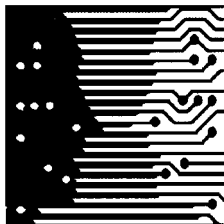


USABLE AUTHENTICATION FOR MOBILE BANKING

By
Ming Ki Chong

Supervised by
Gary Marsden

THESIS PRESENTED FOR THE DEGREE OF MASTER OF SCIENCE
IN THE DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF CAPE TOWN
January 2009



© Copyright 2009

By

Ming Ki Chong

*To my family
and Ndapa*

Abstract

Mobile banking is attractive because it allows people to do banking anytime, anywhere. One of the requirements of performing a mobile banking transaction is that users are required to login before use. The current mobile banking login method is PIN authentication; however, results from other research studies have found that there are usability concerns of using PINs. To overcome some of the concerns, researchers have suggested the use graphical passwords. In this research, we argue that another alternative input technique can be utilized. We explore a novel password input approach, called gesture passwords, of using 3-dimensional discrete gesture motions as password elements. As a result, three systems (PINs, graphical passwords and gesture passwords) were compared.

This dissertation describes the design of two mobile authentication techniques: combinational graphical passwords and gesture passwords. These systems were implemented as prototypes. The prototypes along with a PIN authenticator were evaluated with users. User experience and password retention were evaluated to determine the usability and users' acceptance of each system. Experiments were conducted to evaluate the above. Results from the experiments show that users were able to use all of the testing systems; however, the results reveal that users are more proficient and preferred to use PINs for mobile banking authentication than the other two systems.

Acknowledgements

I would like to express my heartfelt thanks to:

My supervisor

My family

Ndapandula Nakashole

My friends, colleagues and everyone in the post-grad lab

Learn to Earn Khayelitsha Branch (special thanks to Candice Collins and Ncebakazi Vokwana)

WIZZIT Bank (special thanks to Kelvin Chikomo)

Rob Mori of Sun Microsystems for donating the SunSpot equipment

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the NRF.

Table of Contents

Abstract	v
Acknowledgements	vi
1. Introduction	1
1.1. Motivations	2
1.1.1. <i>Usable security</i>	3
1.1.2. <i>Password authentication</i>	4
1.1.3. <i>Memory</i>	4
1.1.4. <i>Perceived trustworthiness and preferences in authentication</i>	5
1.1.5. <i>Context awareness</i>	5
1.1.6. <i>Location</i>	6
1.2. Objectives.....	6
1.3. Organisation of this dissertation.....	7
2. Background	8
2.1. Mobile banking	8
2.1.1. <i>Authentication of mobile banking</i>	9
2.1.2. <i>Issues affecting usability and user performance</i>	10
2.2. Designing for usability and security.....	11
2.2.1. <i>Security needs usability</i>	11
2.2.2. <i>Design goals</i>	12
2.2.3. <i>Usable security needs user-centred design</i>	13
2.2.4. <i>Usable security needs iterative design</i>	14
2.2.5. <i>Authentication interfaces need user-centred interaction design</i>	15
2.3. Trust	16
2.3.1. <i>Defining Trust</i>	16
2.3.2. <i>Initial trust</i>	18
2.3.3. <i>Trust and risk</i>	19
2.3.4. <i>Trust in banking interfaces</i>	20
2.4. Memory	20
2.4.1. <i>How do people remember passwords?</i>	21
2.4.2. <i>Password memorability issues</i>	22
2.4.3. <i>Visual memory</i>	23
2.4.4. <i>Kinesthetic memory</i>	24
2.5. Security threats.....	26
2.6. Authentication schemes.....	27
2.6.1. <i>Biometric-based authentication</i>	29
2.6.2. <i>Token-based authentication</i>	31

