2014

Non-Intrusive Continuous User Authentication for Mobile Devices

Karatzouni, Sevasti

http://hdl.handle.net/10026.1/3225

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.

Non-Intrusive Continuous User Authentication for Mobile Devices

by

Sevasti Karatzouni

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

DOCTOR OF PHILOSOPHY

School of Computing & Mathematics

December 2013

Abstract

Non-Intrusive Continuous User Authentication for Mobile Devices

Sevasti Karatzouni

The modern mobile device has become an everyday tool for users and business. Technological advancements in the device itself and the networks that connect them have enabled a range of services and data access which have introduced a subsequent increased security risk. Given the latter, the security requirements need to be re-evaluated and authentication is a key countermeasure in this regard. However, it has traditionally been poorly served and would benefit from research to better understand how authentication can be provided to establish sufficient trust.

This thesis investigates the security requirements of mobile devices through literature as well as acquiring the user's perspectives. Given the findings it proposes biometric authentication as a means to establish a more trustworthy approach to user authentication and considers the applicability and topology considerations. Given the different risk and requirements, an authentication framework that offers transparent and continuous is developed. A thorough end-user evaluation of the model demonstrates many positive aspects of transparent authentication. The technical evaluation however, does raise a number of operational challenges that are difficult to achieve in a practical deployment.

The research continues to model and simulate the operation of the framework in an controlled environment seeking to identify and correlate the key attributes of the system. Based upon these results and a number of novel adaptations are proposed to overcome the operational challenges and improve upon the impostor detection rate. The new approach to the framework simplifies the approach significantly and improves upon the security of the system, whilst maintaining an acceptable level of usability.

Table of Contents

List of Figures

List of Tables

Acknowledgements

After a long journey and life difficulties in completing this body of work I would like to thank the people that support me through the course of this study.

First and primarily I would like to thank my DoS Dr. Nathan Clarke, without whom I would have never started or completed this work. His invaluable and restless support and guidance, advice and encouragement –so much as a supervisor as well as a friend, have been inspiring and driving forces for me throughout this study. I owe him much of what I have achieved in my studies as well as my professional life.

I would also like to thank my supervisor Prof. Steven Furnell for his support, guidance and feedback on the course of this study. He has been inspiring with his experience and has been an invaluable contributor to me reaching this stage.

I would also like to thank the members of the research group who have supported me primarily in the beginning of this study and for making the office a great place to be and work. Thanks go also to my friends who believed more than me that I am going to submit this one day!

Lastly but more importantly I would like to thank my family, my Dad, my Mum and my sister Charis for their love and restless support. Without them much would not have been possible.

Dad – as promised

Author's Declaration

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

Work submitted for this research degree at the Plymouth University has not formed part of any other degree either at Plymouth University or at another establishment

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

Publications (or presentation of other forms of creative and performing work):

Journal Papers:

Furnell, S., Clarke, N., Karatzouni, S. (2008): "Beyond the PIN: Enhancing user authentication for mobile devices", Computer Fraud & Security, Volume 2008, Issue 8, pp12-17, 2008

Conference Papers

Clarke, N., Karatzouni, S., Furnell, S. (2011): "Towards a Flexible, Multi-Level Security Framework for Mobile Devices", Proceedings of the 10th Security Conference, Las Vegas, USA, 4-6 May, 2011

Clarke, N., Karatzouni, S, Furnell, S. (2009): "Flexible and Transparent User Authentication for Mobile Devices", Proceedings of the 24th IFIP TC 11 International Information Security Conference, Pafos, Cyprus, May 18-20, ISBN: 978-3-642-01243-3, pp1-12, 2009

Clarke, N., Karatzouni, S., Furnell, S. (2008): "Transparent Facial Recognition for Mobile Devices", Proceedings of the 7th Security Conference, Las Vegas, USA, 2nd-3rd June, 2008

Karatzouni, S., Clarke, N., Furnell, S. (2007): "Device- versus Network-Centric Authentication Paradigms for Mobile Devices: Operational and Perceptual Trade-Offs", 5th Australian Information Security Management Conference, Mount Lawley, Australia, 5th December, 2007

Karatzouni, S, Clarke N., Furnell, S. (2007): "Utilising Biometrics for Transparent Authentication on Mobile Devices", Proceedings of the 2nd International Conference on Internet Technologies and Applications, 4-7 September, Wrexham, UK, ISBN: 978-0-946881-54-3, pp549–557, 2007

Karatzouni, S, Clarke, N. (2007): "Keystroke Analysis for Thumb-based Keyboards on Mobile Devices", Proceedings of the 22nd IFIP International Information Security Conference (IFIP SEC 2007), Sandton, South Africa, 14-16 May, pp. 253-263, 2007

Karatzouni, S, Furnell, S., Clarke, N., Botha, R. (2007): "Perceptions of User Authentication on Mobile Devices", Proceedings of the ISOneWorld Conference, Las Vegas, USA, April 11-13, CD Proceedings (0-9772107-6-6), 2007

White Paper Reports

Clarke, N., Karatzouni, S., Furnell, S. (2006): "Operational and perceptual trade-offs between device- and network-centric authentication models", Eduserv research project deliverable, December 2006

Clarke, N., Karatzouni, S., Furnell, S. (2006): "Applicable authentication methods for mobile devices and services", Eduserv research project deliverable, June 2007

Presentation and Conferences Attended:

10th Security Conference, Las Vegas, USA, 4-6 May, 2011

24th IFIP TC 11 International Information Security Conference, Pafos, Cyprus, May 18-20, 2009

2nd International Conference on Internet Technologies and Applications, 4-7 September, Wrexham, UK, 2007

ISOneWorld Conference, Las Vegas, USA, April 11-13, 2007

Third Collaborative Research Symposium on Security, E-learning, Internet and Networking (SEIN 2007), Plymouth, UK, 2007

External Contacts:

Word count of main body of thesis: 51,339

Signed ……   ……

Date   …………….05/12/2013…………..

1 Introduction

This thesis is concerned with the investigation into flexible and robust authentication for mobile devices. The latter aspect has experienced an enormous evolution over the past decade not only regarding hardware features but also a significant number of applications and services for both the personal and business user – establishing a new role in life and business. Whereas the evolution of the hardware has added much value for the storage and processing of information, the evolution of mobile networking enables this data to be communicated, shared and accessed with almost seamless overhead. Given current use of the mobile device and the nature of the information stored and accessed it is likely to contain personal and private information. As such there is a higher risk with misuse of these devices as potential exists for several impact factors to an individual as well as an organisation linked to loss of confidentiality, integrity and availability.

Within this context the security provision on mobile devices needs to address the increasing requirements for protection in order to sufficiently safeguard the device and ensure that only a legitimate and authorised user has the ability to access their data. For this to be addressed there needs to be a robust way to verify the user's identity. Traditionally user authentication on mobile devices has been provided through the use of a Personal Identification Number (PIN) and later on with passphrases. However it has been established that secret-based knowledge techniques have inherent weaknesses as means to verifying someone's identity as they are based on secrets that can be shared, stolen, forgotten or written down. In

the contrast authentication approaches like biometrics that are based on unique characteristics or behaviour tied to the individual can offer a more confident trust to the user as these traits cannot be shared, lost or forgotten and removing the inconvenience of all the latter. Biometric authentication has been seen as alternative, convenient and trusted means, with devices using techniques like fingerprint and face recognition. However the way that even biometric authentication is applied only addressed principally one issue and that is the initial verification of the user that switches on the phone or unlocks at some point. However after initial verification there is no further verification to who is using the device while the use has access to any operation on the device. Safeguards like screen locks provide some further security support if they have been activated however a lot of users seem not to utilise PINs in the first place due to inconvenience.

To address the aforementioned issues this research has investigated the objectives and the currently imposed security requirements for mobile devices and presents a means of addressing those in a convenient but also more secure manner for the user. It proposes a framework for continuous and transparent authentication and evaluates it for its effectiveness and user experience. Through recognising the pitfalls of the evaluated framework, the research continues to seek to improve upon it, by looking into the use of multi-biometric fusion to provide a more robust approach. Furthermore it considers a new approach to the operation of the framework and evaluates its improved effectiveness.

1.1 Background

Recent years have experienced a significant transformation of mobile devices from a communication device to an everyday personal gadget or business tool. Mobile devices have transformed to a necessity of everyday life for the individual and businesses offering a range of applications, service and data storage for the user. With currently more than 6 billion mobile subscribers in the world these type of devices play a significant role in today's world driving a communications market of $398.0 billion in 2012 (MobiThinking, 2012; Sideco, 2012). Given the type of use that is enabled through the use of mobile devices it is imperative to consider the security of the information stored and accessed through them. Business and personal records, emails, spreadsheets and other documents, electronic wallets are all examples of potentially sensitive information that could be stored or access from a mobile device. Given the amount of loss and misuse reported today the risk factor formed in a mobile environment has grown significantly. 60 % of survey respondents said they are using their personal devices to access work email or the company's network making this access the "newest and largest vulnerability in corporate America now" (Confidenttechnologies.com, 2011). At the same time cell phone theft comprises the 40% of all theft in major American cities and close to 314 phones are subject of theft every day only in London (Wirelessindustrynews, 2013). A mobile device unlike the traditional desktop is far more prone to misuse due to the lack of physical borders and control where default security mechanism that can be used to protect assets physically are not applicable in a mobile environment.

Traditional safeguards for mobile devices have been PINs and passwords which research has shown are poorly used as they are considered inconvenient. (Confidenttechnologies, 2011). Furthermore, the mere use of secret knowledge techniques has been suggested as an insufficient means to authenticate, as a secret can be easily shared or stolen. As such newer authentication protection mechanisms have been subsequently researched with biometrics being one alternative authentication technique that has been traditionally seen as a more secure approach to user authentication. Unlike a secret, biometrics which are based on the physiological or behavioural traits of a person are tied to the individual and can more strongly be used in an identity verification process whilst at the same time removing the inconvenience of remembering or carrying a secret. In the realisation that biometrics can offer a more secure alternative to current authentication schemes the market of biometric-based security products and services for mobile phones is growing expected to generate over $161 million revenue by 2015 (Goode Intelligence, 2011). Products like Google's FaceLock and Apple's Touch ID fingerprint sensor show that an investment towards biometrics in mobile devices are currently a reality that companies are investing into given the requirements of more robust security (Facelock, 2013; Apple, 2013).

1.2 Aim & Objectives

The overall aim of this research is to investigate user authentication alternatives for mobile devices[1]. This research directly builds upon a previous research study

---

[1] Although in this report with the term we primarily to mobile phones, any device with mobility capabilities such as small laptops and tablets are considered.

undertaken that initially proposed a transparent and continuous authentication approach (Clarke, 2004). This research starts where the last study ended, through developing and building upon the proposed framework. Upon completion of an operational prototype, the system was fully evaluated, both technically and by end-users. Building upon the findings, the research continued to propose a number of novel approaches to improve upon operational performance and user convenience. The research was partly funded by the EduServ Foundation and a series of white papers were published (see Appendix A).

The specific objectives of this research are:

- Review the current security provision within mobile devices and better understand the risks associated with a mobile environment

- Undertake a requirements analysis on user perspectives and practical implementations of a biometric-based authentication mechanism

- Develop an operational prototype of the NICA framework – a proposed user authentication system that operates in a transparent and continuous fashion.

- Perform a practical evaluation though the use of the prototype in an end-user trial to assess its operation and acquire the user's perspective and acceptance on such an approach

- Perform a further investigation using simulation to model the different scenarios and parameters of the framework and its performance under those.

- Investigate the use of multi-modal/multi-instance biometric fusion within the framework and evaluate whether the operation of the framework improves.

- Propose and evaluate a new approach in the operation of the authentication mechanism to incorporate the best operating attributes of the framework and the outputs of prior evaluations

1.3 Thesis Overview

Chapter 2 provides an overview of the current mobile device usage and the security issues that surrounds it as well as available safeguards. It looks at user authentication and presents an overview of biometric authentication with a particular focus upon identifying techniques that are applicable in the concept of transparent authentication and offer cost-free deployment in current devices.

Chapter 3 presents the requirements analysis stage of this research. A focus group activity was undertaken to explore user views in current authentication as well to assess their receptiveness in the use of biometrics and transparent and continuous authentication. This complemented and built upon a prior quantitative survey that was undertaken (Clarke & Furnell, 2002) A further analysis has been completed to address the risk as currently perceived and handled within the current security provision and how to understand how this needs to further addressed given current usage. The chapter continues to propose a novel approaches to risk assessment

and concludes with an overview of the conceptual architectural issues that would be envisaged.

Chapter 4 provides an overview of the framework under evaluation – NICA, presenting its basic operations and concepts. A short discussion on the developed prototype follows and the methodology and evaluation results of a practical user trial. The trial involved 27 participants who enrolled and utilised the system both as an authorised user and as an impostor given a particular set of tasks while at the end of the practical scenario the users filled a questionnaire evaluating their experience.

Chapter 5 is concerned with presenting the methodology and results of the modelling and simulation of the NICA framework. Whilst the model has a number of merits, a significant number of operational considerations need to be defined. The chapter proceeds to discuss the impact of these upon security and user acceptability.

Chapter 6 seeks to address the issues highlighted by the user trial and modelling by proposing a number of modifications to the framework decision making processes to incorporate fusion. An evaluation of these proposals is presented focussing upon its effectiveness and the added value it brings.

Whilst the improvements proposed in Chapter 6 do improve upon the existing research, they still present a number of challenges. Chapter 7 seeks to re-design the "intelligent" mechanisms that provide transparent and continuous authentication. The new seeks to simplify some of the complexities of the original framework.

The conclusions are presented in Chapter 8. The chapter begins by presenting the achievements of the research and its limitations before finishing with future research directions.

2   Mobile Devices – Security & Risks

2.1   Mobile Devices Usage

The evolution and change on the mobile landscape is close to simulate much of what a traditional computer had to offer. By providing functionality that extends beyond telephony, the mobile device has evolved from being a cumbersome telephone to become a necessity people utilise every day, for a variety of applications. This level of functionality can be seen to be significantly expanding, with devices today having similar processing and memory capabilities to PCs of a few years ago. Indeed, their combination of portability and capability means that handsets such as smartphones and PDAs are starting to have an increasingly significant role as mobile computing and network access devices. The increase in processing power and storage capabilities provides even better options for the advancement of these devices. The majority of the mobile devices at present, offer the ability of organizing and scheduling work, storing and processing documents, connecting to wireless networks, accessing emails, making m-payments, and a number of other functions that the past devices could not support.

Mobile devices have a huge market penetration over the last few years, experiencing a world-wide adoption with currently counting 6.8 billion mobile-cellular subscribers worldwide (ITU, 2013). Given their enhanced capabilities for data store, application and service use compared to their original and traditional phone and SMS facility, mobile devices have taken a significant merit on a market that previously only personal desktops were entitled to. A Google study over US, UK, French, Dutch and

China markets showed that more consumers now have an internet-enabled device than a desktop or laptop computer (Education Stormfront, 2012).

Further to the functionality of the device itself, the number of services that can be accessed through them have evolved too. The major contribution for this evolution of mobile handsets was the evolution of mobile networking. The introduction of Third Generation (3G) technologies and now moving towards Fourth Generation (4G) has provided the underlying mechanism for a wide variety of innovative data orientated services. Currently, the 3GPP family of 3G networks with a 3G/3.5G market being projected to reach 4.27 billion subscribers by 2017 (PRWeb, 2012).

Mobile networking began in the early 80's with the introduction of analogue cellular networks and met its first change in the mid 90's when 2nd generation networks(2G) and the Global System for Mobile Communications (GSM) technology was introduced (Vriendt, 2002). GSM phones brought a boost in mobile usage as the digital factor was introduced giving the option of data transfer and also cheaper communication solutions such as text messaging. With 2G a move towards data-centric services took place and the need for better throughput brought further advancement to the 2G technology, such as General Packet Radio Service (GPRS) or 2.5G and Enhanced Data rates for GSM (EDGE) or 2.75G, offering 8-92 Kb/s and 8-384 Kb/s respectively – almost 3 times the data capacity of GPRS (Mohr & Konhauser, 2000; GSMA, 2012a). With the arrival of 3rd generation technologies that enabled bandwidth of up to 2Mb/s, with Universal Mobile Telecommunications System (UTMS), mobile networks improved even more in terms of what they were able to offer to mobile subscribers. Now with Long Term Evolution (LTE) technology

being used by GSM and CDMA (– another competing for 3G) operators are looking for data transfers of 100Mbps and 50Mbps for downlink and uplink respectively (GSMA, 2012b). The 4G/LTE-Advanced technology which has recently been standardised by ITU and has theoretical peak data rates in the region of 1 Gigabit/s further enabling new features and higher quality services with expectations of 30 times faster connections than 3G (CellularNews, 2012; Practical Ecommerce, 2010). Figure 2.1 shows the evolution of technologies while Figure 2.2 illustrates the change that these advanced technologies have enabled in each step for the service to the user.

.
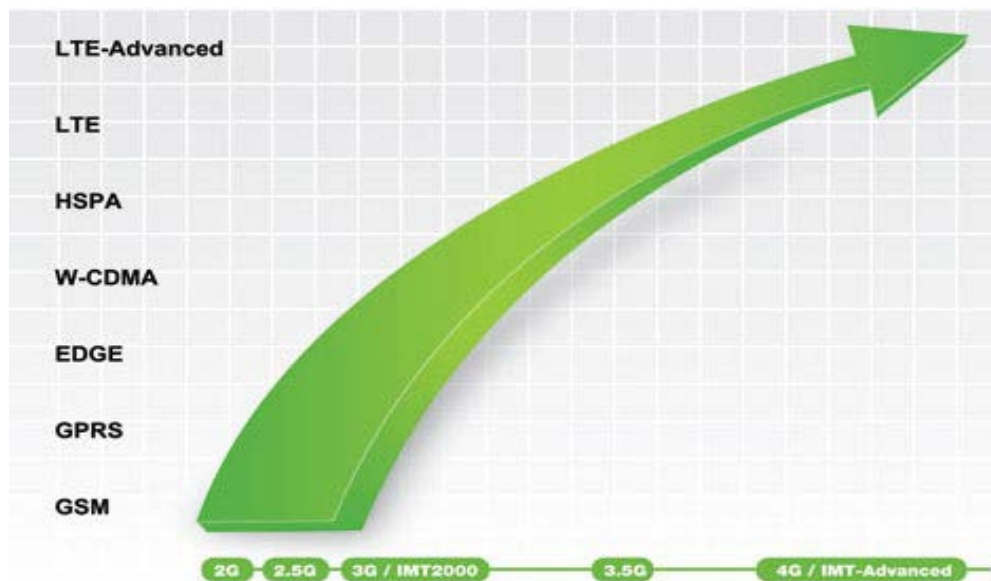
Figure 2.1: Evolution of GSM technologies towards 3G/4G (Source: 3GPP,2012)
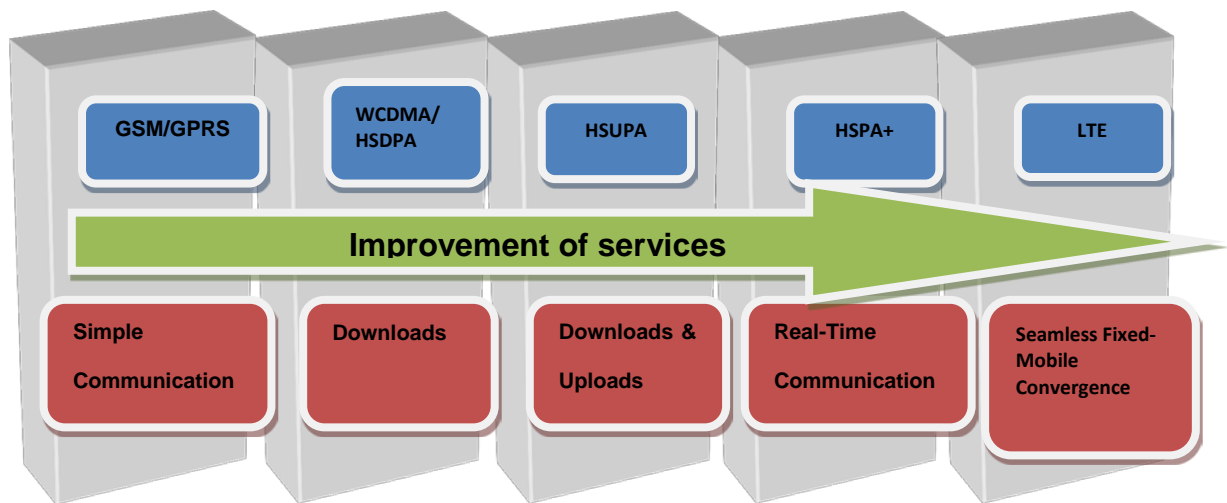
Figure 2.2: The change of services through the evolution of technology. (Adapted from QualComm, 2007)

Following an incline in potential on every step of this evolution, a realization of the role that mobile handsets have to play in the future can be made. Nowadays, GSM and 3GSM accounts for close to 5.37 Billion subscriptions globally (GSAcom, 2012). Figure 2.3 illustrates the increase on the adoption of the mobile solution, and its leading position in relation to other types, having a significant incline in the last few years.
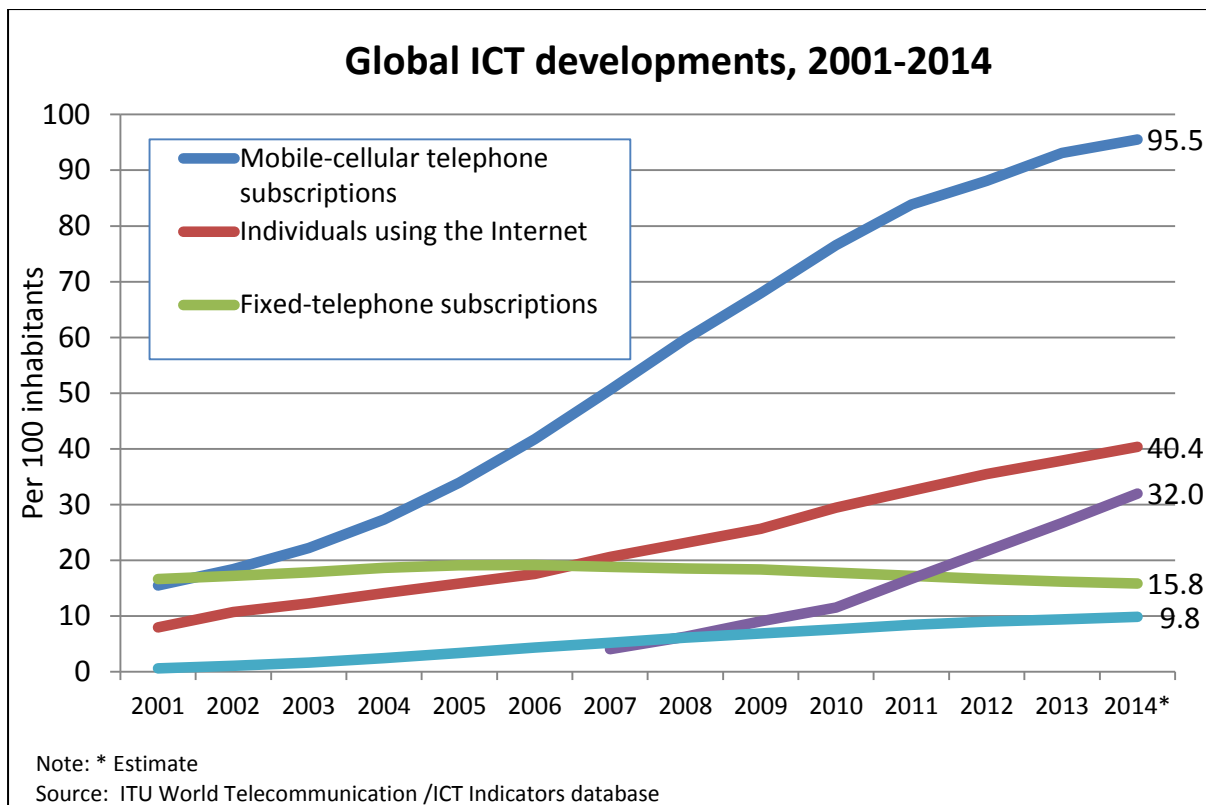
Figure 2.3: Global ICT developments (Source: ITU World Telecommunication, n.d.)

Modern mobile handsets are not only catching up to the functionality with traditional computers but also are taking the lead in adoption in relation to feature devices, with people increasingly integrating the mobile environment into their lifestyle (Comscore, 2012). With smartphones prices dropping significantly over the years the technology becomes far more widespread and accessible (Frommer, 2010). Deloitte reports an increase in smartphone use in the UK up to 72% of UK consumers (aged 16-64) an increase of 14% within 10 months) while a basic mobile phone represents only 30% of the device ownership (Delloite, 2013). The introduction of smartphones and devices such as tablets make mobility of operation appears as the future element of operations and communication. The adoption of all current gadgets seems to be

outpacing any adoption of standard computers of the past. Tablets took less than two years to reach nearly 40 million in use in the US and outpacing smartphones which took 7 years to reach the same (Comscore, 2012). At the same time it is estimated that tablets will reach 760 million by 2016 rendering an annual growth of 46% while by 2015 will reach the 36% of total PC sales (Forrester Research, 2012; Computer Industry Almanac Inc, 2012).

The need for compatibility with desktop applications and the need of working on the road and remotely have early on set a requirement of having an 'always on' computing facility (Lindgren et al, 2002; Mobile Operators Association, 2006). As the market indicates the role that mobile devices started and will continue to play in the future is getting more and more important and the capitalization on mobile devices further to personal use is also occurring in businesses which are incorporating mobile networking into their operations in order to improve their agility. Even as early as 2006 close to 44% of companies surveyed across different countries, were investing in remote working, while already 64% were using PDA's, 43% Blackberry devices and 34% Smartphones for several functions of their business (Ranger, 2006). Virgin Media Business surveyed 5,000 businesses in 2011, showing that 64% of them are equipping employees for mobile working (Newbusiness.co.uk, 2011). By 2009 in the UK remote workers reached the 3.7 million while the global workforce is set to reach 1.3bn in 2015 (CPNI, 2012; Jones, 2013). It is apparent that the effectiveness of being able to be updated and respond to business on the go makes mobile business application and services a powerful tool and as IDC states it has become a top priority for businesses. (Microstrategy, 2012; Onestopclick, 2011).

Forrester research in 2010 showed that the 49% of small businesses own smartphones (Smallbusinessnewz , 2010).

With 3G technology, mobile networking met a proliferate growth on services which are becoming the 'gold' factor for mobile communications. Combining the increased bandwidth of 3G networks and the processing power and storage ability of the devices, the services and information are growing in volume and importance. Not only are network-based activities that were implemented so far through the Internet and web-based applications finding their equivalents in mobile, but also new services that correspond to the actual nature of mobility are coming up.

One such service that has experienced significant demand is the use of the mobile device as a method for micro-payment. The nature of these payments is varied and has been seen as a significant revenue source whilst offering customer satisfaction (KPMG, 2013). Worldwide mobile payment transaction values are going to surpass $171.5 billion in 2012 and value to average 42% annual growth between 2011 and 2016 (Gartner , 2012). Furthermore services like mobile banking, share trading and a range of other sensitive services are going to becoming a common usage scenario for the mobile subscriber. According to Juniper Research, the worldwide number of users of mobile banking is expected to grow from 590 million users in 2012 to reach over a billion users in 2017 (Juniper Research, 2013). A survey by Federal Reserves (Fed) reports that consumers are using mobile banking up to 60 times per month with a median number of mobile banking transactions of 4-5 times on a typical month (Bankfutura, 2012).

Table 2.1 that follows provides an indication of services that 3G/4G networking made a reality.

Services	Examples of Implementation
Text/Image Messaging	SMS, MMS, Email, Instant messaging, Chat
Networking	Internet access Data Synchronization, File transfer, Intranet access
Video services	TV streaming, Video-on-Demand, Video conferencing
Entertainment	Mobile/Internet Gaming, Gambling, Mobile music, Adult entertainment , Social Media
Infotainment	Information/news alerts, Share-trade information
Location-based services	Navigation, location-based information/ commerce
Financial services	Banking, Share-trade, Electronic currency
Mobile commerce	Micro-payments, Ticketing, Advertising
Business applications	Supply chain management, Customer relationship management, Field-sales management

Table 2.1: Examples of 3G/4G data-centric services

Revenues gained by those kinds of services indicates again that subscribers are keen to adopt the possibilities that mobile networking has to offer, and do that through the ease and convenience of an item that they already use, their mobile phone. From network operators to software companies a large focus and investment is taking place to take advantage of the demands and the opportunities that come with 3G/4G (Visiongain, 2012), with 4G revenues expected to reach over $100bl by 2014 as Juniper Research reports(Juniper Research, 2010). As high bandwidth networks such as 3G, WiMAX, and LTE are being deployed, they contribute to the

growth of mobile data services and revenue as the mobile broadband experience comes close to the home broadband experience (Openet Telecom, 2010).

2.2   Security Issues and Considerations

The features and capabilities currently enabled through 3G mobile devices link to a significant risk in relation to protection of information stored or accessed through them. The transition to the mobile environment poses a reconsideration of security provision and it is imperative that requirements need to be established for the protections of those devices. Given their portability, size and lack of physical barriers of protection or even electronic such as firewalls, they can easily become an easy target for misuse or attack, especially in business. This places a high security concern when these devices are used in the workplace, especially with an estimate of 1.3 billion people working on the move by 2015 (IBM, 2012; Scientificamerican.com, 2012). As such the protection of these devices is a more cumbersome issue for security whilst at the same moment their role in the accessing of business and private information is becoming more dominant. According to Canalys worldwide mobile security forecast there is an estimated average investment growth of 44.2% per year which would translate into a $3 billion market by 2015 (Canalys.com, 2011) Given all the updated use and access of a mobile device it is apparent that is imperative to protect them and their data access in a more efficient way.

2.2.1 Security Risk Posed by Mobile Devices

The nature of 3G services implies the access and transmission of data which may be of far sensitive nature than before. For example enabling financial transactions, such as in the case of mobile banking, micro-payments or m-ticketing imposes the use of personal and financial information. Misuse of such services could be of a great financial loss to the owner of the mobile device. If appropriate security is not provided, an impostor could so much use a mobile handset to download or purchase items, charging at the same time the subscriber's account but furthermore endangers the subscriber in general as the use of personal information utilised to access these services could be used for several malicious purposes.

An increasing amount of evidence is available to suggest that mobile devices are being used to store sensitive information, while at the same time being significantly susceptible to compromise. The concern of personal and private information stored in mobile devices is not to be overlooked. A Motorola survey reveals that 34% of users store sensitive data such as their bank account information or work email passwords on their phones, while a quarter of them would prefer to share a toothbrush than share their phone (Forbes, 2012). Jupiter networks' survey reports that 76% of global respondents report they use mobile devices to access sensitive data, such as online banking or personal medical information whereas 89% use their personal device to access critical work information (Jupiter Networks, 2012).

Furthermore, as the use of mobile devices in business increases so does corporate information leakage and financial loss (DarkReading.com, 2012). A Checkpoint survey across IT professionals shows that 47% report customer data is stored on

mobile devices and with 71% declaring that the introduction of mobile devices has increased security incidents (CheckPoint, 2012). Symantec reports that UK companies had the greatest increase in the cost of data breach if the incident involved a lost or stolen device (Symantec, 2013). Figure 2.4 shows an example of the type of information that is stored in mobile devices. Although companies are likely to update their policies after a loss of device incident (DarkReading.com, 2012) - even with enforcing stronger security policies within business that does not necessarily enforces the protection of information when the human factor comes in play. 55% of users admit to forwarding work email or documents to their personal email accounts on their phone (Forbes, 2012). With up to 80% of corporate IP stored in the email archive it can be foreseen that the danger of misuse significantly increases compared to access from PC inside a company's network (Mimecast, 2012).
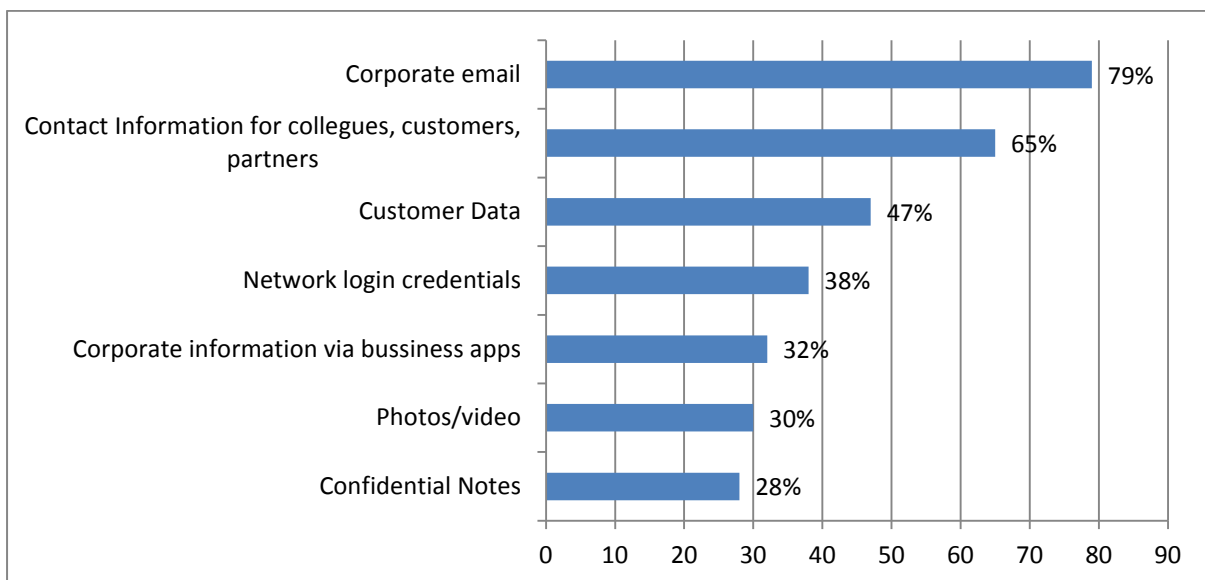
Figure 2.4: Corporate Information Stored on Mobile Devices (Adapted from Checkpoint, 2012)

At the same time incidents that involve mobile devices and the disclosure of personal and corporate information are frequently seen within the news (Clark, 2011; Raywood, 2010; BBC, 2009). A McAfee survey of 1,500 respondents across 14 countries showed that 40% of the organizations say some of their mobile devices have been lost or stolen, half of which contained business-critical information (DarkReading.com, 2011). Data from Transport of London report that more than 15000 mobile phones and 528 laptops were hand-it in as lost in 2013 (Worth, 2013). The issue of theft has been the driving factor behind the Government setting up a National Mobile Phone Crime Unit to specifically target the problem and calling for operators to provide more safeguards on the devices (NMPCU, 2012; Cellan-Jones, 2010). The potential misuse of a device is not necessarily restricted to malicious indent but also to human curiosity. A Symantec- sponsored experiment that purposely abandoned 50 specially set-up smartphones in different public places showed that in 89% of the cases the finders tried to access what appeared to be personal data on the devices (Leyden, 2012).

The concept of Bring your own device (BYOD), poses further risk to business and information. Gartner group predicts that by 2017 half of the companies would require employees to supply their own device for work purposes (Gartner, 2013). With access to corporate information and storage of them on a mobile device that a user may carry around all the time and treating them as their personal device rather than a business tool (which may have been of more restricted use), the risk significantly increases. A survey of 1075 UK employees by TNS Omnibus for Sophos shows that 30% believe their companies lack appropriate security policies and 50% are

concerned that personal information would be at risk in the event of device loss (ComputerWeekly.com, 2011).

Based on the extent of the information and services available on these devices the security threats have now growing on mobile platforms making mobile devices a top concern. It could be said that given the scale of penetration of mobile devices the target of misuse will be shifted to the mobile environment (Juniper Networks, 2013). Exploitation of a mobile device can now mean compromise of both business and personal data making them an attractive target for crime. Given that mobile platforms have not been designed in principle with comprehensive security it further makes it an 'interesting' target for attackers and malware with mobile exploits having significantly increased over the last few years (IBM, 2011). As stated in IBM report the most frequently seen mobile device security threats are (IBM, 2011):

- ➢ Loss and theft
- ➢ Malware
- ➢ Spam
- ➢ Phishing
- ➢ Bluetooth and Wi-Fi

Such evidence collectively demonstrates that devices are now being used to store sensitive information, and that large numbers of them are vulnerable to both accidental and deliberate threats. With the ability to access and store a wide variety of more sensitive information (such as extensive contact lists, diaries, email, corporate information mobile banking and location based services), the need to ensure this information is not misused or abused is imperative. Whereas the theft or

loss of a device might previously have been the principal risk associated with mobile devices, unauthorised access to a device that utilises these information services will potentially result in the disclosure of a greater amount of personal information, endangering a wider variety of aspects in the user's life (which could range from personal identity theft to serious corporate loss and increasingly liability). With this in mind, it is relevant to consider the degree to which related security measures are already provided and utilised.

2.2.2 Security Safeguards on Mobile Devices

A number of safeguards like encryption can be applied on a mobile device. However one of the important requirements in securing devices is sufficiently establishing user identity. Since encryption is intertwined with authentication, the mechanism would not be sufficient if the identity is not efficiently verified. IBM suggested a framework of issues that needs to be addressed regarding the security of a device in a business environment. One of the 5 areas is *identity and access* in which the need strong user authentication and possibly the use of two-factor authentication is underlined whilst also noting that in critical resources re-authentication may also be required, showing that there needs to be also a differentiation between critical and non-critical access (IBM, 2012)

Even with the introduction of encryption such as in Apple iPhone, Fraunhofer Institute Secure Information Technology (Fraunhofer SIT) researchers revealed that it was a trivial task for an attacker using well-known exploits, scripts, and tools to jailbreak and decrypt passwords from the iPhone keychain, including passwords used for personal and corporate email, Wi-Fi, and VPN; even if for devices that were

protected by a screen locking mechanisms or was password enabled (Jupiter Networks, 2012; Ricker, 2011).

2.3 User Authentication - Biometrics

It is widely recognised that authentication can be achieved by utilising one or more of three fundamental approaches: something the user *knows* (password); something the user *has* (token) and something the user *is* (biometric) (Nanavati et al., 2002). The downside of the first approach has already been highlighted, with the use of PINs found to be somewhat lacking in practice. With one of the biggest concerns for example on mobile security to be phishing of passwords regardless the strength of the password/pincode, the risk still remains high (MobiThinking, n.d.; IBM, 2012). Even though PINs are the default mechanism 55% of consumers do not use a PIN to lock their phones (Siciliano, 2011). As Microtrend survey reports 61% of respondents that use a smartphone device even only for work do not use any password protection on their device (Microtrend, 2013)

Similarly to secret knowledge techniques, token based approaches fundamentally rely upon the user to remember something to ensure security, with the token needing to be physically present in order to access the device. However, it is considered that this does not lend itself particularly well to the mobile device context either. The most likely scenario is that users would simply leave the token within the mobile handset for convenience. Indeed, this is the case with the Subscriber Identity Module (SIM) in mobile handsets, which already exists as a token and could be physically removed from a phone when not in use. Users typically do not do this because it is inconvenient, and increases the risk of losing or damaging the SIM card. Nearly 60%

of respondents in a survey state that they would wish to have an easier form of authentication on their devices while 44% do not use the PIN because they find it too cumbersome (Confidenttechnologies, 2011). In contrast to the other methods, the third approach to authentication does not rely upon the user to remember anything – it just requires them to be themselves. Such techniques are collectively known as biometrics, and it is here that the most suitable alternatives for going beyond the PIN may be found.

Biometrics have an advantage over the other two authentication techniques in that authentication is based on unique traits of a person and thus closely links the authentication credentials to the legitimate user, as these cannot be lost, forgotten or shared. As such, in contrast to passwords and tokens, the system does not authenticate the possession of specific knowledge or a token but the presence of the actual person, as it requires extracting their personal identifiers.

The market for mobile phone biometric security products and services are seen to grow and are estimated to generate over $161 million revenue by 2015. A number of mobile devices such as laptops as well as smartphones are equipped with biometric solutions looking towards a more robust authentication solution. From traditional use of fingerprint sensors to more solutions that follow the current use of the device like Apple's patent of swipe unlock with fingerprint recognition (Swider, 2012). Given that fingerprints sensors result in an extra cost on the device, it can be said that there is a move towards more cost effective solutions for deployment of biometric approaches. Other techniques like face recognition or gait recognition are being deployed looking

to utilise either the deployed hardware of the device or the mobile nature of it (Mazo, 2012; Fraud for Thought, 2013; Mims, 2010).

A number of biometrics have the potential to be applied in a mobile handset. Some can leverage the hardware available by default, whereas others require more specific hardware in order to operate. Regardless of the implementation, many of these techniques carry the potential to enhance authentication in a mobile context and do so in a transparent fashion. These following sub-sections provide a fundamental understanding that under-pin biometric authentication, followed by a description of the biometrics that can be applied on a mobile handset.

2.3.1 Characteristics of a Biometric System

As defined by the ISO standard ISO/IEC JTC 1/SC 37, biometrics is the "Automated recognition of individuals based on their behavioural and biological characteristics" (ISO/IEC JTC 1/SC 37 N 3068). Biometrics can be used in two distinct modes: *identification* to determine identity and *verification* to verify a claimed identity.

- *Identification*: In this mode the biometric system reads a sample from the user and tries to find a match by looking at the entire database of registered users. A 1:N comparison is performed and thus is often more demanding in terms of distinctiveness of the biometric characteristics. Identification is commonly used when the goal is to identify criminals, where the subject must be traced from the system without necessarily providing an explicit sample (e.g. airport surveillance).

- *Verification*: In this mode the system tries to verify a claimed identity. The user provides a sample and an identity (e.g. a username). The system retrieves the template that it keeps relative to the claimed identity and checks whether the newly acquired sample matches that template. This is a 1:1 comparison and is in general a much easier procedure to implement as it can be less demanding in both processing and distinctiveness of the features (in order to achieve satisfactory results). Common applications of verification include logical access control. It is this mode of operation this research is primarily focused upon.

2.3.2   A Typical Biometric System

Regardless of the biometric technique or the comparison mode utilised, the way in which the biometric process takes place is identical. A generic example of a biometric system is illustrated in Figure 2.5, where the two key functions of the biometric authentication process are shown - *enrolment* and *authentication*.
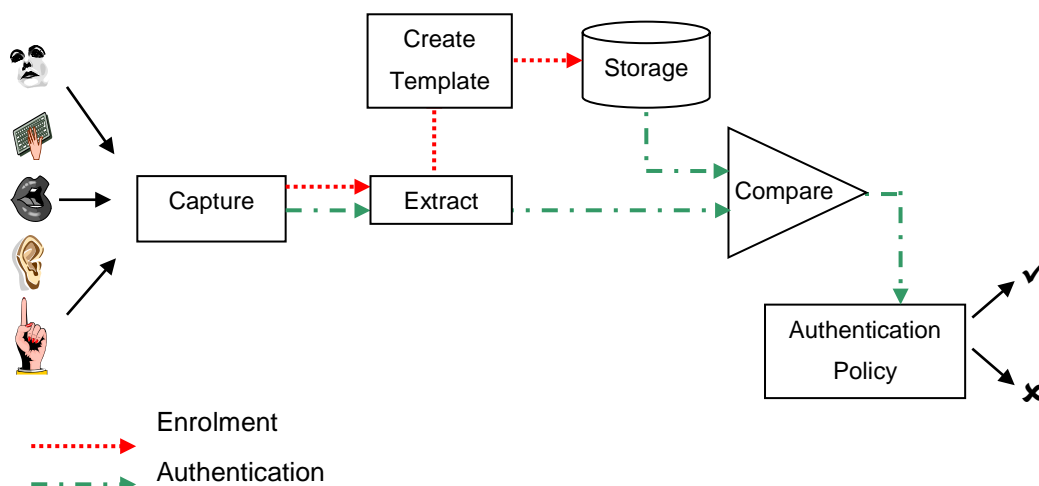
Figure 2.5: A Generic Biometric System

Enrolment represents the procedure where the user provides the biometric information to the system for it to store and generate a reference profile for subsequent authentication. The biometric sample is captured by an appropriate sensor and the reference template is generated through the extraction of features that the system requires to use for authentication (Woodward *et al*, 2003). The reference template is then stored to the template database for it to be used as appropriate.

Authentication represents the process that takes place when a user requests access to the system. At that time, an identification or verification of his identity must take place in order to be established as a legitimate user. A new sample is acquired from the sensor, which is subsequently compared to the reference template. The result of this comparison goes through the authentication policy of the system which determines whether the sample and template are matched closely enough to recognise the user as legitimate. The result of this comparison is unlikely to be a 100% match, as it operates as a function of similarity. Due to the sensor and the user's interaction with it, each time a new sample is acquired it is never exactly the same with any previous samples. Therefore the system relies upon the degree of similarity between two samples. This operational characteristic leads to a number of errors that determine the performance of a biometric system.

2.3.3 Biometric Performance

Biometrics do not operate like passwords, where the correct input of the secret knowledge can assure access to the system with a 100% accuracy. With biometrics a legitimate user might provide a sample, but several factors may still cause them to

be rejected by the system. These factors might be environmental (e.g. a bad acquisition from a fingerprint sensor due to a cut finger; inadequate lighting for face recognition; or too much background noise for voice verification) or related to the underlying uniqueness of the characteristics involved. This might not only lead to rejecting an authorised user but also in accepting an impostor. As the function is based upon the similarity of two samples, the techniques that are based on less distinctive features exhibit a higher probability of an impostor matching the features of a legitimate user and thereby being falsely accepted.

Two basic error rates are commonly used in biometric authentication as performance metrics (Nanavati *et al*, 2002):

- *False Acceptance Rate* (FAR), which represents the probability of an impostor getting accepted by the system (sometimes referred to as the *Impostor Pass Rate*);

- *False Rejection Rate* (FRR), which represents the probability of falsely rejecting an authorised user (sometimes referred to as the *False Alarm Rate*).

A *threshold* setting is attributed to the system, which defines the level of similarity that is acceptable. The threshold value is chosen in order to define what level of FAR and FRR are tolerable for the overall system. In general defining this threshold is a non-trivial task, as the setting will affect both the security and the usability of the system. For example, while a tight setting will result in a lower FAR (and therefore

improve security), it will also risk increasing the FRR, thus impeding usability. This relationship is illustrated in Figure 2.6.
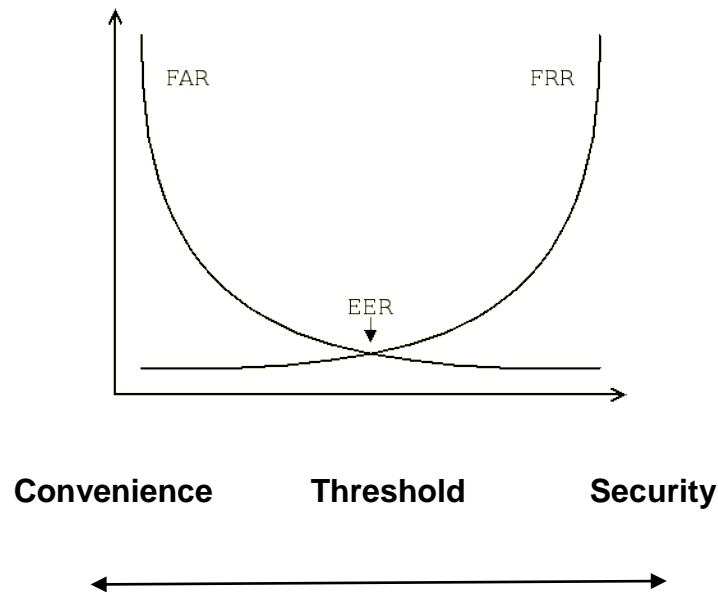
Figure 2.6: Biometric Performance Rates

Ideally these two errors would have a very low value approaching zero at the threshold value. However, the two errors share a mutually exclusive relationship and as such are rarely both at zero (Cope, 1990). The point at which FAR and FRR converge is called the Equal Error Rate (EER), which offers a common reference between biometric systems in order to compare them (Ashbourn, 2000). Although FAR and FRR provide an idea of the accuracy of the system, when looking into the performance of different biometric systems, the EER provides a means of comparison as the FAR and FRR are influenced upon different factors that derive from setting the security of the system. As such EER is a more representative comparison metric for the average performance.

In addition, there are other error rates usually utilised within biometric systems for evaluation:

- *Failure to enrol rate (FTE)*, which refers to situation where the sample is not able to provide enough information to create a template. That can be due to noise from the capture or a lack of features from the user, for example burned fingers.

- *Failure to acquire rate (FTA)*, which refers to the situation where the system is unable to acquire a sample from the user

Although FAR and FRR are the common error metrics, different vendors, evaluation tests and academic research use alternative means to represent performance. For example in some cases the two principal rates are referred to under the names of *Failure Match Rate* (FMR) and *False Non-Match Rate* (FNMR), which represent the errors that derive solely by the comparison between the reference template versus the newly acquired sample. In such cases, what FAR and FRR represent is a combination of the FMR and FNMR and failure to acquire rate (some might include the failure to enrol rate in the equation for the FRR rate) - showing the performance of the whole system for one attempt, as shown in functions 1 and 2 (Mansfield et al, 2001; NSTC, 2006).

(1) FAR(τ) = (1- FTA) FMR(τ)

(2) FRR(τ) = (1- FTA) FNMR(τ) + FTA

, where τ is the threshold value

Given the different interpretations that are possible, attention must be given to reported algorithms or vendor claims to ensure the correct comparison between performance rates is made. Although independent parties, such as the International Biometrics Group, provide evaluation tests in an independent and standardised fashion (enabling the opportunity to directly compare different biometrics under the same experimental circumstances), these are not always the figures reported in marketing contexts. It must also be recognised that performance claims are typically generated from controlled experiments, within confined environments and restricted conditions. Therefore a real-world application is very likely to see a drop in performance.

2.3.4 Biometrics Techniques

Generically biometrics are categorised in two types: *physiological* and *behavioural* (Nanavati *et al*, 2002). Physiological approaches perform authentication based on a physical attribute of a person, such as their fingerprint or their face. By contrast, behavioural biometrics utilise distinct features in the behaviour of the user to perform the relevant classification, such as their voice or their signature.

Physiological biometrics tend to be more trustworthy approaches, as the physical features are likely to stay more constant over time and under different conditions, and tend to be more distinct within a large population (Woodward *et al*, 2003). For

this reason physiological approaches are often used in identification-based systems, whereas behavioural characteristics (which tend not to have such unique characteristics and vary more with time) are therefore mainly used for verification purposes.

An overview of a number of biometric approaches, and an insight into their key functionality and features, is provided the in the following sections.

2.3.4.1 Physiological Biometrics

2.3.4.1.1 Fingerprints

This technique bases its operation on the unique ridge configuration appearing on the finger, which remains unchangeable throughout the person's life (unless injury occurs). Most of the fingerprint systems available base their operation in identifying discontinuities and irregularities - called minutiae - which characterise the ridges and valleys existing in fingerprints (Nanavati *et al*, 2002). Although there are different types of minutiae, the most commonly used is the point where the ridges end and where bifurcations exist (Nanavati *et al*, 2002; Yun, 2003). The Federal Bureau of Investigation (FBI) suggests that there cannot be more than 8 common 'minutiae' between two people (Ruggles, 2002).
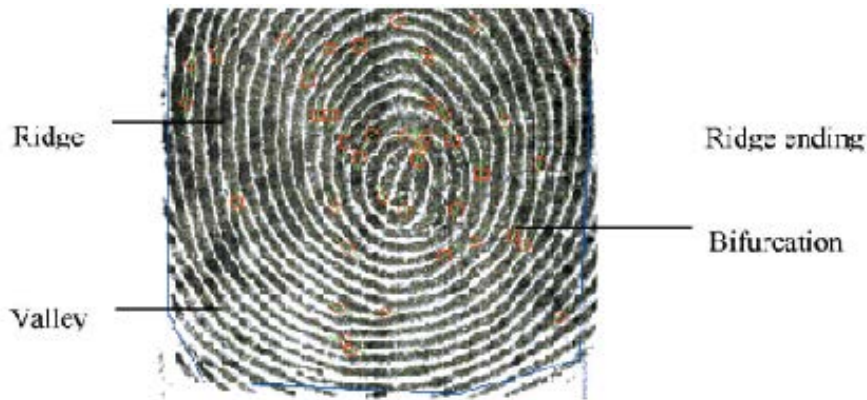
Figure 2.7: Fingerprint Image & Distinct Features (Yun, 2003)

Further from minutiae, there also other techniques that have been adapted to match fingerprint samples. Maltoni *et al* (2003) classify the different techniques as follows:

1. Correlation-based, where two digital fingerprint image samples are compared pixel to pixel given different alignments (i.e. rotation) in order to conclude to a result.

2. Minutiae-based, which compares the common minutiae points between the two fingerprint samples

3. Ridge feature-based, where features in the ridge pattern other than minutiae are utilised such as ridge shape, orientation and frequency etc. This technique is particularly useful in low-quality samples where the minutiae extraction is not sufficient.

Fingerprint images can be categorised as offline and live-scan depending on the way that the sample is acquired. Offline scan is the technique usually performed in forensic applications, where the fingerprint must be collected from a foreign surface.

Live-scan is what is commonly used in automated systems today to perform verification or identification of a person, where the subject must present their fingerprint to a sensor and a live sample is collected. To perform live-scan a number of sensor technologies are utilised (optical, solid-state, ultrasound etc.), each of which varies in quality of acquisition as well as in cost.

There are two ways for a person to present the fingerprint to the sensor. The commonly used approach is to simply apply the fingerprint on the sensing area. Nevertheless this not only creates dirt on the sensor (which gradually leads to badly acquired images), but also requires an extended sensing area to cover the whole fingerprint. As such another technique is for the user to swipe the finger on a smaller area and the image is subsequently recreated from the sliced instances of the fingerprint. This approach requires a far smaller sensor (thus reducing cost) and also keeps the sensor cleaner and raises the performance requirements. On the one hand the system must have had enough throughput in order to be able to capture subsequent images from the sensor, as the reconstruction of the image can be time and computationally demanding (Maltoni *et al.*, 2003).

Generally, the main problem with fingerprint systems is the acquisition of appropriate images to create templates. There a number of factors that play a role in acquiring a good clear sample, such as environmental conditions that might affect the surface of the fingertip (making the image of the fingerprint appearing to fade out). The positioning on the sensor and the finger, and the pressure applied might lead to a poor representation of the distinctive characteristics (Nanavati *et al*, 2003). To counteract this problem raw images are stored as templates (Maltoni *et al*, 2003).

2.3.4.1.2 Facial Recognition

The facial structure of a person provides enough information to recognise one individual from another. The most common approach captures the face and extracts its geometry, looking specifically for the distance between key features such as the points of the eyes, of the side of mouth and the nose (Ashbourne, 2002; Yun, 2003). This is one of the main face recognition techniques – called feature-based, which can be very tolerant in positioning variations. However the automatic tracking of the distinct points is not efficient enough to offer results of high accuracy (Yun, 2003). More recent techniques seek to analyse the face as a whole (Chellappa et al, 1994). Typical approaches of this are Eigenface images and elastic matching, examples of which are illustrated in Figure 2.8 (a) and (b) respectively. Holistic approaches like these can offer higher performance, as they consider all available information rather than simply the distinct points (Yun, 2003). However, these techniques have poor tolerance to posing variations and require a more extensive amount of training data (Chepalla et al, 1994).
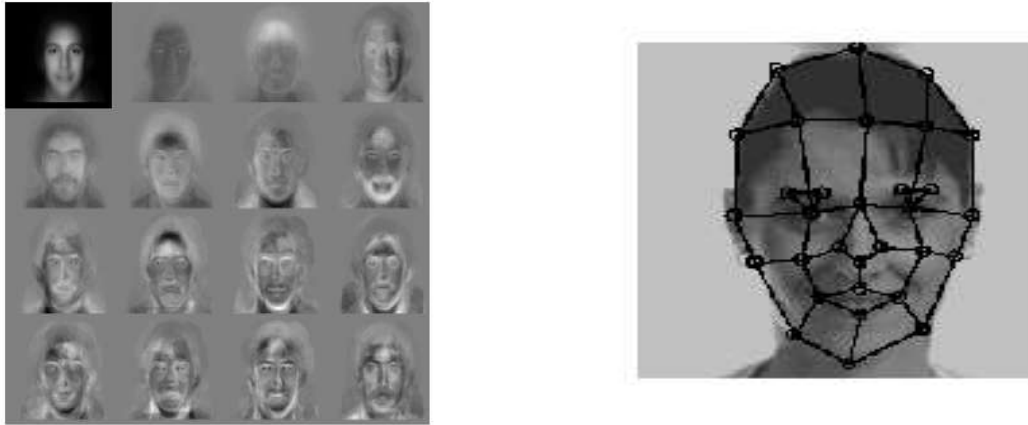
(a) Eigenface   (b) Elastic Matching

Figure 2.8: Face Recognition Techniques (Yun, 2003)

Although face recognition has a good level of accuracy, each approach varies in performance relative to the others depending upon a range of factors such as lighting conditions or the angle of capture (Ashbourne, 2002; Zhang *et al.*, 1997). This complicates its application in a mobile environment where varying conditions are likely to occur (e.g. the level of illumination is likely to change considerably throughout the day). Furthermore the potential of applying this technique in a transparent fashion introduces further complications, as it would be necessary to capture images of the user without them having explicit knowledge. That would result in images being captured in uncontrolled positions, with the user potentially looking in many different directions. Research with promising results in the application of the fashion has been done by utilising different orientation samples to create the biometric profile so that better tolerance can be achieved (Clarke et al, 2008). With the current application of facial recognition for security purposes as e.g. in airports it

is envisaged that more noise tolerant algorithms would be developed that would in the future better support its deployment in other areas such as the proposed one.

2.3.4.1.3 Iris Scanning

The iris of each individual records a complex pattern in the coloured area of the lens which is unique and also remains stable throughout the life of the person (Daugman, 2004). It has been identified that this pattern not only varies between two persons but is distinct for the left and right eye of the same individual, making the technique distinctive and highly reliable. As such it has been used for a number of applications, such as airport security, border control and hospital access.
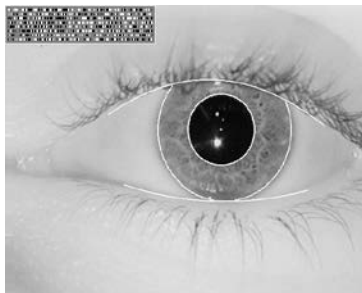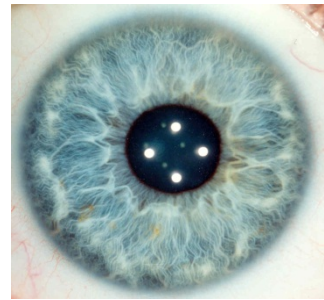
    (a) Iris Area   (b) Iris pattern

Figure 2.9: Example of an Iris (Yun, 2003)

Despite the uniqueness of the features and the high tolerance, the accuracy of the technique relies on the ability to capture those features (Ashbourne, 2002). For that reason, technology plays an important role and specialised capturing sensors are required to capture the iris image. Due to sensitivities in the camera, stillness of the iris and distance from the capturing device are important factors to consider in the design of a system. For example, often a person must stand at least 10-12 inches

from the sensor in order to acquire a good sample, which makes the technique quite intrusive to the user (Ruggles, 2002). Within a mobile context, these requirements would make transparency difficult to achieve.

2.3.4.1.4 Ear Geometry

The human ear has been recently proposed as a basis for a biometric, with a number of research studies suggesting it has adequate distinctive characteristics in order to differentiate between people (Victor et al., 2002; Burge & Burger. 1998). However, the level of distinctiveness that the ear exhibits has yet to be fully established. The application of ear geometry to date has not yet been commercialised, but the distinctiveness of the ear has been utilised in a number of criminal cases (with earmarks are being used as evidence), suggesting the approach has promise (Lammi, 2004).

There are three techniques used for ear identification: photo comparison of the ear, earmarks and thermograph photos. Of these, earmarks are a technique used for crime investigations rather than for general biometric verification. Examples of the other two techniques are illustrated in Figure 2.10. Although the whole ear structure and shape is utilised, as it carries a range of complicated structure features, a special interest is focused on the outer ear and lobe.

(a) Ear features and distances utilised in photo comparison analysis

(b) Thermograph photo utilising colour and textures to identify distinct parts of the ear
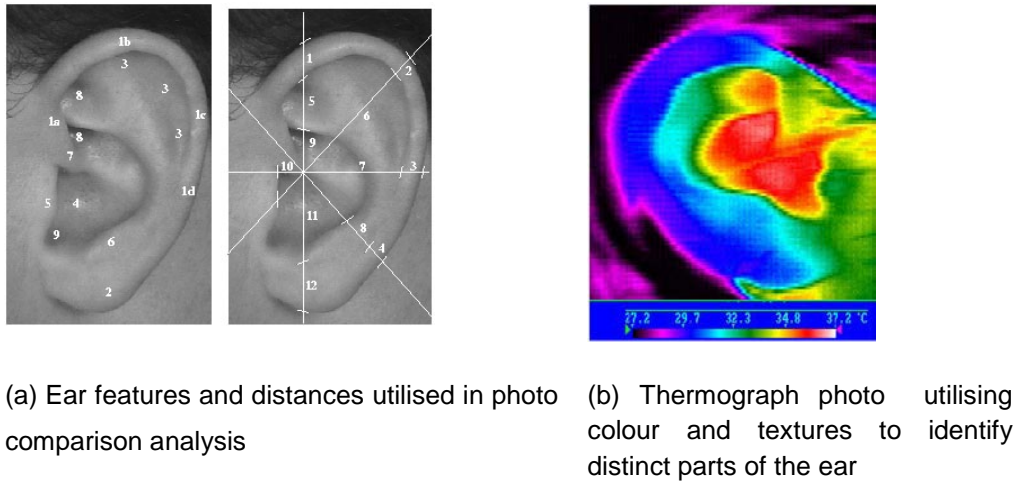
Figure 2.10: Examples of Ear Geometry Techniques (Lammi, 2004)

Ear recognition is often compared to face recognition, as they both constitute appearance-based biometrics. As such some techniques used in face recognition such as Eigenfaces have been also utilised in ear recognition for image analysis. Even though face recognition is a well-established biometric there has been cases where ear recognition has matched its performance, under identical conditions and variations in lighting, posing, etc. (Chang *et al*, 2003).

Ear recognition could be a future solution for application in a mobile device in a similar fashion to face recognition. Nevertheless, the application of the technique in a transparent fashion could be problematic as it requires the ability to acquire adequate full images of the ear (which would not be possible from the natural position when the handset is in use).

2.3.4.1.5 Gait Recognition

Gait recognition is a relatively new method for biometric authentication; looking to identify a person by the way they walk. Even though its biometric application is relatively new, the distinctive nature of a person's gait has been proposed back in

the mid-1960s by psychologists (Murray, 1967). Its application is mainly based on analysing video sequences to identify distinct movements of the person's main body parts (i.e. feet, hands, and angles between the body parts). Based on its operation it has a major advantage of being able to perform identification from a distance. However, in order to be utilised in a mobile handset as a standalone method the device would require a number of additional sensors, such as accelerometers. This kind of application has already taken place using a sensor device attached in a mobile phone which can identify walking characteristics to enable identity verification (Young, 2005).

2.3.4.2 Behavioural Biometrics

Behavioural biometrics have traditionally been less popular than their physiological counterparts as they have suffered from lower performance rates. This has started to change, and techniques such as voice verification are becoming increasingly popular to be used in commercial solutions making it also highly popular in consumer satisfaction (King, 2013). Given the underlying characteristics tend to change more frequently, careful consideration needs to be given to their design and implementation so that there is provision for profile template and retraining.

2.3.4.2.1 Keystroke Analysis

This technique discriminates between users based on their typing characteristics. In recognising users based on typing, two of the characteristics that have demonstrated to provide the most discriminative information are (Furnel et al, 2008):

- *inter-key latency*, which is the interval between two successive keystrokes (at press or at release), *and*

- *hold-time*, which is the interval between the pressing and release of a single key

Figure 2.11: Keystroke Analysis Characteristics

Other characteristics have also been investigated, but have not proved to present significantly more discriminative information for the additional complexity they add to the system. To date, research has demonstrated a successful performance of the technique when applied to regular keyboards. The approach itself can be applied in two modes: static (text-dependent) or dynamic (text-independent). In the static approach, a user is verified against a known text string, allowing a profile to be built for the specific key presses (e.g. combining keystroke analysis with the input of usernames and passwords). By contrast, the dynamic approach permits a user to enter "free-text" and therefore requires a more general profile of keystroke activity. The resulting characteristics are therefore likely to be more variable than their static counterparts.

In general, the technique does not share the distinctiveness of other approaches, resulting in higher error rates. Nevertheless, the fact that it can be applied in conjunction with normal user activity means that the dynamic mode could be a useful basis for transparent authentication. However, research to date has not reached the performance results of the static application of the technique (Leggett *et al.*, 1991; Napier *et al.*, 1995). Nonetheless, studies conducted have concluded with promising results for the application of the technique in a mobile context (Clarke & Furnell, 2006; Karatzouni & Clarke, 2007).

2.3.4.2.2 Voice Verification

This method tries to identify a person from the way they talk. It was one of the early biometric applications commercially available and in general is considered a good potential for many telephony based systems (Ashbourn, 2002). Voice scanning looks to extract discriminative information by examining the dynamics of an individual's speech. The technique does not rely only on the sound of a word or phrase that someone could closely replicate, but it takes under consideration the overall dynamics, which cannot be rendered by mimicking the voice of the legitimate user. There are three ways that voice verification can be performed:

- Text–dependent : The user must repeat a specific pass-phrase.

- Text–prompt : The user is given a new challenge phrase each time to repeat.

- Text–independent : The user can be authenticated regardless of what they are saying.

The first two approaches have been extensively researched and also applied in real world applications as a means of verification. Static verification techniques are much

easier to perform, as the distinct dynamics of the voice can be recorded during enrolment and the repeated pass-phrase is identical each time to the original enrolment. A text-independent approach would have to operate in a dynamic manner, to identify the voice characteristics without a static reference. This is a complicated task as it is difficult to identify the common discriminative features between two samples and puts a significant burden on both the feature extraction and classification algorithms. Although efforts have taken place towards this direction, the technique has still not yielded satisfactory results and lacks any commercial exploitation.

A further downside of this approach is that the quality of sound required for the samples will be unlikely to have the same quality as the reference template which was acquired in a controlled environment (Nanavati *et al., 2002*). The noise that might be captured during the authentication process can significantly affect performance. Especially for remote applications where the voice signal might differ significantly due to outside noise. The application on a mobile environment would be even more problematic, where the practical conditions of use could impose much more interference. Nevertheless, voice verification is considered to be an approach that would be desirable for mobile devices. Moreover the evolution of the technique to operate in a text-independent fashion would enable transparent authentication (e.g. in telephony contexts).

2.3.4.2.3 Signature Recognition

Signature recognition in its non-automated form has been used for thousands of years as people have been signing their name in order to attach their identity to an

object or an action. The method tries to differentiate between users by examining the way in which they sign. The biometric can be realised in a static mode (by comparing the final appearance of the sample against the template), or in a dynamic manner (where the overall dynamics of the user's handwriting, such as pressure, speed, direction and the number of strokes are analysed rather than just the final result) (Ashbourn, 2002; Gupta & McCabe, 1997). The latter approach provides a far stronger and more robust approach, as impostors cannot simply replicate a signature but must replicate the action of making it. As such, most current systems utilise the dynamic implementation of the technique.

2.3.4.2.4 Service Utilization

Service utilization has been a more recent suggestion as a biometric, looking to identify patterns of usage based on specific interactions with applications or services (Furnell *et al.*, 2001). An example of such an approach in a PC environment would be the monitoring of the usage of applications with metrics such as frequency and duration of access. Unfortunately this would involve a large volume of data to process and classify, with the variance also quite high. Nevertheless, prior research has demonstrated sufficient discriminative information to utilise the technique to monitor interactions (Moreau and Vandewalle, 1997). Similar applications have also been used in domains such as fraud detection (Rawlings, 1997).

2.3.5 Comparison of Biometrics

It is often difficult to directly compare different biometric approaches. However, as previously indicated, the EER is often used as a primary indicator. On this basis,

Table 2-1 illustrates the performance of the different approaches based on results from numerous research studies and independent sources.

Biometric Approach	Equal Error Rate (%)
Facial Recognition	2.5, 7 (Mansfield *et al*, 2001)
Voice Verification	3.5 (Mansfield *et al*, 2001)
Fingerprint Recognition	4.5, 6, 9 (Mansfield *et al*, 2001)
Signature Verification	1.19 (Mohankrishnan, 1999), 2.84 (Yeung et al, 2004)
Iris Recognition	0.2 , 3.2 (IBG, 2005)
Keystroke Analysis	1.3 (Obaidat & Sadoun, 1997), 8 (Clarke & Furnell, 2006), 12.2 (Karatzouni & Clarke, 2007)

Table 2-1: Performance of Various Biometrics

Apart from the accuracy or performance of a biometric there are other things to consider when deploying a biometric system. For example, factors such as cost and user friendliness could impose major limitations on the system. The International Biometrics Group (IBG) has identified four factors to consider when choosing a biometric system: *Intrusiveness*, *Distinctiveness*, *Cost* and *Effort* (IBG, 2006). The evaluation of those factors in relation to the biometric approaches is illustrated in the Zephyr Analysis graph by IBG, as seen in Figure 2.12.
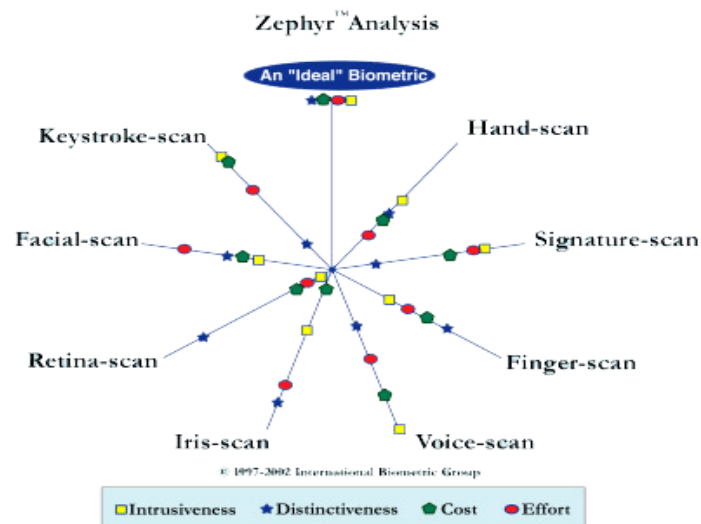
Figure 2.12: Zephyr Analysis of Biometrics

- *Intrusiveness* refers to the involvement of the user in the authentication procedure, in terms of when and in what way they are required to authenticate themselves. For example, a biometric system that requires from the user to interrupt his activity, or demands the authentication procedure to be done under specific conditions, has a high level of intrusiveness.

