Ownership Saturation". 3G. www.3g.co.uk/PR/July2003/5619.htm

2 Ahmavaara, K., Haverinen, H., Pichna, R. (2003). "Internetworking Architecture Between 3GPP and WLAN Systems". IEEE Communications Magazine, November 2003.

3 Anderson, D., Frivold, T., Valdes, A. (1995). "Next Generation Intrusion Detection Expert System (NIDES)". SRI International. http://ccss.isi.edu/papers/anderson_nides.pdf

4 Andersson, C. (2001). GPRS & 3G Wireless Applications. John Wiley & Sons.

5 Anovea. (2004a). "Anovea – Authentication Technology". Anovea. http://www.anovea.com/

6 Anovea. (2004b). "Anovea Authentication Technology – The SVLite SDK". Anovea Inc. http://www.anovea.com/www/products_lit.htm

7 Arc Group. (2003). "Mobile Content & Applications 2003. Arc Group. http://www.3g.co.uk/3GHomeSearch.htm

8 Ashbourne, J. (2000). Biometric. Advanced Identity Verification. The Complete Guide. Springer.

9 Atrua. (2004). "Atrua Premiers First of Kind Intelligent Touch-Based System for Mobile Phone". Atrua Technologies. http://www.atrua.com/news.htm

10 BBC News. (1998). "Computer Red-Box Vulnerable to Hackers". BBC News. http://news.bbc.co.uk/1/hi/sci/tech/47187.stm

11 BBC News. (1999). "Police Play in by Ear". BBC News. http://news.bbc.co.uk/1/hi/sci/tech/246713.stm

12 BBC News. (2004). "Concern over Biometric Passports". http://news.bbc.co.uk/1/hi/technology/3582461.stm

13 Best, J. (2003). "Steal to Order Phone Theft Crackdown". Silicon.Com. www.silicon.com/networks/mobile/0,39024665,39117404,00.html

14 BioAPI Consortium. (2003). "BioAPI Specification (version 1.1)". BioAPI Consortium. http://www.bioapi.org/

15 Biometrics Catalogue. (2004). Biometrics Catalogue. http://www.biometricscatalog.org/

16 BioPassword. (2004). "Security at your Fingertips". Bio Net Systems. http://www.biopassword.com/bp2/welcome.asp

17 Biovisec. (2004). "3D Facial Recognition". Biovisec. http://www.biovisec.com/

18 Bishop, M. (1995). Neural Networks for Pattern Classification. Oxford University Press.

19 BNX Systems. (2004). "BNX Authentication Systems". BNX Systems. http://www.bionetrix.com/bnxauth.asp?mnuID=5

20 Broersma, M. (2004). "WAP Makes Resurgence". ZDNet UK. http://news.zdnet.co.uk/hardware/0%2C39020351%2C39118962%2C00.htm

21 Brown, M., Rogers, J. (1993). "User Identification via Keystroke Characteristics of Typed Names using Neural Networks". International Journal of Man-Machine Studies, vol. 39, pp. 999-1014

22 Cellular Online. (2003). "3Q 2003 Phone Sales Figures". Cellular Online. http://www.cellular.co.za/stats/stats-handsets.htm

23 Cellular Online. (2004a). "Latest Mobile, GSM, Global, Handset, Base Station & Regional Cellular Statistics". Cellular Online. http://www.cellular.co.za/stats-main.htm

24 Cellular Online. (2004b). "Mobile Content shows Revenue Promise says Nokia report". Cellular Online, 1st May 2004. http://www.cellular.co.za/news_2004/may/050104-mobile_content_shows_revenue_pro.htm

25 CESG. (2002). "Common Criteria: Common Methodology for Information Technology Security Evaluation, Biometric Evaluation Methodology Supplement". Biometric Evaluation Methodology Working Group, CESG.

26 Cho, S., Han, C., Han D., Kin, H. (2000). "Web Based Keystroke Dynamics Identity Verification Using Neural Networks". Journal of Organisational Computing & Electronic Commerce, vol. 10, pp 295-307.

27 CIC. (2004). "Electronic Signatures". Communication Intelligence Corp. http://www.cic.com/

28 Clarke, N. (2001). Mobile Phone Security. BEng Project Report. University of Plymouth, UK.

29 Competition Commission. (2003). "Vodafone, Orange and T-Mobile. Reports on references under section 13 of the Telecommunications Act 1984 on the charges made by Vodafone, O2, Orange and T-Mobile for Terminating calls from fixed and mobile networks". Competition Commission. http://www.competition-commission.org.uk/rep_pub/reports/2003/475mobilephones.htm#full

30 Cope, B. 1990. "Biometric Systems of Access Control". Electrotechnology, April/May: 71-74

31 Cover, T. (1965). "Geometric and Statistical Properties of Systems of Linear Inequalities with Applications in Pattern Recognition". IEEE Transactions on

Electronic Computers, vol. 14, pp. 326-334.

32 Daon. (2004). "Daon Biometric Identity Management". Daon. http://www.daon.com/

33 Daugman, J. (1998). "How Iris Recognition Works". University of Cambridge. http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf

34 Demuth, H., Beale, M. (2001). Technical Support Documents – Neural Network Toolbox. MathWorks Inc MatLab (version. 6.1).

35 Denning, D. (1986). "An Intrusion-Detection Model". SRI International. http://www.cs.ucsb.edu/~vigna/IntrusionDetection/id_model.pdf

36 Denning, D. (1999). Information Warfare & Security. ACM Press.

37 Domain Dynamics. (2004). "Company Homepage". Domain Dynamics Ltd. www.ddl.co.uk

38 Dorman, A. (2001). The Essential Guide to Wireless Communication Applications. Prentice Hall.

39 Dubendorf, V. (2003). Wireless Data Technologies. John Wiley & Sons

40 Duda, R., Hart, P. (1973). Pattern Classification & Scene Analysis. John Wiley & Sons.

41 ETSI. (2001). The European Telecommunications Standards Institute. www.etsi.org

42 Evidian. (2004). "Evidian AccessMaster NG". Evidian. http://www.bullsoft.co.uk/security/about/products.htm

43 Federal Information Processing Standards. (1985). "Password Usage", Federal Information Processing Standards Publication 112. http://www.itl.nist.gov/fipspubs/fip112.htm

44 Forman, G., Zahorjan, J. (1994). "The Challenges of Mobile Computing". Mobility: Processes, Computers & Agents. Addison-Wesley (1999).

45 Furnell, S., Illingworth, H., Katsikas, S., Reynolds, P., Sanders, P. (1997). "A Comprehensive Authentication and Supervision Architecture for Networked Multimedia Systems". Proceedings of IFIP CMS, Athens, pp227-238.

46 Furnell, S., Rodwell. P., Reynolds, P. (2001). "A Conceptual Security Framework to Support Continuous Subscriber Authentication in Third Generation Networks". Proceedings of Euromedia 2001.

47 Gaines, R., Lisowksi, W., Press, S., Shapiro, N., (1980). Authentication by keystroke timing: Some Preliminary Results. Rand Report R-256-NSF. Rand Corporation, Santa Monica, CA.

48 Giussani, B. (2001). Roam. Making Sense of the Wireless Internet. Random House Business Books

49 Gold, S. (2004). "Ninety per Cent of Mobile Devices have no IT Security". SecureSynergy. www.securesynergy.com/securitynews/newsitems/2004/apr-04/020404-08.htm

50 Gordon, L., Loeb, M., Lucyshyn, W., Richardson, R. (2004). "2004 CSI/FBI Computer Crime & Security Survey". Computer Security Institute.

51 Graham-Rowe, D. (2001). "Something in the Way She Phone". New Scientist.Com. http://www.newscientist.com/hottopics/ai/somethingintheway.jsp

52 GSM World. (2003). "GSM Statistics". GSM Association. http://www.gsmworld.com/news/statistics/index.shtml

53 Hagan, M., Demuth, H., Beale, M. (1996). Neural Network Design. PWS Publishing Company

54 Harrington, V., Mayhew, P. (2001) Home Office Research Study 235: Mobile Phone Theft. Crown Copyright

55 Hassoum, M. (1995). Fundamentals of Artificial Neural Networks. The MIT Press

56 Haykin, S. (1999). Neural Networks: A Comprehensive Foundation (2nd Edition). Prentice Hall

57 Hogg, R., Ledolter, J. (1989). Engineering Statistics. Maxwell MacMillan International Editions.

58 HP. (2004). "Handheld Devices". Hewlett Packard. http://welcome.hp.com/country/us/en/prodserv/handheld.html

59 Hutchison 3G UK. (2004a). "Introducing 3 – A New Type of Company". http://www.three.co.uk/aboutus/newkind.omp

60 Hutchison 3G UK. (2004b). Three Handsets – Motorola A920. http://www.three.co.uk/explore/handsets/detail.omp

61 I/O Software. (2004). "I/O Software – Advanced Authentication Software SecureSuite XS". I/O Software. www.iosoftware.com

62 Identix. (2004). "Identix. Your Trusted Biometric Provider". Identix. http://www.identix.com/

63 IEEE Computer Society. (2001) IEEE Standard for Local and Metropolitan Area Networks: Overview & Architecture. IEEE Computer Society. http://standards.ieee.org/

64 Imagis Technologies. (2004). "Homepage". Imagis Technologies http://www.imagistechnologies.com/

65 International Biometrics Group. (2004). "Independent Biometrics Expertise". IMG. http://www.biometricgroup.com/

66 IR Recognition Systems. (2004). "Hand Geometry". Ingersoll-Rand. http://www.handreader.com/

67 ISIS. (2003). "Automatic Gait Recognition for Human ID at a Distance". University of Southampton. http://www.gait.ecs.soton.ac.uk

68 Joyce R., Gupta, G. (1990). Identity Authentication Based on Keystroke Latencies. Communications of the ACM, vol. 39; pp 168-176.

69 Kanellos, M. (2002). "Perspective: An Answer to Wi-Fi's Discontents". CNet News.Com. http://news.com.com/2010-1071_3-976822.html

70 Kelly, L. (2002). "Corporate Secrets are Rich Pickings on PDAs". Information World Review. http://www.iwr.co.uk/News/1132042

71 Kotadia, M. (2004). "Gates predicts death of the password". ZDNet UK. http://news.zdnet.co.uk/software/windows/0,39020396,39147336,00.htm

72 Lecomte, J., Clarke, N., Furnell, S. (2003). "Artificial Impostor Profiling for Keystroke Analysis on a Mobile Handset". Advances in Network & Communication Engineering, pp. 55-62.

73 Leggett, J., Williams, G. (1987). "Verifying Identity via Keystroke Characteristics". International Journal of Man-Machine Studies, 28.

74 Leggett, J., Williams, G., Usnick, M. (1991). "Dynamic Identity Verification via Keystroke Characteristics". International Journal of Man-Machine Studies.

75 Lemon, S. (2001). "Acer Laptop Offers Security at Your Fingers". IDG News Service. http://www.pcworld.com/news/article/0,aid,63703,00.asp

76 Lemon, S. (2003). "Laptop sales to outpace analyst predictions, Intel says". IDG News Service. http://www.infoworld.com/article/03/10/21/HNlaptopsales_1.html

77 Lemos, R. (2002). "Passwords: The Weakest Link? Hackers can crack most in less than a minute". http://news.com.com/2009-1001-916719.html. CNET News.Com.

78 Leyden, J. (2002). "Mobile Phone Theft is far Worse than we Thought". The Register. www.theregister.co.uk/content/archive/24138.html

79 Looney, C. (1997). Pattern Recognition using Neural Networks: Theory and Algorithms for Engineers and Scientists. Oxford University Press.

80 Maltoni, D, Maio, D., Jain, A., Prabhakar, S. (20043). Handbook of Fingerprint Recognition. Springer.

81 MatLab. (2002). Comprehensive Mathematical Software. MathWorks. www.mathworks.com.

82 Maxim M., Pollino, D. (2002). Wireless Security. RSA Press.

83 McCullock, W., Pitts, W. (1943). "A Logical Calculus of the Ideas Immanent in Nervous Activity". Bulletin of Mathematical Biophysics, vol. 5, pp. 115-133.

84 Minsky, M., Papert, S. (1988). Perceptrons – Expanded Edition. MIT Press.

85 MIT AI Lab. (2003). "MIT AI Lab Human ID". MIT. http://www.ai.mit.edu/people/llee/HID/intro.htm

86 Monrose, R., Reiter, M., Wetzel, S. (1999). "Password Hardening Based on Keystroke Dynamics". Proceedings of the 6th ACM Conference on Computer and Communication Security.

87 Monrose, R., Rubin, A. (1997). "Authentication via Keystroke Dynamics". Proceedings of the 4th ACM Conference on Computer and Communication Security.

88 Monrose, R., Rubin, A. (1999). "Keystroke Dynamics as a Biometric for Authentication". Future Generation Computer Systems, 16(4) pp 351-359.

89 Moore, M. (2001). "PDAs and Sensitive Data". Information World Review. http://www.iwr.co.uk/Features/1125654

90 Morgan, J. (1999). "Court Holds Earprint Identification Not Generally Accepted in Scientific Community". Forensic-Evidence.com. http://www.forensic-evidence.com/site/ID/ID_Kunze.html

91 Morris, R., Thompson, K. (1979). "Password Security: A Case History". Communications of the ACM, vol. 22, no. 11, pp. 594-597.

92 Nanavati, S., Thieme, M., Nanavati, R. (2002). Biometrics. Identity Verification in a Networked World. John Wiley & Sons.

93 Napier, R., Laverty, W., Mahar, D., Henderson, R., Hiron, M., Wagner, M. 1995. "Keyboard User Verification: Toward an Accurate, Efficient and Ecological Valid Algorithm". International Journal of Human-Computer Studies, vol. 43, pp213-222

94 Nohria, N., Leestma, M. (2001). "A Moving Target: The Mobile-Commerce Customer". Accenture. www.accenture.com

95 NTT DoCoMo. (2004a). "Latest Handsets – 505i Range". http://www.nttdocomo.com/corebiz/foma/try/900i/index.html. NTT DoCoMo.

96 NTT DoCoMo. (2004b). "NTT DoCoMo Company Overview". NTT DoCoMo. http://www.nttdocomo.com/companyinfo/overview.html

97 NTT DoCoMo. (2004c). "NTT DoCoMo Subscriber Growth". NTT DoCoMo. http://www.nttdocomo.com/companyinfo/subscriber.html

98 NTT DoCoMo. (2004d). "NTT DoCoMo FOMA Subscribers Top 3 Million". NTT DoCoMo Press Release Article. http://www.nttdocomo.com/presscenter/pressreleases/press/pressrelease.html?param[no]=436

99 Nuance. (2004). "The Voice Automation Expert". Nuance. http://www.nuance.com/

100 Obaidat, M. S., Sadoun, B. (1997). "Verification of Computer User Using Keystroke Dynamics". IEEE Transactions on Systems, Man and Cybernetics – Part B: Cybernetics, Vol. 27, No.2.

101 Obaidat, M., Macchairolo, D. (1994). "A Multilayer Neural Network System for Computer Access Security". IEEE Transactions on Systems, Man, and Cybernetics, vol. 24, no. 5, pp. 806-813.

102 Ord, T., Furnell, S. (2000). "User Authentication for Keypad-Based Devices using Keystroke Analysis". MSc Thesis, University of Plymouth, UK.

103 PalmOne. (2004). The PalmOne Handheld Family. PalmOne Inc. http://www.palmone.com/us/products/handhelds/

104 PDALok. (2004a). "Biometric Digital Signature". Romsey Associates Ltd. http://www.pdalok.com/default.htm

105 PDALok. (2004b). "PDALok – The Only Way to Lock your Handheld". Romsey Associates. http://www.pdalok.com/default.htm

106 Philipkoski, K. (2002). "Is that Really You? Check my DNA". Wired News. http://www.wired.com/news/medtech/0,1286,56696,00.html

107 Protocom Development Systems. (2003). "Global Password Usage Survey". Protocom Development Systems: Network Security & Innovation. http://www.protocom.com/whitepapers/password_survey.pdf

108 Reynolds, J. (2003). Going Wi-Fi. A Practical Guide to Planning & Building an 802.11 Network. CMP Books

109 Richardson, R. (2003). "2003 CSI/FBI Computer Crime & Security Survey". Computer Security Institute.

110 Rogers, J. (2001). "Data Mining Fights Fraud – Company Operations. Computer Weekly. http://articles.findarticles.com/p/articles/mi_m0COW/is_2001_Feb_8/ai_70650704

111 Rosenblatt, F. (1958). "The Perceptron: A Probabilistic Model for Information Storage & Organisation in the Brain". Psychological Review, vol. 65, pp. 386-408.

112 Rumelhart, D., McClelland, J. (1986). "Parallel Distributed Processing: Explorations in the Microstructure of Cognition", vol. 1. MIT Press

113 SafLink. (2004). "Protecting your Enterprise through Secure Authentication". SafLink. http://www.saflink.com/

114 Sarle, W. (2002). "What is GRNN?". Comp.ai.neural-nets FAQ. http://www.faqs.org/faqs/ai-faq/neural-nets/part2/section-21.html

115 Sharp. (2004). Sharp Zaurus Personal Mobile Tool. Sharp. http://www.sharpusa.com/products/FunctionLanding/0,1050,32,00.html

116 Shaw, K. (2004). "Data on PDAs mostly Unprotected". Network World Fusion. http://www.nwfusion.com/

117 Sherriff, L. (2004). "Orange Kicks off 3G Trials in UK and France". The Register. http://www.theregister.co.uk/content/59/35769.html

118 Smith, R. (2002). Authentication. From Passwords to Public Keys. Addison-Wesley.

119 Smith, T. (2003). "Europe to Adopt Wi-Fi Faster than US". The Register. www.theregister.co.uk/content/69/34225.html

120 Smith, T. (2004a). "Euro PDA biz sees first growth since 2000". The Register. http://www.theregister.co.uk/content/68/35100.html

121 Smith, T. (2004b). "PDA, Smartphone Sales Rocket in Europe". The Register. www.theregister.co.uk/2004/04/20/euro_q1_pda_sales/print.html

122 Socolinsky, D., Selinger, A. (2004). "Thermal Face Recognition in an Operational Scenario". Proceedings of CVPR 2004, Washington DC.

123 Sony Ericsson. (2004). Sony Ericsson P900 Mobile Handset. http://www.sonyericsson.com/p900/main.aspx?regionCode=uk

124 Spillane, R. (1975). "Keyboard apparatus for personal identification". IBM Technical Disclosure Bulletin, 17, 3346.

125 Temple, R., Regnault, J. (2002). Internet & Wireless Security. Institution of Electrical Engineers.

126 Triola, M.(1998). Elementary Statistics. Addison Wesley.

127 Twist, J. (2004). "Wireless Web Reaches Out in 2004". BBC News UK Edition. http://news.bbc.co.uk/1/hi/technology/3341257.htm

128 Umphress, D., Williams, G. (1985). "Identity Verification through Keyboard Characteristics". International Journal of Man-Machine Studies, Vol. 23, pp. 263-273

129 UMTS Forum. (2000). "Shaping the Mobile Multimedia Future – An Extended Vision from the UMTS Forum". http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/umts/Resources_Papers_index

130 UMTS Forum. (2003). Mobile Evolution. Shaping the Future. UMTS Forum. http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/umts/MultiMedia_PDFs_UMTS-Forum-White-Paper-1-August-2003.pdf

131 Vaughan-Nichols, S. (2003). 802.11 Vs. 3G. Wi-Fi Planet. http://www.wi-fiplanet.com/tutorials/article.php/1577551

132 VeriVoice. (2004). "The Sound Solution for Integrating a Robust Voice Verification Technology". VeriVoice. http://www.verivoice.com/

133 Wakefield, J. (2000). "Going, going, gone...Mobile Auction Results". ZDNet UK. http://news.zdnet.co.uk/internet/0,39020369,2078633,00.htm

134 Wood, H. (1977). "The Use of Passwords for Controlling the Access to Remote Computer Systems and Services". Computers and Security, Vol.3. C.T. Dinardo, Ed., p.137. Montvale, New Jersey: AFIPS Press.

135 Woodward, J., Orlans, N., Higgins, P. (2003). Biometrics. Identity Assurance in the Information Age. McGraw-Hill.

136 Yu Hui, S., Hau Yeung, K. (2003). "Challenges in the Migration to 4G Mobile Systems". IEEE Communications Magazine, December 2003.

Appendices

Appendix A
- Survey into the Attitudes & Opinions of Subscribers towards Security

Appendix B
- Theory of Keystroke Analysis

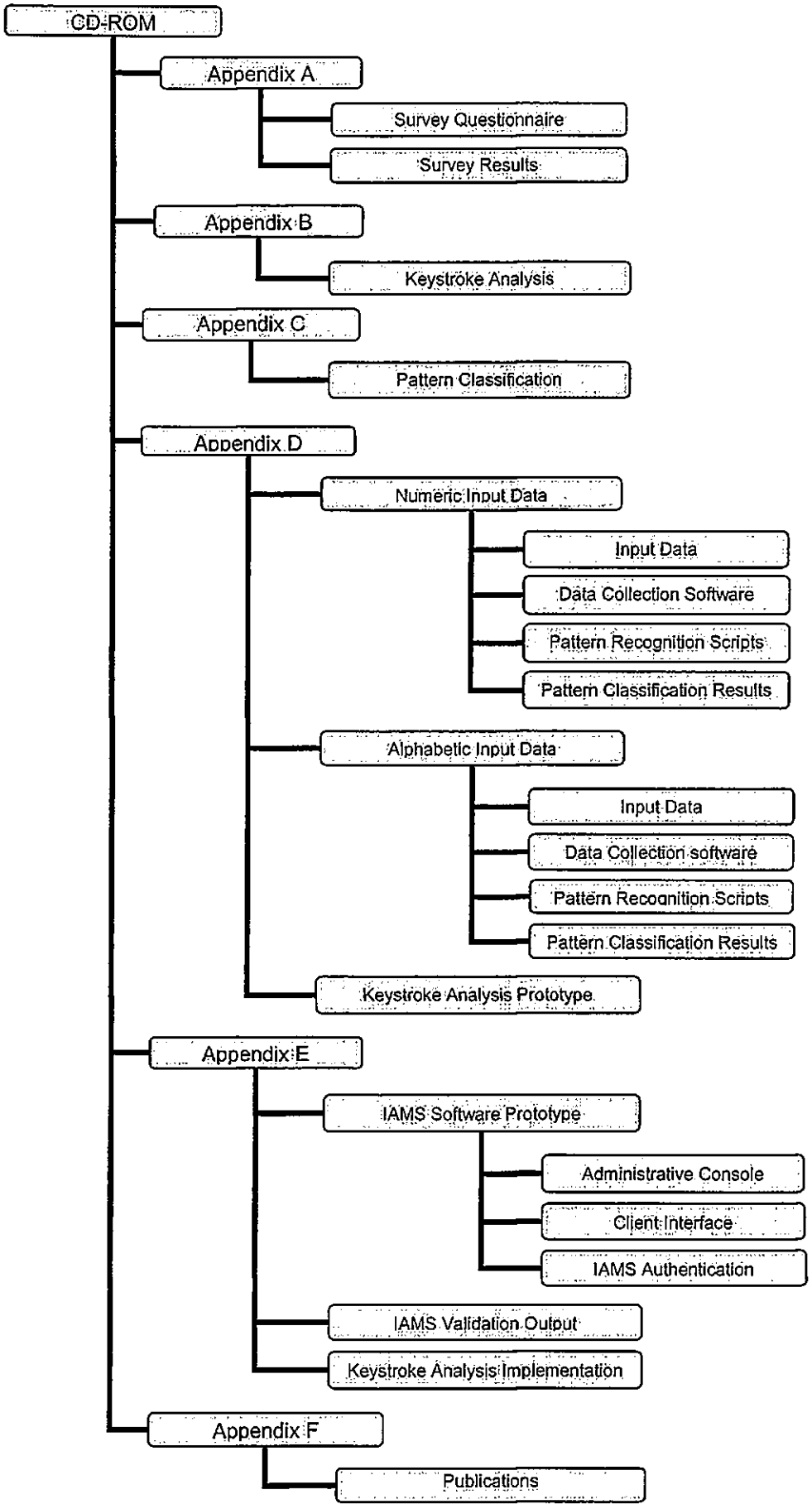
Appendix C
- Theory of Pattern Recognition

Appendix D
- Feasibility Study of Keystroke Analysis

Appendix E
- IAMS Software Prototype

Appendix F
- Publications

The content of a number of these appendices have been included on a CD-ROM. Please turnover for an overview of the CD-ROM file directory.