2.6.3. Knowledge-based authentication.....	33
2.7. Graphical Authentication	35
2.7.1. Locimetric	35
2.7.2. Drawmetric	38
2.7.3. Cognometric.....	41
2.8. Movement-based authentication	45
2.9. Concluding remarks	45
3. Methodology	47
3.1. Significance of research	47
3.2. Research questions and hypotheses.....	47
3.3. Methods.....	49
3.3.1. Participants.....	49
3.3.2. Procedure.....	50
3.3.3. Understanding users	50
3.3.4. Design and prototypes	52
3.3.5. Evaluation.....	53
3.4. Constraints and anticipated problems	55
4. Understanding Users	57
4.1. Interview results	58
4.1.1. Survey 1: interviews with full-time employed users.....	58
4.1.2. Survey 2: interviews with part-time employed and unemployed users.....	62
4.2. Summary and concluding remarks.....	65
5. Design and Prototypes	67
5.1. Graphical authentication	67
5.1.1. Design	67
5.1.2. Low-fidelity prototype.....	69
5.1.3. High-fidelity prototype.....	71
5.2. Gesture authentication.....	75
5.2.1. Design	75
5.2.2. Low-fidelity prototype.....	77
5.2.3. High-fidelity prototype and implementation.....	78
5.3. Chapter summary	82
6. Evaluation.....	83
6.1. Background	83
6.2. Study 1 – User experience.....	85
6.2.1. Method and procedure.....	86
6.2.2. Results.....	90
6.2.3. Discussion.....	98
6.3. Study 2 – Retention of multiple passwords.....	99

CONTENTS

6.3.1. <i>Method and procedure</i>	100
6.3.2. <i>Results</i>	102
6.3.3. <i>Discussion</i>	106
6.4. Summary and concluding remarks.....	107
7. Conclusion	108
7.1. Research questions	109
7.2. Contributions.....	110
7.3. Future work	110
7.3.1. <i>Experiment participants</i>	110
7.3.2. <i>Biometric movement signatures</i>	111
7.3.3. <i>Beyond mobile phones</i>	111
Appendix A: Understanding Users - Survey Questions	112
Appendix B: Features of Gesture Elements	116
Appendix C: Experiment Questionnaires	119
Appendix D: Experiment Data	130
References	135

List of Figures

Figure 1. A queue of bank clients waiting to use an ATM.....	10
Figure 2. Examples of biometrics. Physiological: (a) DNA, (b) eye iris, (c) facial, (d) fingerprint; Behavioural: (e) signature, (f) speech	28
Figure 3. Biometric verification process.....	30
Figure 4. An ATM with fingerprint verification.....	30
Figure 5. (Left) An image of Octopus card. (Right) A user using an Octopus card for payment.	32
Figure 6. An example of Blonder’s graphical password (Blonder, 1996).....	36
Figure 7. Actual (left) vs. predicted (right) click points (Dirik <i>et al.</i> , 2007).....	36
Figure 8. A user locating a password using a Jiminy template (Renaud & De Angeli, 2004).....	37
Figure 9. Input of a DAS password on a 4x4 grid (Jermyn <i>et al.</i> , 1999).....	38
Figure 10. Hand drawn password (left) and system internal interpretation (right) (Jermyn <i>et al.</i> , 1999)	39
Figure 11. Grid selection (Thorpe & van Oorschot, 2004).....	40
Figure 12. A screenshot of Passfaces demo application (Real User Corporation, 2005).....	42
Figure 13. (a) Interface of VIP1 and VIP2, (b) VIP3 (De Angeli <i>et al.</i> , 2005).....	43
Figure 14. Sample images of Random Art (Bauer, 1998)	44
Figure 15. An example of the standard mobile keypad	69
Figure 16. The paper-based prototype of our graphical authenticator.....	70
Figure 17. A screenshot of the slideshow-based prototype	71
Figure 18. Profile images for the graphical authenticator.....	72
Figure 20. An example of a password entry	73
Figure 19. An example of a user input.....	73
Figure 21. Screen shots of the graphical authentication prototype.....	74
Figure 23. A string of tilt left gestures before adjustment. (a) Initial position, (b) Tilt left from position (a), (c) Tilt left from position (b)	76
Figure 22. Gesture password elements. (a) Forward, (b) Backward, (c) Up, (d) Down, (e) Left, (f) Right, (g) Tilt Left, (h) Tilt Right, (i) Swing Left, (j) Swing Right.....	76
Figure 24. Sun SPOT (Small Programmable Object Technology). Left: a base station (or a transceiver); right: a sensor board.....	78
Figure 25. Connections between components	79
Figure 26. Spatial orientation representation of a mobile phone	81
Figure 27. An acceleration wavelet representation of the “Up” gesture element.....	81
Figure 28. One of the participants getting trained by our facilitator	88
Figure 29. The sewing workshop area	89
Figure 30. Histograms of password entry time.....	92
Figure 31. Mean plot of the password entry time	93

CONTENTS

Figure 32. Histogram of password entry attempts 94
Figure 33. Correctness of passwords after 1 week 103
Figure 34. The results of the Kruskal-Wallis ANOVA by ranks analysis..... 103