- *Distinctiveness* of a biometric is the ability of the technique to successfully discriminate between different users, which is in turn related to the uniqueness of the features that each biometric utilises.

- *Cost* is the financial implications that the deployment of a biometric will incur.

- *Effort* refers to the ease that the use of the biometric, including both the procedures of enrolment and verification.

2.3.6 Identifying Appropriate Biometrics

As the prior discussion has identified, various biometric techniques could theoretically be applied to mobile handsets. However, from a practical perspective there are a number of issues to consider. As previously discussed there are issues of usability and cost associated with the selection of a biometric technique. For example, the application of iris scanning in a mobile environment is certainly more problematic if someone considers the sensitivity of the technique and the positional requirements that it imposes, rather than (for example) applying facial recognition as the detail required is far less extensive than the former. Furthermore iris imposes more extensive hardware requirements, as a far more sensitive camera sensor would be required. Even though any biometric will be affected by the environmental/external conditions caused by the use of a mobile, certain techniques can be considered to be more tolerant.

Table 2-2 illustrates a number of biometrics that have the potential to be utilised in a handset, as well as a number of parameters that are considered important for their application. The first factor is the hardware requirements and the potential cost implication of the technique. The additional integration of specialised biometric hardware would aggravate the already high cost of the mobile handset (e.g. AuthenTec a company that develops fingerprint sensors, needed to reduce prices from $3 to $1 to facilitate large-scale deployment (Blau, 2007)). The second factor - accuracy, representing the performance of each technique - has been attributed based on results announced by the International Biometric Group (IBG, 2005) and

National Physical Laboratory (Mansfield et al., 2001). The non-intrusiveness factor refers to the ability of a technique to acquire the necessary samples without requiring any explicit interaction from the user. This provides the capability of authenticating the user at various times, without adding inconvenience to their regular use of the device.

Biometric technique	Sample acquisition capability as standard?	Accuracy	Non-intrusive?
Ear shape recognition	✘	High	✔
Facial recognition	✔	High	✔
Fingerprint recognition	✘	Very high	✘
Handwriting recognition	✔	Medium	✔
Iris scanning	✘	Very high	✘
Keystroke analysis	✔	Medium	✔
Service utilization	✔	Low	✔
Voice verification	✔	High	✔
Gait verification	✘	Unknown	✔

Table 2-2: Potential biometric techniques for mobile devices

From the table it can be seen that the techniques that share the highest accuracy are at the same time more intrusive to the user. As such there will always be a trade-off and a balance to be sought towards satisfying both sides. Nevertheless, there are a number of techniques that can operate transparently without further hardware requirements by utilising the standard built-in hardware and use the users' normal activity. These are:

- *Voice Verification*: Capture voice samples during a voice call.

- *Face Recognition*: Utilise the front camera of the handset during a video conference call or capture snapshots during other interactions when the user will be expected to be looking at the screen.

- *Signature (handwriting) Recognition*: Capture samples while a user utilises an editor in order for example to keep notes.

- *Keystroke analysis*: Capture samples while a user is typing text messages or writing a document.

- *Service Utilization:* Monitor the interaction of the user with the device based on application use, frequency and timing of use, etc.

Each of these techniques could be potentially used to acquire the authentication samples necessary, without disturbing the user and constitute a monitoring mechanism that can maintain trust in the user's identity continuously throughout the usage of the device.

2.3.6.1 Biometric Fusion

Plenty of research to date has looked in the use of multiple biometric inputs in order to strengthen the decision making process. This approach is generally referred to as biometric fusion and it is believed to offer an improved performance in a biometric system that has the ability to incorporate a number of inputs (Ben-Yacoub et al, 1999; Brunelli & Falavigna, 1995; Bigun et al, 1997; Hong & Jain, A.K; Jain et al, 1999).

The concept of fusion techniques is the use of more than one input and the combination of those to create an output. The inputs could be representing the use of more than one sample from the same biometric – *multi-instance/multi-sample* fusion or the use of samples from different techniques – *multi-modal fusion*. Other approaches like multi-sensor- the use of different acquisition sensors, multi-algorithm – the use of different algorithms for feature extraction and/or matching, are also options (Ross, 2007). Depending on the application and resources available, the use of fusion in an authentication system could provide a more informed decision related to user's identity as it may utilise multiple samples of the same feature or utilise a combination of biometric traits for the system to reach its conclusion. By using multiple traits several challenges are addressed such as spoofing attempts are minimised since it would require the simultaneous forgery of more than one biometric, non-universality is addressed by covering a broader spectrum, noisy data that may characterise specific acquired samples and generally offers a more tolerant error approach (Ross, 2007).

It can be foreseen that the performance of the system regarding both security and usability would so much depend upon the quality of the samples as well as the algorithm used in each biometric, but furthermore to the actual fusion decision algorithm to enable a balance between security and usability. When for example utilising fusion of different biometric techniques that ones have higher performance than others and giving to that techniques a considerable higher weight to the decision it may almost diminish any fusion in essence whilst overlooking the rest of the characteristics. If on the other hand the same weighting is applied across all

inputs that may be on the loss of either security or usability as it would not be taking into account the high FAR that may occur in one case or the good performance if there was more reliance on the better techniques on the other. Similarly when utilising samples of the same technique a similar consideration may exist relevant to using different algorithms of the same technique with different robustness or for example have a reliance on the quality of a sample so less quality samples do not get the same contribution to the decision.

Further to its algorithmic consideration, biometric fusion also poses the consideration for technical compatibility. Its application in a deployable system presupposes the need for a common interface for the use and integration of different techniques. This issue is resolved by standardisation of biometric products and algorithms with standards like BioAPI being more widely used.

Biometric fusion can be applied on several levels of the biometric process: at feature level, at matching level or at decision level (Ross, 2001). Figure 2.13 illustrates the operation of fusion depicting all 3 stages that it can occur.
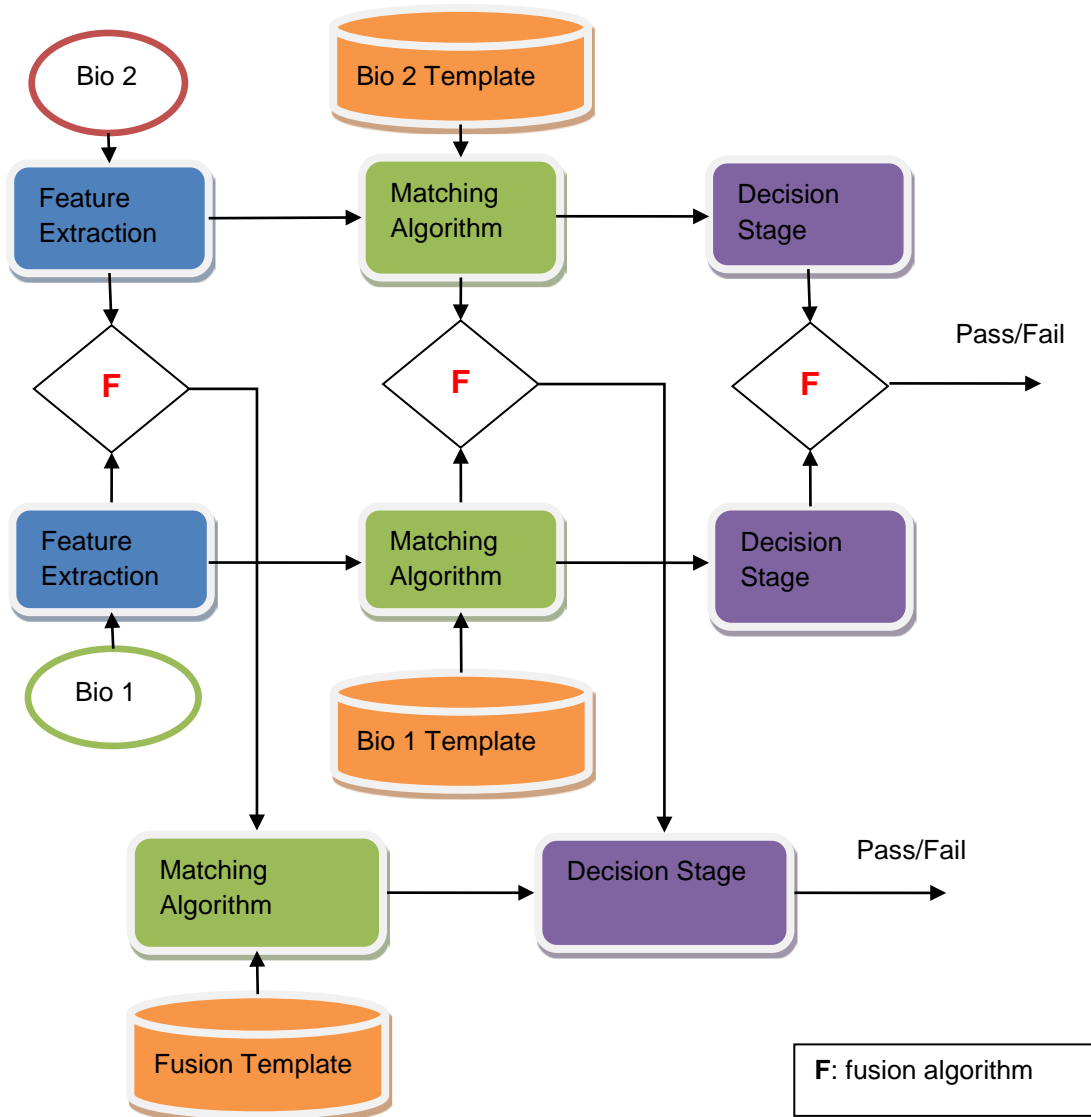
Figure 2.13: Stages for biometric fusion (Adapted from Ross et al (2001)

2.4   Summary

Mobile devices have been identified as a significant risk given the current use and capabilities. Current security provision seems to lack the appropriate robustness to correspond to the respective security requirements. Biometrics have been suggested to be a more secure approach to authentication. In the context of this research seeking to enhance security in a continuous mode, biometric techniques could be

utilised as there are a number of them that lend themselves very well to this concept. The utilisation of these techniques requires a number of considerations in regards to user acceptance, storage of biometric information as well as issues of performance in their operation in a mobile device. The following chapter explores the various issues that derive in the application of such approach including presenting the user's perspectives as well as discussing issues that play a significant role towards an authentication topology of such mechanism.

3 User Authentication on Mobile Devices– Requirements Analysis

This chapter provides an overview of the different requirements that an authentication framework would need to address. Having identified the initial requirement of enhanced authentication and with the focus of this research upon evaluating the effectiveness of biometrics in order to apply transparent and continuous authentication, it was imperative to look at the elements and issues that this approach may introduce or need to be considered. This includes the user's perspective as well as the technical issues that surround the realisation of a biometric based authentication mechanism.

3.1 Establishing the Users' Perspective

In order to establish this research it was imperative to acquire the user's perspective on the security requirements that they have for their mobile devices. That was done though a focus group and the following section presents the basic methodology followed as well as the key results. A detailed description and discussion for this part of this research was published in Karatzouni et al. (2007) (See Appendix B). Pertinent views of the focus group are also presented in Section 3.3 as appropriate in order to provide the views of the users in a discussion on authentication framework topologies.

3.1.1 Focus Group Methodology

To assess views and attitudes regarding the authentication requirements on mobile devices a focus group was conducted, in order to provide a forum for users to express and exchange their perspectives. Whilst an early survey by the research

group had undertaken a quantitative-based study to explore user perceptions (Clarke & Furnell, 2002), it was felt a follow up qualitative study was required to better understand the reasons behind some of the key results.

The focus group aimed to include a mixture of end-users, representatives from the mobile industry, researchers in the area, and representatives from educational technology and university perspectives. It was important to have a multifaceted view on the subject and cover the perspectives of users that were likely to make different use of their device and as such they would have different requirements. Also important was to get the views from the providers' perspective to establish whether they identify an issue on current authentication and how alternative solutions are perceived. A detailed listing of the participants' composition can be found in Table 3-1.

Participant	Background / Basis for inclusion
1	Representative from a UK mobile network operator.
2	Creator of a web resource that tracks mobile technologies and trends
3	Project student, addressing public understanding of biometrics
4	Project student, conducting user trials and evaluation of biometrics
5	Academic, active in the mobile security domain
6	Learning technologist, commencing research into educational uses of mobile devices
7	Psychologist, with research interests in use of mobile technologies
8	Representative from university ICT department, responsible for campus deployment of mobile devices.
9	Academic with interest in human factors of technology.
10	Male mobile phone user
11	Female mobile phone user
12	Female mobile phone user

Table 3-1: Summary of focus group participants

All of the participants were regular end-users of mobile devices, and in many cases conversant with the features and facilities of smartphone devices. As such, they were able to offer perspectives with first-hand knowledge of the more advanced features and facilities that are likely to become the baseline standard in a few years. It is understandable that the time at which the research took place (2007), people were not yet of full adoption of smartphones and their capabilities, at least to the extent that would be expected to be today given penetration of the mobile device.

A number of research questions were created to form the framework of the discussion, addressing the main areas of interest around the objectives of this research on user authentication. A list of the question as well as a brief justification behind them follows.

1. *Do participants recognise a need for security on their current devices?*

   This question aimed to investigate whether users consider their current usage of mobile devices to merit protection, with particular emphasis being given to whether or not user authentication is an important requirement.

2. *How do participants perceive the current authentication facilities, and do they use them?*

   The intention here is to focus participants' attention specifically towards the PIN-based techniques that are dominant upon current devices, exploring opinions about the general nature of the method the extent to which they are used in practice.

3. Do participants envisage a need for greater security provision in the future?

Anticipating that some participants would be unlikely to prioritise a need for authentication based upon their current usage of the device, this question aimed to make them consider the range of emerging and future applications of mobile devices that may involve far more sensitive data. Then they were asked to reassess their views on the requirement for authentication, based on this future scenario.

4. How do participants perceive the potential alternative methods of authentication and the ways in which they could operate?

Assuming that the preceding question would highlight a requirement for further protection, this question aims to elicit opinions about alternative mechanisms (such as token and biometric approaches), and methods of applying them.

The participants were not led towards any particular viewpoints during the discussion of each question. However a discussion guide was formed and followed during the session that would provide the background and the context for the research questions to be answered. The session lasted 100 minutes and was video recorded in order to capture any non-verbal information that could provide further input (i.e. reactions to a certain view) or help to quantitative appraisal of answers (i.e. show of hands as an answer). Transcription of the recorded session followed and analysis of the derived document provided a series of results. Some key results were:

Current Usage & Authentication

- The current usage of their mobile device for the majority of the users was restricted to basic telephony and text messaging although some of them suggested that this is likely to change in the future

- Based on the above point most of the users felt not being at risk as their usage was still limited, and did not involve accessing sensitive information

- Regarding current authentication achieved by the PIN, only 1/3 of them use it at switch on and only one participant used the PIN on standby mode. The rest of the group considered that their use of the phone did not require any protection based on their current usage. However the majority stated concerns for the actual effectiveness and usability of current authentication, noting traditional drawbacks of knowledge-based authentication.

Future Usage & Protection

- Most of the participants agreed that future applications and potential usage of their device would involve access of highly sensitive information and therefore they would see their security requirements altering to correspond to that change and look for enhanced security.

- Another significant point identified by participants as part of this enhanced security is the fact that not all services carry the same risks - something that this report will address later in this chapter. So they would expect to have the

security applied respectively to the risk associated with a specific service or application.

Alternative Authentication

- Looking at the alternatives to knowledge-based authentication – tokens and biometrics, participants were not receptive to the former but highly positive to the adoption of the latter. As previous research had also in the past shown, users are starting to be more open to biometric techniques and consider their use in order to enhance security (Clarke *et al.* 2002).

- In regards to specific biometric techniques, fingerprint was the most popular amongst all, however as one of the participants commented this preference is more likely to derive out of the fact that fingerprint is the most well-known one and therefore users are more familiar with the approach. Interestingly, some suggested the use of biometrics that can be applied based on the use of the device - something that can therefore mitigate any reliance on extra hardware and therefore extra cost of the device as well as extra interaction.

- Another significant outcome based also on the above was also that no single technique can fit the needs of all users and therefore a more flexible approach would be more appropriate.

- Although the matter of privacy of biometrics was commented upon, there was no real concern from the users' perspective in regards to this matter, which

indicates the change in culture towards biometrics as people have been traditionally cautious relatively to this issue. Rather than privacy concern was raised towards the actual usability of the techniques and how well it would work in a mobile context and therefore where it will become a not easy to use security feature.

Going beyond point-of-entry

- The users were asked to provide their views on the application of continuous authentication during the use of the device if this was to be applied in a transparent fashion, in order to provide security at all times and mitigating the users' interaction in comparison to explicit authentication. The views on the matter were mixed. However participants did not appear to be reluctant to the use of such approach, with the only concern focusing again on the usability of the approach.

- A secondary issue was again the issue of privacy but mainly when the participants were asked to comment upon storage of biometric data and who they would perceive to be more appropriate to safeguard that data. Again views were mixed however the majority raised significant concern in regards to the issue of trust to others than themselves. A more detailed discussion specifically on this is provided in Section 3.3.

As this focus group indicated future mobile usage will bring in the foreground the need for more enhanced and flexible authentication. Furthermore even though current usage does not command the need for extra security, current authentication

is perceived to hardly provide any protection in the first place. This focus group provided a significant part of the requirement analysis of this research as the user's perspective is always an important factor when designing security mechanisms.

3.2 Looking at Service Security Requirements

Further from the level of security that can be provided by current authentication, the nature of its implementation also has the disadvantage of only providing authentication at point of entry. Although this could be effective in ensuring initial access to the device, it assumes that all services, applications and information accessible on the device are of equal value, and do not require any further access control restrictions. This was a concern that was also identified during the focus group by the participants. The analysis on the latter issue as well as an example on how security requirements could be attributed on different services is presented in the following sections.

3.2.1 Service Usage & Security Provision

With the increasing functionality of mobile devices the number of services, applications and information accessible to the user is significantly expanding. Basing authentication on point of entry without further control of legitimate access, and without any kind of sensitivity classification for services or data, could create a lack of appropriate protection for access to individual applications and services. For example, arguably the protection required to prevent access to a text message is substantially different to that required to prevent access to a bank account. Figure 3.1 shows a representation of how current authentication schemes deal with

security, keeping a single level of security for all services. Figure 3.2 shows how the threat that derives from each service could add another dimension to the way that the security level is defined. Each service carries a certain risk of misuse and it is believed that this ought to be a factor in deciding the appropriate level of security.
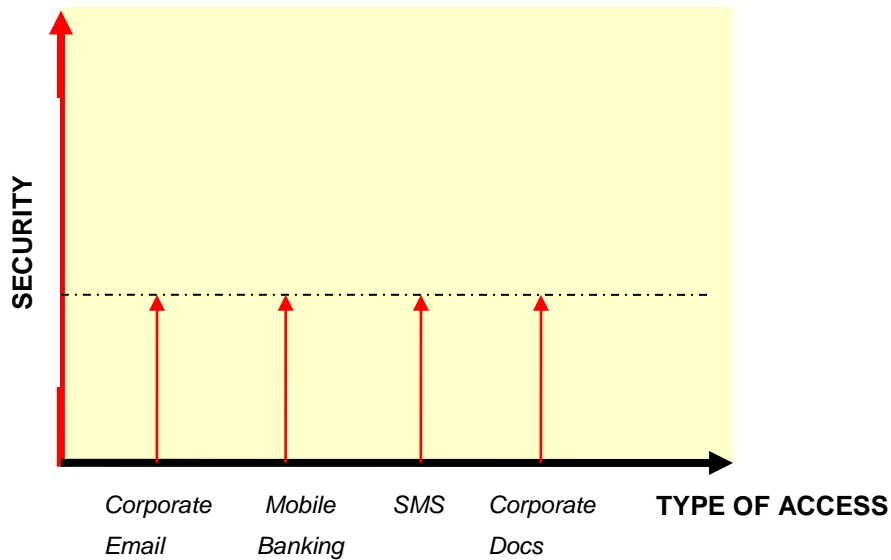
Figure 3.1: Current Security Assessment
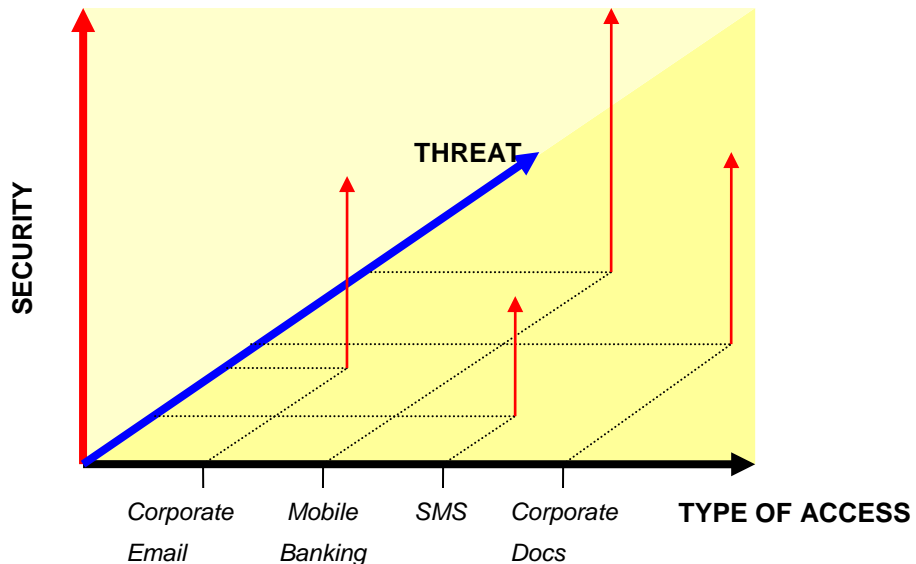
Figure 3.2: Proposed Security Assessment

As such the level of security could be more appropriately assigned to each individual service, so that each service or function can independently require a certain level of authentication and subsequently trust in the user in order for them to get access to the specific service. In this way, more critical operations can be assigned a greater level of security and therefore greater protection, leaving potentially less risky operations to a lower level of trust. It is envisaged that this could provide a balance between the security of highly risk services and usability of less risky ones, without any of the two suffering due to a single security level or mechanism.

Another issue to consider is that the level of security required within an individual service or application is likely to change during the process, as key stages may have a greater risk associated to them than others. In order to carry out a specific task a number of discrete steps are involved, each of which may not carry the same level of sensitivity. Some processes are more critical where others are simply operational steps that assist in the completion of the desired task. A simple example that illustrates this notion is the procedure of accessing what could be an email or an SMS inbox. The user access the inbox and at that instance there is not a real threat involved as the operation cannot lead to any misuse on its own (see Figure 3.3 (a)). Even if the next step is to create a new message and start typing the content, no additional risk exists. The security implications actually start when the user is pressing *'Send'* as it is at that point that the misuse can occur if the user is not the legitimate one. All the previous steps do not involve any kind of threat as no negative effect has taken place in terms of confidentiality, integrity, availability or even financial cost of the data. By contrast, in Figure 3.3 (b), the user again accesses the

inbox, but tries to access the saved messages instead. This time the requirement for greater protection occurs earlier in the process as accessing the saved messages could affect confidentiality by having an impostor reading them. Moreover, if the impostor was subsequently to delete them, the threat level and thus the required security would be even higher, as more factors become engaged, expanding to issues such as integrity and availability. A more complicated example of the above could be seen in mobile banking. Looking at the several steps that need to be taken in order for the service to be completed involves a range of different risks. For instance accessing the service provider in order to make a money transfer, intermediate situations during the process might involve navigating to specific bank pages or other recourses throughout providing personal information until reaching the final transfer.

(a) Sending a Text Message

(b) Reading & Deleting Text Messages
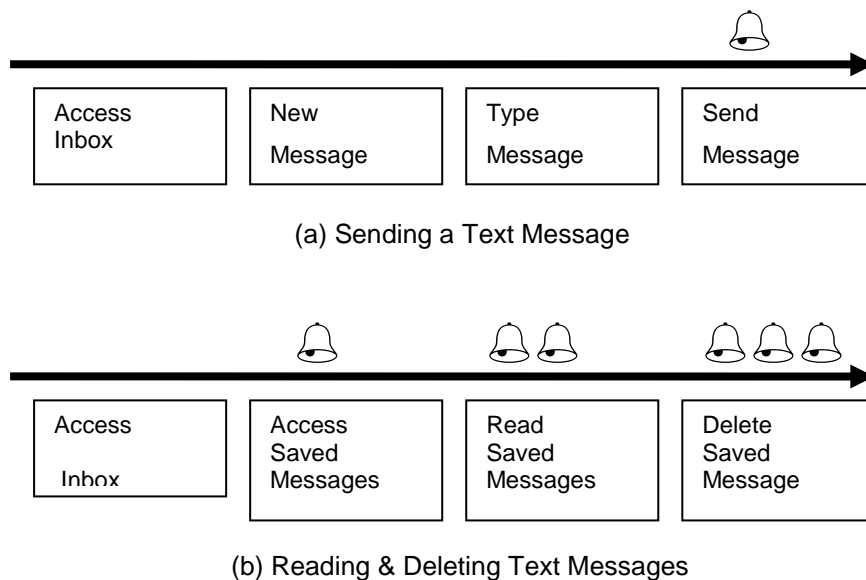
Figure 3.3: Variation of the Security Requirements during Utilisation of a Service

It can be foreseen that each operation has different sensitivities and as such each step of the process changes the threat and therefore the risk level. However, within the context of this thesis only the issue of *inter-process security* is addressed , looking to demonstrate the need for establishing appropriate levels of security for each service and application rather than the device as a whole. *Intra-process security* and therefore establishing security though the duration of a specific service is also another issue to be considered but is not addressed in the context of this research .

3.2.2   Identifying Usage Scenarios

In order to apply individual security levels to applications and services there is a need for threat assessment to classify the security risks associated with them, from both organisational and individual perspectives. From such classification, a security level could be attributed to each type of service and subsequently to the level of trust required in the user.

In order to demonstrate the above concept a number of usage scenarios were identified based upon current and potential future usage of mobile devices at present. Such scenarios can assist in the design of a threat assessment template, examining the security risk that each service encompasses and an associated severity level. In this example a criterion used to classify the different usage scenarios is the way that each service utilises network connectivity. As such the services and functions could be split into those requiring the network, those requiring traditional cellular based services, and those that operate locally on the device. This separation also assists in understanding what forms of authentication can be

subsequently applied; device-centric or network centric techniques. Table 3-2 presents a listing of typical services and functions that can be accessed via a mobile device.

Cellular	Non-Network	Network
Voice Call	Contacts	E-mail
SMS	Calendar	Instant Messaging
MMS	Tasks	Data Synchronization
Video Call	Document Processing	Browsing Information
Voice Mail	Camera use	Downloading Web Content
Fax	Multimedia access	Ticketing
Push-to-Talk	Data synchronization	VoIP
Conferencing	Control of devices	Location-based services (Pull)
Value-added services	Business Applications	Video-on-Demand
	Identification Documents	TV streaming
		M-payments
		E-learning
		E-health
		Business Applications
		Information Services (Pull)
		Adult services
		Gaming
		Gambling
		Electronic Currency
		Voting

Table 3-2: Examples of Usage Scenarios

The classification of risk for each service and application could change to fit the requirements of each party, whether it is an organisation or an individual. However, it

is important for any such approach to be usable for all stakeholders – organisations of all sizes and individuals. The complexity of the risk assessment process therefore would need to change depending upon whether it is being completed by a professional within an organisation or a normal member of the public.

3.2.3 An Risk Assessment Example for Mobile Devices

The ability to assess the level of loss, whether it is financial, personal or perhaps business confidence, is imperative in establishing appropriate controls for the protection of assets. Risk analysis techniques have been developed and widely utilised by organisations to ensure they take account of the threats and vulnerabilities against their systems. Without considering the full range of risks associated with mobile assets, an example method for establishing the level of trust required in the identity of the user wishing to access the application or service is presented here. It is recognised that mobile devices are often owned by individuals and used to store business data (or vice versa). With this in mind, the required security could be defined by responsibility in one of three ways:

1. Organisation is wholly responsible for the device and all applications, services and business processes that operate on it.

2. Personal user is wholly responsible for the device and all applications and services that operate on it.

3. Both organisation and end-user take partial responsibility for particular applications, services and business processes that operate on it. No specific apportioning of responsibility is assumed.

Similarly to risk assessment, it is the responsibility of the appropriate party (or parties) to define the trust level required for each application, service or business process. What actually needs to be assessed will largely depend on whether the device is being used for business or personal purposes. It is envisaged for instance, for personal purposes, the user is likely to utilise the applications and services that are available and provided on the device by the network operator. The range of applications and services will largely depend on the device and therefore be fairly static. For business purposes, the range of applications and services operating on the device is likely to include all of the default functionality (similarly to personal users), but also operate a wider range of third party and bespoke applications. It is therefore important to ensure an organisation has the ability to add applications and services.

The level of trust can be established in several ways. By recognising the different requirements of a personal user versus an organisation, one could potentially use three main models:

1. _**Personal Security Model (PSM)**_ _**: A model to be undertaken by a personal user:**_

   Although risk assessment methodologies are traditional tools used by businesses to identify the level of risks, such an approach is not so viable for the end-user. It could place a significant burden upon novice users, as specialist knowledge and procedures are required. As such a simple means of assigning risk to a service or application could be a more appropriate solution, which could provide a simple way to the personal user to set a risk/security

level to each service or application, without any further analytical view of impact, based on his knowledge and use of the device.

2. *Simple Risk Assessment Model (SRAM): A model to be undertaken by either the personal user, the organisation, or a combination of both:*

This type of model could represent a more focused risk analysis tool than the one for the personal user, useful for more security aware mobile device users. As such it could include a risk analysis process that can incorporate a more complete solution and granularity required in the process but at the same time follow a simplified risk analysis process. Organisations not versed in risk analysis, or lacking related expertise, could also follow this model. In addition, taking into account that the responsibility of the device might reside with more than one party, such model could also permit the choice of which stakeholder has the responsibility of assigning risk to each service or application.

In order to appoint the sensitivity levels, each service could be analysed in terms of the typical consequence that would potentially result from breaches of confidentiality, integrity and availability in each usage context. The consequences considered have been adopted from a standard risk analysis methodology (CRAMM) (Barber and Davey,1992), and are classified as follows:

- Disruption
- Breach of personal privacy
- Embarrassment
- Breach of commercial confidentiality

- Financial loss
- Legal liability
- Threat to personal safety

3. _**Organisational Risk Assessment Model (ORAM)**: A model to be undertaken by organisations incorporating the mobile device functionality into their current risk assessment methodology and tools:_

Many organisations already have formal risk assessment strategies in place, with relevant expertise. As such in this case the model would simply permit them to integrate mobile devices, and the applications and services accessed by them, into the existing risk analysis processes.

Figure 3.4 illustrates the 3 models, where it can be seen that as there is a move towards organisational use there is an increasing reliance upon formal and established risk assessment methodologies.
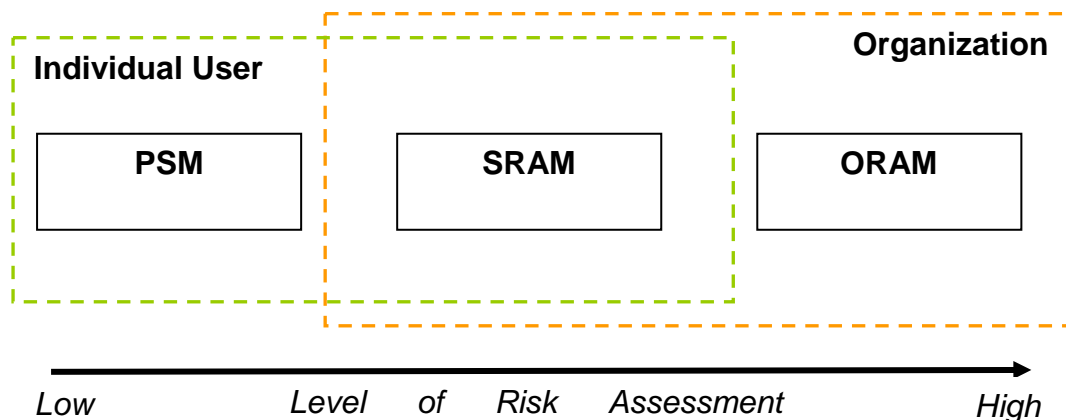
Figure 3.4: Risk Assessment Models

These three models are just an example used here to indicate a way to assist in providing the flexibility required when dealing with differing stakeholder responsibilities and for each party can use the process that best matches their

requirements and ability. As such, even in the case of both the business and the user having responsibility on the contents of the device, each one will be able to attribute security levels to the services that refer to them. A more extensive description of the models can be found in (Clarke et al, 2011) in Appendix B.

This section discussed the need for enhanced authentication as mobile devices evolve to offer functionality that enables the use and access of sensitive information. This need has been established from the views of stakeholders acquired through the focus group. What is also considered important is to address the issue of different security requirements across different services. Therefore a flexible and robust mechanism is required to meet these needs and provide an appropriate level of trust to the user's identity. It is envisaged that the use of continuous authentication during the interaction that the user has with his device is one way that this can be achieved. In order for the latter to be tolerant from a usability perspective the authentication would require a level of transparency. As such the use of biometric techniques that lend themselves very well to transparency is considered in the context of this research.

3.3 Analysis of Authentication Topologies

This research seeks to establish how enhanced security might be achieved, through robust authentication mechanisms that are able to offer the user and network a wider variety of authentication options depending upon the individual, network operator and business security requirements. It is envisaged that an open approach utilising a wide variety of authentication techniques in both an intrusive and transparent fashion will assist in providing the flexibility required to meet the differing security and service

requirements of a large user community. The focus of this section is directed towards the technical and perceptual issues that are involved in the implementation of such authentication framework looking at the trade-offs between a network based versus a device-centric approach.

The topology of an authentication mechanism is an important factor to consider at the outset of the design process, especially when looking to deploy biometric techniques. With numerous stakeholders, (such as network operators, corporate IT administrators and end-users), the ability to provide identity verification in a manner that maintains both security and privacy, and considers the operational impact upon the mobile device is imperative. Unfortunately, however, it is difficult to maintain all these services for all stakeholders, and a trade-off exists between different security and privacy issues, depending upon what the system is trying to optimally achieve.

In the context of networked mobile devices, two principal options exist for where to locate and operate the authentication mechanism: the device or the network. Although to date identity verification has been performed by the device itself this might not be the best approach to take when considering the particular objectives being sought in this research. The following sections will describe the two approaches and proceed to discuss the various issues involved with the topologies. During this discussion representative views from the aforementioned focus group will also be presented as it is important to consider the user's perspective when deciding upon the topology.

3.3.1 A Network-Centric Approach

A network-centric approach will direct all the key computational tasks and storage to the network. The physical placement of the authentication mechanism within the network could be with the network operator, corporate IT administrator, or third-party providing managed authentication services. As illustrated in Figure 3.5, the mobile device itself will act as the biometric sample capturing device and be able to respond to a decision sent from the server to permit or restrict access to a user.

Depending upon the device, its processing capabilities and security requirements it could be possible to partially split the biometric process, where the data extraction phase is conducted on the device and classification on the network. This would assist in reducing the amount of traffic sent across the network.
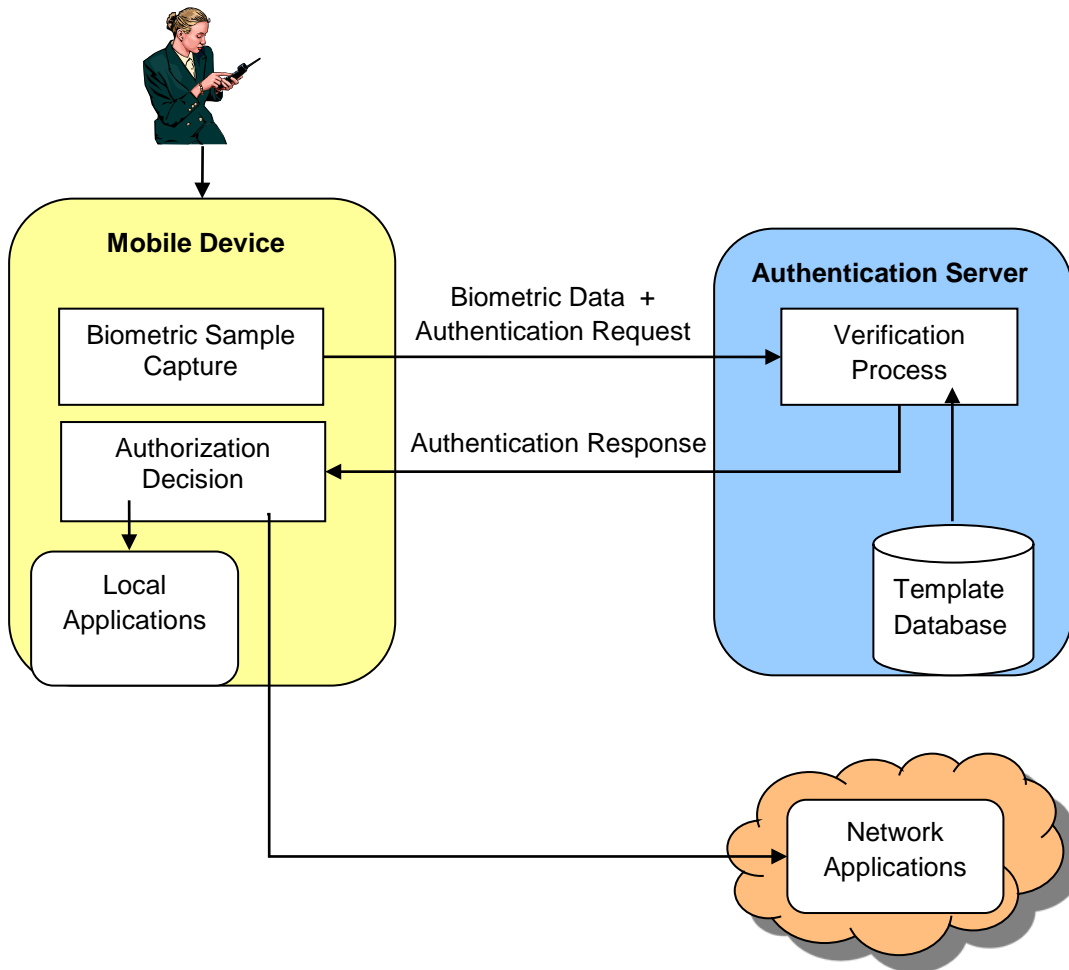
Figure 3.5: A Network-Centric Approach

3.3.2 A Device-Centric Approach

In a device-centric approach the whole biometric process is completed on the device. All the information, algorithms and management controls required for the authentication process are stored upon the device. Furthermore, all the processing required to perform the verification also takes place on the device. Figure 3.6 illustrates an example of such an approach.
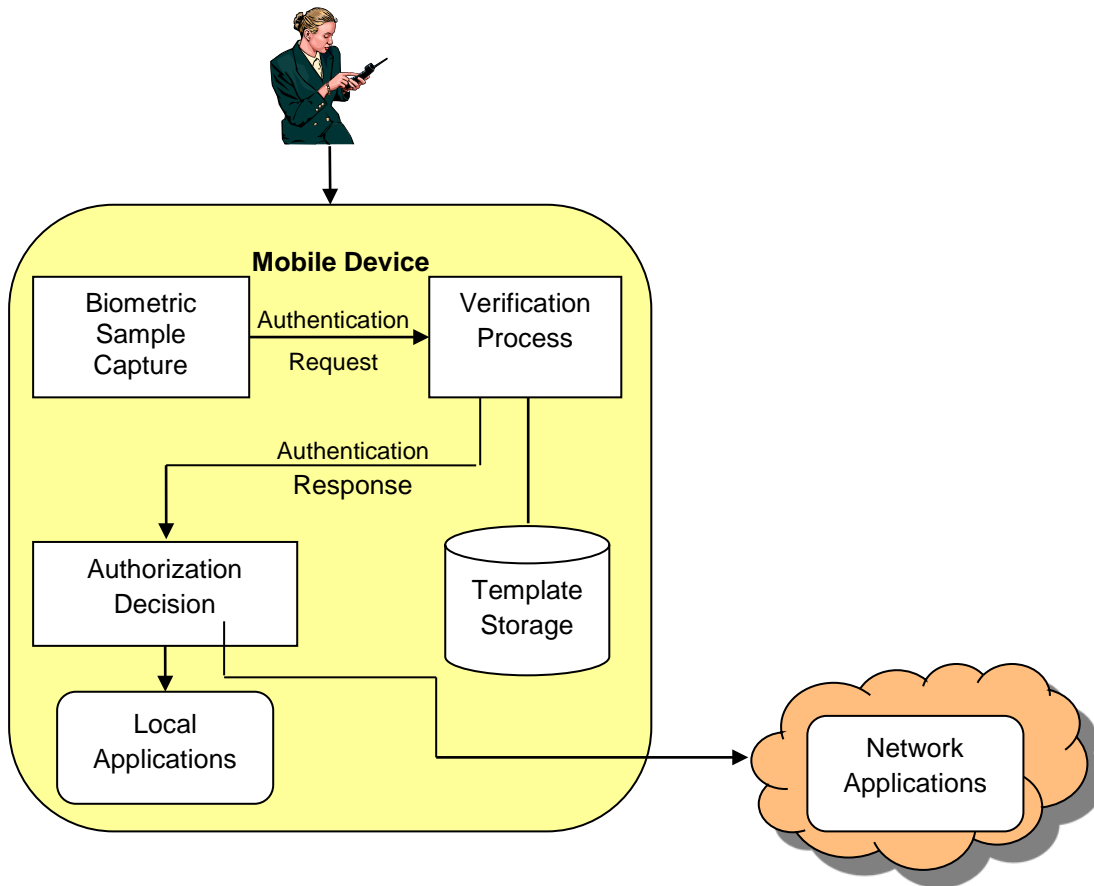
Figure 3.6: A Device-Centric Approach

3.3.3 Trade-Off Considerations

The two approaches have several advantages and disadvantages in their implementations from both social and technical perspectives. Key areas to establish the requirements and trade-offs that exist are:

- User privacy

- Storage and processing of biometric samples

- Network bandwidth requirements

- Network availability

- Mobility and roaming

The following sections address and discuss these issues, examining in detail the trade-offs between the two potential topologies.

3.3.3.1 User Privacy

When considering which topology to deploy, resolving the issue of user privacy is essential for widespread adoption. This becomes even more important when the topology is looking to utilise biometric techniques as the underlying mechanism. Recent years have seen widespread media attention directed towards biometrics, due largely to their inclusion within passport and national identity card schemes (Gomm, 2005; Lettice, 2010). Unfortunately, and for some legitimate reasons, this attention has been somewhat negative towards the benefits of the technology, focussing instead upon privacy concerns (Porter, 2004; TimesOnLine, 2004; Lettice, 2010; Rodriguez, 2012). It is therefore important to ensure the authentication mechanism is designed in a fashion that is sensitive to privacy issues.

The principal concern focuses around the biometric template and sample. In whichever biometric technique that is used, these elements represent unique personal information. Unfortunately, unlike other forms of authentication (such as secret knowledge or tokens, which can be simply changed if lost or stolen), it is not possible to change or replace biometric characteristics - they are an inherent part of the person. Therefore, once lost or stolen, they remain compromised and can no longer be reliably used. As such, the creation and storage of a biometric template or

profile on either the device or the network leads to significant responsibility for the user or the network provider respectively.

Public opinion regarding biometrics has been problematic, not least because of the proposed national ID scheme. This calls for a centralised repository of biometric information for UK nationals, but the ability to secure such databases from external attack and effectively manage authorisation to protect from internal misuse is no small undertaking. Despite the safeguards that one can apply, there will always be the potential for vulnerabilities due to both human factors and technical misconfigurations. Such vulnerability, and moreover the lack of confidence that it engenders, was also raised in the focus group, with participants voicing the concern over security and trust:

"…would you really want your biometric data then stored on the inside of a company that's possibly got people dodgy, people breaking into it already…"

"And even in the network don't think it's all that secure either, because there is always the rogue employee somewhere, who is in the pay of an attacker"

These quotes demonstrate a major fear for the security of the information held remotely. Apart from the technicalities that might be overlooked, there are also examples of carelessness taking place that has led to severe incidents. An illustrative example occurred within an Orange call centre, where employees that had been granted access to full customer records (including information such as

bank details) were sharing their login credentials with other staff (Mobile Business, 2006). This removed any ability to effectively monitor who and when they had access to information. The increased fear of identity theft and fraud makes people even more cautious about their personal information, and how and where they provide it.

With the UK ID scheme, it was seen that people were not very comfortable with providing their biometric information to such a centralised system (Lettice, 2006). As such a device-centric implementation is arguably more favourable from the user's perspective. In such a case, the profile will be stored on their personal device giving no third-party access to the biometric template or samples. This approach is able to satisfy peoples' desire for privacy preservation through giving them direct responsibility for its protection. Nevertheless such reliance does impose concerns about how reliable and also aware the end users will be in safeguarding their devices. As previously mentioned, several surveys have demonstrated that despite the storage of sensitive information in handsets, and despite the earlier cited evidence of loss and theft, users still disregard the use of even the available security measures. This is an important consideration to the choice in topology, as no further protection will be available once the device is stolen. On the other hand one might suggest that as the fear of misuse becomes greater the importance that each subscriber will attribute to each device will change respectively. Storing personal identifiers in the device might lead people to consider their device to be comparable to other forms of important information and ID, such as, passports, credit cards and car keys. Such linkage could potentially change people's perception and attitude toward the security and protection of their devices.

However, there was also a concern raised in the focus group expressing a fear of storage on the device and potential misuse.

"…my concern is where would the fingerprint, let's say like signature, where would be stored? Would that be stored on the phone, so if somebody stole my phone they have my signature which is signed on the back of your bank cards and my fingerprint obviously? What then can people do with the information…obviously if someone knows how to hack into a phone could they use the information?"

It is certain that a biometric database will always constitute an attractive target, making it a more valuable target than a device involving only one person. It would be necessary in such cases to establish regulations and policies for the security of the database and biometric templates, and mandate continuing adherence to them. A central system, though, has an advantage that the system can monitor such activity and try to prevent it, thereby providing a more uniform and controlled protection space, than storage in the device.

People have different views towards the storage of such information as concerns are raised over the security in each storage solution and how potentially easy a breach of confidentiality is. An earlier study conducted by the author's research group attempted to assess public perceptions of biometrics, and performed a survey involving 209 respondents (Furnell and Evangelatos, 2007). One question asked people about their concern about the theft of their biometric data and the potential of using them to cheat a system. The responses are illustrated in Figure 3.7.
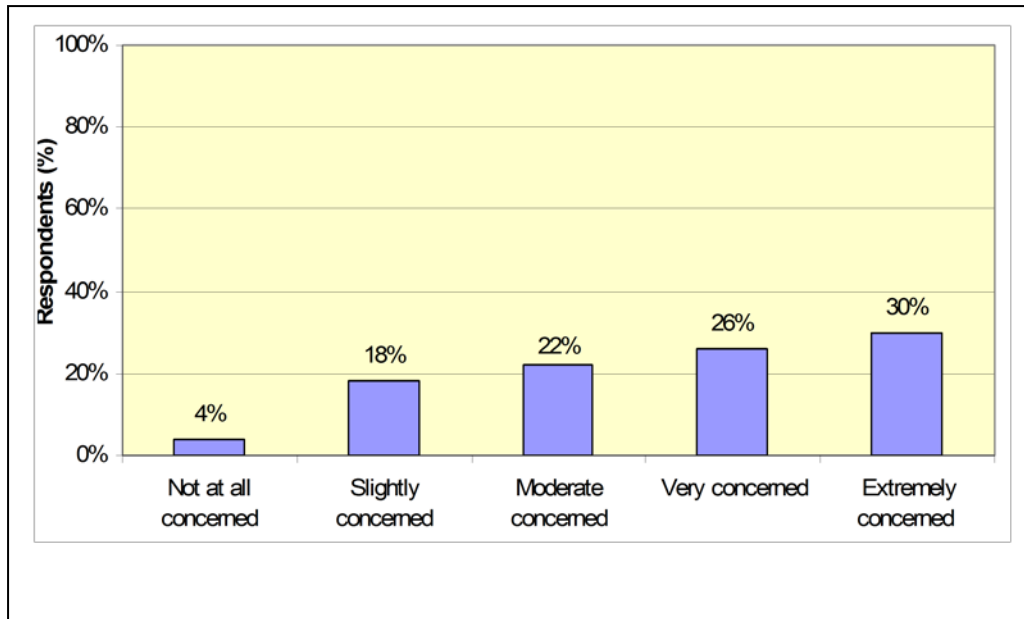
Figure 3.7: Concern that Biometric Information could be Stolen

As seen from the figure the majority of the respondents expressed some level of concern about the security of their data, with only 4% not having any fear of misuse. The same survey also asked where respondents would prefer their biometric data to be stored. 40% supported the network option having the template stored in a central database whereas only the 17% agreed on the device, as illustrated in Figure 3.8. Interestingly, 18% would prefer their biometric templates to be stored in a smartcard. This is analogous to a device-centric approach, as the smartcard must remain with the user, but represents a significant enhancement in physical and logical security of the information.
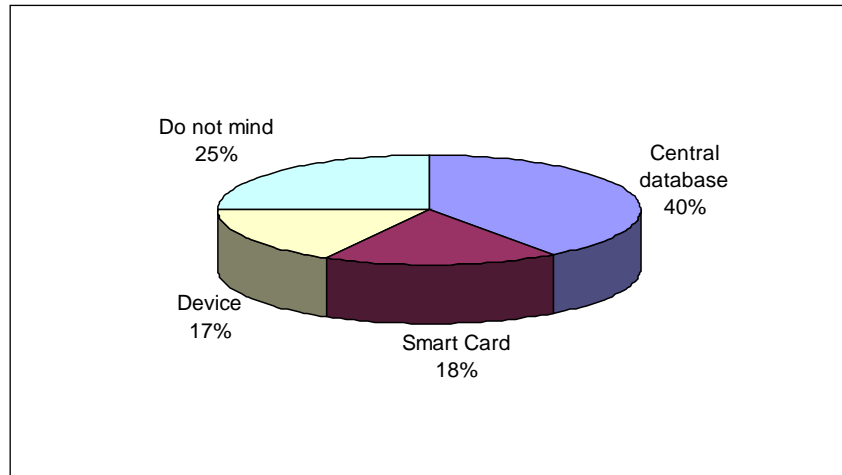
Figure 3.8: Subscriber Preferences on Storage of Biometric Profiles

Privacy concerns that exist for the network implementation could be reduced by ensuring only the biometric templates are stored and not any form of raw data. Several studies have taken place to overcome that issue looking to protect the storage of biometrics using techniques such as distortion of the template. It is also notable that the creation of biometric templates is based upon vendors' own proprietary formats. As such, one biometric template from one vendor will not operate with another vendor's product, as the format and characteristics used to authenticate people differ. This will reduce the potential harm caused by a stolen biometric sample to systems that only utilised that specific vendor's product. The one-way property of creating biometric templates also ensures they cannot be reverse engineered.

3.3.3.2 Storage & Processing Requirements

While the privacy issue represents a challenge of user trust and perception, there are also technical-level considerations in terms of the storage and processing of biometric data. These will again differ according to the chosen topology.

Consideration needs to be given to the storage of the initial biometric template and also the samples that are subsequently used in the process of verification. For current PIN-based approaches this is not an issue, but the storage demands of biometrics are more significant. Issues of storage might exist in both topologies, with individual devices potentially having limited on-board storage, while the network-centric approach may need to cope with the storage of data for high volumes of users.

Different biometric techniques require differing levels of storage memory. Techniques such as face recognition (where multiple images might be needed from different angles in order to achieve a high consistent outcome), or voice verification (where sound files need to be stored), usually require higher storage capacities. Furthermore, as the proposed authentication mechanism aims to take advantage of a number of different techniques, the device or network will need to store more than one template per user, which could potentially become very demanding. Figure 3.9 illustrates typical template sizes from a number of more common biometric technologies.
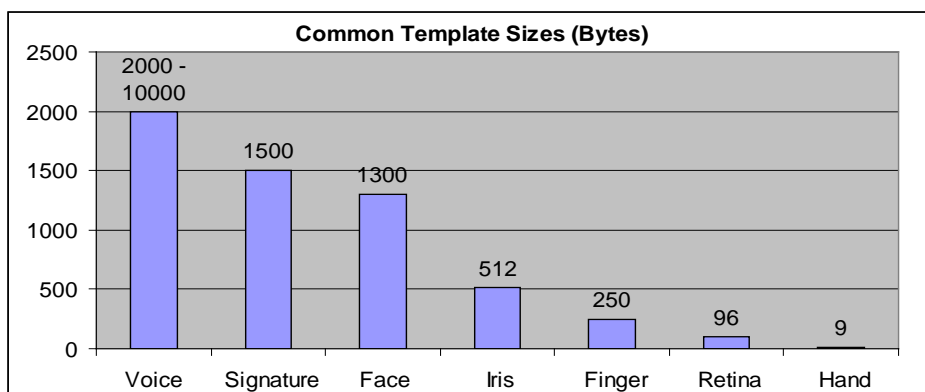
Figure 3.9: Typical Sizes of Biometric Templates (IBG, 2002)

Given the memory available on current mobile device, it can be seen that the storage requirements would not prevent a device-centric implementation. The most demanding approach is voice scanning which can reach the requirements of close to 10KB. Therefore in general terms, storage of biometric templates in a device-centric model does not present any difficulty. However, given the variability in devices and functionality, some care must be taken to ensure that this proposed authentication mechanism is able to operate with all hardware devices, including legacy devices which might have smaller storage footprints.

In terms of processing capabilities, the network-centric approach has an advantage in the sense that devices themselves may have relatively limited capabilities. Indeed, this may actually represent a fundamental obstacle to establishing a device-centric solution. Whereas laptop-level devices may have the capabilities required to process biometric data, the processing power in handheld devices is still limited. Algorithms that are utilised in biometric verification tend to be intensive, as they are based upon complex data extraction and pattern classification techniques (and indeed the impact of this additional processing on the battery of the mobile device would also have to be carefully considered). The process of enrolment and verification will place a serious demand upon resources on many mobile devices. In order to achieve transparent authentication, verification of the user needs to be completed without affecting the user's ability to use the device (e.g. no impairment to other running applications). It would not be satisfactory for the device to pause or hang for a few seconds every time verification was being performed. However, as with the storage footprint, different biometric techniques require varying levels of processing capacity.

It is therefore not necessarily infeasible to consider at least some biometrics operating in a device-centric model. Indeed, signature recognition, fingerprint recognition, keystroke analysis and facial recognition have all been developed for mobile devices early on (PDALok, 2006; NTT DoCoMo, 2003; Clarke & Furnell, 2006; Omron, 2005; Karatzouni & Clarke, 2007).

Over time, the processing constraints are likely to be overcome in the future as the capabilities of handhelds continue to advance. However, from an implementation perspective, a network-centric model would still potentially be easier to deploy and offer a wider range of possible biometric techniques that could be used. Again, however, consideration needs to be given upon the scalability of such an approach - multiplying individual authentication requests by high volumes of users does place a significant demand upon processing.

3.3.3.3 Bandwidth Requirements

A particular consideration in the context of the network-centric approach is the network bandwidth that will be required for the transmission of user authentication data. A device-centric approach has no such implications, as at most it will only be required to perform its normal authentication of the device to the network. By contrast, the network-centric approach will require network bandwidth to send biometric samples to the network, and receive authentication decisions back. Communication across the network will also result in a latency occurring between the initial authentication request and the resulting decision.

Typical bandwidth rates in practical 3G network scenarios are 220-320 kbps for UMTS and 550-1100kbps with HSDPA, although the theoretical rates are a lot higher (3G, 2004). An average 3G portal page, for example, has a size of 40 Kbytes and should theoretically take less than a second to load. However, in reality the actual throughput results in an 8-20 second delay. A usability study in 2005 has shown that users are willing to wait for at least 3 seconds for a page to appear however this today has changed to a "blink of an eye" as Google engineers found, underlying how demanding users are when using their devices (Gissin, 2005, NYTimes, 2012). This willingness to wait is an important consideration and key factor in designing the authentication protocols and deployed mechanisms. Forcing users to wait too long before being given access would result in a negative perception, particularly when the approach is meant to be transparent. A good scoring mobile page e.g. in terms of responsiveness in 2008 would be of size 9.89K with a response time of near 1-1.5s for WiFi and GPRS and 4.40sec for GPRS. Whereas today the same page would be 6.26K with maximum response time for GPRS 3.5sec, showing that bandwidth requirements are sufficient and improving to what was a requirement for standard web pages in the past and (Nubiq, 2008)

As discussed in the previous section, biometric templates can range from as little as a few hundred bytes up to 10Kbytes. These templates contain the unique data that is derived after pre-processing (thereby extracting required features). The option of the device performing this procedure would be a way to decrease the bandwidth requirements as the data sent would be far smaller than the raw sample. However, the ability to perform pre-processing on the device will depend upon the individual

biometric technique and the processing capabilities of the device. If pre-processing can be implemented on the device it can be assumed that the size of data being communicated are similar to those presented in Figure 3.9. A simple computation will show that the largest template of 10Kbytes will require time of 0.36 sec for the lowest given throughput of UTMS (220 kbps). It must be considered though that this might well become larger depending upon the network condition at the time and also takes no consideration of the time taken for the network to actually perform the authentication. Beyond latency for individual users, the issue of scalability needs to be addressed. Large volumes of users sending biometric sample data across the network might have significant impacts upon network resources and increase the level of delay experienced. For example, in 2012 one of the largest operators in the UK accounted over 19 million UK subscribers (Mobile News, 2012). If just 10% of them used such a service, this translates to about 1.9 million users requesting authentication from the network. Of course the burden of the network will depend upon the authentication frequency and this will vary across users as the different use of their device will result in more or less authentication requests.

At first glance one might suggest that current 3G and 4G networks (and certainly future networks) would be able to cope with the requirements. Although this might not be wrong in principle, an investigation of the network consumption does reveal somewhat surprisingly high volumes. Based upon the figures of 1.5 million users Figure 3.10 illustrates the bandwidth required per day for three different types of biometric approach.
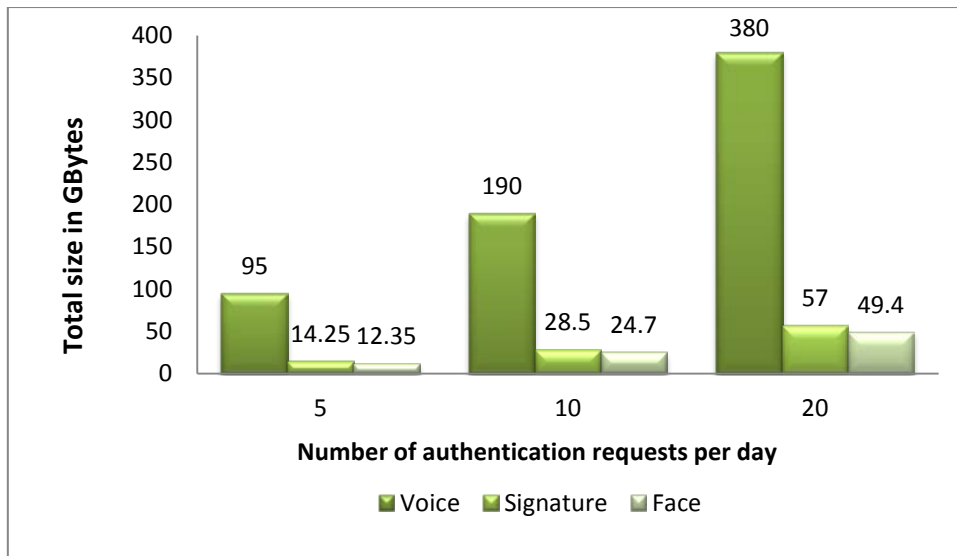
Figure 3.10: Average Biometric Data Transfer Requirements (Based upon 1.5 million Users)

As illustrated in the chart, for voice scan, even a minimum request for authentication of five times results a required data capacity of 95Gbytes for the network provider, whereas with up to twenty requests per day this raises to 380Gbytes. In comparison however, taking a video stream application, (one of the standard 3G applications), for example streaming a high quality video in Youtube requires 3.0Mbit/s (Ad Terras per Aspera, 2010). In a population of 1.9 million subscribers that represents 712 Gbytes to be transferred every second to which the comparison to the authentication requirements may seem affordable in terms of bandwidth. That said, there is a real cost associated with sending data across a network and there will be at least an indirect cost, given that the operator may otherwise be able to use the bandwidth to support revenue-generating services.

3.3.3.4 Availability Requirements

A factor that plays a significant role in a network-centric topology is the establishment of availability. In a fully device-centric approach all aspects required to

perform the authentication are self-contained locally within the device. However, having the authentication process relying upon the network makes a key assumption that the network is available at all times to facilitate the process.

In practice, there are various reasons why network connectivity might not be available, such as loss of coverage, network overload, or server malfunction. The inability to perform an authentication request as and when required will have a significant impact upon the authentication mechanism and its perceived usability.

Of course, if the authentication request is associated with a network-based application or service then one could reasonably argue that there is no inconvenience, as the service would not be available anyway. What would be less acceptable, however, would be reliance upon network availability in order to access applications or features that would otherwise be entirely local. For example, opening a document, accessing contacts, or using Bluetooth to connect to another device, might all require authentication, and this would have a real and unacceptable impact if the process were to rely upon the (unavailable) network.

Participants in the focus group were asked to consider this issue and overall there was a negative opinion on always requiring access from the network. The following viewpoint was typical:

> *"I find it difficult that it might be possible just even to interact with the network operator, because I'd like to use that information even when I don't interact with the network operator."*

It can be suggested that apart from the technical issues that can occur, it seems rather inconvenient to require authentication from the provider. The inconvenience does not only relate to the access of local functionality and applications, but also the general concept - that in order to access any service the user will be obliged to explicitly go through the network provider. This places a burden of inconvenience upon the user, network provider and the authentication mechanism. One of the focus group members specifically summed up the issues surrounding the availability of network resources:

"There is quite a lot stored in the network. Potentially everything can be stored in the network. There is a trade-off between responsiveness and security….Especially if you are not in coverage all period of time and you want to look up someone's name, address or whatever in your address book you haven't got it. So that's completely rejected by the operators. There's got to be some balance between security that happens on the network and immediacy you have on the person... there isn't a simple answer to this sort of question"

3.3.3.5   Mobility & Roaming

A network-centric topology would enable personal mobility (Thai *et al*, 2003) - the ability in principle to get authenticated on any mobile device and have all subsequent use of the device billed to their account. Having the verification coming from the network, the subscriber will be able to use the system from various devices, without any swapping of SIM cards. The device-centric approach lacks such convenience as the storage and authentication of the user is linked to the specific device.

Conversely, however, when considering the issue of roaming, the device-centric topology is more appropriate as authentication of the user can be performed on the device wherever they might be in the world. A network-centric topology would experience significant increases in latency and have to transverse a far larger open network. Unless the local network provider supported the authentication mechanism and had a local version of the biometric template (which would not be likely due to privacy) this increase in delay would again have an impact upon the authentication mechanism which would need to be considered.

But what also happens when roaming is not available? In such a situation, the user will have no way to be authenticated as no access to the provider's network will be available, restricting if not completely preventing any use of the device. There is also the consideration of cost. A home network operator implementing the authentication mechanism might be prepared to bear the cost of network consumption. However, this may not be the case for a roaming network, raising questions of who covers the cost. Currently the charges for roaming are very high rates, although this is starting to change with big operators reducing the occurring costs (Neil, 2013). A device-centric approach would overcome this issue as no reliance upon external resources is required.

3.3.4 Discussion

The prior analysis has shown that comparing the device- and network-centric topologies introduces a varied and complex range of considerations, with each approach offering advantages and disadvantages in different contexts. Attempting to base a solution entirely around the device can introduce processing limitations,

whereas bandwidth and the requirement for connectivity may represent practical constraints for a network-based model. In addition, both approaches may introduce their own privacy-related concerns. Table 3-3 summarizes the key characteristics.

Requirements	Architecture Approach	
	Network-Centric	**Device-Centric**
Privacy	✓ More focused and well monitored security × Biometric profiles kept by third party × Security of central storage with a great amount of personal information	✓ Overcomes privacy issues × Security relies upon the individual
Storage	✓ Able to cope with storage requirements	✓ Likely for new high-tech devices to be able to deal with. × Depends on the amount and type of biometrics used as to the captured samples.
Processing	✓ Able to cope with processing requirements	✓ Likely for new high-tech devices to be able to deal with low demanding techniques × Depends on the type of the device × Depends on the processing requirements of the classification algorithms
Bandwidth	✓ Available networks can provide the required bandwidth × Scalability issues might exist depending on the type of data transmitted	n/a
Availability	× Unable to ensure always-on access	n/a
Mobility & Roaming	✓ Enables the use of the authentication mechanism to a number of devices × Restricts the mobility of the user over different networks and places	✓ Enables user's mobility without placing any restrictions × Binds the authentication to the device.

Table 3-3: A Summary listing of the Advantages and Disadvantages of each Architecture Approach

Based on the issues arising from both potential architectures, it can be argued that no single approach can cover all aspects that are required for the practical implementation of the proposed authentication framework. In order to try to overcome the troublesome aspects of each implementation, it is suggested that a hybrid approach would be more appropriate. Although complicating the underlying authentication system, it would provide a basis for overcoming the disadvantages of both topologies, while retaining their key advantages, so that the aims and objectives of the authentication mechanism can be met.

In such approach both storage and processing would be potentially split over the device and the network, compromising between the issues of device processing capabilities, network availability, and privacy. The nature of the split in the authentication mechanism will depend upon the individual requirements of the user or organisation in relation to privacy and access, and the device in terms of which biometric techniques it can support locally. There will be therefore a number of hybrid approaches that could exist, each covering different issues on different scenarios for different users. For example, in order to deal with the issue of device processing and privacy, there could be the option to store all of the templates in the device, but place the processing functionality on the network, as illustrated in

Figure 3.11. This would satisfy privacy concerns but at the same time discharge the device of any excessive processing tasks. Cryptographic measures could be used to protect the data in transit and during processing. Depending upon the device capabilities, pre-processing can be performed locally when possible, so that the biometric samples that are being sent over the network are kept as small as possible, as illustrated in Figure 3.12.
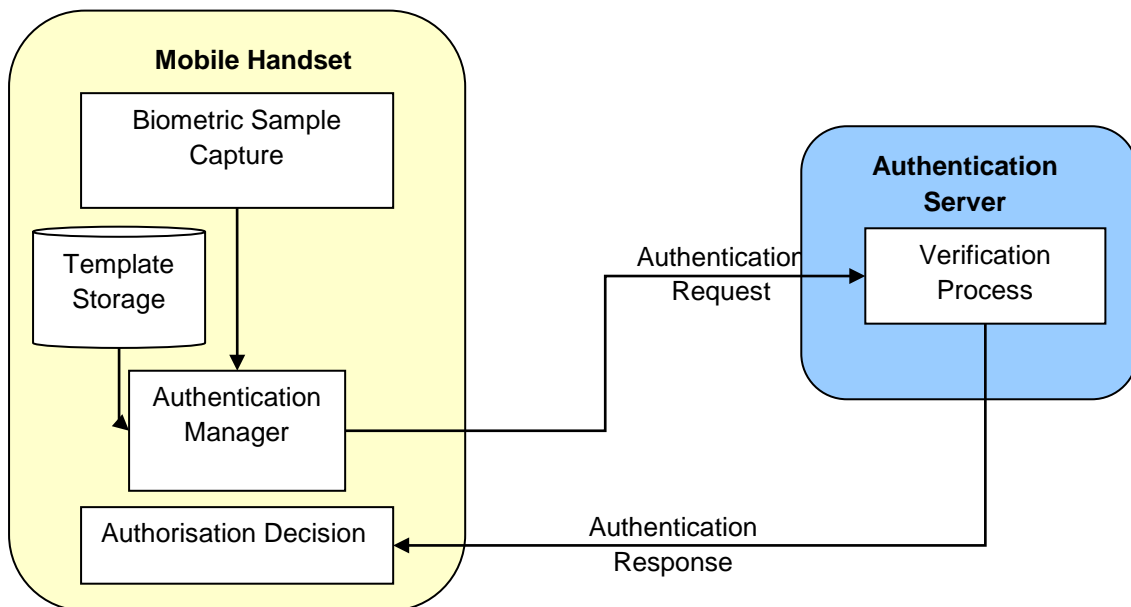
Figure 3.11: Hybrid Approach - Storage of the Template on the Device & Processing on the Network
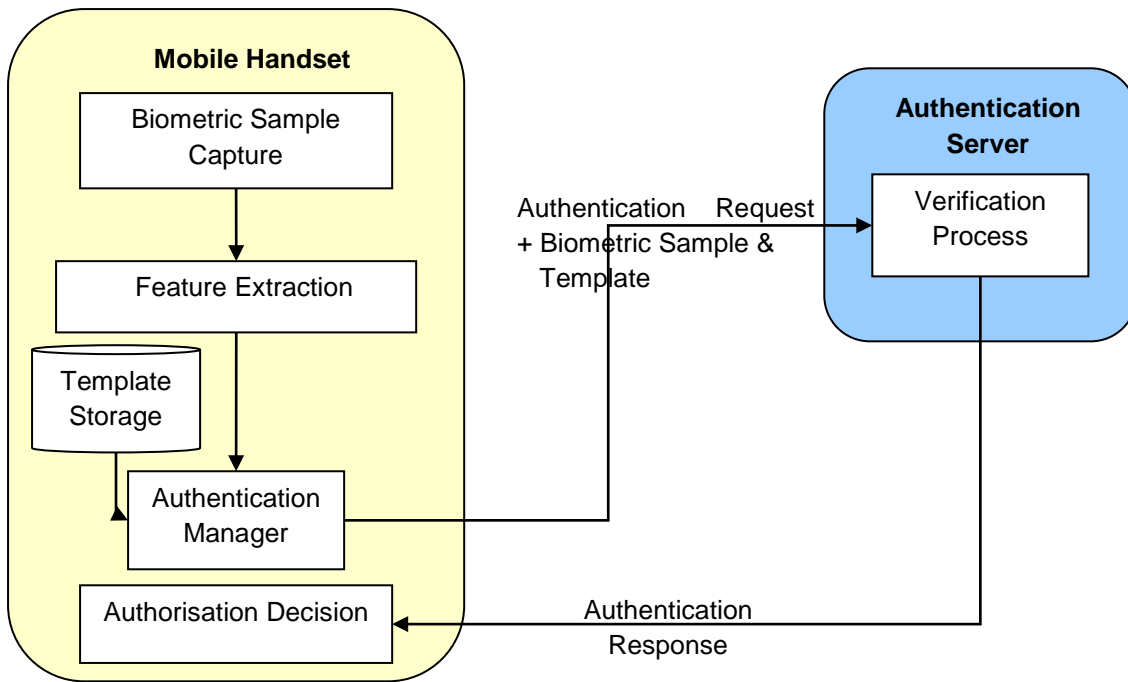
Figure 3.12: Hybrid Approach - Processing on the Network & Storage of the Template and Pre-Processing of Biometrics Samples on the Device

The specific nature of the hybrid system will closely depend upon a wide variety of factors that have been discussed in this chapter. Figure 3.11and Figure 3.12 form only two potential examples of such a system. In order to remove the concerns surrounding network availability it is suggested that at least one authentication technique will always remain on the local device. Although this technique might not provide the level of security strong network-based biometrics might, it will be able to provide an effective means of authenticating short term usage of local applications and functions.