CD-ROM
Appendix A
Survey Questionnaire
Survey Results
Appendix B
Keystroke Analysis
Appendix C
Pattern Classification
Appendix D
Numeric Input Data
Input Data
Data Collection Software
Pattern Recognition Scripts
Pattern Classification Results
Alphabetic Input Data
Input Data
Data Collection software
Pattern Recognition Scripts
Pattern Classification Results
Keystroke Analysis Prototype
Appendix E
IAMS Software Prototype
Administrative Console
Client Interface
IAMS Authentication
IAMS Validation Output
Keystroke Analysis Implementation
Appendix F
Publications

Appendix A

Survey into the Attitudes & Opinions of Subscribers towards Security

Part 1 – Survey Questionnaire

Part 2 – Full Results

Appendix A

Part 1 – Survey Questionnaire

Hypothesis

Mobile Phone users are either not security aware or are unaware of the dangers in regard to the protection of both their handsets and their network subscription.

Objective

A survey to assess the security awareness of mobile phone users.

Mobile Phone Security Survey – How Aware Are You?

Section 1 – About you

1 What gender are you?

Male ☐ Female ☐

2 To which age group do you belong?

< 16 ☐ 17-24 ☐ 25-34 ☐ 35-44 ☐
45-54 ☐ 55-65 ☐ > 65 ☐

3. Are you an employee or student at the University of Plymouth?

Yes ☐ No ☐

Section 2 – Services

A. About your mobile phone subscription:

4. To which network provider do you subscribe?

Vodafone ☐ Orange ☐ BT Cellnet ☐ One2One ☐
Virgin ☐ Other ☐ (Please State:.....)

5. How do you pay for your phone calls?

Contract ☐ Pre-Pay ☐

6. Who is the manufacturer of your current mobile phone?

Nokia ☐ Sony/Ericsson ☐ Motorola ☐ Samsung ☐
Siemens ☐ Bosche ☐ Trium ☐ Other ☐ (Please state.....)

7. When choosing your network operator, please rank the considerations below in order of importance to you.

	Low	Medium	High
Choice of handset(s)	☐	☐	☐
Network Coverage	☐	☐	☐
Operator loyalty	☐	☐	☐
Prices, Deals etc	☐	☐	☐
Reliability	☐	☐	☐
Security feature(s)	☐	☐	☐

8. When selecting your handset, please rank the considerations below in order of importance to you.

	Low	Medium	High
Available Accessories	☐	☐	☐
Battery Life	☐	☐	☐
Brand Loyalty	☐	☐	☐
Games	☐	☐	☐
Infra-Red/Bluetooth Connectivity	☐	☐	☐
Security feature(s)	☐	☐	☐
Swappable fascias	☐	☐	☐

B. About your mobile phone usage:

9. Approximately, how many hours a day is your phone switched on?

<1 ☐ 2-5 ☐ 6-10 ☐ >10 ☐

10. Approximately, how many times in a typical day, do you use your mobile?

a. For making voice calls

< 1 ☐ 2-5 ☐ 6-10 ☐ > 10 ☐

b. All services (except voice calls) including, WAP, SMS, email etc.

< 1 ☐ 2-5 ☐ 6-10 ☐ > 10 ☐

c. Using "inbuilt" features, such as games or the calendar

< 1 ☐ 2-5 ☐ 6-10 ☐ > 10 ☐

11. Please indicate which services you use on your mobile phone?

	Yes	No	Not Available
Voice/Talking	☐	☐	☐
Text Messages (SMS)	☐	☐	☐
Voice or SMS-based Information Services (e.g. football scores, news, lottery, traffic information)	☐	☐	☐
WAP services	☐	☐	☐
Email	☐	☐	☐
International Roaming	☐	☐	☐

12. Please indicate any additional services you would like to see on a mobile phone in the future?

	Yes	No
Video calls/conferencing	☐	☐
eCommerce (On-Line Shopping)	☐	☐
On-line Personal Organiser	☐	☐
Music downloading, playing	☐	☐
Video On Demand (VOD). (i.e. Short video clips, e.g. News, Sports results, Movie previews etc.)	☐	☐
Multimedia Message Service (MMS). (i.e. SMS with sound, video etc.)	☐	☐
Global Positioning System (GPS) services.	☐	☐
Additional Games	☐	☐

Other (please state):.....

Section 3 – Security

A. About your existing mobile phone security:

13. Please indicate which of the following statements applies to you:

Note: The use of the term 'calls' in the following question includes all communications; voice, text, WAP etc.

My mobile phone has :-	*Tick if true*
• been borrowed and tampered with without my permission	☐
• been borrowed and calls were made without my permission	☐
• been stolen, but no calls were made	☐
• been stolen and calls were made	☐
• never been abused or stolen to my knowledge	☐

14. Are you aware of the existence of the International Mobile Equipment Identifier (IMEI) of your handset?

Yes ☐ No ☐

15. Do you use any of the Personal Identification Number (PIN) authentication facilities on your mobile phone?

Yes ☐ No ☐ What is a PIN? ☐

If yes, please indicate which facilities you use, otherwise please go to Q17.

	Yes	**No**	**Not Available**
SIM Access at phone switch-on only *(Default security on all phones)*	☐	☐	☐
Keypad unlock	☐	☐	☐
SIM removal only	☐	☐	☐

16. How often do you change ANY of your mobile phone PINs?

Never ☐ Only initially after purchase (once) ☐ Monthly ☐
Yearly ☐

17. How do you consider PIN authentication?

Convenient ☐ Inconvenient ☐

18. How do you feel generally about the protection the PIN provides against mobile phone misuse?

Very confident ☐ Confident ☐ Adequate ☐ Inadequate ☐
Indifferent ☐

19. Have you ever had to use the Pin Unlock Code (PUK) on your mobile phone, because you forgot your PIN?

Yes ☐ No ☐

20. Do you use the same PIN for multiple services, such as your mobile phone, bank cards, PC access etc?

Yes ☐ No ☐

21. Do you think, in principal, additional mobile phone security is:-

A good idea ☐ A bad idea ☐ Indifferent ☐

B. About future mobile phone authentication:

Note: Biometrics' are the measurement of unique personal characteristics (e.g. Fingerprints, Voice Recognition and Hand Geometry), in our case for authentication purposes.

22. How do you feel about biometric authentication in general?

Good idea ☐ Bad idea ☐ Indifferent ☐

23. Please indicate in the table below which of the following methods of security authentication you are aware of and which you would consider using on a mobile phone?

Security Technique	Aware Of?		Would use on a Mobile Phone?	
	Yes	No	Yes	No
Finger Print	☐	☐	☐	☐
Voice Print	☐	☐	☐	☐
Hand Geometry	☐	☐	☐	☐
Facial Recognition	☐	☐	☐	☐
Iris Scanning	☐	☐	☐	☐
Typing Style *(the way in which you dial numbers)*	☐	☐	☐	☐

24. How would you feel about your mobile phone **continuously** and **transparently** authenticating who is using it?

Good idea ☐ Bad idea ☐ Indifferent ☐

25. For any authentication technique to work, a security profile or signature about you has to exist somewhere. Where would you prefer this security profile to reside?

In the phone (User responsibility*) ☐ In the network (Operator responsibility**) ☐ Don't mind☐

* The personal biometric information about the user would *only* reside in the mobile phone handset, thus it would not be available to authenticate the user on other mobile phones/devices. The privacy of the information stays with the user. If the phone was lost or stolen, any replacement would require re-configuration of the biometric.

** A subscriber's biometric information resides within the network, trusting the privacy to the network operator, thus enabling the network to authenticate the user not only on their mobile phone but any other mobile phone/device they wish to gain access to and have permission to do so.

Section 4 – About your mobile knowledge in general:

26. Which of the following is NOT a UK Network Operator?

Vodafone ☐
Orange ☐
Nokia ☐
One2One ☐
Don't know ☐

27. Which of the following is NOT a mobile phone "buzzword"?

GPRS ☐
WAP ☐
ADSL ☐
3G ☐
Don't know ☐

28. What is the operating bandwidth of a standard GSM connection?

9.6Kbps ☐ 14.4Kbps ☐ 56Kbps ☐ 64Kbps ☐ Don't know ☐

Appendix A

Part 2 – Full Results

This appendix can be located on the CD-ROM

Appendix B

Theory of Keystroke Analysis

Literature Review of Keystroke Analysis

The concept of identity verification based upon the manner in which a person types was first suggested by Spillane (1975), in a paper entitled "Keyboard Apparatus for Personal Identification". Since then, a number of researchers using techniques ranging from simple descriptive statistics to artificial intelligence, have investigated the feasibility of keystroke analysis as a means to authenticate a person. This literature review includes a cross section of the twenty papers reviewed including, papers from the early days where the researchers involved were attempting to prove the concept, to the more recent papers that have tried to use dynamic authentication techniques in order to achieve more non-intrusive authentication. All the papers in this review, with the exemption of the last, discuss keystroke analysis with respect to a full Qwerty keyboard.

A paper by Umphress and Williams (1985) was, for Williams, the first of three papers on the subject of keystroke dynamics spanning five years. The study performed two tests, firstly, to determine how closely the test profile matches the reference profile and secondly, appraising the overall typing characteristics. The reference profile was generated by calculating the latencies for the first six keystrokes in each word and eliminating anomalous keystroke latencies. Two measures of key patterns were produced from the filtered keystrokes, the first was a mean and standard deviation keystroke latency, and the second described the latency between all adjacent letter combinations by defining a 26x26 matrix. The test profile was devised with real-time performance in mind and used the same principles as the reference profile; latencies over 0.75s were ignored, only the first six characters of each word were considered and if a backspace character occurred the word was also ignored. The first test compared the keystroke latency to the appropriate cell in

the digraph matrix of the reference profile. If the test latency was within 0.5 standard deviations of the corresponding latency then the test keystroke is considered valid. A count of those passing the pattern matching process is kept so that a ratio can be computed at any time. In the second test, a count was kept of all the test keystrokes that pass the filtering stage, so that at any time the mean and standard deviation could be calculated and compared to the reference profile using a standard two-tailed t-test for a population mean (assuming normal distribution). The results showed that when the reference profile and test profile were typed by the same person, the ratio of valid latencies to total latencies is greater than 0.6. A total of seventeen participants took part in the study and the overall results were evaluated by designating a degree of confidence to each person. A high confidence being given to participants passing both tests, a medium confidence for passing one, and a low confidence for failing both. Only two of the seventeen were not assessed with a high confidence score, leading to a false rejection rate of 11.7%. The false acceptance rate was calculated by summing all the medium and high confidences of the unauthorised users and dividing by the total to give a false acceptance rate of 5.8%. Umphress and Williams concluded by suggesting the use of keystroke characteristics is not in itself sufficient for personal identification.

Williams' second paper (1987), aimed principally to refine his first experiment, but to also increase the number of participants and the number of filtering methods in an effort to find the smallest amount of data necessary to characterise a person. The filtering methods consisted of three high-pass values of 0.75s (same as previous), 0.5s and 0.3s (obtained from analysis of the input data), and a mixture of valid digraphs. The test sample size was 537 characters, versus 300 for the previous experiment, allowing a more precise reference profile to be generated. The most successful filter method used all lowercase letters including blank with a high-pass filter of 0.5s. The only difference between this filter and

the one used in Williams' (1985) was the inclusion of the blanks as valid characters and the lowering of the high-pass filter. The new filter produced results of 5.5% FRR and 5.0% FAR, indicating a significant improvement in the performance. Although much of this improvement can be attributed to the almost doubling in size of the input data used to generate the reference profile.

In 1990, Williams established a fundamentally different approach to keystroke analysis, namely dynamic identity verification. The major steps in the dynamic identification algorithm were first to generate a reference profile for each person. This was done by computing the frequency, mean and standard deviation for each digraph. The next step was for each of the profiles to be computed with the following reference profile: (a) consider the next keystroke and time value; (b) apply sequential statistics theory to compare the digraph against the reference profile; (c) if possible, determine whether the typist has either passed or failed the test for that particular digraph; (d) compute the number of individual digraph tests that have been passed or failed; (e) depending upon how many digraph tests have been passed or failed, take one of the following actions: (1) accept the typist as valid, (2) reject the typist, (3) neither accept or reject, but continue testing. Under ideal situations every digraph would be used as part of the authentication. However, a number of the digraph pairs were under-represented – the final analysis was based on the top eight digraphs in a 500 character set. A primary goal of this experiment was to accelerate the process of accepting or rejecting a typist in real time and in the final experiment many impostors were rejected less than 100 keystrokes into the document. All but four typists (of 36) were correctly identified giving rise to a FRR of 11.1% and a FAR of 12.8%. Although, as the authors comment, increasing the reference text so as to include more digraph pairs would accelerate the decision process, 100 keystrokes is a considerable

amount of text to be typing before you get authenticated. Whereas static keystroke techniques usually only require 10-20 keystrokes.

Joyce and Gupta (1990) published a paper on a static authentication system with a degree of success not seen in keystroke analysis before. The experiment managed to achieve the first ground breaking results for a keystroke verifier, achieving a FRR of 16.36% and a FAR of 0.25% with a short input string. The reference profile is generated from the user entering his/her username, password, first name and last name eight times. The mean reference signature is then computed by calculating the mean and standard deviation of the eight values for each latency after having removed the outliers. The test profile data is compared with the reference profile, and if the values are above the threshold then the user is rejected (the threshold is defined as being the mean plus 1.5 standard deviations). The evaluation of the verifier was achieved using 33 participants. Once the reference profile was obtained, the user attempted to log on five times and six impostors were randomly selected to attempt to log on for a further five times. Impostors were given the log on data required to successful log on, but had not been present whilst the valid user had logged on. However, the FAR results largely depend on the six randomly chosen impostors and could, under a difference six users, vary the results considerably. Also, an arguable weakness of this approach is concerned with those users who have a large standard deviation and thus large threshold value. Valid users may well find their false rejection rates low but are also likely to find the false acceptance rates also higher, as it would be easier for unauthorised users to gain access due to the wider boundaries of acceptance. An approach which adaptively sets the threshold boundary on a per user basis would likely improve the performance further.

Based principally upon Joyce and Gupta's work, a number of researchers began to more thoroughly research the application of keystroke analysis. One notable investigation came in the form of Brown and Rogers (1993), one of the first papers to use a branch of artificial intelligence referred to as neural networks in order to solve the verification problem. Brown's and Rogers use a number of techniques in their experiment including two different neural networks, the Adaline neural network and the backpropagation neural network, as well as a simple geometric distance measure (for comparative reasons). The key difference between the two neural network topologies is the Adaline network is restricted to a linear problem space, whereas the backpropagation network is capable of performing non-linear problems. The investigation measured both the key hold time and digraph latency, and 25 participants were used in the generation of reference profiles with a further 15 participants used to generate the test impostor data. The investigation is a static based verifier, with authentication based on participant's names. The techniques were all designed in order to minimise the FAR, as a result all three techniques gave a FAR of 0% with the distance measure producing a FRR of 14.9%, the Adaline technique producing a FRR of 17.4% and the backpropagation network producing a FRR of 12.0%. The authors interestingly conclude their paper with the following comment.

> *"An interesting aspect which deserves more attention is the disparity between the results for given individuals using different techniques. One possible explanation is that one technique may be sensitive to some set of identifiable traits in an individual's typing patterns which another technique is missing, while the sensitivities are reversed for a different individual."*

This suggests that a particular technique is more successful with some users than others and that if particular users were able to be identified as being more successful with one technique over another, then multiple techniques could be used in any one verification system in order to decrease the error rates individually. This investigation is similar to

Joyce and Gupta's (1990) research but has introduced the concept of multivariate data (keystroke latency and hold-time) and the use of neural networks which has resulted in a higher performance rate. The extent to which these two factors contributed to the improved performance is unknown.

A paper by Napier, Laverty, Mahar, Henderson, Hiron and Wagner (1995), details two studies. The first reproduced the initial experiment by Leggett and Williams (1987), but with a number of proposed improvements. The first was to use multivariate measure of latency as compared to the single measure and secondly a chi-square based distance between test digraphs and reference profiles instead of a z-test. The procedure followed that of Leggett and Williams (1988), with 67 participants and the results did show an improvement with the multivariate measure producing significantly lower error rates, combined FAR and FRR of 4% (z-test) and 2% (chi-square) compared to the univariate measure of 24% (z-test) and 11% (chi-square). Indicating the measurement of latency in terms of its two orthogonal components of keystroke latency and hold-time significantly increase the sensitivity of the approach. An additional improvement was the use of the chi-square rule which also produced fewer errors over the simpler z-test.

The second study looked at the need to examine the verification algorithm under more ecologically valid conditions and more specifically to test for temporal stability. This involved implementing the new algorithm again, but with independent data that had been collected a week later. It was expected that the performance would be poorer than in the first study (having used a bootstrapping method), and the results obtained have proven this with a combined FAR and FRR of 3.8%. Interestingly, these results were obtained by using a test sample of only 50 digraphs, in comparison to Leggett and Williams requiring more in the region of 100 digraphs before verification.

A paper by Obaidat and Macchairolo (1994) entitled "A Multilayer Neural Network System for Computer Access Security" describes an investigation into a static keystroke analysis authentication system based on a number of neural network configurations. The number of participants in this study is relatively small in comparison to the other papers reviewed with only 16 people. Nevertheless this paper does implement some novel approaches to the pattern classification problem. The input data consisted of 40 input vectors obtained from the username or ID, each of which consisted off 15 values collected over a six week period. The networks used in the classification were a traditional Back Propagation network, a Sum-of-Products network and a novel hybrid Sum-of-Products network. The hybrid network takes the Back Propagation network for the first layer and the Sum-of-Products network for subsequent layers. For the training of the networks the raw data set was separated into two parts, all the even-numbered and odd-numbered patterns of each user, and for any given simulation only half of the data set was used for training. This would ensure the networks were being tested on their ability to generalise, rather than to memorise the training set. An argumentative pitfall of this study arises with the evaluation of the networks where the complete dataset is used, including data that was used for the training of the networks. It would be unlikely for a neural network to misclassify an input that has been used during the training phase, and as such would provide an exaggerated increase in performance. In both the back propagation and hybrid sum-of-products networks, the lowest error rates achieved in one of the simulations was 2.5% and 4.2% respectively (cumulative error rate). The sum-of-products network performed only as well as 6.3%. Conversely, the networks performed as badly as 10.8%, 10.8% and 18.8% for the back propagation, hybrid sum-of-products and sum-of-products respectively. Although the back-propagation network performed best, taking other considerations such as training

time and complexity the hybrid sum-of-products network represents a good compromise, due to the simpler structure of the sum-of-products layer.

A second paper by Obaidat, co-authored by Sadoun (1997) entitled "Verification of Computer Users Using Keystroke Dynamics" builds on his first paper by looking at classifying users not only on the inter-key latencies but also on the hold times. The paper also considers a number of further classification algorithms, both pattern classification and neural network techniques.

The pattern classification techniques include:

1. K-Means Algorithm,
2. Cosine Measure,
3. Minimum Distance Algorithm,
4. Bayes' Decision Rule and
5. Potential Function Rule.

The neural network techniques include:

1. Back Propagation Network (BPNN),
2. Counterpropagation Network (CPNN),
3. Fuzzy ARTMAP,
4. Radial Basis Function Network (RBFN),
5. Learning Vector Quantisation Network (LVQ),
6. Reinforcement Neural Network (RNN),
7. Sum-of-Products (SOP) and
8. Hybrid Sum-of-Products (HSOP).

This paper is to the authors' knowledge, the most comprehensive study in terms of classification techniques and classification features implemented. However, similarly to the first study the number of participants is rather low, with only 15 subjects. The data was collected by each user giving 225 sequences a day over an eight week period, and consisted of user's ID or username. Unlike the first study this study uses a different dataset for training than for testing, resulting in a theoretically more accurate result. The most successful pattern recognition technique was the potential function algorithm followed by Bayes' rule. The minimum distance and K-means gave a similar performance with the least successful algorithm being the cosine measure. The hold time-based classification gave relatively better results as compared to the inter-key time-based classification. For instance the potential function algorithm performed for the inter-key based classification a FRR of 4.7% and FAR of 2.2%, the hold time classification a FRR of 2.9% and FAR of 1.6% and a combination of hold time and inter-key classification a FRR of 1.9% and FAR of 0.7%. In comparison however, the neural network techniques overall performed better. The results have shown the hold-time based classification is superior to the inter-key time-based classification, although the combined inter-key and hold time based classifications result in the lowest error rates. The most successful networks were the LVQ, RBFN and Fuzzy ARTMAP which gave a misclassification error of 0% for both the FAR and FRR. Other successful paradigms included the BP with sigmoid transfer function, HSOP and SOP which gave misclassification errors of (FRR/FAR) 0%/1%, 1%/0.5%, 4%/2.5% respectively. The least successful neural networks were the CPNN and BP with sine-delta transfer function. In all cases the hold time-based classification gave better performance accuracy than the inter-key based approach. The author concludes the paper by commenting about the use of neural networks to identify computer users is not just plausible but is very successful. So the opinion of the researchers, in comparison to

previous studies, is that keystroke analysis is indeed a plausible technique for discriminating users.

Two papers by Monrose and Rubin (1997, 1999) explore the use keystroke dynamics as a biometric for authentication. The main difference between the two papers was the duration of data collection, with the first paper collecting data over a seven week period compared to the more recent paper having collected data over an eleven month period. As such, the results from the more recent paper will be included here. The investigations were designed surrounding four classification algorithms and managed to acquire 63 participants for the study. The four algorithms were a Euclidean distance measure, a non-weighted probability method, a weighted probability method and a Bayesian classifier. The Euclidean distance measure is a straight forward distance comparison between a reference vector, typically a mean vector calculated from the reference profile, and a test vector. Given the test vector resides within a certain distance from the reference vector then the test vector is considered valid. The value of the distance between valid and invalid test vectors is definable by the designer of the verification system and can by variable between users. In the non-weighted probability method a score is obtained based on the probability of observing the test vector in the reference profile, given the reference mean and standard deviation. Higher probabilities are given to test vectors that are closer to the reference mean. The weighted probability measure comes from the understanding that some features are more reliable than others simply because they come from a larger sample set or have a relatively higher frequency in the written language, so it would be reasonable to attach weights to those features. Therefore the notion of weights is added to the non-weighted probability formulae. The Bayesian approach used a standard Bayesian classifier, assuming the input data is distributed according to a Gaussian distribution. The participants were asked to retype a few sentences from a list of available phrases. The paper evaluated the results by

combining the acceptance of the authentic user and the rejection of the impostor, i.e. combining all the correct results together. The correct identification rate using the Euclidean distance was 85.63%, the non-weighted probability was 85.63%, the weighted probability was 87.13% and the Bayesian classifier was 92.14% representing an improvement of almost 5% over the next best result. The paper however includes no information as to the length of the sentences and the number of characters required to provide the authentication. Interestingly, the study also included the use of "free-text" (text independent authentication) as a dynamic approach to authentication but the results were found to vary too significantly to be of reliable use.

Cho, Han, Hee Han and Kim (2000) also included the multivariate input data (hold time and inter key latency) and neural networks. This study essentially repeats the previous Obaidat (1997) study with slight modifications to the procedure. Twenty five participants were used in the study, each being asked to enter a password of 7 characters. The participants entered the password between 150 to 400 times with the last 75 being used to test the network. The authors did however remove 4 participants from the study due to the large variance of their input data, which will artificially bias the results when considering the plausibility of the approach towards the general population, as the other studies have done. The network implemented was a Multi Layered Perceptron model and it was compared against a *K*-NN approach. The *K*-NN approach with *K* equal to one gave an average FRR of 19.5% with a FAR 0% whereas the multi-layered perceptron model gave a FRR of 1.0% with a FAR of 0%, representing a significant improvement. The results achieved here are very encouraging for static authentication, although care must be taken considering the relative artificial selection of participants.