List of Tables

Table 1. Significance of differences of user experience between the password systems	95
Table 2. Results of the password entries in Study 1	130
Table 3. Results of the user experience questionnaire	132
Table 4. Results of the context awareness questionnaire.....	132
Table 5. Two-way table of CA4 in Table 3	133
Table 6. Two-way table of CA5 in Table 3	133
Table 7. Results of the trust questionnaire.....	133
Table 8. Two-way table of UT1 in Table 6	133
Table 9. Individual scores of the password retention test in Study 2	134

List of Acronyms

ATM	Automated Teller Machine
GSM	Global System for Mobile communications
HCI	Human-Computer Interaction
M-Banking	Mobile Banking
PDA	Personal Digital Assistant
PIN	Personal Identification Number
RFID	Radio-Frequency Identification
SIM	Subscriber Identity Module
USSD	Unstructured Supplementary Service Data
VIP	Visual Identification Protocol (De Angeli <i>et al.</i> , 2005)
WAP	Wireless Application Protocol

1. Introduction

Mobile banking (also known as m-banking) is the term used for performing banking transactions or accessing financial services via a mobile device such as a mobile phone. It has revolutionized the banking industry with new business models to offer convenient self-service banking options to their customers. With mobile banking, a client may be sitting in the most remote location, but as long as the client has a mobile phone with network connectivity, the client can access his/her account anytime, anywhere.

For a client to use mobile banking, the bank requires the client to register for the service. During registration, the client receives (or provides) a four or five digit Personal Identification Number (PIN) as a password. To access the service, the client is required to enter the correct combination of his/her identification (usually the account number or the mobile number) and the registered PIN to authenticate. Yet, this mechanism is unsatisfactory. The use of a text-based password requires a trade-off between security and memorability; the trade-off arises from the limitation of human memory, and, as a result, passwords are easily forgotten.

To avoid the risk of forgetting passwords, users often adopt insecure behaviours, such as writing down their passwords and storing them in an insecure location or disclosing their passwords to perceived trusted parties (Adams & Sasse, 1999). Users adopt such insecure behaviours because they lack security awareness; and they often construct their own inaccurate model of possible security threats (Adams & Sasse, 1999). As a result, users neglect the importance of practising correct security habits. Weirich & Sasse (2001) conducted a study to understand the factors influencing peoples' security behaviours. Their findings show that peoples' misbehaviours are often caused by negligence and ignorance. To force users to adopt the correct behaviour, they suggest organizations use the *fear appeals* approach (a method of persuasion by frightening people to comply with a particular message by describing its negative outcomes if the message was not obeyed) to persuade users in training and online support. Although providing security education could increase users' security awareness, however, it does not improve the usability of a security system. At the same time, this approach increases the load on the users; instead of

educating users about system security, it is more important to build a system with usable security.

In the search towards a usable security solution for mobile banking, in this dissertation, we are particularly interested in exploring the usability of password systems for authentication using mobile phones.

1.1. Motivations

System security is often considered to be a technical issue. However, at the forefront of a security system lays the user authentication; when users are involved, security is more than technical: it needs to be practical and usable. The goal of security is to build systems that are not only theoretically, but also actually, secure (Tognazzini, 2005). Security is only achieved by means of a partnership between the user and the technology (Renaud & De Angeli, 2004), and mechanisms have to be used correctly by the users of the system to achieve the protection intended by the security designer.

Unfortunately, users are considered as the weakest link in the security chain (Schneier, 2000), and users are often blamed for the failure of a security system. User failures occur in a system when the users cannot comply with the behaviours required by the security system. Sasse & Flechais (2005) identified two reasons why users fail to show the required behaviour: users do not want to behave in the way required; users are unable to behave as required. Take password authentication, for example; password policies are often restraining and generating passwords that are difficult to remember and consequently, this results in people writing down or sharing passwords to avoid losing the passwords. Security policies that increase the loads on users' memory or require extra effort from users are bounded to suffer from one (or both) of the reasons pointed out by Sasse & Flechais. Although system designers can argue that users are at fault for not complying with the security policies, but, in the end, it is the system that is paying the price of having a service that cannot be used by its users. When users fail to comply with security policies, it is not a failure of the users, but a usability failure of the system.