In devices with more possessing capacity, the hybrid approach would also be able to provide the ability to split the biometric templates, having the most intensive and demanding biometric techniques on the network and the others with fewer

requirements on the device. Another basis for determining this split could also be the uniqueness attributed to them for privacy issues.

This hybrid authentication model must incorporate a level of intelligence so it is able to understand when and how the security requirements can be attributed, and how the framework needs to adapt between different authentication techniques to handle those requirements. For example, if a user sends a text message or makes a local voice call then the operation need not be considered that critical, whereas accessing a mCommerce service or making an international call could demand more protection. The authentication mechanism should recognise this and select techniques that are appropriate to the context.

Having discussed in some detail the advantages and disadvantages of network-versus device-centric topologies, it is concluded that no single topology could achieve the desired aims. Therefore the principle of a hybrid version that is able to encompass the advantages of both systems and assist in mitigating the key disadvantages can be seen as more appropriate.

3.4   Conclusion

It can be foreseen that such authentication architecture will involve a number of consideration in terms of a topology. Most possibly the latter will need to be flexible to fit the differing requirements of individual users and individual techniques. In order have a practical view on the operation of such flexible framework that apart from the topology also encompasses further difficulties and evaluate the actual operation, a practical implementation of a pre-proposed framework has taken place and the

following chapter will provide the details and results of its implementation and consequent evaluation.

4 The NICA Framework – Implementation and Evaluation

Based on the requirements analysis for security on mobile devices, the need for a flexible authentication framework that can intelligently handle the differing requirements of individual users and devices has been identified. Furthermore, it is envisaged that the enhancement of current point-of-entry authentication with a mechanism based on biometric techniques that can offer continuous and transparent authentication can offer a more robust way to establish user identity.

In order to evaluate the feasibility of such approach a previous proposed framework designed to offer transparent authentication through the use of biometric techniques has been adopted. Based on this framework a prototype was developed and an evaluation using this prototype was undertaken. Section 4.1 briefly describes the aforementioned framework and its basic operation whereas Sections 4.2 and 4.3 describes the developed prototype and the evaluation phase and results respectively.

4.1 NICA Framework

The framework selected for evaluation – called NICA (Non-Intrusive Continuous Authentication), is a framework that formed the core basis for a research project funded by Eduserv and is based upon prior work undertaken by the research group and was previously known as the IAMS architecture (Clarke & Furnell, 2007). It utilises biometric techniques to provide transparent and thus continuous authentication while the user interacts with the mobile device.

NICA 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 transparently. 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 by the system. A number of services can also be defined as protected, where a specified level of security will be required to access them. The system will monitor the level of trust to the user and can allow or restrict access to those protected services. The purpose of the framework is to provide a highly modular authentication way 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.

4.1.1   NICA Architecture

NICA architecture supports two topologies:

- A server based topology where the all the storage and processing is taking place on the server, and

- A device based topology where either the functionality is split between the device and the server or the system operates solely on the device.

This allows for the architecture to work in cases where connection exists or not so that security is always in place for the user. Flexibility is also given to the storage of biometric information as it can be stored and configured as the user wishes and furthermore to the performance requirements as for example more intensive processing can be carried out on the server side and less intensive techniques can be used for the device.

Figure 4.1 illustrates the server topology. In this case there are 3 main engines:

- The Authentication Engine which is responsible for dealing with the authentication samples and authentication decisions,

- The Biometric Engine that deals with the biometric techniques and runs the authentication algorithms,

- The Communications Engine which is responsible for the exchange of information between the device and the server.

The system has also another main component which is the Authentication Manager. The Manager is the core component of the framework and is responsible for coordinating the functionality of the framework and in some cases of the different engines.

The framework also encompasses 3 databases:

- The Input Cache which stores all captured samples from the user's interaction

- The Biometric Profile database which holds the biometric templates of the individual user as well as approved biometric samples

- The Hardware Compatibility database which holds information about the device and compatible techniques.

The Client database hold information about the individual clients and it includes the Authentication Assets which provides hardware dependent information authentication techniques available to each mobile device, in order for the Authentication Manager to select the most applicable input sample to authenticate the user
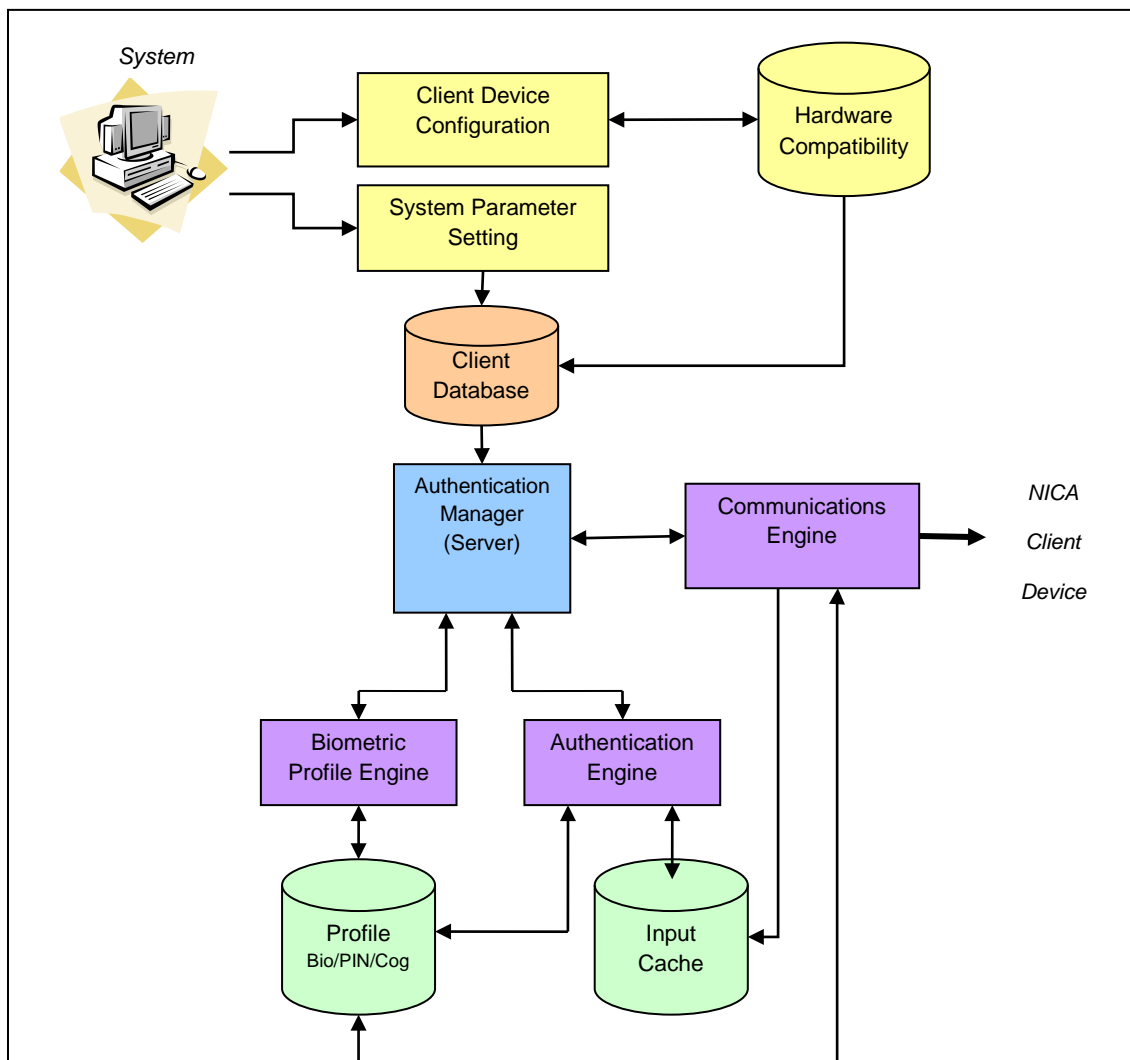
Figure 4.1: NICA Server Architecture

The device based topology- illustrated in Figure 4.2, holds identical components to the server one. However in the case of the device based approach an extra engine – the Data Collection engine is also presented which is responsible for capturing the samples during user interaction. Also an extra component for the device approach is also the Intrusion interface and the security status which is the output of the system that is used to restrict access or display relevant information. These components also exist in the server topology to capture and control access respectively.

The topology will slightly change depending on whether the system will operate on a standalone mode or a client-server mode. As such some of the engines might not be required – i.e. the Communication Engine in the standalone mode, or change from the device to the server for processing or storage issues- i.e. move the Biometric engine to the server that can more easily deal with the intensive biometric algorithms.
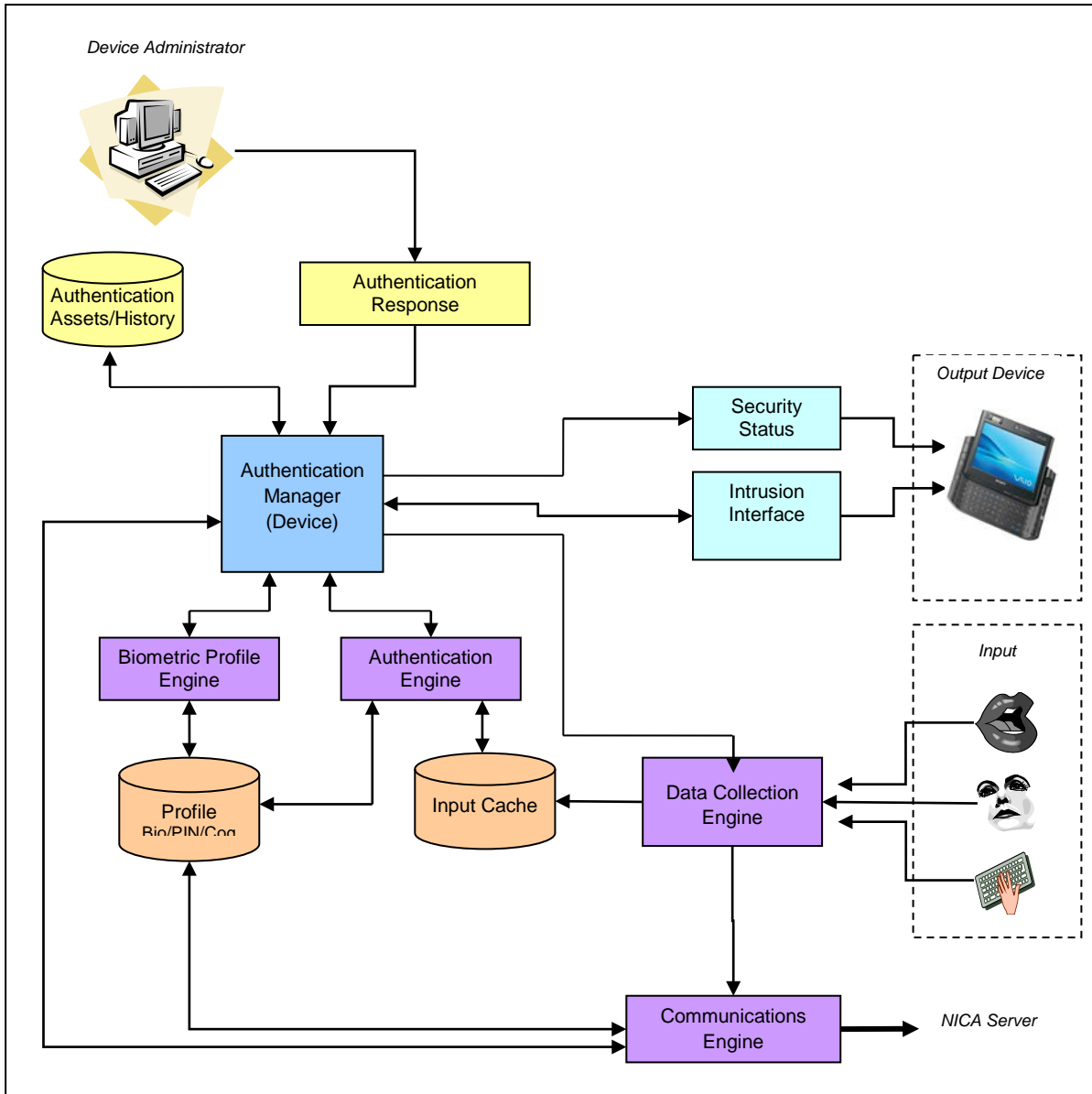
Figure 4.2: NICA Device Architecture

As this is not meant to be a detailed description of the specification, an outline of how security is established will be described in more detail, specifically, the Integrity Level and the Alert Level that define the core operation of the framework and help to establish the security provided in the device as well as the usability of the system. A reference to the detailed specification of the framework can be found in NICA (2007).

The security in a NICA system is built based on a series of authentication techniques that are enabled on the user's device. Each of the techniques - which could be either biometric or secret knowledge, is attributed with a confidence level. This level mainly corresponds to the error rates that each biometric technique can achieve so that they can be appropriately used to provide effective security. Table 4-1 illustrates confidence levels based on FAR rates. For secret knowledge techniques confidence levels P0 and P1 indicates their existence but are not comparatively related to the B* confidence levels.

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 4-1: Confidence Levels

Confidence levels are an indication of the security that a technique can achieve. The actual security of the system is defined by the Integrity Level. This level is a number that fluctuates between two values – 5 and -5, and its changes are a result of each authentication request. These fluctuations depend on each authentication technique that is utilised and the corresponding confident level. Table 4-2 illustrates an example of this notion.

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 4-2: System Integrity

As can be seen each confidence level and therefore the related technique can cause a specific change on the System Integrity. This is achieved by subtracting or adding a value that represents the allowed change for each technique to the current Integrity Level. If the authentication is successful then the value is added otherwise is subtracted. However what can also be noted on the table is that each technique can be used to achieve a Maximum Integrity Level to ensure that high trust is not achieved based on techniques that do not have relatively high confidence. In order to establish that the Integrity Level does not remain the same while the device stays inactive and therefore there is risk of misuse, the Integrity level is also getting decreased periodically regardless of any authentication by a degradation function.

The value attributed in each technique can be defined so much based on the performance of the technique but also based on the usability of each technique from a specific user (i.e. voice verification might not work that well for some user but another technique which is not considered that secure might do). As such there is the capacity here so that the respective value to the technique can be attributed individually to each user in order for him to have the more appropriate experience though the use of the system. Depending on the implementation of such framework, that may be configured by an administrator or be the preference setting of the actual

user. The Integrity Level at all times represents the trust of the system to the user and therefore the security level of the device.

The second core process of the system is the Alert Level, which is implemented by the Authentication Manager. The latter as aforementioned is responsible to decide which authentication method to use. This is coordinated based on the most recent samples captured as well as the technique that is more appropriate at a given time. Essentially the most recent sample on a specified time frame that is a sample of a highest confidence technique will be selected to be used for authentication. The Alert Level is the process that implements this functionality as well as deciding the next step based on the authentication decision. Figure 4.3 outlines the Alert Level mechanism.

The Alert Level is run by the Authentication manager that periodically initiates authentication requests based on which level the process stands. The Alert level is suggested in the original NICA specification to be triggered every 10-25 min depending on the type of user. As can be seen there are 6 steps on the process. The first 3 levels are transparent authentications that will be performed based on the most recent sample as aforementioned. At the beginning the first authentication will take place based on the most recent sample. If that fails the Alert Level will go to the next step taking again the most recent sample otherwise will return to the 'safe mode' which postpones the Alert Level. If all transparent requests fail then (reaching level 4) an intrusive request will be made while at the same time restricting access to the device as it is only up to a point that transparent authentication can be utilised for the sake of security. If authentication is successful then the Alert Level will drop

again to level 1 but only if a biometric is used. If only a secret knowledge technique is utilised then it is will only drop to level 3 waiting for a new transparent authentication with a biometric to mitigate any weaknesses of the secret based approach. If the authentication though request fails the Alert Level will be raised on level 4 where an intrusive authentication using the highest confidence technique available will be used and if it fails again it will go to level 5 where a two-factor authentication will be utilised – keystroke analysis based on a secret knowledge question. At that point if the authentication fails the device will be locked restricting all access to the user.

The decision of each authentication request made by the Alert Level will cause the Integrity Level to change respectively based on the confidence level of the technique utilised. The Integrity Level is not used during the Alert Level to affect any decision. It will only be used effectively in the case that a user will try to access a service that the system has set to be protected. NICA provides the facility to safeguard particular services by attributing an integrity value as the minimum requirement to be reached in order for the user to access them. If the Integrity level is sufficient to access the service then access will be allowed otherwise the user will be prompted with an intrusive request. This last process is also achieved by the Alert Level by setting the latter to level 4 and therefore putting the system into alert mode like it would happen if all transparent requests would fail. As has been seen in the risk analysis sections each service carry a different risk but also the different steps within that service. Although NICA defines only the start of a service as a requirement the intra-service usage could also be an addition to the framework to establish more convenience.

AS – Authentication Security

```
┌─────────────────────────────┐
│ Transparent          AL=1   │
│ Authentication Request      │
│ Most Recent Input Data      │
│ from the Cache              │
└─────────────────────────────┘
```

Authentication Response — PASS / FAIL

```
┌─────────────────────────────┐
│ Transparent          AL=2   │
│ Authentication Request      │
│ Remaining Data in Input     │
│ Cache                       │
└─────────────────────────────┘
```

Authentication Response — PASS / FAIL

```
┌─────────────────────────────┐
│ Transparent          AL=3   │
│ Authentication Request      │
│ Next Input Data             │
└─────────────────────────────┘
```

Authentication Response — PASS / FAIL

```
┌─────────────────────────────────────────────┐
│ Intrusive                      AL=4          │
│ Authentication Request                       │
│ User Required to Enter Biometric             │
│ (B3/B2) or PIN/Cognitive Question (1st)      │
└─────────────────────────────────────────────┘
```

Authentication Response — PASS (Number Only) / PASS (Biometric (& Number)) / FAIL

```
┌─────────────────────────────────────────────┐
│ Intrusive                      AL=5          │
│ Authentication Request                       │
│ User Required to Enter Biometric (B3/B2)     │
│ or PIN/Cognitive Question (2nd)              │
└─────────────────────────────────────────────┘
```

Authentication Response — PASS (Number Only) / PASS (Biometric (& Number)) / FAIL

```
┌─────────────────────────────┐
│ Intrusive            AL=6   │
│ LOCK DEVICE                 │
│ Request Unlock Code from    │
│ Administrator               │
└─────────────────────────────┘
```

Figure 4.3: Alert Level Process Algorithm

In order for the framework to compensate for keeping the integrity high whilst there is no use of the device, a degradation function has been defined. This function performs an Integrity drop of 0.5 every a certain amount of minutes so that the trust to the user reduces over time. As defined in the NICA (2007) specification the amount of min suggested was 30min for a frequent user and 50 min for infrequent use.

4.2   The Prototype

In order to evaluate the proposed idea an operational prototype was developed that will enable the functionality of the selected NICA authentication framework so that it could be practically evaluated. The approach taken in the prototype implementation is mainly a server centric model where all the intelligence resides in the server and the client acts as a mechanism for data collection and interface control. A standalone mode of prototype was also available however this was not tested during in the user evaluation phase as the processing requirements of the biometric algorithms made such an approach very time consuming and infeasible given the available devices at the time.

As can be seen in Figure 4.4, one machine is acting as the server where the authentication manager controls and handles all operations, the biometric engine, the authentication engine and well as the databases. The server supports the concurrent connection of multiple clients that can communicate and exchange data with the server in order to perform the authentication through the relevant communication engines.

On the client side a thin-client was developed to support capturing face, voice and keystroke biometric samples, in addition to monitoring all service and application usage so based on user interactions and usage of the device the system would capture the relevant and appropriate sample. This information was sent back to the server in order for the system to make the appropriate decisions and run the relevant authentication requests. The thin-client also had an intrusive authentication interface mechanism that restricts access to the device depending on the response of the authentication requests or when the user tries to access a service for which they do not have permission – so representing level 4 onwards of the Alert Level process.

Two devices were used as clients: a Sony VAIO UX1 running Windows Vista and an HP Mini- Note 2113 running Windows XP, both of which are illustrated in Figure 4.4. Although the initial desire for the prototype and the evaluation was to utilise smartphones, the restrictions posed by the OS and SDKs available at the time led to the selection of devices with a full OS. Similar restrictions were posed by the processing capabilities of the available at the time devices given the requirements of the biometric techniques. As such the Sony Vaio was selected as a close enough substitute to a small device with similar characteristics of a smartphone regarding the holding of the device and the hardware such as front facing camera, keyboard etc. The HP device was selected as a mobile device to represent a portable device with a different layout and holding as a normal laptop, notebook would be used. The Vaio was running Windows Vista whereas the HP notebook run Windows XP testing the prototype's portability in different OS.

Figure 4.4: The overall configuration of the prototype

The prototype implemented the majority of functions and database structures of NICA with only minor modifications to the architecture to support the implementation. These were simple internal updates e.g. although the databases were central to the server and common for all users there was a core authentication manager that handles multiple individual threads of user-tight managers to monitor processes and serve individual users. Similarly in practice the Communications Engine was present in the stand-alone mode although not present in the initial conceptual framework as there was a need for monitoring network connectivity. As aforementioned the prototype was able to operate in both a server-client mode as well as a standalone client mode as well as switching between the two approaches. In the event that the connectivity was lost with the server and could not establish a connection it was able to switch to a standalone mode and once connectivity was re-established it would switch back to network operation.

Matlab scripts for voice verification and face recognition were acquired and adapted to the requirements of the prototype for enrolment and verification. Keystroke analysis scripts were built-in house. The attempt to utilise also a commercially available SDK for signature recognition was made, however conflicts between the SDK and VB.NET did not allow for its final use on the prototype.
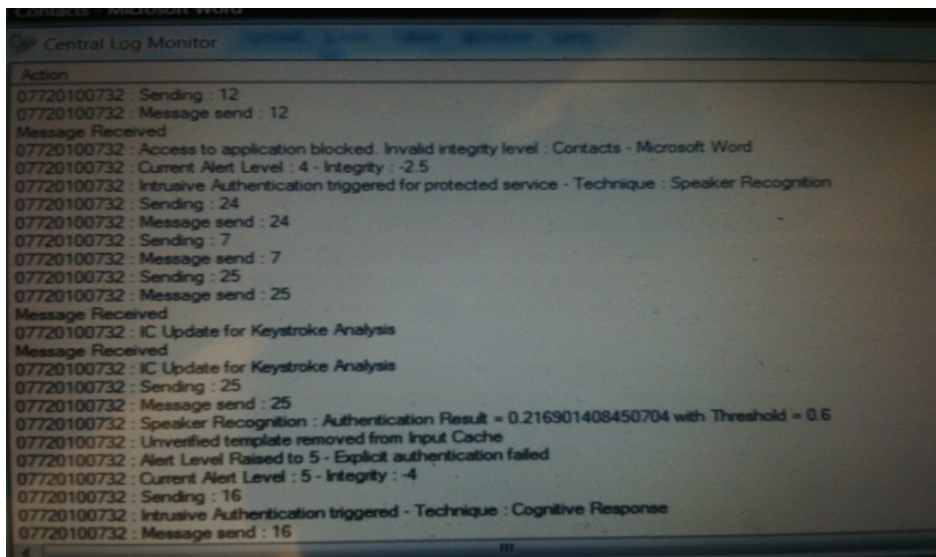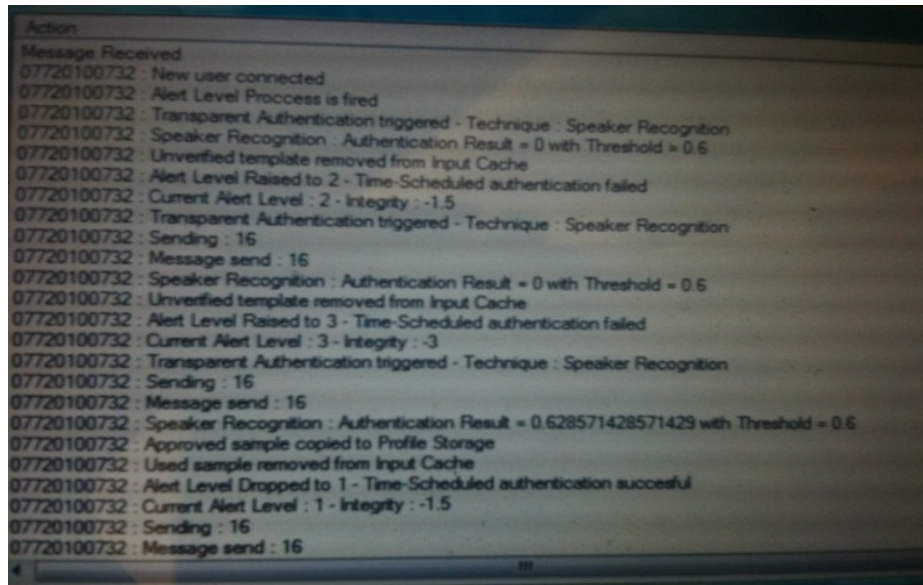
Figure 4.5: Example of the central monitor screen indicating Alert Level operation a) whilst going through L1 to L3 with available voice samples b) whilst accessing protected services leading to L4 and L5
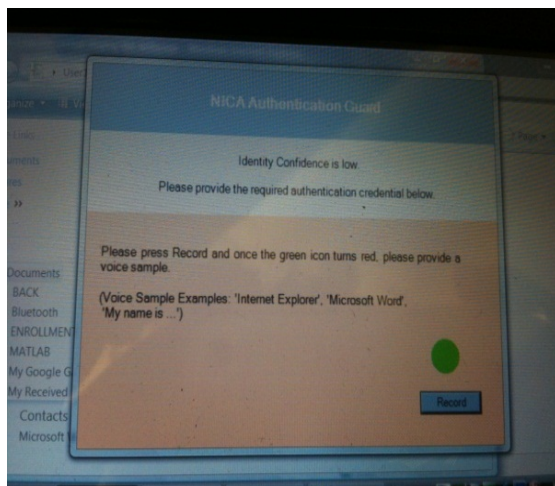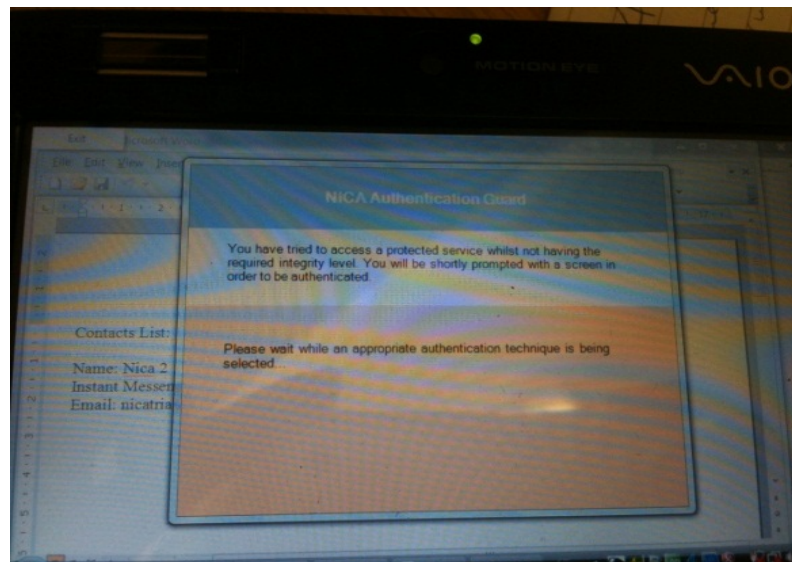
<center>(a)</center>
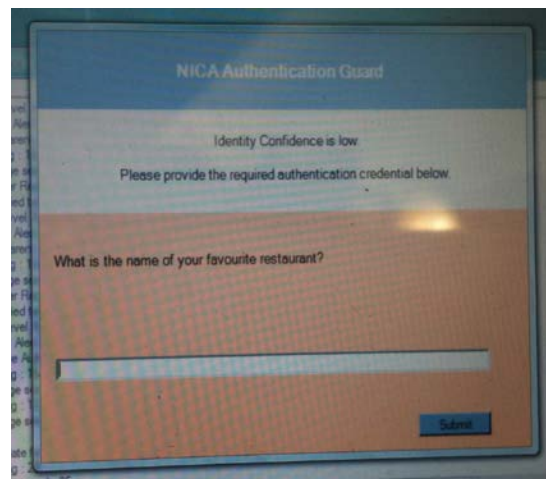
<center>(b)</center>

Figure 4.6: Example of intrusive interfaces of blocking access to any actions on device. a) Voice Recognition b) Cognitive Question with keystroke analysis

4.3 User Trial

In order to evaluate the effectiveness and perceived usability of the authentication framework in a hands-on context, the prototype was used as the basis for a series of trial activities. This was imperative in order to establish the effectiveness of such approach and potential issues that derive from the practical application of the latter before further progress of this research and design of a new approach.

4.3.1 Methodology

A methodology was developed so that important aspects of the framework could be assessed and evaluated in practice. Apart from monitoring the operation by collecting information from the system that would help the evaluation such as number of samples and authentication requests, a questionnaire was also available to assess the user experience and acquire any comments from the users. The questionnaire is available in Appendix C. The user trial was split to two phases:

Enrolment Phase: The participants used the prototype to provide face, voice and keystroke biometric samples that would be subsequently used to create their biometric profiles. They were also asked to define two cognitive questions that could be used for secret knowledge questions in case the biometric authentication failed and they reached the last intrusive request as described in the previous section. A simple to use and intuitive interface was used to capture the samples. 8 samples for face and 9 for voice were captured. For the face samples they were asked to capture 8 samples with slight variations on their position when facing the camera. For voice they were called to repeat the name of 3 applications that they were going to call subsequently as part of the scenario under the assumption that the system was using a voice recognition application. Also 15 keystroke samples were captured for each cognitive response they gave, in order to create the keystroke profiles for the two-factor authentication. The enrolment process took no more than 15 minutes per person and at the end the participants were asked to complete the first questionnaire.

Usability Phase: Each participant was asked to follow a series of steps that would force an interaction with the device while the authentication prototype was running on the background. This would enable for biometric samples to be captured transparently as well as force access to services set to be of high security in order to test the operation of the alert level algorithm and the authentication mechanism in general. The length of this phase varies as each user had a different interaction with the device and therefore took differing times to complete each task. The average time of this phase was 45 minutes. After completion of the scenario, the user was asked to fill in a questionnaire assessing their experience and the system. After that the users were asked to play the role of an impostor on the same device using the profile of another person and by using the same steps see how quickly the system will recognise that they were not the legitimate users. Again the users were asked to fill a questionnaire and assess their views again based on the new experience of the system, as now they had a further perspective from the security side rather than the usability of the system when they were acting as the legitimate users.

The user trial involved 27 participants, with all of them having at least a basic knowledge of using a computer. In order to ensure that the users would have something to do during the 'usability' phase of the trial and to ensure that contexts would occur in which different aspects of the prototype could be utilised, each user was asked to work through a given set of tasks (see Appendix C). The rationale for each stage of user activity is shown in Table 4-3.

Activity	Rationale
Search for contact details of the other participant.	Involves the use of a local application with mildly sensitive data.
Establish an IM session and exchange initial greetings.	Involves keyboard and/or voice interaction.
Each user opens a web browser and searches for hotels in Las Vegas. Each user should find 3 options.	Involves the prolonged use of an unsecured web browsing session.
Users discuss the options they discovered via IM and agree a choice.	Returns the user to IM and provides a basis for a reasonably involved discussion.
Users visit a secure 'travel agent' site, and provide the name of the agreed hotel plus other booking details.	Involves the use of a secure browsing session (thus demanding stronger authentication assurance from NICA) and gives the users a basis for entering keyboard information.
Each user opens a local 'expenses' file and record the estimated costs of the trip.	Involves the use of a sensitive local file and requires keyboard entry.
Each user creates a Word document that presents a biography statement, and types a standard disclaimer that permits the conference to post the details online.	This ensures a prolonged period of typing activity in a less bursty context that IM. The aim of getting the users to type a biography is that it allows them to type free text on a topic that they should be able to say something about. The aim of getting them to type a disclaimer statement is that it will represent known text in which we can ensure representation of profiled keywords.
Email the document to the other user as an attachment for checking.	Involves the use of a further application context (i.e. email).
Each user checks and edits the other's document as appropriate and sends it back.	Continues the use of Word and email, and thereby prolongs the overall session to give Face and Keystroke metrics more opportunity for testing.

Table 4-3: User trial activity and rationale

At the outset of each trial session the participants were briefed about the purpose of the experiment and what each phase would involve. Each user used the same device in both phases to mitigate any effect on the biometric samples from the device hardware.

4.3.2 User Assessment of the Prototype

The results from the evaluation overall demonstrated a positive opinion for the authentication system with 92% of the users considering the proposed system offered a more secure environment in comparison to traditional forms of authentication (Figure 4.7).
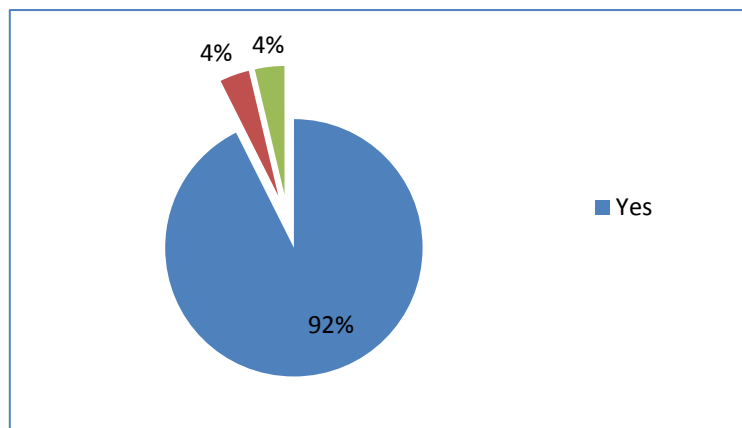
Figure 4.7: Did NICA provide a more secure environment?

The users were also asked to evaluate how convenient the system was in a scale of 1 to 5, the results of which appear in Figure 4.8. Although the responses were mixed a slight skew towards the system being convenient exists on average. It is worth noting that through observation of the evaluation, participants' opinions were affected by the delays that occurred on the system while trying to manage all the processing. These occurred in some cases where applications might have been initialising

concurrently giving extra overhead to the system with NICA running on the background. A real system would not have such significant delays.
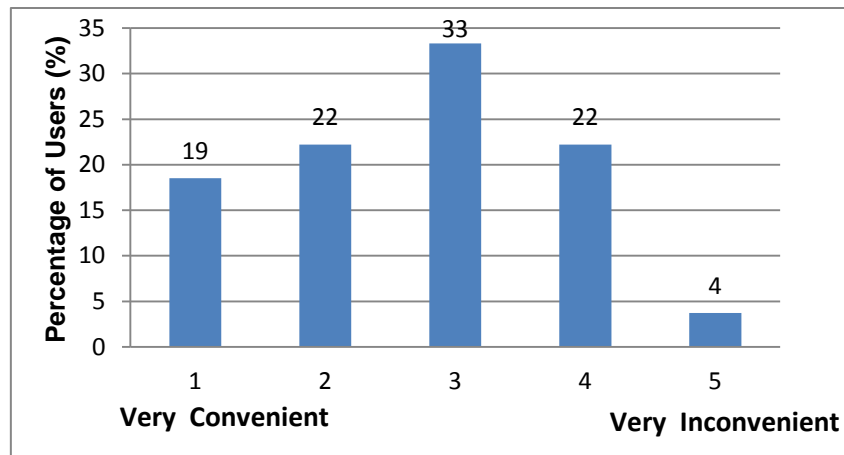
Figure 4.8: Perceived convenience of the NICA prototype

Furthermore the above views were also affected by the transparency of the system which was not always ideal. The lack of robust algorithms caused a lot of transparent authentication requests to fail prompting some of the users with more intrusive requests that they would normally get. In order to mitigate that a manual trimming of the threshold was taking place during the experiment in order not to allow the lack of accuracy from the biometric algorithms to affect the performance of the actual system. Nevertheless what also happened in the experiment was that the scenario included access to a number of protected services in a small amount of time causing even more intrusive requests to occur but not necessarily having the chance to build the required confidence to user while authenticating them transparently. Unfortunately, it was not possible to have the participant's use the system for a prolonged period of days, so therefore the experimental study had to artificially include a number of steps to fully evaluate the prototype. It is likely this artificial

environment resulted in a more negative attitude towards the system than what would have occurred in practice. The responses of the participants with regards to the transparency of the system are illustrated in Figure 4.9.
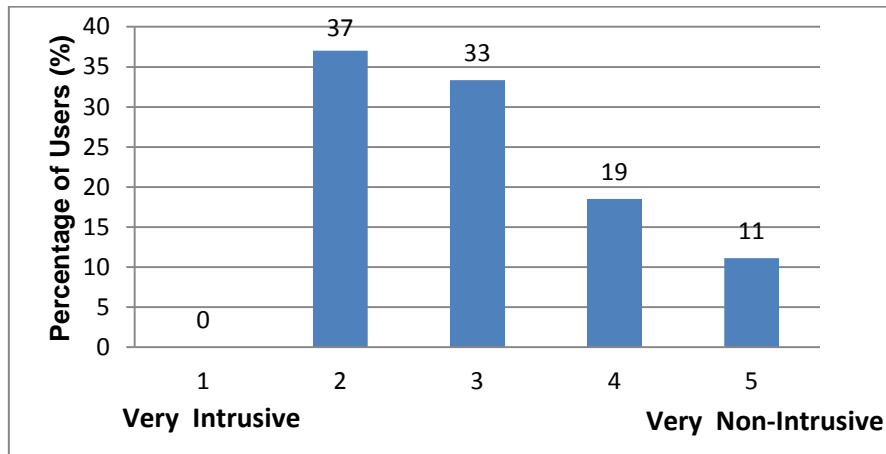
Figure 4.9: Perceived intrusiveness of the new authentication system

With regard to the individual techniques that were utilised, a slight preference existed towards voice verification and keystroke analysis (Figure 4.10). From verbal feedback from participants there was a strong preference to techniques that did not require much user interaction or be very time consuming. As such, cognitive responses as an intrusive means of authentication were not very popular. The same occurred with face recognition as the algorithm utilised required more time than other techniques to perform the authentication and also they had to keep facing the camera until a sample was captured. At the same time voice verification (in its intrusive form) appeared to be more preferable as the user only had to repeat a small phrase and had a very quick response from the NICA server. Although many of the above were affected by the robustness of the algorithms utilised it still provides an insight that users prefer to have a higher level of security with the least overhead

in their interaction. Usability and convenience were stronger preferences than security.
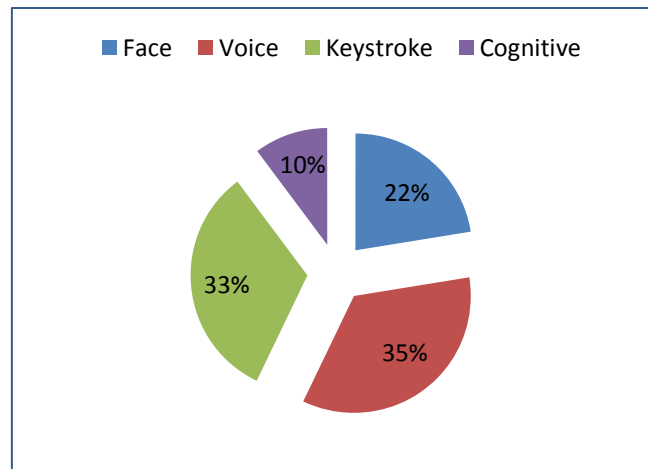
Figure 4.10: Participants preference towards the authentication techniques utilised

Regardless the aforementioned problems regarding the convenience of the system, the majority of the users – 70%, registered a preference to the use of transparent and continuous authentication as a protection mechanism (Figure 4.11). Although many of the participants suggested that the requests were too many the idea of being constantly protected and specifically having extra security for highly sensitive information was very appealing to them. As such, 81% of the users said that they would use such system in practice as they would feel more protected than using traditional means of authentication. Although the remaining 19% stated they would not use it, their justification was that although they believed the system would offer higher security they do not perceive that their current use of their mobile device actually required a higher level of protection as they do not store or access personal information. This was actually an opinion that had arisen on a number of occasions during discussions with stakeholders. A body of users exist for which the mobile

device is only and will remain only a telephony-based device. They have no desire to use the device for any other purpose and as such do not perceive the need for additional security.
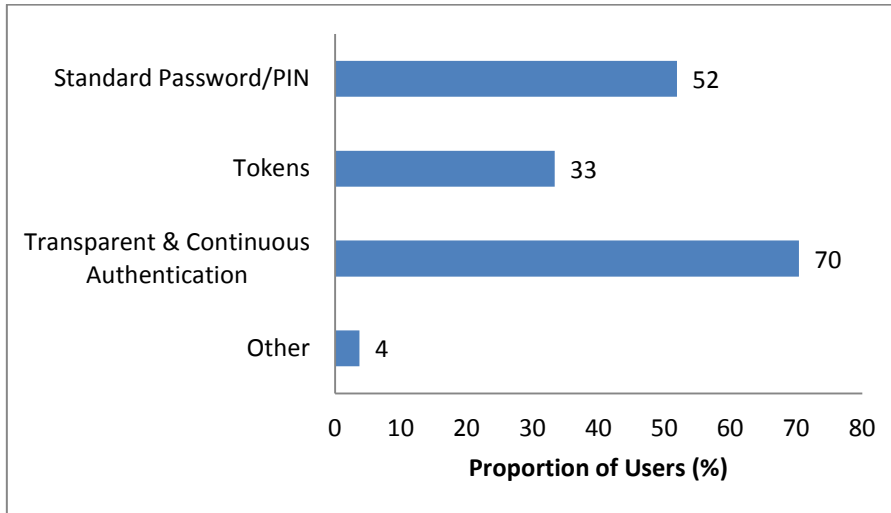
Figure 4.11: Participants authentication preferences

When the evaluation came to the participants acting as impostors it must be noted that although a number of users were not very positive when acting as the authorised user, when it became more positive was when they saw the performance of the system reacting to an impostor. When the users where asked where the system managed to recognise them and locked them out in a timely manner 81% said yes. When the users where asked on how secure the system was their answers were very positive with the majority leaning to being very secure (Figure 4.12).
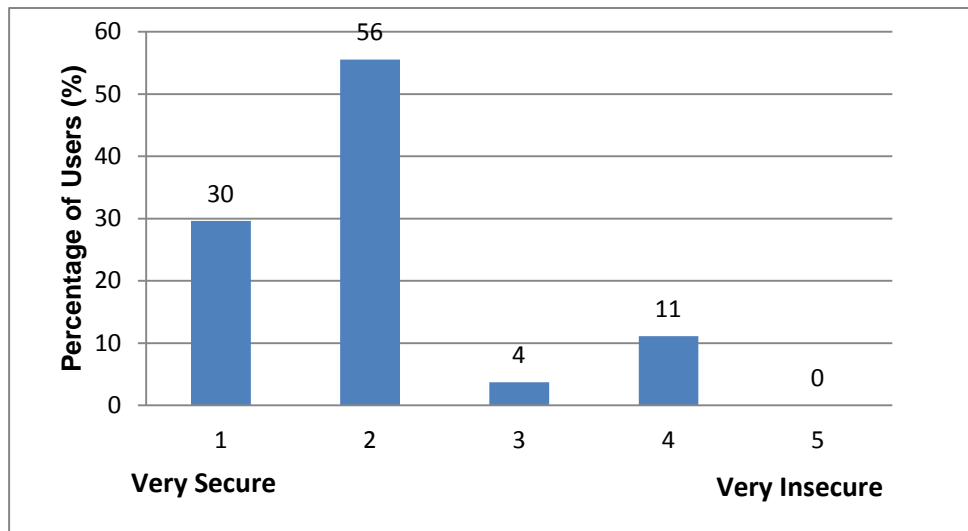
Figure 4.12: The security of the system against impostors.

In a question asking them to assess how much of the personal information they managed to access the majority of the participants indicated that they managed to access little or no information (as illustrated in Figure 4.13). It is also interesting to note the contradictory nature of participants. Although some users found that continuous authentication provided too much protection at the moment, another set of participants felt that NICA should have identified impostors when simply accessing applications such as Internet or Windows Explorer and no sensitive data. At the same time there was an obvious variation to what people perceive to be personal and how tolerant they are of the security methods. Nonetheless, what was apparent from the experiment overall is that (perhaps unsurprisingly) people would like to have the highest level of protection with the minimal interference from the system and the higher convenience.
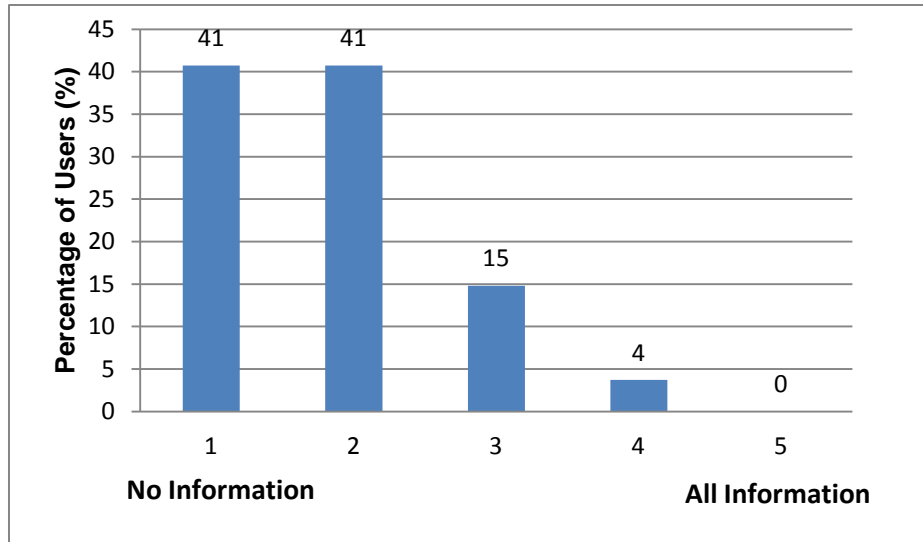
Figure 4.13: The level of information accessed before the system locks down

4.4   Conclusion

The evaluation of the discussed framework clearly demonstrates the strengths and weaknesses of such system. It is evident from the findings that such a transparent and continuous system has real merit and a large proportion of users feel it would provide the additional security they desire for their mobile devices. Unfortunately, with almost half of the world's population having a mobile device, it is difficult to establish an approach that satisfies all users. Therefore the consideration of the latter and the development of such flexible approach that can utilise a variety of biometrics and other authentication techniques and through a series of operational settings can vary the level of security both transparent and intrusive is beneficial. Through this flexibility it is hoped the majority of users will be able to find a suitable mixture of settings and techniques they prefer and desire.

Whilst the prototype and subsequent evaluation has illustrated a number of key findings, it is important to highlight that if the system was operating within

specification (i.e. the performance of the biometric techniques was good in the transparent operation and the operational performance of the server was managed rather than everything operating for a single server) the nature of the transparency would mean few users would ever realise or experience intrusive authentication. During the evaluation, however, the framework was configured to perform authentication on a more frequent basis than would normally be the case in order to ensure that sufficient judgements were made during the trial session. This was done in order to ensure that participants would see the full extent of the system in operation, but the consequence was that participants encountered more intrusive authentication requests than would normally be expected. In some trial sessions, these requests were too frequent and time consuming, and participants therefore acquired a more negative impression of the prototype.

The above issues were weaknesses so much of the implemented framework and the core process that it involves as well as of the biometric techniques. Concerning the former there were a number of issues identified during the evaluation trial which indicated that a more efficient approach is required in order for the Alert Level algorithm to operate more effectively. In many cases the way that the system worked would mitigate any good performance of the user due to the degradation function and the lack of timely dynamic decisions as these were not properly pre-analysed in the utilised framework to better fit particularly the time constrains of the evaluation. Furthermore the biometric techniques as they were techniques designed for explicit intrusive authentication lacked their actual performance when tried to apply them transparently or intrusively.

5   Modelling NICA

The implementation and user evaluation of NICA framework gave an insight as to the security effectiveness as well as usability under real usage scenarios for authorised and impostor users. Given the limitation that were introduced during the practical evaluation in regards to the restricted time that events required to take place and performance of biometric techniques it was considered imperative to perform a further investigation of the framework utilising simulations under different type of conditions in order to be able to test the performance of the approach further. A simulation environment would provide the opportunity of testing the framework under different conditions and removing the effect of the poor performance of biometric algorithms that are independent of the framework. The following sections will describe the series of simulations that took place to evaluate the performance of the NICA framework and the data used.

5.1   NICA Simulation - Methodology

5.1.1   Data

In order to be able to simulate NICA the production of appropriate data was required. In order to represent real-life data as close as possible, mobile activity data were sought in order to have a basis for the amount and type of usage. These type of data would be the basis regarding the number of events that could be generated within specific time periods that could subsequently be generating biometric samples and therefore feed the authentication algorithm.

For this purpose the MIT Reality Dataset (MIT Human Dynamics Lab, 2004) was utilised. This MIT database is a collection of data that has recorded the mobile phone usage of 106 users over a period of several months including timestamps of when interaction such as voice calls, SMS and launching of application occurred. Utilising this database it was possible to base the timed events to possible sample capturing. This would give a close representation to a real-world scenario in regards to the operation of an authentication framework such as NICA that relies on the capturing of samples as a result of the user's interaction with the device. Each time an event occurs depending on the NICA configuration and the device capabilities this could link the capturing of at least one sample. Although the dataset was a strong basis for its use within the framework simulation it must be said that in a real situation if NICA was applied more samples had the potential to be captured. As MIT has only recorded the launch of a specific operation which in this simulation was linked only to one sample being generated, in reality after launching an application a user would continue in most cases having more interaction and therefore causing the generation of far more samples than what is available here. For example, MIT has recorded the event of launching a web browser which could lead to e.g. the capture of a face sample as the user is looking at the device. Given though that the user will possibly continue to navigate to sites or type search terms or write an email, all these interactions carry the possibility of more biometric samples to be captured. Furthermore the data set represents data captured in 2004 and therefore the device capabilities were more restricted than today as well as therefore the use of the device. This further poses an argument that capturing of samples would occur in more frequent basis than the current data set. As a Nokia study reports mobile users

cannot leave their device alone for more than 6 minutes (Digital marketing university, n.d). The current dependence of business and communication upon mobile phones including even in things like social networking and gaming suggests the increased average capturing of samples given the phone interaction compared to the simpler use of the device that MIT has recorded. For the purposes of this simulation only the recorded events were used. Although artificial methods could be used to add extra events this was not applied at this point since the basis of using the data in the first place was to avoid artificial generation of mobile usage. This of course limits however the amount of samples that could be utilised per hour and therefore limits the operation of the framework causing possibly the more often leading to L3 that waits on next input by not finding samples available.

5.1.2 Data Extraction & Production of Data sets

In order to produce the data sets required for the simulation it was important to identify how the data can be used. As a first stage the data from 100 users were used – 6 had to be omitted for the solely purpose of missing some of the information required for the automatic extraction. Using Matlab as a processing environment a number of scripts were written in order to extract the events generated for each user as well as the timestamps of these events in a usable format (Appendix D).

Given that each user will have a very subjective use of their device an initial analysis was made in order to identify whether the different users could be classified based on the extend that they were making use of the device. Since the operation of NICA framework relies on the presence of samples having a classification based on usage levels of the device and therefore the dynamic of having samples being generated

and the frequency of those, would be useful to better assess the performance of the framework under different scenarios. For this purposes the activity of each user was split based on each hour and 2 metrics were calculated:

- o The average number of samples captured per hour
- o The intervals between 2 subsequent samples

The first metric would help to classify users regarding the usage of the device whereas the second could be useful for the same purposes but could also be used as an insight as to how the framework could be getting affected by large spawns in sample capturing. It could inform the time window that the Alert Level process uses to be triggered or to seek for valid samples. Nevertheless as aforementioned there is always scope in real configuration of NICA to provide for more samples.

A further basic analysis was undertaken to see whether specific time periods were characteristic of the user so that could be an aspect to consider in the NICA framework. As such the time and periods during the day were considered in order to identify average usage of the device (with simple means) but there was no characteristic output of such analysis. Given the subjectivity in the use of the device each user had variability of that usage in different hours with no indication as to usage periods that could be useful in the context of this research.

An analysis of the above 2 aforementioned metrics was completed and averages across all hours for all users were produced. At this stage from these averages, the hours where activity would generate less than 6 samples - which would mean with the highest time span 1 sample every 10 minutes, were removed as it was

considered that it would not provide enough data for a characteristic use of such framework and it would affect the analysis at this stage as a lot of hours will even generate 0 events as the device is not always going to be in use. Is it quite apparent that NICA relied heavily upon samples being present for the mechanism to have any significant effect or be operating in a transparent mode. In very low usage it would operate closer to a time locking mechanism such as PIN protection provided in current devices and as such there was no scope in evaluating this here as the objectives were the evaluation of transparency. The averages of the metrics selected were produced across the users which however showed very similar results with no particular differentiation between users as to their activity during the hour or between accessing of different services and data. As such showing that there were no useful outcomes to be found solely based on the metrics extracted that could assist in determining the level of usage of particular users – e.g. a high usage user versus a low usage user.

As an outcome of the above analyses it was considered that although the use of a specific biometric technique will be dependant somehow on the user and the device, the actual level of usage within a specific timeframe does not carry the same dependency. Furthermore for the purposes of this simulation the profile of a particular user is not important as a heavy user may have high activity for an hour and none for another and vice versa for an infrequent user. What is important is to be able to evaluate the operation of the framework under specific time periods based on the number of samples generated rather than particular users. The specific activity or user was deemed irrelevant. As such all data were collated with the

individual user aspect removed and the data were split again this time based on the levels of activity per hour. Three distinct data sets where created:

- **Low Usage** : Set of hours with x number of events in the range of $6 < x < 20$

- **Medium Usage** : Set of hours with x number of events in the range of $20 < x < 40$

- **High Usage** : Set of hours with x number of events in the range of $x > 40$

As expected the majority of the hours fell into the Low Usage category. As it was later realised during the simulation phase the amount of hours for medium use but furthermore for high usage were far too many given all the simulation permutations used resulting to too time consuming simulation with not much added value in relation to a smaller dataset. As such only 765 hours was used for all levels of usage to have a common basis. The number of hours represented in each category is listed in Table 5-1.

	Total Hours of Usage available	Total Hours of Usage used
Low Usage	30104	765
Medium Usage	4436	765
High Usage	765	765

Table 5-1: Hours produced based on levels of activity

These data sets form the basis for simulation representing the timed events at which a biometric sample can be generated. For each of these events the sample captured could represent a different biometric technique depending on the type of activity on the device and the configuration that the framework would have. Since this

information was not available given the data at hand, an artificial generation of the type of sample that would be generated at each time event was introduced. However rather than specifying a specific technique that could have been used, what was generated is the confidence level linked to a specific technique. As the simulation is not concerned with specific biometric algorithms rather than looking at how the framework operates, the information required was confidence levels in order to be able to calculate Integrity update values and Alert level decisions. For each of these confidence levels a specific technique or biometric algorithm could be linked to each of them in a real life scenario depending on their performance. As such for each timed event a random selection between the four confidence levels (B0, B1, B2, B3) used in the framework was made. The use of artificial data at this point is not believed to affect or bias the operation of the framework as the confidence levels are randomly assigned with a fair distribution across them. Given also the large number of the hours there is an expected fairness in the spread of confidence levels. Although in a real life scenario this fairness is not a requirement and is not a necessarily expected result as it is largely dependent on the use of the device by a particular user as well as the configuration of the capturing mechanism, for the purposes of this simulation at least it ensures that there is no bias towards low confidence or high confidence techniques.

Since no real samples were existent in order to be able to run biometric algorithms, the other requirement for the simulation was the ability to have an authentication decision for each event. Although not all events would be selected as part of the simulation as that would depend on whether their times would fit with the trigger of

the alert level algorithm, they all needed that decision in case they were selected for authentication. On this occasion applying an artificial generation of authentication decisions, values between 0-1 were randomly generated and linked to each time event. This decision would represent the outcome of a biometric algorithm in case the specific sample linked to this event was selected from the algorithm. This was not a type of information that such simulation could acquire otherwise.

Two data sets were created with this technique: a set of data for the authorised user with random values above a threshold of 0.5 and a set of data for impostors with random values below the same threshold. These two data sets were created for each category of usage. In order to be representative of a biometric based authentication, a further processing of the data introduced also in the authorised and impostor data set the FRR and the FAR respectively for each confidence level. As no specific technique was used in order to be able to utilise published error rates of the respective techniques, the error rates were introduced based on the error rates defined by NICA to represent each confidence level. Since NICA does not define a specific percentage but ranges of error rates of techniques that could be represented in each confidence category, 2 different data sets were produced. One to represent the best case scenario with the FAR and FRR in the minimum setting, and a worst case scenario with the FAR and FRR in the maximum limit of each confidence level. The limits of the error rate are depicted in Table 5-2.

	EERs			
	B3	**B2**	**B1**	**B0**
Best Case EER	0%	2%	5%	10%
Worst Case EER	2%	5%	10%	20%

Table 5-2: EER introduced in data sets

Similarly here the artificial generation of values does not create any positive bias on the simulation. Given that pass or fail values are created with incorporating representative EERs it closely represents a real scenario and NICA specification. Arguably in a real life scenario the actual values maybe higher for an authorised user and lower for the impostor. That would actually create a disadvantage for the simulation as the fusion techniques as part of their decision algorithm take into account this output value of each biometric algorithm in order to reach a positive or negative conclusion. However given that the samples in real life are captured transparently it is expected that some of the samples would not be as good as others due to e.g. the user not explicitly posing in front of the camera, environmental conditions introducing noise in voice samples due to the nature of a mobile device. That would mean that unless there is a quality check for the use of a specific sample, the output decision that defines a match of the sample to an identity might not have such a high value. Given all the above the random selection of values closely represents a fair representation of actual outputs to the extent that that is possible.

As a result of the data production the datasets produced were a best and a worst case EER for each of the low, medium and high usage profile data so both cases can be tested under each usage frequency and denote and differentiation.

5.2 Simulation & Results

The original NICA framework was written in VB.NET but for the purposes of these experiments the simulation code was developed in Matlab as a more efficient simulation environment. The simulation followed the same principles as would the framework in a real time scenario with the exception being that the operation was tested over the period of only an hour. As such each set of results represents how the integrity of the system would change over the course of an hour considering that at point 0 being the start of that hour the integrity of the system equals to 0. The simulation would start at time 0 considering that is the time the first sample would be available rather than the actual beginning of an hour as collected from the MIT database. The decision was made on the basis that this would mean that the device is at use.

The operation of the NICA framework is based on the concept of transparency and as such the focus was on the transparent levels of operation. Given that in the occasion of misuse from an impostor or bad conditions and error rates for the authorised user the framework is led to the intrusive stages where explicit authentication is taking place, the focus of this experiment did not consider any failure after that. Meaning that in the event that an authorised user reached the intrusive stage, the simulation would assume successful authentication and reset to Level 1 of the AL algorithm whereas for an impostor it would lead to lock of the device and consequently end the simulation for that hour. Given that at an intrusive stage a B3 technique would be used, that was accumulated in the operation and

thus the integrity would be raised for the authorised user or drop for an impostor accordingly.

The main objective of the simulation was to record and evaluate how the integrity level and therefore confidence in the user would vary across each hour given different usage and biometric performances. Furthermore to assess how this would affect accessing of protected services.

5.2.1 Determining Time Windows

Further to the data sets created, a further aspect that needed to be considered was the time variables of the framework. These are the timing at which the Alert Level mechanism is triggered (AL time window) as well as the time period of the degradation function where there is an automatic drop of the Integrity Level of the system (IL time window). In the original NICA specification these are loosely determined as AL window being 10-25 min and IL being 30 min for high users and 50 for infrequent users. These times appear good for usability but quite insufficient for security. This level of time settings could be more appropriate possibly during periods of inactivity or for users that do not use the device very often or for highly secure services. On such occasions the authentication requirements could be lower and therefore more often authentication would be possibly too much. Also for the purposes of this simulation, since time periods of 1 hour is being assessed, it would not be of much purpose to utilise these kinds of settings.

Also building upon the experience of the practical evaluation, where a number of tasks required the accessing of secure services and sufficient activity, smaller times

were required in order to be able to build such confidence that accessing secure services would be done in a transparent fashion or to be able to detect the unauthorised use of the device. During the evaluation of NICA these indicative values could not be kept as the timing restrictions of the user evaluation required a far more timed compacted approach and thus far smaller time windows were used. Given that the users were having constant interaction with the device and therefore continuously generating samples it was possible to set lower time windows and check the operation of the framework. This could be easily scaled given a longer period with less interaction as the operation would be similar and the only thing changing would be the time of events.

An investigation was required to establish the effect of these timed events. The matter of the Alert Level being triggered too often for example could lead to exaggerating authentication. This may result to largely intrusive operation if the samples are not available as the framework would regularly reaching L3, which could become problematic in the occasion of occurring high FRR. Although the latter establishes the security of the framework it needs a balancing approach relevant to usability. The other time variable which is the periodic drop in the Integrity Level to mitigate against any misuse opportunities during periods of inactivity, low usage or lack of high confidence biometric samples, also requires consideration. A big time window could lead to maintaining high integrity without any activity taking place and therefore concerns of misuse where a small window could lead to intrusive requests for accessing protected services as the Integrity Level would not have the opportunity to being maintained for long after successful authentication.

Within the space of this simulation given that periods of one hour were being used there was the requirement to also use smaller time windows. Furthermore the use of 30 or 50 min for the Integrity degradation seems to be a long time for it to have a significant effect on the security as the timing is too far apart given the specified drop of 0.5. Given the occasion for example that an authorised user may have reached a IL of 4 or 5 and the device fell into the hands of the impostor it could take more than 50 or 100 minutes to restrict access to highly secure services. As such a set of different values was created to test their effect on the framework but as the different combinations could be endless, only a subset was tested trying to keep a timing relative between the two variables was kept to represent the original specification of the framework. As such a scale was used based on the indicative values considering the AL at 20 min and the IL drop at 50 and then the rest between the 2 timings by halving the time windows by a factor of 2 each time. The time windows presented in Table 5-3 were used.

Alert Level (AL) Time Windows	Integrity Level (IL) Time Windows
2	5
5	12
10	25
20	50

Table 5-3: AL and IL Time windows used in simulation

Given the current use of devices these are times that could be justified as appropriate. As research reports, during downtime, 91% of employees check their email every 6-12 minutes (BasicITSolutions, 2013). Average number of times a user checks their phone is nine times an hour which could translate to 6-7 min per hour

and that this may increase to once every six seconds for 'highest frequency users' (Dailymail.co.uk, 2013). Although these numbers may not always translate to full use of the device they could be characteristic of device access and possible sample capture.

5.2.2 Authorised User

During the simulation for each hour of use a number of variables were recorded to accumulate the operation. The primary focus was how integrity would vary across each hour as it is the means to determine how secure as well as usable the framework is.

The initial sets of simulation focused on the high usage profiles with best EERs as they were expected to show the framework operating at its optimum performance given the available data. The performance of NICA for an authorised user profile across all hours of high usage for each set of time windows can be seen in Figure 5.1.
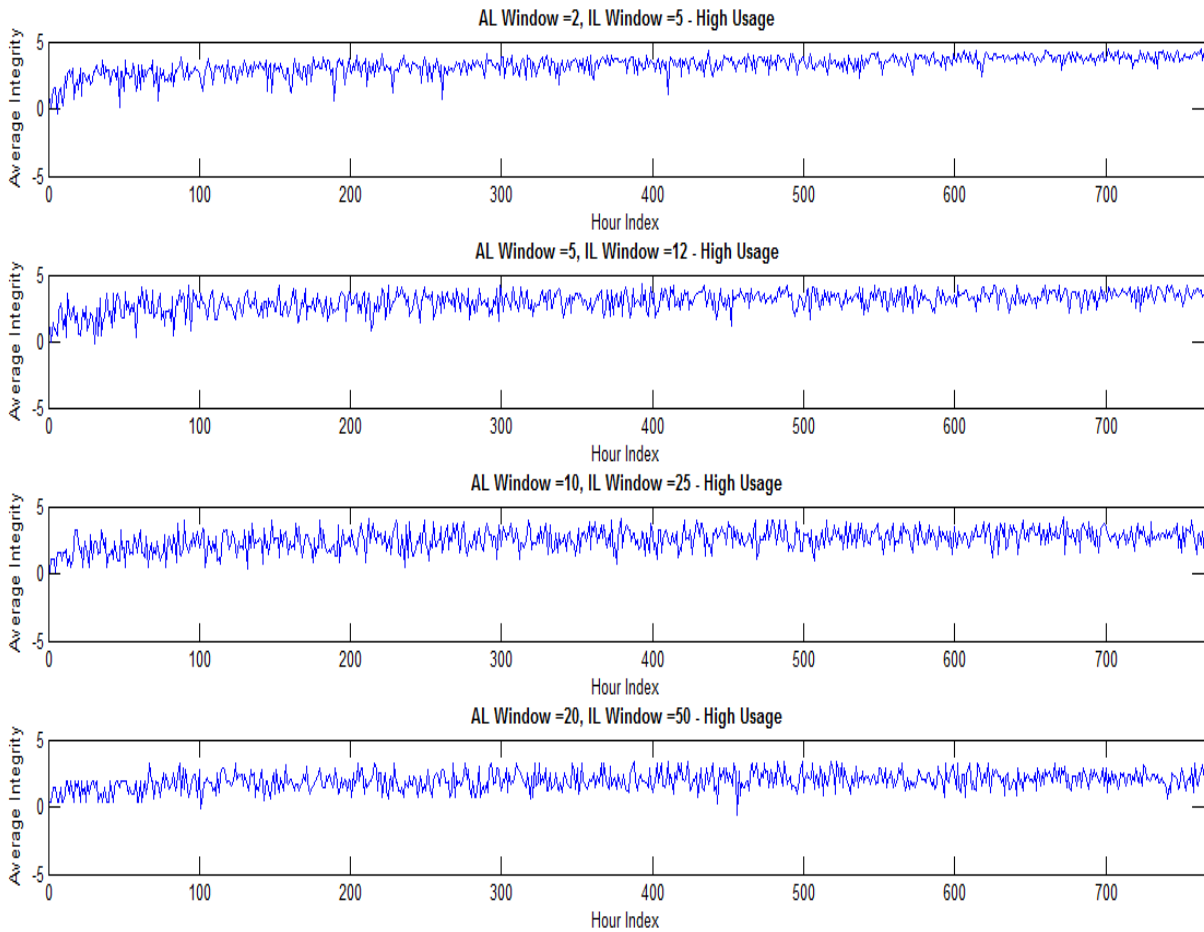
Figure 5.1: NICA performance on different time windows for an authorised user

It can be seen from the graphs that the framework manages to maintain an average integrity above 0 with minor exceptions close to 0. For some hours the average integrity is quite high such as above 4, which means that the usability of the framework could be quite good in many cases. What can be noticed also is that the framework performs better with the smaller windows rather than larger one. This effect can be explained as in the former case authentication occurs far more often and even dropping the integrity often does not have a major effect on the integrity so that it cancels the successful alert level operation. With frequent authentication in place even if samples are not always available to the AL mechanism or the

techniques available may be of lower confidence, the framework still manages to maintain a fair level of trust. Although utilising small windows could result in samples not being available and thus having the effect to continue to dropping integrity due to the degradation function while the AL is e.g. waiting for a new sample to come in, it appears that this effect is counteracted. The same could occur or be further reinforced with high false rejection error rates that would make the AL mechanism to be moving to the next levels and reducing integrity. However since in this case the best error rates are used it is unlikely for this to be affecting the results. On the other hand when having bigger time windows (like AL-25 & IL-50) seems to be an effect of having only a few authentications occurring per hour and as such the integrity is unlikely to have the opportunity to be raised. The degradation function will only lower the integrity once so that is not quite affecting the average here. It can be seen that these 2 parameters play a significant role on how NICA will be able to operate regardless of the biometric techniques used and as well as the usage of the device.

Given the variability across the hours it is not trivial to determine the best performance across the band for all windows. As such the overall performance across all hours in regards to the average integrity can be used. This can be seen in Table 5-4.

NICA Average Integrity for Authorised User

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
NICA Best EERs	3.237	3.0007	2.5353	1.941
NICA Worst EERs	3.2266	3.0356	2.5422	1.9475
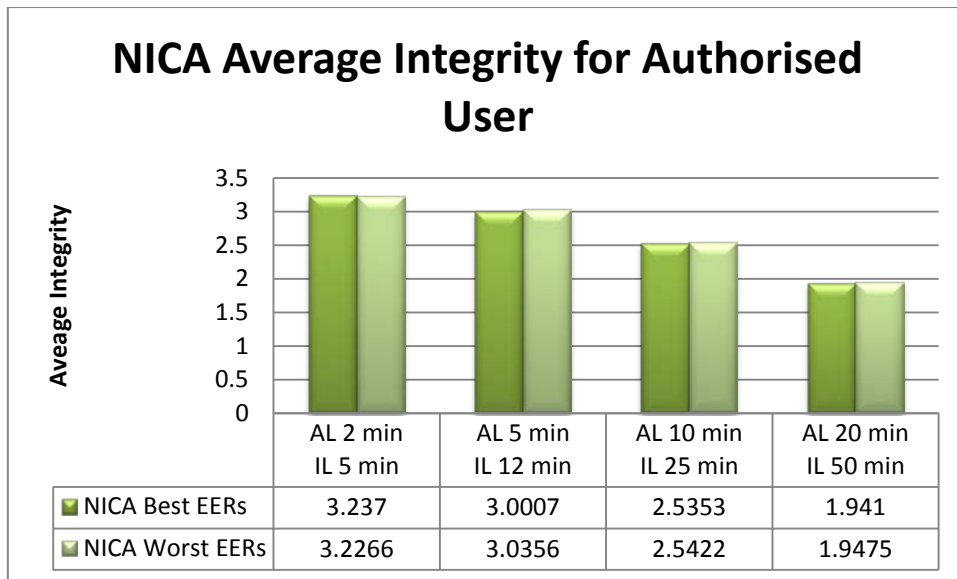
Table 5-4: NICA Average Integrity across all hours based on EERs

It can be seen that the average values show that again the smaller the windows the better the framework performs by a noticeable amount (close to 1.3 degrees of confidence between the edge windows). Given the large number of hours and the integrity averages it appears that this performance is a representative result of the framework performance. Although there is variability regarding the amount of activity during each hour and the particular timings of that activity and therefore captured samples that are factors that performance would be dependent upon, as had been seen in Figure 5.1 there is a clear distinction where the framework operates better. What can also be seen from the table is that there is not a significant difference between the Best and Worst EER scenarios. Actually the worst EERs provide a slightly better average which is insignificant however it could be explained due to the fact that in case of a failure the AL mechanism would likely at some point reach an

intrusive stage and therefore there would be a force of a more confident technique and subsequently a higher increase on the integrity.