The final paper reviewed was the only paper that looked at using the numeric keypad of a full-sized alpha numeric keyboard. Ord and Furnell (2000) looked at authenticating a person using a static keystroke analysis approach. The study had 14 participants which each inputted the same numerical code on the keypad 50 times over a period of 6 months. The dataset was split into two with 30 input samples being used to generate the reference profile and 20 samples to test the classifier. The authors decided on a neural network approach to classification, implementing a Multi-Layered Perceptron model with back propagation learning. The results are not as good as previous research into keystroke analysis has suggested, but of course the different input medium must also be considered. The classifier achieved a FAR of 9.9% with a fixed FRR of 30%. The authors described the cause of this higher error rate to be due to a minority of users with very high error rates, and as such it could be concluded that this technique may only be applicable to users that can enter the input data within certain tolerances. This is a finding that has been reiterated by the exclusion of certain poor performing users from Cho et al's (2000) investigation.

It is very difficult to directly compare and contrast many of these studies in terms of their verification system and performance as their method for evaluating (and calculating) the error rates differ depending upon the aim of the study. For example, while some were static-based verifiers, others were dynamic-based with varying character lengths inputted. However overall the studies have in a number of cases shown encouraging results in the ability of pattern classifiers to correctly discriminate between users. It can been seen from the studies that neural network classifiers have on a number occasions performed both well in their own respect and better in comparison to the more traditional statistical and pattern recognition techniques. Notably, the original idea of keystroke analysis proposed that a persons typing rhythm is distinctive and all the original studies focussed upon the keystroke latency (the time between two successive keystrokes), however, more recent

studies have identified the hold time (the time between pressing and releasing a single key) as being as discriminative. The most successful networks implemented a combination of both inter key and hold time measures, illustrating the use of both measures have a cumulative and constructive effect upon performance. Another conclusion that can be drawn from the reviewed papers is the inability for keystroke analysis to perform successfully for a minority cross section of users. These users tend to have high inter-sample variances and have few distinctive typing rhythms. As such, any authentication system that implements a keystroke analysis technique would also have to consider the small number of users that will exhibit too higher an error rate in order to ensure both the security and user convenience factors required by the overall system are met.

Appendix C

Theory of Pattern Recognition

Theory of Pattern Classification

Pattern classification or pattern recognition is an area of science with connections to many subjects such as engineering, computing and medical diagnosis. Due to its wide application, the development of pattern recognition techniques has varied greatly depending upon the background discipline of the researcher. Consequently, many different techniques have been created from what would typically have been orthogonal research areas, from statistics to artificial intelligence.

This section describes the prerequisites required for a pattern recognition system, before continuing to describe an overview of the statistical and neural network theory required to design a pattern classifier.

1 Development of a Pattern Recognition System

Although, many different pattern recognition techniques have been developed, the majority of them utilise a common framework, as illustrated in Figure 1. They begin with a method of reading or sensing the pattern to be classified. The sensor can take various forms and will largely depend on the pattern classification problem itself. In this particular situation it takes the form of sensing keypad interactions. The pre-processing and post-processing stages are optional and will manipulate the sensor data into a more usable or functional form if necessary, such as removing outliers and scaling the input. Feature extraction is the process of removing the actual discriminative information from the pre-processed data and is one of the curial stages

in the pattern classification design. The pre-processed data is likely to contain information that is one of three types:

1. Positive discriminative information
2. Negative discriminative information
3. No discriminative information

When working correctly the feature extraction process should extract the positive discriminative information. Negative discrimination contains the information that hinders the pattern classification process, and no discrimination information makes the task of pattern classification more difficult, typically by placing the problem in a higher dimensionality. This is known as the curse of dimensionality (Bishop, 1995), and thus requires a more complex pattern classification technique, but adds nothing in terms of improving performance to the classifier.

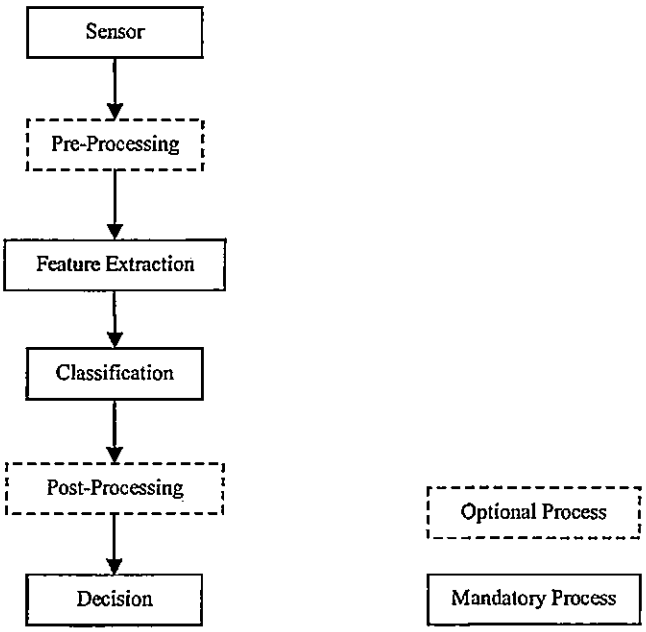


Figure 1 A Pattern Classification System

The classification stage utilises a particular pattern recognition technique, and is the key stage in the pattern recognition process. The choice of pattern recognition technique can often determine the success or failure of pattern recognition system. A system too simple for the problem will not discriminate enough, whereas a system too complex for the problem will create far too complex discriminative boundaries enabling poor generalisation to new data (the concept of generalisation and the issues arising from not controlling it are addressed in section 3.1). Finally, in the pattern recognition system, a final decision is to be made which determines which class of object the input belongs too. This typically can take the form of a threshold function, for instance, above the threshold the input is class 1 and below, class 2.

2 Statistical Pattern Classification

The traditional approach of solving a pattern recognition problem is through the use of a statistically based technique, with much of the work on keystroke analysis pre-1990 being completed using such techniques. Although a wide range of statistical techniques have been developed over the years this report focuses on three principal techniques:

1. Mean & Standard Deviation Technique
2. Minimum Distance Techniques
3. Hypothesis Techniques

These three techniques encompass a range of approaches that have been implemented in previous pattern classification research, from the simple mean and standard

deviation technique utilised by Umphress and Williams (1985), to the more complex hypothesis techniques utilised by Napier et al (1995). The reason for their inclusion in this study is two-fold – as a means to evaluate the performance of statistical techniques in their own right, but also as a means of comparison against the more modern neural networks approaches.

2.1 Mean & Standard Deviation Technique

A traditional pattern classifier, this technique utilises a user's mean and standard deviation, calculated from their reference profile to determine whether an input sample is from an authorised user or an impostor. The authentication decision is based upon the principal that an authorised users input will fall within the profile mean plus or minus a predefined number of standard deviations and an unauthorised users input vectors will not (Umphress & Williams, 1985). The technique assumes a user's input data is normally distributed, so a probability exists that 68% of an authorised users input will fall within 1 standard deviation and 95% within 2. Figure 2 illustrates a fictitious example of normal distribution plots for a number of users.

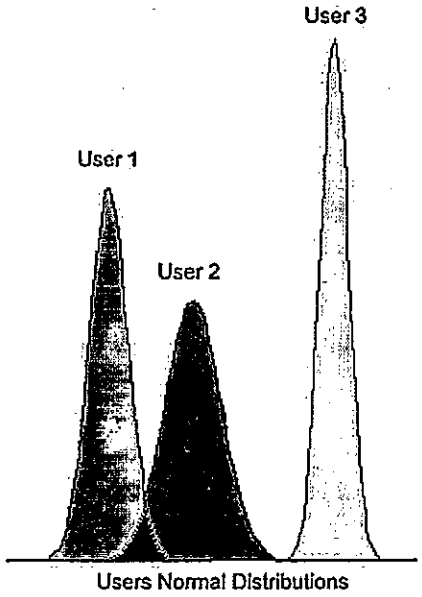


Figure 2 Normal Distribution Plot

Although this technique has many application advantages such as the lower processing requirements and faster speed of training, it is also the simplest algorithm implemented in this study and as such is not overly powerful. For instance, if a user had a large standard deviation then the classifier would naturally have a high false acceptance due to impostor input vectors residing within the mean and standard deviation envelope. This would however be tied to a lower false rejection rate.

2.2 Minimum Distance Technique

The minimum distance technique calculates the distance between two vectors, a reference mean vector and the input sample vector. If the resulting distance is considered small enough then the input sample is deemed to have come from an authorised user, if not then from an impostor.

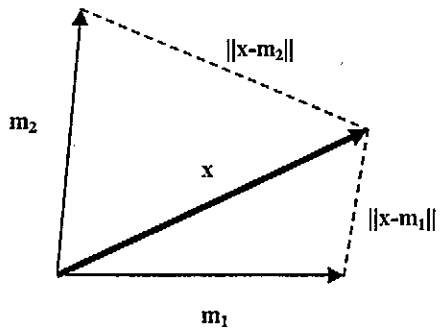


Figure 3 Vector Distance Calculation

Figure 3 illustrates this vector distance calculation, between the reference vector x and a number of input vectors m. The shorter the distance between these two vectors, the higher the probability of both input vectors belonging to the same person.

Distance is calculated using:

$\| x - m_k \|$ where x = input vector; m_k = reference profile vector

Here || u || is called the norm of the vector u and corresponds to different ways of measuring distance. In this study a linear distance metric is shown (Duda & Hart, 1973):

- Euclidean Metric (Linear)

$$\| u \| = (u_1^2 + u_2^2 + u_3^2 + ...u_d^2)^{\frac{1}{2}}$$

$$\| u \| = ((x_1 - m_{k_1})^2 + (x_2 - m_{k_2})^2 + (x_d - m_{k_d})^2)^{\frac{1}{2}}$$

Where, $x_1 = 1^{st}$ component of the input vector

$x_2 = 2^{nd}$ component of the input vector

x_d = d'th component of the input vector

m_d = d'th component of the reference template

From an investigative perspective the distance permitted to be acceptable as an authorised user can be varied for each user in order to achieve the most optimal results.

2.3 Hypothesis Technique

Statistical hypothesis tests are used to test a hypothesis that some variable differs between two groups (Hogg & Ledolter, 1989). In this study, the hypothesis test is to determine that an input sample comes from the authorised user or not. The specific hypothesis test described in this study is the t-test.

The t-test is used when the sample size is typically small and the standard deviations are unknown but assumed equal. As the sample sizes in a keystroke analysis approach might well reside in either case, it is appropriate to describe both tests.

The null and alternative hypotheses for the t-test is:

Null Hypothesis, H_0: *Input Vector Mean* = *Reference Profile Mean*

$\mu_0 = \mu_x$

Alternative Hypothesis, H_1: *Input Vector Mean* *Reference Profile Mean*

μ_0 μ_x

As the alternative hypothesis is "*not equal to*" a two-tailed z and t test are required and the level of significance, α, will vary in order to determine the most efficient level in terms of the performance rates. The test statistics for both tests are:.

$$t = \frac{\bar{x} - \mu_0}{\frac{s_x}{\sqrt{n}}}$$

Where, $\bar{x}$ = Mean input vector;

u_0 = Mean reference vector or template

S_x = Sample variance of input vector

n = Population size

3 Neural Network Pattern Classification

Neural Networks, known originally as Artificial Neural Networks in order not to get confused with their biological counterparts, is a branch of artificial intelligence concerned with mimicking the functionality of biological neurons. The background work in neural networks occurred in the late 19th and early 20th centuries, however the modern view of neural networks began with McCulloch and Pitts (1943) who demonstrated that networks of artificial neurons could theoretically compute any arithmetic or logical function. However, it was not until 1958 that the first practical application of neural networks was created (Rosenblatt, 1958), with the invention of the perceptron network, and its ability to perform pattern recognition. However this first network suffered from some inherent weaknesses, which were identified in an infamous book by Minsky et al (1969) called Perceptrons. For instance, single layer perceptron networks were unable to solve non-linear problems and although Rosenblatt et al. designed multi-layer networks to overcome this issue they were not able to modify their learning algorithms to train the network. This new learning rule did not arrive until 1986 when the backpropagation algorithm was invented by Rumelhart and McClelland. It was at this stage where the field of neural networks opened up and found real interest in a large number of applications and industries.

In this section, a number of network topographies will be introduced that have in past experience proven successful and exemplify pattern associative problems such as this (Looney, 1997; Obaidat et al., 1997).

In particular this section will describe the following neural network topologies:

1. Feed-Forward Multi-Layered Perceptron Model
2. Radial Basis Function Model
3. Generalised Regression Model

3.1 Feed-Forward Multi-Layered Perceptron

The multi-layered perceptron (MLP) network as the name might suggest is constructed using a number of perceptron layers with the key advantage of being able to perform non-linear problem solving. The feed-forward multi-layer perceptron network is built up with an input layer, an output layer and one or more hidden layers, although when counting the number of layers in a network the input layer is omitted as it provides no processing of data – so a 3 layer network would consist of an input layer, 2 hidden layers and an output layer. Every input is connected to every neuron in the layer, with each connection containing an associated weight. It is these weights that store and provide the neural network with their apparent memory. Figure 4 illustrates a 3 layer MLP and each layer essentially consists of the same repeating layer connected to the output of the previous layer.

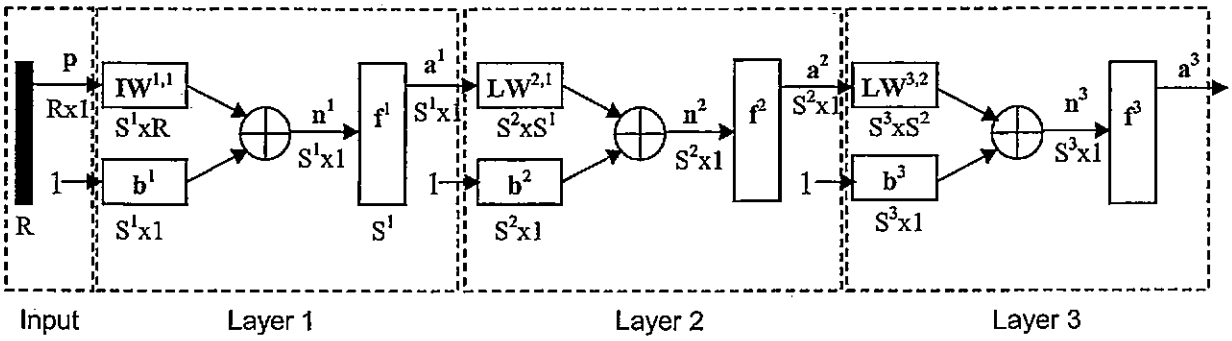


Figure 4 Three Layer Feed-Forward MLP

The network is comprised of the following components.

p - Input vector

R - Dimension of input vector P

S^x - Number of neurons in layer x

$IW^{a,b}$ - Input Weight ~ 'a' indicates destination, 'b' indicates source

$LW^{a,b}$ - Layer Weight ~ 'a' indicates destination, 'b' indicates source

b^x - Bias value in layer x.

a^x - Output from layer x.

x - A number from 1 to 3

When constructing a MLP network a number of decisions need to be made regarding the network variables, which depend largely upon the complexity of the problem the network is to solve. Unfortunately very few guidelines or instructions exist to indicate what the value of these design variables should be given a certain complexity of problem, so a process of trial and error, in combination with previous investigations and experience, is often used as a guide for construction. The main design variables are:

1. Number of neurons in each layer
2. Number of layers in the network
3. Transfer function
4. Training/Learning algorithm
5. Number of epochs (training cycles)

Given sufficient neurons and a good training strategy, a single hidden layer MLP network is able to mathematically approximate any function to an arbitrary accuracy (Bishop, 1995), so an argument exists as to whether networks with more than one hidden layer are ever required. The reasoning behind networks needing more than one hidden layer has been suggested by Looney (1997) and Bishop (1995), amongst others, is that the extra layers might make a more efficient approximation in the sense of achieving the same level of accuracy but with fewer neurons, weights and biases. However, care needs to be taken as adding too many hidden layers will cause network performance to degrade rather than improve. Care needs to be taken to ensure the network has sufficient neurons to solve the problem, but not too many to make training computation too difficult and time consuming. Intertwined with the problem of the number of neurons is the number of training epochs you train the network with. Too few and the network cannot solved the problem and too many and the network does not generalise very well. The problem of generalisation is a wider issue for MLP networks and will be discussed shortly. The choice of transfer function is very problem dependant, if the problem to be solved is inherently linear then linear transfer functions would suffice, whereas more complex and non-linear problems would be suited to a non-linear transfer such as the hyperbolic tangent sigmoid function. This

transfer function is particularly useful due partly, for its non-linear properties and ability to squash the input into a +1 to -1 range, and also, from its success in previous neural network investigations (Obaidat et al., 1997; Ord et al, 2000).

MLP networks have a number of different training algorithms (or learning algorithms), although the most common utilised is the Backpropagation algorithm (Haykin, 1999; Hagan et al., 1996). Figure 5 illustrates the training process of the MLP network. Training is performed first by a forward sweep of the network, generating the output. The output is then compared to a known or desired output and an error is generated. This error is then, through a backward sweep of the network, fed back to the individual weights and biases. The proportion of the error given to each weight is dependent on the contribution made by that weight to the final result.

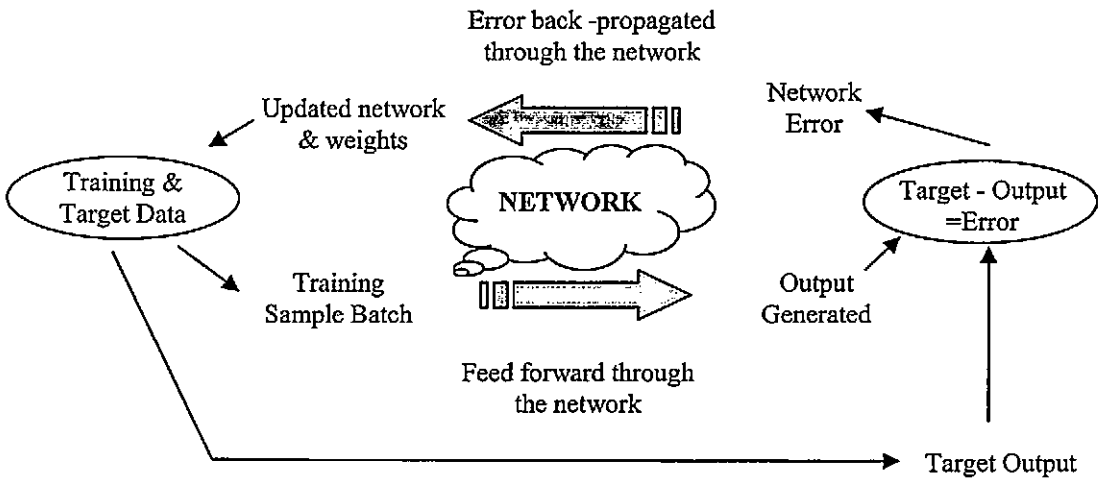


Figure 5 MLP Training Process

The simplest backpropagation method is an approximate steepest descent algorithm, in which the performance index is a mean square value, causing the convergence towards expected outcomes (Hagan et al. 1996). Hence the importance of the training

data and why it must be representative of the problem to be solved. A particular problem of backpropagation algorithms is they have a tendency to converge towards a local minimum rather than the desired global minima and as such a variation on the steepest descent algorithm has been design to include a momentum term. The momentum term allows a network to respond not only to the local gradient, but also to movements in the error surface, acting like a low pass filter allowing the network to ignore small features in the error surface. A second term can also be added to speed up the process of convergence. By adding an adaptive learning rate, the training process can maximise the rate without causing oscillations, changing the rate dependant upon the local error surface. Too small learning rate would result in long convergence times (Demuth & Beale, 2001).

The problem of generalisation, as highlighted previously, describes the ability of a network to successfully output the correct response given an unseen or new input. When you train the network to perform a task, only a finite amount of training data exists and the network learns the problem from that dataset. A fictitious example of generalisation is illustrated in Figure 6. As the complexity of model is increased, so the decision boundary can become more complex, and hence give a better fit to the training data. However the best generalisation performance can often be obtained from an intermediate level of complexity.

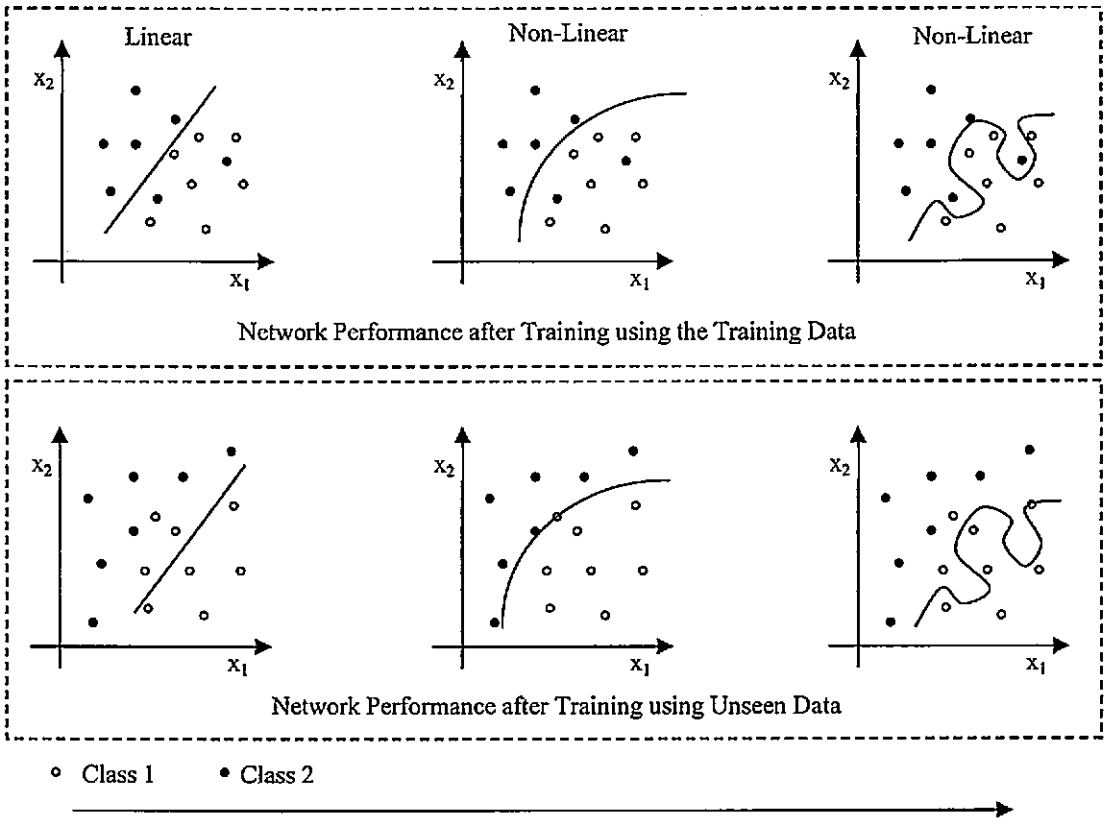


Figure 6 Problem of Poor Generalisation

Generalisation is less of an issue for situations where the number of network parameters is small compared to the training data, as the network is able to refine the network weights and biases to a broader spectrum of input data. For networks without enough training data, the test of the network comes when presenting the network with new and unseen data and for the network to successfully classify the input. In order for a network to achieve this, it needs to be able to generalise well. One method for ensuring good generalisation is to construct a network that is just large enough to provide an adequate fit, since the larger the network in use the more complex functions it can approximate, as demonstrated in Figure 6. This is a difficult task to achieve in practicality as there are no guidelines defining the size of a network given a

problem of given complexity. Alternatively, the designer could choose an oversized network configuration and control the complexity of the decision boundaries formed through the number of epochs the network is trained with – the more a network is trained, the more complex the decision boundaries will become in an attempt to minimise the error.

3.2 Radial Basis Function Networks

Radial basis function (RBF) networks are very similar mathematically to MLP networks in that they both provide techniques for approximating arbitrary non-linear functional mappings between multi-dimensional spaces (Bishop, 1995). The RBF network consists of two layers, plus an input stage, illustrated in Figure 7. The first layer, again often referred to as the hidden layer, is the radial basis layer. This layer applies a non-linear transformation from the input space to the hidden space, which in most applications is of higher dimensionality. This is achieved by first calculating the Euclidean distance between the input vector and the weight matrix, which in turn, through matrix multiplication is combined with a bias to provide an extra element of sensitivity. The next stage in the layer is to present the result the matrix multiplication to the radial basis transfer function, which acts as a detector producing a 1 whenever the input vector is identical to its weight vector. An illustration of the radial basis transfer function is shown in Figure 8. The second layer or output layer is a linear layer which is capable of linear separation of the classes. The rationale behind such a paradigm is that a pattern classification problem cast in high dimensional space is more likely to be linearly separable than in low dimensional space (Cover, 1965).