1.1.1. Usable security

Security design has therefore two aspects; the technological and the usability aspects. In the past, the technological aspect had received a lot of attention; whilst, the usability aspect was almost entirely neglected. Security systems are often not designed with users' needs and users' limitations in mind. Although the goal of a security system is to have mechanisms to protect the system, it is also important that the mechanisms are usable by the legitimate users. While security and usability are often seen as competing (or conflicting) design goals (Sasse & Flechais, 2005), in some cases, the burden on the user can be lessened while the system security remains the same. For example, password systems such as Déjà Vu (Dhamija & Perrig, 2000) and VIP (De Angeli, Coventry, Johnson, & Renaud, 2005) use graphical images for authentication – the technique based on one of the heuristics of user interface design, *recognition rather than recall* (Nielsen, 2005) – to reduce the loads on users' memory while the security remains the same (more on graphical authentication is discussed in Chapter 2).

Although traditionally research in security was viewed as primarily relating to theoretical and technical issues, in recent years, usable security has become a growing field of research, specifically, in the HCI domain (e.g. the workshop on HCI and Security Systems at CHI 2003 (Patrick, Long, & Flinn, 2003); Security user studies: methodologies and best practices at CHI 2007 (Egelman, King, Miller, Ragouzis, & Shehan, 2007); the Symposium On Usable Privacy and Security¹). Adams & Sasse (1999) and Whitten & Tygar (1999) have been influential and generated debates in the research field of usable security; their studies are only the beginning of usable security investigations. More research is needed to understand limitations, needs, and requirements, of the human factors in security systems (Renaud & De Angeli, 2004), especially on mobile devices.

¹ Symposium On Usable Privacy and Security: <http://cups.cs.cmu.edu/soups/index.html>

1.1.2. Password authentication

Authentication refers to the process of confirming or denying an individual's claimed identity (Jansen, 2003, p2).

Currently, the most prevalent form of individual verification is password authentication. Arguably, almost every participant of information systems uses passwords (Tari, Ozok, & Holden, 2006). Although it is the most widely used security mechanism, it has drawbacks from a usability standpoint. Some of the problems with passwords are well known: users select weak passwords that are easy to guess (Adams & Sasse, 1999; Yan, Blackwell, Anderson, & Grant, 2004; De Angeli *et al.*, 2005); ones that are susceptible to dictionary attacks (Yan *et al.*, 2004); users often leave their passwords as the system default or an empty password (Bishop, 2006); and so on. Users are not inherently motivated to adopt secure password behaviour (Adams & Sasse, 1999); when users failed to choose and manage password securely, the systems are bound to open loopholes that attackers can exploit (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005a). As a result, the challenge arises as to how to make password authentication usable and secure; At the same time, it must be effective; passwords must be easy to remember, yet hard to guess (Bishop, 2006). In other words, the second challenge arises as how to make passwords strong and memorable.

1.1.3. Memory

Human memory has a limited capacity to remember the arbitrary text and number strings that make up a password. People regularly forget their passwords. The *Power Law of Forgetting* describes how rapidly people forget almost immediately after learning, followed by a gradual decay thereafter (Bahrick, 1984 cited in Wiedenbeck *et al.*, 2005b). This implies people may not recall their passwords correctly after a long period (Sasse *et al.*, 2001), and results in password retention deficiency. To overcome this deficiency, people select passwords to which they can attach meaning.

Studies in cognitive psychology have shown that people's ability to recognize pictures is far superior to their ability of recalling words (Paivio, Rogers, & Smythe, 1968; Nelson, Reed, & Walling, 1976). Graphical authentication researchers have exploited this concept in an attempt to

replace text-based passwords with pictures to improve password memorability. Although research has suggested numerous methods for graphical authentication, most of the research solutions are designed for desktop computers that have a large display. A few studies on graphical authentication for mobile devices have been investigated. For example, Jansen *et al.* (2003) have reported a visual login technique for mobile devices; however, their solution was designed for handheld devices such as Personal Digital Assistants (PDAs), which are not suitable for standard mobile phones that have a small display screen.

Previous studies on graphical authentication have shown that using visual aids can help users to encode passwords into their long-term memory, but there are other retention approaches that can be exploited to increase password memorability; kinesthetic memory (or muscle memory) is a one of those approaches. Instead of using text-characters or images, a password can be made up of multiple gestures. Through practice, the password movements can gradually consolidate into the user's memory. However, we have been unable to find any research investigating how kinesthetic memory can assist users in remembering passwords.