To get a closer look an analysis was undertaken to explore how the average integrity changes based on the number of samples used and therefore the amount that authentication is taking place each hour. Figure 5.2 demonstrates the integrity in relevance to the number of samples used per hour. The top graph in each subfigure shows the average integrity across each hour of use. The mid graph represents the amount of samples used during that hour during transparent operation whereas the lower graph shows the number of intrusive requests that have occurred on the hour. The hours are sorted based on the number of used samples. As the hours are independent of each other in this simulation this does affect the representation of the results.

AL Window =2, IL Window =5 - High Usage
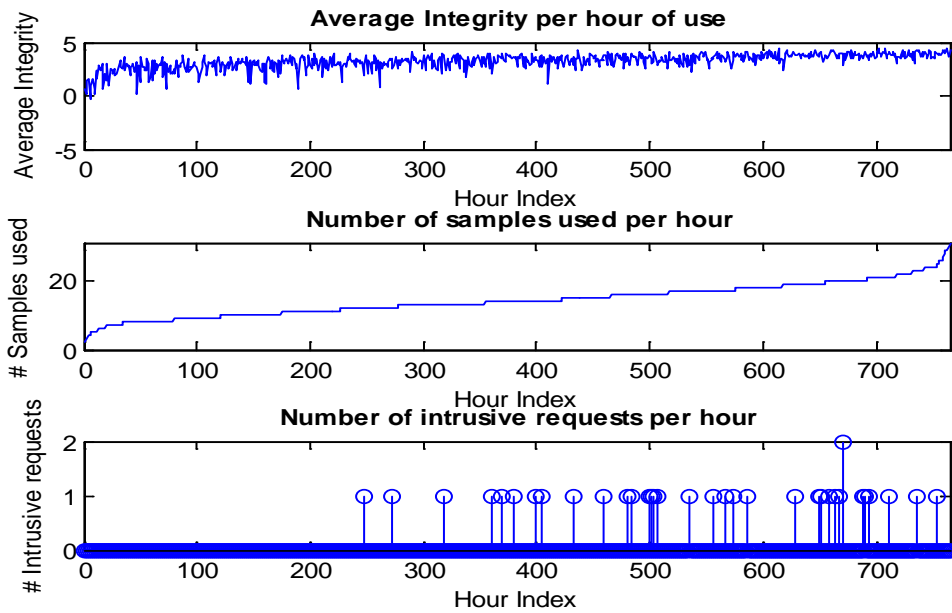
AL Window =5, IL Window =12 - High Usage
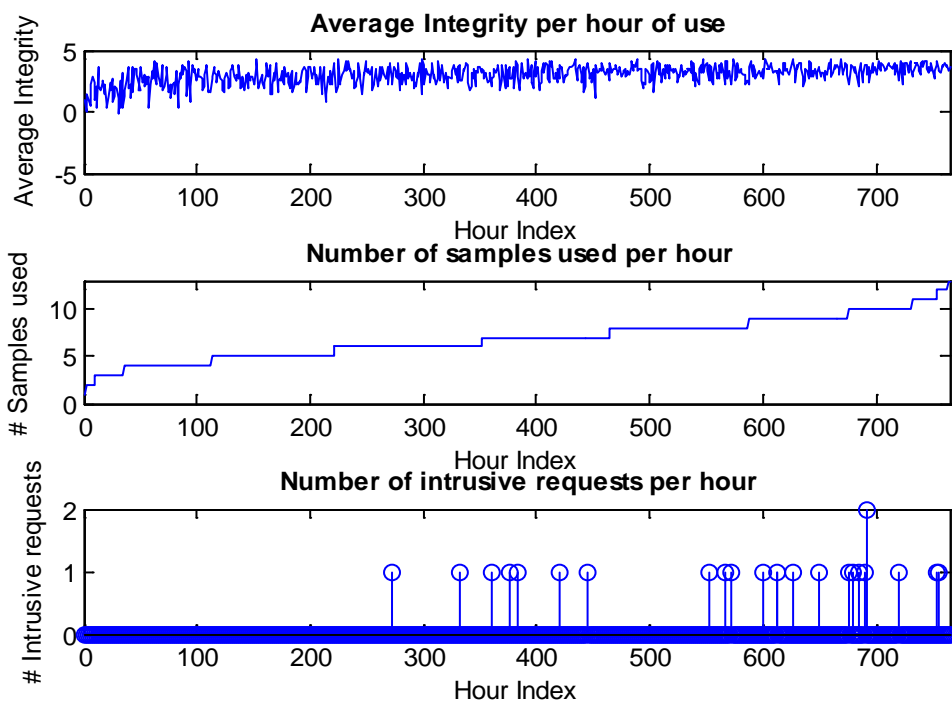
AL Window =10, IL Window =25 - High Usage
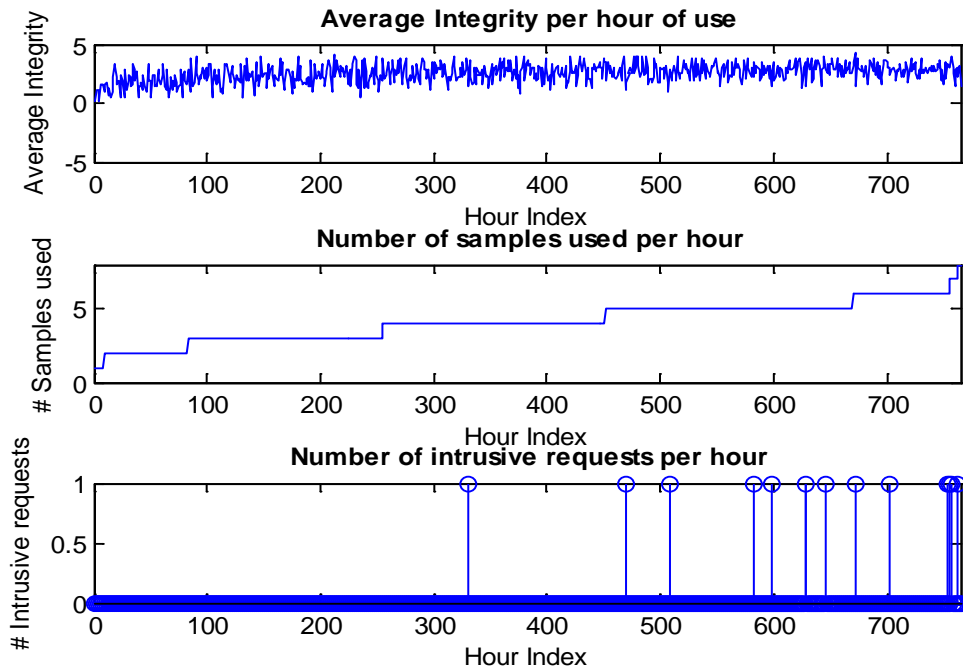
AL Window =20, IL Window =50 - High Usage
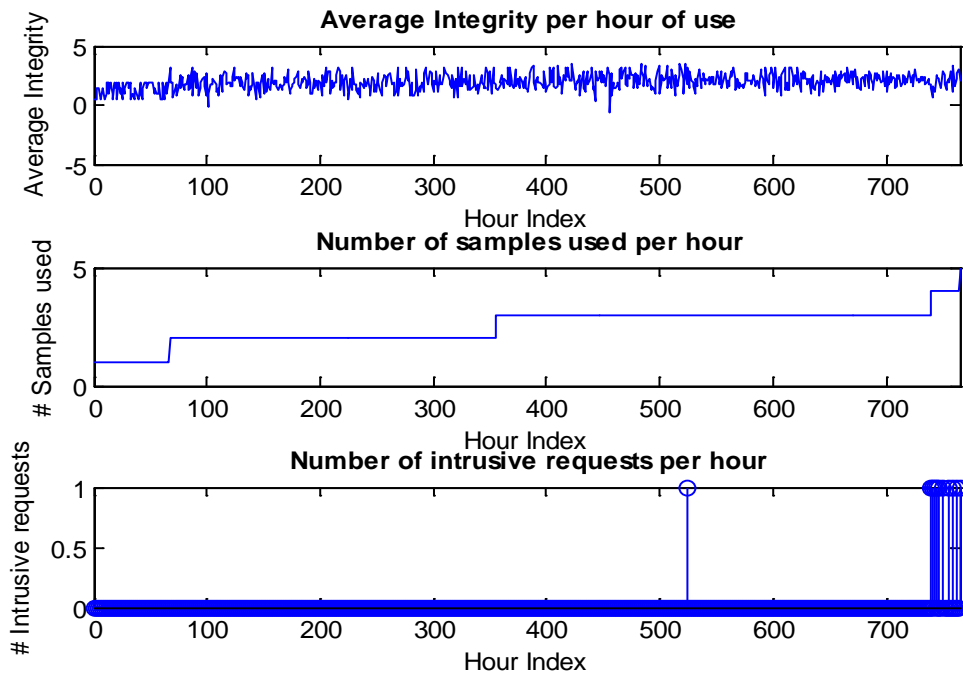
Figure 5.2: NICA Performance for Best EERs

As can be seen from the graphs the number of authentication requests on average has a positive effect on the integrity of the system with a noticeable upwards graph particular for the small windows. It can be noticed that for smaller time windows the number of samples likely to be utilised is more variable from the larger time windows which may reach the use of up to 8-9 samples and therefore a far more subtle change can be seen in integrity. What is also worth underlying is that in the smallest time windows it appears that the effect of frequent authentication seems to cause a more stable average integrity compared to the use of less samples. Although it is uncertain as to why this is occurring it is likely that in the event that samples are always available to be used there is a constant maintenance of the integrity whereas if samples are not available the AL will be likely waiting for a long time at L3 for the next sample whilst at the same time IL is dropping or be prone to a FRR which would lower the integrity of the system. At the same time, larger windows allow for less authentication requests during the hour and therefore the finding samples in good timing are therefore very few.

Regarding the transparency of the system as can be seen on the lower graph the amount of intrusive authentication requests that occur during the hour are minimal varying between 0-1 with the majority being at 0 and with only two occasions of hours with 2 intrusive requests. It is also apparent that the more samples being used -which in this occasion is a matter of timing of events and availability, the likelihood of an intrusive request increases. This is logical as the possibility of a false rejection event occurring is higher. As transparency has a dependency upon the performance of biometric techniques it is likely that a real system will be more prone to worst

performance, nevertheless given the representative EERs used, it appears that the framework has the ability of dealing with this failure quite well maintaining a fair level of transparency. As aforementioned the average performance of NICA shows that even with worst case EERs the framework still performs at the same level. To examine this further Figure 5.3 represents the intrusive requests for Best and Worst EERs as means of comparison where it can be seen that Worst case EERs increase the occurrences of intrusive requests but still minimally reach the maximum of 2 requests per hour showing that the framework deals with these failures. This further confirms the fact that the user evaluation was largely affected by the high EERs occurring due to poor biometric algorithms rather than the framework itself.

AL Window =5, IL Window =12 - High Usage
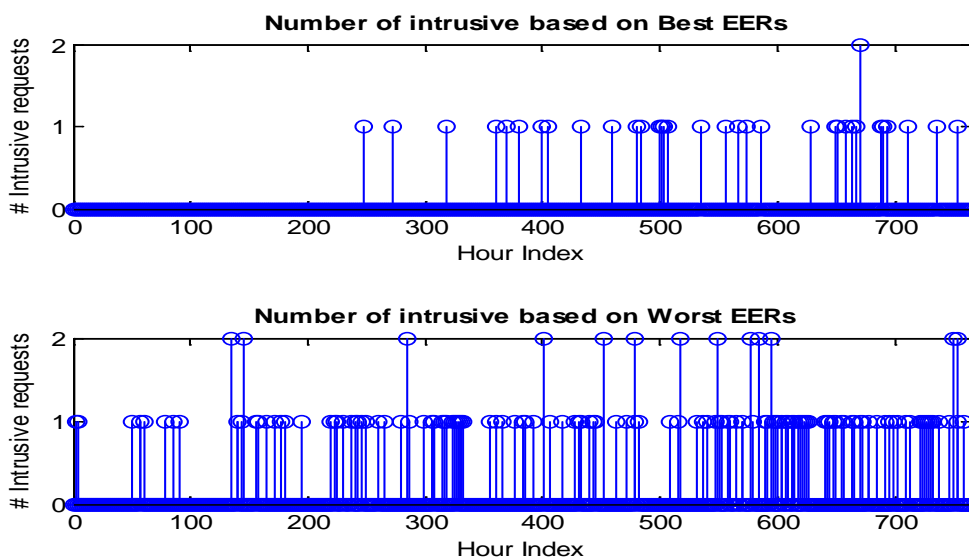
AL Window =10, IL Window =25 - High Usage
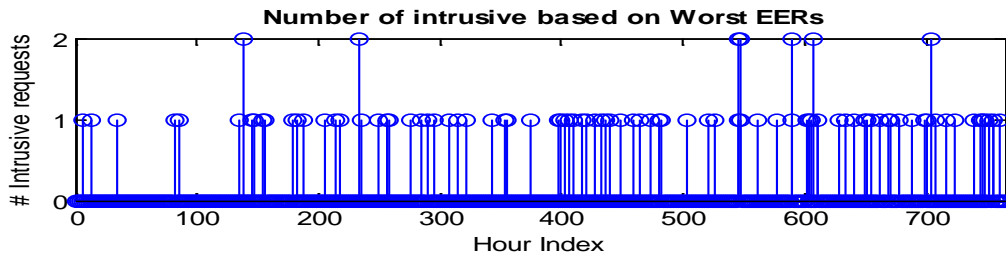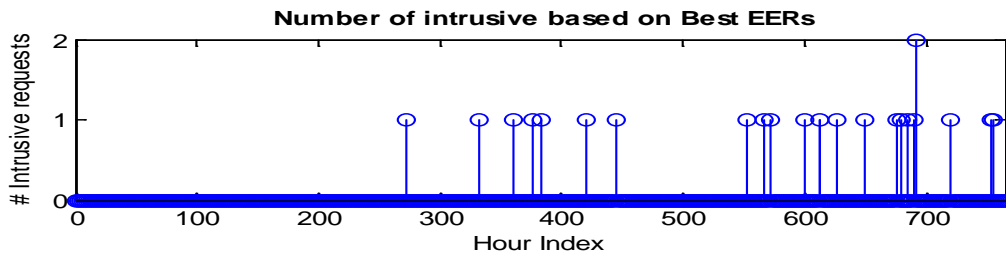
AL Window =20, IL Window =50 - High Usage
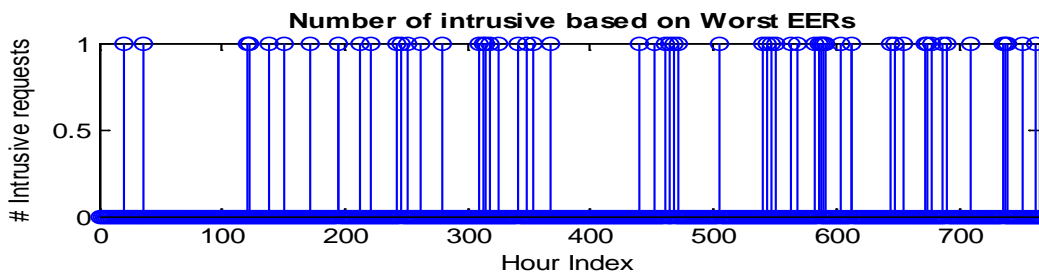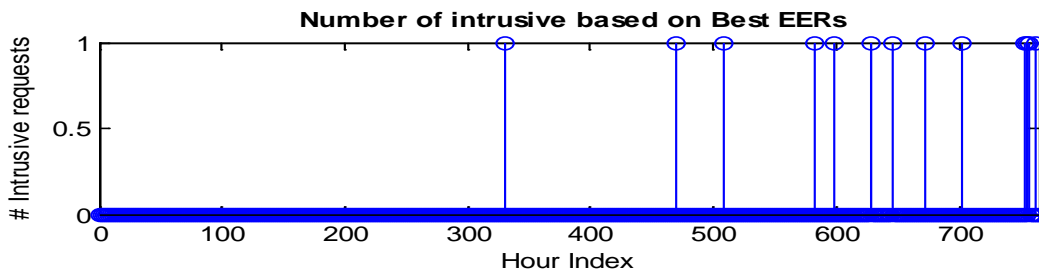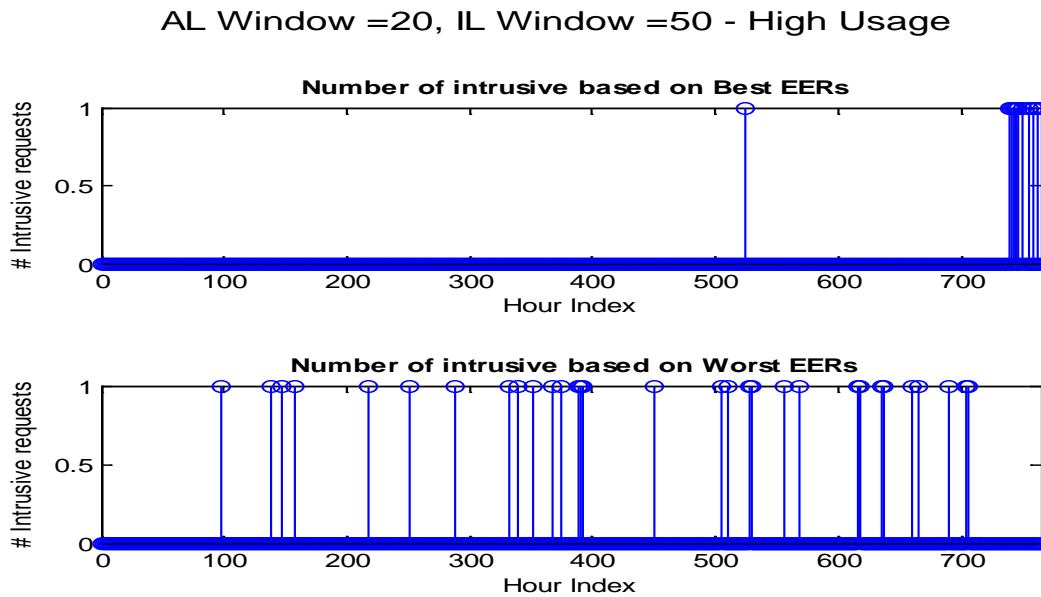
Figure 5.3: Intrusive requests in Best and Worst EERs for High Usage

A different representation of the results is given in Figure 5.4. These graphs represent the average integrity achieved in regions of samples used. So for example what is the average integrity across hours that max of 10 samples was utilised, or max of 20 samples etc. Given that integrity is lowered or increased based on one sample per time on this occasion the number of samples represent how many times the user will be authenticated per hour. This includes the failed authentication request which will lead to decrease of the integrity. Here is clearer – at least for the small windows, that frequent authentication leads to higher trust for the given dataset with a much greater number of samples. The latter also shows that although the dataset at hand does not explore the full possibilities of the samples that could be available in real life usage, even these levels of usage/activity are generally sufficient for the mechanism to work.

AL Window =2, IL Window =5 - High Usage

AL Window =5, IL Window =12 - High Usage

AL Window =10, IL Window =25 - High Usage

AL Window =20, IL Window =50 - High Usage
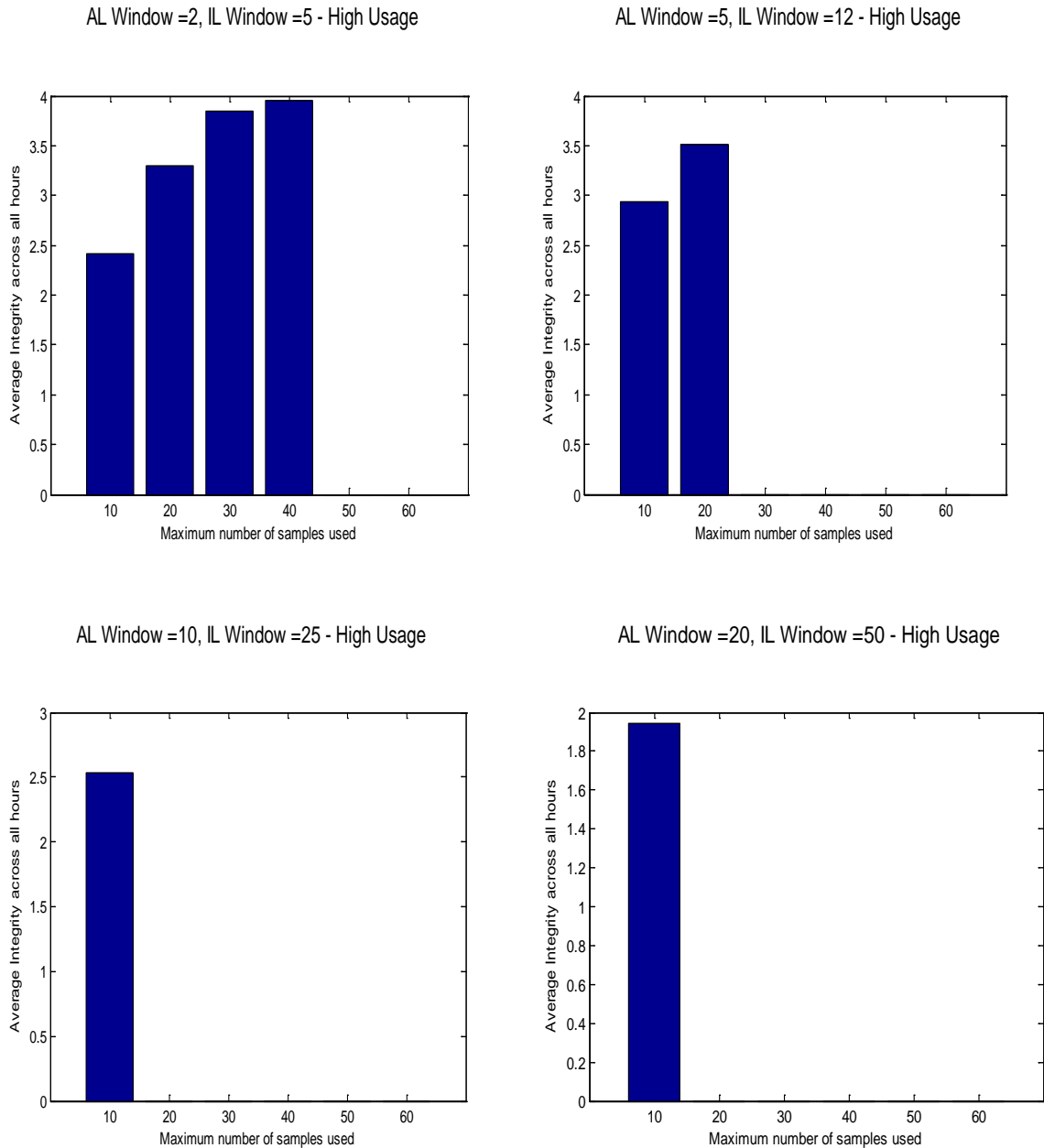
Figure 5.4: Average number of samples used per category

To see how lower usage would affect these results the simulation of the hours with medium and low usage where put to the same test. Figure 5.5 and Figure 5.6 represent the results of NICA operation under the different windows for medium usage and low usage respectively. It can be seen that the dynamics of framework

are less in lower levels of usage as the amount of samples do not allow for heightening the integrity, experiencing close to one degree less integrity per level of usage. In medium usage the smaller windows (AL=2, AL=5) appear to perform well but with minimal differences whereas in low usage this occurs for the middle windows (AL=5, AL=10). This performance can be explained as, as expected the less the activity the less possible for a sample is to be available. At the same time it can be again seen that the large windows (AL=20) never perform well in achieving a good level of trust. It is quite apparent the significance that the timed windows plays in the operation of the framework given the levels of usage/activity of the device. It can be seen that the framework still manages to at least maintain a positive integrity however quite a lot lower for the low usage. This would mean that at least for the hours with very few samples the framework could be quite intrusive at least for protected services depending on the timing of events.

NICA Performance on Medium Usage

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
NICA Best EERs	2.7332	2.628	2.2977	1.8743
NICA Worst EERs	2.723	2.5684	2.2819	1.8559
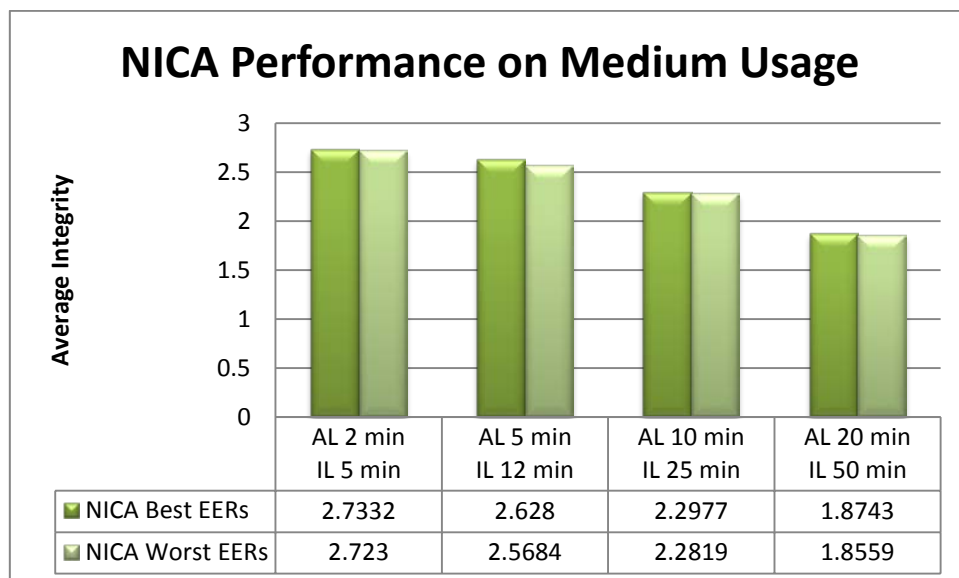
Figure 5.5: Average Integrity on Medium Usage

NICA Performance on Low Usage

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
NICA Best EERs	1.5032	1.7084	1.7306	1.5628
NICA Worst EERs	1.4856	1.7282	1.7472	1.5919
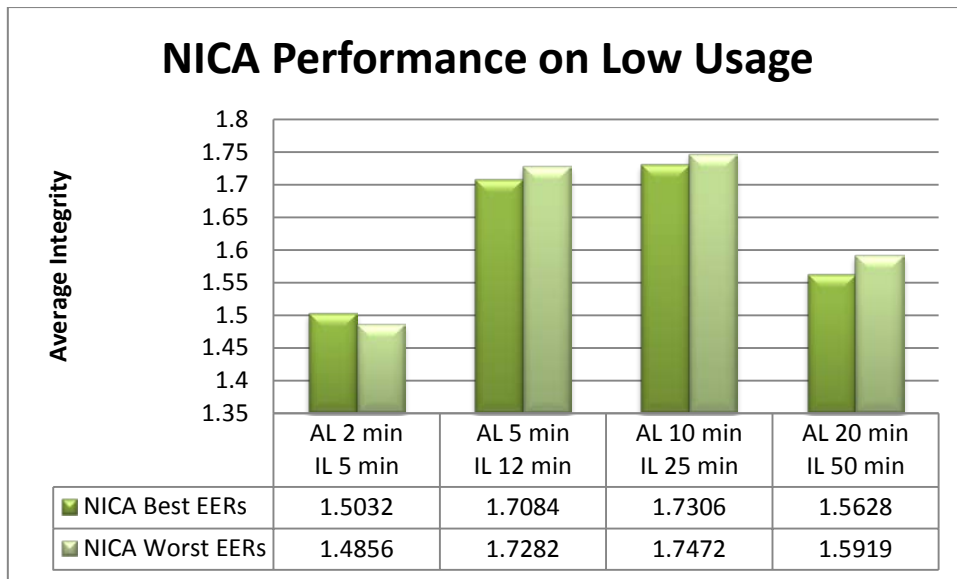
Figure 5.6: Average Integrity on Low Usage

Figure 5.7 show the average number of intrusive requests generated as a default operation of the AL mechanism and it can be seen that the number remains again below 1 request per hour.

Average Number of Intrusive Request based on Usage and EERs

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
High Usage on Best EERs	0.0458	0.0314	0.0183	0.0144
High Usage on Worst EERs	0.2013	0.132	0.0784	0.0418
Medium Usage on Best EERs	0.0209	0.0144	0.0092	0.0092
Medium Usage on Worst EERs	0.1176	0.0797	0.0523	0.0353
Low Usage on Best EERs	0	0	0	0
Low Usage on Worst EERs	0.0261	0.0235	0.017	0.0105

Figure 5.7: Average Number of Intrusive Requests based on Usage and EERs

5.2.3 NICA Impostor

The above section investigated the authorised user and the operation of the framework in regards to transparency and its ability to maintain a representative trust to the user. The security aspect of the framework needs to be assessed as to the ability of an impostor to utilise the system. The same series of data were used and the respective EERs where introduced to represent the FAR of the different techniques. The average integrity of the system for an impostor under high usage can be seen in Figure 5.8. It can be seen that the framework reaches a very low integrity which represents a good security for the system. The below -4 values show that the user not only will not be able to access secure services even before but also that the accessing of the open services of the system would be restricted and the impostor would be essentially locked out. Similar results are achieved for low and medium usage, which can be seen in Table 5-5.

Although the integrity of the system on average is quite low a more representative metric for the security of the system would be to see how fast the impostor would be locked out and to what extent the accessing of secure services is restricted and provides a better insight in to the role of the time windows on the system in regards to security. This will be examined in Section 5.2.4 that looks at the protected services.

NICA Average Integrity for Impostor

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
■ NICA Best EERs	-4.9088	-4.8792	-4.8511	-4.7743
■ NICA Worst EERs	-4.8872	-4.8184	-4.7229	-4.5418
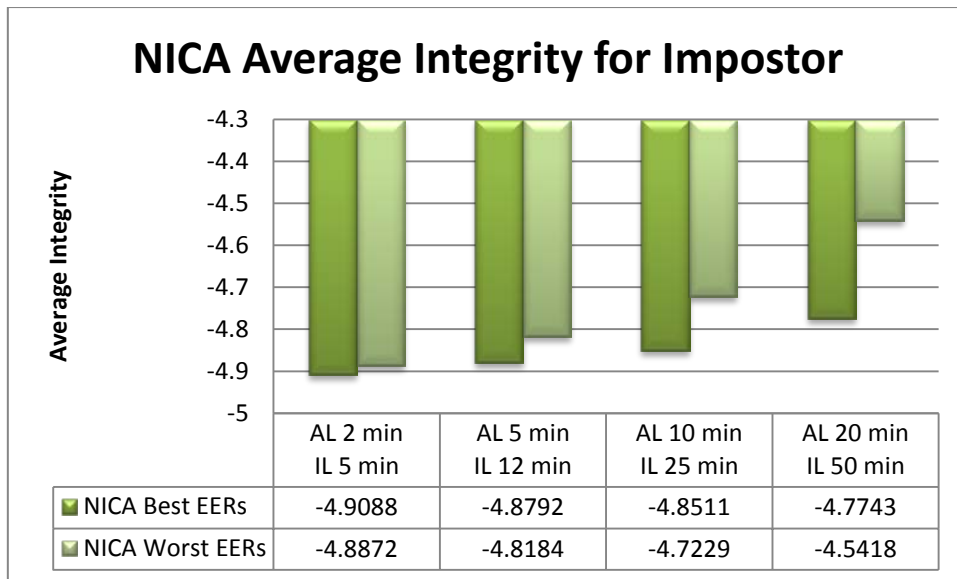
Figure 5.8: NICA average Integrity for Impostor on High Usage

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
Low Usage				
	-4.8432	-4.8055	-4.7763	-4.7446
	-4.8406	-4.7956	-4.7622	-4.7222
Medium Usage				
	-4.8739	-4.8489	-4.8297	-4.7738
	-4.8477	-4.7804	-4.6952	-4.5853
High Usage				
	-4.9088	-4.8792	-4.8511	-4.7743
	-4.8872	-4.8184	-4.7229	-4.5418

Table 5-5: Average Integrity for Impostor in based on usage and time windows

5.2.4 Protected Services and Security

The two-pronged approach of NICA allows for monitoring during access of secure services. After the simulation of the standard NICA operation in monitoring of the confidence level to the user, the performance of NICA regarding protection of secure services was assessed. This series of tests provided insight as to how often an authorised user or an impostor would be requested to get authenticated whilst using of the device to access a protected service, thereby assessing usability and security respectively.

The same dataset was used to provide the basis for testing. In the previous sets of testing all events were considered the same as far as the framework was concerned. In this case some of the events would need to be events generating access to a protected service. Given the limited number of events it was considered rather than removing some of the events from the generation of the confidence level and assign them to be events of accessing a protected service, a different approach was considered. Each timestamp of each event present in each hour was considered to generate an event for accessing a protected service with a skew of 5 seconds later. This decision would have a 2-fold effect. First of all it would generate a sufficient amount of protected accesses relative to the normal access of the device. Although this could potentially bring a negative effect to the performance by testing a lot of protected access events relatively to the user activity it was considered appropriate for this simulation as it is relative to the rest of the operation rather than generated random events during e.g. no usage of the device. It also gives a better representation of the network for a user that requests more often access to a secure

service during its normal use of the device as well as a stress test to the system. The second effect is the request of a protected service being close to a previous authentication request which could bring though a positive or negative effect the latter due to error rates. Given that it could be either it was not considered to provide artificial benefit to the simulation of any of the approaches, merely a more representative model. Furthermore this would only be the case on certain occasions as even though the protected service event happens every 5 seconds after each sample/event on the device that doesn't mean that the specific event/sample would have been used for authentication at the specific timing and therefore minimising the effect that this would have. As the operation of the device is just a subjective matter of user and hour of use the only solid basis can be the times of the data set used. All other activity would need to be somehow linked to the latter in an artificial way based on some logical suggestions.

To have a basis of comparison Table 5-6 shows the average number of protected services access events that occur per hour on the different types of usage. As can be seen the number of protected services particularly for high usage is quite high which would provide an exaggerated scenario however envisaged to provide a good test for the transparency of the system.

Type of Usage	Average Number of Protected Services Access
High Usage	57.2
Medium Usage	25.9
Low Usage	9.9

Table 5-6: Average number of protected services access events

As defined in NICA each protected service has a respective security level which shows the amount of integrity that the user needs to have in order to access it. As such, each of the protected services got attributed a randomly required level of integrity for accessing it. The values varied from 0-5 to represent from no or low protection up to high security services and a fair split was done across these values. This would give a variation of security services to be able to assess the system under different types of access requirements.

In the event that a user tries to access a protected service and does not have the required integrity level they will be faced with an intrusive request. Although at normal operation in any authentication request NICA specifies the decrease/increase of the integrity given a fail/pass, the framework does not specify the increase of the integrity at the intrusive request if that is a result of trying to access a secure service with insufficient integrity. Given that the lack of the appropriate IL to access a secure service results in the intrusive stage 4 of the Alert algorithm it could be a matter of increasing or decreasing the IL similar to the normal operation. However it could be argued that the user would only be granted temporary access to the service looking to increase usability whilst having at the same time the opportunity to reach an appropriate IL in the next transparent authentication. In the latter occasion the IL operates solely as the alarm and monitoring mechanism to establish user identity rather than establishing the requested IL. It could be argued that not applying an increase on the IL provides more security with the risk of affecting usability in the event of that stage being reached again soon. At the same time increasing the IL provides the user with a better chance of continuing to maintain a higher security

level during the continuous use of the secure service and reducing the chance of an intrusive request. Both would depend on the individual situation of device usage and the trade-off will exists. To evaluate that effect, both approaches during accessing secure services were simulated.

Two series of tests took place. The first test would put NICA framework under the test of accessing all the created protected service as a series of events during each hour with no integrity updates occurring if the required integrity has not been reached. During the first test another aspect of the framework is accessed. To see the performance of NICA in the occasion that the protected services are accessed as independent events during normal operation on NICA irrespective of any previous protected service access. So it demonstrates as well how well the device operates transparently and manages to reach appropriate levels of integrity for accessing secure services seamlessly in the case of an authorised user and how well it establishes security in the event that an impostor tries to access a protected service after an authorised user has been accessing it. The second test would be introducing the integrity update after an intrusive request and access how this can affect the operation of NICA and possibly add to the performance. At this test the services are seen as series of events.

5.2.4.1 Authorised User

Table 5-7 refers to the first test and presents the results of the simulation for the different levels of usage for Best and Worst EERs as per the original specification of the framework, which allows for no change in integrity after successfully accessing a protected service and as well as aforementioned see the service access as

independent events. As can be seen the framework manages to maintain a certain level of transparency with avoiding explicit authentication with a ratio of close to 1:4, 1:3 and 1:2 in the cases of high, medium and low usage respectively. The specific scenario presented here is quite extreme as for example for high usage an average of 57 events represents a protected service being access almost every minute if we see this as series of events. It does however provide a good stress test for the framework. For that occasion the 28.3% for high usage translates to 16 intrusive requests on average per hour which demonstrates a fair level of transparency - with the 13 out of the 16 requests represent services of Level 4 and Level 5, not though ideal. However it is envisaged that this will not occur very often, when considering this as series of events, given a continuous use of the device. Given the particular dataset as well that provides fewer samples than could in practice shows that potentially a more transparent operation could be achieved. It can be foreseen that the highest the usage the less intrusive the approach is which was envisaged to be the case given the higher integrity that was seen to be achieved in the previous test. For low usage the mechanism is expected to operate more intrusively as there is not an opportunity to acquire possibly enough samples to raise integrity to required levels. Given this approach the big time windows affect the transparency of the system with the requests more than doubling from the smallest to the largest windows. This demonstrates an insufficiency of the mechanism to provide the required integrity transparently at the rate that the protected services are accessed. Given that this is an extreme scenario with a high rate of services produced at the earlier stages of the hour it could be largely affecting the performance of the framework. The results also show that the bigger time window would have a stronger

negative effect on the framework in the case of increased number of services being used. This application of not increasing integrity in the framework as a result of a protected service also translates to a highly intrusive nature of such system in the event that activity is performed that requires continuous access to such services whether this is assessed as a series of events or independent events.

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
High Usage (57 services per hour)	**Number of Intrusive Requests**			
Using Best EER approaches	**16.1906** (28.3%)	**22.0901** (38.6%)	**27.0078** (47.2%)	**32.3016** (56.4%)
Using Worst EER approaches	**16.3525** (28.6%)	**21.8629** (38.2%)	**26.9399** (47.1%)	**32.1345** (56.1%)
Medium Usage(26 services per hour)				
Using Best EER approaches	**9.2376** (35.6%)	**11.2402** (43.3%)	**12.9295** (49.9%)	**14.6658** (56.5%)
Using Worst EER approaches	**9.3251** (36.0%)	**11.3133** (43.6%)	**12.9517** (49.9%)	**14.7507** (56.9%)
Low Usage (10 services per hour)				
Using Best EER approaches	**4.9256** (49.3%)	**5.2533** (52.6%)	**5.6149** (56.2%)	**5.9974** (60.0%)
Using Worst EER approaches	**4.8995** (49.0%)	**5.1619** (51.7%)	**5.5222** (55.3%)	**5.889** (58.9%)

Table 5-7: Intrusive Requests as absolute numbers and percentages as a result of accessing a protected service as series of events without integrity updates or as independent access events

Looking to establish the difference that an update in integrity each time a successful access of a protected service occurs would add to the framework, a second series of tests calculated the latter case. The results- as presented in Table 5-7, show that

such addition to the original framework largely improves the performance as it would automatically add a significant increase to the trust of the user. Although it is not guaranteed that e.g. a B3 technique would be used each time for accessing a protected service, it is more likely that protected services would be protected with the more confident techniques and therefore the integrity update due to a successful authentication would significantly add to the integrity and therefore the transparency of the system as seen from the results. This is specifically apparent for extreme scenario of high usage which shows an 8.3% possibility of intrusiveness which translates to 4.7 intrusive requests per hour compared to the 57 generated events showing a high level of transparency. The aforementioned effect of accessing a protected service very early on the start of device activity is counteracted here with the cost of an intrusive request which however establishes a far more transparent system for the reminder of the activity.

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
High Usage (57 per hour)	Number of Intrusive Requests			
Using Best EER approaches	**4.7454** (8.3%)	**3.6645** (6.4%)	**2.9204** (5.1%)	**2.3982** (4.2%)
Using Worst EER approaches	**4.7324** (8.3%)	**3.6488** (6.4%)	**2.9491** (5.2%)	**2.4334** (4.3%)
Medium Usage(26 per hour)				
Using Best EER approaches	**3.3825** (13.0%)	**2.8198** (10.9%)	**2.4922** (9.6%)	**2.248** (8.7%)
Using Worst EER approaches	**3.4465** (13.3%)	**2.8355** (10.9%)	**2.5026** (9.6%)	**2.2493** (8.7%)
Low Usage(10 per hour)				
Using Best EER approaches	**2.3081** (23.1%)	**2.0822** (20.8%)	**2.0157** (20.2%)	**1.9843** (19.9%)
Using Worst EER approaches	**2.2337** (22.4%)	**2.0457** (20.5%)	**1.9687** (19.7%)	**1.9439** (19.5%)

Table 5-8: Intrusive Requests in absolute number and percentages as a result of accessing a protected service with integrity updates and access as series of events

A further point to be noticed in these results that although the medium to bigger windows maintain a better level of integrity on average, the number of intrusive requests slightly drops as the window increases. This effect shows how the degradation function possibly affects the framework. Although here the difference translates to 1-2 requests which can be considered minimal compared to the large amount of requests per hour, since this is an average across many hours of use shows a notable effect. This result underlines the importance of balancing these 2 timing events for the better operation of the system. As the integrity increase would

be dependent on the biometric samples, having activity for example that only allows the capturing of low confidence samples while the degradation function is running could cause the framework to be far more intrusive than other occasions. Given the drop in integrity together with the restriction of being able to raise the integrity above certain levels and a quite big gap between authentication requests, it is expected to have a more intrusive system.

A further analysis was done to see which type of protected services get affected mostly by generating intrusive requests. Whether this occurs largely for highly protected services or occurs also for minimum risk services which would minimize transparency. Table 5-9 shows the average number of protected service access that occur within each hour split on required level of trust (always looking at high usage hours) together with the number of intrusive requests that the user will receive when trying to access the services. The table shows both approaches with or with no update in the integrity each time a protected service is accessed. As can be seen with no update the majority of the highly protected services would generate intrusive authentication while at the same time with having the integrity updated the system becomes far more transparent. The highly protected services with trust level 5 would still generate some intrusive events far less however whilst the services will trust required < 5 will reach in average close to full transparency. This demonstrates that the system has the ability to reach a high level of trust during a fair usage of the device and be secure whilst maintaining a high transparency to the user. Full transparency could exist depending on the timing of events in each scenario but nevertheless is not expected anyway at all times as the whole purpose of the trust

monitoring and the integrity level is exactly to monitor occasions where the level of trust is not sufficient to guarantee access in these services and therefore a certain intrusive due to higher risk is expected and accepted.

Integrity Required	Average Number of Generated Protected Services	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
		No Update in Integrity				With Update in Integrity			
0	9.4	0	0	0	0	0	0	0	0
1	9.7	0.4	0.6	1	1.5	0.1	0.1	0.1	0.1
2	9.7	1.2	2.2	3.3	4.7	0.2	0.2	0.2	0.2
3	9.8	2.5	4.2	6	7.9	0.3	0.3	0.3	0.3
4	9.4	4.5	6.6	7.9	8.9	0.7	0.6	0.6	0.6
5	9.2	7.7	8.4	8.9	9.2	3.5	2.5	1.8	1.3

Table 5-9: Number of intrusive requests generated on average per hour due to protected service access of each trust level (based on high usage and best EERs)

In consideration of any bias that the above data may have formed in regards to the quantity of the protected services per hour or the timing after each sample a series of test data was created that would represent a random set of protected services that occurred during the recorded activity of each hour. This means that the service accesses occur between the interval of the first and the last sample recorded each hour. Seven datasets represented the following – one represented 20 random selected services across all trust levels from 0-5 and 6 datasets representing 20 services in which each set all required the same level of integrity e.g. one dataset only with services needing a trust level of 5 to assess the operation of the system on each required security level. All datasets correspond to the same timed event with however different need of service access.

Integrity required in each dataset	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
Random fair split (20 services per hour)	3.2	2.9	2.6	2.3
0 (20 services per hour)	0.1	0	0	0
1 (20 services per hour)	0.3	0.3	0.3	0.3
2 (20 services per hour)	0.9	0.8	0.8	0.8
3 (20 services per hour)	1.7	1.4	1.3	1.4
4 (20 services per hour)	3.2	2.3	2	1.9
5 (20 services per hour)	9.3	5.6	4.1	3.2

Table 5-10: Number of intrusive requests based on randomly timed protected service access events for an authorised user

It can be seen that a good level of transparency is achieved for the lower security services. For the high trust ones the smaller the window the more intrusive the framework becomes with a fair transparency for middle windows. Although the bigger the window the framework appears more as aforementioned this is largely an effect of the degradation function with possibly an intrusive request happening early in the hour. It can be said that given the random spread of the events, in a real world scenario where the service access would be linked to normal activity of the device the framework would be expected to be even more transparent. In the event that a highly protected service occurs in periods of inactivity or not sufficient authentication then the framework of course would lead to intrusive authentication (as this is its purpose to gain a strong level of trust).

5.2.4.2 Impostor

To evaluate the performance of the system under impostor the number of access to any protected services was investigated, representing the FAR in this case. This would give an indication as to whether given the present impostor data the user

would have any opportunities to access a protected service without being authorised to do so. The results as presented in Table 5-11 showed virtually no access to protected services demonstrating high security of the system given the present datasets. The non-rounded zero's in the results of high usage show that in some occasions an impostor has gain access to a service. Analysis showed that this occurs in the event that in the beginning of activity during the hour were integrity is 0 if an FAR occurs as first access the impostor would gain access if accessing a service immediately after that authentication succeeds. However the services that they would be gaining access were only the services represented by 0 integrity meaning low or no security and in the case of the worst EERs for high usage there were also the occasions of accessing a service with required trust of 1 which also represent very low security requirements.

	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
High Usage (57 services per hour)	**Number of protected services accessed**			
Using Best EER approaches	**0.0039** (0.0068%)	**0.0039** (0.0068%)	**0.0039** (0.0068%)	**0.0039** (0.0068%)
Using Worst EER approaches	**0.0261** (0.0456%)	**0.0287** (0.0501%)	**0.0287** (0.0501%)	**0.0287** (0.0501%)
Medium Usage (26 services per hour)				
Using Best EER approaches	**0** (0.0000%)	**0** (0.0000%)	**0** (0.0000%)	**0** (0.0000%)
Using Worst EER approaches	**0.0104** (0.0401%)	**0.0104** (0.0401%)	**0.0104** (0.0401%)	**0.0104** (0.0401%)
Low Usage (10 services per hour)				
Using Best EER approaches	**0** (0.0000%)	**0** (0.0000%)	**0** (0.0000%)	**0** (0.0000%)
Using Worst EER approaches	**0** (0.0000%)	**0** (0.0000%)	**0** (0.0000%)	**0** (0.0000%)

Table 5-11: Protected service access by an impostor in absolute numbers and possibility of access with integrity updates

5.3 Discussion

Given the NICA results it can be suggested that the security as well as the transparency the system is notably increased based on the number of samples used. Furthermore, the time windows appear to notably affect the operation of the framework with more frequent authentication offering a more balanced approach between security and usability. The introduction of integrity updates due to an intrusive request also improves upon performance taking advantage of a high confidence technique. The original degradation function triggering at 20-50min is somewhat unrealistic as it will have a minimal effect upon the security of the system. Degrading Integrity by 0.5 every 30 mins or 50 mins would take, if the integrity was 5 to reduce to 0, 4.5 hours and 7.5 hours respectively, offering little to the protection of the device. As such, further investigation could seek to determine how these time windows could be alternatively balanced to improve upon security and usability as well as reconsider the degradation function and its effect on the framework.

Compared to the user evaluation the framework gave fair performance – as there was a beneficial situation where the biometric algorithms have no effect in performance. The data attempts to represent a system close to a real scenario showing that integrity increases as long as samples are available. Managing to maintain a good integrity whilst keeping security.

6   Modelling of enhanced fusion models

Following the practical evaluation and simulation of NICA and the results obtained an objective was set to explore the improvement of certain operations. Further to the increase of the integrity upon accessing a protected service which showed a notable improvement to the transparency of the framework one of the core operations of NICA was revisited – how biometric samples are used.

Given the fact that NICA operates only on one sample it overlooks the fact that the device could be capturing more than one sample within certain periods. That could be a waste of authentication opportunities that can provide a greater level of confidence for the user's identity. Given that fusion approaches utilise more than one sample have shown to provide a better operation it was envisaged that an investigation into the use of fusion techniques would enable the production of a more robust approach and the improvement of the NICA framework.

As the capturing mechanism constantly is capturing samples of different biometrics both of the following approaches could be implemented:

- Multi-Instance approach - Use of multiple inputs of the same biometric: A number of biometric samples of a single biometric captured over a specific timeframe could be utilised. This will enable the biometric algorithm to make a more informed decision by having multiple traits to base its decision. At the same time the existence of bad samples could be mitigated or at least decrease the possibility of FAR and FRR due to that cause.

- Multi-modal approach: Use of a single input of multiple biometrics: In this case samples of different biometric techniques are utilised. This could enable a more fine balance and tuning tied to the individual user and its preference and furthermore balancing the performance of the individual biometric techniques. Given that certain techniques may not operate well due to the user or mobile conditions this provides a fused mechanism with the capacity to mitigate some of the downsides of those occasions. This approach could furthermore provide another variance to the security of an individual service, creating a more multifaceted way to attribute security levels.

It is envisaged that any of the above approaches would provide a more dynamic system in comparison to the current one. The original approach although it offered the flexibility of the use of a number of biometric approaches its final decision was very much static based on a single outcome. As became apparent in the evaluation this was far from ideal for certain users and the way that they utilised the mobile device, which on top of the bad performance of the biometric algorithms would sometimes make the authentication decision questionable. For example during the user trial, the use of the Vaio device for some users would produce very bad image samples as the way that the users were holding the device while typing would not capture the entire face resulting to failure of the biometric algorithms. In this case the use of more than one sample or the use of more than one technique during that authentication process could produce a more valid result. That however needs to be balanced so the decision is largely based on the stronger or more appropriate

biometric. Therefore consideration needs to be also given to the way that the technique and the weight on the decision will be attributed.

At the same time the system could tune the biometric inputs to fit the individual requirements of the user in case for example certain techniques and features are not very characteristic for a specific user. In such a case the reliance could shift placing more weight to techniques that work better for the specific user. The aforementioned approaches (multi-modal & multi-instance) are by default available for direct application from the NICA framework as depending on the samples available a multi-modal or a multi-instance approach has the dynamic of being applied. As the framework looks to acquire the most recent samples with the higher confidence samples of the same biometric or samples from multiple biometrics could be selected.

A reconsideration of the framework and adaptation of the original NICA framework process and authentication mechanisms that would enable fusion of biometric decisions has taken place as well as an evaluation against the performance of the original NICA. The following sections describe these adapted models and the nature of the simulations and results.

6.1   Enhanced Simulation Models

Two enhanced approaches were developed for enhancing the NICA operation with fusion. These two models were consequently put to the same tests as the NICA framework (highlighted in Chapter 5) in order to compare the enhanced fusion models to NICA performance. These approaches looked to see how the use of more

than one sample at the time depending on availability, could provide a more confident result and a better usability of the framework. The fusing of the results of more than one authentication decision would mean that the authentication decision should be stronger. The way that the weight of the decision and as well as the decision itself would affect the authentication algorithm is presented in the following sections. No differentiation was used in regards to multi-instance or multi-modal as both of them could occur depending on the availability of particular samples.

6.1.1 Fusion Approach 1 – NICA with 2 samples fusion:

In this approach the first investigation was undertaken to examine the effect of using more than one sample would have on NICA performance. Furthermore, how this approach could be incorporated into the NICA framework and update how the Alert Level mechanism would work. In this approach the authentication algorithm seeks to use 2 samples instead of one if that is available. Depending on the presence of the samples the Alert level algorithm would respond respectively in order to take into account on how many samples were used and the confidence of these samples. The fusion occurs at decision level by utilising the individual decisions based on each sample.

For this enhanced framework the authentication manager looks each time to utilise at maximum 2 samples. Triggered every x number of minutes, the algorithm seeks to recover 2 samples from the input cache. Amongst the present samples in the input cache the selected 2 samples must:

- Have been captured within a set time window of y minutes that defines how recent the samples must be. If only one sample satisfies this condition then the framework defaults back to NICA operation.

- Be samples of biometric techniques with the highest confidence level possible. In the event that e.g. one of the 2 samples does not represent the highest confidence level the next available best confidence level technique will be selected.

The above ensures that the samples are timely ensuring a greater validity as well as utilising the best samples for a more confident decision. Even though in certain occasions even if 2 samples exist they do not represent a high confidence technique, they still provide a more confident decision since the authentication decision rather than using only one of the 2. The latter may not be as beneficial when using biometric algorithms with high error rates compared when using more confident techniques; however, it provides a more informed decision. An alternative approach in the criterion of selecting the samples could be a configurable setting of the framework that defines the best performing techniques for the specific use and/or device.

6.1.1.1 Alert Level Modifications

The Alert Level algorithm was modified to incorporate the new aspect. In NICA the AL would reset to L1 at any point that the authentication decision was positive with the only difference in this rule being during intrusive authentication if the technique used was not a biometric, in which case the AL would only go the L3 waiting for the next sample. This process provides usability but it is a possible shortfall depending on FARs. As such resetting the AL to L1 with the only basis of one sample and therefore more prone to a security risk due to possible FAR. In this version there was an effort to mitigate this by moving to different levels depending on how many samples are being used.

In the approach with 2 sample fusion, in the event of the authentication decision being the outcome of 2 samples the AL would reset from the current level to L1. However if the authentication decision is the outcome of only 1 sample then the AL will only reset to the previous level. That was envisaged as a more confident approach to the security aspect of the framework so that the AL resets only due to the strongest possible operation of the framework as it currently stands with 2 samples, whereas the less stronger approach still maintains usability but attributed less weight on the security aspect. Given this mechanism a one sample authentication decision can reset the authentication framework to L1 but not if the AL level has already reached L3 which would mean that at least 2 continuous authentication requests have failed already. The only occurrence that a one sample technique would reset to L1 is that a 1 sample approach has failed giving some leverage to the algorithm.

The same reverse operation happens in the event that a 2 sample based authentication fails. Respectively in this case the AL will jump directly to L3. With this decision the transparency of the framework is being kept and gives one more chance to the user with waiting for the next input as well as maintaining a better security by removing the possibility of yet again another transparent level. With this step also the chance of consequently having a reset of the AL due to a one sample based authentication is mitigated as by jumping to AL 3 if the next authentication happens on one sample and is successful then the AL will go back to AL 2 rather than AL 1 as would happen in NICA. In order for finally the AL to reach 1 only on one sample that will mean at least 2 successful one sample based authentications.

In order for the above solution to operate accordingly to the AL algorithm a further modification had to be introduced. When the AL algorithm reaches 3 in NICA that would mean that the algorithm would wait for a newly captured sample to come in. In this modified version that would mean that the framework on AL 3 would always only authenticate on 1 sample at that point as only the next captured sample would be taken into account. Since this is a fusion approach the framework in the updated form would still wait for a new sample to come in so there is a current sample being taken into account in the authentication decision process as well at the same time looking to utilising any other sample that fits the pre-defined time window for valid timely samples. The latter would enable the possibility for fused authentication at L3 and enabling the opportunity for also resetting the AL directly back to one if the outcome was positive. Given a high use of the device is very likely that more than one sample are going to be captured depending on the configuration of the capturing

mechanism and therefore more than one newly captured samples could be actually used at this point.

The logic of the Alert level algorithm is depicted in Figure 6.1.
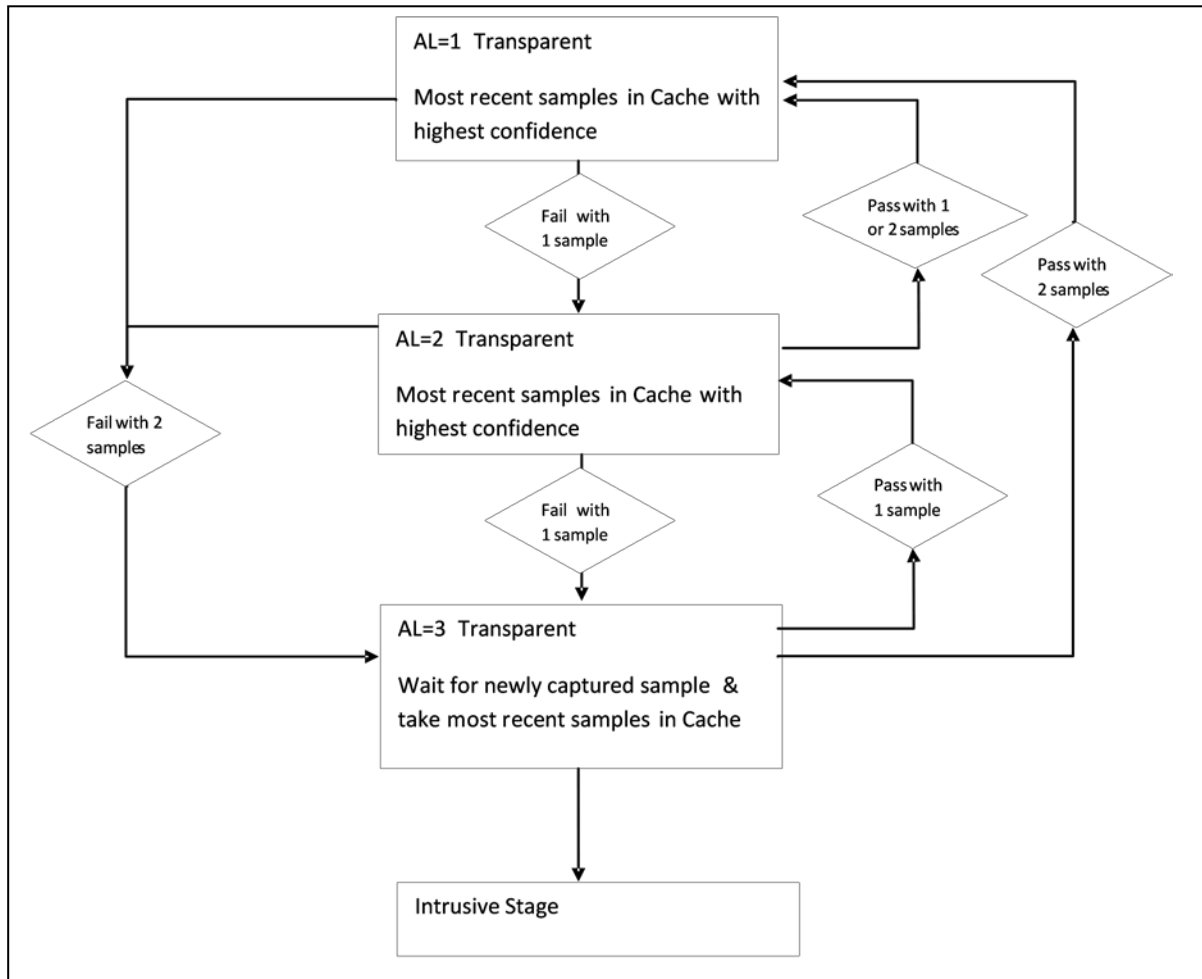
Figure 6.1: Operation of the transparent levels of AL with 2 sample fusion

For purposes of usability and transparency it was decided that a failed authentication on 2 samples would still provide the opportunity to the user for another transparent authentication. As such the AL failing at any of the 2 transparent levels will only go to L3 rather to an intrusive stage providing for a trade-off between security and usability

at this event. Given that the techniques used would not necessarily at all times be of high confidence it was considered that such opportunity was a valid approach. A more enhanced decision making could take this factor into account in order to make the decision making of the AL rely on the confidence levels rather than the number of samples used but this is not something that was evaluated in this research. The number of factors that could be taken into account are numerous and the combinations too many for all aspects to be evaluated to this extent.

6.1.1.2 Decision Level Fusion

In the NICA framework the way that the Alert Level process will proceed is dependent upon the positive or negative result of the authentication based on one sample. Depending on whether the authentication decision is above or below the specified threshold for determining successful authentication the AL will reset to AL 1 or jump to the next level respectively. When utilising one sample the output of the authentication decision is a number between 0 and 1 as being outputted by the biometric algorithm and therefore a straight forward decision can be made relatively to the threshold. In this fusion approach as 2 samples are being used and therefore there are 2 different outputs from the same or different algorithms, fusion of these two outputs is required in order to decide whether the overall authentication response lies above or below the threshold.

There are several ways that the outputs of different algorithms could be used. Depending on the samples utilised the algorithms may be of the same or a different confidence and of the same or different biometric technique. Given the definition and operation on NICA and its reliance on confidence levels attributed on different

techniques and algorithms, that was an aspect that needed to be incorporated in the fusion. A simple for example mean of the biometric decisions used would not be appropriate at this point as different techniques have different performance and therefore confidence that can be relied upon. As such in order to calculate the fused output a weighted average was used that would take into account the confidence level of the technique and the output of the algorithm. The weighted decision calculation is depicted in the following formula:

$$Weighted_{Decision}$$

$$= \frac{(Weight_{BioTechnique_1} * Decision_{BioTechnique_1} + Weight_{BioTechnique_2} * Decision_{BioTechnique_2})}{Weight_{BioTechnique_1} + Weight_{BioTechnique_2}}$$

The weight of each biometric technique is based on the confidence level as defined in Table 6-1. The weighting could be configurable as stands for other values of the framework. In this case it was considered appropriate that this type of weighting would provide an adequate differentiation between the different confidence levels without proving however an extreme benefit to any of them if e.g. the second algorithm gave the opposite result. As such balancing the fusion of the response to not have a significant skew towards only one of the technique as in that case the benefit of having more than one samples would be significantly mitigated.

Confidence Level	Weight based on Confidence Level
B3	3
B2	2
B1	1
B0	0.5

Table 6-1: Decision Level weights according to confidence levels

In the event that only one sample is present and used then the decision will only be based on the single output of the authentication decision as any weighting is cancelled out.

The above process helps in determining the decision of the authentication request and how the AL will proceed, however there is one more aspect to consider and that is how the Integrity level would be modified. On the NICA framework each time an authentication request is taking place as part of the Alert level process an update on the Integrity level of the system was made to reflect how the trust to the user was affected by authentication request. A decrease or increase change would be occurring to the IL in case of a failed or a successful authentication respectively. The amount that this increase or decrease would be dependent on the confidence of the biometric technique used (This can be seen in Table 4-2 - The more confident the technique the highest the change on the IL).

As in this case more than one sample are used as happened with the weighted decision in the authentication request a similar principle needed to be applied here so that the use of composite authentication can be also reflected in the integrity of the system. Given that a more confident approach is being used that should be able to provide more confidence to the user identity or remove that confidence if the authentication is unsuccessful. In this occasion the decision was made to update the IL based on the sum of the increment/decrement value corresponding to the two techniques being used. Although a weighted average was considered initially in this

occasion it did not appear appropriate as when techniques with different weighting are being used the resulting value has less effect compared to if one sample being used opposing to the core idea of this approach. A similar effect occurs even if techniques have the same confidence as the weighted average will again result being the same as if one sample was used. So the IL updates is reflected in the following formula.

$$IntegrityLevelUpdateValue = IntegrityLevelUpdateValue_{BioTechnique_1} +$$

$$IntegrityLevelUpdateValue_{BioTechnique_2}$$

6.1.2 Fusion Approach 2 – NICA with 3 samples fusion:

A similar approach was used for this version of NICA. In this occasion the use of maximum 3 samples was applied. This staged approach was utilised so that it was possible to see whether by increasing the number of samples the effect on the authentication was becoming negative rather than improving performance. Although use of any sample available could be another approach this simulation gave an insight as will be seen in the simulation results section on how the increase of samples affects the performance.

As in the first approach the Authentication Engine will seek to identify from the input cache the number of most recent samples available based on a specific time window. If more than 3 samples are present then the ones representing the highest confidence techniques will be utilised. If 3 recent samples are not present then will look to retrieve 2 following the same principle and if that is not possible then will seek for 1 sample etc.

6.1.2.1 Alert Level Modifications

The Alert Level was again modified to reflect the use of 3 samples. A similar updated decision making in regards to which level should the transition of the AL process be needed to take place. This is reflected in Figure 6.2.
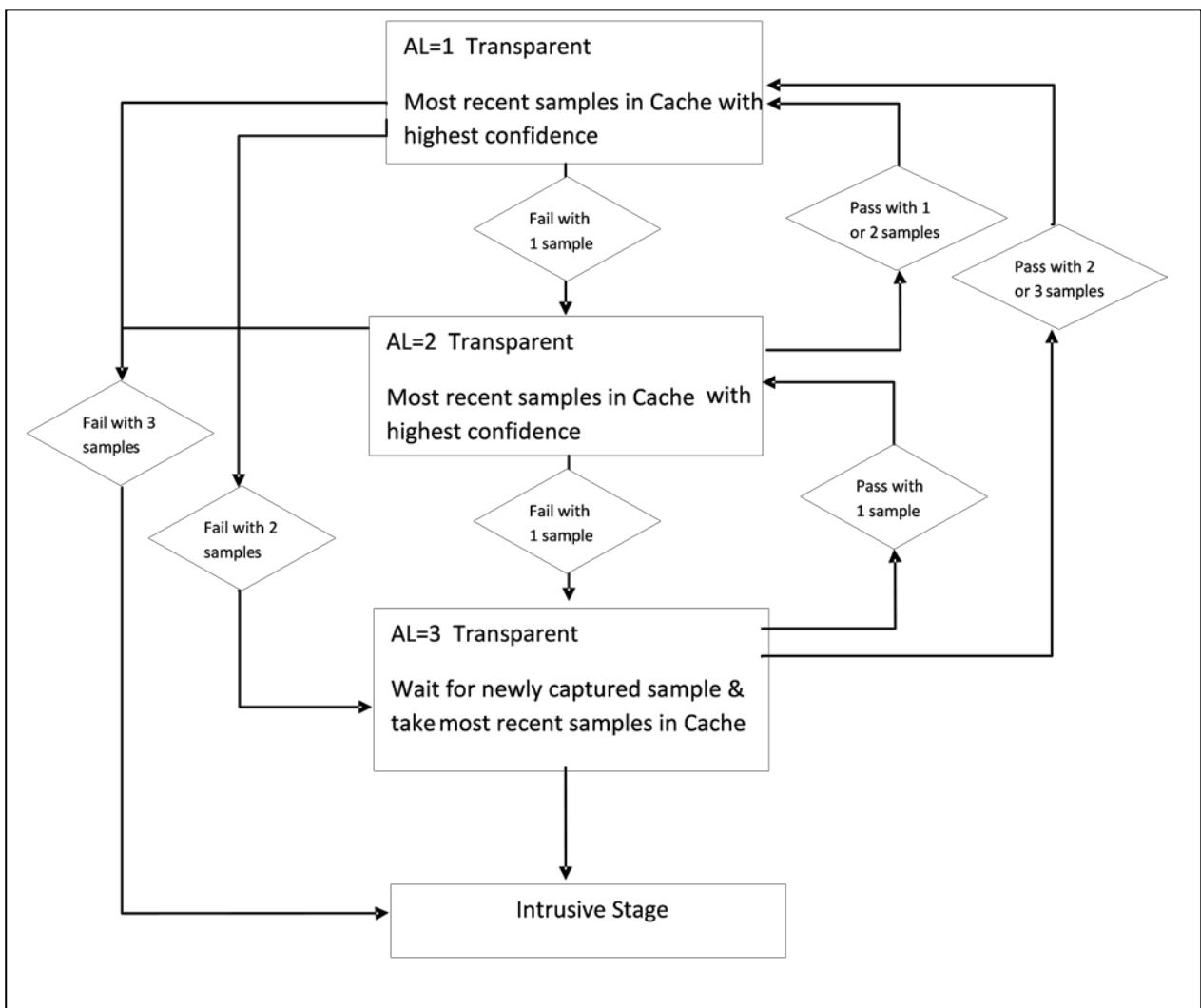
Figure 6.2: Operation of the transparent levels of AL with 3 sample fusion

In this occasion it was decided that if 3 samples are being used and the authentication fails at any stage it is more confident to say that the authentication decision based on the fusion of 3 samples can give a trust-reliant result not to provide another opportunity for transparent authentication and directly introduce a intrusive interface for explicit authentication. As aforementioned in the previous sections this principle was not applied in the first version to mitigate the event of having a low performance technique driving the AL directly to an intrusive stage. However given 3 samples this decision can be made more confidently. If 3 samples are not present then the operation defaults back to the first approach as can be seen in the flow chart.

6.1.2.2 Decision Level Fusion

The same principle was followed as in the first approach with now though the weighted average of the fusion to represent all 3 techniques if 3 samples are used. Similarly the update on the IL to reflect the sum of all integrity change value of the 3 techniques.

6.2   Fusion models simulation

The simulation seeks to follow what would be considered as normal operation of the framework. The only exception to the rule is that in the enhanced versions of NICA which could be utilising 1, 2 or 3 samples each time and reset to -1 level for the former 2 or -2 levels for the latter. During transparent operation when utilising one sample then the alert level mechanism drops only -1 level in the event of successful authentication. However in the simulation during the intrusive stage it will reset to

level 1 without taking the number of samples into account considering a successful pass. In a real case scenario it would only request one explicit sample but that could depend on the setting of the framework – as it could extend to also to composite authentication with fusion. However since these samples would be provided explicitly it is envisaged to be clearer, better sample(s) that would be characteristic enough for the biometric algorithms to have a good performance, something that as aforementioned is not always going to be the case for the transparent stages and therefore the intrusive stage would be expected to be less prone to FAR. This decision on the intrusive stage is based on using the strongest available technique and therefore confidence level on the device and for the purposes of this experiment a B3 level was used. As such also the integrity level was modified respectively in each occasion.