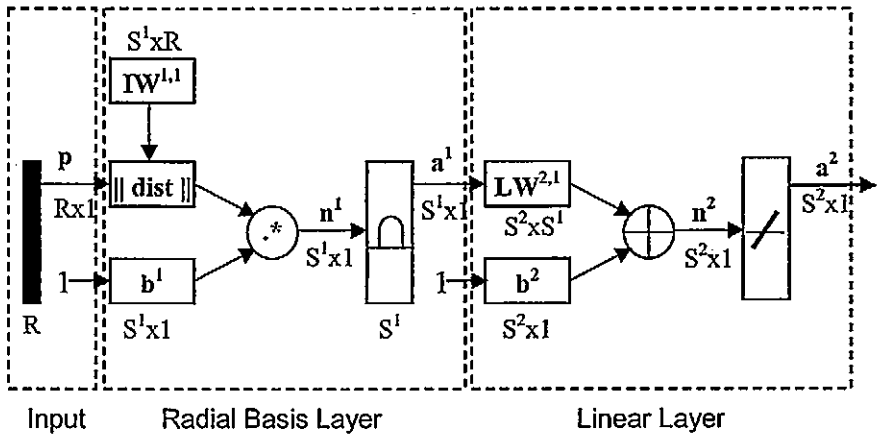


Figure 7 Radial Basis Network

p - Input vector

R - Dimension of input vector P

S^x - Number of neurons in layer x

$IW^{a,b}$ - Input Weight ~ 'a' indicates destination, 'b' indicates source

$LW^{a,b}$ - Layer Weight ~ 'a' indicates destination, 'b' indicates source

b^x - Bias value in layer x.

a^x - Output from layer x.

x - A number from 1 to 2

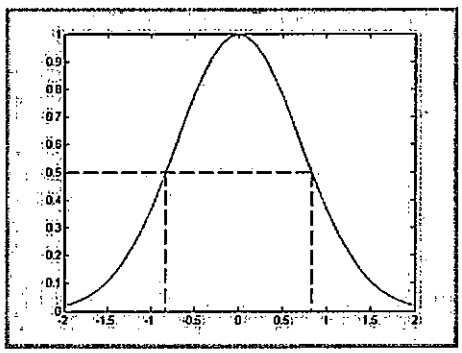


Figure 8 Radial Basis Transfer Function

The training process for the RBF network is to iteratively add one neuron at a time until the sum-squared error falls beneath an error goal or the maximum number of neurons has been reached. This tends to lead to one of the major disadvantages of

RBF networks in that even when designed efficiently they may have many times more neurons than a comparable feed-forward MLP with sigmoid transfer functions. The reason for this is that sigmoid transfer functions can have outputs over a large region of the input space, whereas radial basis neurons only respond to a relatively small region of the input space, resulting in more neurons being required the larger the input space is. Conversely however, RBF networks often take far less time to train than their MLP counterparts and do not get stuck in local minima as MLP networks often do, as the input data need only be presented to the network once.

Additionally, from an implementation perspective RBF networks have far fewer network variables to define than MLP networks with no decisions over network layers, number of training epochs or even number of neurons, culminating in fewer network combinations to design and test. The design variables are:

1. Goal – mean squared error, defaulted to zero
2. Spread – Radial Basis function spread
3. Maximum number of neurons – defaulted to equal up to the number of input vectors (also referred to as an Exact RBF network)

However, RBF networks suffer the same generalisation problem as MLP networks with large spread values allowing for a smoother function approximation and better generalisation, by allowing a number of the radial basis neurons to overlap thus giving a number of neurons fairly large outputs at any given moment. However, if the spread value is too large, each neuron is effectively responding to the same large area of input space, too small and the network does not generalise well (Hassoum, 1995).

3.3 Generalised Regression Networks

A Generalised Regression Neural Network (GRNN) is a network that utilises the radial basis layer. GRNN is described as a universal approximator for smooth functions, given enough training data (Sarle, 2002). The GRNN can be thought of as a normalised RBF network and is very similar to the Exact RBF network, with a second linear layer replaced by a special linear layer. This special layer provides a weighted average of the target values of training vectors close to the given input vector.

The network topology is illustrated in Figure 9.

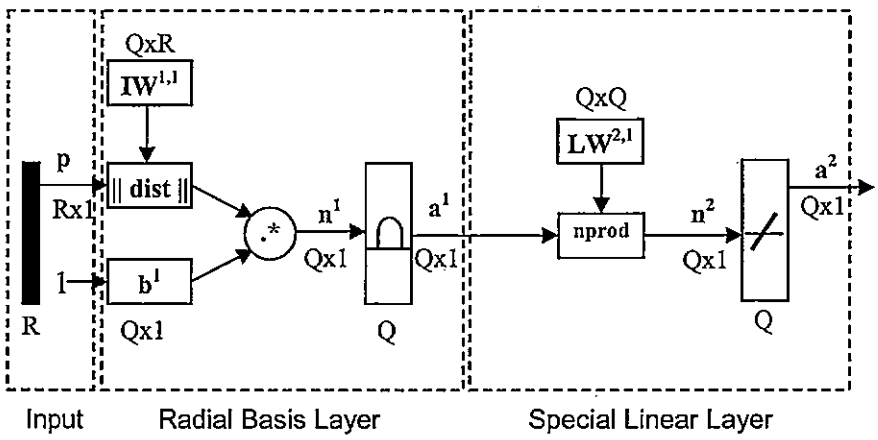


Figure 9 Generalised Regression Network

p - Input vector

R - Dimension of input vector P

Q - Number of neurons in layer x – number of training vectors

$IW^{a,b}$ - Input Weight ~ 'a' indicates destination, 'b' indicates source

$LW^{a,b}$ - Layer Weight ~ 'a' indicates destination, 'b' indicates source

b^x - Bias value in layer x.

a^x - Output from layer x.

x - A number from 1 to 2

The main drawbacks of GRNNs is that it suffers badly from the curse of dimensionality (Bishop, 1995) – network complexity increases exponentially with the dimension of the input space – and the one-to-one mappings of training vectors to neurons can give rise to large and complex networks.

However, GRNNs are amongst the fastest trained neural networks and only require a single network parameter to be defined, the spread. As with RBF networks, the larger the value of spread, the smoother the function approximation will be. Typically to fit data closely, the use of a spread value smaller than the distance between input vectors should be used (Demuth & Beale, 2001). As only a single parameter needs to be defined, iteratively training GRNNs with varying values for spread in order to optimise network performance, is far less time consuming than for MLP networks.

Appendix D

Feasibility Study of Keystroke Analysis

Part 1 – Numeric Input Data

Part 2 – Alphabetic Input Data

Part 3 – Keystroke Analysis Prototype

Appendix D

Part 1 – Numeric Input Data

This appendix is divided into the following sub-sections:

1. List of Input data utilised by participants in the study
2. Data Collection application – Source code
3. MatLab pattern classification – Source code
4. Pattern Classification Results

This appendix can be located on the CD-ROM

Appendix D

Part 2 – Alphabetic Input Data

This appendix is divided into the following sub-sections:

1. List of Input data utilised by participants in the study
2. Data Collection application – Source code
3. MatLab pattern classification – Source code
4. Pattern Classification Results

This appendix can be located on the CD-ROM

Appendix D

Part 3 – Keystroke Analysis Prototype

This appendix can be located on the CD-ROM

Appendix E

IAMS Software Prototype

Part 1 – IAMS Software Code

Part 2 – IAMS Validation Output

Part 3 – Keystroke Analysis Implementation

Appendix E

Part 1 – IAMS Software Code

This appendix is divided into the following sub-sections:

1. IAMS Authentication Manager software code
2. Administrative Console software code
3. Client Interface software code

This appendix can be located on the CD-ROM

Appendix E

Part 2 – IAMS Validation Output

```
Initialising Database Connections...

IAMS Client Database Connected
IAMS Profile Database Connected
IAMS Input Cache Database Connected

Database Connections Complete.

Initialising Biometric Modules...

Initialised Facial Recognition
Initialised Keystroke Analysis

Initialisation Complete!

Device Connected: 07976367359

Client Parameters...
System Integrity Level: 0
Authentication Level: 1
System Integrity Period: 20

System Integrity Level: 0

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 0

Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Tempaory Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

System Integrity Level: 0.5

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 0.5

Biometric Technique: Keystroke Analysis Sub Category: Telephone_01248618453
Biometric Sample has been moved into the Tempaory Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

System Integrity Level: 1.5

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 1.5
```

```
Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Tempaory Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

System Integrity Level: 2

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 2

Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Tempaory Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

System Integrity Level: 2

Connection closed: 192.168.3.11
```

```
Initialising Database Connections...

IAMS Client Database Connected
IAMS Profile Database Connected
IAMS Input Cache Database Connected

Database Connections Complete.

Initialising Biometric Modules...

Initialised Facial Recognition
Initialised Keystroke Analysis

Initialisation Complete!

Device Connected: 07976367359

Client Parameters...
System Integrity Level: 0
Authentication Level: 1
System Integrity Period: 20

System Integrity Level: 0

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 0

Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Failed

Authentication Level: 3

System Integrity Level: -0.5

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Facial Recognition
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Unable to locate Facial Print within Image with sufficient detail

Biometric Failed

Authentication Level: 3

System Integrity Level: -2.5

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Cognitive Response
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Cognitive Response
Authentication Result: Password Failed
Authentication Level: 4
```

Test 1b - IAMS_Output_Log.txt

```
System Integrity Level: -4.5

Processing Intrusive Biometric Input Sample...
Device Unlock Code Entered Correctly!
Authentication Level: 1
Authentication Level: 1

System Integrity Level: 0
```

```
Initialising Database Connections...

IAMS Client Database Connected
IAMS Profile Database Connected
IAMS Input Cache Database Connected

Database Connections Complete.

Initialising Biometric Modules...

Initialised Facial Recognition
Initialised Keystroke Analysis

Initialisation Complete!

Device Connected: 07976367359

Client Parameters...
System Integrity Level: 0
Authentication Level: 1
System Integrity Period: 20

System Integrity Level: 0

Processing Intrusive Biometric Input Sample...
Authentication Level: 1

System Integrity Level: 0

Biometric Technique: Intrusion Sub Category: Facial Recognition
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success

Biometric Passed

Authentication Level: 1

System Integrity Level: 2

Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 2

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Facial Recognition
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success
Biometric Passed

Authentication Level: 1

System Integrity Level: 4

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate
```

```
Authentication Level: 2

System Integrity Level: 4

Biometric Technique: Facial Recognition Sub Category: None
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success

Biometric Passed

Authentication Level: 1

System Integrity Level: 5

Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 5

Processing Biometric Input Sample...
Biometric Technique: Facial Recognition Sub Category: None
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success

Biometric Passed

Authentication Level: 1

System Integrity Level: 5
```

```
Authentication Level: 1
System Integrity Level: 0

Initialising Database Connections...

IAMS Client Database Connected
IAMS Profile Database Connected
IAMS Input Cache Database Connected

Database Connections Complete.

Initialising Biometric Modules...

Initialised Facial Recognition
Initialised Keystroke Analysis

Initialisation Complete!

Device Connected: 07976367359

Client Parameters...
System Integrity Level: 0
Authentication Level: 1
System Integrity Period: 20

System Integrity Level: 0

Processing Intrusive Biometric Input Sample...
Authentication Level: 1

System Integrity Level: 0

Biometric Technique: Intrusion Sub Category: Facial Recognition
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Unable to locate Facial Print within Image with sufficient detail

Biometric Failed

Authentication Level: 2

System Integrity Level: -2

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Cognitive Response
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Cognitive Response
Authentication Result: Password Failed
Authentication Level: 3

System Integrity Level: -4

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Cognitive Response
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Cognitive Response
Authentication Result: Password Failed
Authentication Level: 3
```

```
System Integrity Level: -5

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Cognitive Response
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Cognitive Response
Authentication Result: Password Failed
Authentication Level: 4

System Integrity Level: -5

Processing Intrusive Biometric Input Sample...
Device Unlock Code Entered Correctly!
Authentication Level: 1
Authentication Level: 1

System Integrity Level: 0
```

```
Initialising Database Connections...

IAMS Client Database Connected
IAMS Profile Database Connected
IAMS Input Cache Database Connected

Database Connections Complete.

Initialising Biometric Modules...

Initialised Facial Recognition
Initialised Keystroke Analysis

Initialisation Complete!

Device Connected: 07976367359

Client Parameters...
System Integrity Level: 0
Authentication Level: 1
System Integrity Period: 20

System Integrity Level: 0

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 0

Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

Authentication Level: 1

System Integrity Level: 0.5

Processing Intrusive Biometric Input Sample...
Authentication Level: 1

System Integrity Level: 0.5

Biometric Technique: Intrusion Sub Category: Facial Recognition
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success

Biometric Passed

Authentication Level: 1

System Integrity Level: 2.5

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2
```

```
System Integrity Level: 2.5

Biometric Technique: Keystroke Analysis Sub Category: Text_eta
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

Authentication Level: 1

System Integrity Level: 2.5

Processing Biometric Input Sample...
Biometric Technique: Keystroke Analysis Sub Category: Telephone_01248618453
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Passed

Authentication Level: 1

System Integrity Level: 3

Processing Biometric Input Sample...
Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 3

Biometric Technique: Facial Recognition Sub Category: None
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success

Biometric Passed

Authentication Level: 1

System Integrity Level: 5
```

```
Initialising Database Connections...

IAMS Client Database Connected
IAMS Profile Database Connected
IAMS Input Cache Database Connected

Database Connections Complete.

Initialising Biometric Modules...

Initialised Facial Recognition
Initialised Keystroke Analysis

Initialisation Complete!

Device Connected: 07976367359

Client Parameters...
System Integrity Level: 0
Authentication Level: 2
System Integrity Period: 20

System Integrity Level: 0

Processing Biometric Input Sample...
Authentication Level: 2

System Integrity Level: 0

Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Failed

Authentication Level: 3

System Integrity Level: -0.5

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Facial Recognition
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Unable to locate Facial Print within Image with sufficient detail

Biometric Failed

Authentication Level: 3

System Integrity Level: -2.5

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Cognitive Response
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Cognitive Response
Authentication Result: Password Failed
Authentication Level: 4

System Integrity Level: -4.5
```

```
Processing Intrusive Biometric Input Sample...
Device Unlock Code Entered Correctly!
Authentication Level: 1
Authentication Level: 1

System Integrity Level: 0

Connection closed: 192.168.3.11
```

```
Initialising Database Connections...

IAMS Client Database Connected
IAMS Profile Database Connected
IAMS Input Cache Database Connected

Database Connections Complete.

Initialising Biometric Modules...

Initialised Facial Recognition
Initialised Keystroke Analysis

Initialisation Complete!

Device Connected: 07976367359

Client Parameters...
System Integrity Level: 0
Authentication Level: 1
System Integrity Period: 20

System Integrity Level: 0

Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 0

Processing Biometric Input Sample...
Biometric Technique: Keystroke Analysis Sub Category: Telephone_Dynamic
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Failed

Authentication Level: 3

System Integrity Level: -0.5

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Facial Recognition
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success

Biometric Passed

Authentication Level: 1

System Integrity Level: 1.5

Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 1.5

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Facial Recognition
```

```
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success

Biometric Passed

Authentication Level: 1

System Integrity Level: 3.5

Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 3.5

Processing Biometric Input Sample...
Processing Biometric Input Sample...
Biometric Technique: Keystroke Analysis Sub Category: Telephone_01248618453
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Biometric Technique: Keystroke Analysis Sub Category: Text_eta
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Failed

Authentication Level: 3

System Integrity Level: 3

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Facial Recognition
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Fail

Biometric Passed

Authentication Level: 1

System Integrity Level: 5

Authentication Request...
Authentication Technique Utilised: Keystroke Analysis
Biometric Failed

Authentication Request...
Authentication Request - No Sample Present to Authenticate

Authentication Level: 2

System Integrity Level: 4

Processing Biometric Input Sample...
Biometric Technique: Facial Recognition Sub Category: None
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated
```

```
Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success

Biometric Failed

Authentication Level: 3

System Integrity Level: 2

Processing Intrusive Biometric Input Sample...
Biometric Technique: Intrusion Sub Category: Facial Recognition
Biometric Sample has been moved into the Temporary Caching Area
Input Cache Updated

Intrusive Authentication Request...
Authentication Technique Utilised: Facial Recognition
Facial Authentication Result: Success

Biometric Passed

Authentication Level: 1

System Integrity Level: 4

Connection closed: 192.168.3.11
```

Appendix E

Part 3 – Keystroke Analysis Implementation

This appendix can be located on the CD-ROM

Appendix F

Publications

LIST OF PUBLICATIONS

*Those marked with a * are included for reference. A copy of all publications can be found on the CD-ROM under "Publications".*

Journal & Conference Papers

Clarke, N., Furnell, S., Lines B., Reynolds, P. 2004. "Application of Keystroke Analysis to Mobile Text Messaging". Proceeding of the 3rd Security Conference, Las Vegas, USA.

Lemote, J., Clarke, N., Furnell, S. 2004. "Artificial Impostor Profiling for Keystroke Analysis on a Mobile Handset". Advances in Network & Communication Engineering

Clarke, N., Furnell, S., Lines B., Reynolds, P. 2003. "Keystroke Dynamics on a Mobile Handset: A Feasibility Study". Information Management & Computer Security.*

Clarke, N., Furnell, S., Lines B., Reynolds, P. 2003. "Using Keystroke Analysis as a mechanism for Subscriber Authentication Mobile Handsets". Proceedings of the IFIP SEC 2003 Conference, Athens, Greece.*

Clarke, N., Furnell, S., Reynolds, P. 2002. "Biometric Authentication for Mobile Devices". 2002. Proceedings of the 3rd Australian Information Warfare and Security Conference, Perth, Australia. ***(Recipient of Best Paper Award).****

Clarke, N., Furnell, S., Lines B., Reynolds, P. 2002. "Subscriber Authentication of Mobile Phones through the Implementation of Keystroke Dynamics". 2002. Proceedings of the 3rd International Network Conference (INC 2002), UK.

Clarke, N., Furnell, S., Lines B., Reynolds, P. 2002. "Advanced Subscriber Authentication Approaches for Third Generation Mobile Systems". Proceedings of the 3rd International Conference on 3G Mobile Communication Technologies, IEE, UK.

Clarke, N., Furnell, S., Rodwell, P., Reynolds, P. 2002. "Acceptance of Subscriber Authentication Methods for Mobile Telephony Devices". Computer & Security.*

Poster Presentations

Clarke, N., Furnell, S., Rodwell, P., Reynolds, P. 2002. " Non-Intrusive Biometric Authentication for Mobile Device". 5th World Conference & Exhibition on the Practical Application of Biometrics, UK. ***(Recipient of Best Student Poster).***

Clarke, N., Furnell, S., Rodwell, P., Reynolds, P., Dowland, P. 2001. "Non-Intrusive Subscriber Authentication for 3G Mobile Systems". Britain's Younger Engineers, House of Commons, UK.

Keystroke Dynamics on a Mobile Handset: A Feasibility Study

N.L. Clarke[†], S.M. Furnell[†] B.M. Lines[†] and P.L. Reynolds[‡]

[†] Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, Plymouth, United Kingdom.
[‡] Orange Personal Communications Services Ltd, Bradley Stoke, Bristol, United Kingdom.
Email: nrg@plymouth.ac.uk

Abstract

With the introduction of third generation phones, a technological transition is occurring in which the devices begin to have similar functionality to that of current personal digital assistants. The ability of these phones to store sensitive information, such as financial records, digital certificates and company records, makes them desirable targets for impostors. Current security for mobile phones is provided by the Personal Identification Number (PIN), which has weaknesses from both technological and end-user perspectives. As such, non-intrusive and stronger subscriber authentication techniques are required. This paper details the feasibility of one such technique, the use of keystroke dynamics. This feasibility study comprises a number of investigations into the ability of neural networks to authenticate users successfully based upon their interactions with a mobile phone keypad. The initial results are promising with individual users' classification performing as well as 0% false rejection and 1.3% false acceptance

1 Introduction

Mobile phones are becoming an ever-increasing part of our lives, with users becoming more reliant upon the services that they can provide. The evolution has been directed towards the provision of data services, by increasing data rates through technologies such as the General Packet Radio Service (GPRS) and the emerging third generation networks, which will enable a broadband service of up to 2Mbps (UTMS Forum 1998). With this increase in information capability, the mobile phone will begin to acquire many of the uses a personal computer has today. Access security currently takes the form of a Personal Identification Number (PIN), a secret-knowledge approach that relies heavily on the user to ensure its validity. For example, the user should not use the default factory settings, tell other people their PIN, or write it down. Apart from the technological arguments, a recent survey into attitudes and opinions of mobile phone customers found that 45% of respondents thought the PIN to be inconvenient and did not use the facility (Clarke et al. 2001). The findings also demonstrated the user's awareness of the security implications, with 81% of respondents overwhelmingly in supported for more security. Therefore the protection against unauthorised access and use of mobile phones is currently questionable – not because users do not want protection, but because they do not like the current method by which it is achieved.

It is clear that an alternative means of subscriber authentication is required to replace the PIN, but at the same time, other forms of secret knowledge-based approach are likely to be regarded as similarly inconvenient. It is, therefore, considered appropriate to examine the

potential of a fundamentally different strategy. Amongst the most powerful approaches to facilitate this are biometrics, which are based not on what the user *knows*, but who the user *is*. Biometrics can include physiological characteristics, such as fingerprints and hand geometry, and behavioural traits, such as voice and signature. Another behavioural biometric is keystroke dynamics, which measures the typing pattern of a user. This paper presents the findings of an investigation into the feasibility of using keystroke dynamics to authenticate users on a mobile handset, according to the way in which they use the keypad.

2 Background Concepts

The principal concept behind keystroke dynamics is the ability of the system to recognise patterns, such as characteristic rhythms, during keyboard interactions. A significant amount of prior research has been conducted in this domain, dating back to the 1980s (Legett and Williams 1988; Joyce and Gupta 1990; Monrose and Rubin 1999). However, all of these studies, have focused upon alphabetic inputs from a standard PC keyboard. Little work to date has considered the feasibility of assessing numeric input as the basis for authentication (Ord 1999), and to the best knowledge of the authors, no work has evaluated the application of the technique to a context such as a telephony handset (although the idea was previously proposed by Furnell et al. (1996)).

The assessment of keystroke dynamics can be based upon the more traditional statistical analysis or relatively newer pattern recognition techniques, and previous published studies have incorporated both approaches. The results generally favour the effectiveness of the pattern recognition, with neural network approaches having been shown to perform well (Cho et al. 2000). The network configurations of particular interest are the *Feed-Forward Multi-Layered Perceptrons (MLP),* as they have particularly good pattern associative properties and provide the ability to solve complex non-linear problems (Bishop 1995).

The size of the neural network in terms of number of layers, and number of neurons per layer, plays a key role in the processing ability of the network. However, in the design of neural networks very few, if any, solid rules exist to govern the size of neural networks, with respect to problem complexity. As such, concerns over network size are solved in this study through an iterative process of review and modification. For more information about the design, structure, training and implementation of neural networks, see reference (Bishop 1995; Haykin 1999).

As with other biometric techniques, the performance of the neural network classification for keystroke dynamics is measured using two error rates, the False Acceptance Rate (FAR) and False Rejection Rate (FRR). The former represents the level to which impostors are authorised by the network, and the latter is the likelihood an authorised user being rejected. However with keystroke dynamics, as with all biometric techniques, a threshold must be chosen for the error rates. The trade-off exists between high security/low user acceptance (a threshold value that provides a low FAR and high FRR) and low security/high user acceptance (a threshold value that provides a high FAR and low FRR). It is generally held as being infeasible to simultaneously achieve zero as they share a mutually exclusive relationship (Cope 1990). The point at which the FAR and FRR errors coincide is termed as the Equal Error Rate (EER) (Ashbourn 2000) and is often used as a performance measure

when comparing biometric techniques. These measures are used as the basis for evaluating the practical experiments discussed in this paper.

3 Experimental Procedure

The eventual application of keystroke dynamics to a mobile phone would ideally authenticate a user by monitoring his or her continuous use of the phone, during activities such as the entry of telephone numbers, use of the menu system, and composition of text messages. However the objective at this stage is to investigate the feasibility of the technique rather than to provide a complete solution to the problem. As such, the initial study has been confined to two types of data, namely:

1. PIN code, representing a 4 digit number plus the enter key (i.e. 5 key presses in total).
2. Telephone Number, including area code, representing a 10/11 digit numerical number plus the call key (i.e.11/12 key presses in total).