1.1.4. Perceived trustworthiness and preferences in authentication

One aspect of usable security not covered any study we could find, was an investigation into the users' perception of trustworthiness of the systems being evaluated. Currently, password authentication is the most commonly used verification scheme and users have adapted to use passwords for authentication. Although alternatives, such as graphical passwords, have been proven to be more usable, it is arguable that users may prefer to use text-based passwords from the standpoint of familiarity. Therefore, investigation of perceived trust and preferences between password systems is essential.

1.1.5. Context awareness

Users' behaviour of using authentication systems can be influenced by the physical environment and context in which the systems are used (Sasse *et al.*, 2001). Users are aware of security threats when the physical security level is low (Adams & Sasse, 1999). Furthermore, if the physical environment has obvious flaws, users may feel password protection is meaningless because they feel anyone can gain access (Adams & Sasse, 1999). Although, in the case of m-banking

authentication, we are safe to assume users are most likely to login in a private area, we could find no research done to investigate users' perception of logging into their m-banking account in a public area. Since m-banking is location independent, it is important to understand if users would feel free to use the system in a public environment.

1.1.6. Location

Mobile banking has been predicted to change the way how people bank in the developing world (Ivantury & Pickens, 2006). There are numerous developing countries offering mobile banking, but only a handful of them are successful. South Africa, one of the successful countries, is currently seeing a huge uptake of mobile banking (Kayle, 2008). Although mobile banking in South Africa is deemed as a success, many South Africans (especially people from the low-income sector) still have negative perceptions about mobile banking (Ivantury & Pickens, 2006). Research by Ivantury & Pickens identified that "mobile banking providers must find the right balance between human interaction and technology to appeal to more low-income customers." (2006, p.8). In an attempt to improve mobile banking technology in South Africa, we select South Africa as the primary location of this research.

1.2. Objectives

The aims of our research are threefold:

1. We first needed to understand the adoption, and potential adoption, of mobile banking, specifically in South Africa. This can help us understand the potential of people using remote authentication via their mobile phones. For this, we conduct surveys with people who have incomes and qualify for mobile banking.
2. Next, we aim to design authentication systems for mobile devices. The focus is to design usable password authentication systems and to exploit alternative memory systems that can help users store passwords in their long-term memory.
3. Finally, we want to determine the usability of the designed systems through prototypes, empirical studies, and evaluations.

1.3. Organisation of this dissertation

This thesis is organized into the following chapters. Chapter 2 outlines the background literature used in formulating our research, as well as the previous investigation in usable authentication. The methodology adopted for this research is explained in Chapter 3. Chapter 4 presents the results of a survey which aims to understand users' habit of use of mobile phones. This is followed by Chapter 5 that introduces two new authentication systems for mobile devices. Analysis of the designs along with its results and discussions are presented in Chapter 6. Finally, the main conclusions from this research and the discussion of future work are presented in Chapter 7.

2. Background

In this chapter, we review and evaluate the existing literature regarding the issues of building usable authentication for mobile banking. The headings described in this chapter are based on the topics established in the motivations section in the introduction chapter.

2.1. Mobile banking

According to GSM association, there are over 3.6 billion GSM subscribers in the world in the second quarter of 2008 (GSM Association, 2008a), and 1.2 million new connections everyday (GSM Association, 2008b). With such a rapid growth in mobile usage, the number of subscribers is predicted to exceed 4 billion by the first quarter of 2010 (GSM Association, 2008b), or possibly earlier. Currently (2008) in South Africa alone, the mobile penetration rate has reached up to 83% (Integrat, 2008). With such a high adoption, many entities are focused on providing services via the mobile channel.

Financial services, especially mobile banking services, are amongst those being focused on. At the moment, there are more people with access to a mobile phone than with access to a bank account across the developing world (Porteous, 2006). There is a high potential for using the mobile channel to bank the “unbanked”. In 2007, GSM Association launched the Mobile Money Transfer programme with the aim to make remittance services easier for migrant workers and to mobilize financial services for the “unbanked” (GSM Association, 2007). With the expanding potential, mobile banking is predicted to revolutionize the way people do banking in developing countries (Ivantury & Pickens, 2006).

So far, there are a handful of banks and businesses that provide mobile banking services in developing countries. Among them, the successful groups are from the Philippines, Kenya, and South Africa. Globe Telecom’s GCash from the Philippines and Safaricom’s M-PESA from Kenya use a text-based SIM Application Toolkit implementation to provide their services; Wizzit and FNB from South Africa also use text-based implementation, but their services are offered through the USSD (Unstructured Supplementary Service Data) channel; whilst, Nedbank

and Standard bank from South Africa offer their services through WAP (Wireless Application Protocol) technology and .mobi² sites. Whilst they use different implementations, there are commonalities across all platforms, and one of those commonalities is authentication.