6.2.1   Alert Level & Integrity Change Time Windows

Given the experience of the NICA original prototype development, evaluation and the simulation results further to the performance of the biometric algorithms it was apparent that 2 important elements that play a significant role in the performance of the framework – the AL Window and IL Window. These 2 factors have been seen to significantly impact the performance of the framework and as such further different approaches were considered in this simulation. The time windows in which the Alert level is triggered plays a significant role to determining how often authentication would take place, which is in turn dependent on the availability of samples. Particularly in the simulation of the fusion versions as more than one samples would

be sought the timing of authentication request could be also of more significance to the performance of the approaches.

Given that there is the requirement for transparency but also monitoring the security level of the device at the same time these two aspects and consequently the time variables are proportionally inverse with each other - as always happens when seeking to balance security and usability. As seen in the previous simulation the more often the Alert level mechanism gets triggered the more security can be achieved and the less often the integrity drops the more convenience can be established by minimising the security aspect and vice versa. The problem exists at finding a balance between the two variables so that the one does not diminish the effect that the other has on the operation of the framework. Given the previous simulation results it was considered that there is scope to further investigate the relativeness of these two values and how effective they may be.

Based on the above a number of different time window settings were decided to be tested during the simulation. This was envisaged to provide a further insight of how these variables affect operation. The time settings are depicted in Table 6-2

Alert Level (IL) Time Windows	Integrity Level (AL) Time Windows		
2	1	2	6
5	3	5	12
10	7	10	25
20	15	20	50

Table 6-2: Time windows

The values selected represent 3 different settings for the IL time window – to be less, equal or more than the AL timing. That would give an idea on how the framework will be affected from having the IL drop in different frequencies. For each of the AL windows each of the corresponding IL window was tested. The above windows were tested so much for the fusion approaches as well as the original framework.

6.2.2 Summative Comparison Results

The following section presents the results of the fusion models in comparison to the original NICA as well as the evaluation of the different time windows. The results discussed here will be focusing on best EERs as the worst EERs produced a similar result as happened in the first tests and therefore the results will not be discussed here but can be found in Appendix D.

6.2.2.1 Fusion Models vs NICA

Using the same datasets as in Chapter 5, simulation code was written for the adapted fusion models. The results of the simulation for the previously used time windows are depicted in Figure 6.3 and the original NICA results are included for the purposes of comparison. As can be seen the fusion models manage to achieve and maintain a higher trust than NICA whilst utilising one sample. This is the case for all time windows achieving a 3.8-4.0 for the 2 smaller windows. Although the integrity of close to 3 is also achieved for the large time windows as aforementioned although it provided good usability the security of the system is not considered appropriate given the large time span. It can be seen how also this large gap in authentication also drops average integrity by a great amount as no much opportunity to

authenticate exists. Nevertheless it is apparent that the use of fusion raises the trust for an authorised user to a quite higher level which it is expected to be interpreted in high levels of transparency for protected service access whilst maintain good security with short authentication time spans.

A further notable result is that the improvement coming from exploring 3 sample fusion model is minimal. This could be the effect of non-existent samples for such authentication or that simply the chosen fusion or framework operation does not benefit from such approach/algorithm. Given that these results represent high usage profiles the latter is more likely to be the major reason in this case as samples are likely to be available. However this is arguable given the consideration that the particular dataset as aforementioned represent only initiation e.g. of an application rather than the samples that can be selected during its usage. The other consideration could be that the samples available may not at all cases represent high confidence samples. However given the fair randomness of the confidence levels that have been generated this is unlikely to have a significant effect here.

NICA vs Fusion Models for Authorised User

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
■ NICA	3.237	3.0007	2.5353	1.941
■ NICA with 2 sample fusion	3.8536	3.9809	3.6921	2.916
■ NICA with 3 sample fusion	3.8709	4.0013	3.7387	2.9644

Average Integrity
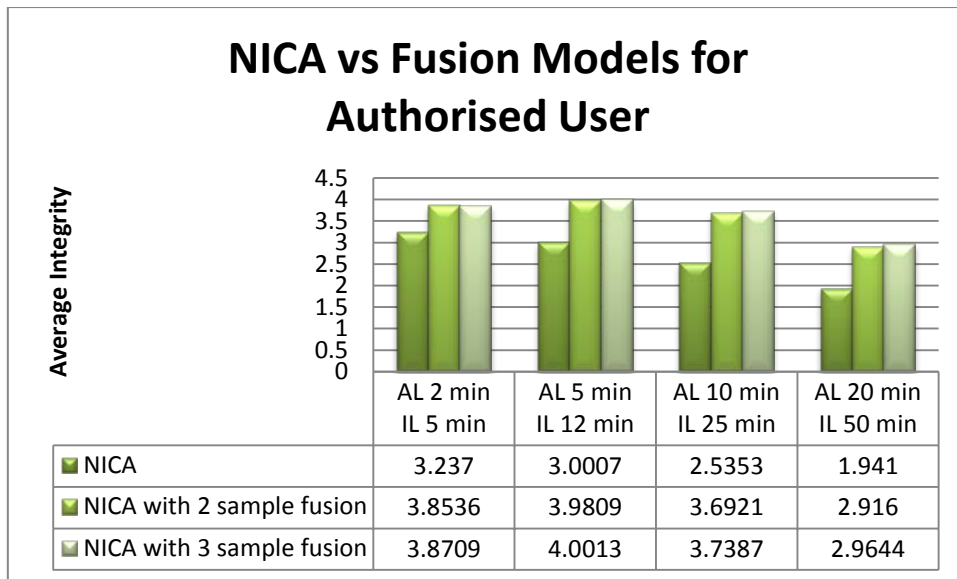
Figure 6.3: NICA vs Fusion Models for Authorised User on High Usage

Although there was a consideration that the use of fusion could cause a negative effect on the framework due to FRRs but as can be seen from the results this is not the case. The performance does not seem to be negatively affected from larger updates in integrity as a result of the weighting functions showing that a fair distribution of weightings has been achieved. Also given that the AL does not reset after the use of one sample rather it sets at -1/-2 level of the AL it allows for more enhanced monitoring of the device and seem to assist in maintaining the integrity on high levels and therefore managing to reach a better level of trust. Although these two parameters have not been assessed individually here the combination of them works towards the increased integrity. It would have been good to see these two factors working in practice together so much to be able to also assess how this increased authentication may affect issues like processing or be prone to negative effect due to FRR but this is not possible due to time restrictions.

Figure 6.4 shows a characteristic example of how average integrity changes according to samples to give a visual representation across the 3 approaches on the one of the best performing time windows. As can be seen the larger improvement occurs as the number of samples used increases. The hours are not arranged necessarily the same on all graphs rather than being represented on increased order based on the number of samples that have been used in each approach to detect whether the increased number of samples used in each authentication actually affected the good operation of the framework. What can be noticed is that fusion has a more consistent performance regardless of the number of samples that are being used providing that would potentially benefit the approach in differing sample availability. The representation of the results for comparison across the same hour for all models can be seen in Figure 6.5 where again the improved performance is apparent where also it can be noticed as seen previously that fusion models are too close in performance and there is not much improvement in using further fusion.
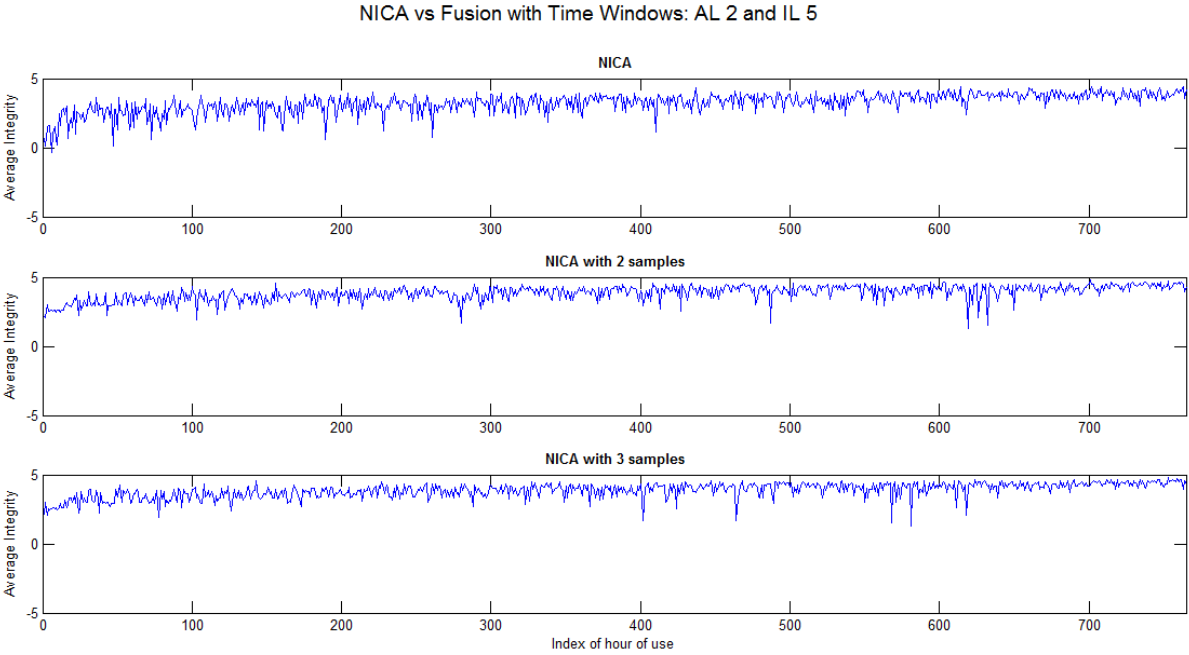
Figure 6.4: NICA vs Fusion Models across all hours based on best performing window.
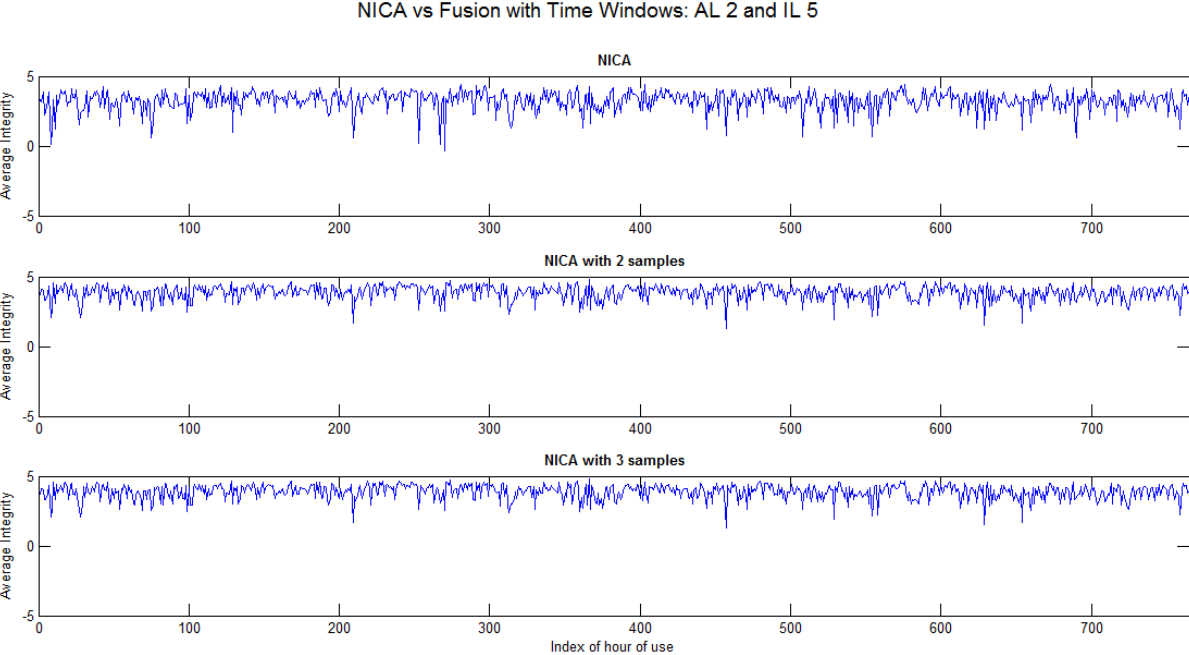
Figure 6.5: NICA vs Fusion Models across all unordered hours based on best performing window

The individual performance across a specific hour varied from case to case. Although there are quite clear limits of where mainly integrity lies in each approach,

there were of course particular hours that the framework would not perform well under specific approaches. This is mainly an effect of the number of samples and timing of them as well the biometric technique coming each time at specific steps of the AL mechanism. So for example if in the enhanced version of NICA utilising 2 samples, if low confident techniques are being used at the upper levels of the mechanism that mean that the AL would be constantly reducing the level but not resetting the AL mechanism. In cases as for example where the AL will be waiting for the next sample to come in and there is no activity on the device, a two-fold effect occurs. The integrity would keep dropping periodically as it is an independent function whereas the AL mechanism would be tilted and on hold not having the chance to raise the integrity of the system causing the latter to be reduced significantly.

Similar improved results for fusion were achieved for medium and low usage profiles. The results are depicted in Figure 6.6 and Figure 6.7. Fusion models manage to achieve a much higher integrity regardless the lower usage of the device showing fusion outperforming the original NICA and offering a better operation of the system.

NICA vs Fusion on Medium Usage

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
NICA	2.7332	2.628	2.2977	1.8743
NICA with 2 sample fusion	3.3854	3.6112	3.3015	2.6034
NICA with 3 sample fusion	3.4024	3.6432	3.3349	2.6324
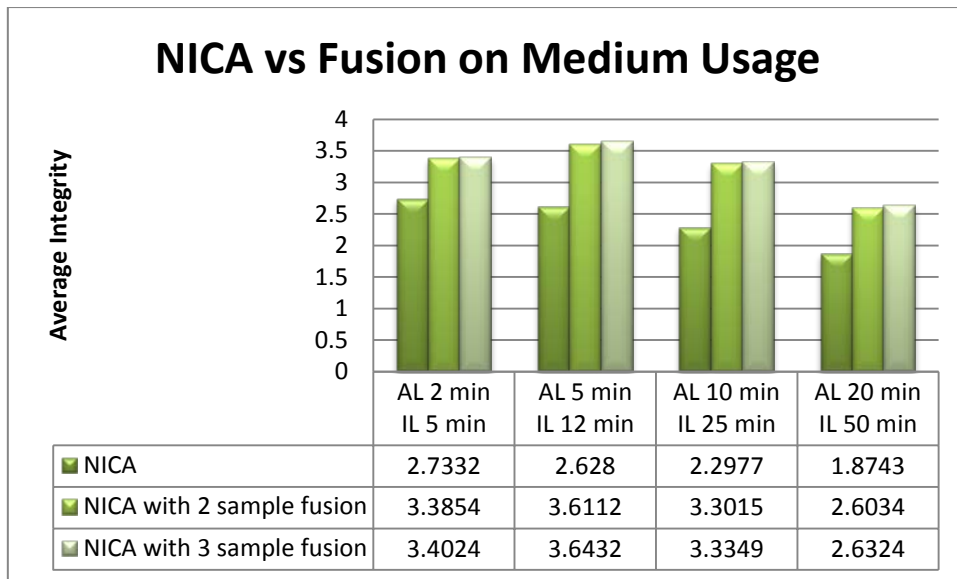
Figure 6.6: NICA vs Fusion Models for Authorised User on Medium Usage

NICA vs Fusion on Low Usage

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
NICA	1.5032	1.7084	1.7306	1.5628
NICA with 2 sample fusion	2.409	2.4741	2.318	1.8843
NICA with 3 sample fusion	2.4738	2.498	2.3314	1.8966
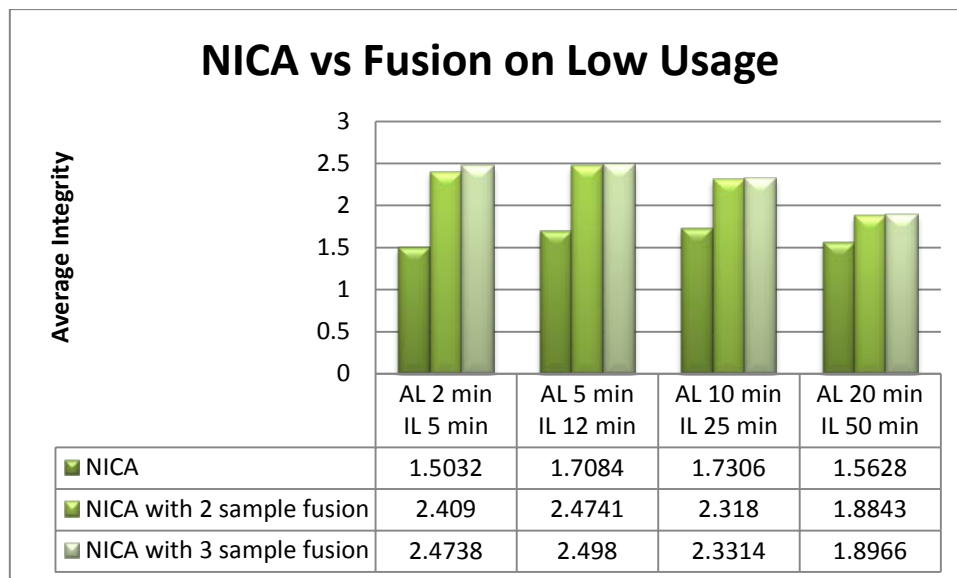
Figure 6.7: NICA vs Fusion Models for Authorised User on Low Usage

The results for an impostor are presented in Figure 6.8 which show that fusion models follow a good level of security for impostor as NICA did with no particular

differentiation. Although this can provide an indication of how the integrity drops, the real test for the security aspect is better evaluated though protected service access.

	AL 2 min IL 5 min	AL 5 min IL 12 min	AL 10 min IL 25 min	AL 20 min IL 50 min
NICA	-4.9088	-4.8792	-4.8511	-4.7743
NICA with 2 sample fusion	-4.9116	-4.8878	-4.8677	-4.8138
NICA with 3 sample fusion	-4.9116	-4.8878	-4.8677	-4.8138
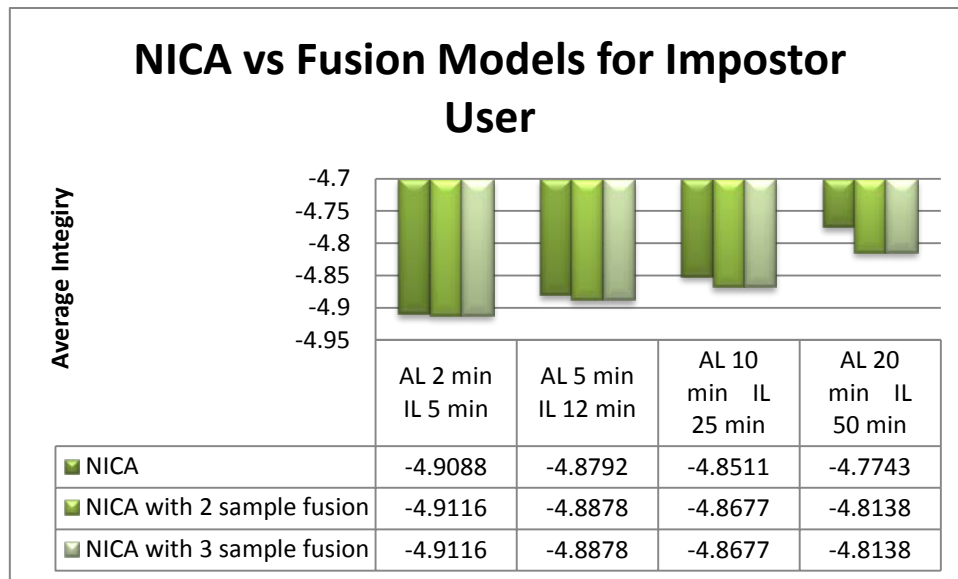
Figure 6.8: NICA vs Fusion models for Impostor User

The simulation results for the authorised user gave the results depicted in Figure 6.9. The graphs show the average integrity achieved by the system across all hours when using the 3 different variations of the framework. As can be seen from the graphs the original NICA framework has the worst performance across the band. Both the enhanced versions achieve a better integrity to be maintained.

As it can be seen on the graphs the time windows and their relativeness notably affect the framework performance. It can be noticed how the integrity for the larger windows appear less effective. Given these series of tests what is to be noticed is that on average when integrity is dropping more regularly than the AL is triggered this notably decreases the integrity of the system. This is solely the effect of IL dropping too regularly since the AL mechanism stays constant and counteracting

any positive effect that the AL mechanism has. However these changes are more notable in the smaller time windows and far more subtle to the larger windows as anyway the relative events are going to occur less frequently.

It can be seen that for windows like AL=10 & AL=20 the average integrity is maintained close to 3 or even above for the enhanced frameworks and close to 1-2 degrees lower for NICA. Although this means that the user will be likely to be experiencing high usability depending on the application use, it also again places a concern regarding system security as given to this level of integrity as authentication is low with this type of large windows. We can see also that the average integrity does not change significantly for the AL time windows 5 and 10 for the enhanced versions where the IL window are the same of greater than the AL window, experiencing a variation less than 0.5. That is potentially the effect of the degradation function having little to add to the integrity of the system as in comparison with the role of the authentication requests.

Based on these results it can be suggested that the relativeness of time windows are originally defined in NICA with the AL window being smaller than the IL window offers a better performance however they need to be a few degrees smaller than originally defined. More frequent authentication can lead to a higher integrity being maintained and particularly with the fusion models this reaches quite high and satisfactory levels- something that will be further investigated with protected access.

What becomes apparent from the results is that the single dimensionality of NICA causes the integrity to rise only as much as the corresponding biometric technique used each time allows which in turn is affected by the IL drop every so often. The

values between the increase due to a successful authentication request and the IL drop are quite close that unless the timings are very far apart and big in duration the IL drop overpowers as it is most likely to occur more often. Whereas with the enhanced models given the integrity could be raised more confidently and thus higher provides a bigger opportunity to the framework to be usable. Both of the 2 approaches have an effect on security and a potential risk. In the former NICA approach the fact that bigger time windows would mean more intrusive system whereas as to the latter approach the framework could potentially raise the integrity high and if the IL window does not have a quick effect on it would be also leaving a window of opportunity for misuse. The way that the framework operates this is not an aspect that can be mitigated but requires a more individual configuration of these settings which again are not going to fit all scenarios.

Average Integrity with AL time window 2 min

	IL - 1min	IL - 2min	IL - 5min
NICA	-1.9495	1.3795	3.237
NICA - 2 sample fusion	0.8177	2.5787	3.8536
NICA - 3 sample fusion	0.8807	2.6092	3.8709

Average Integrity with AL time window 5 min

	IL - 3min	IL - 5min	IL - 12min
NICA	0.4466	1.9715	3.0007
NICA - 2 sample fusion	2.6976	3.43	3.9809
NICA - 3 sample fusion	2.7394	3.4668	4.0013

Average Integrity with AL time window 10 min

	IL - 7min	IL - 10min	IL - 25min
NICA	1.2953	1.8867	2.5353
NICA - 2 sample fusion	3.0053	3.3633	3.6921
NICA - 3 sample fusion	3.0814	3.4393	3.7387

Average Integrity with AL time window 20 min

	IL - 15min	IL - 20min	IL - 50min
NICA	1.3225	1.5708	1.941
NICA - 2 sample fusion	2.4919	2.6985	2.916
NICA - 3 sample fusion	2.5738	2.78	2.9644

Figure 6.9: NICA vs Fusion Models for the Authorised User based on time windows variations

The aforementioned effect of the relativity between the IL time window and AL window is apparent in Figure 6.10 and Figure 6.11. It can be noticed in more detail here (Figure 6.10) how the different combinations affect the original NICA framework

with seeing that the original defined relativeness of the time windows disbenefit the operation whereas the reverse balance between the windows improves as the time windows become larger. Although the former case still provides better security and transparency it makes more apparent that the setting of such framework cannot follow a fit-all-users approach as it very much depends on various factors such as use, timing, user profile and biometric techniques that are likely to affect the efficient performance of the system.

As has been aforementioned and can be seen in Figure 6.11 for the fusion approaches these changes are far more subtle and integrity manages to be maintained in high levels with again the small time windows being a better approach.
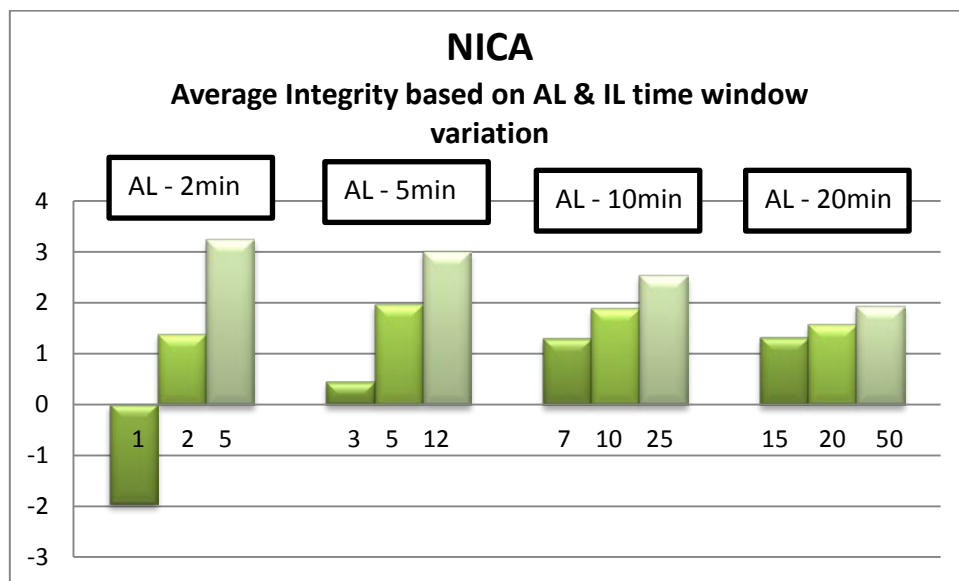
Figure 6.10: NICA performance with time window variation
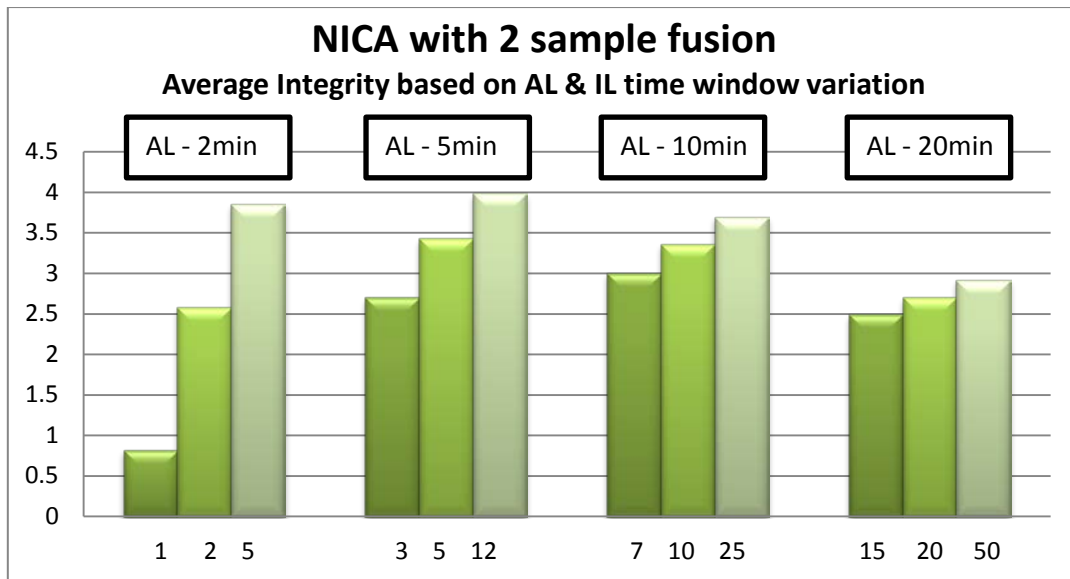
Figure 6.11: NICA with 2 sample fusion with time window variation

Smaller windows do not only operate better in regards of raising integrity due to triggering more frequent authentication but also because it is likely that usage may be concentrated at a particular time period within e.g. each hour. That means that triggering more authentications whilst the device is in use would likely be able to find samples to implement the authentication requests. Figure 6.12 shows the example of a high usage hour whilst NICA is running demonstrating how integrity varies. It can be seen how the availability of samples only exists within a particular interval and the integrity is gradually raised till samples are not present anymore and even if the AL is triggered no authentication is taking place. As such the degradation function is the only operable component that gradually decreased integrity till the end of hour. Figure 6.13 shows the same example when NICA fusion is applied. As can be noticed fusion is able to utilise available samples and therefore achieve higher integrity throughout the hour within that smaller period. As such the benefits of fusion

in conjunction with smaller windows take better advantage of cases when the usage of device is restricted in time as such potentially is at a better position in offering a good level of transparency to the user. Use the following 2 samples to show that integrity does not have the chance to increase as the samples are crowded to only a specific interval.
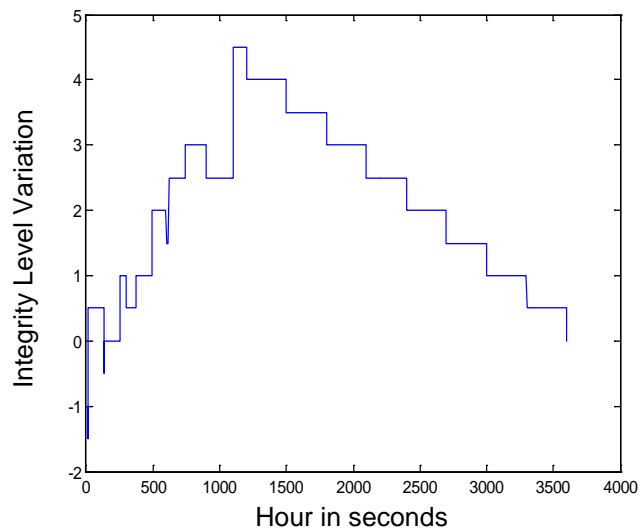
Figure 6.12: Variation of integrity when NICA is applied
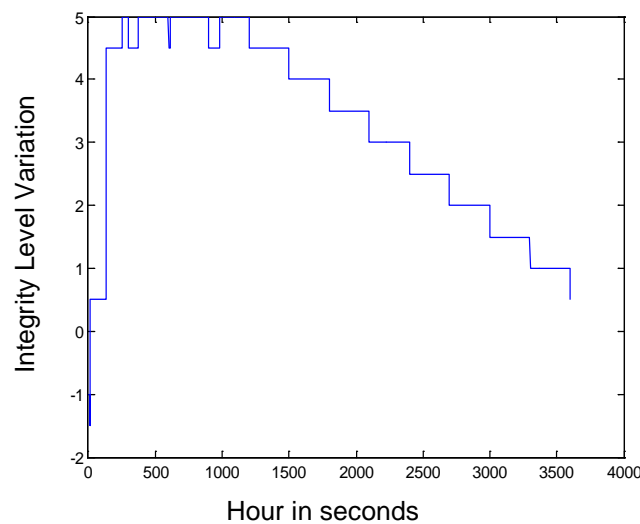
Figure 6.13: Variation of integrity when NICA fusion is applied

6.2.2.2 NICA vs Fusion models - Protected Services Results for Authorised User

To assess the performance of fusion in the protection of protected services and transparency of the approach, a similar simulation to Chapter 5 was implemented. The simulations run for all approaches and all time windows. Table 6-3 presents the results of the simulation for NICA and the 2 new versions relatively to the time windows displaying the average number of intrusive requests occurring per hour in the high usage scenario. These results represent the case the IL was not updated as originally defined by NICA framework.

As can be seen there is a significant reduction of intrusive requests due to the fusion models on all time windows, further underlying that offers a far more transparent approach for the user. These results provide a more representative view of the general average as to how much less intrusive the framework becomes with being able to establish a higher IL even with the use of a further sample. Although it was seen in the previous section that certain changes were more subtle than others that still this translates to a fair amount of intrusive requests which could play a fair role in the transparency of the framework.

	Time Window & Integrity drop			
IL same as AL	AL 2 - IL 2	AL 5 - IL 5	AL 10 - IL 10	AL 20 - IL 20
NICA	25.74	28.12	31.21	34.59
NICA with 2 sample fusion	9.99	12.79	17.66	24.81
NICA with 3 sample fusion	9.48	12.25	17.01	24.23
IL less than AL	**AL 2- IL 1**	**AL 5- IL 3**	**AL 10- IL 7**	**AL 20- IL 15**
NICA	44.06	37.39	34.94	36.17
NICA with 2 sample fusion	16.08	15.89	19.58	26.08
NICA with 3 sample fusion	15.2	15.28	19.02	25.55
IL more than AL	**AL 2- IL 5**	**AL 5- IL 12**	**AL 10- IL 25**	**AL 20- IL 50**
NICA	16.19	22.09	27.01	32.3
NICA with 2 sample fusion	7.33	11.27	16.31	23.83
NICA with 3 sample fusion	7.05	10.91	15.92	23.45

Table 6-3: NICA vs Fusion – Number of intrusive requests as a result of accessing protected services during high usage with no integrity update as series of events or as independent events during the hour (57 services per hour)

It can be seen here more clearly than the previous section is that smaller windows seem to perform better here as well in most cases for the different versions of AL and IL timings. Given the analysis of the overall results, the degradation function does not seem to be the key player in the transparency of the framework here as in occasions that it is triggered more often that still maintains a fair level of access. The downside here seems to be the missed opportunities for authentication that could affect integrity and the luck of integrity increase during an active usage period.

As has been aforementioned the translation of the results is 2 fold. The results in Table 6-3 show not only intrusiveness of NICA with no updates in case of the scenario of all protected services occurring as a series of events but also any of

them occurring proving further the outperforming of fusion with a significant improvement in transparency.

When introducing the update on integrity as a result of the intrusive request on protected service, the result with fusion further improves (Table 6-4). With the results presented on high usage profiles it can be seen that such approach makes the framework far more transparent for the user whilst managing to establish a good level of trust.

	Time Window & Integrity drop			
IL same as AL	AL 2 - IL 2	AL 5 - IL 5	AL 10 - IL 10	AL 20 - IL 20
NICA	7.16	5.06	3.92	3.07
NICA with 2 sample fusion	4.84	3.71	3.1	2.61
NICA with 3 sample fusion	4.82	3.7	3.1	2.61
IL less than AL	**AL 2- IL 1**	**AL 5- IL 3**	**AL 10- IL 7**	**AL 20- IL 15**
NICA	10.82	6.55	4.73	3.64
NICA with 2 sample fusion	7.75	5.23	4.05	3.34
NICA with 3 sample fusion	7.74	5.23	4.05	3.34
IL more than AL	**AL 2- IL 5**	**AL 5- IL 12**	**AL 10- IL 25**	**AL 20- IL 50**
NICA	4.75	3.66	2.92	2.4
NICA with 2 sample fusion	3.38	2.97	2.59	2.33
NICA with 3 sample fusion	3.37	2.97	2.59	2.33

Table 6-4: NICA vs Fusion – Number of intrusive requests as a result of accessing a protected service during high usage as a series of events with integrity update (57 services per hour)

Here it can be seen that the smaller the window the intrusive requests increase by close to 1 and fusion performs for that amount better. Here the effect of the degradation function within the larger windows has little to no effect considering it takes place once or twice during the hour. In contrast with the original NICA the degradation function differences are more apparent here although appears to again play a small role given the little difference in the results. The amount of improvement in fusion is less in comparison to the original NICA with no integrity updates during

protected service access however still shows that it can be a better solution given sample availability as it can reach higher integrity in a shorter amount of time.

6.2.2.3 NICA vs Fusion models - Protected Services Results for Impostor

To assess the performance of each approach for an impostor a series of two tests took place. One was looking at the system starting from IL=0 and the other starting from IL=5 at the beginning of each hour. That would give the opportunity to see the response of the system so much after a period of inactivity as well as the occasion of an impostor accessing the device directly after an authorised user has established the highest levels of integrity and assess the opportunities of misuse. The results presented in Table 6-5 and Table 6-6 represent the occasion of an impostor accessing any of the protected services at their given time as independent events though the hour examining how many services would an impostor be able to access in an effort to access the device at any of these times.

	Time Window & Integrity drop			
IL same as AL	**AL 2 - IL 2**	**AL 5 - IL 5**	**AL 10 - IL 10**	**AL 20 - IL 20**
NICA	0.0313	0.0587	0.0914	0.1567
NICA with 2 sample fusion	0.0248	0.0431	0.0718	0.1162
NICA with 3 sample fusion	0.0248	0.0431	0.0718	0.1162
IL less than AL	**AL 2- IL 1**	**AL 5- IL 3**	**AL 10- IL 7**	**AL 20- IL 15**
NICA	0.03	0.0522	0.0888	0.1514
NICA with 2 sample fusion	0.0248	0.0431	0.0718	0.1162
NICA with 3 sample fusion	0.0248	0.0431	0.0718	0.1162
IL more than AL	**AL 2- IL 5**	**AL 5- IL 12**	**AL 10- IL 25**	**AL 20- IL 50**
NICA	0.0339	0.0601	0.0914	0.1567
NICA with 2 sample fusion	0.0248	0.0431	0.0718	0.1162
NICA with 3 sample fusion	0.0248	0.0431	0.0718	0.1162

Table 6-5: Number of protected services accessed by an impostor during high usage as independent events starting at IL=0 (57 services per hour)

As seen in Table 6-5 there is a small opportunity of misuse due primarily to false positives which translates to accessing the lowest security services defined at 0 which basically means basic use of the device by the same amount presented in the table. Of course this may increase depending on the false positives that may occur. When running the same experiment under the scenario of accessing the protected services as a series of events and therefore the intrusive interface would be invoked at the first occasion of accessing a protected service without the required security (where the simulation in the hour would end as well unless there was a false positive), the results showed a 0.0068% possibility of accessing any services almost diminishing any misuse. Fusion with 2 or 3 samples show no differentiation as the integrity that can be achieved did not change much between the two approaches.

The more representative and stress test is when starting at IL=5 the results of which are presented in Table 6-6. As can be seen for all windows there is close to at least an opportunity of accessing a protected service which translates of accessing close to 1 protected service per hour with that possibility increasing as the windows get larger (as would be expected). This time this does not only translate to access of only low security services but also to highly protected services however with a small amount of 0.035% for level 5 and 0.14% for level 4 leading down to 0.65% for basic usage for the best performing windows of AL-2 & IL-5. Full breakdown of the results can be found in Appendix D.

	Time Window & Integrity drop			
IL same as AL	**AL 2 - IL 2**	**AL 5 - IL 5**	**AL 10 - IL 10**	**AL 20 - IL 20**
NICA	1.0718	1.4791	2.0783	3.0339
NICA with 2 sample fusion	1	1.312	1.7742	2.3016
NICA with 3 sample fusion	1	1.312	1.7742	2.3016
IL less than AL	**AL 2- IL 1**	**AL 5- IL 3**	**AL 10- IL 7**	**AL 20- IL 15**
NICA	1.0209	1.3903	1.9883	2.9138
NICA with 2 sample fusion	0.9634	1.2337	1.6958	2.2298
NICA with 3 sample fusion	0.9634	1.2337	1.6958	2.2298
IL more than AL	**AL 2- IL 5**	**AL 5- IL 12**	**AL 10- IL 25**	**AL 20- IL 50**
NICA	1.141	1.5653	2.2689	3.3238
NICA with 2 sample fusion	1.0718	1.3956	1.9426	2.564
NICA with 3 sample fusion	1.0718	1.3956	1.9426	2.564

Table 6-6: Number of protected services being accessed by an impostor during high usage as independent events starting at IL=5 (57 services per hour)

Table 6-7 shows the results when an impostor is trying to access the protected services as a series of events. Here there is again an improvement although more subtle which is however expected given the small window that there is any chance to misuse the device. Nevertheless it appears that fusion has a better chance to close down access in comparison with NICA whilst the window is small enough as there is going to be a bigger drop in integrity. The latter counteracts the possibility of false positives and impacts on the integrity far greater than the degradation function.

IL same as AL	Time Window & Integrity drop			
	AL 2 - IL 2	**AL 5 - IL 5**	**AL 10 - IL 10**	**AL 20 - IL 20**
NICA	0.8185	0.9478	1.124	1.3916
NICA with 2 sample fusion	0.7781	0.8864	1.0574	1.3094
NICA with 3 sample fusion	0.7781	0.8864	1.0574	1.3094
IL less than AL	**AL 2- IL 1**	**AL 5- IL 3**	**AL 10- IL 7**	**AL 20- IL 15**
NICA	0.7924	0.906	1.0614	1.3198
NICA with 2 sample fusion	0.7585	0.8446	0.9948	1.2389
NICA with 3 sample fusion	0.7585	0.8446	0.9948	1.2389
IL more than AL	**AL 2- IL 5**	**AL 5- IL 12**	**AL 10- IL 25**	**AL 20- IL 50**
NICA	0.8251	0.9491	1.124	1.3916
NICA with 2 sample fusion	0.782	0.8877	1.0574	1.3094
NICA with 3 sample fusion	0.782	0.8877	1.0574	1.3094

Table 6-7: Number of protected services being accessed by an impostor as series of events during high usage at IL=5 (57 services per hour)

The same series of tests were performed for the random sets of 20 protected services starting at IL=5 as a better stress test. Table 6-8 shows the results for all versions proving only here the best performing windows in general. For a set of results please refer to Appendix D. Here all versions seem to perform well compared to each other with little change; leaving misuse opportunities with the majority being at lower risk services with a 1.65% and 1.5% possibility of falsely access by an impostor for fusion as independent events and a series respectively till the framework manages restrict access.

	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
	As independent events				As a series of events			
NICA	0.4634	0.6449	0.8668	1.1971	0.3172	0.376	0.4648	0.5326
NICA with 2 samples	0.4504	0.6057	0.782	1.0261	0.3094	0.3616	0.4386	0.5065
NICA with 3 samples	0.4504	0.6057	0.782	1.0261	0.3094	0.3616	0.4386	0.5065

Table 6-8: Possibility of a protected service being accessed by an impostor during high usage for random timed protected services (20 services per hour)

6.3   Discussion & Conclusion

This chapter looked at the application of fusion within the NICA framework seeking to see the effect on its performance. After introducing modifications to the NICA mechanisms to incorporate fusion, a series of experiments showed that the fusion approaches give an improvement compared to the original framework over various timing windows. Fusion seems to be able to maintain a better trust on the authorised user based on the given usage scenarios whilst utilising the available biometric samples. Given availability of samples, fusion offers a more confident result and therefore being able to raise integrity at higher levels and providing better transparency. Even though the improvements in terms of the integrity maintained are subtle in some cases it stills offers a more trustworthy approach, as decisions when applicable are based on more than one sample. That is a two-fold benefit not only in the ability of raising the integrity but also possibly lowering the possibility of misuse straight after the use by an authorised user since the presence of authorised samples would not be able on their own to permit access. In NICA, the most recent sample with higher confidence could be that of an authorised user given particular timings. With fusion that effect can be possibly counteracted.

The improvement was found to be subtle for the best combinations of time windows however by fusion performing better compared to the one-sample approach in different time window combinations shows that it offers a more flexible and dynamic approach in comparison to the latter more linear approach. Given that the series of these experiments was testing the data only taking into account the biometric EERs without taking into account the environmental conditions it is believed that the

performance of fusion and one-sample approach is closer that it would be in real conditions. As mentioned in the beginning of this chapter fusion is expected to be more tolerant to FRR due to bad and/or mobile conditions given that the decision is based on more than one sample and/or technique.

The operation of fusion and the change in the decision process so that the AL does not reset to L1 after a successful one sample authentication gave the opportunity to the framework raise better levels of integrity whilst at the same time providing better protection to the device a FAR due to a bad sample or failing of a biometric algorithm would not provide access to an impostor for the duration of the AL hibernation.

Fusion seems to also operate better across all levels of usage activity. Although the difference is not substantially large compared to one-sample authentication it is considered a more confident decision based system and in far less intrusive. This can be seen particularly in the protected service results based and on how NICA was originally defined. In the event of a protected service access NICA would utilise the IL simply as a monitoring mechanism in such event causing no change in IL. That produced a largely intrusive mechanism as even though the user would gain access to a protected service their current IL status at that particular moment would not be raised and the AL would also hibernate. Given cases where protected service access continues the user would keep getting intrusive interfaces going through the same process with no chance for the IL to be raised in a state that allows for transparent use of the device. At these occasions the application of fusion brought better results as it gave the framework the opportunity during usage of the device to maintain a heightened level of integrity and thus making the framework far less

intrusive. The introduction on the IL change at any case of intrusive authentication further counteracted the intrusiveness of original NICA with the results showed that introduces a significant improvement in all NICA versions. Given the large number of protected services tested here it is expected that scaling this down to normal operation the percentage of intrusive requests could be minimal however that would depend on the timing of access relevantly to the at time use of the device. Given a period of inactivity the user would need most likely to authenticate for a high security usage as though is the purpose of the framework and thus protect the device from unauthorised access.

As seen in the results and the different variations that are possible there is need to configure the framework to match the usage of the device. Given that for low, medium and high usage there is a difference in performance as well as the complication that the time variables bring to the framework's operation is unsure as to how it would best suit a particular user. As seen in the initial analysis of the datasets as well the usage of the device is not subjective to particular periods and as such it would not be easy to establish a fit all configuration regarding time windows that would provide the optimal configuration for both transparency and security at all times.

7 CASper – a New Framework Approach

The simulation of NICA and the enhanced approaches gave an insight to the large variability of the factors affecting authentication. The amount of settings that are required and the different options that exist create a problem from a practical perspective. For example, what are the most appropriate time windows for each type of usage and user. The objectivity that is required in the definition of those variables poses a problem to the way that the framework currently operates. This trade-off between offering flexibility and a user-specific configuration of the authentication mechanism becomes very apparent when setting those variables and realising the impact they have upon authentication.

7.1 CASper Enhancement Model

To try to counteract the above issues a different approach was sought that would provide a solution to the security and usability trade-off without the challenges of defining the variables. The approach moves somewhat away from the multi-level approach whilst keeping the multi-sample fusion authentication that appears to help the authentication decision. The simulation of the protected services component showed that monitoring based upon the confidence level was operating well in both approaches and thus this was an aspect of the framework that was kept within this new concept.

Identifying the problems of the AL and IL time windows and their interconnectivity and dependencies it was considered that tying those 2 aspects together would provide an easier and a more realistically configurable framework. Given that these

may be aspects that a user needs to set there needs to be a way of providing a more usable approach and one that a user can easily become familiarized with and understand the consequences of the settings - to the extent that user awareness allows. Given that the possible stakeholders selecting to utilise such mechanism would have a certain level of privacy concerns and possibly business requirements a certain level of awareness would be expected. But also for a simple home user it is an easier to understand approach – by implementing a 'trust on-trust off' mechanism, something that is closer what an average user can comprehend in regards to security.

The approach to merge the AL and IL together was achieved with rather than providing 2 timed events with possible opposite effect on the system – of one seeking to maintain/raise and the other lower integrity, one timed event would take place. That event would seek for appropriate authentication samples and modify the integrity of the system based on the authentication decision in a weighted manner depending on the number of samples pursuing 2 sample fusion that showed confident performance. The 3 sample fusion approach was not pursued for testing this approach as showed minimal differentiation in these set of tests, however given the setting of the approach any type of multilevel fusion can be incorporated. In the event of a successful result the integrity would be raised accordingly whilst maintaining access to the device and the AL mechanism would be reset and retriggered in x minutes. Otherwise the authentication would be triggered again seeking for the next available and timely samples. If authentication requests are

failing, the system would keep dropping the integrity level till it reaches its minimum value of -5 where the system would be locked leading to the respective AL level 6.

The degradation function as originally defined has been removed. Since the user has gained the integrity at a specific time and by defining a small enough time window of retriggering the AL mechanism there is little scope to decrease integrity as it is assumed that the user continues to use the device. In this way the authorised user is not negatively affected by a periodic drop of the integrity that eliminates the effect the authentication has achieved so far –something that was also a restrictive outcome of the evaluation. At the event the AL mechanism retriggers and that no samples are present, then integrity of the system is reset at 0 and keep waiting for the next available sample. This would be representing a case of inactivity and therefore the trust to the user resets to minimum. In this way no window of misuse is left open which essentially also means no access of protected services. In the case that an impostor will pick up the device then CASper due to the continuous monitoring would continue to decrease the integrity (unless FARs occur constantly) and thus restricting access to any services till lock down of the device. This counteracts the presence of the degradation function by targeting to establish a balance between security and transparency of operation. Even if the impostor have picked up the device straight after an authorised user which would mean that authorised samples are going to exist in Cache, using the fusion approach it increases the possibilities of rejecting the impostor. Although CASper provides more flexibility to the impostor as well as it may take more authentications to reach the device lock that it may in NICA, the use of the integrity for accessing any services would provide protection and restriction to that

anyway and therefore not risking the accessing of sensitive data or services. At the same time resetting integrity to 0 rather than locking access does not lock access to any basic use of the device. The CASper algorithm operation is depicted in Figure 7.1. As can be seen CASper does not quite have levels as NICA. There is primarily a cyclical operation of looking for samples kind of representing a loop between the L1 and L3 (–if reached) of NICA. All access is controlled via the IL. In the particular implementation as no intrusive stages are concerned device lock occurs when IL reaches -5. In a more generic specification of such approach a series of intrusive stages could be introduced at -5 or even at any level under IL of 0 and therefore provide a staged shut down of the device at any failed request after that. That could be a user or an administrator preference to be set up during device configuration. However, given the way the algorithm works, it is considered that defining an intrusive authentication at every level under 0 could trigger frequent intrusive requests in cases of inactivity. Essentially this is a surpass of levels which are now controlled by the IL in regards to how many opportunities the user gets. In that way restricted access is achieved however without a set number of efforts that the user gets.
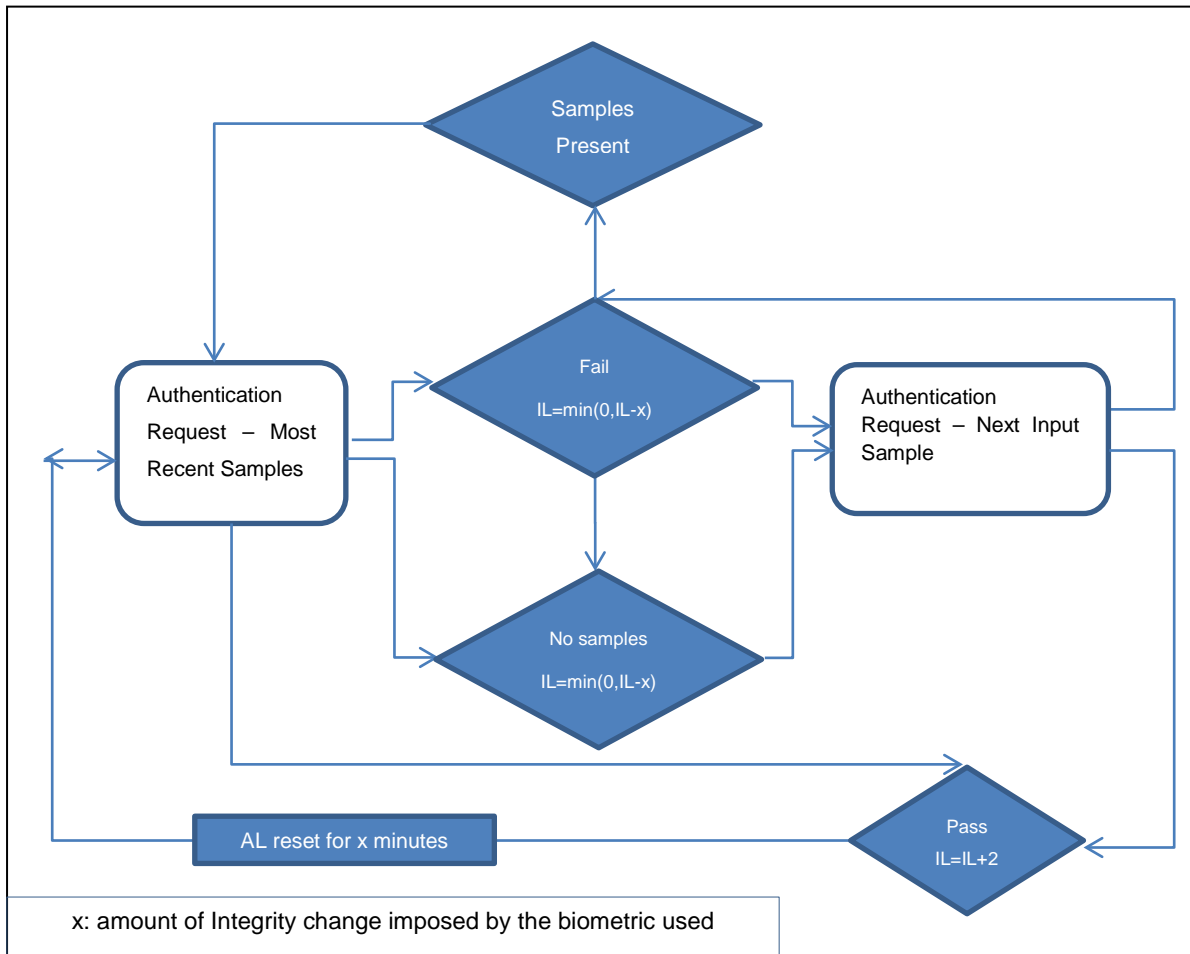
Figure 7.1: CASper Alert Level Mechanism

The predefined degradation function which is meant to reduce the confidence to minimise chances of inactivity, has a minimal effect as the amount of change is small and will take a long time to reset integrity to 0 as has been seen before as well as keeping integrity at a certain levels whilst there may be no activity on the device. In CASper this is done automatically with a small disadvantage however to transparency. For example after a period of inactivity if the user tries to access a protected service straight away they would be experiencing an explicit authentication. However this trade-off is considered less significant in comparison to

the security as given the previous approach the window of misuse becomes bigger. At any time if a request comes for a protected service the operation follows the same approach as to assessing whether the current integrity matches the security criteria. If not then explicit authentication would be requested as normal again updating the integrity level accordingly. In the event of an unsuccessful authentication whilst accessing a protected service the framework will continue the same operation while zeroing integrity. Given that high confidence techniques would be used like B3 which would be modifying the integrity by 2 this would mean that till the lock down of -5, 3 intrusive requests would be reached at maximum before lock down and therefore giving at worst case scenario 1 more intrusive stage to the user compared to NICA. However given that the integrity of the system is lowered at the same time access to any services is protected at any case and therefore the security of the system is not compromised.

At the same time this approach although it does not necessarily offer an intrusive opportunity by default after 3 transparent fails as NICA, it does still allow the use of the device by an authorised user in the event of bad conditions that would restrict fair acquisition of some techniques for authenticating the user providing some opportunity of getting good samples. Although access to protected services may be restricted the user can still have any pre-defined basic use of the device and when they wish to access a protected service then of course they would need to provide explicit authentication as would happen in NICA as well. If they reach the predefined level that would provide them with an intrusive authentication opportunity this would raise the integrity level and more opportunities exists of regaining the trust to the

authorised user by looking for samples whilst not locking the device and not burden the integrity further by a periodic drop at the same time. Something that in the event of the impostor would act negatively as the trust would be continuously dropping under constant authentication whilst restricting access to services. In both NICA and CASper, these opportunities are given to counteract also poor environmental conditions however it does not necessarily mean that it would allow for the biometric techniques to work even intrusively as for example a noisy or a dark environment would not allow for good samples regardless of the way of acquisition. As such in both systems the intrusiveness may exists more than envisaged as the performance relies on samples and algorithm performance.

With these modifications several aspects are simulated and substituted with one function and simplifying the operation as well as the setting of the framework. The requirement of different variables setting is minimised and the only requirement remains the definition of the one timed event – that being the triggering of the AL mechanism. At the same time transparency is maintained at all times apart of lock down or access of protected services.

7.2   CASper Simulation Results

The simulation for CASper followed a similar approach to NICA and fusion models with the same datasets. In regards to the simulation in this case only one timing variable needed to be set and that is the triggering of the authentication mechanism – the CAS window. The windows used to be tested here were 2, 5, and 10 minutes. Taken the lessons learned and the aforementioned discussion of triggering of the

authentication mechanism every 20 minutes being insufficiently long it was not used in this simulation.

In these series of tests looking at the average integrity across the hour CASper did not appear at first to manage to maintain high levels of average integrity compared to similar time windows with NICA versions. As can be seen in Figure 7.2 CASper maintains low average integrity across the hour however appear to be consistent regardless the time window in comparison with NICA which varied in cases close to 1 degree depending on the time window. This may translate to a more consistent solution regardless configuration but that is to be examined from the further results. The low percentages of average integrity in comparison to NICA were not an unexpected result. Given that CASper operates on a binary state of some or no Integrity whilst no samples are present or a fail authentication occurs does not keep the integrity raised as NICA does. NICA maintains the integrity between authentication windows as the degradation function only modifies it by a small amount. That provides of course a better average with leverage on transparency and a trade-off to security. Given the difference in operation makes here average integrity not great means of comparison as was for NICA versions. The later results of demonstrating transparency and security during protected service access provides a better insight where the basis for protection of the framework lies.

CASper performance for Authorised User on High Usage

	2	5	10
■ HighU	1.6977	1.6463	1.6468
■ MediumU	1.0155	0.9651	1.07
■ LowU	0.4528	0.4369	0.5859

Average Integrity (y-axis, values 0 to 1.8)
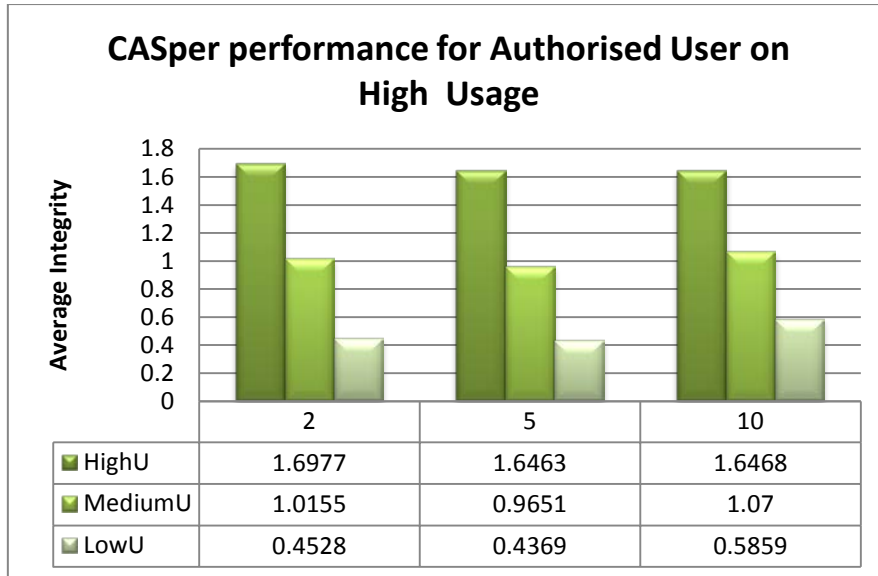
Figure 7.2: CASper average Integrity for the authorised user during high usage hours

Figure 7.3 demonstrates the average integrity of CASper across the different hours of high usage showing an increase of average integrity towards the right side of the graph that represents hours with higher sample availability. Given the possibility of more samples CASper may have the ability to maintain higher levels of integrity for the particular active periods as in each authentication the integrity can be increased or at least maintained due to authentication being able to take place. However is not expected to ever be higher from NICA as aforementioned due to its binary 'on-off' mechanism.
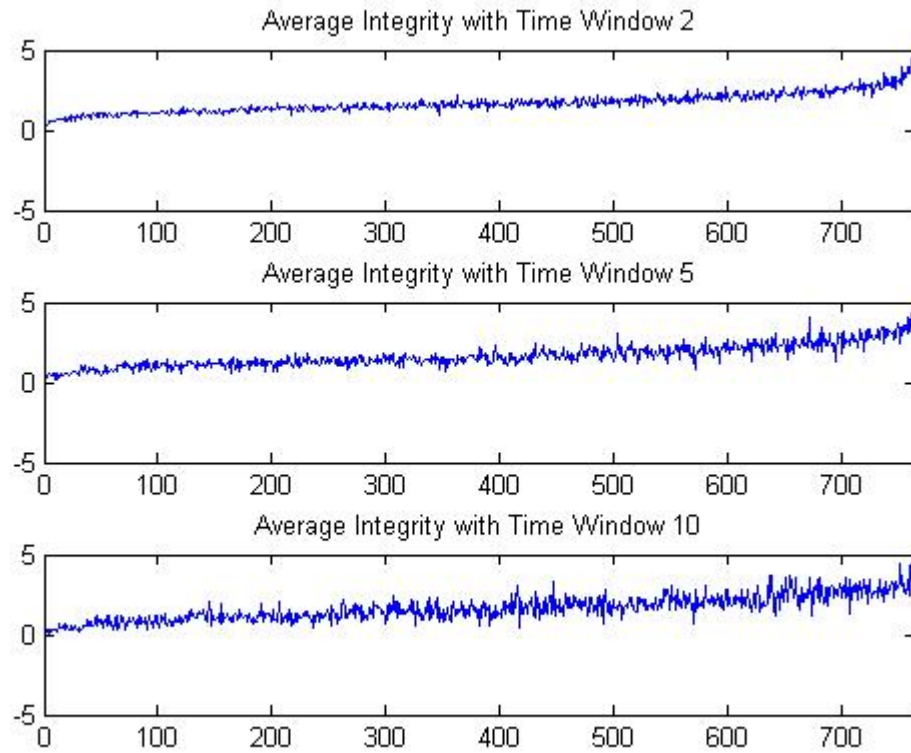
Figure 7.3: CASper average integrity in all high usage hours by increasing number of samples

Simply for demonstration reasons the impostor percentages are also presented here where CASper shows the similar averages as NICA does. However the security against an impostor needs to be assessed with the protected service access tests.
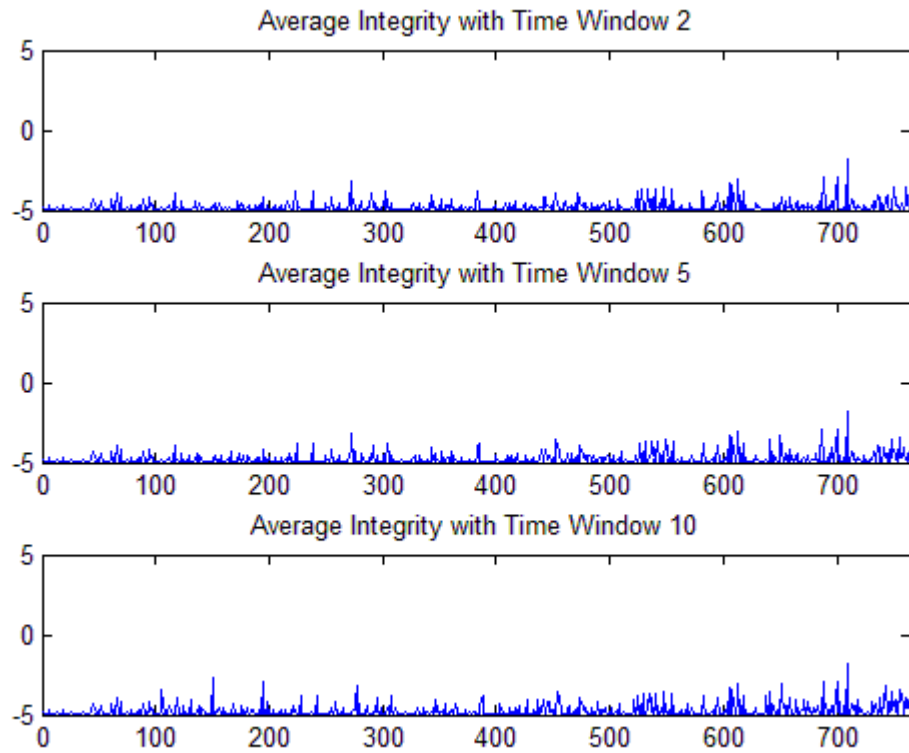
Figure 7.4: CASper average integrity for an impostor during high usage hours.

To provide a representation of the difference between the two algorithms Figure 7.5 shows how integrity changes during a random hour for NICA and CASper.
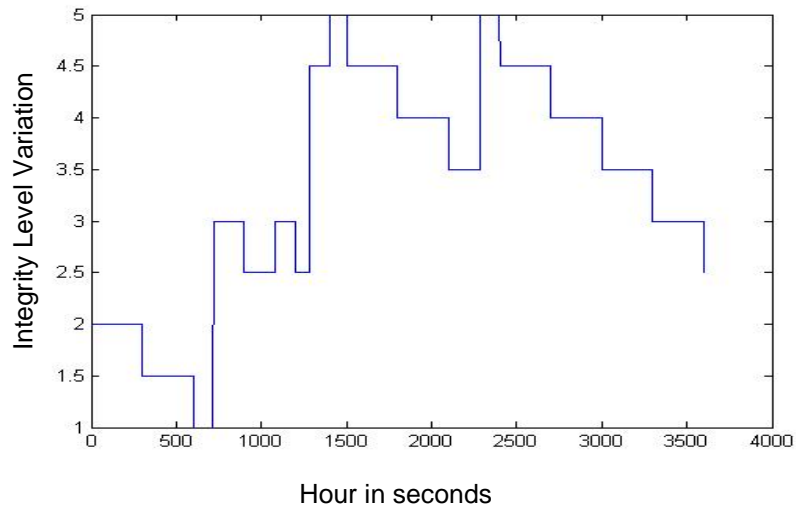
(a) NICA
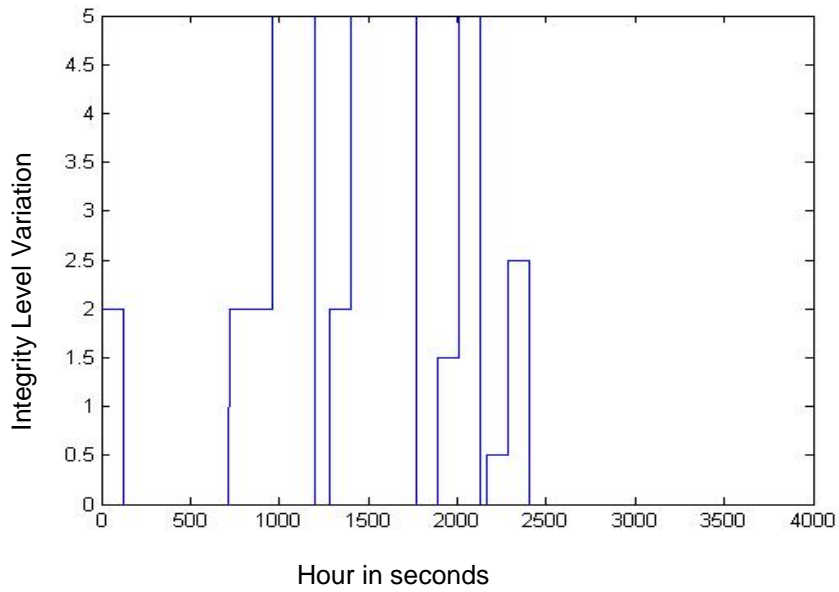
(b) CASper

Figure 7.5: NICA(a) & CASper(b) integrity changes during an hour

As can be seen from the figures NICA manages to maintain its average integrity high due to the degradation function whereas CASper operates binary and although it allows for the integrity to be raised in high levels by the close of windows or failed authentication it zeros integrity closing any window for misuse. That leads to the need to rebuild the integrity from 0 each time samples are not present or fail. NICA on the other side maintains any gained integrity for longer offering good transparency but lower security. As can be seen from the particular example in Figure 7.5(a) although the last sample used and present was at close to minute 40 for 20 minutes after the integrity is maintained down to 2.5 of course at no use of the device. If during that period there was some use of the device there is the possibility for unauthorised access which however depending on the timing of the access in relation to the alert level triggering could be counteracted by running 2-3 authentication requests. CASper on the other side drops that possibility by directly closing the window after 2 min (in this example of window). But furthermore in the event of an impostor accessing a device only one unauthorised sample (with the exception of a false positive) would deny service access directly.

7.2.1 Protected services Results

7.2.1.1 Authorised User

The same series of datasets used in NICA were used to test the tolerance of CASper mechanism. As discussed earlier no intrusive levels where defined here apart from device lock and therefore the simulation of each hour stops at IL=-5 by continuously dropping integrity as normal. The results (Table 7-1) appears to be a bit more intrusive than NICA for the best performing windows as again expected given the

automatic integrity drop. In the initial tests the integrity updates would occur in transparent authentication were also applied here including a zeroing of integrity in case of fail. The subtle improvement that occurs with larger time windows makes the system a bit more transparent but it is to be accessed in relation to an impostor accessing the system as well.

	Authentication Window		
Level of Usage	2	5	10
High (57 services per hour)	6.5875	5.7141	4.5966
	(11.5%)	(10.0%)	(8.0%)
Medium (26 services per hour)	5.7376	5.2363	4.3512
	(22.1%)	(20.2%)	(16.8%)
Low (10 services per hour)	3.4399	3.2885	2.9204
	(34.4%)	(32.9%)	(29.2%)

Table 7-1: Number of Intrusive Requests as a result of accessing a protected service during high usage with integrity updates as series of events

However, looking to improve the approach given the binary operation of CASper consideration was given to the way that integrity updates work. In NICA they were introduced to take advantage of an authentication requests that in the original specification the user was not getting benefit from. Whilst accessing a protected service and getting authenticated the trust of the system could still be quite lower. So e.g. after inactivity the user may have trust of 1 getting authenticated for a service of level 5 and remain at integrity 1 whilst accessing a highly secure service. Even with the integrity updates that oxymoron still stands as even if the integrity still gets heightened at 3 with B3 level technique the user still accesses services which does not appear to have the integrity for. As such it was considered that CASper

particularly given its binary operation would benefit in transparency whilst an intrusive request as a result of protected service access occurs the integrity of the system to match the required integrity of the protected service that they are accessing. As such although CASper would always be a bit more intrusive it gives a user the opportunity during protected service access whilst the device in use to maintain the privileges gained by any intrusive requests and better represent the level of trust. Table 7-2 shows the results when the absolute match to the protected accessed each time is presented providing a small improvement to the system however what is believed a more representative trust to the user. The particular improvement comes from level 4 and 5 services in occasions where the user would not have the chance to always reach the integrity required with transparent authentication. Regarding the levels of usage CASper matches NICA performance in all types by a varying degree of 0.5-1.5 more intrusive requests per hour in all cases showing a standard comparative performance regardless the usage.