From these sets of data, three investigations were designed, which sought to assess the ability of a neural network to classify users based upon:

1. Entry of a fixed four-digit number, analogous to the PINs used on many current systems. The users entered the same four-digit code thirty times. Twenty of these inputs were utilised in the training of the neural network, with the remaining ten used as validation samples.
2. Entry of a series of telephone numbers. Fifty mock telephone numbers are entered per user. The classification of inputs was expected to increase inter-sample variance, and thereby make it harder for the network to classify. Thirty samples were used in the training of the network, with the remaining twenty used as validation samples.
3. Entry of a fixed telephone number in order to facilitate a comparison against the results from the second experiment. As with the fixed four-digit investigation, there are thirty samples, twenty for training and ten for validation.

A total of sixteen test subjects provided the input data required for all three investigations. The neural networks in all investigations were trained with one user acting as the valid authorised user, whist all the other users are acting as impostors.

A specially written application was used to collect the sample data. However, it was considered that the standard numerical keypad on a PC keyboard would not be an appropriate means of data entry, as it differs from a mobile handset in terms of both feel and layout, and users would be likely to exhibit a markedly different style when entering the data. As such, the data capture was performed using a modified mobile phone handset, interfaced to a PC through the keyboard connection. Figure 1 shows a screenshot from the data capture software that was used.

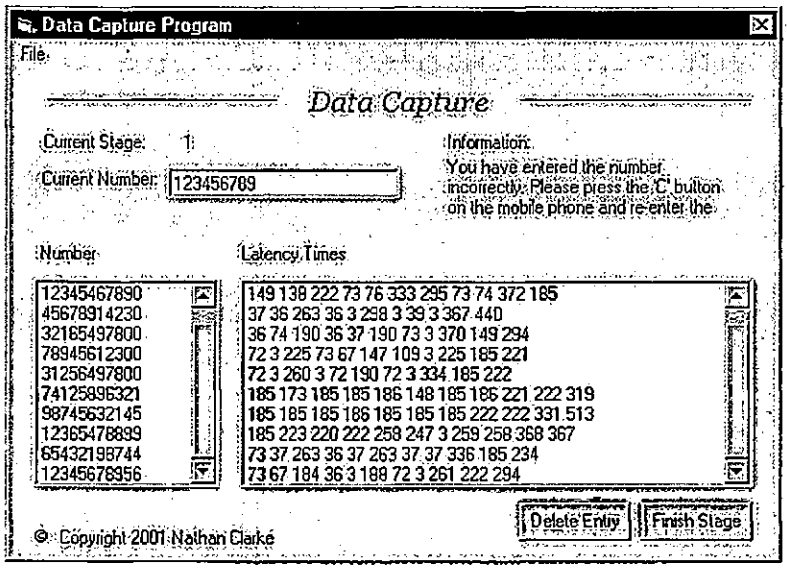


Figure 1 : Data Capture Software

Due to the limitations of data collection, the input data required for training and testing of the authentication system had to be collected in a single session. Ideally, the data would be collected over a period of time, in order to capture a truer representation of the users typing pattern. For example, by asking the user to type in 50 telephone numbers all at once, could result in an exaggerated learning curve.

4 Results

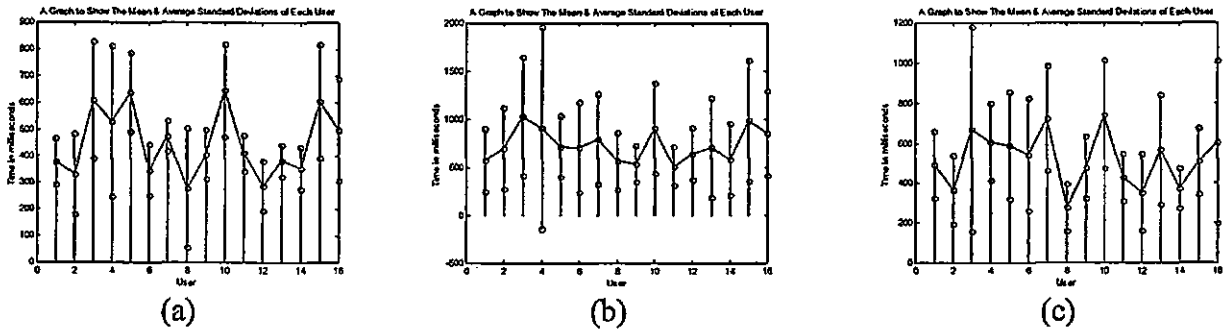
The analysis of the input data allows an insight into the complexities of successfully authenticating a person from a single input vector of latency values. The problem is that latency vectors observed from a single user may incorporate a fairly large spread of values. This spread, otherwise known as variance, is likely to encompass input vectors that closely match other users. Because users' latency vectors do not exist on clearly definable classification regions, the problem is made that much more complex for the neural networks.

Two types of variance exist in the latency data:

- inter-sample variance, which ideally would be zero, so that every sample a user inputs would be identical and therefore easier to classify.
- inter-user variance, a measure of the spread of the input samples between users, which would be ideally as large as possible in order widen the boundaries between classification regions.

An initial analysis of the inter-sample variance indicates that they are not ideal by any means, however some users obviously have smaller inter-sample variances than others. The graphs in Figure 2 illustrate the inter-sample mean for each of the users in each investigation. Significant differences can be noted between the three sets of results, such as generally smaller standard deviations and the lower average latency for the fixed telephone number tests when compared to those from the test in which varying numbers were used. This was expected, in the sense that users would become used to entering the fixed telephone number,

and therefore the inter-sample variation would progressively decrease. However, the 4-digit PIN investigation shows the lowest inter-sample variance, possibly indicating strong classifiable regions.



(a) (b) (c)

Figure 2 : Mean & Standard Deviation of User's for (a) 4-digit PIN, (b) varying telephone numbers, and (c) fixed telephone numbers

It is interesting to note that the inter-user variance is not considerably larger than the inter-sample variances, as would be favourable, indicating that less well defined classification boundaries exist.

Analysis of individual network performances shows unfavourably large error rates, with some users experiencing FAR/FRR pairs of 41%/20% and 37%/60% in the telephone number investigation. The large error rates suggests there are groups of users with more similar typing characteristics than others, thus making it difficult for the networks to classify them correctly. In particular, two groups of users were identified as having high false acceptances as each other. One such group is illustrated in figure 3(a), with figure 3(b) illustrating a group of dissimilar user inputs. However, in constrast, some users exhibited much more encouraging FAR/FRR figures, such as 1.3%/0% and 4%/10%, both of which were observed in the PIN code investigation. Results such as these suggest that keystroke characteristics can indeed be used to facilitate correct classification, but further development is required in improving network sensitivity and generalisation in other cases.

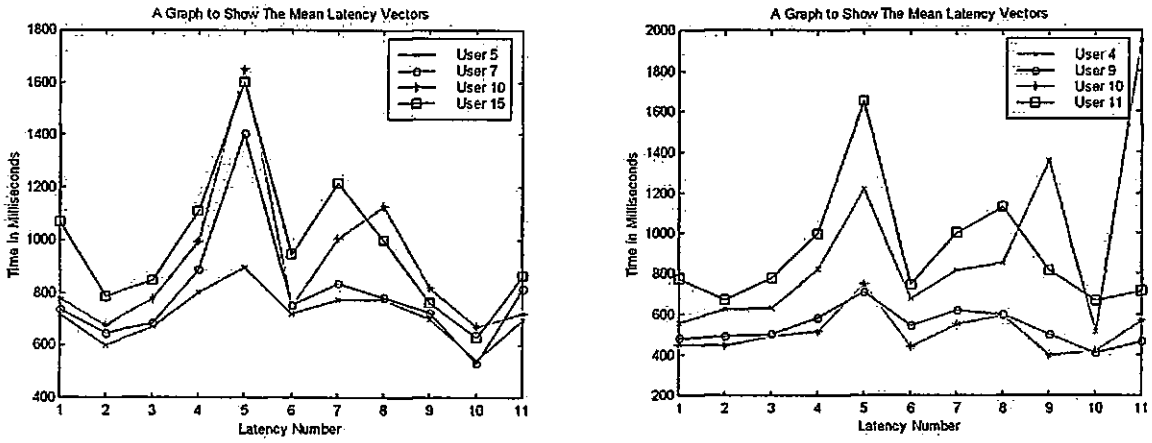


Figure 3 : (a) Similar User Input Latency Vectors (b) Dissimilar User Input Latency Vectors

The overall performances of the neural networks are illustrated in figures 4(a), (b) and (c). The optimum configurations for the MLP's were 11 inputs, 22 neurons for both the 1st and 2nd hidden layers, and 1 neuron in the output layer (i.e.11-22-22-1) for the telephone number based investigations, while the configuration for the PIN based investigation was 4-8-8-1. Unsurprisingly the fixed input networks of the PIN and fixed-telephone investigations performed substantially better than the pseudo-random telephone investigation. The difference between the two telephone investigations are an improvement in the FRR of over 50% and 35% in the FAR. Interestingly, the results indicate that the neural networks can classify the 4-digit PIN input at least as well as an 11-digit fixed telephone input. It would be normal to assume the more information a system has, the better it is able to classify the inputs.

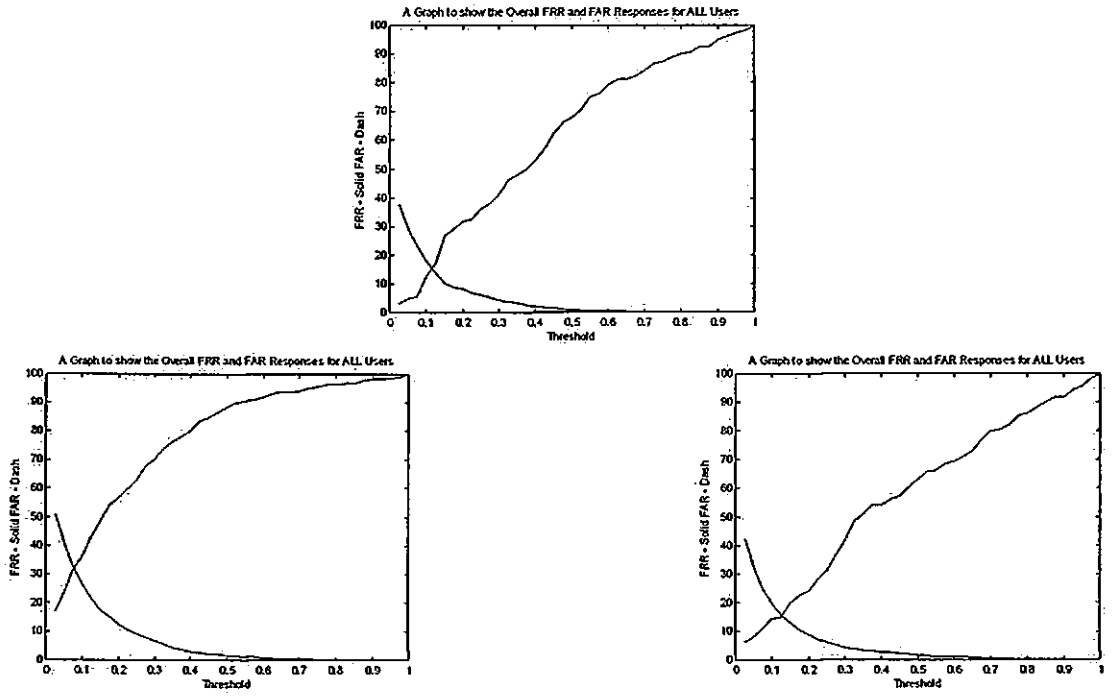


Figure 4 : Overall FRR & FAR for the (a) PIN Code Input Neural Network (b) Pseudo-Random Telephone Neural Network (c) Fixed Telephone Neural Network

The exclusivity of the FA and FR rates are clear, as one error rate decreases the other increases. The equal error rates (EER) for this study are shown in table 1. The threshold value assigned to the network is the level at which the network operator considers that the compromise between security and convenience has been established. For this study, the threshold level was kept constant throughout each of the networks per investigation to enable comparison. Both the PIN Code and mock telephone number networks were given static thresholds of 0.1, and the fixed telephone a threshold of 0.125. Tables of results for a static threshold level can be seen in table 1.

Investigation	FAR (%)	FRR (%)	EER (%)
PIN Code	18.1	12.5	15
Varying Telephone	36.3	24.3	32
Fixed Telephone	16	15	15

Table 1 : Investigation Results

5 Discussion

The investigations have shown the neural networks ability to classify valid and invalid users with a relative degree of success. The networks ability to classify users entering a varying series of telephone number was, as expected, the weakest of network configurations. The classification of fixed 4-digit input suggests that the entering of a PIN number has a quite unique dialling pattern of its own. The reason for this might lie in the fact that users become familiar with typing the 4 digit PIN quite quickly, enabling improved classification. The fixed telephone number has more digits, so while the entry is more consistent than for a variable series of phone numbers, it is not as fluid as the PIN code. However, more practice would probably improve this. Additionally, the 11-digit input has a longer feature set, making it more difficult for an impostor to duplicate.

From the two investigations surrounding the telephone number input, it can be seen that improvements in the inter-sample variance experienced between the varying and fixed telephone numbers has provided a proportionality higher improvement in network performance. However, it should also be noted that the inter-sample and inter-user variances are not the only relationships that determine the neural networks ability to classify users. For instance, the inter-sample variance of User 8 in the PIN investigation is one of the largest in the user group and covers the input latency range of other users, indicating a small inter-user variance. Yet, User 8 has the best FAR and FRR of all the users.

From the analysis of the individual network performances, it is clear that some networks perform far better than others. For instance User 9 in the PIN investigation has an FAR of 90% with Users 11 and 13. This could indicate one of two problems. Firstly, the typing patterns of those users are just too similar and no network would be able to successfully classify those users on a regular basis, or, more likely, it may be the case that the network is not sensitive enough to users data and through further training of the networks with those users with similar responses will help increase network sensitivity. Either way, this error rate is completely unsatisfactory and any further development will need to monitor the individual user performances, not just the average. Conversely, it is worth noting that individual networks performed as well as 0% FRR and 1.33% FAR, indicating that user typing patterns can be classifiable with a good degree of accuracy.

The FAR and FRR errors indicate how often a valid and invalid user will be authenticated onto the system. The trade off between the inconvenience of valid users not being accepted and invalid users being accepted means ideally a level has to be chosen at which these are both minimised. However the likelihood is one error rate will be minimised over another. From the results, if the FAR were to be set in the 2% range this would translate to having an FRR of approximately 55% for the PIN code and fixed telephone inputs. Inversely, setting the FRR in the 5% range (lowest FRR level) corresponds to approximately an FAR of 40%. It would be likely that a level in between theses extremes would be chosen by the network operator, to ensure the impact on legitimate users is minimised, but keeping a practical and useable level of security.

6 Conclusion

This paper has presented an investigation into the feasibilty of using keystroke analysis as a means of enhancing subscriber authentication on mobile handsets. Although the mis-authentications observed at this stage indicate that a practical implementation would prove too error prone, the nature of the investigtions, and the controlled environment in which they were carried out, are believed to be large contributing error factors (as well as actually being necessary to establish a worst case senerio).

The implementation employed in this study has adapted the neural network approach to determine the feasibility of a keystroke-based technique. As such, several areas for possible further research and experimentation can be identified. The first would be to obtain more representative input data, which would ideally incorporate all user input data from the mobile phone (including keystrokes relating to SMS text message entry and menu interactions), and be obtained over a reasonable period of time, in order to ensure a truer representation of users normal behaviour.

From an analysis perspective, further developments could include:

- Removal of outliers from the source input. A quick analysis of the user input data shows a small number of anomalies, which could be unfavourably biasing the network. This will have the effect of reducing the inter-sample variance.
- Increased network sensitivity by training the network using impostor input data that closely matches that of the authorised user, rather than training with all impostor input data.
- Use of generalisation techniques, such as early stopping and regularisation, to optimise the training of the network.
- Analysis of network structure, in terms of network interconnections and transfer functions. Although feed-forward backpropagation networks are amongst the best pattern associators at present, this need not be the case. A structure may exist that is better able to classify this particular problem.
- Updating network configuration over time through re-training.

However, no matter how accurate keystroke analysis becomes, the mutually exclusive relationship between false acceptance and false rejection rates would mean that it is unlikely that 0% can be achieved for both simultaneously. Therefore the study suggests the best implementation of a keystroke analysis authentication technique would be as part of a larger hybrid authentication algorithm, involving two or more non-intrusive biometric authentication techniques for normal authentication.

The technqiues discussed here will be the focus of futher research and practical experimentation by the authors.

References

Ashbourn, J. 2000. *Biometric. Advanced Identity Verification. The Complete Guide.* Springer.

Bishop, M. 1995. *Neural Networks for Pattern Recognition.* Oxford University Press.

Cho, S., Han, C., Han, D., Kim, H., 2000. *Web Based Keystroke Dynamics Identity Verification using Neural Networks.* Journal of Organisational Computing & Electronic Commerce, Vol. 10, No.4, pp 295-307.

Clarke, N., Furnell, S., Rodwell, P., Reynolds, P. 2001. *Acceptance of Subscriber Authentication for Mobile Telephony Devices.* Computers & Security. (In press)

Furnell, S.M.; Green, M.; Hope, S.; Morrissey, J.P. and Reynolds, P.L. 1996. *Non-Intrusive Security Arrangements to support Terminal and Personal Mobility.* Proceedings of EUROMEDIA 96, London, UK, 19-21 December 1996. pp167-171.

Haykin, S. 1999. *Neural Networks. A comprehensive Foundation. Second Edition.* Prentice Hall.

Cope, B. 1990. "Biometric Systems of Access Control", *Electrotechnology*, April/May: 71-74

Joyce, R., Gupta, G., 1990. *Identity Authorisation Based on Keystroke Latencies.* Communications of the ACM, 33(2): 168-176, February.

Legett, J., Williams, G., 1988. *Verifying User Identity via Keystroke Characteristics.* International Journal of Man-Machine Studies, Vol 28, pp 67-76.

Monrose, F., Rubin, A., 1999. *Keystroke Dynamics as a Biometric for Authentication.* Future Generation Computer Systems, 16(4) (2000) pp 351-359.

Ord, T. 1999. *User Authentication Using Keystroke Analysis with a Numerical Keypad Approach.* MSc Thesis, University Of Plymouth, UK.

UMTS Forum. 1998. *The Path Towards UMTS – Technologies for the Information Society.* Report Number 2. http://www.utms-forum.org/reports.html

Using Keystroke Analysis as a mechanism for Subscriber Authentication on Mobile Handsets

N.L. CLARKE*, S.M. FURNELL*, B. M. LINES* and P.L. REYNOLDS**

*info@network-research-group.org
Network Research Group
Department of Communication and Electronic Engineering
University of Plymouth
PLYMOUTH
PL4 8AA
United Kingdom
Tel: +44 1752-233520 Fax: +44 1752-233520

** Orange Personal Communications Services
Bradley Stoke
BRISTOL
United Kingdom

Key words: Keystroke Analysis, User Authentication, Biometrics, Mobility.

Abstract: The mobile communications industry will experience an evolutionary step within the next two years with the introduction of third generation mobile networks, completing the handset transition from a purely telephony device of the first generation analogue networks into a multimedia multi-purpose mobile communications tool. The ability of these new handsets to store and access sensitive information such as financial records, digital certificates and company records in association with a large handset penetration (864 million subscribers) makes them a desirable target for impostors. The authentication technique for current mobile phones has many weaknesses from a technological and subscriber perspective, and as such non-intrusive and stronger subscriber authentication techniques are required. This study investigates the plausibility of one such technique that of keystroke analysis, comparing and contrasting a number of pattern recognition and neural network based approaches to classification. It was found that neural network-based

approaches performed substantially better than the pattern recognition-based approaches with false acceptance and false rejection rates of 3.2%.

1. INTRODUCTION

The mobile communications sector has witnessed substantial growth in recent years with global mobile subscribers forecasted to rise from 864m in 2002 [1] to 1,848m by 2004 [2]. However, in parallel with this rise in ownership there has been a rise in mobile related abuse, with over 700,000 handsets stolen from subscribers in 2001, in the UK [3]. It can be conjectured that the more advanced capabilities of third generation handsets with their ability to pay for products using micro-payments and digital money, surf the internet, buy and sell stocks, transfer money and manage bank accounts will make the handsets even more desirable targets. Current authentication for handsets is achieved through a PIN (Personal Identification Number) approach, which relies heavily on the user to ensure its validity. For example, the subscriber should not use the default setting, tell other people, or write it down. Apart from the technological arguments, a recent survey into attitudes and opinions of mobile phone subscribers found that 45% of respondents thought the PIN to be inconvenient and did not use the facility [4]. The findings also demonstrated the user's awareness of the security implications, with 81% of respondents in support for more security.

Approaches to the verification of an identity can be achieved in one of three ways. Something the user *knows, has* or *is* [5]. The first approach is a secret-knowledge technique identical to the PIN and will therefore be just as inconvenient. The second is based on the user having to carry a token. However, due to the very nature of a mobile handset it is likely to remain within the handset permanently and thus diminished any security the token would provide (for example, subscriber's use of the SIM). The last approach, commonly termed as biometrics, is based on some unique characteristic feature of a person and includes physiological characteristics such as, fingerprints and hand geometry and behavioural traits such as a person's voice and signature. Another behavioural biometric is keystroke analysis which measures the typing characteristic of a user. In this context it has a number of advantages including a keypad that already resides on the device and the possible non-intrusive application of the technique thereby reducing user inconvenience. This paper will compare and contrast the performance of a number of pattern recognition and neural network approaches to solving the problem of keystroke analysis on a mobile handset keypad.

2. KEYSTROKE ANALYSIS

The principal concept behind keystroke analysis is the ability of the system to recognise patterns, such as characteristic rhythms, during keyboard interactions. In particular, this study utilises the time between two successive keystrokes (known as a digraph pair) and is referred to as the inter-keystroke latency. Classification is achieved by comparing an input sample against a reference template for the claimed user and given sufficient similarity the input sample is deemed to have come from the authorised user. The reference template is securely acquisitioned from the user when they enrolled on the system initially. However this template matching process gives rise to a characteristic performance plot between the two main error rates governing biometrics, the False Acceptance Rate (FAR), or the rate at which an impostor is accepted by the system, and the False Rejection Rate (FRR), or the rate at which the authorised user is rejected from the system. A third error rate known as the Equal Error Rate (EER) is used as a comparative measure between biometric techniques and equates to the mean value of the FAR and FRR [6].

A significant amount of prior research has been conducted in this domain, dating back to the 1980s. However, all of these studies have focused upon alphabetic inputs from a standard PC keyboard. Little work to date has considered the application of keystroke analysis to a mobile handset keypad, which has obvious tactile and interoperability differences. A previous feasibility study by the authors [7] has demonstrated promising results. However, the classification algorithm was an un-optimised neural network classifier. It is the aim of this paper to present a number of classification algorithms, including optimised neural network configurations, in order to define the most appropriate classifier for this particular problem.

3. CLASSIFICATION ALGORITHMS

Previous researchers have utilised a number of pattern recognition approaches such as linear and non-linear distance techniques [8], z-tests [12] and Bayesian classifiers [16], with more recent research efforts focussing on the use of neural network approaches [14-16]. A number of these techniques were selected on the basis of providing a broad range of classification techniques and this section will give a brief outline of them. For more detailed information and analysis of the techniques refer to references [8, 12, 18-22].

- *Mean & Standard Deviation Algorithm.*

  This is a traditional pattern recognition algorithm [8], based on the assumption that users keystroke latencies for a given digraph pair will be similar within an acceptable tolerance. A mean and standard deviation is calculated from the user's reference profile for the most regular digraph pairs which is used in comparing against an unseen input vector. If a sufficient number of digraph pair keystroke latencies reside within the tolerance envelope then the user is deemed to be the authorised user, if not, then an impostor.

- *Z-Test*

  The z-test is a statistical hypothesis test which can be used to establish whether an input vector comes from a particular sample population or not. The test assumes the sample size is large, so that the central limit theorem applies and we can use the normal distribution and assume that the sample standard deviation is an estimate of the population standard deviation. The null and alternative hypotheses are defined as:

  Null Hypothesis, H_0*:*
  Reference Profile Mean, μ_x = *Input Vector Mean,* μ_o
  Alternative Hypothesis, H_1*:*
  Reference Profile Mean, μ_x *Input Vector Mean,* μ_o

  The z-test investigation is a two-tailed test and will vary the level of significance, α in order to determine the most efficient level in terms of the performance rates.

- *Euclidean Distance Algorithm*

  The Euclidean distance algorithm is a linear minimum distance technique that computes the Euclidean distance between an input vector and reference profile. If the distance is within a predefined tolerance level then the input vector is deemed to have come from the authorised user, if not then an impostor. The Euclidean distance is calculated using:

  $\| x - m_k \|$ Where x = input vector; m_k = reference profile

  Here $\| u \|$ is called the norm of the vector u and corresponds to different ways of measuring distance. The Euclidean metric is calculated using:

  $$\| u \| = (u_1^2 + u_2^2 + u_3^2 + ...u_d^2)^{\frac{1}{2}}$$

- *Mahalanobis Distance Algorithm*

  The Mahalanobis distance algorithm is a non-linear minimum distance technique which uses the same mechanism as the Euclidean algorithm but with a difference technique for measuring the distance. The Mahalanobis metric is calculated using:

$$r^2 = (x - m_x)^T C^{-1} (x - m_x)$$

  In principal the non-linear problem solving abilities of the Mahalanobis classifier should provide better decision boundaries and improve the performance over the Euclidean algorithm.

- *Feed-Forward Multi-Layered Perceptron (FF MLP) Neural Network*

  A FF MLP utilising a backpropagation training algorithm are best known for their pattern associative properties. Patten associative networks work by training the network to respond in a certain way given a certain input sample and backpropagation training is mathematically proven to converge towards the most optimal results [20]. However great care needs to be taken to ensure the training data is representational of the problem the network is to solve.

  Unfortunately FF MLP networks have no rules governing what the network parameters need to be given a certain complexity of classification problem. As such trial and error approaches are often utilised in order to achieve the most desirable performance rates.

- *Radial Basis Function (RBF) Neural Network*

  RBF networks are very similar mathematically to MLP networks in that they both provide techniques for approximating arbitrary non-linear functional mappings between multi-dimensional spaces. An advantage of RBF over FF MLP is their ease of implementation with only two network parameters to define, i.e., the mean sum-squared error and the spread of the radial basis neurons. The network works on the principle of transforming the input space into a higher dimensionality in the likelihood that it will be more linearly separable [20].

- *Generalised Regression Neural Network (GRNN)*

  GRNNs are another network topology often used for function approximation tasks and have a similar network paradigm to the RBF networks. GRNNs are again useful because of their ease of implementation and in particular their speed of training. A potential disadvantage is the one-to-one mapping of training vectors to radial basis neurons resulting in a large and computationally complex network with large training datasets.

- *Learning Vector Quantisation (LVQ) Neural Network*

  LVQ networks are a supervised version of vector quantisation [22] designed for adaptive pattern classification. The network paradigm utilises a competitive layer which will automatically learn to classify input samples similar to an unsupervised clustering technique, however the LVQ network also has a mechanism to transform the competitive layer classes into target classifications defined by the user. This technique was used with notable success in [16].

Each of the classification techniques implements an identical mechanism for the evaluation of valid and impostor input samples, so that a fair comparison of the approaches can be achieved. The correct or false acceptance of a user is based not on the success or failure of individual digraphs but on a complete input sample.

4. EXPERIMENTAL PROCEDURE

The eventual application of keystroke analysis to a mobile phone would ideally authenticate a user by monitoring their use of the phone, during activities such as the entry of telephone numbers, use of the menu system, and composition of text messages. However, the objective at this stage is to investigate a number of classification techniques rather than to provide a complete solution to the problem. As such, the initial study has been confined to two types of data, namely:

1. Entry of a fixed four-digit number, analogous to the PINs used on many current systems.
2. Entry of a fixed eleven-digit number, analogous to the telephone numbers in which you would enter on a handset.

A total of sixteen test subjects were asked to enter the data for both sets of data thirty times. Twenty of these inputs were utilised in the generation of the reference profile, with the remaining ten used as validation samples. The pattern classification tests were performed with one user acting as the valid authorised user, whist all the other users are acting as impostors. A specially written application was used to collect the sample data.

A standard numerical keypad on a PC keyboard was not deemed to be an appropriate means of data entry, as it differs from a mobile handset in terms of both feel and layout, and users would be likely to exhibit a markedly different style when entering the data. As such, the data capture was

performed using a modified mobile phone handset, interfaced to a PC through the keyboard connection.

5. RESULTS

An analysis of the input data allows an insight into the complexities of successfully authenticating a person from a single input vector of latency values. The problem is that latency vectors observed from a single user may incorporate a fairly large spread of values and as such do not exist on clearly definable classification regions. Figure 1 illustrates some similar and dissimilar input vectors as an indication of the difficulties the pattern classification techniques have in discriminating between users.

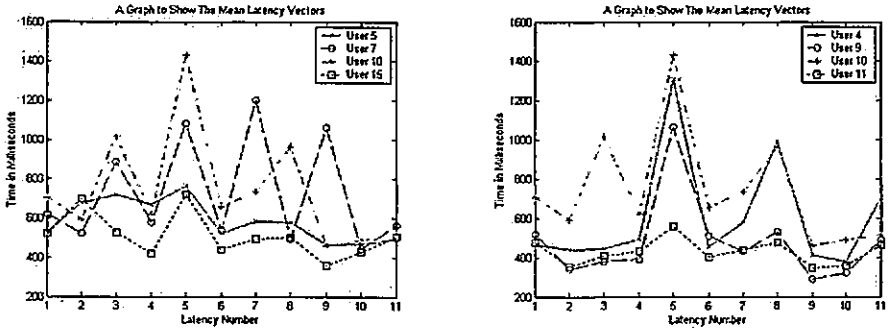


Figure 1: (a) Dissimilar User Input Latency Vectors (b) Similar User Input Latency Vectors

In order to help improve the boundaries between user's responses any input vectors three standard deviations away from the users mean latency value were removed. Table 1 illustrates the effect upon the dataset sizes.

Input	Original # of Samples	Modified # of Samples	Training Dataset Size	Validation Dataset Size
4-Digit	30	26	18	8
11-Digit	30	21	14	7

Table 1: Training & Validation Dataset

Figures 2 and 3 illustrate the results of the comparison of the various classification techniques. The most successful pattern recognition technique with the 4-digit input was the Euclidean technique, with an EER of 14.2%, followed by the mean and standard deviation algorithm, with an EER of 17.7%. Conversely, with the 11-digit input, the mean and standard deviation algorithm performed most successfully with an EER of 17.9%, followed by

the Euclidean technique with an EER of 21.2%. The worst classifier with both the 4-digit and 11-digit inputs was the Mahalanobis algorithm, with EERs of 19.3% and 28.7% respectively. This is somewhat unusual as the Mahalanobis distance algorithms performance was significantly inferior to its linear distance (Euclidean) counterpart. Re-testing both the Euclidean and Mahalanobis algorithms with the validation dataset replaced with the training dataset found that the performance of the Mahalanobis algorithm superseded the Euclidean as would be expect due to the non-linear boundaries it can form. The fact it does not perform as well using the validation dataset would suggest the more general boundaries produced by the Euclidean technique are more appropriate to the complete dataset, indicating the training dataset may not be as representative as required.

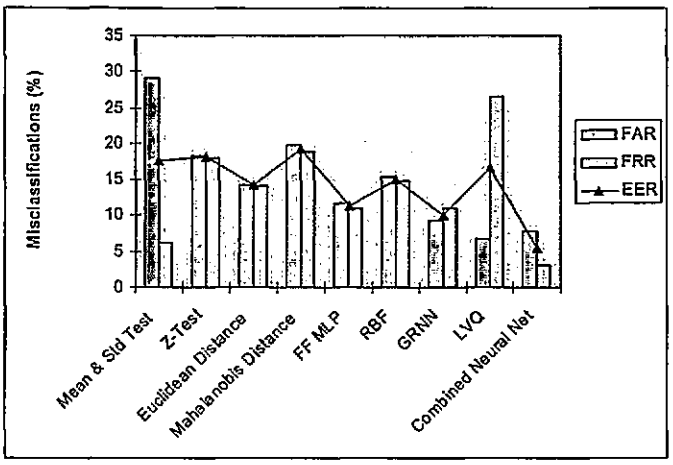


Figure 2: Classification Results for the 4-Digit Input

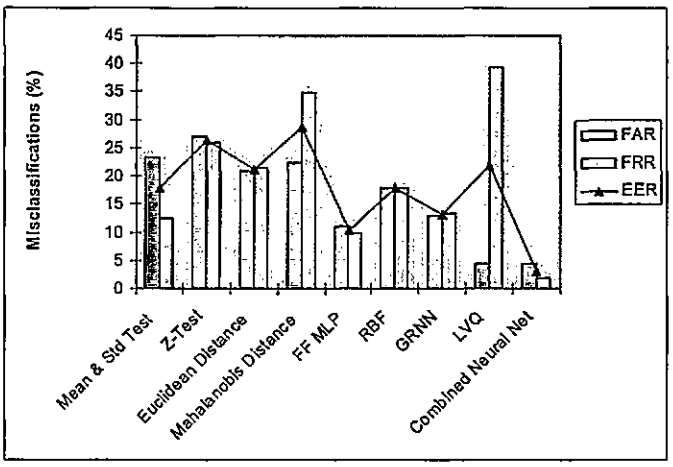


Figure 3: Classification Results for the 11-Digit Input

Overall it was the neural network based approaches that performed best, significantly improving the performance rates. The GRNN was most successful with the 4-digit input achieving a EER of 10.1%, followed by the FF MLP with an EER of 11.3%. Conversely again this role was reversed with the 11-digit input, as the FF MLP was the most successful, obtaining an EER of 10.4%, with the GRNN achieving an EER of 13.1%.

Analysis showed that individual user's performance varied with the different neural network techniques, with some users performing better on one than another. As such a combined neural network technique was created using the best result achieved by each user in any of the neural based techniques, resulting in the classifier achieving an EER of 5.5% and 3.2% with the 4-digit and 11-digit inputs respectively – by far the best result achieved thus far.

As both the 4-digit and 11-digit inputs represent a static keystroke analysis approach, in that they discriminate users based on a identical input string, an extension to the investigation was sought that provided a dynamic approach, in order to gauge the viability. As such 16 participants entered 50 random telephone numbers, which after outliers were removed decreased to 38 (26 for training and 12 for validation). A larger dataset was utilised so that more training data was available due to the more difficult task of discriminating users based on varying input vectors. The results, as would be expected, show the performance of the classification algorithms to be far poorer than the static-based techniques, with the best performance being achieved by the feed-forward MLP with an EER of 24.8%. Using the combined neural network technique the EER reduces to 16.1%.

6. DISCUSSION

The investigations have shown the ability for classification algorithms to correctly discriminate between users with a relatively good degree of success, with neural network approaches performing significantly better than their pattern recognition counterparts. The general performance of the 4-digit input vector, (analogous to the PIN) suggests that the entering of a PIN number on a mobile handset has a quite unique dialling pattern, perhaps due to user's previous experience of having to enter such short sequences on a regular basis. Classification algorithms typically find verification simpler when the input vector is larger, as it will typically contain more discriminative information. Overall, this was not the case, with the 4-digit input outperforming the 11-digit input, suggesting that although the user's entry of a fixed 11-digit number is more consistent than for a variable series of numbers, it is not as fluid as the 4-digit PIN input.

From an analysis of the classification algorithms, it is clear that some of the individual network performances experienced 40%+ false acceptance and false rejection rates. This would indicate two problems. Firstly, a user's input varies too considerably from input to input for even a static keystroke analysis technique to prove useful, or secondly, the classifier may not be sensitive enough to the users' data. Both of these problems could be counteracted as the user enters more and more data to the classification engine. However, this error rate is currently unsatisfactory in a mobile operator context and further developments will need to monitor the individual error rates not only the average. Conversely, a number of classifiers (particularly the neural network based techniques) experienced a number of users achieving an FAR and FRR of 0%, reiterating the ability for user's keypad interactions to be discriminative.

Although the static-based classifiers were relatively successful, any effective implementation of keystroke analysis would depend on the ability to provide dynamic-based classification in order to provide non-intrusive, ad hoc authentication. Although the results for dynamic-based classification have been poor in comparison with a static approach they are nevertheless encouraging, especially considering the small datasets with which the classifier was trained and validated. It may also be possible to improve dynamic authentication performance by utilising the more static elements of a varying input such as the area code of a telephone number, thereby reducing the number of varying telephone numbers that could be entered.

The mutually exclusive relationship that exists between the false acceptance and false rejection mean that it would be unlikely for both error rates to achieve near 0% simultaneously [23]. Therefore, the study suggests the best implementation of a keystroke analysis authentication technique would be as a larger hybrid authentication algorithm, involving two or more non-intrusive biometric authentication techniques, such as utilising voice recognition during a voice call, and facial recognition during a video conference.

7. CONCLUSIONS & FUTURE WORK

The implementation employed in this study has focussed on the feasibility of a keystroke analysis technique using a number of classification algorithms. Although neural network approaches have clearly outperformed the traditional pattern recognition techniques, the variability of the results in and between the neural network approaches means that much scope remains for fine tuning the networks – especially if larger and more representative input data were made available, with a larger group of participants. In

particular, the most successful algorithm implemented in this study was the combined neural network, but the use of such a technique in practicality is difficult, as training the user iteratively on a wide spread of networks is computational intense and time consuming. In order for this technique to be of any practical relevance it would be necessary to develop an algorithm for analysing a user's input data and (dependant on its complexity) decide which network was most relevant.

This study used keypad interactions exclusively linked with dialling numbers. However the use of mobile handsets for data services such as SMS (Short Message Service) messaging, and other mobile related interactions such as the menu system, opens the possibility of authenticating a user by other means such as the way in which they type words and characters. Additionally, recent research has shown that using classification algorithms that utilise both the inter-keystroke time and hold-time (the time taken to press and release a single key) has more distinct and thus discriminative information than the traditional inter-keystroke timings used in this study [16, 24].

8. REFERENCES

[1] Cellular Online. September 2002. www.cellular.co.za

[2] Giussani, B. 2001. Roam – Making Sense of the Wireless Internet. Random House Business Books, London, UK.

[3] BBC. 2002. "Huge surge in mobile phone thefts", BBC News Report, 8th January 2002. http://news/bbc.co.uk/hi/english/uk/newsid_1748000/1748258.htm

[4] Clarke, N.L., Furnell, S.M., Rodwell, P.M. and Reynolds, P.L. 2002. "Acceptance of subscriber authentication methods for mobile telephony devices". Computers & Security, vol. 21, no.3, pp. 220-228.

[5] Wood, H.M. 1978. "The Use of Passwords for controlling the Access to Remote Computer Systems and Services". Computers & Security, vol. 3.

[6] Ashbourn, J. 2000. *Biometric. Advanced Identity Verification. The Complete Guide.* Springer.

[7] Clarke, N.L., Furnell, S.M., Lines, B., Reynolds, P.L. 2002. "Subscriber Authentication for Mobile Phones using Keystroke Dynamics". Proceedings of the Third International Network Conference (INC 2002), Plymouth, UK. pp.347-355.

[8] Umphress D., Williams, G. 1985. "Identity Verification through Keyboard Characteristics". International Journal of Man-Machine Studies, vol. 23, pp. 263-273.

[9] Leggett, J., Williams, G. 1987. "Verifying Identity via Keystroke Dynamics". International Journal of Man-Machine Studies, vol. 28, pp 67-76.

[10] Joyce, R., Gupta, G. 1990. "Identity Authorisation Based on Keystroke Latencies". Communications of the ACM, 33(2): 168-176.

[11] Brown, M., Rogers, J. 1993. "User Identification via Keystroke Characteristics of Typed Names using Neural Networks". International Journal of Man-Machine Studies, vol. 39, pp 999-1014.

[12] Napier, R., Laverty, W., Mahar, D., Henderson, R., Hiron, M., Wagner, M. 1995. "Keyboard User Verification: Toward an Accurate, Efficient and Ecologically Valid Algorithm". International Journal of Human-Computer Studies, vol.43, pp 213-222.

[13] Monrose, R., Rubin, A. 1999. "Keystroke Dynamics as a Biometric for Authentication". Future Generation Computer Systems, 16(4) pp 351-359.

[14] Cho, S., Han, C., Han D., Kin, H. 2000. "Web Based Keystroke Dynamics Identity Verification Using Neural Networks". Journal of Organisational Computing & Electronic Commerce, vol. 10, pp 295-307.

[15] Obaidat, M., Macchairolo, D. 1994. "A Multilayer Neural Network System for Computer Access Security". IEEE Transactions on Systems, Man, and Cybernetics, vol. 24, no. 5, pp. 806-813.

[16] Obaidat M., Sadoun, B. 1997. "Verification of Computer Uses Using Keystroke Dynamics". IEEE Transactions on Systems, Man, and Cybernetics – Part B: Cybernetics, vol. 27, no. 2, pp.261-269.

[17] Ord, T., Furnell, S. 2000. "User Authentication for Keypad-Based Devices using Keystroke Analysis". MSc Thesis, University of Plymouth, UK.

[18] Triola, M. 1998. *Elementary Statistics (7th Edition)*. Addison Wesley.

[19] Hogg, R., Ledolter, J. 1989. *Engineering Statistics*. Macmillan Publishing.

[20] Bishop, M. 1995. *Neural Networks for Pattern Classification*. Oxford University Press.

[21] Haykin, S. 1999. *Neural Networks: A Comprehensive Foundation (2nd Edition)*. Prentice Hall.

[22] Kohonen, T. 1997. *Self Organising Maps*. Springer.

[23] Cope, B. 1990. "Biometric Systems of Access Control". Electrotechnology, April/May: 71-74.

[24] Robinson, J., Liang, V., Chambers, J., MacKenzie, C. 1998. "Computer User Verification Using Login String Keystroke Dynamics". IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans, vol. 28, no.2, pp. 236-241.

Biometric Authentication for Mobile Devices

N.L. Clarke[1], S.M. Furnell[1] & P.L. Reynolds[2]

[1]*Network Research Group*
Department of Communication & Electronic Engineering
University of Plymouth
Plymouth
United Kingdom
Email: info@network-research-group.com

[2]*Orange Personal Communications Services Ltd*
Bradley Stoke
Bristol
United Kingdom

ABSTRACT

Mobile devices have found an important place in modern society, with hundreds of millions currently in use. The majority of these use inherently weak authentication mechanisms, based upon passwords and PINs, which can potentially be compromised and thereby allow attackers access to the device and its stored data. A need for stronger authentication is identified and the discussion considers the application of various biometrics to a mobile platform. The feasibility of one such approach, that of keystroke dynamics, is examined, revealing promising results – with individual performances of 0% false rejection rate and 1.3% false acceptance rate being observed. However, higher overall error rates of 15% lead to the proposal of a hybrid, non-intrusive approach to authentication.

KEYWORDS

Mobile Devices, Authentication, Biometrics

INTRODUCTION

The ability to communicate and work whilst on the move has given rise to an explosive growth in mobile devices. Primarily this growth has come out of mobile phone related technologies with worldwide subscribers now in excess of a billion (UMTS Forum, 2002), but it can also be seen that both the use of Personal Desktop Assistants (PDA's), and laptop computers has been growing with popularity (Richardson, 2002; Gibson, 2001). However, this rise in computing mobility could cause a number of security issues, in particular with attackers accessing the data stored on the devices.

The most popular access security to date takes the form of the password or PIN (Personal Identification Number), a secret-knowledge approach that relies heavily on the user to ensure continued validity. For example, the user should not use the default factory settings, tell other people, or write it down. However the poor use of passwords and PINs has been widely documented, with many laptops owners using simple passwords that dictionary attacks can crack in seconds and with many mobile phones and PDA users not even using the security available. Recent surveys have indicated that 44% of mobile phone users do not use the PIN and 25% of PDA users do not a password (Clarke et al., 2002a; Leyden, 2002). Taking a crude comparison with current mobile phone subscribers, this would indicate that some 500 million mobile phones have no access security. Although this is not a particular issue currently with the second generation mobile phones with their limited storage and computing abilities, this will change with the advent of third generation networks and a convergence of PDA and mobile phone functionality (Giussani, 2001). Mobile phones will be able to store detailed information about friends and family, include digital certificates, bank details and be able to access a wide range of data services through your phone account – ranging from the purchasing of goods to watching movies. Interestingly the same mobile phone survey found that, in contradiction to not using the protection already available with 41% of respondents citing inconvenience, that 81% of respondents wanted more security.

So an alternative means of subscriber authentication is required to replace the secret-knowledge based approaches. It is therefore appropriate to examine the potential of a fundamentally different strategy. From the available techniques, that of token-based authentication and biometric based authentication, only the latter really seems plausible, since tokens would also have to be carried with you along with the device or more commonly left permanently in situ. Biometrics, are based not on what the user *knows*, or what they carry, but who the user *is*, some unique characteristic. After explaining the biometric concept in more detail, this paper considers the techniques that could potentially be deployed on mobile devices, along with a brief example of a practical implementation.

THE NEED FOR AUTHENTICATION ON MOBILE DEVICES

As previously indicated, a large number of mobile devices are currently in use with little or no authentication security. A recent survey into the use of PDAs discovered a third of users who have already had their PDA stolen once still do not use a password, however, one of the cited uses for a PDA by respondents was to store all the passwords and PINs they regularly use for other systems (Leyden, 2002). This highlights two primary issues; firstly, the inherent weaknesses of secret-knowledge based techniques such as the password in that they can be written down in the first place, and secondly the importance of the data being stored on the device. There is a third issue raised concerning user perception and realisation of the security problems. Any person storing sensitive

information on a device without securing that device clearly has little comprehension of the associated security issues.

The security weaknesses and threats associated with PDAs are important because although the number of devices currently in use is relatively small (in the order of tens of millions), the mobile phone is set to absorb and surpass much of the functionality of current PDA devices. The difference in numbers is from tens of millions of PDAs to hundreds of millions of mobile phones. If authentication mechanisms were left as they currently stand, then the threat posed by attackers would inconvenience users through cost associated with misuse and an almost certain increase in the theft of the devices. For example, the UK Home Office reported some 700,000 mobile phone thefts from subscribers in 2001 and this number can only be set to increase as mobile phones are packed with more technological wizardry (Harrington et al, 2001).

Concerns can also be expressed in relation to laptop computers. For example, the UK Ministry of Defence (MoD) admitted to losing over 600 laptops over a five year period (BBC, 2002), many obviously containing very sensitive information. Although it is likely that many laptops are stolen merely to be resold as a piece of equipment, rather than for the information stored upon them, this cannot be the case it all thefts. Infosecurity reported in May 1999, that 57% of computer crimes involving break-ins on corporate servers were linked to stolen laptops that enabled the breach (Broomfield, 2000).

BIOMETRIC APPROACHES & IMPLEMENTATION

The use of biometrics has existed for hundreds of years in one form or another, whether it is a physical description of a person or perhaps more recently a photograph. Consider for a moment what it is that actually allows you to recognise a friend in the street or allows you to recognise a family member over the phone. Typically this would be their face and voice respectively, both of which are biometrics. Biometrics are based on unique characteristics of a person, and are typically subdivided into two categories, physiological and behavioural. Physiological biometrics are those based on classifying the person according to some physical attribute, such as their fingerprints, their face and their hand. Behavioural biometrics rely on a unique behaviour of the person such as, their voice and the way in which they write their signature.

Biometrics all work on the basis of comparing the biometric sample against a known template, which is securely acquisitioned from the user when he or she enrolled on the system initially. However this template matching process gives rise to a characteristic performance plot between the two main error

rates governing biometrics. The False Acceptance Rate (FAR), or rate at which an impostor is accepted by the system, and the False Rejection Rate (FRR), or rate at which the authorised user is rejected from the system. The error rates share a mutually exclusive relationship as one error rate decreases, the other tends to increase, giving rise to a situation where neither of the error rates are typically both at zero percent (Cope, 1990). Figure 1 illustrates an example of this relationship.