Level of Usage	Authentication Window		
	2	5	10
High (57 services per hour)	5.6227 (9.8%)	4.765 (8.3%)	3.7794 (6.6%)
Medium (26 services per hour)	4.9491 (19.1%)	4.4373 (17.1%)	3.624 (14.0%)
Low (10 services per hour)	3.0914 (30.9%)	2.8969 (29.0%)	2.5209 (25.2%)

Table 7-2: Number of Intrusive Requests as a result of accessing a protected service during high usage with integrity updates as series of events to match the level of service integrity requirements

Compared to fusion the difference for high usage translates to 0.5-2.2 more intrusive requests for CASper which out of the 57 protected services that are being accessed does not seem to cause a significant downside to transparency. The break down compared to NICA fusion is presented in Table 7-3. It can be seen that CASper closely matches the scores of fusion and although there is a very small improvement coming at higher protected services it does not seem to be of statistical significance.

Integrity Required	2	5	10	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
	Casper with Update in Integrity			NICA fusion with 2 samples with Update in Integrity			
0 (9.4 services per hour)	0.01 (0.1%)	0.01 (0.1%)	0.01 (0.1%)	0 (0.0%)	0 (0.0%)	0 (0.0%	0 (0.1%)
1 (9.7 services per hour)	0.21 (2.2%)	0.17 (1.8%)	0.13 (1.3%)	0.06 (0.6%)	0.06 (0.6%)	0.06 (0.6%)	0.06 (2.2%)
2 (9.7 services per hour)	0.73 (7.5%)	0.57 (5.9%)	0.41 (4.2%)	0.16 (1.6%)	0.17 (1.8%)	0.17 (1.8%)	0.17 (7.5%)
3 (9.8 services per hour)	1.13 (11.5%)	0.89 (9.1%)	0.68 (6.9%)	0.31 (3.2%)	0.32 (3.3%)	0.33 (3.4%)	0.33 (11.5%)
4 (9.4 services per hour)	1.44 (15.3%)	1.2 (12.8%)	0.93 (9.9%)	0.52 (5.5%)	0.53 (5.6%)	0.55 (5.9%)	0.57 (15.3%)
5 (9.2 services per hour)	2.11 (22.9%)	1.93 (21.0%)	1.61 (17.5%)	2.33 (25.3%)	1.88 (20.4%)	1.48 (16.1%)	1.19 (22.9%)

Table 7-3: Number of intrusive requests generated on average per hour due to protected service access of each trust level (based on high usage and best EERs)

The results for random protected services following the absolute integrity match are presented in Table 7-4. As it can be seen CASper does not achieve the transparency of NICA fusion with generating close to 1.8 intrusive requests more than NICA, matching a near 20% of intrusiveness compared to than 11% of NICA fusion in 20 protected services. What can be noticed is that CASper gradually increases intrusiveness whereas NICA fusion is highly transparent for lower security services while becoming a bit more intrusive for services of level 5 - making NICA fusion a more appropriate choice here.

Integrity Required	2	5	10	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
	Casper with Update in Integrity			NICA fusion with 2 samples with Update in Integrity			
ALL(0-5) (20 services per hour)	4.094	4.004	3.401	2.285	2.257	2.201	2.14
0	0	0	0	0	0	0	0
1	0.41	0.36	0.24	0.03	0.05	0.06	0.03
2	0.59	0.52	0.42	0.07	0.12	0.15	0.07
3	0.85	0.81	0.64	0.17	0.27	0.33	0.17
4	0.95	0.95	0.82	0.34	0.4	0.52	0.34
5	1.29	1.36	1.28	1.66	1.42	1.15	1.66

Table 7-4: Number of intrusive requests generated on average per hour due to 20 random timed protected service access of each trust level (based on high usage and best EERs)

7.2.1.2 Impostor

As seen in the previous section CASper matches or is a bit more intrusive than NICA and NICA fusion when it comes to protected service access. Comparison for the security of CASper is provided here regarding the ability of CASper to lock down access to protected services. The results of the latter for false positive access when protected services are access as a series of events throughout the hour with IL starting at 0 and 5 are depicted in Table 7-5. Results for NICA fusion are also presented for comparison. In regards to security CASper matches NICA performance in locking access for IL=5 but performs better than NICA fusion particularly evidently in the stress test of starting at IL=5. CASper manages in all 3 types of usage to restrict access and with low percentages. For IL=0 there isn't much differentiation as the periodic zeroing out of CASper and the intrusive interface of NICA do not give much opportunity for access anyway.

Integrity Required	2	5	10	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
	Casper			NICA fusion with 2 samples			
	IL=0			IL=0			
High (57 services per hour)	0.0039 (0.01%)	0.0039 (0.01%)	0.0039 (0.01%)	0.0039 (0.01%)	0.0039 (0.01%)	0.0039 (0.01%)	0.0039 (0.01%)
Medium(26 services per hour)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Low (10 services per hour)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
	IL=5			IL=5			
High (57 services per hour)	0.2755 (0.48%)	0.3812 (0.67%)	0.547 (0.96%)	0.7820 (1.37%)	0.8877 (1.55%)	1.0574 (1.85%)	1.3094 (0.48%)
Medium (26 services per hour)	0.1710 (0.66%)	0.1828 (0.70%)	0.1932 (0.74%)	0.6436 (2.48%)	0.6645 (2.56%)	0.6775 (2.61%)	0.6906 (0.66%)
Low (10 services per hour)	0.1671 (1.67%)	0.1671 (1.67%)	0.1671 (1.67%)	1.1501 (11.51%)	1.1671 (11.68%)	1.1749 (11.76%)	1.1815 (1.67%)

Table 7-5: Number of Protected services accessed by an impostor per hour on average during all types of usage as series

When the protected service happens as independent events in the hour so testing access from an impostor at any given time CASper again shows better performance when noticing the stress test of IL=5 as can be noticed in the results presented in Table 7-6. For IL=5 shows how the gradual decrease in NICA during periods of inactivity may increase the chances of misuse whereas with CASper most likely the

zeroing out in IL largely minimizes the same opportunities. Particularly evident in lower levels of usage when with high inactivity the integrity would still remain high for large periods of time with no evidence of the user's identity. Here as with the authorised user whereas with NICA one can notice large variations depending on the time window, CASper shows a more consistent approach with closely matching performance in all cases.

Integrity Required	2	5	10	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
	Casper			NICA fusion with 2 samples			
	IL=0			IL=0			
High (57 services per hour)	0.0339 (0.06%)	0.0561 (0.10%)	0.0901 (0.16%)	0.0248 (0.04%)	0.0431 (0.08%)	0.0718 (0.13%)	0.1162 (0.20%)
Medium (26 services per hour)	0.0039 (0.02%)	0.0078 (0.03%)	0.0183 (0.07%)	0.0026 (0.01%)	0.0026 (0.01%)	0.0065 (0.03%)	0.0091 (0.04%)
Low (10 services per hour)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
	IL=5			IL=5			
High (57 services per hour)	0.3355 (0.59%)	0.4765 (0.83%)	0.6762 (1.18%)	1.0718 (1.87%)	1.3956 (2.44%)	1.9426 (3.39%)	2.5640 (4.48%)
Medium (26 services per hour)	0.2037 (0.79%)	0.2272 (0.88%)	0.2454 (0.95%)	0.7624 (2.94%)	0.9164 (3.53%)	1.0274 (3.96%)	1.2428 (4.79%)
Low (10 services per hour)	0.1906 (1.91%)	0.1906 (1.91%)	0.1906 (1.91%)	1.8094 (18.11%)	1.8943 (18.96%)	1.9922 (19.94%)	2.0261 (20.28%)

Table 7-6: Number of Protected services accessed by an impostor per hour on average during all types of usage as independent events

Table 7-7 presents the breakdown of the above 2 scenarios in regards to the security level of the protected services that are being accessed for the IL=5 case. It can be seen that for the protected services at level 5 there is not much opportunity for misuse utilising either approaches. For lower level services CASper outperforms in all cases.

Integrity Required	2	5	10	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
	Casper Independent Protected Access			NICA fusion with 2 samples Independent Protected Access			
ALL	**0.3355**	**0.4765**	**0.4765**	**1.0718**	**1.3956**	**1.9426**	**2.5640**
0	0.2350	0.2846	0.3446	0.3564	0.4909	0.7363	1.0144
1	0.0209	0.0418	0.0757	0.2454	0.3029	0.3864	0.4791
2	0.0235	0.0379	0.0653	0.2010	0.2467	0.3277	0.4138
3	0.0183	0.0339	0.0640	0.1762	0.2154	0.3003	0.3956
4	0.0209	0.0366	0.0692	0.0770	0.0992	0.1384	0.1841
5	0.0209	0.0457	0.0614	0.0209	0.0470	0.0627	0.0888
	Casper Serial Protected Access			NICA fusion with 2 samples Serial Protected Access			
ALL	**0.2755**	**0.3812**	**0.5470**	**0.7820**	**0.8877**	**1.0574**	**1.3094**
0	0.1828	0.2010	0.2311	0.1919	0.2102	0.2389	0.2820
1	0.0144	0.0313	0.0614	0.1971	0.2141	0.2454	0.2872
2	0.0222	0.0366	0.0640	0.1540	0.1684	0.1971	0.2467
3	0.0183	0.0339	0.0640	0.1462	0.1619	0.1945	0.2454
4	0.0209	0.0366	0.0692	0.0757	0.0914	0.1240	0.1645
5	0.0209	0.0457	0.0614	0.0196	0.0444	0.0601	0.0862

Table 7-7: Number of Protected services accessed by an impostor per hour on average during all types of usage as independent and series at IL =5 split down to protected service level

The same test took place for the 20 random timed services where again the results are better for the security provision of CASper with the latter giving a 0.55% opportunity of misuse in the smaller window where NICA gives a 2.25%.

Integrity Required	2	5	10	AL 2 IL 5	AL 5 IL 12	AL 10 IL 25	AL 20 IL 50
	Casper Independent Random Protected Access			NICA fusion with 2 samples Independent Random Protected Access			
ALL	**0.1188**	**0.1475**	**0.2102**	**0.4504**	**0.6057**	**0.782**	**1.0261**
0	0.1031	0.1162	0.1371	0.121	0.18	0.268	0.346
1	0.0065	0.0104	0.0222	0.108	0.137	0.155	0.218
2	0.0026	0.0065	0.0183	0.099	0.127	0.162	0.21
3	0.0052	0.0117	0.0196	0.09	0.116	0.136	0.17
4	0	0.0026	0.0078	0.03	0.044	0.054	0.063
5	0.0039	0.0039	0.0104	0.004	0.007	0.014	0.027
	Casper Serial Random Protected Access			NICA fusion with 2 samples Serial Random Protected Access			
ALL	**0.0587**	**0.0783**	**0.1266**	**0.3094**	**0.3616**	**0.4386**	**0.5065**
0	0.0444	0.0496	0.0614	0.0809	0.094	0.1123	0.1266
1	0.0052	0.0078	0.017	0.0666	0.0796	0.0914	0.1044
2	0.0013	0.0052	0.0144	0.064	0.0705	0.0953	0.1057
3	0.0052	0.0117	0.0196	0.0705	0.0809	0.0927	0.1031
4	0	0.0026	0.0078	0.0261	0.0352	0.0379	0.0457
5	0.0039	0.0039	0.0104	0.0039	0.0065	0.0144	0.0274

Table 7-8: Number of Random Protected services accessed by an impostor per hour on average during all types of usage as independent and series at IL =5 split down to protected service level

7.3 Discussion

The modifications of CASper that aimed so much at simplifying the authentication process in terms of parameter settings as well as removing/minimising the effect that the degradation function has on the trust to the user during inactivity or tolerance in false positives, showed to provide a better response in security whilst maintaining transparency at a tolerable level.

Although on average the integrity that CASper maintains through the hour is not comparable in performance with NICA and NICA fusion, is not as aforementioned the directed means of comparison as the 2 approaches use a different core operation. The particular tests of protected services are the real test in this occasion as they are the ones that better define so much the security as well as transparency of the system. In those CASper showed to closely match the transparency of NICA. However the effect of automatically zeroing out the integrity makes CASper a bit more intrusive as expected with 1-2 requests more than NICA fusion. On the other hand however it increases the security of the system whilst also providing a more easily conceived and configurable framework possibly for the simple user. As aforementioned the maximum effect here in the performance of NICA is the degradation function in contrast with CASper that it does not maintain its trust to the user when there is inactivity or a negative authentication response and therefore at any time where the user's identity could be questionable and the user has not 'earned' the particular integrity.

Given that both approaches- NICA fusion and CASper operate with good performance in general, it is a matter of selection between the levels of security and transparency expected and required. Given the different requirements that different stakeholders may have both approaches and understanding the difficulties in establishing a 'work-for-all-and-always' setting, the less the variables that contribute in the configuration of such a mechanism the more user-friendly an approach is and possibly more easy to tune to a person's requirement given the experience of the user with their interaction with the device. It is seen that CASper offers a simplified approach and a more consistent approach regarding performance under different levels of usage and timed events. Also closely matching the PIN settings as for example how long before the device is locked, it provides a user friendly configuration approach that is closer to user perception and culture.

8 Conclusions

Mobile devices have posed many questions in regards to their security provision given their ubiquitous use for the home user and business. This research is concerned with an examination into user authentication and has made a contribution on identifying the security requirements and how these can be addressed through non-traditional means. Building upon the requirements and prior art a framework was proposed and examined as a more robust means to authentication – providing continuous authentication whilst trying to maintain usability to the user. Whilst testing performance and applicability of the examined framework it sought approaches to improving upon the originally envisaged approach in terms of security and transparency as well as realising operational considerations. The following sections discuss the outcomes, achievements and limitations of the research.

8.1 Achievements of Research

This research addresses the subject of user authentication looking to suggest a more robust solution to current user authentication provision on mobile devices. Through the process of proposing, modelling and evaluating a new approach to user authentication the following achievements have been met.

- *An investigation in the security issues and authentication alternatives on modern mobile devices*

  The study established the need for better securing mobile devices due to the increased risk they carry nowadays. The alternative suggestion of biometric authentication was presented to improve upon the insufficiencies of secret

knowledge techniques and particular techniques that can enable a more user-friendly and convenient approach was identified. Biometric fusion was also identified as a more confident process in establishing user's identity (Chapter 2).

- *Investigation into the user's perspective regarding security provision and alternatives means to authentication (Chapter 3)*

Using a focus group this study acquired the perception of users which was a key issue as there are the ones that are the end receivers in any authentication approach. The study with the end users gave an insight that reflects the literature as well by identifying that users so much denoted the desire for more enhanced authentication when usage of the device requires it as well though privacy concerns regarding biometric profiles. Given the time of the study, it is expected that the desire for enhanced authentication will become higher as the sensitivity of access is increasing while privacy concerns decrease as the techniques are more and more deployed in everyday life e.g. face recognition in airports, fingerprint scanners in schools.

- *Investigation into the different security requirements of data and services (Chapter 3)*

The need for moving away from one level of security fits all approach; it was established that different types of services carry different risks and therefore security requirements. By identifying the latter and the different requirements

that stakeholders may have risk assessment models were proposed. The models proposed can be closely linked with the authentication seen in this study which allows for tying the security of each access with particular authentication requirements and therefore providing a level of differentiation.

- *Consideration of the authentication topologies and potential trade-offs (Chapter 3)*

The study identified topologies that a biometric system could use in order to operate looking at server and device based topologies and analysing the counter benefits and pitfalls whilst establishing the practicalities that may burden or allow for such implementation with device and network capabilities as well as cost. As there are several concerns so much in terms of privacy as well as control of the volume of the data and how this can be addressed by the operators so much in terms of cost as well as operationally it was important to consider these issues in such system.

- *Proposed and practically evaluated a framework for transparent and continuous authentication through a user trial by developing an operational prototype(Chapter 4)*

Building upon the identified requirements this study presents a framework-NICA, as means to more robust authentication by transparently establishing user trust throughout the operation of the device. By developing an

operational prototype of the NICA framework a user evaluation utilising the latter was conducted and the user acceptance was acquired. The response was positive in terms of how the users would be open in utilising such system which was important to establish for the future of such system. 92% of the users felt that the use of such system would provide a more secure environment. In regards to system convenience using a 0-5 Likert Scale, 41% of the users considering the system very convenient (with rating 1&2) however as limitations existed on the transparency achieved given the time limitations and biometric algorithm performance (commercial or build-in) 33% of users rated the at 3 in regards of convenience with the rest 16% considering the system inconvenient. However it gave an important insight on how such framework could operate and the feedback of users given its use.

- *Evaluation of the proposed framework though a series of simulations (Chapter 5)*

Looking to evaluate the framework further to the practical evaluation the study modelled NICA with a simulation approach under different scenarios of usage. Different settings regarding primarily the framework timed-event settings were tested to examine its operation and practicalities. Best performance with scenarios of high usage were given using compact timed-events as authentication would occur more often with average integrity achieved being 3.2 for an authorised user with close to 0 intrusive requests. Regarding accessing protected services under the same scenario a 25 intrusive requests

on an intense scenario of 52 protected services access per hour was achieved. Impostor tests showed good performance with 0.0068% false access under the same aforementioned scenarios. Simulation of the examined framework led to identifying difficulties and pitfalls in the system configuration and also led to modifications that improved on the framework transparency.

- *Investigate the incorporation of fusion in the proposed framework and proposed new framework models(Chapter 6)*

The study examined how the deployment of fusion can improve on the performance of the framework through proposing new approaches on the core authentication mechanism. Simulation results demonstrated that given high usage of the device fusion permits for higher trust of the user to be achieved whilst maintaining security against an impostor. An improvement to 3.8% average integrity was achieved and an improved 9.9 intrusive requests out of 52 protected service access. A further improvement in the handling of how the integrity gets modified during protected service access further improved the performance of the system when using fusion at 4.8 intrusive requests out of 52 protected service accesses. Regarding impostor access the performance was kept at high security compared to NICA with similar results with minimal improvement. Given the high complexity and subjectivity that exists in the usage of the device, difficulties in configuring such framework to always fit the requirements of each user were identified.

- *Proposed a new framework approach to improve on the configuration limitations and pitfalls*

An alternative approach to the core authentication mechanism is proposed – CASper, which uses a binary control of the integrity to mitigate any misuse particular in areas of inactivity whilst simplifying the configuration of the framework. In an effort to counteract the complexities of time settings that derive from users and usage, CASper is seen as a more easily configurable approach whilst maintaining the performance as well as improving the security that NICA provides. CASper achieved kept the convenient aspect by generating on the similar scenarios 5.6 intrusive requests out of 52 and achieved a better security aspect with 0.27 false access by an impostor to a protected service compared to 0.78 that of NICA fusion. Closely matching the PIN settings as for example how long before the device is locked, it provides a user friendly configuration approach that is closer to user perception and culture whilst maintaining good convenience and offering a more secure approach.

8.2 Limitations

The study focused in examining an alternative in user authentication on mobile devices. Although the research met its objectives a number of limitations were imposed upon the outcomes of the work.

The performance of biometric solutions in particular applications require a good performance in a non-exclusive setting for capturing of biometric samples which have not yet established. For these kinds of systems to be put in place there are need to be algorithms that can support transparency with good error rates are they are core in the good performance of such system. As such the practical evaluation was largely affected by the poor performance enforcing a far more intrusive experience than the envisaged one.

The system was tested so much with real users as well as simulative scenarios. The former was restricted as aforementioned so much by the algorithms as well as the restrictive timings and therefore could not have a much representative result of the system its perceived operation. The latter gave a further and better insight to the performance however still the data sets used as basis in this study do not provide necessarily the best basis for today. It could have been useful and more insightful to be able to have real data of current smartphone users of different areas and interest in device usage as well as being able to run a pre-longed user study with real users.

8.3 Future Work

As seen in the practical evaluation as well as the simulation, biometric performance plays such significant role in its operation. Whether that is a no-yes decision or as in NICA fusion and CASper part of the authentication algorithm, the system cannot operate transparently without confident biometric decisions. This is affected both from the strength of the algorithm as well as the quality of samples. Continuation of previous work (Clarke et al, 2011; Karatzouni et al, 2007) and further research could

seek into pursuing the improvement of the techniques when acting in a transparent manner.

Further scope exists in further examining the operation of the framework. For example introducing a pre-processing engine could be a benefit as an addition to the system in these cases where it provides feedback regarding the quality of samples to the authentication algorithm. As such inappropriate samples do not get utilised or get little weight in the process and the confidence in decision becomes part of the decision algorithm. Furthermore the performance of biometric algorithms could also be weighted in the decision in the same way that the particular biometrics are. As such the confidence levels may not necessarily attributed based on the type of the biometric but based on the EERs of a particular algorithm. Simulating how the above may improve the confidence in which the system may operate could be beneficial.

So much form a home user as well as a business user so that further analysis can be done regarding the usability of such system as well as possibly identifying patterns in the use of the device. More particularly future research could seek to apply the system in practice for a prolonged period of time and oversee the applicability of the approach in an everyday scenario. Furthermore experiments to assess impostor scenarios with real users in order to test how deliberate efforts of misuse can 'cheat' the operation of the framework could be of benefit. Although the simulation data were based on real usage could not substitute real data. As such practical evaluations could also produce data sets that could be tested also consequently in a simulative environment. As such future research could seek to contact practical evaluations of the examined system so much in artificial

environments to test impostor access as well as prolonged use of the system for a period of time. Restrictions exist in such approach as there are issues of privacy and there must be particular restrictions in the type of data that can be collected and analysed. Artificial settings would be easier in practice however they pose timing restrictions that would burden the amount of results that can be obtained.

This research addressed the issue of inter-process security and the differing requirements of various services and data access. Future research may look to address intra-process security by looking at the particular requirements and models that can serve this issue.

8.4   Authentication in Modern Mobile Devices

The modern mobile device is going continue to evolve so much as means of communication as well as business. A device that gains grounds everyday into people's lives opens new ways for services to be implemented and data to be accessed for purposes of personal ease, work, revenue, entertainment etc. Given the capabilities of the modern devices however the risk that the device carries regarding storage and access also increases, imposing an important identified requirement for enchasing the security provision.

This research looked at this changing landscape and by identifying and assessing the differing requirements and needs, examined options for more robust authentication whilst analysing, further developing and updating a proposed solution. Suggesting continuous and transparent authentication as more enhanced and fitted approach to current and future devices, established its acceptance from a user's

perspective as well as the possible ability to secure the device in a user-friendly manner with biometric solutions that are believed as more confident means to confirm user identity.

In conclusion given the modern device it is essential that future authentication should not only seek improve in terms of creating a stronger lock to accessing the information but also a more appropriate lock that corresponds to the sensitivity of the data accessed and while they are being accessed.

9 References

1. 3GPP (2012) : "About 3GPP", Available at: http://www.3gpp.org/About-3GPP

2. Alastair Cummings, Mark Nixon and John Carter (2010) "A Novel Ray Analogy for Enrolment of Ear Biometrics." In: *IEEE Fourth Conference on Biometrics: Theory, Applications and Systems*, September 2010, Washington DC, USA

3. Ad Terras per Aspera (2010): "Approximate Youtube Bitrates", Available at: http://adterrasperaspera.com/blog/2010/05/24/approximate-youtube-bitrates via http://stackoverflow.com/questions/5073374/bandwidth-question

4. Apple (2013): "iPhone 5s: About Touch ID security", Available at:http://support.apple.com/kb/ht5949

5. Ashbourn, J. (2000): "Biometrics: Advanced Identity Verification, The Complete Guide", Springer, London, UK, 2000

6. Bankfutura (2012) : "Why do people use mobile banking?", Available at: http://www.bankfutura.com/2012/05/why-do-people-use-mobile-banking/

7. Barber, B. and Davey, J. (1992): "The use of the CCTA risk analysis and management methodology CRAMM", Proceedings of MEDINFO92, North Holland, pp. 1589 –1593.

8. BasicITSolutions (2013): "BYOD: Key insights", Available at: http://www.basicitsolutions.com/byod-key-insights/

9. BBC (2009): "Pension details of 109,000 stolen", Available at: http://news.bbc.co.uk/1/hi/business/8072524.stm

10. BBC (2008): "'60,000' devices are left in cabs", Available at: http://news.bbc.co.uk/1/hi/7620569.stm

11. BBC (2013): "314 mobile phones stolen in London every day", Available at: http://www.bbc.co.uk/news/uk-england-london-21018569

12. Ben-Yacoub, S., Abdeljaoued, Y., Mayoraz, E.(1999): "Fusion of Face and Speech Data for Person Identity Verification", IEEE Transactions on Neural Networks, Vol. 10, No. 5, pp. 1065-1074, September 1999

13. Bigun, E., Bigun, J., Duc, B., Fischer, S.:(1997)"Expert conciliation for multi modal person authentication systems by Bayesian statistics," *Proceedings of the 1st International Conference of Audio- Video-Based Biometric Person Authentication,* Berlin, Germany, Springer, pp. 291–300, 1997

14. Blau, J. (2007): "3GSM - Biometrics to ease CIO's cell phone concerns", ComputerWorld.com, Available at: http://www.computerworld.com.au/index.php?id=1862495582

15. Brunelli, R., Falavigna, D. (1995): "Person identification using multiple cues," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 17, pp. 955–966, October 1995.

16. Burge, M. and Burger, W (1998): "Ear Biometrics", BIOMETRICS: Personal Identification in a Networked Society, Jain, A., Bolle, R. and Pankanti, S., Kluwer Academic, 1998, pp. 273-286.

17. Canalys.com (2011):"Mobile security investment to climb 44% each year through 2015", Available at: http://www.canalys.com/newsroom/mobile-security-investment-climb-44-each-year-through-2015

18. Cellan-Jones, J (2010): Government calls for action on mobile phone crime, Available at:http://news.bbc.co.uk/1/hi/technology/8509299.stm

19. CellularNews (2012): 3G/UMTS Mobile Subscriber Base Passes One Billion Landmark , Available at: http://www.cellular-news.com/story/52727.php

20. Chang, K., Bowyer. K.W., Sarkar, S., Victor, B. (2003): "Comparison and Combination of Ear and Face Images in Appearance-Based Biometrics", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 9, September 2003, pp. 1160-1165.

21. CheckPoint (2012):"The impact of mobile devices on information security**:** A survey of IT professionals", Available at: http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

22. Chellappa, R., Wilson, C.L., Sirohey, S. (1994): "Human and Machine Recognition of Faces: A Survey", University of Maryland Computer Vision Laboratory. Available at http://lcv.stat.fsu.edu/research/geometrical_representations_of_faces/PAPERS/face_recognition_survey1.pdf

23. Clark, J (2011): "NHS laptop loss could put millions of records at risk", Available at:http://www.zdnet.co.uk/news/security-management/2011/06/15/nhs-laptop-loss-could-put-millions-of-records-at-risk-40093112/

24. Clarke, N.L., Furnell, S.M, Rodwell, P.M, Reynolds, P.L (2002): "Acceptance of Subscriber Authentication Method for Mobile Telephony Devices", Computers & Security, 21, 3, 220-228

25. Clarke, N (2004): "Advanced User Authentication for Mobile Devices", PhD Thesis, University of Plymouth, 2004

26. Clarke, N.L., Furnell, S.M. (2005): "Authentication of Users on Mobile Telephone - A Survey of Attitudes and Practices", Computers & Security, vol. 24, no.7, pp.519 - 527.

27. Clarke, N.L., Furnell, SM. (2006): "Authenticating Mobile Phone Users Using Keystroke Analysis", International Journal of Information Security, pp1-14, 2006

28. Clarke, N.L., Karatzouni, S., Furnell, S.M.(2008)"Transparent Facial Recognition for Mobile Devices", Proceedings of the 7th Security Conference, Las Vegas, USA, 2nd-3rd June, 2008

29. Clarke NL, Karatzouni S, Furnell SM (2011): "Towards a Flexible, Multi-Level Security Framework for Mobile Devices", Proceedings of the 10th Security Conference, Las Vegas, USA, 4-6 May, 2011

30. ComputerWeekly.com (2011): "Infosec 2011: The security advantages and pitfalls of personal mobile devices in the workplace", Available at: http://www.computerweekly.com/video/Infosec-2011-The-security-advantages-and-pitfalls-of-personal-mobile-devices-in-the-workplace

31. Computer Industry Almanac Inc (2012): "Worldwide Tablet Sales Will Reach Nearly 36% of Total PC Sales in 2015 ", Available at: http://www.c-i-a.com/pr012012.htm

32. Computerworlduk.com (2012): "BYOD - Best practices and effective policies in a bring your own device environment", Available at: http://www.computerworlduk.com/business-it-hub/management-briefing/3350113/bring-your-own-device-effective-policies-practice-in-byod-environment/

33. Comscore (2012): "comScore Releases the "2012 Mobile Future in Focus" Report", Available at:

   http://www.comscore.com/Press_Events/Press_Releases/2012/2/comScore_Rel eases_the_2012_Mobile_Future_in_Focus_Report

34. Confidenttechnologies.com (2011): "Survey Shows Smartphone Users Choose Convenience Over Security", Available at:

   http://confidenttechnologies.com/news_events/survey-shows-smartphone-users-choose-convenience-over-security

35. CPNI (2012): "Personnel security in remote working: A good practice guide", Available at: http://www.cpni.gov.uk/documents/publications/2012/2012004-personnel_security_in_remote_working.pdf?epslanguage=en-gb

36. Crabtree, J., Nathan, M., Roberts, S.

   (http://www.theworkfoundation.com/assets/docs/publications/103_mobileuk.pdf

37. Cope, B. (1990): "Biometric Systems of Access Control", Electrotechnology, April/May: pp. 71-74

38. Cunningham, P.(2012): "Get mobile! Mobile internet usage poised to overtake PC by 2015", Available at: http://www.indulgemedia.com/blog/get-mobile-mobile-internet-usage-poised-overtake-pc-2015

39. Dailymail.co.uk (2013): "How often do you check your phone? The average person does it 110 times a DAY (and up to every 6 seconds in the evening)", Available at: http://www.dailymail.co.uk/sciencetech/article-2449632/How-check-phone-The-average-person-does-110-times-DAY-6-seconds-evening.html

40. DarkReading.com (2011):"Half Of Lost Or Stolen Mobile Devices Store Sensitive Company Data", Available at: http://www.darkreading.com/cloud-

security/167901092/security/news/229625511/half-of-lost-or-stolen-mobile-devices-store-sensitive-company-data.html

41. Daugman, J. (2004):"How Iris Recognition Works", Available at:

    http://www.cl.cam.ac.uk/~jgd1000/irisrecog.pdf

42. Deloitte (2013): "The Deloitte Consumer Review – Beoynd the hype: The true potential of mobile", Available at: http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/Consumer%20Business/uk-cb-consumer-review-edition-5.pdf

43. Digital marketing university (n.d.): Mobile optimization: It's about your customer not your website, Available at: http://digital-marketing-university.com/Blogs/Burns-Marketing/May-2013/Mobile-optimization-Its-about-your-customer.aspx

44. Education Stormfront (2012): "Study: Phones Outnumber PCs In Most Markets", Available at: http://educationstormfront.wordpress.com/2012/01/26/study-phones-outnumber-pcs-in-most-markets/

45. Facelock (2013): "Facelock", Available at: http://www.facelock.mobi/

46. Forbes.com (2012): "The Latest Infographics: Mobile Business Statistics For 2012", Available at: http://www.forbes.com/sites/markfidelman/2012/05/02/the-latest-infographics-mobile-business-statistics-for-2012/

47. Forrester Research (2012): "Forrester: 375 Million Tablets Will Be Sold Globally In 2016", Available at:

    http://www.forrester.com/Forrester+375+Million+Tablets+Will+Be+Sold+Globally+In+2016/-/E-PRE3384

48. Fraud for Thought (2013):"Biometrics bolstered in the mobile space", Available at: http://fraudforthought.com/index.php/biometrics-bolstered-in-the-mobile-space/

49. Frommer, D. (2010): "25 Awesome Charts On The State Of The Wireless Industry", Available at: http://www.businessinsider.com/25-charts-on-the-state-of-the-wireless-industry-2010-5?op=1

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

51. Furnel, S., Katsikas, S., Lopez, J., Patel, A. (2008): "Securing Information and Communication Systems: Principles, Technologies and Applications", Information Security and Privacy Series, Artech House, 2008

52. Furnell, S. and Evangelatos, K. (2007): "Public awareness and perceptions of biometrics", *Computer Fraud & Security*. Issue 78

53. Gartner (2012): "Gartner Says Worldwide Mobile Payment Transaction Value to Surpass $171.5 Billion", Available at: http://www.gartner.com/it/page.jsp?id=2028315

54. Gartner (2013): "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes", Available at: http://www.gartner.com/newsroom/id/2466615

55. Gissin, I. (2005) : "Reality check: A 3G-user experience". http://www.totaltele.com/View.aspx?ID=75921&t=4

56. Gomm, K. (2005) : "Full biometric ID scheme to reach the UK 'by 2009". http://news.zdnet.co.uk/hardware/0,1000000091,39232692,00.htm

57. Goode Intelligence (2011): "Goode Intelligence publishes mobile phone biometric security analyst report". Available at: http://www.goodeintelligence.com/media-centre/view/goode-intelligence-publishes-mobile-phone-biometric-security-analyst-report

58. Gupta, G., McCabe, A. (1997): "A Review of Dynamic Handwritten Signature Verification",James Cook, University, Townsville, Australia.

59. GSAcom (2012): "GSM/3G Stats", Available at: http://www.gsacom.com

60. GSMA (2012a): "EDGE", Available at: http://www.gsma.com/aboutus/gsm-technology/edge/

61. GSMA (2012b): "LTE", Available at: http://www.gsma.com/aboutus/gsm-technology/lte/

62. Harmonized biometric vocabulary; *ISO/IEC JTC 1/SC 37 N 3068*, working draft 2009-. 02-28,

63. Hong, L. Jain, A.K. : "Integrating faces and fingerprint for personal identification", *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 20, 1997.

64. IBG (2001): "Biometrics Explained", Available at: http://www.kubase.com/v2/pdf/Biometrics%20Explained.pdf

65. IBG (2005): "Independent Testing of Iris Recognition Technology (ITIRT)", International Biometric Group, Available at: http://www.biometricgroup.com/reports/public/reports/ITIRT_report.htm

66. IBG (2006): "Which is the best biometric technology", International Biometric Group, Available at: http://www.biometricgroup.com/reports/public/reports/best_biometric.html

67. IBG (2012): "Primary face recognition technologies": Available at:

http://www.ibgweb.com/products/reports/free/primary-facial-recognition-

technologies

68. IBM (2011) : "Securing mobile devices in the business enviroment", Available at:

http://www-

935.ibm.com/services/uk/en/attachments/pdf/Securing_mobile_devices_in_the_b

usiness_environment.pdf

69. IBM (2012) : "Securing mobile devices in the business environment", Available at:

http://www-

935.ibm.com/services/uk/en/attachments/pdf/Securing_mobile_devices_in_the_b

usiness_environment.pdf

70. ITU World Telecommunication(n.d.): "Statistics & Database: Global ICT trends",

Available at: http://www.itu.int/ITU-D/ict/statistics/

71. ITU (2013): "ictFacts and Figures", Available at: http://www.itu.int/en/ITU-

D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

72. Jain, A.K., Hong, L., Kulkarni, Y.: (1999)"A multimodal biometric system using

fingerprints, face and speech," in *Proceedings of the 2nd International

Conference of Audio- Video-Based Biometric Person Authentication,* Washington,

D.C., March 22–23, pp. 182–187, 1999

73. Jones, P. (2013): "The Mobile Workforce", PrintIT, Spring 2013, pg.15, Available

at: http://www.binfo.co.uk/PrintIT_Spr13/files/assets/basic-html/page15.html

74. Jupiter Networks (2012) : "A GLOBAL STUDY INDEXING CONSUMER

CONFIDENCE IN MOBILITY", Available at:

http://www.juniper.net/us/en/local/pdf/additional-resources/7100155-en.pdf

75. Jupiter Networks (2013): "Juniper Networks Mobile Threats Report", Available at: http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf

76. Juniper Research (2013): "Press Release: Mobile Banking Users to Exceed 1 billion in 2017, Representing 15% of Global Mobile Subscribers", Available at: http://www.juniperresearch.com/viewpressrelease.php?pr=356

77. Juniper Research(2010): "Press Release: Mobile Payments Market to Quadruple by 2014, reaching $630bn in value, although still only accounting for around 5% of ecommerce retail sales", Available at: http://www.juniperresearch.com/viewpressrelease.php?pr=173

78. Juniper Research (2010): "Press Release: 4G LTE Revenues Projected to Exceed $100bn Globally in 2014, Despite Uncertainty about New Data Plans, says Juniper Research,", Available at: http://www.juniperresearch.com/viewpressrelease.php?pr=213

79. Karatzouni S, Clarke NL (2007): "Keystroke Analysis for Thumb-based Keyboards on Mobile Devices", Proceedings of the 22nd IFIP International Information Security Conference (IFIP SEC 2007), Sandton, South Africa, 14-16 May, pp. 253-263

80. King, R (2013): "Biometric Research Note: Mobile devices to drive bank adoption of voice biometrics", Available at: http://www.biometricupdate.com/201301/mobile-devices-to-drive-bank-adoption-of-voice-biometrics

81. KPMG (2013): "The Mobile Evolution: The challenges and opportunities of mobile", Available at:

http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/mobile-evolution/Documents/mobile-evolution.pdf

82. Lammi, H. (2004). "Ear Biometrics", Lappeenranta University of Technology, Available at: http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Lammi.pdf

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

84. Lettice, J. (2006): "Compulsory and centralised - UK picks hardest sell for ID cards", Available at: http://www.theregister.co.uk/2006/03/13/ou_idcard_study/

85. Lettice, J (2010): "Biometric passport 2.0 scrapped alongside ID cards, NIR", Available at: http://www.theregister.co.uk/2010/05/12/tory_libdem_id_scrappings/

86. Leyden, J (2012): "Finders of lost mobes can't resist staring at privates", Available at: http://www.theregister.co.uk/2012/03/13/smartphone_honey_stick/

87. Lindgren, M., Jedbratt, J., Svensson, E. (2002): "Beyond Mobile: people, Communications and Marketing in a Mobilized World", Palgrave, New York, US, 2002

88. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S. (2003): "Handbook of fingerprint recognition", Springer, 2003

89. Mansfield, T., Kelly, G., Chandler,D. and Kane, J. (2001): "Biometric Product Testing Final Report", Issue 1, National Physical Laboratory, 2001.Available at: http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf

90. Matt Carmichael , (2012) : "Stat of the Day: Mobile Phones Overtake PCs", Available at: http://adage.com/article/adagestat/mobile-phones-overtake-number-pcs-key-global-markets/232304/

91. Mazo, G (2012): "How to set up Face Unlock on your Android phone", Available at: http://www.androidcentral.com/how-set-face-unlock-your-htc-one-x-or-evo-4g-lte

92. McKen, M., Joseph, K., Thieme, M. (2004): "Biometric Fusion Demonstration System Scientific Report", International Biometric Group, Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA436410

93. Microstrategy (2012): "The Convergence of Mobile Technology and Mobile Intelligence", Available at: http://www.microstrategy.com/mobile/platform/The_Convergence_of_Mobile_Technology_and_Mobile_Intelligence.pdf

94. Microtrend(2013): "Mobile Security Report - Britain's Culture of Careleness with Mobile Devices", Available at: http://www.trendmicro.co.uk/media/misc/tm-mobile-security-report-uk.pdf

95. MimeCast (2012): "Mimecast Extends Mobile Services to Windows Phone and Android", Available at: http://www.mimecast.com/About-us/Press-releases/Dates/2012/5/Mimecast-Extends-Mobile-Services-to-Windows-Phone-and-Android/

96. Mims, C (2010): "Smart Phones that Know Their Users by How They Walk", Available at: http://www.technologyreview.com/view/420835/smart-phones-that-know-their-users-by-how-they-walk/

97. MobiReady (2012): "dotMobi Compliance & mobileOk checker", Available at: http://ready.mobi

98. MobiThinking (n.d): "The insider's guide to mobile security", Available at:

http://mobithinking.com/mobile-device-security

99. MobiThinking (2012); "Global mobile statistics 2012", Available at:

http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats#subscribers

100. Mobile News (2012):"Vodafone revenues drop but UK customer numbers

increase", Available at: http://www.mobilenewscwp.co.uk/2012/11/13/vodafone-

service-revenues-drop-but-customer-numbers-rise/

101. Mobile Operators Association (2006) :"Base stations and masts" , Available

at: http://www.mobilemastinfo.com/information/masts.htm

102. Mobile Business. (2006): "Orange Data Not Secure",

http://www.mbmagazine.co.uk/index.php?option=com_content&task=view&id=14

41&Itemid=2&PHPSESSID=d6fc7ad0c429dae5956c3ffd9466a84d

103. Mohankrishnan, N., Wan-Suck, L., Paulik, M.J. (1999): "A performance

evaluation of a new signature verification algorithm using realistic forgeries",

Proceedings of the 1999 International Conference on Image Processing (ICIP

'99), Kobe, Japan, IEEE Computer Society, 1999, Volume 1, pp. 575 -579

104. Mohr, W., Konhauser, W.(2000): "Access Network Evolution Beyond Third

Generation Mobile Communications", IEEE Communications Magazine, pp.122-

133, December, 2000

105. Moreau, Y., Vandewalle. (1997): "Fraud Detection in Mobile Communications

using Supervised Neural Networks". Proceedings of SNN: Europe"s Best Neural

Network Practice.

106. Murray, M.P. (1967) : "Gait as a total pattern of movement", American journal

of Physical medicine Vol. 46(1), pp. 290-333

107. Nanavati, S., Thieme, M., Nanavati, R. (2002):" Biometrics: Identity Verification in a Networked World ", John Wiley & Sons, New York, US,2002

108. 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

109. Neal, D. (2013): "T-Mobile US drops high global roaming charges", Available at: http://www.theinquirer.net/inquirer/news/2299873/t-mobile-us-drops-high-global-roaming-charges

110. Newbusiness.co.uk (2011): "Mobile working- massive growth seen", Available at: http://www.newbusiness.co.uk/news/mobile-working-massive-growth-seen

111. NICA (2007): "Non-Intruisve Continuous Authentication", Research Project Site, Available at: https://www.cscan.org/nica/

112. NMPCU. (2012): "Welcome to National Mobile Phone Unit".Available at: http://www.met.police.uk/mobilephone

113. NSTC (2006): "Biometric Glossary", National Science & Technology Council"s Subcommittee on Biometrics, Available at: http://www.biometrics.gov/docs/glossary.pdf

114. NTT DoCoMo (2003): "DoCoMo's Newest 505i Handset Features Fingerprint Authentication". http://www.nttdocomo.com/pr/2003/000985.html 80

115. Nubic (2008): "The Growing Use of Mobile Websites for Business Communications and Promotion", Available at: http://www.nubiq.com/white-papers/GrowingUseofMobileWebsites.pdf

116.   NYTimes (2012):"For Impatient Web Users, an Eye Blink Is Just Too Long to Wait", Available at: http://www.nytimes.com/2012/03/01/technology/impatient-web-users-flee-slow-loading-sites.html?pagewanted=all

117.   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

118.   Omron. (2005): "Omron Announces "OKAO Vision Face Recognition Sensor", World's First Face Recognition Technology for Mobile Phones". http://www.omron.com/news/n_280205.html

119.   Onestopclick(2011): "Mobile working is a top priority for business, claims IDC" , Available at: http://connectivity.onestopclick.com/technology_news/mobile-working-is-a-top-priority-for-business-claims-idc_801233346.htm

120.   Openet Telecom (2012): "Closing the Mobile Data Revenue Gap ",Available at:

http://ibmtelconewsletter.files.wordpress.com/2011/02/wp_closing_mobile_data_revenue_gap_a4.pdf

121.   PDALok. (2006): Signature Recognition. PDALok. http://www.pdalok.com

122.   Porter, H. (2004): "If you value your freedom, reject this sinister ID card".http://www.guardian.co.uk/idcards/story/0,15642,1375858,00.html

123.   Practical Ecommerce (2010): "Mobile Bandwidth: An Expert Explains 3G, 4G, WiFi", Available at: http://www.practicalecommerce.com/articles/2377-Mobile-Bandwidth-An-Expert-Explains-3G-4G-WiFi

124.   PRWeb (2012): "Global 3G/3.5G Subscribers Are Projected to Reach 4.27 Billion by 2017, According to New Report by Global Industry Analysts, Inc.",

Available at:

http://www.prweb.com/releases/3G/WCDMA_CDMA_pathway/prweb8973329.htm

125. MIT Human Dynamics Lab (2004): "Reality Mining Dataset", Available at:

http://realitycommons.media.mit.edu/realitymining.html

126. QualComm, 2007: "Evolution of Wireless Applications and Services",

Available at: http://www.qualcomm.com/media/documents/files/evolution-

wireless-applications-and-services-whitepaper.pdf

127. Ranger, S. (2006): "Office space shrinks as mobile computing grows",

Silicon.com, Available at:

http://networks.silicon.com/mobile/0,39024665,39159195,00.htm

128. Rawlings, A. (1997): "UMTS Part 2 - Is the future of UMTS secure", Available

at: http://cordis.europa.eu/infowin/acts/ienm/bulletin/03-1997/umts2.html#r1

129. Raywood, D (2010): "Details of 24,000 people lost following laptop theft from

training company", Available at http://www.scmagazineuk.com/details-of-24000-

people-lost-following-laptop-theft-from-training-company/article/173586/

130. ResearchandMarkets (2011):"Mobile Phone Biometric Security - Analysis and

Forecasts 2011-2015", Available at:

http://www.researchandmarkets.com/reports/1842654/mobile_phone_biometric_s

ecurity_analysis_and

131. Ricker, T(2011): "Researchers steal iPhone passwords in six minutes",

Available at: http://www.engadget.com/2011/02/10/researchers-steal-lost-iphone-

passwords-in-6-minutes-video

132.   Rodriguez, K (2012): "Biometric National IDs and Passports: A False Sense of Security": Available at: https://www.eff.org/deeplinks/2012/06/biometrics-national-id-passports-false-sense-security

133.   Rogers P. (2012): "2012 Mobile Internet Usage Statistics", Available at: http://www.gpmd.co.uk/blog/2012-mobile-internet-statistics/

134.   Ross, A (2007): "AN INTRODUCTION TO MULTIBIOMETRICS", FIND ACTUAL PUBLICATION SOURCE", Available at: http://www.sas.ewi.utwente.nl/open/courses/intro_biometrics/Ross07.pdf

135.   Ross, A., Anil. J., Qian, J.(2001): "Information Fusion in Biometrics", Proc. of 3rd Int'l Conference on Audio- and Video-Based Person Authentication (AVBPA), pp. 354-359, Sweden, June 6-8, 2001.

136.   Ruggles, T. (2002): "Comparison of biometric techniques", Available at: http://www.bio-tech-inc.com/bio.htm

137.   Scientificamerican.com (2012); "1.3 Billion Workers to Go Mobile by 2015", Available at: http://www.scientificamerican.com/article.cfm?id=1point3-billion-workers-to-go-mobile

138.   Sideco, F. (2012), "Mobile Communications Revenue to Rise by Double-Digit Margin in 2012", Retrieved from http://www.isuppli.com/Mobile-and-Wireless-Communications/News/Pages/Mobile-Communications-Revenue-to-Rise-by-Double-Digit-Margin-in-2012.aspx

139.   Siciliano, R (2011): "The Rise of Smartphones and Related Security Issues", Available at: http://www.infosecisland.com/blogview/13078-The-Rise-of-Smartphones-and-Related-Security-Issues.html

140. Silicon.com (2006): "Vodafone Makes Mobile Micro-Payments Easy Using PaymentsPlus by Valista", Available at:

http://whitepapers.silicon.com/0,39024759,60161517p,00.htm

141. Smallbusinessnewz (2010): "Smartphone Use High Among Small Business Owners", Available at: http://www.smallbusinessnewz.com/smartphone-use-high-among-small-business-owners-2010-10

142. Swider, M. (2012):"Apple patents fingerprint sensor for biometric iPhone unlock", Available at: http://www.techradar.com/news/phone-and-communications/mobile-phones/apple-patents-fingerprint-sensor-for-biometric-iphone-unlock-1104176

143. Symantec, 2013 "2013 Cost of Data Breach Study: Global Analysis ", Available at:

https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

144. Thai, B., Wan, R., Seneviratne, A., Rakotoarivelo, T. (2003): "Integrated Personal Mobility Architecture: A Complete Personal Mobility Solution", Mobile Networks and Applications, Volume 8, Number 1, 27-36

145. Thompson, S. (2012): "Infographic: The power of mobile", Available at: http://torsionmobile.com/tag/size-of-the-mobile-market/

146. TimesOnLine (2004): "ID and Ego: It is right to experiment with identity cards". http://www.timesonline.co.uk/article/0,,542-1089392,00.html

147. Victor, B., Bowyer, K., Sarkar, S. (2002): "An evaluation of face and ear biometrics", Proceedings of International Conference on Pattern Recognition, pp. 429-432, August 2002.

148. Visiongain (2012):"THE MOBILE BROADBAND MARKET 2012-2017",
Available at: http://www.visiongain.com/Report/809/The-Mobile-Broadband-Market-2012-2017

149. Vriendt, J.D., Laine, P., Lerouge, C., Xu, X. (2002): "Mobile network evolution: A revolution on the move", IEEE Communications Magazine, April 2002. Available at: http://www.sis.pitt.edu/~dtipper/3G_evol_paper.pdf

150. Wirelessindustrynews (2013): "Stolen smartphones account for 40 percent of thefts in major U.S. cities", Available at: http://www.wirelessindustrynews.org/news-jun-2013/3450-06052013-win-news.html

151. Woodward, J.D, Orlans, N., Higgins, P. (2003) : "Identity Assurance in the Information Age", McGraw-Hill, Berkeley, California

152. Worth, Dan (2013): "More than 15000 lost mobile phones on London Underground pose security risks": Available at: http://www.v3.co.uk/v3-uk/news/2318727/more-than-15-000-lost-mobile-phones-on-london-underground-pose-security-risks

153. Yang, L., Winters, K., Kizza, J.(2008): "Biometric Education with Hands-on Labs", Proceedings of the 46th Annual Southeast Regional Conference, Pages 18-23

154. Yeung, D., Chang, H., Xiong, U., George, S., Kashi, R., Matsumoto, T., Rigoll, G. (2004): "SVC2004: First International Signature Verification Competition", Lecture Notes in Computer Science, Volume 3072/2004, pp.16-22

155. Young, K. (2005) : "Mobile phone security comes with a swagger", Available

at: http://www.computing.co.uk/vnunet/news/2144116/system-locks-mobiles-

user-walk

156. Yun, W.Y. (2003): "The „123" of Biometric Technology", Information

Technology Standards Committee, Available at:

http://www.itsc.org.sg/synthesis/2002/biometric.pdf

157. Zhang, J., Yan, Y., Lades, M. (1997) : Face Recognition: Eigenface, Elastic

Matching, and Neural Nets, Proceedings of the IEEE, Issue 9 , Vol. 85, pp. 1423

– 1435 82

10 APPENDICES

APPENDIX A - List Publications

Journal Papers

Furnell SM, Clarke NL, Karatzouni S (2008): "Beyond the PIN: Enhancing user authentication for mobile devices", Computer Fraud & Security, Volume 2008, Issue 8, pp12-17, 2008

Conference Papers

Clarke, N., Karatzouni, S., Furnell, S. (2011): "Towards a Flexible, Multi-Level Security Framework for Mobile Devices", Proceedings of the 10th Security Conference, Las Vegas, USA, 4-6 May, 2011

Clarke, N., Karatzouni, S, Furnell, S. (2009): "Flexible and Transparent User Authentication for Mobile Devices", Proceedings of the 24th IFIP TC 11 International Information Security Conference, Pafos, Cyprus, May 18-20, ISBN: 978-3-642-01243-3, pp1-12, 2009

Clarke, N., Karatzouni, S, Furnell, S. (2008): "Transparent Facial Recognition for Mobile Devices", Proceedings of the 7th Security Conference, Las Vegas, USA, 2nd-3rd June, 2008

Karatzouni, S., Clarke, N., Furnell, S. (2007): "Device- versus Network-Centric Authentication Paradigms for Mobile Devices: Operational and Perceptual Trade-Offs", 5th Australian Information Security Management Conference, Mount Lawley, Australia, 5th December, 2007

Karatzouni, S, Clarke N., Furnell, S. (2007): "Utilising Biometrics for Transparent Authentication on Mobile Devices", Proceedings of the 2nd International Conference on Internet Technologies and Applications, 4-7 September, Wrexham, UK, ISBN: 978-0-946881-54-3, pp549–557, 2007

Karatzouni, S, Clarke, N. (2007): "Keystroke Analysis for Thumb-based Keyboards on Mobile Devices", Proceedings of the 22nd IFIP International Information Security Conference (IFIP SEC 2007), Sandton, South Africa, 14-16 May, pp. 253-263, 2007

Karatzouni, S, Furnell, S., Clarke, N., Botha, R. (2007): "Perceptions of User Authentication on Mobile Devices", Proceedings of the ISOneWorld Conference, Las Vegas, USA, April 11-13, CD Proceedings (0-9772107-6-6), 2007

White Paper Reports

Clarke, N., Karatzouni, S., Furnell, S. (2006): "Operational and perceptual trade-offs between device- and network-centric authentication models", Eduserv research project deliverable, December 2006

Clarke, N., Karatzouni, S., Furnell, S. (2006): "*Applicable authentication methods for mobile devices and services*", Eduserv research project deliverable, June 2007

APPENDIX B – Copies of selected publications

1. Karatzouni, S, Furnell, S., Clarke, N., Botha, R. (2007): "Perceptions of User Authentication on Mobile Devices", Proceedings of the ISOneWorld Conference, Las Vegas, USA, April 11-13, CD Proceedings (0-9772107-6-6), 2007

2. Karatzouni, S., Clarke, N., Furnell, S. (2007): "Device- versus Network-Centric Authentication Paradigms for Mobile Devices: Operational and Perceptual Trade-Offs", 5th Australian Information Security Management Conference, Mount Lawley, Australia, 5th December, 2007

3. Karatzouni, S, Clarke, N. (2007): "Keystroke Analysis for Thumb-based Keyboards on Mobile Devices", Proceedings of the 22nd IFIP International Information Security Conference (IFIP SEC 2007), Sandton, South Africa, 14-16 May, pp. 253-263, 2007

4. Karatzouni, S, Clarke N., Furnell, S. (2007): "Utilising Biometrics for Transparent Authentication on Mobile Devices", Proceedings of the 2nd International Conference on Internet Technologies and Applications, 4-7 September, Wrexham, UK, ISBN: 978-0-946881-54-3, pp549–557, 2007

5. Clarke, N., Karatzouni, S, Furnell, S. (2009): "Flexible and Transparent User Authentication for Mobile Devices", Proceedings of the 24th IFIP TC 11 International Information Security Conference, Pafos, Cyprus, May 18-20, ISBN: 978-3-642-01243-3, pp1-12, 2009

6. Clarke, N., Karatzouni, S., Furnell, S. (2011): "Towards a Flexible, Multi-Level Security Framework for Mobile Devices", Proceedings of the 10th Security Conference, Las Vegas, USA, 4-6 May, 2011

Perceptions of User Authentication on Mobile Devices

S.Karatzouni[1], S.M.Furnell[1,3], N.L.Clarke[1] and R.A.Botha[2]

[1] Network Research Group, School of Computing, Communications & Electronics, University of Plymouth, Plymouth, UK
[2] Centre for Information Security Studies, School of Information and Communication Technology, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
[3] School of Computer and Information Science, Edith Cowan University, Perth, Australia

Abstract

The increasing range of data and services accessible from mobile devices, such as cellphones and PDAs, leads to questions about the adequacy of security provision, particularly in relation to authentication of the user. In this context, this paper describes the findings from a focus group that was conducted to examine four research questions: whether users recognise a need for security on their current devices; how they perceive the current authentication facilities, and whether they use them; whether they envisage a need for greater security provision in the future; and their perceptions of alternative authentication methods and the ways in which they could operate. The overall results showed that users envisage a need for enhanced security as their usage of the device changes to incorporate more sensitive functions. Furthermore, from the options discussion, a preference towards the use of biometric authentication was expressed by the majority of the participants.

Keywords: *Security, authentication, mobile, cellphone, PDA.*

Introduction

Mobile devices such as cellphones and PDAs are becoming more sophisticated tools, with data processing, storage and communication capabilities getting closer to the functionality of desktop computers. As a consequence, the information that can be accessed through and stored on them is becoming more sensitive. This has already been witnessed with other forms of mobile device (e.g. laptops) and as a result they now represent a recognised area of risk. For example, 53% of respondents in Ernst & Young's Global Information Security Survey 2005 identified mobile computing as the issue that raises the major security concerns (Ernst & Young, 2005). Furthermore, in another survey amongst 2,035 IT professionals, 80% of respondents identified their main security fear as employees misplacing or losing the device, as well as not using appropriate security settings (Red Herring, 2006). Against this background, a concern can be raised regarding the ability of current security measures to safeguard the device. Significant amongst these is the user authentication method, which for current phones and PDAs is principally achieved by the use of Personal Identification Numbers (PINs). However, questions can be raised about whether this method will remain sufficient, and (if not) what methods users may be willing to tolerate in its place.

The purpose of this research was to assess views and attitudes regarding the authentication requirements on mobile devices. In order to achieve that, a focus group

was conducted, in order to provide a forum for users to express and exchange their perspectives. The next section presents the objectives and methodology of the research. This is followed by the main discussion, relating to the results obtained, leading to overall conclusions in the final section.

Research objectives and investigative methodology

The focus group was conducted in September 2006, and lasted around 100 minutes. The composition of the participant group is outlined in Table 1, including a mixture of end-users, representatives from the mobile industry, researchers in the area, and representatives from the educational technology and university perspectives. In addition to these, invitations had also been issued to other industry-based representatives, but unfortunately (despite some initial follow-up) these did not lead to final participation.

Participant	Background / Basis for inclusion
1	Representative from a UK mobile network operator.
2	Creator of a web resource that tracks mobile technologies and trends
3	Project student, addressing public understanding of biometrics
4	Project student, conducting user trials and evaluation of biometrics
5	Academic, active in the mobile security domain
6	Learning technologist, commencing research into educational uses of mobile devices
7	Psychologist, with research interests in use of mobile technologies
8	Representative from university ICT department, responsible for campus deployment of mobile devices.
9	Academic with interest in human factors of technology.
10	Male mobile phone user
11	Female mobile phone user
12	Female mobile phone user

Table 1 : Summary of focus group participants

All of the participants were regular end-users of mobile devices, and in many cases conversant with the features and facilities of smartphone devices. As such, they were able to offer perspectives with firsthand knowledge of the more advanced features and facilities that are likely to become the baseline standard in a few years.

A number of research questions were created to form the framework of the discussion, addressing the main areas of interest around the objectives of this research on user authentication. A list of the question as well as a brief justification behind them follows.

1. Do participants recognise a need for security on their current devices?

This question aims to investigate whether users consider their current usage of mobile devices to merit protection, with particular emphasis being given to whether or not user authentication is an important requirement. The general expectation, based upon prior survey work (Clarke *et al*. 2002; Clarke and Furnell, 2005) was that many participants would not view their own need for security to be particularly high.

2. *How do participants perceive the current authentication facilities, and do they use them?*

The intention here is to focus participants' attention specifically towards the PIN-based techniques that are dominant upon current devices, exploring opinions about the general nature of the method the extent to which they are used in practice. The investigators' expectations here were again partially informed by the earlier research, such that it was anticipated that many participants would not be using the current facilities at all (in part based upon their reasoning from question 1).

3. *Do participants envisage a need for greater security provision in the future?*

Anticipating that some participants would be unlikely to prioritise a need for authentication based upon their current usage of the device, this question asks them to consider the range of emerging and future applications of mobile devices that may interest them. From this, they are asked to reassess their views on the requirement for authentication, in view of the increased sensitivity of data or services that may then be involved.

4. *How do participants perceive the potential alternative methods of authentication and the ways in which they could operate?*

Assuming that the preceding question would highlight a requirement for further protection, this question aims to elicit opinions about alternative mechanisms (such as token and biometric approaches), and methods of applying them.

Although some expectations had been formed as a result of previous research, the participants were not led towards any particular viewpoints during the discussion of each question (nonetheless, the conclusions drawn from the first two questions proved to be generally as anticipated, thus justifying the progression towards the subsequent discussion issues). A discussion guide was formed and followed during the session that would provide the background and the context for the research questions to be answered. The session was video recorded in order to capture any non-verbal information that could provide further input (i.e. reactions to a certain view) or help to quantitative appraisal of answers (i.e. show of hands as an answer).

Focus Group Results

The focus group session began with some background discussion about the participants' use of their mobile devices, with consideration specifically directed towards mobile phones and PDAs, rather than laptops or single-function devices such as media players. This section begins with brief comments in relation to this usage, before proceeding to discussion of the main findings, based around the research questions. It should be noted that, due to overlaps in the related discussions, research questions 1 and 2 are discussed within a single subsection, whereas the extent of discussion arising from question 4 has led to it being split over two subsections. All of the sections are supported by direct quotes from the participants in order to

evidence the views expressed. In all cases, the quotes are exactly as spoken, although in some cases segments have been omitted for brevity (denoted by '…') and in other cases the authors have added wording in brackets in order to provide clarification.

Background of attendees on the use of mobile devices

The majority of participants indicated that their usage of mobile devices had not changed in recent years, and focused mainly upon traditional functionality such as telephony and text messaging. Even where some considered a mobile device as a necessity to their everyday lives, the main driver tended to be communication.

> *"If I left the house without it I would feel a little bit naked. It's like you can't get in touch with people"*

> *"A lot of people are using it more and more. I'm aware of that…but personally…for me it's just a communication tool…that's it"*

> *"I never actually use any of the features, I just text and that's it … Occasionally I use the camera phone feature a bit"*

Although some participants stated that they had used services such as downloading content (e.g. ringtones) or video conferencing, this was mainly for experience's sake rather than an ongoing usage. Nevertheless a minority (mainly owning high-end devices) used them for accessing e-mail or browsing the web on a more regular basis, including in a business context:

> *"I mean if I had to lose this [device] at this point in time … I would be completely lost, because I run my diary, I basically run everything that I do with this kind of thing"*

The potential for greater adoption of services was also identified by some attendees, suggesting that the usage of the device is likely to change in the future.

Current need for security and use of the available security mechanisms

Surveys have repeatedly reported that although users store a great amount of sensitive information on their devices, little attention is given to protecting them using the available security mechanisms (Pointsec, 2005; Kucan, 2003)**.** It was therefore important to see how users assess their own security requirements based on their use of their device.

The main discovery was that participants did not feel at risk as their usage was limited to services that do not involve storage or access of highly sensitive information.

> *"As a general user who is only using it for personal use, there's no data on there that I class that sensitive"*

> *"I use this [Pocket PC] just for access to the exchange server and nothing else…So the issue of security hasn't arisen with this yet, but probably will do at some stage"*

> *"I think it depends from which context you are using it in, cause the security you are going to need in it, is going to depend on the sensitivity of the data…the only thing that I got that is sensitive is friends' phone numbers and address details"*

As participants did not generally recognise a current security requirement it was interesting to assess how they perceived the nature and adequacy of current authentication methods. Today's mobile devices are mainly protected by the use of PINs. However, previous research has suggested that users often perceive these to be an insufficient and inconvenient method, and consequently do not use them (Clarke *et al*. 2002; Clarke and Furnell, 2005). Similar views were also expressed by the participants, as only a third of them claimed to use PIN protection at switch on and only one used a PIN in standby mode. Meanwhile, the rest did not use any protection at all. Some based their decision not to do so on the fact that they did not perceive their current usage would pose any concern (which follows from the views in the previous section):

> *"Passwords and that kind of stuff, I've just never done it. I think the thing is with me that obviously because I just text and I don't do anything else, from a sensitive point of view there is no information that I perceive is valuable enough to be worth worrying about"*

> *"I'm not sure that anybody would want to steal my information, I don't perceive myself to be that important"*

However, even those that did make use of the mechanism expressed concern as to the level of security that it could provide in some contexts:

> *"I suppose for accidental loss or whatever, that will be fine because people are not going to guess your keyword or your PIN code or whatever. However PIN codes and things are limited … basically something that can be attacked in numerous ways"*

Although the sensitivity of information played a role, other comments mentioned traditional downsides of PINs such as forgetting them, and a viewpoint from many participants was that the PIN can only protect them if their phone is switched off (i.e. if someone acquired the device when already switched on they would find no requirement for reauthentication). The following comments were typical in relation to PINs:

> *" I think any security that is going [to] lock me out every now and then…is the reason I don't use PINs now cause I always forget my PIN…*

> *"I never turn my phone off so if I lost it, it would be on anyway"*

> *"I've used them before. It's simple to use, it's just…I don't see any point using it myself cause I never turn my phone off"*

These views underline the fact that PIN-based point-of-entry authentication is perceived to provide limited protection. A further factor that may have influenced attitudes towards security and use of current facilities was the fact that none of the participants had experienced a security incident:

> *"No, that's probably why I'm not so that worried about the security.*
> *I've never actually lost my phone, only ever dropped it when I'm drunk*
> *and reset it and things like that but never lost the phone"*

As such, it was perhaps not surprising to find that the general view was negative when asked about paying more for a device in order to increase security. The following comments were typical, suggesting that even if they considered paying, the protection itself was not the direct driver:

> *"No, not even for a second"*

> *"Well I don't know. If my phone had a fingerprint scanner on it, I'd*
> *think that was cool so yeah I'd pay more".*

Overall, therefore, it was clear that participants did not currently perceive a significant need to protect their devices. Even though this view was basically formed due to the limited usage of their devices, it was also partially informed by attitudes towards PIN-based authentication, which participants felt was not sufficient (and thus making use of it would hardly add any further protection for their devices).

Perceptions of future security requirements and responsibility

As the participants' limited security requirements were expected, an objective was to assess how future adoption of more sensitive services might affect their opinions. The majority certainly agreed that using more data-centric and sensitive services would increase their desire for protection:

> *"If you are using it from a business context, obviously you know the*
> *more important the data then the stronger security is going to be*
> *needed."*

> *"Although I don't use my phone for an awful lot more than texting at*
> *the moment, as phones get more sophisticated and easy to use etc ...*
> *I'm going to start using it for mobile banking or whatever the nature*
> *of the data that I'm gonna be using is going to become more sensitive*
> *definitely"*

Another aspect that was highlighted was the fact that stronger security would desirable in certain uses of the phone, as the danger of misuse would be increased.

> *"For example, if I make a local call ... maybe I'm not that worried ...*
> *But certainly when I want to start dialling international numbers or*
> *something maybe I do want to make sure that it's stronger*
> *authenticated. Maybe when I start to accessing documents that sit in a*

specific area of my device which is business documents then I want to be authenticated"

This view came in agreement with previous work by some of the authors that has suggested that linking the level of security to the service access would be a way of enhancing protection based on the sensitivity of the data (Clarke and Furnell, 2006). From this perspective, the question was explicitly posed as to whether it would be desirable to have distinct levels of security in order to be authenticated depending upon the service or data use. The general thought was that it could be a positive way to enhance security, but only if that was applied in a manner that maintained convenience:

> *"I don't want to have strong security for texting, but I do want to have some security for mobile banking, so different levels of security definitely would be the way to do it"*

> *"It depends how you put it. How many levels? I would be happy with one or two. Right now I'm using my phone. Do I want to enter a text message? All right, next level. Do I want to browse the Internet? Another level . . . one level or two levels would be fine. But getting it too far, it would be 'all right which level do I need? I need access 3 or access 5?"*

The idea of using their device to access more sensitive information led some participants to reassess the possibility to pay for additional security:

> *"When you start becoming more aware about stuff [dangers/threats] like that, you start realizing what you are doing with the phone as well. I think then you realize, actually I like the idea of [a network operator] providing higher security and I'll pay for that"*

Nevertheless there was also the view that the even future would impose more fears, there would be an expectation of security provision from the side of the services that are being offered, rather than the device itself:

> *"The type of data that I use my mobile phone with, and will use in the future, won't be very different from the one that I use in my PC anyway. It will just be a different access device. So I expect, if I'm going to be using data that are sensitive from a personal level, it will only be with services that I expect to be secure anyway. I wouldn't necessarily pay extra for that because that is their whole point of existence"*

Proceeding from this, it was interesting to see who participants generally considered to be responsible to provide security in the first place. Faced with this question, less than a third felt that it should be their own responsibility to ensure the security of their device. In terms of accessing services, the responsibility for security was felt to lie with a service provider (in order to secure the access and the data), rather than looking to protect the device itself in a more robust way:

"But then you are accessing bank accounts details that you're just using the mobile or whatever device you are using to access something somewhere else so the security is there...Responsibility for bank details should be with the banks, so they look after your confidential detail and security for your own device should be yourself"

The idea of making the network provider responsible for securing access to services and information was not viewed positively, again reflecting the fact that participants would prefer a distinction in the different roles.

"Not only you are trusting them with your password details but also that implies that they are never going to make a mistake, that they are never not going to pass your username and password on to somebody else. If I'm going to authenticate myself and log myself into a particular server, I actually want control of that. As much as I hate passwords, I want to have control over who I login with"

"Having my network provider say 'Oh don't worry, we'll authenticate you to the bank', that's something that I want them separately. You just give me network access, I'll deal with the bank, don't worry about it"

Given that most of the participants would prefer additional protection to be on their side rather than relying on the provider, it is relevant to consider the form(s) that this could take. As such, the next discussion topic proceeded to consider alternative authentication methods.

Views & attitudes towards alternative methods of user authentication

As alternatives to the PIN, participants were asked to consider two approaches – tokens and biometrics - and the way that they could be applied in the context of mobile phones.

Participants were not receptive to using tokens. Considering the device to be a token itself, the idea of needing to have something else to access it was not well-received:

"My first opinion would be that is just something else to lose...you still have the same issues with the token, because somebody could pinch the token, or I would lose it more likely"

"It's also the annoyance. Unless it's something you wear all the time... if I want to make a phone call I also have to take my watch or my key ring or whatever"

Unlike tokens, there was relatively high acceptance of the potential to use biometric techniques. As previous work has shown, users are starting to be more open to biometric techniques and consider their use in order to enhance security (Clarke *et al.* 2002). When the participants were asked which biometrics they would like to see implemented on mobile handsets and would be more willing to use, the majority

agreed that fingerprints would be adequate enough to safeguard the device, while at the same time seeming convenient:

"Personally I'd use fingerprint, it's easy…"

"I think fingerprint recognition would be fine on a phone…the average person who's gonna steal this, even if they do know how to fake the latex and so how to fake the finger, why would they bother? Just to break into somebody's mobile phone?"