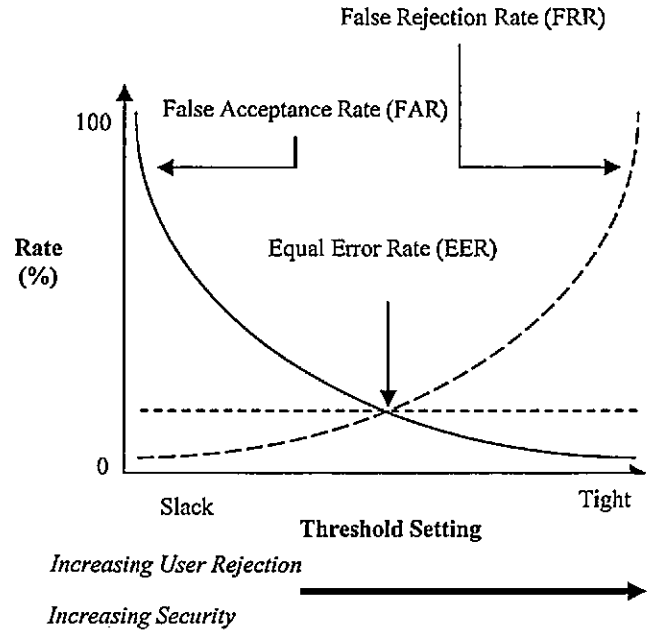


Figure 1 Mutually exclusive relationship between the False Acceptance & False Rejection Rates

This leads to a trade-off situation between high security and low user acceptance (due to fact the authorised user is being rejected a large proportion of the time) and low security and high user acceptance, to which a decision has to made about what threshold setting to set that meets both the security requirements of the device and acceptance levels of users. The point at which the error rates cross is called the Equal Error Rate and is used in industry as a comparative measure between different biometric approaches (Ashbourn, 2000).

The next section provides an overview to the most common biometrics that could be implemented within a mobile terminal, indicating what the unique characteristic the technique attempts to classify users upon and how the biometric is obtained. For more general information on any of the approaches discussed here, consult Nanavati et al. (2002) and Smith (2001).

Physiological Biometrics

- Fingerprint Recognition

  The most commonly deployed biometric, with a mature and proven technology. The fingerprint comprises of ridges and valleys that form distinctive patterns, such as loops, swirls and arches. The ridges and valleys are characterised by discontinuous and irregularities known as *minutiae* – these are the distinctive features on which most fingerprint technologies are based. In order for the fingerprint image to be captured a specialist reader is required.

- Facial Recognition

  This utilises the distinctive features of the human face in order to authenticate a user. The features often used are those which change very little over time, such as the upper ridges of the eye sockets, areas around the cheekbones, sides of the mouth, nose shape and the relative position of these features relative to each other. The facial image itself can be generated from any static camera or video system that is able to generate image of sufficient quality, such as web camera.

- Iris Scanning

  Iris scan technology works by utilising the distinctive features of the human iris and has the potential to be one of the most successful biometrics (Harrison, 2001). Iris recognition requires the acquisition of a high-resolution image of the eye, illuminated by an infrared imager, in order to effectively map the details of the iris. The device to capture this image can vary from a desktop camera to a dedicated camera for integration into physical access units. The main distinctive feature used for authentication is known as the *trabecular meshwork*, although other features are also used, such as furrows, freckles and the corona.

Behavioural Biometrics

- Voiceprint Recognition

  Voiceprint recognition as the name would imply authenticates person by their vocal characteristics. The authentication can in principle be achieved both text dependently – where the user speaks a predefined word or sentence – and text independently where authentication is not dependent on the word(s) you speak, although, the latter is obviously a more difficult task to achieve successfully. Voiceprint recognition is similar to facial recognition and keystroke dynamics it that it can leverage existing hardware on the device, although some manufacturers do specify or provide a particular microphone that is calibrated with its authentication algorithm.

- Signature Recognition

  This is achieved through using the distinctive aspects of a human signature to authenticate users. There are two underlying processes to signature recognition – static – where the completed signature is compared to a template version and authentication is given dependent on the comparison, or more comprehensively – dynamically – where behavioural components such as the speed, pressure and stroke order are also taken into account, hence making it less susceptible to forgery. The majority of signature-scan systems therefore use an electronic tablet that can record the dynamics of writing.

- Keystroke Dynamics

  Keystroke dynamics is a technique that authenticates a person by the way in which they type on keyboards/keypads. The typical distinguishing characteristic is the latency between successive keystrokes. Similar to signature recognition, keystroke dynamics can be achieved using static and dynamic approaches, with the former being the easier. Static authentication involves the user entering a predefined keyword such as their username/password, whereas dynamic authentication is text independent and will authenticate a user given any sequence of text. Since no additional hardware is required this has been a favoured technique, with much research on the subject since the 1980's (Gaines, 1980) but the performance of such a technique is comparatively weak against fingerprint and facial recognition systems, with currently only one commercially available product based on the static mode of authentication (Biopassword, 2002).

- Service Utilisation

  This technique is achieved by monitoring the distinctive way in which a person interacts with a device. Measured factors could include the time and type of calls dialled (long distance, local, premium rate numbers for instance), SMS text messages sent to whom and when, and web pages visited over a period of time. The longer the period the more precise the technique becomes. The unique pattern(s) in a person's behaviour can be identified using a branch of artificial intelligence referred to as data mining (Singh et al., 2001). This is a comparatively new method of behavioural biometric and consequently has no commercial product to date.

The survey by Clarke et al. (2002a) also indicated that users wanted more security for their current second generation phones which in itself indicates user's awareness of security issues, and were prepared to use biometrics to achieve the desired level of security. Figure 2 illustrates user's responses towards some of the techniques previously described, considering their application to a mobile phone environment.

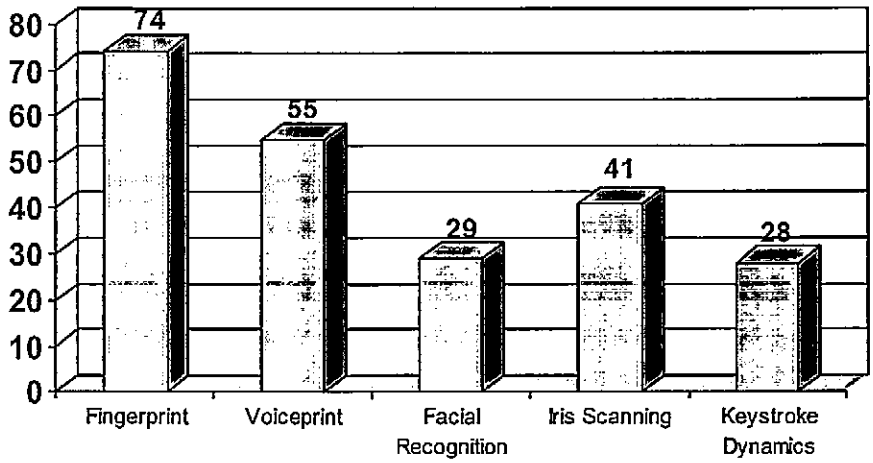


Figure 2 User's Biometric Preferences

The extent to which the biometrics previously described can be used within a mobile terminal device depends largely on the available hardware. It is unlikely, due mainly to cost, that many users will be willing to buy the additional hardware unless there are other real tangible benefits to be gained, such as a camera –which can be used for facial recognition but also take holiday pictures for instance. The only time where it would be conceivable for additional security-specific hardware purchases would be when the cost associated with the hardware is relatively small in comparison to the device to which it is protecting. This is likely to discount mobile handsets and PDAs as they are not likely to be expensive enough, but perhaps not laptops, where the upper boundary resides around $3700 ($6600 AUD). Otherwise it can be generally held true that the only biometric approaches available are those that can be easily (and cheaply) implemented on current devices. Typical biometric approaches that can be implemented on current mobile devices are given in table 1. This is by no means a definitive list as many devices differ in their hardware specifications. For instance some Acer laptops now have fingerprint recognition built into the system (Thornton, 2001) and some PDAs do not currently have the expandability to include a camera.

Mobile Phone	PDA	Laptop
➢ Voice Recognition via in-built microphone ➢ Keystroke Dynamics via scaled-down keyboard ➢ Facial Recognition via add-on or built-in camera ➢ Iris Recognition via add-on or built-in camera	➢ Voice Recognition via in-built microphone ➢ Facial Recognition via add-on camera ➢ Iris Recognition via add-on camera ➢ Signature Recognition via touch sensitive display	➢ Keystroke Dynamics via keyboard ➢ Fingerprint Scanner (via optional PCMCIA slot) ➢ Facial Recognition via in-built camera ➢ Iris Recognition via in-built camera

Table 1 Applicable Biometric for Mobile Devices

MOBILE BIOMETRICS IN PRACTICE

Keystroke dynamics is of particular interest as the approach has a number of advantages over other biometrics that make it useful as an authentication technique for mobile devices, mainly, the lack of additional hardware required and the ability to implement a solution completely transparently to the user, therefore resolving any issues of user inconvenience (the issues of convenience and intrusiveness are discussed in the following section). Although it is recognised that many PDAs do not have keyboards or keypads, a general market trend of late has seen the introduction of either add-on keyboards or scaled down versions (HP, 2002; HandSpring, 2002) to which keystroke dynamics can be applied. Of course no single biometric approach will encompass all mobile devices due to the differing hardware configurations, but the authentication mechanism proposed in this paper will take this into account.

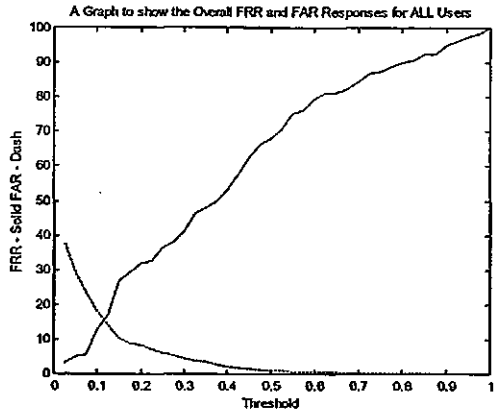
The history of keystroke dynamics dates back over twenty years with many research papers having been published, Joyce et al. (1990), Leggett et al. (1988) and Monrose et al. (1999) to name but a few. However, all studies to date with the exception of Ord (2000) have focussed on the ability to classify users on the basis of their interaction with a keyboard and not a keypad, as is common to mobile phones. To the authors best knowledge there have been no studies involving a mobile phone keypad – Ord's study used the numeric keypad from a computer keyboard, where the location and tactile differences are considered large enough to warrant an independent study. Thus a study was devised to investigate the feasibility of a keystroke dynamics technique on a mobile phone.

From the foundation Ord's study, a series of investigations were designed to examine the feasibility of using keystroke dynamics on a mobile handset (Clarke et al., 2002b). Three experiments were conducted, each involving a total of 16 participants:

1. the entry of a four digit number, analogous to the PINs used on current devices;
2. the entry of a series of varying telephone numbers;
3. the entry of a fixed telephone number.

The first and third investigations required the participants to enter the numeric keystroke sample thirty times, with twenty samples then being used to create a reference profile, and the remaining ten for subsequent testing. The second investigation required a larger number of samples due to the changing nature of the input string, and thus the need to train the authentication system more accurately. Fifty samples were taken, with thirty for training and twenty for testing.

Previous studies have shown neural networks to provide an effective foundation for keystroke analysis (Ord, 2000; Cho et al., 2000) and they have consequently been used in these investigations. The neural network structure is constructed on the feed-forward back-propagation network (Bishop, 1995), best exemplified for pattern recognition techniques.



Investigation	FAR (%)	FRR (%)	EER (%)
PIN Code	18.1	12.5	15
Varying Telephone	36.3	24.3	32
Fixed Telephone	16	15	15

Table 2 Keystroke Dynamics Results

Figure 3 Keystroke Dynamics Performance Chart

The results demonstrate the potential to distinguish authorised users from impostors, although arguably not to any great accuracy. However, the experimental procedure used in this study was performed under controlled conditions, with users all entering the same input data - a condition that is unlikely in the real world. Additionally, the design, and implementation of the neural network used for classification was primitive and un-optimised. Continuation of the study beyond this feasibility stage requires variables such as pre-processing, generalisation, network sensitivity and network configuration to be considered and analysed.

Further development of the technique will also consider other forms of user interaction with mobile handsets, in order to attempt to profile behaviour in different contexts. For instance, the way in which someone types when entering an SMS message is likely to be different to the way in which they enter a telephone number. Some users will use certain applications or functionality on the phone more often than others; will dial certain number more than others; and equally as important will not use or dial certain people or services. All of these factors could potentially be used as discriminating characteristics, leading to a stronger overall verification technique.

CONCLUSIONS

Mobile devices are going through an evolutionary period with the combined ability to have high computer processing on small handheld devices, and the formidable success of the mobile phone industry. Users are no longer chained to their desks and mobility has become an important factor in

many people's life. This has left an increasing security problem generally, with a major issue being authentication.

The current form of authentication is a very cheap solution but suffers from a number of inherent weaknesses, such as the lack of and improper use of passwords and PINs. Biometrics are amongst the most powerful authentication tools as they are based on a unique human characteristic.

Biometrics' on mobile devices are also an effective tool for non-intrusive authentication, as different approaches can be implemented whilst the user is interacting with the device. In the context of a mobile phone, voice recognition can be used to authenticate a user whilst they are speaking on the phone, keystroke dynamics whilst they are typing SMS messages and facial recognition when they use video conferencing facilities. Thus a hybrid non-intrusive authentication mechanism utilising the available biometrics on each mobile device as the underlying authenticator would provide a transparent and secure solution.

REFERENCES

Ashbourn, J. (2000). Biometric. Advanced Identity Verification. The Complete Guide. Springer.

BBC. (2002). MOD Loses 600 Laptops. BBC News Online.
http://news.bbc.co.uk/hi/english/uk/newsid_1757000/1757792.stm

Biopassword (2002). www.biopassword.com

Bishop, M. (1995). Neural Networks for Pattern Recognition. Oxford University Press.

Broomfield, S. (2000). It's Not Just a Laptop Anymore!. Information Impacts Magazine.
www.cisp.org/imp/february_2000/broomfield/02_00broomfield.htm.

Cho, S., Han, C., Han, D., Kim, H. (2000). Web Based Keystroke Dynamics Identity Verification using Neural Networks. Journal of Organisational Computing & Electronic Commerce, Vol.10, No.4, pp.295-307.

Clarke, N., Furnell, S., Rodwell, P., Reynolds, P. (2002a). Acceptance of Subscriber Authentication for Mobile Telephony Devices. Computers & Security, Vol.21, No.3, pp.220-228.

Clarke, N., Furnell, S., Lines, B., Reynolds, P. (2002b). Subscriber Authentication for Mobile Phones using Keystroke Dynamics. Proceedings of the Third International Network Conference (INC2002), Plymouth, UK, 16-18 July 2002. pp347-356.

Cope, B. (1990). Biometric Systems of Access Control. Electrotechnology, April/May: 71-74.

Gaines, R., Lisowksi, W., Press, S., Shapiro, N. (1980). Authentication by keystroke timing: Some Preliminary Results. Rand Report R-256-NSF. Rand Corporation, Santa Monica, CA.

Gibson, B. (2001). Apple Slips to 8th in US laptop sales. MacCentral Online. http://maccentral.macworld.com

Giussani, B. (2001). Roam – Making Sense of the Wireless Internet. Random House Business Books, London.

HandSpring. (2002). Treo 270. HandSpring. www.handspring.com

Harrington, V., Mayhew P. (2001). Home Office Research Study 235: Mobile Phone Theft. Crown Copyright.

Harrison, L. (2001). Iris Recognition is Best Biometric. The Register. www.theregus.com

Joyce R., Gupta, G. (1990). Identity Authentication Based on Keystroke Latencies. Communications of the ACM. Vol. 39; pp 168-176.

Leggett, J., Williams, G. (1988). Verifying Identity via Keystroke Characteristics. International Journal of Man-Machine Studies, 28.

Leyden, J. (2002). PDAs Make Easy Pickings for Data Thieves. The Register. www.the register.co.uk/content/54/25478.html

Monrose, F., Reiter, M., Wetzel, S. (1999). Password Hardening Based on Keystroke Dynamics. Proceedings of the 6th ACM Computer and Communication Security Conference.

Nanavati, S., Thieme, M., Nanavati, R. (2002). Biometrics. Identity Verification in a Networked World. John Wiley & Sons.

Ord, T. (1999). User Authentication Using Keystroke Analysis with a Numerical Keypad Approach. MSc Thesis, University Of Plymouth, UK.

Richardson, T. (2002). PDA Shipment Growth Slows. The Register. www.theregister.co.uk.

Singh, H., Furnell, S.M., Lines, B. and Dowland, P.S. (2001). Investigating and Evaluating Behavioural Profiling and Intrusion Detection Using Data Mining. Proceedings of International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, St. Petersburg, Russia, 21-23 May, 2001.

Smith, R. (2002). Authentication. From Passwords to Public Keys. Addison Wesley

Thornton, C. (2001). Fast laptop includes built-in fingerprint reader. PC World.com. www.pcworld.com/news.

HP. (2002). Targus iPAQ™ Bundle. HP. http://athome.compaq.com/store/default.asp?page=optionCategories&SuperCategoryID=97

UMTS Forum (2002). Long Term Potential Remains High For 3G Mobile Data Services. www.umts-forum.org/reports.html. pp 5.

Acceptance of subscriber authentication methods for mobile telephony devices

Abstract

Mobile phones are now an accepted part of everyday life, with users becoming more reliant on the services that they can provide. In the vast majority of systems, the only security to prevent unauthorised use of the handset is a four digit Personal Identification Number (PIN). This paper presents the findings of a survey into the opinions of subscribers regarding the need for security in mobile devices, their use of current methods, and their attitudes towards alternative approaches that could be employed in the future. It is concluded that, although the need for security is understood and appreciated, the current PIN-based approach is under-utilised and can, therefore, be considered to provide inadequate protection in many cases. Surveyed users responded positively towards alternative methods of authentication, such as fingerprint scanning and voice verification. Based upon these findings, the paper concludes that a non-intrusive, and possibly hybrid, method of authentication (using a combination of techniques) would best satisfy the needs of future subscribers.

Keywords

Authentication, Mobile, GSM, UMTS, Biometrics.

Introduction

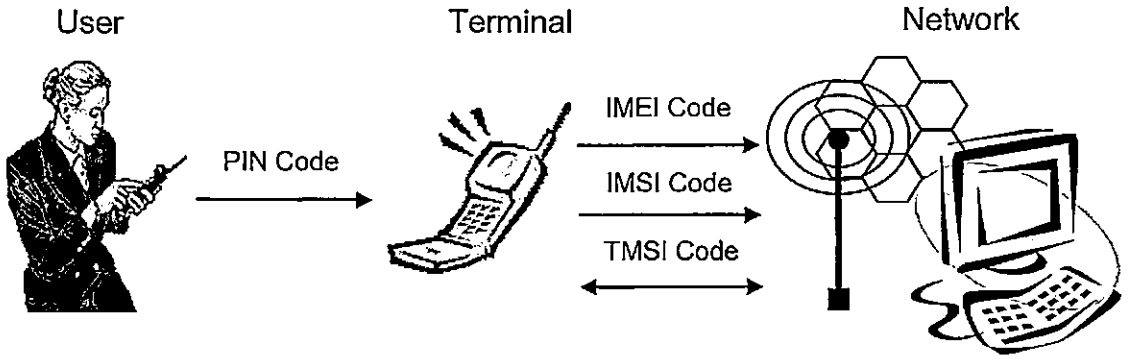
The mobile phone market has witnessed phenomenal growth in recent years, such that the phone itself is now regarded as an essential everyday item by millions of people. Indeed, cellular subscribers currently total around 479.5 million worldwide, a 56.87% growth on the previous year, with forecasts for the end of 2003 estimating that the number of subscribers will be in the region of 1.073 billion [1].

In addition to increasing subscribers, the capabilities of the phones themselves will also improve. With the introduction of third generation mobile devices, part of the ITU IMT-2000 initiative [2], a broadband service of up to 2Mbps will be on offer, providing the potential for true multimedia services [3]. As the technology advances, the range of potential services also expands. Whereas the first generation analogue phones of the 1980s were purely aimed at the provision of voice telephony services, the arrival of second generation (digital) phones in the early 1990s ushered in basic data services such as SMS (Short Message Service) text messaging. In more recent years, devices supporting the Wireless Application Protocol (WAP) have facilitated limited Internet access, and the emergence of faster access technologies, such as GPRS (General Packet Radio Service) and UMTS (Universal Mobile Telecommunications System), will hasten the convergence of the mobile phone with Personal Digital Assistant (PDA) devices. This, in turn, will significantly increase the range of in-built and network-based applications of the device, thus also increasing the range of potentially sensitive and private information that the devices will hold.

As the sensitivity of information stored on a mobile device increases, the need for effective security also increases. The 3rd Generation Partnership Project (3GPP), who provide the technical specifications and regulations for UMTS, have recognised the need for secure data communications and produced appropriate standards [4]. However, security over the air interface is only one aspect of the problem, and it is also important to ensure appropriate protection of the device against unauthorised access. Current mobile handsets do incorporate some level of protection in this respect, but it is fairly rudimentary, and as the need for security increases there is the potential to incorporate more advanced methods. At this stage, however, questions remain about the security measures that customers would expect, and tolerate, to protect their personal information. This paper considers the need for security on mobile handsets, end-user attitudes towards current authentication measures, and their views in relation to future service opportunities and the consequent security requirements that these will impose.

Subscriber authentication in mobile systems

At the time of writing, the dominant mobile network standard is GSM (Global System for Mobile communications), which accounts for 63% of the global cellular market [1]. The authentication security that the GSM networks currently provide is focused between the terminal devices and the network, as shown in Figure 1, with a number of checks being made to ensure that the handset is permitted to use the network, has not been reported stolen etc. By contrast, the security between the terminal and the subscriber is currently quite rudimentary, with subscriber authentication based upon the use of a Personal Identification Number (PIN).



PIN – Personal Identification Number
IMEI – International Mobile Equipment Identifier
IMSI – International Mobile Subscriber Identifier
TMSI – Temporary Mobile Subscriber Identifier

Figure 1 : User - Terminal – Network Security Processes

For the majority of mobile phones, the PIN is the only form of authentication required in order for a user to be able to access the device. The authentication process will typically only allow the user to enter the number incorrectly a finite number of times (typically three) before the Subscriber Identity Module (SIM) within the phone becomes locked and requires a special

unlock password (PUK) from the network service provider. In this way, brute force attacks on the PIN code (where every combination is systematically tried) are avoided. However, the security here assumes two things: firstly, that the PIN facility is activated, and secondly, that the user has not compromised its protection (e.g. by not changing it from the factory default, by writing it down, or by telling someone else) in the many that frequently occurs with other knowledge-based authentication approaches, such as passwords [5].

If the PIN facility is enabled, it may (depending on the make/model of phone) provide two levels of authentication. All phones can be configured to request the PIN when they are switched on (normally only allowing emergency calls in its absence). Some models also allow locking of the keypad when switched on, requiring PIN re-entry before each use. As such, the PIN is capable of providing protection, and to date it has generally been regarded as providing sufficient security, given that the information held on the devices is relatively limited (e.g. telephone numbers, simple text messages, etc.), and thus of little value to a thief. Therefore the main threat comes through unauthorised usage of the phone, which only exists in a finite window before the phone is reported stolen and subsequently disabled by the network operator. Recently, with the advent of WAP-enabled second-generation phones, there has been a movement towards the storage of more sensitive material. For example, some handsets contain a credit card reader that is able to make transactions over WAP-enabled web sites. Although this still requires a PIN identification before use, it does pose the question of how far we can rely on PIN codes, how secure they are, and how secure users believe them to be.

Whereas PIN-based authentication relies on something the user *knows*, an alternative method is authentication via something the user *is*, a domain more commonly referred to as biometrics. There are two categories of biometric authentication [6]:

- Physiological biometrics, based upon bodily characteristics (e.g. fingerprint analysis, facial recognition, iris scanning and ear geometry).

- Behavioural biometrics, based upon the way people do things (e.g. voice print, typing style).