Others were more open to techniques that could be linked to their normal use of the device or be derived from the features already existing on the device.

"There's a Korean phone that does facial recognition. I don't know how successful it is"

"Voice as well…obviously when you are talking"

Despite the fact that different kinds of biometrics were suggested by the attendees, fingerprint scanning was the most popular. As the technique is one of the most well-known biometrics, the question was posed as to whether this preference was linked to the greater knowledge of the technique in comparison with other approaches. The responses were mixed, with the general view being that it is just more convenient than other options. However, one participant also observed that it is a matter of culture, as many of us feel familiar with fingerprinting as a result of seeing it used in crime movies and the like. It was conjectured that other approaches would achieve similar acceptance on mobile devices if they were similarly familiar from other contexts:

"If … in order to get into the school, you needed to have your iris scanned then it would be like: 'All right, I had my iris scanned all my life, I don't mind really'"

In respect to the fingerprint versus other techniques, an argument that was made was the fact that biometric approaches that could depend on the use of the device are not applicable throughout all users as each one differs in their usage. As such biometrics like fingerprints can provide a common solution.

"I only use it for voice, he [another attendee] only uses it for texting. It's a mobile so one way or another you will have to hold it in your hand to actually use it so fingerprint is the most appropriate from that perspective"

This view underlines the fact that as no approach fits all needs, whether that is PINs or certain biometrics. Thus instead of providing one solution that some users are not willing to use, having a flexible mechanism that could conform to each user's needs while at the same time fulfilling the different security requirements would be a more appropriate approach. This is again compatible with the previous proposals from the authors (Clarke and Furnell, 2006)

Another issue raised in the discussion of biometrics was that of privacy, which has traditionally been presented as one of the factors that make people cautious about using the technology (Cavoukian, 1999). However, in terms of influencing preference towards certain techniques, privacy was not of much concern for the group. Most attention was given to the lack of accuracy and the excessive effort that biometrics (especially those based upon behaviour) may require, but also in certain techniques that they felt they could be less secure in their application on mobile phone:.

> *"The thing is even though it's a telephony device, the one I would be more uncomfortable using is voice, because anyone else can hear it"*

> *"And having any background noise affects voice recognition"*

> *"My problem I found is the signature recognition. I didn't like the voice recognition but as we were saying earlier for mobile phones that will be the most acceptable really. But the signature recognition I had problems with. My signature is never the same five times in a row, so I would get locked out of my mobile phone if I did that"*

> *"You can see…It's something about seeing an iris…if it went wrong and I was locked out … I'd feel out of control"*

On that basis, although acknowledging the level of security that biometrics can provide, participants would have little tolerance of getting falsely rejected and being locked out of the device:

> *"If it always let <u>me</u> through I'd be prepared to put up with that [false acceptance errors], because it's still a greater level of security that I use now and it's still not bothering me….I'm prepared to let the mistake happen as long it's not for me, as long as I am always let through"*

Transparent & continuous authentication versus traditional point-of-entry methods

With the issue of personal convenience still in mind, participants were asked to consider whether authentication can run in the background without the user having explicit knowledge about when it was taking place or needing to make explicit effort to provide authentication details. This has been suggested not only to overcome issues of intrusiveness that PINs or biometrics such as fingerprints could pose, but also to provide a continuous authentication solution versus the point-of-entry verification of PINs that was attributed a lack of protection by the attendees. Asked how they would feel about such a mechanism, attendees offered varying responses:

> *"I would like it cause if it doesn't interfere with you and there is no different reason anyway so there is no problem is it?"*

> *"I don't have a problem with this in a sense that I don't worry about the device monitoring me, but I will probably if something pops out and say 'No, you are not who you say'. Soon as it does that switch it off and then switch it on again"*

"That will be annoying…it would be like 'Oh it thinks it's not me'"

"Will it be a bit like when your battery is lowering gives you a warning? 'Cause how would you know? You make three mistakes or there are three different things in the background"

The negative views were mainly due to fears that false rejections could cause potential inconvenience by interrupting legitimate use of the device. There was also concern that the casual use of a mobile phone would not permit this type of authentication, as it would be difficult to acquire a consistent biometric profile at all times, again raising the issue of rejection rates:

"It's okay if you use it at your desk or something maybe but…I mean the nature of the mobile phone is that you don't generally use it like that. If you are sitting in a train or in a car or you are walking and you want to do something …I can't imagine that the way that I use it that I could be following a pattern. I'd get that three exceptions every five minutes kind of thing…I would feel uncomfortable"

Despite the potential intrusiveness, there was also the view that it would be preferable to have explicit authentication so that the user is always conscious of the procedure:

"I don't like the idea of any form of machinery interacting with me, without me giving it express permission that it may. I just don't like it, full stop"

Nevertheless that was not an issue for the majority of the participants. It was interesting enough that the main issue was usability and convenience, and less the issue of privacy that is often brought up in relation to biometrics. More focus on privacy came when the group was asked to give their opinion on how such an approach should be implemented - specifically in terms of the authentication taking place locally in the device or in the network (and thus where the biometric profile would need to be held):

"My concern is where would the fingerprint, let's say like signature, where would be stored? Would that be stored on the phone, so if somebody stole my phone they have my signature which is signed on the back of your bank cards and my fingerprint obviously? What then can people do with the information…obviously if someone knows how to hack into a phone could they use the information?"

As seen above the fear of having a device lost or stolen would discourage the idea of keeping the profile on the phone. On the other hand, there was also a view that storing the profile in the network would pose not only issues of control (moving from the user to the provider) but also the issue of who handles that information when it is on the side of the provider. In that context there were negative views about storing profiles in the network:

> *"Would you really want your biometric data stored on the inside of a company that's possibly got people, dodgy people breaking into it already?"*

Aside from trust towards the provider, two more issues were raised by the attendees in respect to the remote storage of the profile. First was the issue of immediacy of access and availability:

> *"Potentially everything can be stored in the network. There is a trade-off between responsiveness and security....Especially if you are not in coverage all period of time and you want to look up someone's name, address or whatever in your address book you haven't got it...There's got to be some balance between security that happens on the network and immediacy you have on the person"*

Similar to the issue of immediate access, participants indicated that they would not like to have explicit interaction with the provider in order to get authenticated. The preference was towards achieving authentication locally.

> *"I'd like to use that information even when I don't interact with the network operator. Because I can certainly use authentication as well, so I can't think that it can be just the network operator"*

Conclusions

This research recorded the views and attitudes of mobile phone users towards security on mobile phones. Most participants in the focus group did not see a significant need for security on their current mobile phones. However, the possibility of using their mobile phones for more than just calls and short messaging was recognized. The members of the focus group that used their mobile phones for more advanced tasks acknowledged that some form of security is important.

This was also reflected in the current use of authentication mechanisms. Most participants either did not use any authentication mechanism, or only used a PIN request at power up time, and were generally concerned with the inconvenience of current mechanisms. However, they were also receptive to the view that future, more sensitive uses of their device would necessitate greater use of security, and were therefore open to the consideration of alternative authentication methods.

Taking into consideration the concerns regarding the convenience of authentication mechanisms, it is not surprising that most participants were positive towards the use of biometrics and specifically fingerprinting. However, some privacy concerns were raised, particularly as to what exactly gets stored and where it gets stored. Others were concerned about being monitored continuously, especially if unaware of the fact.

This research supports the researchers' view that further work towards a comprehensive framework for authentication on mobile devices is indeed necessary. Furthermore it provided valuable insights into user perspectives on these matters.

Acknowledgements

References

Cavoukian, A. (1999) Privacy and Biometrics, Information & Privacy Commissioner of Ontario, Canada, http://www.ipc.on.ca/images/Resources/pri-biom.pdf

Clarke, N., Furnell, S.M, Rodwell, P.M, Reynolds, P.L (2002) Acceptance of Subscriber Authentication Method for Mobile Telephony Devices, Computers & Security, 21, 3, 220-228

Clarke, N.L., Furnell S.M. (2005) Authentication of Users on Mobile Telephones - A Survey of Attitudes and Practices, Computers & Security, 24, 7, 519-527

Clarke, N.L., Furnell S.M. (2006) A Composite User Authentication Architecture for Mobile Devices, Journal of Information Warfare, vol. 5, no. 2, 11-29

Ernst & Young (2005) *Global Information Security Survey 2005 : Report on the Widening Gap*, http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_20 05/$file/EY_Global_Information_Security_survey_2005.pdf

Kucan, B. (2003) Stolen PDAs Provide Open Door to Corporate Networks, Help Net Security, 1 August 2003, http://www.net-security.org/article.php?id=533

Red Herring (2006) Mobiles Scream for help: UK-based mobile security company adds security to mobile phones, 2 October 2006. http://www.redherring.com/Article.aspx?a=18907&hed=Mobiles+Scream+for+Help

Pointsec (2005) IT Professionals Turn Blind Eye to Mobile Security as Mobile Survey Reveals Sloppy Handheld Habits, Pointsec News Release, 18 November 2005, http://www.pointsec.com/news/newsreleases/release.cfm?PressId=108

Device- versus Network-Centric Authentication Paradigms for Mobile Devices: Operational and Perceptual Trade-Offs

S. Karatzouni, N.L. Clarke and S.M. Furnell
Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

The increasing capability and functionality of mobile devices is leading to a corresponding increase in the need for security to prevent unauthorised access. Indeed, as the data and services accessed via mobile devices become more sensitive, the existing method of user authentication (predominately based upon Personal Identification Numbers) appears increasingly insufficient. An alternative basis for authentication is offered by biometric approaches; which have the potential to be implemented in a non-intrusive manner and also enable authentication to be applied in an ongoing manner, beyond initial point-of-entry. However, the implementation of any authentication mechanism, particularly biometric approaches, introduces considerations of where the main elements of functionality (such as the processing of authentication data, decisions making, and storing user templates/profiles) should reside. At the extremes, there are two alternatives: a device-centric paradigm, in which the aforementioned aspects are handled locally; or a network-centric paradigm, in which the actions occur remotely and under the jurisdiction of the network operator. This paper examines the alternatives and determines that each context introduces considerations in relation to the privacy of user data, the processing and storage of authentication data, network bandwidth demands, and service availability. In view of the various advantages and disadvantages, it is concluded that a hybrid approach represents the most feasible solution; enabling data storage and processing to be split between the two locations depending upon individual circumstances. This represents the most flexible approach, and will enable an authentication architecture to be more adaptable to the needs of different users, devices and security requirements.

Keywords

User Authentication, Biometrics, Mobility.

INTRODUCTION:

The mobile networking landscape has changed significantly over the last decade with a transition from large form factor telephony devices to small multi-purpose multimedia communications devices. The recent introduction of Third Generation (3G) technologies has provided the underlying mechanism for a wide variety of innovative data orientated services, with approximately one million users every day adopting these new features (Best, 2006a). At the same time, the level of functionality can be seen to be significantly expanding, with devices today having similar processing and memory capabilities to PCs of a few years ago.

This transition imposes serious security considerations for mobile users, especially as incidents involving mobile devices and the disclosure of personal and corporate information are appearing within the media more frequently (Vance, 2006; Noguchi, 2005). One survey in the UK reported that within six months more than 54,000 mobile handsets were simply left on the back of London cabs, and another survey reported UK mobile phone theft accounted for 45% of all theft (Leyden, 2005; British Transport Police, 2006).

In this context it is relevant to consider the degree to which related security measures are already provided and utilised. It is widely recognised that authentication can be achieved by utilising one or more of three fundamental approaches: something the user *knows* (password); something the user *has* (token) and something the user *is* (biometric) (Nanavati et al. 2002). Currently, the most widely deployed authentication methods are passwords and PINs - secret knowledge approaches that rely heavily upon the user to ensure continued validity. For example, the user should not use the default factory settings, share their details with others, or write the information down. However, the poor use of passwords and PINs has been widely documented (Pointsec, 2005; Clarke et al. 2002), and many mobile users do not even use the security which is available. Similarly to secret knowledge techniques, token based approaches fundamentally rely upon the user to remember something, with the token needing to be physically present in order to access the device. However, it is considered that this does not lend itself particularly well to the mobile device context either. The most likely scenario is that users would simply leave the token within the mobile handset for convenience.

In contrast to the other methods, the third approach to authentication does not rely upon the user to remember anything – it just requires them to be themselves. Such techniques are collectively known as biometrics, and it is here that the most suitable alternatives for going beyond the PIN may be found. Biometrics have been suggested to be able to provide a more secure approach to authentication as the technique relies upon unique personal identifiers of the person. Therefore a user is not required to remember anything, and at the same time they cannot be lost or forgotten.

However, in order to establish an authentication mechanism for mobile devices - especially when biometric approaches are utilised, careful consideration is needed to address the trade-off between a network-centric versus device-centric implementation, with issues such as performance, privacy and mobility being essential to the adoption of a new approach. The purpose of this paper is to discuss the technical and perceptual issues that are involved in the implementation of the either approach and propose a solution that takes the best advantage of both. To this end, the basic characteristics of the two paradigms are presented in section 2, followed by a discussion of the resultant trade-offs in section 3. Section 4 then presents the proposed hybrid paradigm, leading to overall conclusions in section 5.

AUTHENTICATION TOPOLOGIES FOR MOBILE DEVICES:

The topology of an authentication mechanism is an important factor to consider at the outset of the design process. With numerous stakeholders (such as network operators, corporate IT administrators and end-users) the ability to provide identity verification in a manner that maintains both security and privacy, and considers the operational impact upon the mobile device is imperative. Unfortunately, however, it is difficult to maintain all these services for all stakeholders, and a trade-off exists between different security and privacy issues depending upon what the system is trying to optimally achieve. Although to date identity verification has been performed by the device itself this might not be the best approach to take when considering the number of issues that may result from both a security and usability perspective.

A Network-Centric Approach

A network-centric approach will direct all the key computational tasks and storage to the network. The physical placement of the authentication mechanism within the network could be with the network operator, corporate IT administrator, or third-party providing managed authentication services. As illustrated in Figure 1, the mobile device itself will act as the biometric sample capturing device and be able to respond to a decision sent from the server to permit or restrict access to a user.

Depending upon the device, its processing capabilities and security requirements, it could be possible to partially split the biometric process, where the data extraction phase is conducted on the device and classification on the network. This would assist in reducing the amount of traffic sent across the network. Nevertheless however, the focus of this paradigm is on all major computational and memory requirements being resident on the network rather than the device.
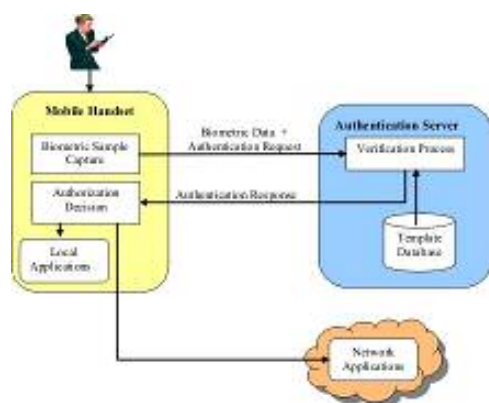

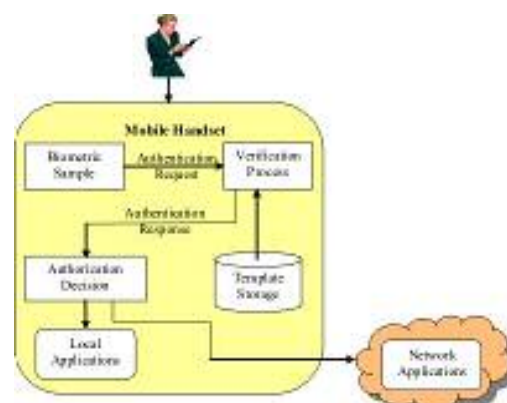Figure 1 A Network-Centric approach   Figure 2 A Device-Centric approach

A Device-Centric Approach

In a device-centric approach the whole biometric process is completed on the device. All the information, algorithms and management controls required for the authentication process are stored upon the device.

Furthermore, all the processing required to perform the verification also takes place on the device. Figure 2 illustrates an example of such an approach.

TRADE-OFFS BETWEEN THE PARADIGMS:

The two approaches described above have several advantages and disadvantages from both social and technical perspective. The principal areas to establish the trade-offs that exist are:

- User privacy
- Storage and processing of biometric samples
- Network bandwidth requirements

- Network availability
- Mobility and roaming
-

The following sections address and discuss these issues in turn, examining in detail the trade-offs between the two potential topologies.

User Privacy

When considering which topology to deploy, resolving the issue of user privacy is essential for widespread adoption. This becomes even more important when the topology is looking to utilise biometric techniques as the underlying mechanism. Recent years have seen widespread media attention directed towards biometrics, due largely to their inclusion within passport and national identity card schemes (Gomm, 2005). Unfortunately, and for some legitimate reasons, this attention has been somewhat negative towards the benefits of the technology, focussing instead upon privacy concerns (Porter, 2004; TimesOnLine, 2004). It is therefore important to ensure the authentication mechanism is designed in a fashion that is sensitive to privacy concerns.

The principal issue focuses around the biometric template and sample. In whichever biometric technique that is utilised, these elements represent unique personal information. Unfortunately, unlike other forms of authentication (such as secret knowledge or tokens, which can be simply changed if lost or stolen), it is not possible to change or replace biometric characteristics - they are an inherent part of the person. Therefore, once lost or stolen, they can remain compromised and no longer be reliably used. As such, the creation and storage of a biometric template or profile on either the device or the network leads to significant responsibility for the user or the network provider respectively.

Public opinion regarding biometrics has been problematic, not least because of the proposed national and boarder control schemes that are in implementation in many countries. These call for a centralised repository of biometric information for all nationals, but the ability to secure such databases from external attack and effectively manage authorisation to protect data from internal misuse is no small undertaking. Despite the safeguards that one can apply, there will always be the potential for vulnerabilities due to both human factors and technical mis-configurations. Such vulnerability, and moreover the lack of confidence that it engenders, was also raised in a focus group that took place in order to acquire users' views and attitude towards security on their devices (Karatzouni et al. 2007), where participants voiced the concern over security and trust:

> *"...would you really want your biometric data then stored on the inside of a company that's possibly got dodgy people, people breaking into it already..."*

> *"And even in the network [I] don't think it's all that secure either, because there is always the rogue employee somewhere, who is in the pay of an attacker"*

These quotes demonstrate a major fear for the security of the information held remotely. Apart from the technicalities that might be overlooked, there are also examples of carelessness taking place that has led to severe incidents. An illustrative example occurred within an Orange call centre, where employees that had been granted access to full customer records (including information such as bank details) were sharing their login credentials with other staff (Mobile Business, 2006). This removed any ability to effectively monitor who and when they had access to information. The increased fear of identity theft and fraud makes people even more cautious about their personal information, and how and where they provide it.

Recent discussions in the UK regarding a national ID card scheme has suggested that people are not very comfortable with providing their biometric information to a centralised system (Lettice, 2006). As such, a device-centric implementation is arguably more favourable from the user's perspective. In such a case, the profile will be stored on their personal device giving no third-party access to the biometric template or samples. This approach

is able to satisfy peoples' desire for privacy preservation by giving them direct responsibility for its protection. However, introducing such responsibility also brings concerns about how reliable and aware the end users will be in safeguarding their devices. As previously mentioned, several surveys have demonstrated that, despite the storage of sensitive information in handsets, and despite the earlier cited evidence of loss and theft, users still disregard the use of the available security measures. This is an important consideration to the choice in topology, as no further protection will be available once the device is stolen. On the other hand, one could suggest that as the fear of misuse becomes greater, the importance that each subscriber will attribute to the device will change respectively. For instance, storing personal identifiers in the device might lead people to consider their device to be comparable to other forms of important information and ID, such as, passports, credit cards, and car keys. Such linkage could potentially change people's perception and attitude toward the security and protection of their devices.

However, there was also a concern raised in the focus group expressing a fear of storage on the device and potential misuse.

> *"...my concern is where would the fingerprint, let's say like signature, where would be stored? Would that be stored on the phone, so if somebody stole my phone they have my signature which is signed on the back of you bank cards and my fingerprint obviously? What then can people do with the information...obviously if someone knows how to hack into a phone could they use the information?"*

It is certain that a biometric database will always constitute an attractive target, making it a more valuable target than a device involving only one person. It would be necessary in such cases to establish regulations and policies for the security of the database and biometric templates, and mandate continuing adherence to them. A central system, though, has an advantage that the system can monitor such activity and try to prevent it, thereby providing a more uniform and controlled protection space, than storage in the device.

People have different views towards the storage of such information as concerns are raised over the security in each storage solution and how potentially easy a breach of confidentiality is. A recent study conducted by the authors' research group attempted to assess public perceptions of biometrics, and performed a survey involving 209 respondents (Furnell and Evangelatos, 2007). One question asked people about their concern regarding the theft of their biometric data and the potential of using them to cheat a system. The responses are illustrated in Figure 3.
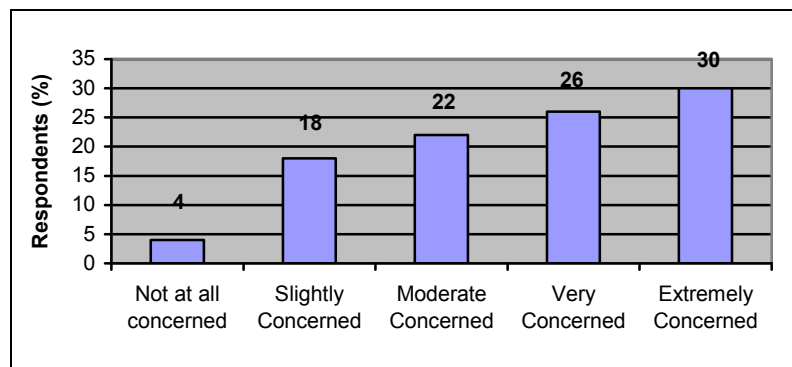
Figure 3 Concern that biometric information could be stolen

As seen from the figure, the majority of the respondents expressed some level of concern about the security of their data, with only 4% not having any fear of misuse. The same survey also asked where respondents would prefer their biometric data to be stored. Forty percent supported the network option whereas only seventeen percent agreed on the device (as illustrated in Figure 4). Interestingly, 18% would prefer their biometric templates to be stored in a smartcard. This is analogous to a device-centric approach, as the smartcard must remain with the user, but represents a significant enhancement in physical and logical security of the information.
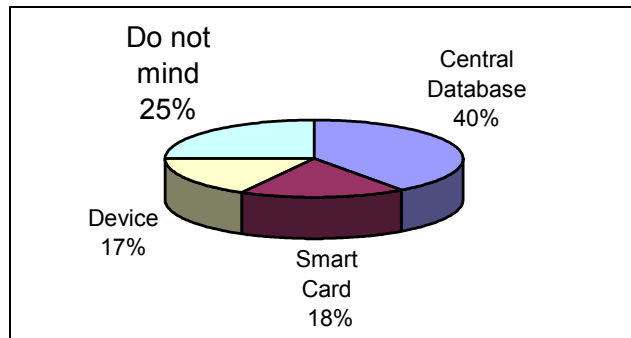
Figure 4 Subscriber preferences on storage of biometric profiles

Privacy concerns that exist for the network implementation could be reduced by ensuring only the biometric templates are stored and not any form of raw data. Several studies have taken place to overcome that issue, looking to protect the storage of biometrics using techniques such as distortion of the template. It is also notable that the creation of biometric templates is based upon vendors' own proprietary formats. As such, one biometric template from one vendor will not operate with another vendor's product, as the format and characteristics used to authenticate people differ. This will reduce the potential harm caused by a stolen biometric sample to systems that only utilised that specific vendor's product. The one-way property of creating biometric templates also ensures they cannot be reversed engineered.

Storage and Processing Requirements

While the privacy issue represents a challenge of user trust and perception, there are also technical-level considerations in terms of the storage and processing of biometric data. These will again differ according to the chosen topology.

Consideration needs to be given to the storage of the initial biometric template and also the samples that are subsequently used in the process of verification. For current PIN-based approaches this is not an issue, but the storage demands of biometrics are more significant. Issues of storage might exist in both topologies, with individual devices potentially having limited onboard storage, while the network-centric approach may need to cope with the storage of data for high volumes of users.

Different biometric techniques require differing levels of storage memory. Techniques such as face recognition (where multiple images might be needed from different angles in order to achieve a high consistent outcome), or voice verification (where sound files need to be stored), usually require higher storage capacities. Furthermore, as the proposed authentication mechanism aims to take advantage of a number of different techniques, the device or network will need to store more than one template per user, which could potentially become more demanding. Figure 5 illustrates typical template sizes from a number of more common biometric technologies.
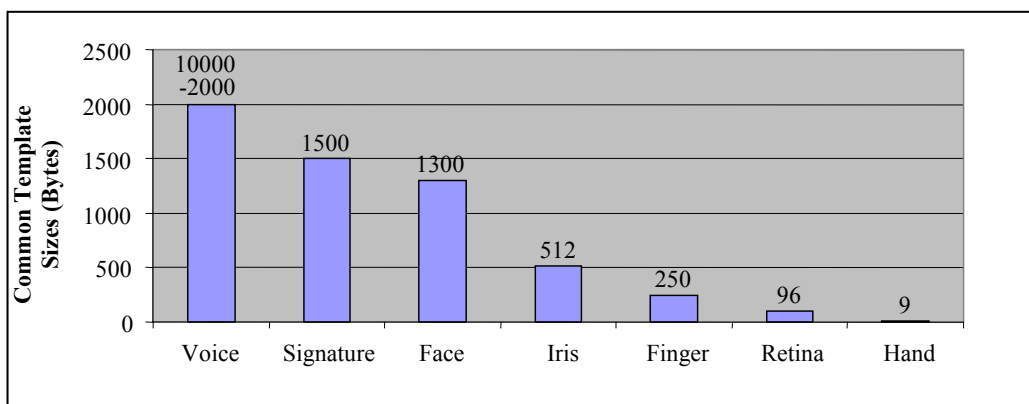
Source: International Biometric Group, 2002

Figure 5 Typical sizes of biometric templates

Given the memory available on current mobile device, it can be seen that the storage requirements would not prevent a device-centric implementation. The most demanding approach is voice scanning which can reach the requirements of close to 10KB. Therefore in general terms, storage of biometric templates in a device-centric paradigm does not present any difficulty. However, given the variability in devices and functionality, some care must be taken to ensure that this proposed authentication mechanism is able to operate with all hardware devices, including legacy devices which might have smaller storage footprints.

In terms of processing capabilities, the network-centric approach has an advantage in the sense that devices themselves may have relatively limited capabilities. Indeed, this may actually represent a fundamental obstacle to establishing a device-centric solution. Whereas laptop-level devices may have the capabilities required to process biometric data, the processing power in handheld devices is still limited. Algorithms that are utilised in biometric verification tend to be intensive, as they are based upon complex data extraction and pattern classification techniques (and indeed the impact of this additional processing on the battery of the mobile device would also have to be carefully considered). The process of enrolment and verification will place a serious demand upon resources on many mobile devices. In order to achieve transparent authentication, verification of the user needs to be completed without affecting the user's ability to use the device (e.g. no impairment to other running applications). It would not be satisfactory for the device to pause or hang for a few seconds every time verification was being performed. However, as with the storage footprint, different biometric techniques require varying levels of processing capacity. It is therefore not necessarily infeasible to consider at least some biometrics operating in a device-centric paradigm. Indeed, signature recognition, fingerprint recognition, keystroke analysis and facial recognition have all been developed for mobile devices (PDALok, 2006; NTT DoCoMo, 2003; Clarke and Furnell, 2006; Omron, 2005).

Over time, the processing constraints are likely to be overcome as the capabilities of handhelds continue to advance. However, from an implementation perspective, a network-centric paradigm would still potentially be easier to deploy and offer a wider range of possible biometric techniques. Again, however, consideration needs to be given upon the scalability of such an approach - multiplying individual authentication requests by high volumes of users does place a significant demand upon processing.

Bandwidth Requirements

A particular consideration in the context of the network-centric approach is the network bandwidth that will be required for the transmission of user authentication data. A device-centric approach has no such implications, as at most it will only be required to perform its normal authentication of the device to the network. By contrast, the network-centric approach will require network bandwidth to send biometric samples to the network, and receive authentication decisions back. Communication across the network will also result in a latency occurring between the initial authentication request and the resulting decision.

Typical bandwidth rates in practical 3G network scenarios are 220-320 kbps for UMTS and 550-1100kbps with HSDPA, although the theoretical rates are a lot higher (3G, 2004). An average 3G portal page, for example, has a size of 40 Kbytes and should theoretically take less than a second to load. However, in reality the actual throughput results in an 8-20 second delay. A usability study has shown that users are willing to wait for at least 3 seconds for a page to appear (Gissin, 2005). This willingness to wait is an important consideration in designing the authentication protocols and mechanisms. Forcing users to wait too long before being given access would result in a negative perception, particularly when the approach is meant to be transparent.

As discussed in the previous section, biometric templates can range from as little as a few hundred bytes up to 10Kbytes. These templates contain the unique data that is derived after pre-processing (thereby extracting the required features). The option of the device performing this procedure would be one way to decrease the bandwidth requirements, as the data sent would be far smaller than the raw sample. However, the ability to perform pre-processing on the device will depend upon the individual biometric technique and the processing capabilities of the device. If pre-processing can be implemented on the device it can be assumed that the size of the data being communicated is similar to those presented in Figure 5. A simple computation will show that the largest template of 10Kbytes will require time of 0.36 sec for the lowest given throughput on UTMS (220 kbps). It must be considered though that this might well become larger depending upon the network condition at the time and also takes no consideration of the time taken for the network to actually perform the authentication. Beyond latency for individual users, the issue of scalability needs to be addressed. Large volumes of users sending biometric sample data across the network might have significant impacts upon network resources and increase the level of delay experienced. For example, last year one of the largest operators in the UK accounted over 15 million subscribers (Richardson, 2005). If just 10% of them used such a service, we would be talking about 1.5 million users requesting authentication from the network. Of course the burden of the network will

depend upon the authentication frequency and this will vary across users as the different use of their device will result in more or less authentication requests.

At first glance one might suggest that current 3G networks (and certainly future networks) would be able to cope with the requirements. Although this might not be wrong in principle, an investigation of the network consumption does reveal somewhat surprisingly high volumes. Based upon the figures of 1.5 million users Figure 6 illustrates the bandwidth required per day for three different types of biometric approach.
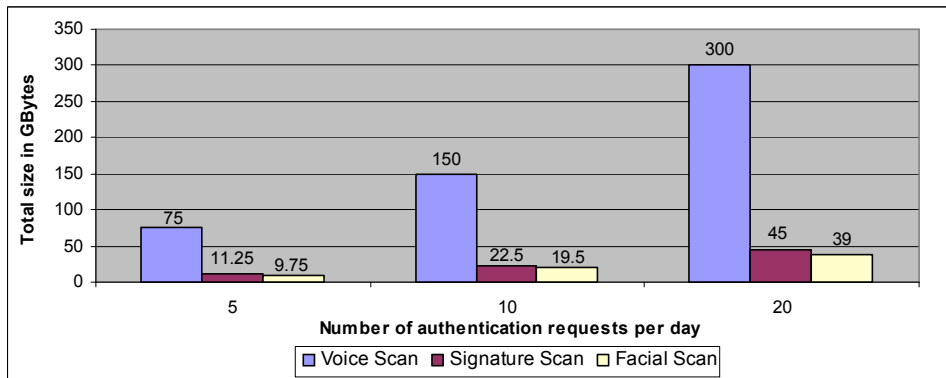
Figure 6 Average biometric data transfer requirements (Based upon 1.5 million Users)

As illustrated in the chart, for voice scan, even a minimum request for authentication of five times results a required data capacity of 75Gbytes for the network provider, whereas with up to twenty requests per day this raises to 300Gbytes. In comparison however, a video stream application, (one of the standard 3G applications), has bandwidth consumption close to 200Kbps for each user (Bruce, 2006). In a population of 1.5 million subscribers that represents 37Gbytes to be transferred every second. That said, there is a real cost associated with sending data across a network and there will be at least an indirect cost, given that the operator may otherwise be able to use the bandwidth to support revenue-generating services.

Availability Requirements

A factor that plays a significant role in a network-centric topology is the establishment of availability. In a fully device-centric approach all aspects required to perform the authentication are self-contained locally within the device. However, having the authentication process relying upon the network makes a key assumption that the network is available at all times to facilitate the process. In practice, there are various reasons why network connectivity might not be available, such as loss of coverage, network overload, or server malfunction. The inability to perform an authentication request as and when required will have a significant impact upon the authentication mechanism and its perceived usability.

Of course, if the authentication request is associated with a network-based application or service then one could reasonably argue that there is no inconvenience, as the service would not be able available anyway. What would be less acceptable, however, would be reliance upon network availability in order to access applications or features that would otherwise be entirely local. For example, opening a document, accessing contacts, or using Bluetooth to connect to another device, might all require authentication, and this would have a real and unacceptable impact if the process were to rely upon the (unavailable) network.

Participants in the focus group were asked to consider this issue and overall there was a negative opinion on always requiring access from the network. The following viewpoint was typical:

> *"I find it difficult that it might be possible just even to interact with the network operator, because I'd like to use that information even when I don't interact with the network operator."*

It can be suggested that apart from the technical issues that can occur, it seems rather inconvenient to require authentication from the provider. The inconvenience does not only relate to the access of local functionality and applications, but also the general concept - that in order to access any service the user will be obliged to explicitly go through the network provider. This places a burden of inconvenience upon the user, network provider and the authentication mechanism. One of the focus group members specifically summed up the issues surrounding the availability of network resources:

"There is quite a lot stored in the network. Potentially everything can be stored in the network. There is a trade-off between responsiveness and security….Especially if you are not in coverage all period of time and you want to look up someone's name, address or whatever in your address book you haven't got it. So that's completely rejected by the operators. There's got to be some balance between security that happens on the network and immediacy you have on the person... there isn't a simple answer to this sort of question"

Mobility and Roaming

A network-centric approach would enable personal mobility (Thai et al. 2003) - the ability, in principle, to get authenticated on any mobile device and have all subsequent use of the device billed to their account. Having the verification coming from the network, the subscriber will be able to use the system from various devices, without any swapping of SIM cards. The device-centric approach lacks such convenience as the storage and authentication of the user is linked to the specific device.

Conversely, however, when considering the issue of roaming, the device-centric topology is more appropriate as authentication of the user can be performed on the device wherever they might be in the world. A network-centric topology would experience significant increases in latency and have to transverse a far larger open network. Unless the local network provider supported the authentication mechanism and had a local version of the biometric template (which would not be likely due to privacy) this increase in delay would again have an impact upon the authentication mechanism which would need to be considered.

Also, what happens when roaming is not available? In such a situation, the user will have no way to be authenticated as no access to the provider's network will be available, restricting if not completely preventing any use of the device. There is also the consideration of cost. A home network operator implementing the authentication mechanism might be prepared to bear the cost of network consumption. However, this may not be the case for a roaming network, raising questions of who covers the cost. Currently the charges for roaming are very high, although this is expected to reduce in time (Best, 2006b). A device-centric approach would overcome this issue as no reliance upon external resources is required.

DISCUSSION:

The prior analysis has shown that comparing the device- and network-centric topologies introduces a varied and complex range of considerations, with each approach offering advantages and disadvantages in different contexts. Attempting to base a solution entirely around the device can introduce processing limitations, whereas bandwidth and the requirement for connectivity may represent practical constraints for a network-based paradigm. In addition, both approaches may introduce their own privacy-related concerns.

Based on the issues arising from both potential architectures, it can be argued that no single approach can cover all aspects that are required for the practical implementation of the proposed authentication framework. In order to try to overcome the troublesome aspects of each implementation, it is suggested that a hybrid approach would be more appropriate. Although complicating the underlying authentication system, it would provide a basis for overcoming the disadvantages of both topologies, while retaining their key advantages, so that the aims and objectives of the authentication mechanism can be met.

In such an approach both storage and processing would be potentially split over the device and the network, compromising between the issues of device processing capabilities, network availability, and privacy. The nature of the split in the authentication mechanism will depend upon the individual requirements of the user in relation to privacy and access, and the device in terms of which biometric techniques it can support locally. There will be therefore a number of hybrid approaches that could exist, each covering different issues on different scenarios for different users. For example, in order to deal with the issue of device processing and privacy, there could be the option to store all of the templates in the device, but place the processing functionality on the network. This would satisfy privacy concerns but at the same time discharge the device of any excessive processing tasks. Cryptographic measures could be used to protect the data in transit and during processing. Depending upon the device capabilities, pre-processing can be performed locally when possible, so that the biometric samples that are being sent over the network are kept as small as possible.

The specific nature of the hybrid system will closely depend upon a wide variety of factors that have been discussed in this paper. In order to remove the concerns surrounding network availability it is suggested that at least one authentication technique will always remain on the local device. Although this technique might not provide the level of security strong network-based biometrics might, it will be able to provide an effective means of authenticating short term usage of local applications and functions.

In devices with more possessing capacity, the hybrid approach would also be able to provide the ability to split the biometric templates, having the most intensive and demanding biometric techniques on the network and the others with fewer requirements on the device. Another basis for determining this split could also be the uniqueness attributed to them for privacy issues.

This hybrid authentication paradigm must incorporate a level of intelligence so it is able to understand when and how the security requirements can be attributed, and how the framework needs to adapt between different authentication techniques to handle those requirements. For example, if a user sends a text message or makes a local voice call then the operation need not be considered that critical, whereas accessing an mCommerce service or making an international call would demand more protection. The authentication mechanism should recognise this and select techniques that are appropriate to the context.

CONCLUSION:

With the growing popularity and functionality of mobile devices, the personal and financial cost of the device being misused or abused is increasing. As such, the ability to ensure and maintain identity verification of the user is imperative. Unfortunately, when considering the different types of authentication mechanism currently available, none satisfy the requirements for all users across all mobile devices. This situation is only complicated when you consider the dynamic and varied environment within which mobile devices operate, with varying functionality, processing and memory capabilities, differing network access technologies and a number of possible stakeholders all interested in the device.

Having discussed in some detail the advantages and disadvantages of network- versus device-centric paradigms, it was concluded that no single approach could achieve the desired aims. Therefore this paper has proposed the principle of a hybrid version that is able to encompass the advantages of both systems and assist in mitigating the key disadvantages. Future research will assess the viability of such an approach via the design and practical implementation of an associated architectural framework.

REFERENCES:

Best, J. (2006a), "3G reaches 50 million users worldwide", CNET.com, 10 February 2006, URL
http://news.cnet.co.uk/mobiles/0,39029678,49251672,00.htm

Best, J. (2006b), "Mobile roaming price-cuts in sight", Silicon.com, 12 December 2006,
http://networks.silicon.com/mobile/0,39024665,39164649,00.htm

British Transport Police (2006), "Mobile phone theft", URL

http://www.btp.police.uk/issues/mobile.htm

Bruce, J. (2006), "Trends in high-speed mobile video", Portable Design, March 2006, URL
http://pd.pennnet.com/display_article/249575/21/ARTCL/none/Appli/Trends_in_high-speed_mobile_video/

Clarke, N.L., Furnell, S.M, Rodwell, P.M, Reynolds, P.L (2002), "Acceptance of Subscriber Authentication Method for Mobile Telephony Devices", Computers & Security, 21, 3, pp220-228

Clarke, N.L., Furnell, S.M. (2006), "Authenticating Mobile Phone Users Using Keystroke Analysis", International Journal of Information Security, pp1-14, 2006

Denning, D. (1999), "Information Warfare and Security", Addison – Wesley, US

Furnell, S. and Evangelatos, K. (2007), "Public awareness and perceptions of biometrics", *Computer Fraud & Security*, January 2007, pp8-13.

Gissin, I. (2005), "Reality check: A 3G-user experience", TotalTelecom, 19 October 2005, URL
http://www.totaltele.com/View.aspx?ID=75921&t=4

Gomm, K. (2005), "Full biometric ID scheme to reach the UK 'by 2009", ZDnet.co.uk, 20 October 2005, URL http://news.zdnet.co.uk/hardware/0,1000000091,39232692,00.htm

IBG (2002), "How large are biometric templates?", International Biometric Group, URL http://www.biometricgroup.com/reports/public/reports/template_size.html

Karatzouni, S., Furnell S.M., Clarke N.L., Botha R.A. (2007), "Perceptions of User Authentication on Mobile Devices", Proceedings of the ISOneWorld Conference, Las Vegas, USA, April 11-13, CD Proceedings (0-9772107-6-6) 200

Lettice, J. (2006), "Compulsory and centralised - UK picks hardest sell for ID cards", The Register, 13 March 2006, http://www.theregister.co.uk/2006/03/13/ou_idcard_study/

Leyden, J. (2005), "Londoners Top World in Leaving Laptops in Taxis", The Register, 25 January 2005, URL http://www.theregister.co.uk/2005/01/25/taxi_survey/

Leyden, J. (2006), "Where's My 3.5G Handset?", The Register, 18 July 2006, URL http://www.theregister.co.uk/2006/07/18/informa_mobile_report/

Mobile Business (2006), "Orange Data Not Secure", Mobile Business Magazine, 22 November 2006, URL

http://www.mbmagazine.co.uk/index.php?option=com_content&task=view&id=1441&Itemid=2&PHPSESSID=d6fc7ad0c429dae5956c3ffd9466a84d

Nanavati, S., Thieme, M., Nanavati, R. (2002), "Biometrics: Identity Verification in a Networked World", John Wiley & Sons, New York, US,2002

Noguchi, Y. (2005), "Lost a BlackBerry? Data Could Open A Security Breach", Washington Post, 25 July 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/07/24/AR2005072401135.html

NTT DoCoMo (2003), "DoCoMo's Newest 505i Handset Features Fingerprint Authentication", http://www.nttdocomo.com/pr/2003/000985.html

Omron. (2005), "Omron Announces "OKAO Vision Face Recognition Sensor", World's First Face Recognition Technology for Mobile Phones", http://www.omron.com/news/n_280205.html

PDALok (2006), "Signature Recognition", PDALok, http://www.pdalok.com

Pointsec (2005), "IT professionals turn blind eye to mobile security as mobile survey reveals sloppy handheld habits", URL http://www.pointsec.com/news/newsreleases/release.cfm?PressId=108

Porter, H. (2004), "If you value your freedom, reject this sinister ID card", The Guardian, 17 December 2004, URL http://www.guardian.co.uk/idcards/story/0,15642,1375858,00.html

Richardson, T. (2005), "O2 posts upbeat trading update", The Register, 27 September 2005, URL http://www.theregister.co.uk/2005/09/27/o2_update/

Thai, B., Wan, R., Seneviratne, A., Rakotoarivelo, T. (2003), "Integrated Personal Mobility Architecture: A Complete Personal Mobility Solution", Mobile Networks and Applications, Vol. 8, No. 1, 27-36

TimesOnLine (2004), "ID and Ego: It is right to experiment with identity cards", Times Online, 27 April 2004, URL http://www.timesonline.co.uk/article/0,,542-1089392,00.html

Vance, A. (2006), "Lost Ernst & Young laptop exposes IBM staff", The Register, 15 March 2006, URL
http://www.theregister.co.uk/2006/03/15/ernstyoung_ibm_laptop/

COPYRIGHT

Keystroke Analysis for Thumb-based Keyboards on Mobile Devices

Sevasti Karatzouni and Nathan Clarke

Network Research Group, University of Plymouth, Plymouth, PL4 8AA,
United Kingdom, nrg@plymouth.ac.uk
WWW home page: http://www.network-research-group

Abstract. The evolution of mobile networking has opened the door to a wide range of service opportunities for mobile devices, increasing at the same time the sensitivity of the information stored and access through them. Current PIN-based authentication has proved to be an insufficient and an inconvenient approach. Biometrics have proven to be a reliable approach to identity verification and can provide a more robust means of security, as they rely upon personal identifiers. Amongst various biometric techniques available, keystroke analysis combines features that can offer a cost effective, non-intrusive and continuous authentication solution for mobile devices. This research has been undertaken in order to investigate the performance of keystroke analysis on thumb-based keyboards that are being widely deployed upon PDA's and Smartphone devices. The investigation sought to authenticate users whilst typing text messages, using two keystroke characteristics, the inter-keystroke latency and hold-time. The results demonstrate the approach to be promising, achieving an average EER=12.2% with the inter-keystroke latency based upon 50 participants. Uniquely to this tactile environment however, the hold-time characteristic, did not prove to be a reliable feature to be utilised.

1   Introduction

The proliferation of mobile devices and mobile networking has introduced new challenges for the protection of the subscribers' assets. The security risks are no longer associated only with safeguarding the subscriber's account. With the introduction of 3rd generation mobile networks, the services and information accessible through mobile handsets has increased in sensitivity, as micro-payments, mobile banking and location-based services are all now a reality for the mobile world [1]. Statistics show that mobile theft in the UK accounts 45% of all theft [2], a fact,

which when combined with the information that can be stored on mobile handsets and the attraction that high-tech devices can pose, presents a further concern for enhanced security.

Current authentication, principally achieved by PINs, is not enough to substantially safeguard today's mobile handsets and the data accessed through them. As a secret knowledge technique it has several well established drawbacks, such as being shared, written down or kept at factory default settings [3]. Furthermore, as survey results demonstrate, subscribers consider it an inconvenient method and as such tend not to use it in the first place, leaving their device completely unprotected [4]. This is not only limited to the general public, as the Mobile Usage Survey 2005 reveals, only 2 thirds of the IT managers surveyed have enabled password security in their mobile devices, despite acknowledging the amount of sensitive business information that is stored upon them [5].

Of the two remaining authentication approaches - tokens and biometrics, the latter can offer a more viable approach. Token-based authentication implemented to date by SIM cards does not provide any protection for the user as it is unlikely to be ever removed from the device. Biometrics could provide an enhancement on the current security, as authentication is based upon a unique characteristic of a person. This fact introduces a unique level of security that other approaches are unable to accomplish, as it relates the process to a person and not to the possession of knowledge or a token. A biometric approach that can provide a cost-effective and a non-intrusive solution for mobile handset authentication is keystroke analysis, a technique which is based on the typing dynamics of a user.

The purpose of this research is to investigate the feasibility of keystroke analysis on thumb-based keyboards based on text messaging input, looking to apply this technique as an authentication method for mobile handsets that offer that unique tactile interface. The paper proceeds with section 2 describing the unique characteristics utilised in keystroke analysis and provides an overview of keystroke analysis studies to date. Sections 3 and 4 describe the methodology and results of the study. A discussion of the results, placing them in context and areas for future research are presented in Sections 5 and 6.

2   Keystroke analysis

Keystroke analysis is a behavioural biometric that attempts to verify identity based upon the typing pattern of a user, looking at certain physical characteristics of their interaction with a keyboard. Considerable research has been undertaken on the method since first suggested by Spillane [6] in 1975, with studies identifying two main characteristics that provide valuable discriminative information:

- Inter-keystroke latency, which is the interval between two successive keystrokes, and
- Hold-time, which is the interval between the pressing and releasing of a single key

The majority of the studies to date have investigated the feasibility of keystroke analysis on full QWERTY keyboards [7 – 10], showing good results for both of the characteristics mentioned. In general, the inter-keystroke latency has demonstrated better discriminatory characteristics for classification in comparison to hold-time.

As in all biometrics the method to assess the performance of keystroke analysis, is by using the False Acceptance Rate (FAR), which indicates the probability of an impostor being granted access to the system, and the False Rejection Rate (FRR), which represents the degree to which a legitimate user is rejected. A trade-off exists between these rates, in terms of increasing security (and therefore increasing user inconvenience) and increasing user convenience (and thus decreasing the security). The point at which those two rates cross is referred to as the Equal Error Rate (%) and is used as a more objective means of comparing the performance of different biometric techniques.

The underlying classification algorithms utilized in keystroke analysis were traditionally statistically based [7, 8, 10]. However, advancements in neural networks have shown this technique to be more successful. A summary of key literature and results within the domain of keystroke analysis on PC keyboards is illustrated in Table 1.

Table 1. A summary of literature & results on keystroke analysis on PC keyboards

Study	Users	Input	Inter-key	Hold-time	Approach	FAR (%)	FRR (%)
Umpress & Williams[7]	17	Alphabetic	●		Statistical	11.7	5.8
Joyce & Gupta [8]	23	Alphabetic	●		Statistical	0.3	16.4
Brown & Rogers [9]	25	Alphabetic	●	●	Neural N.	0	12
Obaidat & Sadoun [10]	15	Alphabetic	●	●	Neural N.	0	0
Ord & Furnell [11]	14	Numerical	●		Neural N.	9.9	30

Although continuous research on keystroke analysis has been conducted since the 1980's, it was not until more recently that the method was assessed on interfaces provided on mobile phones where the tactile environment considerably differs. A series of studies accessed the method on regular mobile phone keypads with promising outcomes, achieving an EER of 8% based on numerical input [12]. Nevertheless, the performance of keystroke analysis for other tactile environments such as thumb-based keyboards is undocumented. Thumb-based keyboards constitute an interesting gap in research as they provide the extensive interface of a PC keyboard and the thumb-based properties of a mobile phone.

3   Methodology

This study looked into the feasibility of authenticating a user whilst typing text messages. Two different types of analysis were conducted in the context of this research: static analysis utilising the inter-keystroke latency and pseudo-dynamic utilising the hold-time characteristic. A total of fifty participants took part in the study, involving the largest population of participants for a study such as this and enabling more statistically significant results to be concluded. The participants were asked to enter thirty messages, with each message specifically designed to ensure that certain requirements are met.

For the static analysis six varying sized keywords were included in the text messages providing a static classification component. The varying nature of the static keywords permitted an evaluation of the word length versus performance. Thirty repetitions of each keyword were included, to ensure enough data for classification. The words selected are listed in Table 2, along with the number of inter-keystroke latencies that they involve and the number of samples used for training and testing after outliers were removed (a standard procedure for keystroke analysis studies [7-15].

Table 2. Keywords used for inter-key latency

Keyword	# Inter-keystroke latencies	#Samples after outliers' removal	Training Set	Testing Set
everything	10	27	18	9
difficult	9	26	18	8
better	6	27	18	9
night	5	27	18	9
the	3	26	18	8
and	3	27	18	9

Fig. 1. An XDA IIs thumb-based keypad   **Fig.2.** Screenshot from experiment software

Literature has showed that attempts to perform dynamic analysis on keystroke dynamics [13, 14] did not yield satisfactory results. As such an attempt was made to utilize a static component – the recurrent letters, in a dynamic form of analysis. The

pseudo-dynamic analysis was based upon the hold-time of the six most recurrent letters in the English language – 'e', 't', 'a', 'o', 'n' and 'i' - an adequate number of repetitions of which were included within the messages.

The text messages were entered using an XDA IIs handset that deploys a representative example of today's thumb-based keyboards, as illustrated in Figure 1. In order to capture the keystroke data, appropriate software was developed using Microsoft's Visual Basic .NET, and deployed on the handset. A screenshot of the software is illustrated in Figure 2. As usual in keystroke analysis studies, corrections were not permitted in case the user misspelled a word as this would undesirably interfere with the data [7]. Instead, the whole word had to be retyped in the correct form. Although it would be preferred to collect the data during multiple sessions, as a more indicative typing profile of the users could be captured, the data collection was performed in a single session, to maximise the number of participants that completed the study.

4 Results

4.1   Inter-keystroke latency

An initial analysis of the input data showed a fairly large spread of values on the inter-keystroke latencies. Even though smaller keywords were expected to give a greater consistency in the typing pattern because of their length and commonality, that was not the case. Additionally, the difference between the values of the different users was not large. These factors put a burden on the classification algorithm, as they make the classification boundaries between users very difficult to establish successfully. Figure 3, illustrates the mean and standard deviation for the larger keyword 'everything' for all users as an example of the problem.
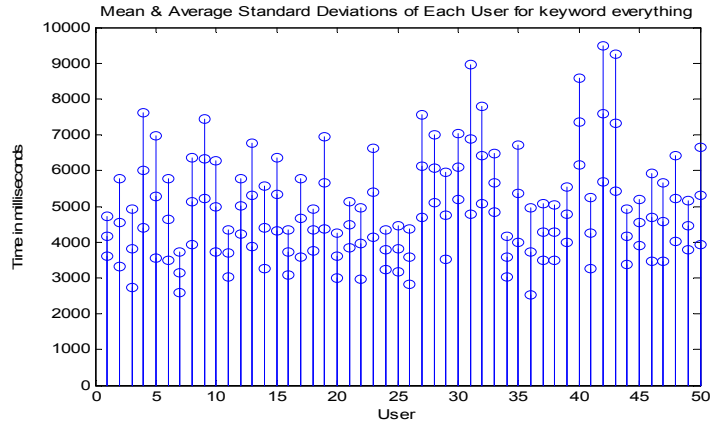
Fig. 3. Mean & Standard deviation for keyword everything

A number of analyses were undertaken, using Feed Forward Multilayer Perceptron Neural Network (FF-MLP) as it had demonstrated better performance in previous studies over other techniques [10, 12, 15, 16, 17]. Different network configurations were tested, looking for optimum performance. The best results achieved were for the keyword 'everything' with an EER of 23.4%. This was somewhat expected as the larger keywords contain more keystroke latencies and subsequently more discriminative information.

As illustrated in Table 3, the results show the FRR is much higher from the FAR which can be explained by the large number of impostors (49) extensively training the network versus the one authorised user. Furthermore, the number of samples assigned to the testing of the classification was small, resulting in the FRR encountering large steps in its transitions when being evaluated.

Although the error rate is fairly high, there were cases of users reaching an EER below 10% with the best case of user 1 achieving an EER of 0.3%, showing the ability to classify some users. The rest of the keywords resulted in higher error rates, with the error increasing as the length of the keyword was reducing. The best results for each keyword are illustrated in Table 3.

Table 3. Best results for each keyword

Keyword	FAR (%)	FRR (%)	EER(%)
everything	12.8	34.2	**23.5**
difficult	13.2	43.0	**28.1**
better	18.0	43.1	**30.5**
night	21.3	45.8	**33.5**
the	23.7	41.5	**32.6**
and	24.3	43.6	**33.9**

The average results of different networks showed minimal change in the EERs, although individual performances did vary. This suggests that the network does not

optimise for individual users but rather forces a standard training scheme upon the user. To overcome this problem a different approach was utilised by Clarke & Furnell [12], which provided an improvement in performance through optimising the number of training epochs. A gradual training technique was performed, training the network for an extensive number of epochs but periodically evaluating the performance. The results showed a noticeable decrease in the error rates with best case achieving an EER of 12.2% for the larger keyword. The summary of the gradual training results are presented in Table 4.

Table 4. Gradual training results for all keywords

Keyword	FAR (%)	FRR (%)	EER(%)
everything	15.8	9.1	**12.2**
difficult	16.8	12.0	**14.4**
better	23.5	14.4	**18.9**
night	24.2	14.4	**19.3**
the	29.3	19.5	**24.4**
and	28.7	17.6	**23.1**

Noticeably, for the keyword "everything", 20 users achieved an FRR of 0% with a respective FAR below 10%, with the best user achieving an FAR of 0.7% and FRR of 0%. The list of best and worst case users for all keywords are illustrated in Table 5. The results underline the requirement for different training intensiveness for each user, and that the inter-keystroke latency offers the discriminative data to classify users in the specific tactile interface.

Table 5. Best & worst case results from gradual training

Keyword	Best Case		Worst Case	
	User	EER (%)	User	EER (%)
everything	2	**0.4**	6	**32.4**
difficult	11	**1.3**	46	**34.1**
better	49	**1.6**	27	**34.2**
night	34	**2.3**	25	**40.5**
the	26	**6.4**	39	**45.8**
and	11	**5.4**	5	**49.4**

4.2   Hold-time

In contrary to the inter-keystroke latency investigation, the hold-time characteristic provided little discriminative information to classify users. A series of tests on different network configurations using all six letters (as to provide the largest possible input vector) resulted in an EER of around 50%, showing little classification performance. The same error rate was achieved using different size subsets of the letters with smaller input vectors (but with the advantage of more repetitions of each

letter) and also with a larger input vector of eight letters through the addition of letters 'r' and 's', as they appear next on the reoccurrence list.

In order to further assess the performance of hold-time, a group of only 20 users was utilised aiming to help the classification problem by reducing the amount and complexity of information presented to the network and thus assisting in the discrimination of authorised and unauthorised users. However, no change in the performance was experienced. Even when gradual training was applied, using the six letters set, no significant improvement was observed. Sample results from various tests are provided in Table 6. Even though there was a 10% decline on the EER using gradual training, the results are still too high to suggest that hold-time can offer any valuable discriminative information.

Table 6. Sample results from various tests on hold-time

Set	Training	Users	FAR (%)	FRR (%)	EER(%)
6 letters	normal	20	49.5	49.4	**49.5**
6 letters	normal	50	31.3	69.0	**50.2**
8 letters	normal	50	26.7	72.9	**49.8**
3 letters	normal	50	22.1	77.6	**49.9**
6 letters	gradual	50	34.2	36.8	**36.8**
6 letters	normal	20	49.5	49.4	**49.5**

5   Discussion

As the results showed the inter-keystroke latency can provide an effective means of differentiating between users. When based on a latency vector of 10, an EER of 12.2% was achieved with the gradual training approach. As was expected the use of smaller input vectors resulted in a corresponding increase in error rates, as the amount of unique discriminative information and feature space reduced.

With regards to the inter-keystroke latency, this study did not experience the very low rates in performance that have been found in previous studies based on regular keyboards. It is suggested that a number of aspects differentiate this investigation from previous studies. The keyboard utilised in this study provides a completely different tactile interface than traditional keyboards, with a more restricted keystroke interface, reduced distance between the keys and smaller key depth. In addition, the number of fingers utilised in typing has also been reduced from typically 10 fingers and thumbs to 2 thumbs. Both of these factors restrict the typing dynamics, as the combinations of the fingers in conjunction with the timing of the keystrokes and movement to achieve them, are reduced. This results in a smaller feature space for the keystrokes characteristics to reside in and subsequently making it more difficult to distinguish between them. Furthermore, although the layout was familiar to all users as it shares the same layout with a PC keyboard, some of the participants experienced difficulty in identifying the placement of the keys due to the different way of typing.

The hold-time characteristic did not provide any real evidence to suggest that it can be utilised in this specific typing interface, though there are a number of factors

that may explain the inability of the keystroke feature. Firstly, the keys that the thumb-based keyboard deploys are very small related to the chunky tactile environment that a normal keyboard offers, restricting the interval length between the pressing and releasing of a key and thus not providing much differentiation in values. Although the hold-time has performed well on regular keypads [12], the keys were larger than the keyboard used in this experiment and the method of calculating the hold time was different. In the study by Clarke & Furnell [12], the hold-time was defined by the first key press down until the last key release, increasing immediately the range of values and thus the feature space (for instance, for the character 'c' the number 1 button would need to be pressed three times).

Furthermore in a thumb-based keyboard, fingers stay almost static due to the limited area. As such, the hand movement which appears in PC keyboards and may affect the pressing of a key is unlikely to happen in this case. What must also be noticed is that some participants complained about the feedback from the keyboard, as they could not at all cases be sure if they had pressed a key, which might have further complicated matters.

6   Conclusions

This research conducted a feasibility study on the utilisation of keystroke analysis as an authentication method in devices that offer the tactile environment of a thumb-based keyboard. The results showed that from the two traditionally used keystroke characteristics, the inter-keystroke latency gave promising results in-line with previous studies undertaken. However, unusually the hold-time characteristic gave no promise of a potential use in this kind of keystroke interface, though further research must be undertaken to determine this conclusively.

Future research will be conducted looking to optimise network configurations for the inter-keystroke latency to take into account the bias towards the network responding in favour of the impostor. Furthermore, the use of different keywords will be investigated, as will the concurrent use of more than one keyword within a single authentication request, the latter aspect having the potential to substantially improve performance. In respect to hold-time, further tests are required before concluding to its ineffectiveness, exploring the use of longer input vectors and different letter subsets. A future experiment will also look to utilise different thumb-based keyboards that offer a slight different tactile environments than the one utilised in this study. Additionally, future work will seek to investigate the performance of the technique in environments representing more practical situations, thereby providing more balanced results. Factors such as the user's interaction with the handset whilst they are walking and their physical condition (e.g. tired or stressed) can be investigated for their impact upon performance.

This study has demonstrated promising results for the use of keystroke analysis, using a significantly large number of participants than previous studies. Although the accuracy of the method does not compete in distinctiveness with other biometrics such as fingerprints, the nature of keystroke analysis in that it can provide a monitoring authentication mechanism, transparent to the user (which is not feasible

for many other techniques) is a positive attribute. If used regularly and in conjunction with other transparent authentication techniques, keystroke analysis can be an effective means of providing a more enhanced level of security.

7   References

1. The UTMS Forum, Mobile Evolution – Shaping the future (August 1, 2003); http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/umts/ MultiMedia_PDFs_Papers_Paper-1-August-2003.pdf

2. British Transport Police, Mobile phone theft (August 20, 2006); http://www.btp.police.uk/issues/mobile.htm

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

4. N. Clarke, S.M. Furnell, P.M. Rodwell, P.L. Reynolds, Acceptance of subscriber authentication method for mobile telephony devices, *Computers & Security*, 21(**3**), pp220-228, 2002.

5. Pointsec, IT professionals turn blind eye to mobile security as survey reveals sloppy handheld habits (November 17, 2005); http://www.pointsec.com/news/release.cfm?PressId=108

6. R. Spillane, Keyboard Apparatus for personal identification, IBM Technical Disclosure Bulletin, 17(**3346**) (1975)

7. D. Umphress, G. Williams, Identity Verification through Keyboard Characteristics, *International Journal of Man-Machine Studies*, 23, pp. 263-273 1985.

8. R. Joyce, G. Gupta, Identity Authentication Based on Keystroke Latencies, *Communications of the ACM*, 39, pp 168-176 1990.

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

10. M. S. Obaidat, B. Sadoun, Verification of Computer User Using Keystroke Dynamics, *IEEE Transactions on Systems, Man and Cybernetics – Part B: Cybernetics*, 27(**2**), (1997)

11. T. Ord, User Authentication using Keystroke Analysis with a Numerical Keypad Approach, (MSc Thesis, University of Plymouth, UK, 1999)

12. NL. Clarke, S.M. Furnell, Authenticating Mobile Phone Users Using Keystroke Analysis*, International Journal of Information Security*, ISSN:1615-5262, (2006), pp.1-14

13. G. Leggett, J. Williams, Verifying identity via keystroke characteristics, *International Journal of Man-Machine Studies*, Vol. 28(1), (1988), pp.67-76

14. R. Napier, W. Laverty, D. Mahar, R. Henderson, M. Hiron, M. Wagner, Keyboard User Verification: Toward an accurate, Efficient and Ecological Valid Algorithm, *International Journal of Human-Computer Studies*, 43, pp.213-222 (1995).

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

16. S. Haykin, *Neural networks: A Comprehensive Foundation (2nd edition)*, (Prentice Hall, New Jersey, 1999)

17. M. Bishop, *Neural Networks for Pattern Classification*, (Oxford University Press, New York, 1995)

UTILISING BIOMETRICS FOR TRANSPARENT USER AUTHENTICATION ON MOBILE DEVICES

Sevasti Karatzouni, Nathan L. Clarke and Steven M. Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
info@network-research-group.org

ABSTRACT

Mobile devices have become a ubiquitous computing device, with over a third of the world's population now owning a device. The nature of the device has expanded far beyond its original inception as a telephony device, now capable of accessing and storing a wide-variety of information. Given this increased access, the ability to effectively provide security has become increasingly important. Key to these is authentication of the user to the device.

Unfortunately current authentication methods such as the PIN are found to be severely lacking in providing any level of security beyond initial point-of-entry, with the level of protection being provided here arguable insufficient. This paper proposes the application of biometric techniques in a transparent and non-intrusive fashion to enable continuous and user convenient authentication of the user. The proposed mechanisms seek to adapt current classification algorithms in a manner that trades off a small degree of security for larger improves in the robustness and user acceptance of the approach.

KEYWORDS

Biometrics,   Authentication,   Mobility

1. INTRODUCTION

The increasing capabilities of mobile handsets and networks have enabled the creation of a wide range of data-centric services. The volume of information that can be stored and accessed through mobile devices have become enormous. This has raised significant concerns regarding the sensitivity of the information for both individual and more particularly organisations. A recent study by Gartner reports 80% of organisations' critical information is stored on mobile devices [1]. It can be therefore suggested that providing appropriate protection against unauthorised access to information becomes significantly important.

A significant component of the device security consists of user authentication. The current authentication facility in mobile handsets is primarily achieved by the Personal Identification Number (PIN). Unfortunately PINs, being a secret-knowledge technique, have a number of well documented drawbacks: security relies on the user and therefore bad practices from the latter significantly diminishes the security that PINs provide [2].

An alternative solution towards more robust authentication is biometrics, which as they are based on personal identifiers; they closely relate the authentication credentials to the user and thus are able to provide more robust trust to the authentication decision. Biometrics are beginning to constitute a significant impact on the authentication market and their adoption is increasing every year for a range of industries and applications where authentication and identification of a user is required. Their application has already taken place on mobile handsets and it is estimated that in general mobile biometric solutions are going to contribute $268 million towards total mobile identity and access management market by the year 2011 [3].

To date however, all authentication approaches, including biometric approaches, have focussed upon establishing point-of-entry authentication of the user. Although this is imperative to establish at the beginning of a session, unfortunately no further verification of the user is undertaken until the device is switched off again. With the increasing reliance upon mobile devices, few devices are now actually even switched off, removing any protection point-of-entry solutions offer. The ability to provide non-intrusive authentication in a transparent fashion, without the explicit interaction of the user will assist in establishing the identity of the user throughout the session. Of the three authentication approaches: secret-knowledge, tokens and biometrics, only the latter really provides an effective mechanism to achieve this. Through the careful application of particular biometric techniques it could be possible to not only increase security but do so in a user convenient manner. It is important however to utilise techniques that lend themselves towards transparent application. Although in principal many techniques do the ability to achieve this in practice is somewhat restricted. This paper discusses the issues involved in deploying several key biometric techniques in a transparent fashion and proposes a mechanism to achieve this.

The paper is structured as follows. Section 2 presents a background in biometric authentication with section 3 discussing the application of specific techniques to a mobile device. Section 4 discusses the issues that restrict the envisaged application, examining the modifications required to enable transparency. The conclusions are given in Section 5.

2. BIOMETRIC AUTHENTICATION

Biometrics as defined by the International Biometric Group (IBG) is *the automated use of physiological or behavioural characteristics to determine or verify identity* [4]. The operation of biometrics is based on a process of establishing the level of similarity between two samples: a reference template stored in the system that was acquired during enrolment and a new acquired sample provided by the user each time that authentication must take place. A typical biometric system is illustrated in Figure 1.

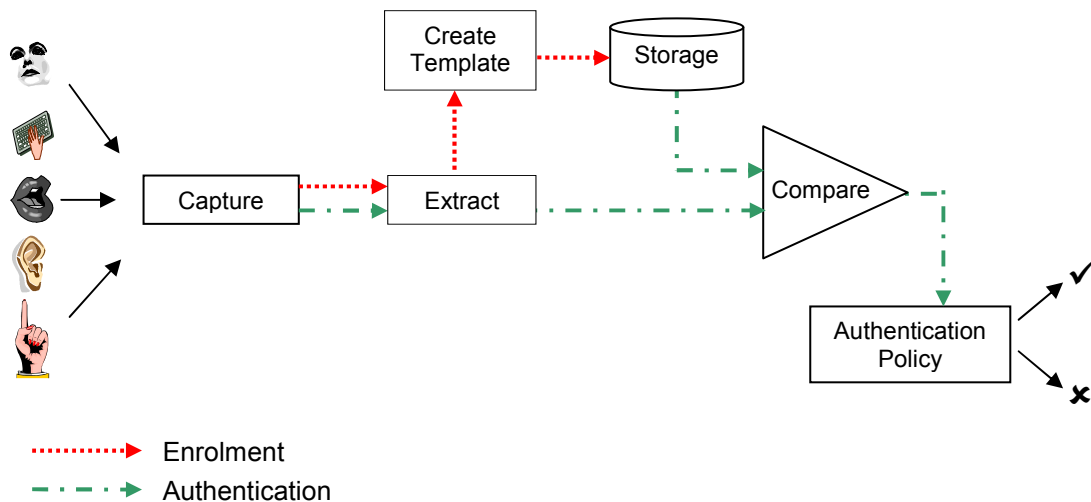Figure 1. A typical biometric system

Each time a new sample is fed into the system the distinct features are extracted and then subsequently compared to the reference template. This extraction differs per technique in order to preserve privacy of the stored information, as well as to improve performance. Even though biometrics can be provide more robust security, the result of the comparison is a function of

similarity between the two samples and as such can lead towards two principle error rates that affect the performance of the system:

- *False Rejection Rate (FRR)*, which corresponds to the rate at which a legitimate user is falsely being denied access to the system, and

- *False Acceptance Rate (FAR)*, which represents the rate at which an impostor getting accepted by the system

Although biometric performance is the outcome of a number of factors such the feature extraction, the algorithms used to perform the comparison and also environmental conditions, the principal contribution towards good performance is the distinctiveness of the characteristics utilised. This distinctiveness varies amongst the different biometric techniques; especially between behavioural and physiological biometrics as the latter tend to be much more distinct than their behavioural counterparts. An overview of a number of biometrics of interest follows addressing the above issues as well as presenting how each technique operates.

2.1. Face Recognition

The facial structure carries a distinct geometry which can be utilised to discriminate between users. There are different ways that face recognition is performed. Traditional approaches make use of distances formed between specific key points of the face such as the points of the eyes, of the side of mouth and the nose etc [5, 6]. Though more recent techniques tend to examine the holistic view of the face's geometry concurrently utilising a number of characteristic attributes [7]. Although that makes them more demanding in terms of processing, it at the same time makes them more efficient. In all the above techniques the representation of the face is 2-dimensional which appears to be very sensitive to varying illumination, posing or facial expressions [8]. More recent research has focussed upon 3D representations in order to improve tolerance to the aforementioned variations.

2.2. Voice Verification

Voice verification seeks to differentiate between people based on their way of speech. Voice scanning is looking to extract discriminative information from a person's voice by examining the dynamics of his speech. In that way, the technique does not rely only on the sound of a word or phrase that someone could closely replicate, but it takes under consideration the overall dynamics which can not be rendered by mimicking the voice of the legitimate user. Voice verification can operate in three fashions:

- Text – dependent : the user is authenticated based on predefined keywords
- Text – prompt : the used is authenticated based on a challenge scenario
- Text – independent : the user is authenticated regardless what they say

Although all three have been extensively researched only the two first have been applied successfully.