Much research has gone into developing these techniques into practical systems, and they are already employed as alternative authentication methods in desktop PC environments - for example, 9% of the respondents to the 2001 CSI/FBI Computer Crime and Security Survey claimed to use biometric security technologies [7]. In addition, there is already evidence of their application within the mobile domain. The Sagem MC959 handset, for example, incorporates a fingerprint recognition system into the back panel [8]. When considering the application of biometrics, in the context of mobile handsets, appropriate thought needs to be given to the practicality of the technique. It is noticeable, for example, that physiological techniques generally require additional hardware, such as the fingerprint scanner, to be added, whereas behavioural techniques do not. Implementation of behavioural techniques can be achieved through software only. Clearly, for mass-market devices, component cost is a major consideration, and handset prices are already subsided by network operators in many countries in order to keep the cost down for the consumer. However another major consideration to take into account is how the subscribers actually feel about security. Customers in today's world dictate the success or failure of a product, so their attitudes and opinions are important factors to take into consideration.

A survey of subscriber attitudes towards mobile security

A survey was conducted to assess the attitudes and opinions of current mobile subscribers towards authentication on their phones. To this end, a questionnaire was devised that assessed the following aspects:

- how the phone is used (e.g. voice communications, text messages etc.) and how subscribers would like to use their phones in the future. This gauges the level to which additional security is necessary - if the phone is used purely for voice communications then the need for increasing security is questionable.

- users opinions about the current form of authentication, the PIN.

- whether users believe there is a need for increasing security, and if so how would they like to see a solution implemented.

The survey was distributed as hard copies to a wide range of people, with one proviso – in order to be able to offer a valid opinion, the respondents had to be current or past users of mobile phones. A total of 138 paper-based copies where returned. An on-line version was also created, achieving another 23 responses. Thus, a final total of 161 responses were obtained, and the results are analysed in the sections that follow.

General

The survey was not aimed at any specific age group or gender, the hope being to obtain a good cross section of users. As shown in Figure 2 below, 53.5% of respondents were in the 17-24 age group. Although at first glance this figure does not suggest a particularly representative sample, it is actually a fair reflection of mobile phone ownership in the UK, where the survey was focused. Recent market research studies have illustrated that teenagers now account for a significant proportion of phone purchases, particular in relation to pre-pay phone options [9]. With this in mind, the predominance of younger respondents in this study is less surprising, and serves to make the results a more accurate reflection of typical subscriber attitudes.

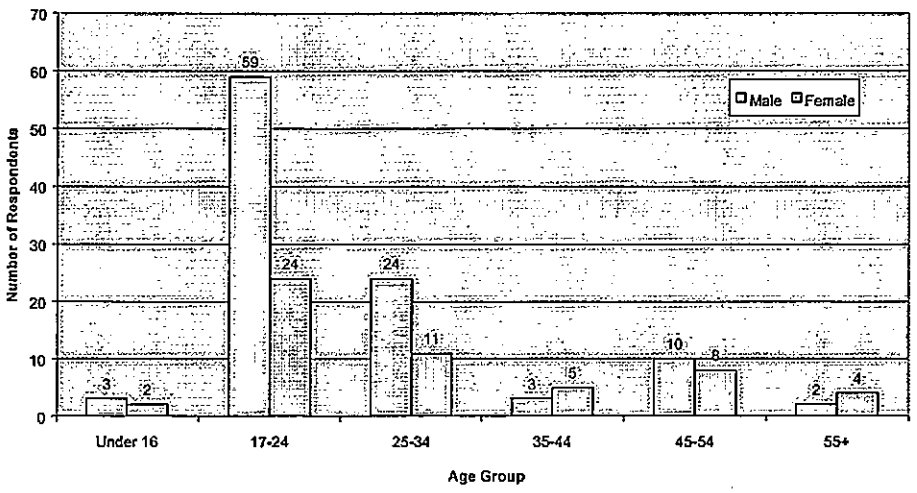


Figure 2 : Gender and age split in the respondent group

The desire to remain contactable is apparent from how long respondents leave their handsets switched on. 57% of those questioned said they kept their phone switched on for greater than ten hours a day, with 19% claiming between six and ten hours, and the percentage descending in order to 11% for less than one hour a day. These findings have a couple of implications:

- The need to leave the phone on comes in part from the need to stay in touch. So is the mobile phone the users principle means of doing this? Those switching on for less than one hour are likely to be users who only switch on when they wish to use the phone themselves. Thus either do not wish to be kept in contact with or have another principle means of communication, for instance a landline phone. Those leaving their phones on for a long period of time are likely to consider their phones to be there major means of contact, showing a possible long-term commitment towards the use of mobile phones.

- With the large number of respondents leaving their phone on, this could have implications for security, especially those who do not have or do not use a PIN facility to lock their keypad on standby.

Different phone manufacturer's, although providing a range of different phones, often keep the same software functionality, i.e. Nokia and its proprietary menu system. Nokia and Motorola's use of the PIN is no different in principle. However, whereas Motorola provides the facility to lock the keypad whilst on standby, Nokia however does not. In this particular sample, 57% of respondents are Nokia owners, of whom 96% leave their phone on for more than one hour a day, and 87% leave it on for more than six hours a day. This results in a significant number of unlocked phones on stand-by mode for long periods of time every day, leaving them with effectively no defence from un-authorised use if lost or accidentally left unattended.

Mobile phone usage - present and future

Unsurprisingly, results indicate that the vast majority use their mobile phone for talking. More interestingly, however, 90% of respondents regularly use text messages as a means of communication. Figure 3 illustrates these findings, in addition to responses for a range of other current services. The other services are newer, and from the responses have not been adopted as widely at present. A possible discrepancy in the data exists surrounding the use of the email service. Although this service is currently available on only a small proportion of handsets, 64% responded 'yes' or 'no' to the question of whether they used the facility. It is considered likely that many respondents who answered 'no' were doing so because their phone does not offer them the option (and, therefore, they should ideally have selected the 'not available' option on the questionnaire). This hypothesis also applies to the use of WAP services. However, it is valid to note the proportion of users that do use their phone for WAP and email services stands at 6% and 9% respectively, indicating an emerging acceptance and use of advanced data services.

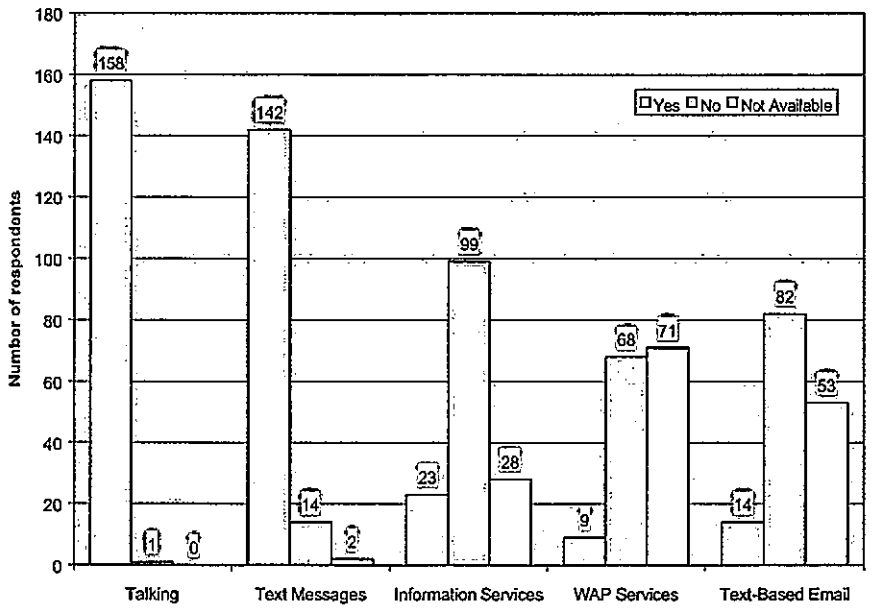


Figure 3 : Services used by respondents

Respondents were also asked whether they would consider using a small range of other services that are likely to be offered by future mobile handsets. The questionnaire specifically suggested the options 'video conferencing', 'online shopping', 'World Wide Web', 'Downloading music' and 'Personal Organiser', as well as offering respondents the option to suggest other ideas that would interest them. The results strongly suggested that the adoption of advanced mobile service is likely to continue, with 40% looking to use video conferencing, 43% interested in online shopping, 58% desiring mobile web access, 53% wishing to download music, and 73% wanting an integrated personal organiser. Although the latter would not necessarily involve communication between phones and the network, the data stored in personal organisers could well contain sensitive information such as bank account details etc. The additional services that were suggested by respondents included 'digital money', 'radio', and 'global positioning system' – all of which are very likely to emerge in combination with telephony handsets. Overall, it is also worth noticing that 88% of respondents did want to use some form of additional service.

Usefulness of current security

As previously discussed, the primary method of user authentication for mobile phones is the PIN, which is able to provide up to two levels of security. Although 89% of respondents knew about the PIN facility, only 56% of them use it in either form. The survey shows that 76% of respondents had phones with only one level of security (at power on). Of those users that did have both levels of security, only 46% of them used the second level on a regularly basis. Asking whether the respondents feel entering a PIN number is inconvenient, 41% responded 'yes' with the same percentage also expressing doubts about the level of protection the PIN can provide. Although the results are not conclusive enough to put an argument for or against the usefulness of the PIN facility, there are a number of significant points that can be drawn from the data:

- 11% of respondents did not know about the PIN facility. On the face of it, this is a relatively small percentage, but on a worldwide scale that accounts for 52.8 million subscribers who do not even know that security is available.

- Of the 44% of respondents who do not use the PIN facility, 65% of them considered it to be inconvenient, thus suggesting a good reason why they do not use it.

- Providing additional levels of security does not necessarily provide the user with additional protection if s/he does not use it through inconvenience. 64% of respondents for whom the ability to PIN-protect the phone between calls is available, still do not use the facility because they find entering the PIN inconvenient.

- A significant proportion of respondents, 41% do not have confidence in the protection the PIN facility provides, indicating users believe their phone is still at risk from misuse even if the PIN facility is in use.

- 52% of female respondents do not use the PIN facility compared to 39% of males.

The survey also asked respondents to comment about issues relating to the compromise of security. When asked to consider compromise by another party, only 11% of users believed that their phone had been used without their permission. The real percentage is likely to be higher, from misuse that has gone undetected. For instance people who may use the phone briefly without the owner's knowledge. Those respondents who answered positively to this question are likely to have had their phone stolen, and thus detected the misuse. The questions also considered compromise of protection arising from the subscribers' own actions. There are several ways in which subscribers may invalidate the PIN security, such as revealing the number to someone else, forgetting it, or writing it down. Table 2 presents a summary of the findings here.

	Yes (%)	No (%)
Forgotten It	17	83
Told Someone Else	26	74
Taken a Written Note Of It	6	94

Table 2 : Respondents who invalidate their PIN protection

Attitudes towards future authentication options

With mobile handset manufacturers and network operators both aiming to provide users with additional services, the need for security is likely to increase. This survey has identified that users are already using data services, and are willing to use future services as and when they become available. It is an encouraging sign that the respondents also recognise the need for security, with 81% believing it would be either good or very good to have more security. Only two respondents thought it would be bad idea. This recognition shows that users are aware of the need for security, and are also possibly worried about their current level of protection. Interestingly, however, the desire for more security shows a downward trend as the respondents' age increases, as shown in Table 3.

Age Group	Responded positively to additional security (%).
Under 16	100
17-24	89
25-34	72
35-44	66
45-54	68
55 or older	42

Table 3 : Respondents opinions on having additional security

Having established that respondents were generally accepting of additional authentication measures, the survey proceeded to assess their preferences for the forms that it could take. Having determined that PIN-based protection is problematic, it is considered that other authentication methods based upon something the user *knows* (e.g. passwords) would be equally under-utilised or inconvenient. The implication of this is that the most sensible route for improving authentication is to base the approach upon a biometric technique (the other option for authentication, basing it upon something the user *has*, is likely to offer little advantage, as the phone itself is something the user has, and any supplementary authentication token would be likely to be kept with the device). With this in mind, the survey respondents were presented with a range of biometric authentication options and asked to indicate which of them would be preferable to the PIN. The biometrics offered as options were as follows: fingerprint recognition, voice print recognition, ear geometry, facial recognition, iris scanning, and typing style All of these techniques have been the focus of previous research, and some are already widely recognised as commercial products in the domains of physical access control and desktop computing [10]. Techniques such as ear geometry (in which the subscriber would be identified by the physical shape of their ear) and typing style (in which authentication would be based upon characteristic inter-keystroke latencies observed when subscribers dial numbers or otherwise interact with the keypad) are less recognised in the marketplace, but are considered particularly suited to non-intrusive application in a telephony context. The respondents' opinions in relation to the techniques are illustrated in Figure 4.

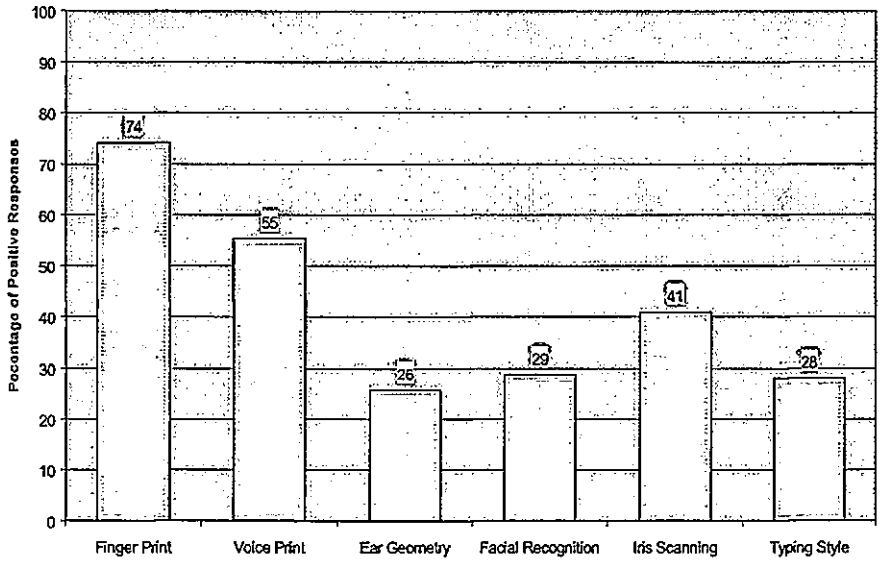


Figure 4 : Positive responses to biometric authentication techniques

The results showed a strong preference towards fingerprint analysis, with approximately three quarters of the respondents selecting this option. Voice print analysis and iris scanning also achieved good scores, albeit significantly lower than fingerprint analysis in both cases. The remaining three techniques were demonstrably less popular, appealing to just over a quarter of respondents in each case. However, any conclusions drawn from these results should be tempered with the observation that the respondents are likely to have responded most positively to those ideas that they have already heard of. Fingerprints have long been known to provide a means of successfully identifying people, and indeed such techniques are already being used in mobile phones. Voice print analysis has also attracted much attention through the media, computer software applications, and also in the phone industry (albeit in the context of voice recognition for dialling numbers, rather than as a means of authentication). It is also fairly easy to understand this authentication technique, as people generally sound different. Techniques such as ear geometry and typing style are newer, and less information is known about them. Although keystroke analysis techniques have been extensively researched for use in PC-based authentication [11,12], it is not a widely advertised or used technique. As for ear geometry, although it is not very difficult to imagine how this technique might possibly work, there are no current implementations on the general market, and knowledge about this technique would, therefore, have been very limited amongst the respondents.

The point, therefore, is not to regard the results as a conclusive attitude towards one technique over another. The key observation that can be made is that all techniques were (to some degree) considered favourably, and that if a technique were to be implemented that was less known about generally, a degree of education and awareness before wide scale adoption.

One advantage of certain biometrics when compared to the PIN is that they offer the potential for authentication to be performed on a continual basis rather than as a one-off judgement. Respondents were, therefore, asked whether they would consider continuous authentication during a call to be acceptable. The results revealed that 41% of respondents considered continuous authentication during a call to be a good idea, while 24% were against the idea, and 35% were indifferent to the idea. However, the actual number of users willing to break during their call to authenticate themselves is likely to be low, which implies that any

continuous authentication method implemented would have to be non-intrusive (without explicit action by the user). Certain authentication techniques will clearly lend themselves to this better than others, for instance voiceprint, as the user would be talking on the phone already. Techniques such as keystroke analysis would not typically be viable during a traditional voice call, but could potentially provide a measure of authentication as each call is initiated, or during the conduct of keypad-oriented, non-voice sessions.

For all authentication techniques, including the PIN, some information needs to be stored so that a comparison is possible with the input data. The final objective of the survey was to establish users opinions on where this profile should be stored – on the phone or in the network. The advantage of storing the profile on the phone is that authentication can then occur completely on the phone, with the result that no personal details are communicated to and from the network, and the network traffic overhead is minimised. However, the disadvantage is that the user is then restricted to being authenticated on the one phone. By having profile information stored on the network, users would be able to login at any network access point, thus enhancing their personal mobility. It would also enable the network operator to monitor the success or failure rates for possible misuse. Where a preference was expressed, the opinions from the survey respondents clearly favoured the profile being held in the handset, with 52% of respondents selecting this option. By contrast, 26% favoured the network, while 20% did not mind and 2% did not understand the question. Given that the respondents were probably not be giving much thought to the issue of the network overheard, it is likely that their preference for the handset-based profile relates to the ability to retain control over their own profile data.

Discussion

Although the results have suggested the desire for a greater level of security, this clearly represents something of a contradiction when it is considered alongside the fact that many respondents do not even use the current method that has been provided for them. This suggests that it is the security technique, rather than the concept of security, that users are rejecting, and as such a move towards non-intrusive methods of authentication may provide the protection that users are looking for, but without the associated inconvenience that is currently perceived. Although fingerprint scanning was a favourite technique, it does not necessarily lend itself to non-intrusive implementation, as the user would need to place his/her finger on the scanner. If the scanner were to be placed in a natural area on the phone where a finger would normally be placed to hold the device, then the level of intrusiveness would be arguable. Voiceprint lends itself to both one-off and continuous monitoring of voice communications, but would either lose its non-intrusiveness, or the ability to authenticate, on data communications. Keystroke analysis also lends itself to non-intrusive authentication for one-off monitoring and would be more likely to facilitate continuous monitoring during the utilisation of keypad-oriented services.

Since none of the biometrics discussed can provide non-intrusive authentication for all possible scenarios, and secondly cannot provide 0% false acceptance and false rejection rates, it would seem logical to provide a hybrid model of authentication, using a number of non-intrusive methods as first/second line security, with the PIN (or some other knowledge-based methods) providing a fallback method if needed. Current research is focusing upon the realisation and evaluation of such an approach, and the authors are investigating the application of biometrics in this context. A preliminary investigation of keystroke analysis has been conducted to assess whether it is possible to authenticate people from the way in

which they dial numbers on a standard GSM handset. Although the results are not conclusive at this stage (with false acceptance and false rejection errors of around 15% being observed), it is considered that refinement of the technique may yield better performance. The full results from this element of the investigation will be published in due course.

Conclusions

The survey findings have indicated a weakness of the current security provisions on mobile handsets, in that the authentication technology is optional and, therefore, not used by a large proportion of users. However, subscribers have shown both the need and the desire for additonal security, and have responded positively towards a number of alternative authentication techniques. At the same time, the results showed that many respondents do not use the current security techniques that are available to them. In view of this, it can be assumed that a non-intrusive method of authentication may prove to be most acceptable and widely utilised by end users.

With the introduction of the third generation phones, a range of new services will become available from mobile devices – services that the respondents in the survey indicated that they would be keen to use. In this context, the protection of users' information must become a prime concern, especially when considering the possible sensitivity of the data, and the need for a sucessful transition into a multi-billion dollar m-commerce market. Security is, therefore, essential, and approaches must be employed that subscribers will tolerate and use.

References

[1] Intekom. 2001. *Latest Global & Regional Cellular Statistics.* http://home.intekom.com

[2] ITU. 2001. Full description of the IMT-2000 (International Mobile Telecommunications) initiative located on the ITU (International Telecommunications Union) website at www.itu.int, Radio-Communication (ITU-R) division.

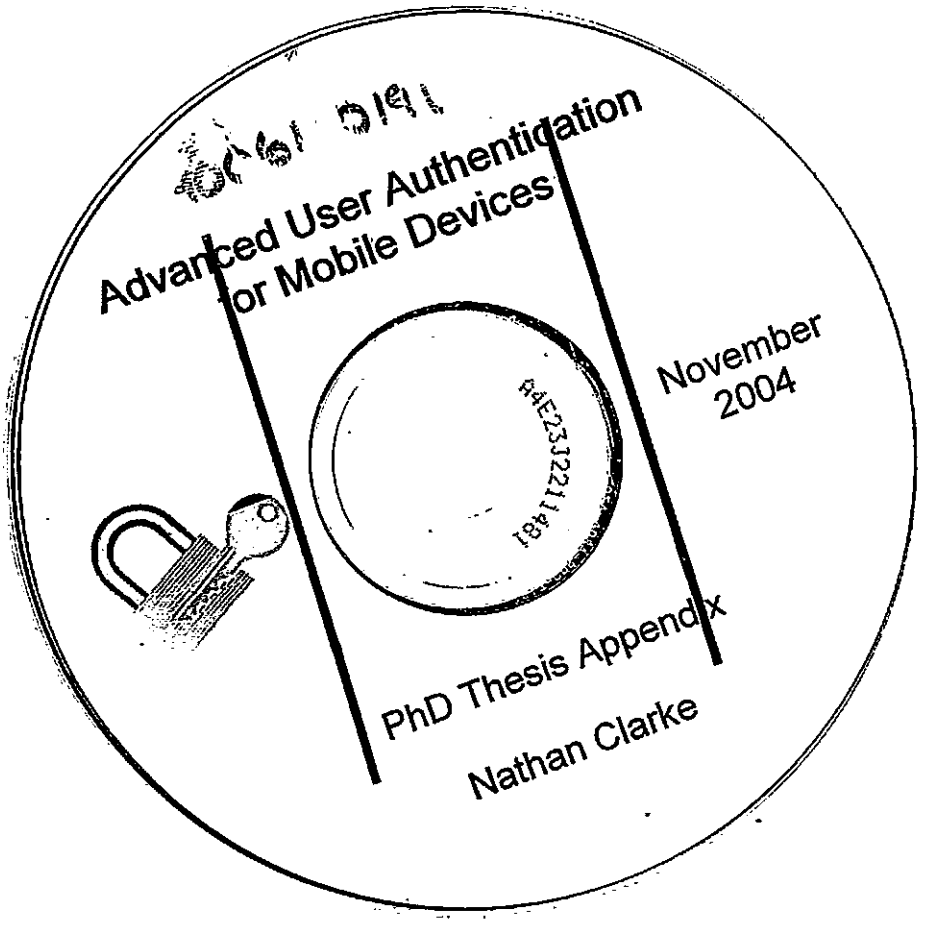
[3] UMTS Forum. 1998. *The Path towards UMTS – Technologies for the Information Society.* Report no. 2. The UMTS Forum. http://www.umts-forum.org/reports.html

[4] 3GPP. 2000. *Terms of Reference: Services and System Aspects – Working Group 3.* TSG SA WG3 – Security. http://www.3gpp.org/TSG/ToR/TSG-SA/sa3-tor.htm

[5] Jobusch, D.L. and Oldehoeft, A.E. 1989. "A Survey of Password Mechanisms: 1", *Computers & Security*, Vol. 8, No. 7: 587-604.

[6] Cope, B.J.B. 1990. "Biometric Systems of Access Control". *Electrotechnology*, April/May: 71-74.

[7] CSI. 2001. '2001 CSI/FBI Computer Crime and Security Survey', *Computer Security Issues & Trends*, vol. VII, no. 1. Computer Security Institute. Spring 2001.


Advanced User Authentication for Mobile Devices
November 2004
PhD Thesis Appendix
Nathan Clarke

[8] SAGEM. 2000. "SAGEM points a finger at GSM", Press Release, 24 January 2000. http://www.sagem.com/en/communiques-en/cp-1sem2000-en.htm#mc 959 id empreinte

[9] Miller, S. 2001. "Mobile sales soar, driven by teenage market", MediaGuardian report, 23 May 2001. http://media.guardian.co.uk/newmedia/story/0,7496,495263,00.html.

[10] Polemi, D. 1997. *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable*, Institute of Communication and Computer Systems, National Technical University of Athens. April 1997.

[11] Legget, J. and Williams, G. 1988. "Verifying identity via keystroke characteristics", International Journal of Man-Machine Studies, 28.

[12] Joyce, R. and Gupta, G. 1990. "Identity Authentication Based on Keystroke Latencies", Communications of the ACM, Volume 33, February 1990.