2.3. Signature Verification

This technique utilises the uniqueness of a persons signature to verify a user's identity. Although its first application was to only look at the final result of the user's signature, newer approaches utilise other characteristics in conjunction to improve against forgery. As such a number of dynamics on the user's handwriting are taken into consideration; for example, pressure, speed, direction and the number of the strokes [5, 9]. In that way even if the final result appears to have the same signature characteristics in regards to actual image of the

signature, the dynamics that would be involved can not be counterfeit and as such the measurements would be substantially different. Most of systems nowadays utilised the dynamic approach of the technique.

2.4. Keystroke Analysis

Keystroke analysis is a biometric that tries to discriminate between users based on the way they type in a keyboard. Two features of the overall keystroke dynamics are traditionally utilised as they appear to carry more discriminative information. These are:

- Inter-key Latency: the interval between two successive keystrokes
- Hold Time: the interval between pressing and releasing a key

The technique has not reached the performance of other mainly physiological characteristics, however it has been thoroughly researched as its nature enables authentication to be performed with great transparency to the user. A downside that exists is with respect to the large amount of training data that the technique requires in order to classify between users, however given time to collect this issue is reduced. Keystroke analysis although had been extensively researched for regular keyboards it was not until recently that was assessed for keypads deployed in handsets where the tactile environment differs. The performance of the technique on mobile handsets has showed promising results by research undertaken by the authors in the past [10, 11].

3. BIOMETRICS FOR MOBILE DEVICES

There are a range of biometric techniques currently that have the potential to be utilised within a mobile context but each of them has certain trade-off in terms of cost and performance as well in regards to the option to operate transparently. Table 1 lists techniques that their application is feasible on a mobile device as well as a number of criteria important for their selection.

Table 1. Potential biometric techniques for mobile devices

Biometric technique	Sample acquisition capability as standard?	Accuracy	Non-intrusive?
Ear shape recognition	✘	High	✔
Facial recognition	✔	High	✔
Fingerprint recognition	✘	Very high	✘
Handwriting recognition	✔	Medium	✔
Iris scanning	✘	Very high	✘
Keystroke analysis	✔	Medium	✔
Service utilization	✔	Low	✔
Voice verification	✔	High	✔
Gait verification	✘	Unknown	✔

It can be seen that techniques that share the highest accuracy are at the same time more intrusive to the user. As such there will always be a trade-off and a balance to be sought towards satisfying both aspects of security and convenience. However there are a number of techniques that can operate transparently without further hardware requirements which can significantly reduce cost. Furthermore the aim of achieving transparent authentication imposes the requirement for approaches that are based on the regular use of the device so that no explicit interaction is required. In that basis the techniques to utilise should be also based on integrated

hardware in current and future devices, which is used during normal usage of the device. As such feasible examples of techniques that this might be achieved by - based on current capabilities of the devices, are:

- *Voice Verification*: Capture voice samples during a voice call.

- *Face Recognition*: Utilise the front camera of the handset during a video conference call or furthermore capture snapshots during a normal interaction of the user with his phone as their will be facing the front of their phone.

- *Signature Recognition*: Capture samples while a user utilises an editor in order for example to keep notes.

- *Keystroke analysis*: Capture samples while a user is typing text messages or writing a document.

- *Service Utilization:* Monitor the interaction of the user with the device based for instance on application use, frequency and timing of use etc. (Service utilisation has not yet be developed as an explicit biometric yet)

However, the effective application of the above techniques is not simple in the manner desired, as issues arise when looking to apply them in a mobile environment and moreover transparently.

4. EFFECTIVE APPLICATION ISSUES

Even though the biometric techniques discussed previously have a number of real world applications, their application in the envisaged manner within a mobile environment is restricted due to the way that the sample is captured and how the classification algorithms are implemented. Furthermore, although the nature of the approaches has the potential for transparency, current implementations of them are based on well defined point-of-entry conditions. The following sections will examine the issues that restrict their application and also the methods by which the techniques can be adapted to transparent application.

4.1. Face Recognition

The use of the technique to date has typically focussed upon very well defined environments, with controls on the illumination, facial orientation and distance from the capture device. In a mobile device these conditions are far more variable with authentication needing to take place under a wide-variety of different environmental conditions. The implementation of the technique in a transparent fashion will only seek to complicate these requirements further. The user will not be explicitly asked to pose as the sample is captured and could suffer from a number of bad variables such as poor lighting due to time of day or location, having a significant difference in facial orientation as the user is looking away from the mobile device.

In order to overcome the above issue of transparency and thus improve the tolerance of the technique to variations, two options are available. Firstly to undertaken research looking to improve the classification algorithms and remove the dependence upon these factors. Secondly, look to adapt current classification algorithms in a fashion that achieves transparency. This research proposes to opt for the latter choice, as research into improving classification algorithms has and will continue to take place and designing a process that adapts existing approaches rather than designing a single mechanism provides more flexibility. Unfortunately, when looking to adapt currently algorithms, the process is essentially trading with the FAR and

FRR of the system: typically trading less security (higher FAR) in favour of a higher level of robustness and user acceptance (lower FRR).

The proposed method of adapting existing algorithms is to move away from a one-to-one comparison of an image with a template, and replace the template with a series of images that represent various facial orientations of the authorised user. In this way, existing pattern classification algorithms can still be applied, however the approach should overall be more resilient to changes in facial orientation. As under this proposed mechanism, each sample will effectively be compared to a series of images stored within the template, the number of verifications performed will increase. This will therefore introduce an increased likelihood that an impostor is accepted by an appropriate similarity with at least one of the series of images. Under this proposed system, the FAR will only ever be as good as the original FAR of the algorithm being used, with more realistically an increase in the FAR being experienced (as illustrated in equation 1). Conversely however, under this proposed system the FRR will at worst equal that of the previous FRR, but more realistically will be lower (as illustrated in equation 2).

$$FAR_{new} \geq FAR_{old} \qquad \text{(Equation 1)}$$

$$FRR_{new} \leq FRR_{old} \qquad \text{(Equation 2)}$$

The advantage of trading of the FAR and FRR in facial recognition is two fold:

1. Facial recognition approaches have quite distinct characteristics and experience good levels of performance in terms of FAR and FRR. Indeed, facial recognition systems are often used in identification systems as well as verification systems. The use of them for verification does not require such distinctiveness.

2. The relationship between the FAR and FRR is not linear but non-linear, with small changes in the FAR typically resulting in larger changes in the FRR.

It is therefore possible to take advantage of these properties to provide a little less security for a larger improvement in the robustness and usability of the approach.

4.2. Voice Verification

Although voice verification can be performed using one of three types of input, the only effective solutions to date have been based on the text-dependent and text-prompted inputs. Unfortunately neither of these approaches can offer transparency to the verification process as the user would be required to repeat predefined or real-time generated words prompted from the system. The text independent approach is the ideal solution to the issue of achieving transparency, enabling the system to analyse the voice of the user while they use voice applications and extract the distinct features regardless of what the user says. However, to date this technique has not managed two achieve satisfactory classification results as the inputs into the classification algorithm tend to be too variable.

Similarly to the proposed mechanism for facial recognition, it is not the purpose of this solution to further the research being undertaken within the voice verification domain, of which there is much. Instead through modifying the method by which existing algorithms are used the objective of transparency can be achieved. The solution proposes to utilise the combination of three existing technologies:

1. Voice Verification – Text-dependent mode. To perform voice verification on single static phrases or words.

2. Voice Recognition. To perform recognition of the words being spoken.

3. Database. To provide a mechanism of indexing and storing the words and voice templates.

The use of voice recognition would enable recognition of the spoken word/phrase and can subsequently index them in a database of words spoken. Given a carefully designed enrolment process, the database of indexed words would be sufficiently large for a text-dependent voice verification approach to then be applied to the static word. The process of enrolment and verification is illustrated in Figure 2 and Figure 3.
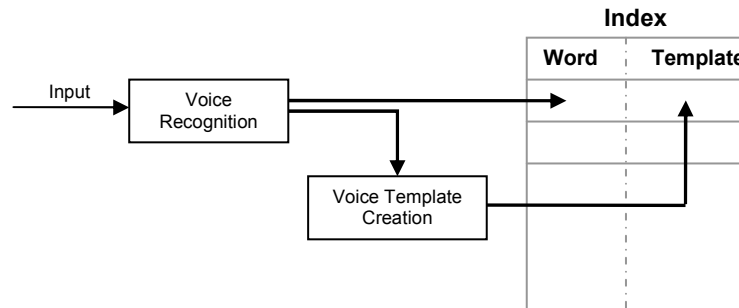
Figure 2. Voice Enrolment Process
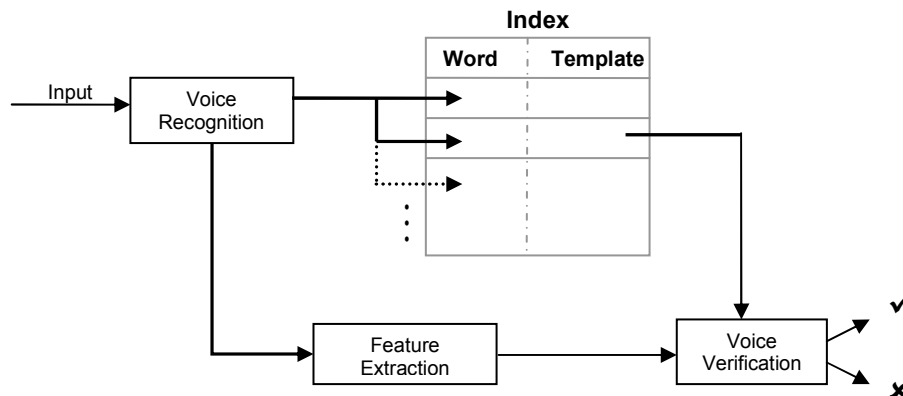
Figure 3. Voice Verification Process

Through applying the algorithms in this manner the system is able to take advantage of strong performance experienced by text-dependent voice verification. The possible disadvantage is the enrolment database of index words not being sufficiently large to enable static classification to take place – none of the phrases spoken in practice appear in the enrolment database. Given the one-to-one verification that takes place (versus a one-to-many) it is not anticipated that the level of security will be affected either positively or negatively, however the transparency and subsequent usability of the approach should improve significantly.

4.3. Signature Recognition

In order to achieve the objective of transparency, a requirement exists to authenticate a user, not based upon their signature (as this would need to be obtained intrusively) but based upon written words a user might scribe using the stylus on the touch-sensitive screen. In essence, it is not signature recognition that is required but handwriting verification.

The move towards dynamic signature classification has assisted in the ability to measure unique characteristics of how a user writes rather than simply the final image. This places less reliance upon the uniqueness of the final signature (and the word in this particular scenario). Therefore, although two written words might appear to look the same (a fairly trivial task) it is highly unlikely there were written in an identical fashion.

Unfortunately, current systems can only deal with simple one-to-one comparisons and in order to achieve transparency, the system would need to be equipped with the ability to verify a user by whichever word they scribed. Implementing a design approach, similar to voice verification, where a database is utilised to index written words during enrolment would assist in providing a dictionary of previously scribed words within which to perform verification.

This approach would also suffer from the same disadvantage as voice, in that a previous sample must be stored in the database for verification to be performed. However, with carefully designed enrolment processes, this problem can be minimised. It will also theoretically not affect the security, however initial prior research undertaken by the authors have already demonstrated good performance of this approach, indeed with it providing better security than when used in its traditional signature recognition mode [12].

4.4. Keystroke Analysis

Keystroke analysis even in a text-dependent mode is one of the weaker forms of biometric authentication, suffering from large variations in typing characteristic leading to worsening levels of security and user inconvenience. Utilising keystroke analysis in text-independent mode has not resulted in performance rates that would be useful in practice. It is therefore necessary to utilise the static (text-dependent) mode of operation and seek to apply current algorithms in a fashion to achieve transparency.

For the transparent use of the technique a similar approaches to the above could be used, by indexing the words typed by the user. Studies in the past have been performed by the authors utilising for reference a number of keywords likely to occur in text messages. The results showed promising results indicating that such approach could be effectively used for achieving transparency [10, 11]. Nevertheless due to the less distinctive nature of keystroke features it is suggested that a large index of words must be utilised and the use of more than one word in each verification in order to further improve the verification decision (as illustrated in **Figure 4**).
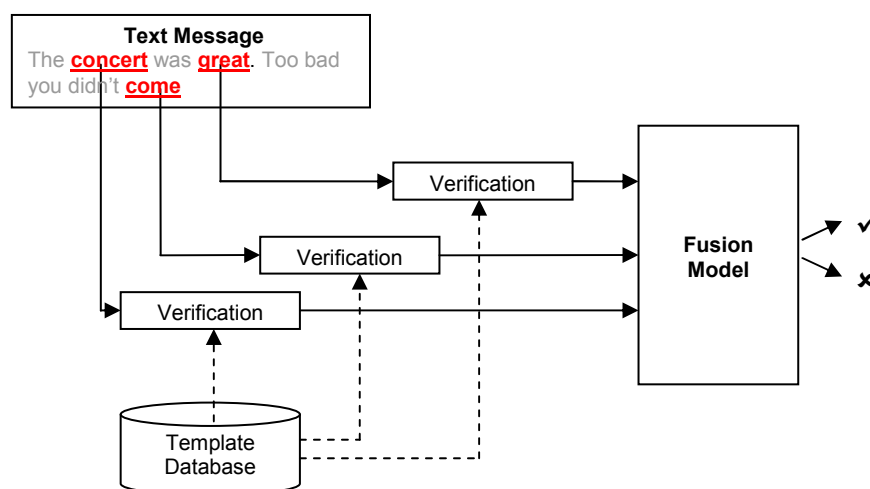

Figure 4. Fusion model for keystroke analysis

The modification proposed to this approach will not negatively affect the security provided, as a one-to-one based verification is still being performed. It should however improve the robustness and importantly achieve transparency.

5. CONCLUSIONS

The changing nature of mobile computing imposes the requirement for enhanced and robust security. Biometrics can address this issue and provide more trust with respect to the user's identity. Furthermore, if implemented correctly they can provide a mechanism to transparently and thus continuously maintain trust of the user.

However, such application is yet restricted due to current implementations and mechanisms have been proposed that focus upon the integration of technology and the use of the more static characteristics. Through the manipulation of security and user convenience, techniques can be applied in a transparent fashion.

Further research is required however to assess to what degree these proposed mechanisms will improve user convenience and importantly at what cost to security.

REFERENCES

[1]   Martin, A. (2005) *Tackling mobile security*, SCMagazine,
        http://scmagazine.com/uk/news/article/520403/tackling-mobile-security

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

[3]   ITWALES (2006) *Mobile security products to be incorporated into handsets by 2011*,
        http://www.itwales.com/997788.htm

[4]   IBG (2007) *Which is the best biometric technology*, International Biometric Group,
        http://www.biometricgroup.com/reports/public/reports/best_biometric.html

[5]   Ashbourn, J. (2000): "Biometrics: Advanced Identity Verification, The Complete Guide",
        Springer, London, UK, 2000

[6]   Yun, W.Y. (2003): "The '123' of Biometric Technology", Information Technology Standards Committee, Available at: http://www.itsc.org.sg/synthesis/2002/biometric.pdf

[7]   Chellappa, R., Wilson, C.L., Sirohey, S. (1994): "Human and Machine Recognition of Faces: A Survey", University of Maryland Computer Vision Laboratory. Available at http://lcv.stat.fsu.edu/research/geometrical_representations_of_faces/PAPERS/face_recognition_survey1.pdf

[8]   Bronstein, A.M., Bronstein, M.M., Kimmel, R. (2003) *Expression-Invariant 3D Face Recognition*, Proceedings of Audio & Video-based Biometric Person Authentication (AVBPA), Lecture Notes in Computer Science, Vol. 2688, Springer, 2003, pp. 62-69

[9]   Gupta, G., McCabe, A. (1997): "A Review of Dynamic Handwritten Signature Verification",James Cook, University, Townsville, Australia

[10]   Clarke, N.L., Furnell, SM. (2006): "Authenticating Mobile Phone Users Using Keystroke Analysis", International Journal of Information Security, pp1-14, 2006

[11]   Karatzouni S, Clarke NL (2007): "Keystroke Analysis for Thumb-based Keyboards on Mobile Devices", Proceedings of the 22nd IFIP International Information Security Conference (IFIP SEC 2007), Sandton, South Africa, 14-16 May, pp. 253-263

[12]   Clarke, N.L., Mekala, A.R. (2006): "Transparent Handwriting Verification for Mobile Devices",
         Proceedings of the Sixth International Network Conference (INC2006), Plymouth, UK, 11-14
         July, pp277-288, 2006

Flexible and Transparent User Authentication for Mobile Devices

Nathan Clarke, Sevasti Karatzouni and Steven Furnell
Centre for Information Security & Network Research, University of
Plymouth, Plymouth, PL4 8AA, United Kingdom, nrg@plymouth.ac.uk
WWW home page: http://www.cisnr.org

Abstract. The mobile device has become a ubiquitous technology that is capable of supporting an increasingly large array of services, applications and information. Given their increasing importance, it is imperative to ensure that such devices are not misused or abused. Unfortunately, a key enabling control to prevent this, user authentication, has not kept up with the advances in device technology. This paper presents the outcomes of a 2 year study that proposes the use of transparent and continuous biometric authentication of the user: providing more comprehensive identity verification; minimizing user inconvenience; and providing security throughout the period of use. A Non-Intrusive and Continuous Authentication (NICA) system is described that maintains a continuous measure of confidence in the identity of the user, removing access to sensitive services and information with low confidence levels and providing automatic access with higher confidence levels. An evaluation of the framework is undertaken from an end-user perspective via a trial involving 27 participants. Whilst the findings raise concerns over education, privacy and intrusiveness, overall 92% of users felt the system offered a more secure environment when compared to existing forms of authentication.

1 Introduction

Recent years have witnessed a considerable increase in the power and capabilities of mobile devices, with the users of today's smartphones and PDAs having access to a far richer range of features and functionality than they enjoyed a few years ago. Although offering a number of clear benefits, this transition poses serious security considerations for mobile users. With the ability to access and store a wide variety of more sensitive information, the need to ensure this information is not misused or abused is imperative. Whereas the replacement cost arising from loss or theft might

previously have been the principal risk associated with mobile devices, unauthorized access to its data could now be a far more significant problem (introducing threats ranging from personal identity theft through to serious corporate loss and increasingly liability).

Given the changing nature of the mobile device and network, it is necessary to consider whether the current authentication on mobile handsets is capable of providing the level of security that is necessary to meet the changing requirements. Even with increasingly large amounts of literature suggesting that secret-knowledge techniques are ineffective (Lemos, 2002; Denning, 1999), the Personal Identification Number (PIN) is still the most widely used approach on mobile devices. The increasing requirement for protection is evidenced by a survey of 230 business professionals, which found that 81% considered the information on their PDA was either somewhat or extremely valuable. As a result, 70% were interested in having a security system for their PDA (Shaw, 2004).

Looking beyond secret-knowledge, two other forms of authentication are available, namely tokens and biometrics. However, only the latter are able to realistically provide more secure mechanisms for user authentication. Tokens rarely authenticate the user, but rather authenticate the presence of the token; with the assumption being the legitimate user is in possession of the token. Moreover, its application within a mobile device context would require a user to remember both the device and token or more commonly simply leave the token in situ within the device (e.g. the use of the SIM card). However, given the evolving nature of mobile devices, simply replacing one authentication mechanism with another is arguably not sufficient. Rather, only through an analysis of the requirements can an effective solution be proposed.

This paper presents the results from a two-year study investigating and proposing a new user authentication approach for mobile devices. The paper begins by presenting the research undertaken to develop and understand the requirements in order to derive the objectives of the system. Section 3 then broadly describes the proposed framework; in particular, focusing upon the key processes that enable security and usability. Section 4 presents the end-user trial of the system, with the final section describing the conclusions and future work.

2   Analysis of stakeholder requirements

In order to establish an understanding of stakeholder requirements, a qualitative and quantitative research methodology was undertaken. Stakeholders were largely divided into two groups: end-users of mobile devices and managers of mobile devices/networks (e.g. network operators, system administrators). It was determined that the end-user group, representing the principle stakeholder group, it would be assessed both qualitatively through a survey and quantitatively through focus-group. It was felt, due to the specialist nature of the other group of stakeholders and getting sufficient access to them, a quantitative focus-group based methodology would be most appropriate. To this end, two activities were undertaken:

1. A survey of end-user attitudes and opinions towards current and future forms of user authentication technologies. A total of 297 participants took part in the survey and complete published results can be found in Clarke & Furnell (2005).
2. A focus group activity involving all stakeholders. A total of 12 participants took part and a series of questions were put forward regarding current authentication and the security requirements of current and future services. In order to maximise the usefulness of the focus group, this activity was devised based upon the analysis and findings of the survey. Detailed information on the focus group and its outcomes can be found in Karatzouni et al. (2007).

In summary, the survey found that 34% of the 297 respondents did not use any PIN security. In addition, even for those respondents who did use the PIN at switch-on only, 85% would leave their handset on for more than 10 hours a day, thereby undermining any security the PIN might provide. Interestingly, however, it would appear that users do have an appreciation of security, with 85% of respondents in favour of additional security for their device.

Within the focus group these findings were not so evident, with the end-user group finding it difficult to understand why such protection was required. Whilst this was somewhat expected given current usage (with most end-users simply using their device for telephony or texting); the few enterprise-level users of devices (using advanced features such as email and corporate network access) that participated in the focus group understood and agreed with the need for better protection. Moreover, once the possible future uses of the mobile devices were explained to end-users (for instance micro-payments and accessing back accounts), they also understood the need for better security. From the other stakeholder groups, it became evident that existing controls were not sufficient, with system administrators particularly concerned regarding the increasing integration of mobile devices within their organisations network and the effective control and management of them.

When taking the feedback into consideration and reflecting upon all the other requirements, such as: varying hardware configurations and processing capabilities of mobile devices; network versus device centric operation; an enormous end-user population of approximately 2.7 billion (GSM Association, 2008); privacy of end-user data (particular biometric based); it became evident that a flexible authentication scheme would be preferable. As no single authentication technique would be suitable for all situations it would be far more appropriate to provide a suite of authentication techniques within an appropriate framework that could provide an overall authentication approach for mobile devices.

From the analysis of stakeholder requirements, it is envisaged that a successful authentication mechanism for mobile devices must address a number of requirements:

- 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 link security to service provision, so that for instance the risk associated with sending a text message and accessing a bank account can be understood and be incorporated with the decision making process ;
- 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.

From these requirements a Non-Intrusive and Continuous Authentication (NICA) system was devised.

3   Non-Intrusive and Continuous Authentication (NICA) for mobile devices

NICA operates by utilising a combination of secret knowledge and biometric techniques within a flexible framework. The framework operates by initially establishing 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 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..

3.1   Proposed Framework

Architecturally this system could take many forms, but it is proposed that a number of key components would be required, such as an ability to capture and authenticate biometric samples, an intelligent controller, administrative capabilities and storage of the biometric profiles and authentication algorithms. Although principally conceived around a client-server topology, the system also has the flexibility of operating in an autonomous mode to ensure security is maintained even during periods with limited or no network connectivity. Figure 1 outlines the functional components of the architecture.

The client-side includes all of the components illustrated in Figure 1 and the server-side architecture includes all but the input and output components (the Data Collection engine, Security Status and Intrusion Interface). The implementation of the architecture will differ depending upon the context that a device is being used within. For instance, in a standalone implementation the device has no use for the Communications Engine – as no network exists to which it can connect. Meanwhile,

in a client-server topology the components 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 NICA differently, such as network bandwidth and availability, centralised storage and processing of the biometric templates, and memory requirements of the mobile device. For example, in order to minimise network traffic, the network administrator may require the host device to authenticate user samples locally, 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.
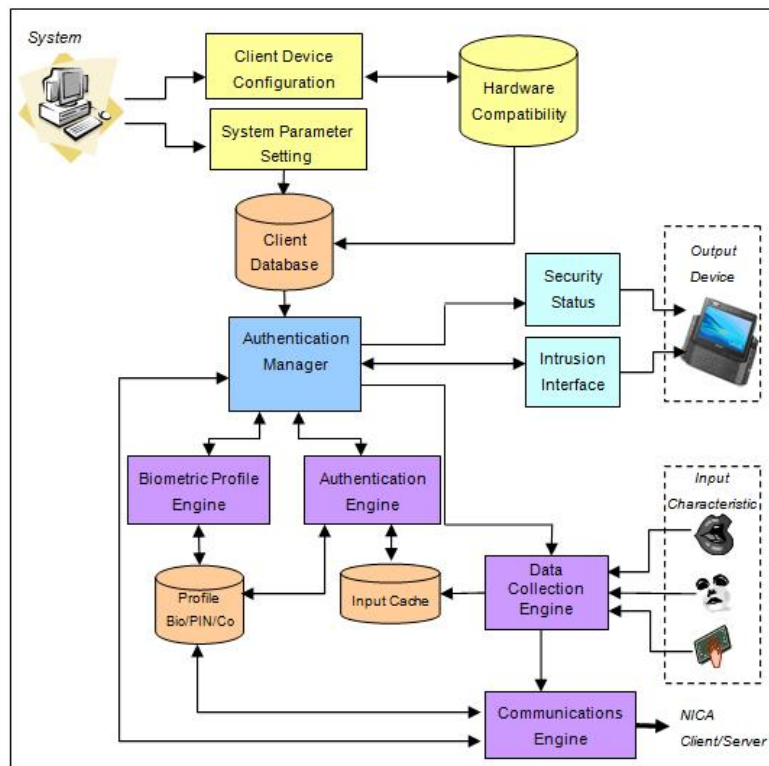

Fig. 1. NICA Architecture

3.2   Security and usability processes

The principal objective of the system is to maintain the level of security required commensurate with the services being provided by the device and to achieve this in a user friendly and convenient fashion. To this end, two key processes operate to ensure this:

- Authentication Confidence Level   • Alert Level

The Authentication Confidence Level (AuCL) process assists in ensuring security through maintaining a continuous level of confidence in the identity of the user. It is a sliding numerical value between -5 and +5 (these values are merely suggestions rather than definitive values), with -5 indicating low security, 0 a normal 'device switch-on' level, and +5 indicating a high security level. The confidence level is modified depending upon the result of authentication requests and the time that has elapsed between them. The magnitude to which the AuCL is modified is dependent upon the authentication technique – recognising that a difference exists between strong biometrics such as face and fingerprints and weaker biometrics such as keystroke analysis. A protection mechanism also exists to ensure a user utilising a weaker biometric is unable to achieve high levels of confidence. This confidence level is then associated with the services and information the device is capable of providing, so that a user who already has sufficient confidence to access a service is automatically provided access. However, should a user request access to a service for which they currently do not have sufficient confidence for, a subsequent intrusive authentication request will be made.

The Alert Level is the second of the key security processes working at the core of this framework. Its purpose is to ensure continuous identity verification of the user in a transparent and therefore convenient fashion. There are six levels (depicted in Table 1) 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 compromise between requiring a good level of user convenience and better security. Through mixing transparent and intrusive authentication requests into a single algorithm it is intended that the majority of authorised users will only experience the transparent stages of the algorithm. The intrusive stages of the algorithm are required to ensure the validity of the user by utilising the stronger authentication tools before finally locking the device from use.

The Alert Level 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 inconvenience from the authorised user perspective. 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 this 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 companion process, the AuCL, 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 than not (even if not consecutively as required by the Alert Level), reducing the AuCL 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. In a practical situation, it is likely an impostor will be able to undertake tasks with a low risk, such

as, a telephone call or sending a text message, for a short period of time before the system locks down. 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.

Table 1. Escalation of the alert level

Alert Level	NICA Authentication action
1	Perform transparent authentication using the most recent data in input cache.
2	Perform transparent authentication using remaining data in input cache.
3	Perform transparent authentication using the next available user input.
4	Issue an intrusive authentication request using a high-confidence method.
5	Issue a further intrusive authentication request using a high-confidence method.
6	Successive authentication failure invokes a system lock.

3.2   NICA prototype

A proof-of-concept prototype was developed in order to assess the effectiveness of the proposed framework. The prototype, based upon the client-server model, comprised of four software systems:

1. Authentication Manager – providing the entire server-side operational functionality, including, biometric profiling, authentication and data synchronization.
2. Administrative Console – containing all the administrative and system settings, and providing a visualisation of active devices and their operational status.
3. Client-Side Interface – providing the simulated mobile handset functionality, data capture and intrusion control.
4. Databases – an SQL server containing all the server-side databases.

The hardware utilised for the prototype included a Samsung Q45 that acted as the Authentication Manager, Console Manager and contained the databases. The nature of these components meant they could be deployed in separate systems. The clients were deployed on a Sony Vaio UX1 and HP Mini-Note 2133 running Microsoft Vista and XP platforms respectively. Whilst these client devices are classed as mobile devices, they do not represent the traditional mobile handset that the framework was devised for. The decision to utilise these platforms over mobile handsets was largely due to development constraints within the timeframe of the funded project – as mobile platform development would have had to been undertaken using unmanaged code in C++, rather than rapid prototyping languages such as Visual Basic.

Having undertaken a thorough examination of biometric technologies and the commercial products that were available, it was determined that few suitable

commercial biometric solutions existed for integration within NICA. The principal reason for this was the lack of available Software Development Kits (SDKs), with vendors preferring to design bespoke solutions for customers rather than license their biometric solutions for development. The project therefore identified some facial and voice verification algorithms developed in MatLab and sought to modify these for use within NICA (Rosa, 2008) These were accompanied by keystroke analysis algorithms previously created by the authors (Clarke and Furnell, 2006). It was considered that these biometric approaches would provide the appropriate variety of transparent and intrusive authentication required for the proof-of-concept.

4   End-user trial of NICA

In order to evaluate the approach, a user trial was conducted that ultimately involved 27 participants. The trial activity was split to two phases:

- *Enrolment Phase:* The participants used the prototype to provide face, voice and keystroke biometric samples that would be subsequently used to create their biometric profiles and also define two cognitive questions. A simple to use and intuitive interface was used to capture the samples. 8 samples for face, 9 for voice and 15 for each cognitive response they gave (which they were asked to provide 2) from which keystroke information was extracted. The enrolment process took no more that 15 minutes per person and at the end the participants were asked to complete the first questionnaire that looked to assess their experience.

- **Usability Phase:** Each participant was asked to follow a series of steps that would force an interaction with the device while the authentication prototype was running on the background. This would enable for biometric samples to be captured transparently as well as force access to services set to be of high security in order to test the operation of the alert level algorithm and the authentication mechanism in general. In order to ensure that the participants would have something to do during the 'usability' phase of the trial, and to ensure that contexts would occur in which different aspects of the prototype could be utilised, each user was asked to work through a given set of tasks such as using Instant Messenger, Microsoft Word, Microsoft Excel and an Internet Browser. The length of this phase varies as each user took different periods of time to interact with the device and complete the tasks. The average time of this phase was 45 minutes and on average over 60 biometric samples were captured from each participant during the usability phase of the trial. After completion of the scenario, the user was asked to fill in a questionnaire assessing their experience and the system.

    After that, the participants were asked to play the role of an impostor on the same device using the profile of another person and through using the same steps see how quickly the system would recognise that they were not the legitimate users.

The results from the evaluation overall demonstrated a positive opinion of the authentication system, with 92% of the users considering that it offered a more secure environment in comparison to traditional forms of authentication. The participants were also asked to evaluate how convenient the system was in a scale of 1 to 5, the results of which appear in Figure 2. Although the responses were mixed, a slight skew towards the system being convenient exists on average. It is worth noting that through observation of the evaluation, participants' opinions were affected by the delays that occurred on the system while trying to manage all the processing. These occurred in some cases where applications might have been initialising concurrently and thus giving extra overhead to the system with NICA running in the background. This was a function of the prototype and a real system would not have such significant delays.
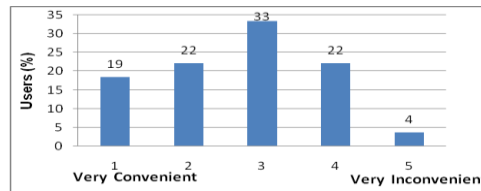
Fig. 2. Perceived convenience of the NICA prototype

Furthermore the above views were also affected by the transparency of the system which was not always ideal. The lack of robust biometric algorithms caused a lot of transparent authentication requests to fail, prompting some of the users to experience more intrusive requests that they would normally get. Unfortunately the biometric techniques being utilised were largely developed in-house due to a lack of availability of commercial algorithms. In order to mitigate the errors a manual trimming of the threshold was taking place during the experiment in order not to allow the lack of accuracy from the biometric algorithms to affect the performance of the actual system. Nevertheless, what also happened in the experiment was that the scenario included access to a number of protected services in a small amount of time causing even more intrusive requests to occur but not necessarily having the chance to build the required confidence in the user while authenticating them transparently. Unfortunately, it was not possible to have the participants use the system for a prolonged period of days, so therefore the experimental study had to artificially include a number of steps to fully evaluate the prototype. It is likely this artificial environment likely resulted in a more negative attitude towards the system than what would have occurred in practice. The responses of the participants with regards to the transparency of the system are illustrated Figure 3.

Fig. 3. Perceived intrusiveness of the new authentication system

With regard to the individual techniques that were utilised, there was a slight preference towards voice verification and keystroke analysis. From verbal feedback from participants there was a strong preference to techniques that did not require much explicit user interaction and were not very time consuming. As such, cognitive responses as an intrusive means of authentication were not very popular. The same occurred with face recognition as the algorit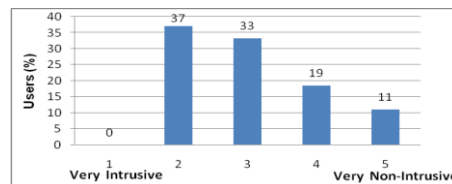hm utilised in the prototype required more time than other techniques to perform the authentication and the user also had to keep facing the camera until a sample was captured. At the same time voice verification (in its intrusive form) appeared to be more preferable as the user only had to repeat a small phrase with a subsequent quick response from the NICA server. Although many of the above were affected by the robustness of the algorithms utilised it still provides an insight that users prefer to have a higher level of security with the least overhead in their interaction. Usability and convenience were stronger preferences than security.

Regardless of the aforementioned problems regarding the convenience of the system, the majority of the users (70%) registered a preference to the use of transparent and continuous authentication as a protection mechanism. Although many of the participants suggested that the requests were too frequent the idea of being constantly protected and specifically having extra security for highly sensitive information was very appealing to them. As such, 81% of the users said that they would use such system in practice as they would feel more protected than using traditional means of authentication. Although the remaining 19% stated they would not use it, their justification was that although they believed the system would offer higher security they do not perceive that their current use of their mobile device actually required a higher level of protection as they do not store or access personal information. This was actually an opinion that had arisen on a number of occasions during discussions with stakeholders. A body of users exist for which the mobile device is only (and will remain only) a telephony-based device. They have no desire to use it for any other purpose and as such do not perceive the need for additional security.

When the evaluation came to the participants acting as impostors it must be noted that although a number of users were not very positive when acting as the authorised user, their opinion became more positive when they saw the performance of the system reacting to an impostor. When the participants were asked whether the system managed to detect them and locked them out in a timely manner, 81% said yes. When the users where asked on how secure the system was their answers were very positive with 86% leaning to being secure or very secure.

5. Conclusions & Future Work

The research has resulted in the development of an operational proof-of-concept prototype, which is not dependent upon specific hardware and is functional across Windows XP and Vista platforms. It is able to operate in both client-server and standalone modes, and has successfully integrated three biometric techniques.

The evaluation of NICA clearly demonstrates the strengths and weaknesses of the proposed system. It is evident from the findings that such a transparent and continuous system has real merit and a large proportion of the participants felt it would provide the additional security they desire for their mobile devices. Unfortunately, with almost half of the world's population having a mobile device, it is difficult to establish an approach that satisfies all users. NICA has specifically considered this and developed a flexible approach that can utilise a variety of biometric and other authentication techniques and through a series of operational settings that can vary the level of security both transparent and intrusive being provided. Through this flexibility it is hoped the majority of users will be able to find a suitable mixture of settings and techniques they prefer and desire.

Whilst the prototype and subsequent evaluation has illustrated a number of key findings, it is important to highlight that if the system was operating within specification (i.e. the performance of the biometric techniques was good and the operational performance of the server was managed rather than everything operating for a single server) the nature of the transparency would mean few users would ever experience intrusive authentication. During the evaluation, however, the framework was configured to perform authentication on a more frequent basis than normal in order to ensure that sufficient judgments were made during the trial session. This was done in order to ensure that participants would see the full extent of the system in operation, but the consequence was that they also encountered more intrusive authentication requests than would normally be expected. In some trial sessions, these requests were too frequent and time consuming, and participants therefore formed a more negative impression of the prototype.

The study has accomplished its overall aims of developing a next generation user authentication system. It has taken into account stakeholder considerations of usability, flexibility and convenience and provided a system that can improve the level of security in a continuous and transparent fashion – moving beyond traditional point-of-entry authentication. Whilst the prototype has a number of operational shortcomings, it is not anticipated that any of these would actually prevent a NICA-type approach from being operationally viable in the future. The project has also identified a host of additional avenues that require further consideration and research. In particular future work will focus upon three aspects:

1. Transparency of biometric techniques – Developing biometric approaches that will not only operate in point-of-entry mode but in a transparent fashion with varying environmental factors.
2. Privacy of biometric samples – the importance of this data is paramount and large adoption of any biometric system will only occur when such issues can be resolved to the satisfaction of all stakeholders.
3. Developing a risk assessment and management strategy for mobile devices. Given the wide-stakeholder group, varying responsibilities from general users to network operators and system administrators, it is imperative that an approach is designed so that the level of risk associated with a particular service request can be better understood and therefore protected.

The authors have already begun to consider the issue of transparency with respect to facial recognition, signature recognition and keystroke analysis (Clarke et al., 2008; Clarke and Mekala, 2007; Clarke and Furnell, 2006) and will continue to address other key biometric approaches.

5 Acknowledgements

6 References

Clarke, N.L., Furnell S.M. (2005) Authentication of Users on Mobile Telephones - A Survey of Attitudes and Practices. Computers & Security, 24, 7, 519-527

Clarke, N.L., Furnell, SM. (2006) Authenticating Mobile Phone Users Using Keystroke Analysis. International Journal of Information Security, pp1-14, 2006

Clarke, N.L., Mekala, A.R. (2006) Transparent Handwriting Verification for Mobile Devices. Proceedings of the Sixth International Network Conference (INC2006), Plymouth, UK, 11-14 July, pp277-288, 2006

Clarke, N.L., Karatzouni, S., Furnell, S.M. (2007) Transparent Facial Recognition for Mobile Devices. Proceedings of the 7th Security Conference, Las Vegas, 2-3rd June 2008.

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

Karatzouni, S., Furnell, S.M., Clarke, N.L., Botha, R.A. (2007) Perceptions of User Authentication on Mobile Devices. Proceedings of the ISOneWorld Conference, Las Vegas, CD-Proceedings (0-9772107-6-6)

GSM World (2008) GSM Subscriber Statistics. GSMWorld.Com, http://www.gsmworld.com/

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

Rosa, L. (2008) Biometric Source Code. Advanced Source Code, http://www.advancedsourcecode.com

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

Towards a Flexible, Multi-Level Security Framework for Mobile Devices

N.L.Clarke, S.Karatzouni and S.M.Furnell

Centre for Information Security & Network Research,
School of Computing, Communications & Electronics, University of Plymouth, Plymouth, United Kingdom

Email: nrg@plymouth.ac.uk

Abstract

The mobile device has become a ubiquitous technology that is capable of supporting an increasingly large array of services, applications and information. Given their increasing importance, it is imperative to ensure that such devices are not misused or abused. Unfortunately, a key enabling control to prevent this, user authentication, has not kept up with the advances in device technology. Although frequently reported as weak and insufficient, Personal Identification Numbers (PINs) are still the predominant form of authentication. Moreover, this form of authentication is point-of-entry only; thus failing to re-establish the authenticity of the user beyond power-on. This paper proposes the use of transparent, continuous biometric authentication of the user: providing more secure identity verification; minimising user inconvenience; and providing security throughout the period of use. It is also recognised that not all services, applications and information have the same security requirements and the paper proposes an approach for establishing what level of security to provide based upon individual services and applications. The *Personal Security Model (PSM)*, *Simple Risk Assessment Model (SRAM)* and *Organisational Risk Assessment Model (ORAM)* are three techniques for establishing the security requirements for individual services and applications based upon the responsible stakeholder (i.e. end-user or organisation) and their associated level of knowledge.

1. Introduction

The mobile networking landscape has changed significantly over the last decade, with a transition from large form factor telephony devices to small multi-purpose multimedia communications devices. The recent introduction of Third Generation (3G) technologies has provided the underlying mechanism for a wide variety of innovative data orientated services, with approximately one million users every day adopting these new features (Best, 2006).

By providing functionality that extends beyond telephony, the mobile device has evolved from being a simple telephone to become a necessity that people utilise every day, for a variety of applications. This level of functionality can be seen to be significantly expanding, with devices today having similar processing and memory capabilities to PCs of a few years ago. Indeed, their combination of portability and capability means that handsets such as smartphones and PDAs are likely to have an increasingly significant role as mobile computing and network access devices.

This transition poses serious security considerations for mobile users. With the ability to access and store a wide variety of more sensitive information, the need to ensure this information is not misused or abused is imperative. Whereas the replacement cost arising from loss or theft might previously have been the principal risk associated with mobile devices, unauthorised access to

its data could now be a far more significant problem (introducing threats ranging from personal identity theft to serious corporate loss and increasingly liability).

Given the changing nature of the mobile device and network, it is necessary to consider whether the current authentication on mobile handsets is capable of providing the level of security that is necessary to meet these requirements. Interestingly, it can be seen that although devices have undergone several generations of improvements in technology and functionality, the mechanism used for providing identity verification has not changed or even been modified. Even with increasingly large amounts of literature suggesting secret-knowledge techniques are ineffective (Lemos, 2002; Denning, 1999), the Personal Identification Number (PIN) is still the most widely used approach on mobile devices.

Looking beyond secret-knowledge, two other forms of authentication are available, namely tokens and biometrics. However, only the latter are able to realistically provide more secure mechanisms for user authentication. Tokens rarely authenticate the user, but rather authenticate the presence of the token; with the assumption being the legitimate user is in possession of the token. However, given the evolving nature of mobile devices, simply replacing one authentication mechanism with another is arguably not sufficient. Rather, only through an analysis of the requirements can an effective solution be proposed. This paper establishes the need for flexible and multi-level security for mobile devices, to meet the demands for all stakeholders (end-users, network operators, system administrators). Section 2 provides an overview of the existing security provision of mobile devices and section 3 introduces the need for multi-level and continuous identity verification. Section 4 proceeds to propose a series of mechanisms for establishing the level of security that should be attributed to different services – moving authentication away from the device and point-of-entry towards continuous verification tied to service and application usage.

2. Current security provision for Mobile Devices

As the range of data and services expands, it is increasingly desirable for users to protect their devices via appropriate authentication methods. The dominant method for achieving this on current devices is the use of 4-8 digit PINs, which can be applied to both the device and the user's Subscriber Identity Module (SIM) - a removable token containing the cryptographic keys required for network authentication.

The PIN is a secret-knowledge authentication approach, and thus relies upon some knowledge that the authorised user has. Unfortunately, such techniques have long-established drawbacks, with weaknesses often being introduced as a result of the authorised users themselves. These are most clearly documented in relation to passwords, with bad practices including the selection of weak (guessable) strings, as well as sharing details with other people, writing them down and never changing them (Lemos, 2002; Morris and Thompson, 1979). A survey assessing authentication and security practices on mobile handsets found that 34% of the 297 respondents did not use any PIN security (Clarke & Furnell, 2005). In addition, even for those respondents who did use the PIN at switch-on only, 85% would leave their handset on for more than 10 hours a day, thereby undermining any security the PIN might provide. Interestingly, however, it would appear that users do have an appreciation of security, with 85% of respondents in favour of additional security for their device. The increasing requirement for protection is further evidenced by a survey of 230 business professionals, which found that 81% considered the information on their PDA was either somewhat or extremely valuable. As a result, 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).

With the aforementioned evolution of mobile device functionality and access, the requirement for additional and/or advanced authentication mechanisms is becoming more apparent. The original specifications for security in third generation (3G) networks identified the importance of authenticating users in the more advanced environment that would be provided. Specifically, it was stated that *"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"* (3GPP, 2001). The reference to performing the authentication *during* service delivery is particularly interesting, and a potential interpretation is to use more advanced techniques that would enable periodic or continuous re-verification of the user. However, it is notable that the introduction of 3G handsets to date has not witnessed any large-scale advancement over previous authentication approaches. Having said this, a small number of operators and handset manufacturers have identified the need to provide alternative authentication mechanisms. For instance, NTT DoCoMo's F505i handset comes equipped with a built-in fingerprint sensor (NTT DoCoMo, 2004). However, although fingerprint technology increases the level of security, the technique remains point-of-entry only and intrusive from the perspective of the user.

3. An Analysis of the Security Requirements on Mobile Devices

Another observation in relation to the current point-of-entry authentication is that it tends to assume that all services, applications and information accessible on the device are of equal value, and do not require any further access control restrictions.   However, it can be argued that different services and data require different security provision.
For example, the protection required by a text message is substantially different to that required by a bank account. Figure 1shows a representation of how current authentication schemes deal with security, keeping a single level of security for all services. Figure 2**Error! Reference source not found.** shows how the threat derived from each service could add another dimension to the way in which the security level is defined. Each service carries a certain risk of misuse, and this ought to be a factor in deciding the appropriate level of security.
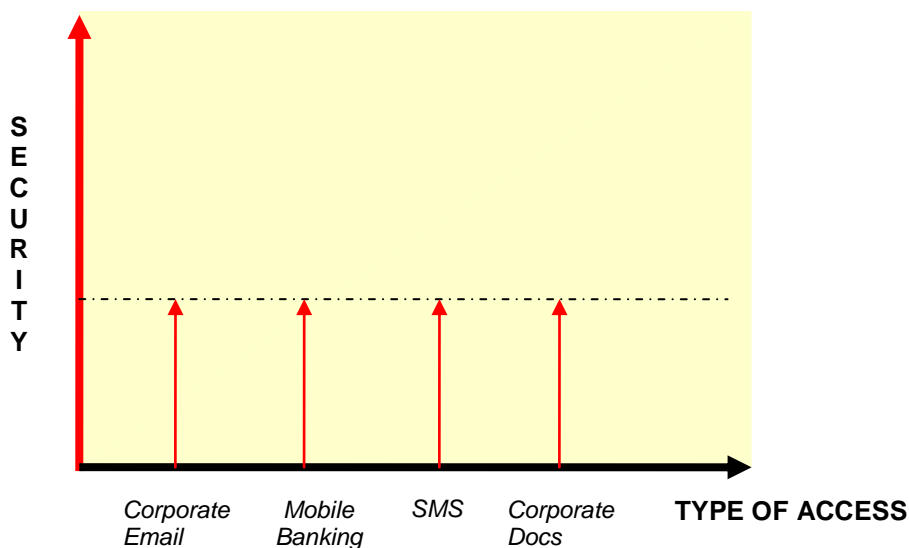
Figure 1: Current Security Assessment
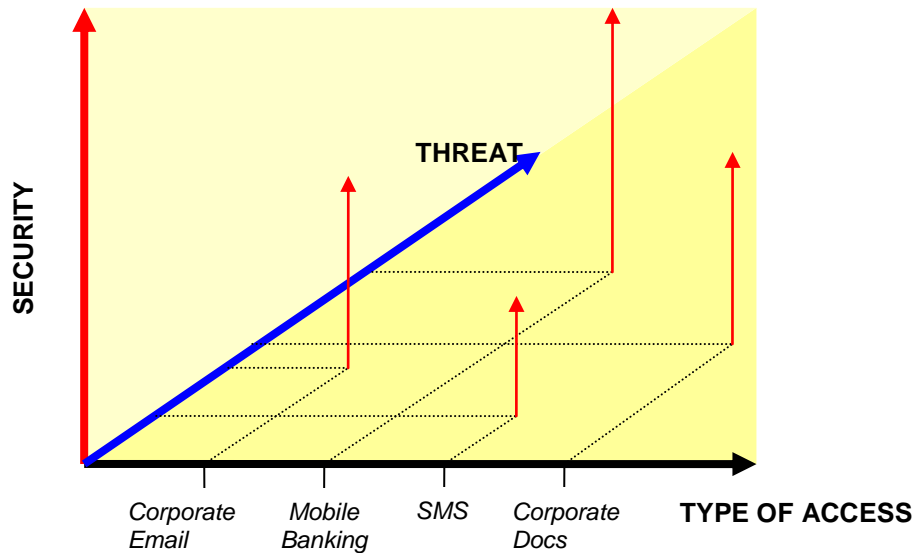
Figure 2: Proposed Security Assessment

The level of security is more appropriately assigned to each service, so that each service or function can independently require a certain level of authentication (and consequently trust in the legitimacy of the user) in order to grant access to the specific service. In this way, more critical operations can be assigned greater protection, leaving less risky operations to a lower level of trust.

It can also be argued that the level of security within a service or application is likely to change during the process, as key stages will have a greater risk associated to them than others. In order to carry out a specific task, a number of discrete steps are involved, which may not carry the same level of sensitivity (i.e. some processes are more critical, whereas others are simply operational steps that assist in the completion of the desired task). A simple example that illustrates this notion is the procedure of accessing an email inbox. The user access the inbox and at that instance there is not a real threat involved as the operation cannot lead to any misuse in its own right (see Figure 3 (a)). Even if the next step is to create a new message and start typing the content, no additional risk exists. However, the security implications actually start when the user is pressing *'Send'* as it is at this point that the adverse impacts from impostor actions would actually begin. By contrast, in Figure 3 (b), the user again accesses the inbox, but tries to access the saved messages instead. This time the requirement for greater protection occurs earlier in the process, as accessing the saved messages could affect confidentiality if an impostor reads them.

(a) Sending a Text Message

(b) Reading & Deleting Text Messages
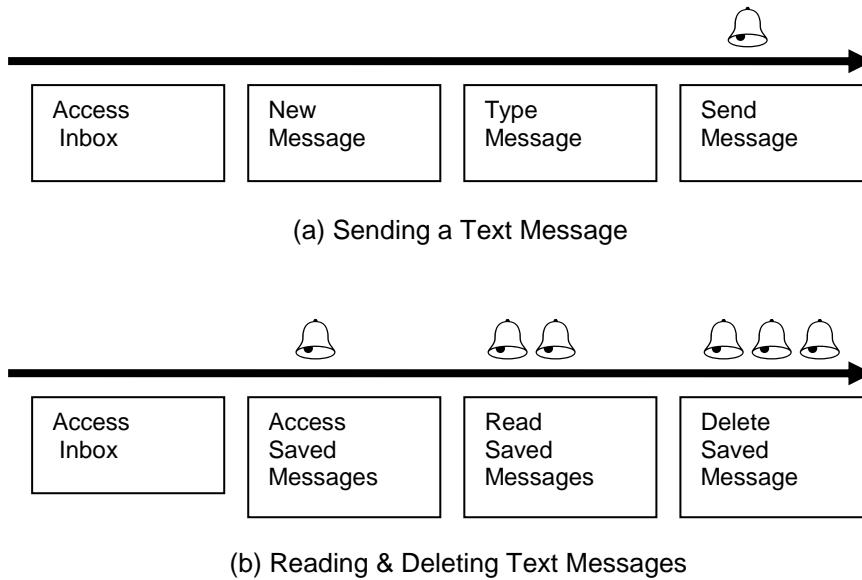
Figure 3: Variation of the security requirements during utilisation of a service

It can be foreseen that each operation has different sensitivities and as such each step of the process changes the threat and therefore the risk level. However, within the context of this paper only the issue of *inter-process security* is addressed, establishing appropriate levels of security for each service and application rather than the device as a whole. *Intra-process security* will be addressed as part of further research.

In order to apply individual security levels to applications and services there is a need for threat assessment to classify the security risks associated with them, from both organisational and individual perspectives. From this classification, a security level could be attributed to each type of service, and subsequently to the level of trust required in the legitimacy of the user.

Within this research a number of usage scenarios were identified based upon current and potential future usage of mobile devices. These scenarios assist in the design of a threat assessment template, examining the security risk that each service encompasses and an associated severity level. A criterion used to classify the different usage scenarios is the way that each service utilises network connectivity. As such the services and functions can be split into those requiring the network, those requiring traditional cellular services, and those that operate locally on the device. This separation also assists in understanding what forms of authentication can be subsequently applied; device-centric or network centric techniques. Table 1 presents a listing of potential services and functions that can be accessed via a mobile device.

Cellular	Non-Network	Network
Voice Call	Contacts	E-mail
SMS	Calendar	Instant Messaging
MMS	Tasks	Data Synchronization
Video Call	Word Processing	Browsing Information
Voice Mail	Camera use	Downloading Web

		Content
Fax	Multimedia access	Ticketing
Push-to-Talk	Data synchronization	Location-based services (Pull)
Conferencing	Control of devices	Video-on-Demand
Value-added services	Business Applications	TV streaming
	Identification Documents	Micro-payments
		E-learning
		E-health
		Business Applications
		Information Services (Pull)
		Adult services
		Gaming
		Gambling
		Electronic Currency
		Voting

Table 1: Examples of Usage Scenarios

The classification of risk for each service and application would change to fit the requirements of each party, whether it is an organisation or an individual. However, it is important to remember that this research is looking for an approach that is usable for all stakeholders – organisations of all sizes and individuals. The complexity of the risk assessment process therefore needs to change depending upon whether it is being completed by a professional within an organisation or a normal member of the public.

4. Risk Analysis for Mobile Devices

In order to determine the level of authentication required for each service, it is appropriate to consider the implications arising from misuse. This in turn requires a means of assessing the risk in a particular context. Risk analysis techniques have been developed and widely utilised by organisations to ensure they take account of the threats and vulnerabilities against their systems. However, rather than consider the full range of risks associated with mobile assets, this paper presents a method for establishing the level of trust required in the identity of the user wishing to access the application or service. It is recognised that mobile devices are often owned by individuals and used to store business data (or vice versa). With this in mind, the required security can be defined by responsibility in one of three ways:

1. The organisation is wholly responsible for the device and all applications, services and business processes that operate on it.
2. The end-user is wholly responsible for the device and all applications and services that operate on it.
3. Both organisation and end-user take partial responsibility for particular applications, services and business processes that operate on it. No specific apportioning of responsibility is assumed.

Similarly to risk assessment, it is the responsibility of the appropriate party (or parties) to define the trust level required for each application, service or business process. What actually needs to be assessed will largely depend upon whether the device is being used for business or personal purposes. For example, it is envisaged that, for personal purposes, the user is likely to utilise the applications and services that are available and provided on the device by the network operator. The range of applications and services will largely depend upon the device, and therefore be fairly static. For business purposes, the range of applications and services operating on the device will include all of the default functionality (similarly to personal users), but also operate a wider range of third party and bespoke applications. It is therefore important to ensure an organisation has the ability to add applications and services.

The level of trust can be established in several ways. Recognising the different requirements of a personal user versus an organisation, the following alternative models are proposed:

- *Personal Security Model (PSM)* to be undertaken by a personal user.
- *Simple Risk Assessment Model (SRAM),* to be undertaken by either the personal user, the organisation, or a combination of both.
- *Organisational Risk Assessment Model (ORAM)*, to be undertaken by organisations incorporating the mobile device functionality into their current risk assessment methodology and tools.

Figure 4 illustrates the 3 models, with an increasing reliance upon formal risk assessment methodologies as one moves towards organisational use.
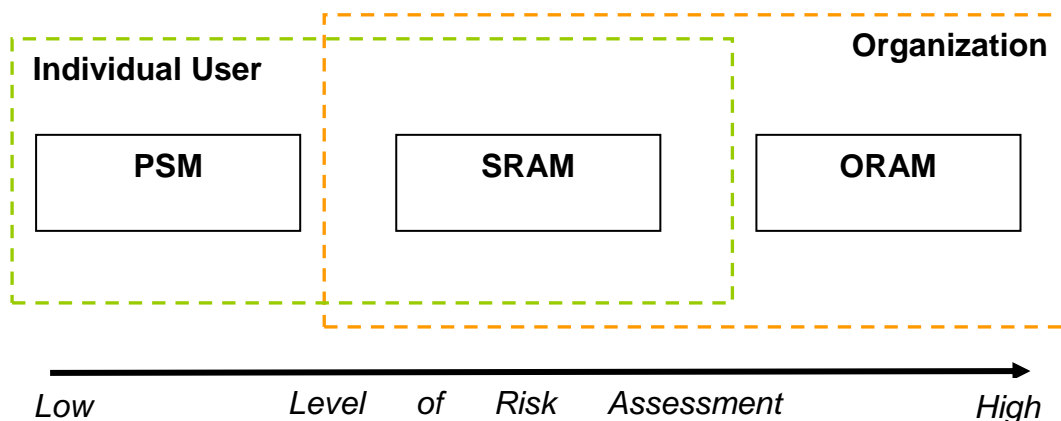
Figure 4: Risk Assessment Models

*Personal Security Model (PSM)***:** Although risk assessment methodologies are traditional tools used by businesses to identify the level of risks, such an approach is not so viable for the end-user. It would place a significant burden upon novice users, as specialist knowledge and procedures are required. The PSM approach offers a simple means of assigning risk to a service or application. Based on the knowledge and also the personal use of the device, an individual user will simply set a risk/security level to each service or application, without any further analytical view of impact. Figure 5 illustrates an example of the PSM model using a low/medium/high rating for attributing the security to each service.

Service	Security Level		
	Low	Medium	High
SMS	✓		
Voice Call	✓		
Video Call		✓	
Email		✓	
Electronic Currency			✓
⋮			

Figure 5: Example of PSM

The type of value that is attributed to each of the services is also left flexible, with further research required to evaluate different approaches. However, as an illustration, potential solutions could include:

- Numeric scale (e.g. 1 (low) to 10 (high))
- Likert scale (e.g. Strongly disagree – Strongly agree)
- Boolean response (e.g. Yes – No)

Recognising that many end-users may not even be willing to go this far in terms of explicitly assessing their own needs, it is also conceivable that a default profile could be established for the standard services on a device, which the user could then tune if inclined to do so (i.e. in a similar manner to aspects such as the security settings in other contexts, such as web browsers).

Simple Risk Assessment Model (SRAM): This model can operate in one of three ways depending upon where the responsibility resides for undertaking the assessment (.i.e. with the personal user, the organisation, or both).

SRAM represents a more focused risk analysis tool than the PSM, useful for more security-aware mobile device users. It follows a risk analysis process, but focuses only upon mobile devices. Personal users who feel PSM does not provide the granularity required in the process will be able to utilise this model and follow a simplified risk analysis process. Organisations not versed in risk analysis, or lacking related expertise, will also be able to follow this model. In addition, taking into account that the responsibility of the device might reside with more than one party, this model also permits the choice of which stakeholder has the responsibility of assigning risk to each service or application.

In order to determine the sensitivity levels, each service can be analysed in terms of the typical consequence that would potentially result from breaches of confidentiality, integrity and availability in each usage context. The consequences considered have been adopted from a standard risk analysis methodology, namely CRAMM (Barber and Davey,1992), and are classified as follows:

- Disruption
- Breach of personal privacy
- Embarrassment

- Financial loss
- Legal liability
- Threat to personal safety

- Breach of commercial
  confidentiality

Figure 6 illustrates the application of the SRAM model. As with the PSM model, the values to be attributed to the services can vary depending upon what is most appropriate to the circumstance.

Service	Commercial confidentiality	Personal privacy	Disruption	Embarrassment	Financial loss	Legal liability	Personal safety
SMS	Low	Low	Low	Low	Low	Low	Low
Voice Call	Low	Low	High	Low	Low	Low	Medium
Video Call	Low	Low	Medium	Low	Medium	Low	Low
Email	High	Medium	High	Medium	Low	Medium	Low
Business Applications	Medium	Low	High	High	Medium	High	Low
Calendar	Low	Medium	Medium	Low	Low	Low	Low
Data synchronization	High	Low	Medium	Medium	Medium	High	Low
⋮							

Figure 6: Example of SRAM

Organisational Risk Assessment Model (ORAM): Many organisations already have formal risk assessment strategies in place, with relevant expertise to conduct them. As such, this final model simply permits them to integrate mobile devices, and the applications and services accessed by them, into their existing risk analysis processes.

The three models can be used independently and assist in providing the flexibility required when dealing with differing stakeholder responsibilities. The rating of each service is completed irrespective of the risk assessment process and therefore each party can use the process that best matches their requirements and ability. As such, even in the case of both the business and the user having a responsibility for the contents of the device, each one will be able to attribute security levels to the services that refer to them.

Although the use of any of these methods introduces a degree of subjectivity into the process (particularly with larger ranges of options) this method is widely utilised and accepted in risk assessment techniques. Therefore, as long as an informed person within the organisation is undertaking the assessment, it will be as good as any other form of risk assessment. This assumption however cannot be made for the personal user, who is likely to have little (if any) experience of risk assessment. It is therefore important that we more carefully define how the end-user will assign values. In order to minimise the subjectivity of responses, it seems prudent to minimise the number of options available to the user, with more clearly defined meanings for each option. Given each personal user will experience a standard list of applications/services on

their device, this additional information regarding the impact of each choice can be built-in to the process by the network operator.

5. Conclusions and Future Work

Enhanced identity verification is imperative to protect today's ubiquitous and powerful mobile devices. Although many advances have been made in handset technology and the networks that support them, little has changed in the way we verify the user's using them. Moreover, it is no longer a matter of simply replacing one point-of-entry authentication approach with a more powerful approach. Instead, a more fundamental understanding of what we use the mobile device for is required so that effective controls can be put in place to protect the assets appropriately.

This paper has argued the need to adopt continuous, multi-level authentication of the user, tied specifically to the services and applications that are used. Possible approaches for establishing the required level of protection (considering both the services and the skills of the stakeholders) have been proposed. This work forms an integral part of on-going research into developing a non-intrusive and continuous authentication architecture for mobile devices. Future work will involve implementing the risk assessment mechanisms and developing an open-source architecture for integrating the enhanced authentication technologies.

References

3GPP. (2001). "3G security; Security threats and requirements". 3GPP TS 21.133, 3rd Generation Partnership Project. http://www.3gpp.org/ftp/Specs/html-info/21133.htm.

Barber, B. and Davey, J. (1992): "The use of the CCTA risk analysis and management methodology CRAMM", Proceedings of MEDINFO92, North Holland, pp. 1589 –1593.

Best, J. (2006). "3G reaches 50 million users worldwide", http://news.cnet.co.uk/mobiles/0,39029678,49251672,00.htm

Clarke NL, Furnell SM. (2005). "Authentication of users on mobile telephones - A survey of attitudes and practices". Computers & Security, vol. 24, no. 7, pp519-527, 2005

Denning, D. (1999) : "Information Warfare and Security", Addison – Wesley, US

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

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

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

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

Appendix C – Briefing and evaluation pack for the user trials

User ID:_____

An Evaluation Study into
Flexible and Transparent User Authentication for Mobile Devices

Introduction

As the capabilities of mobile devices continue to evolve they introduce additional demands in terms of security. An issue that has traditionally been poorly served is user authentication, with the majority of devices relying upon PINs or passwords, which people often find inconvenient and hard to remember. This project has sought to develop technologies to increase the level of security being provided whilst minimising inconvenience.

The purpose of this evaluation is to establish the effectiveness of the technology that has been developed from an end-user perspective.

Study Brief

The study will involve two phases:

1. <u>Enrolment phase</u>: This is a short session where your biometric samples are captured and templates created for use in the main evaluation phase. This should take approximately 20 minutes to complete.
2. <u>Evaluation phase</u>. This is the main evaluation where you will test the usability of the technology by going through a series of scenarios; such as writing a word document, chatting on Instant Messenger and surfing the web. You will be asked to complete a short questionnaire upon completion of this phase. This phase should take approximately 45 minutes to complete.

The whole study should not take more than 1.5 hours to complete from start to finish for which you will receive £15. You will only receive payment upon successful completion of both phases of the study.

Who can take part?

Participants need to have at least a basic understanding of how to use the applications used in the trial task, namely Microsoft Word, Internet Explorer, Windows Messenger and Outlook email.

Right to withdraw

Whilst we value your participation in the study, we appreciate your right to privacy. All biometric data collected for the study will be forensically removed from all mobile devices and computers upon completion of the study (in August 2008). You also have the right to withdraw from the study at any time during the process. Please note that withdrawing your participation will forfeit any payments.

Further information

For further information, or to withdraw from the study, please contact:

Miss Sevasti Karatzouni (skaratzouni@plymouth.ac.uk)

For further information on the study, please visit our website: www.cisnr.org/nica

CONSENT FORM

FACULTY OF TECHNOLOGY

Full title of project:
Flexible and Transparent User Authentication for Mobile Devices

Name of researcher:

Steven Furnell/Nathan Clarke/Sevasti Karatzouni

Please Initial Box

1. I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask questions.

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving reason.

3. I agree to take part in the above study.

_____   _____   _____

Name of Participant   Date   Signature

_____   _____   _____

Name of Researcher   Date   Signature

Phase 1 – Enrolment

The purpose of this phase of the study is to obtain your biometric samples so that templates can be created for use in the main evaluation. In order to achieve this, you will be asked to complete two exercises:

1. Undertake the system's welcome and enrolment session – this will capture a series of voice, face and keystroke samples.
2. Write a series of dialogues in a word document – this will capture additional keystroke samples for use by our keystroke analysis module.

After completion of the first exercise, a short questionnaire will be presented.

Tasks:

1. Your session supervisor will enable the application and provide the device to you. Please follow the instructions. Upon completion, please answer the accompanying questionnaire.
2. Open a word document and type the three cognitive responses you chose in exercise 1 thirty times each.

Thank you for completing phase 1 ☺

Please ensure you book your second session with your session supervisor before you leave!

Phase 1 – Enrolment

Questionnaire

1. On a scale 1-5 (with 1 being easy and 5 being difficult), how difficult did you find the enrolment process overall? (Please circle)

    Very Easy   Very Difficult

    1   2   3   4   5

2. With respect to the individual biometric techniques, how difficult did you find the enrolment process? (On a scale 1-5, with 1 being easy and 5 difficult)

	Very Easy				Very Difficult
Cognitive	1	2	3	4	5
Face	1	2	3	4	5
Voice	1	2	3	4	5

3. Did you find the information provided to you on the screens sufficient to complete the tasks? (Please circle)

    Yes   No

4. Was the enrolment process time consuming?

    Yes   No

5. Would you be happy to complete such an enrolment process as a one-off process when first purchasing a new mobile device?

    Yes   No

6. Are there any other information/comments or experiences you would like to make regarding the enrolment process?

_____
_____

Phase 2 – Evaluation

The purpose of this phase of the study is to determine the usability of the developed prototype from an end-user perspective. To order to achieve this, you will be given a "typical scenario" in which you have to interact with a number of common applications and services whilst the authentication system operates in the background.

In order to facilitate this "typical scenario" you will be working and communicating via the computer with a second participant. After completion of this phase, a questionnaire will be presented asking questions about your experience. You will then be asked to repeat this "typical scenario" but playing the role of an impostor (i.e. in order to see if, and how quickly, the system can detect you!). This will enable us to establish an understanding of both usability and security of the system.

Tasks:

In all cases, where an application is required to start and no information is provided, please navigate to it using voice command.

1. Using *File Explorer* navigate to *My Documents* and open the Word document named *Contacts.doc*

2. Using the contact information, start *MSN Instant Messenger* using the mouse and open a dialogue with the contact you retrieved from *Contacts.doc*.

3. Exchange greetings with the contact and introduce yourself. Spend a couple of minutes discussing what programmes you are studying and what you like (or dislike) about Plymouth.

4. Open *Internet Explorer* and navigate to *Google.* Spend a few minutes looking for various hotels in Las Vegas for 5-10th August 2008. Try and find the 3 cheapest options.

5. Return to *Instant Messenger* and discuss with your contact what you have found. Decide between you which you feel would be the best option.

6. From the *Favourite's* list in *Internet* Explorer, click-on the travel agent link and place the booking information into the form.

7. Using *File Explorer* navigate to *My Documents* and open the Excel document named *Expenses.xls.* Enter the costs of the hotel on this spreadsheet.

8. Create a new Word document. Put a title of Biography and save it to *My Documents.* Now complete a short biography of yourself. No more than 2 or 3 paragraphs that describe your academic and/or professional experiences. You may also include you hobbies and other interests.

9. Open *Outlook* and click on new email. Put "Biography Information" in the subject field and include the email of your contact (you can retrieve this from *Contacts.doc*). Attach your *Biography.doc* to the email and send it.

10. You should also receive a Biography statement from your contact. Open it and review the statement. Check the grammar and spelling and send the edited document back to your contact using email.

Please now complete the following questionnaire

Phase 2 – Evaluation

Usability Questionnaire

1. On a scale 1-5, how intrusive or transparent did you feel the new authentication system was?

Very Intrusive   Very Non-intrusive

     1   2   3   4   5

2. Do you feel the system is providing a more secure environment than traditional/normal forms of authentication?

     Yes   No   Don't Know

3. Did you think the intrusive authentication requests were?

     Easy to use   Difficult to use   Indifferent

4. On a scale 1-5, how convenient did you feel the new authentication system was?

     Very   Very
     Convenient   Inconvenient

     1   2   3   4   5

5. Do you have any preference towards any of the authentication techniques utilised? (Please circle all that apply)

     Face Recognition   Voice Verification   Keystroke Analysis
         Cognitive

6. Do you dislike any of the authentication techniques utilised?

     Face Recognition   Voice Verification   Keystroke Analysis
         Cognitive

7. Was there anything you particularly liked or disliked about the system?

Liked:_____
_____
Disliked:_____
_____

8. Having now experienced transparent and continuous authentication; which of the following authentication systems would you prefer to use in practice? Please tick.

Standard password or PIN

Token-based authentication (e.g. having an access card for the device)

Transparent & Continuous Authentication

None

Other   Please specify:_____

9. Can you explain your response in question 8?

_____
_____
_____

10. Are there any changes or improvements you could suggest?

_____
_____
_____
_____

11. Assuming you required a level of security for your mobile device; would you use such a system in practice?

Yes   No

Any why?

_____
_____
_____

Phase 2 – Evaluation

Impostor Questionnaire

1. Was the system able to identify you were an impostor in a timely manner?

      Yes   No

2. Were you able to access any personal information before the system locked?

No Information   All Information

    1   2   3   4   5

3. How usable did you find the system when acting as an impostor?

Very Un-usable   Very Usable

    1   2   3   4   5

4. Did you feel the system locked you out in a timely manner?

      Yes   No

5. Having now played the role of both authorised user and impostor, how secure do you feel the system is?

Very Secure   Very Insecure

    1   2   3   4   5

6. Any further comments or observations regarding the system?

_____
_____
_____
_____

Thank you for your time!

273

APPENDIX D (Electronic): Code & Full Simulation Results