2.1.1. Authentication of mobile banking

Although mobile banking services are offered through different platforms or implementations, nevertheless, the underlying services remain the same. Regardless of the platform, all implementations use the same login method, PIN authentication. Before conducting a transaction, a client is required to login with a PIN (some systems may also require their users to input a valid identification), and only a valid PIN code will grant the client access to the service.

In general, a bank account can be accessed via more than one route. Besides mobile banking, bank clients can access their account through an ATM (requires a bank card and an ATM PIN), internet banking (requires a user identification, a PIN or password, and some implementations require a one-time password), and mobile banking. Yet all these channels do not apply the same technique for authentication. Future, some banks require their clients to remember multiple passwords (or PINs) for the same account, each password for a different channel. Banks adopted this approach for safety reasons; if a password of a channel is compromised, then at least the other channels will still be safe because they use different passwords. Although this increases system security, it only benefits the administrator at the bank; from a user's perspective, remembering multiple passwords for the same account is chaotic (Adams & Sasse, 1999).

There are not many studies that had investigated the topic of usable logins for mobile systems. Nevertheless, the concept of usability of authentication is similar across different devices, such as ATMs (De Angeli *et al.*, 2005; Moncur & Leplâtre, 2007) and personal computers (Brostoff & Sasse, 2000; Renaud & De Angeli, 2004; Wiedenbeck *et al.*, 2005). Since the concepts are

² .mobi (or dotMobi) is a top-level domain dedicated to deliver the optimized internet for viewing on a mobile device. It is managed by mTLD global registry- <http://mtld.mobi/>.

closely related, the discoveries from the previous studies of usable authentication can be applied into the topic of finding usable authentication for mobile banking.

2.1.2. Issues affecting usability and user performance

As previously mentioned in the introduction chapter, physical locations and the environment of use affect users' perception of security threats. To elaborate further on this point, Ashbourn (2000) identifies the following issues that could affect users' overall performance when using an authentication mechanism: *Public and private milieus, the presence of a queue, time pressure, and environmental conditions.*

The presence of a queue may affect users' mental state; as the users may worry about how they appear to others, and the users may feel nervous when they are being watched by others (Sasse *et al.*, 2001). However, this issue does not apply to mobile banking. Unlike ATMs at popular locations where people queue for access (see Figure 0 for example), mobile banking allows users to execute transactions with their own equipment and their choice of location, at the users' own comfort.

The time pressure issue is also not relevant. Since transactions can be executed at anytime, anywhere, users are not required to spend time to travel a distance to access their bank accounts.



Figure 0. A queue of bank clients waiting to use an ATM

This means users have more time to execute transactions. On the other hand, the time pressure can still manifest if the transaction or the connection is time-consuming, as slow transaction speeds can frustrate users.

The issue of environmental conditions is important. People find complacency in strong physical secure surroundings (Sasse *et al.*, 2001). Conversely, if the surroundings have obvious flaws, people may feel vulnerable to being observed.

Besides environment issues, Ashbourn (2000) also identifies that the criticality of a transaction can affect user stress levels and potentially impacts user performance. For instance, if a client has to transfer a large sum of money, the user proceeds with the transaction with extra care leading to an increase in user pressure.

Although some of the issues mentioned above may seem trivial, however, the critical issues must be considered for designing a usable mobile banking solution.

2.2. Designing for usability and security

The topic of usability in security systems was briefly introduced in the previous chapter. In this section, we examine this topic in detail.

2.2.1. Security needs usability

Before the discussion of usable security begins, the idea of why usability is needed in security systems should first be examined. Imagine the following scenario: a system engineer was given the task to design a system with foolproof security mechanisms without the need of usability consideration. With such a specification, perhaps the best design is to switch off the system, lock it in a titanium vault, and throw away the key forever. This way, the system guarantees security; however, it is inaccessible and not usable at all. Although this example is excessively extreme, the argument remains the same for all security systems. If a security system was designed without considering usability, the end result is just as good as not having a system, because the system is most likely would not be used by anyone. For instance, a password system can easily require its users to remember random passwords that are over fifty characters long.

Theoretically, it is very secure; however, people have problems remembering text without meanings due to memory limits. Unless the user has photographic memory, the immediate reaction of everyone would be to write down the passwords and storing them in an accessible location, which is as good as not having the password protection

Security mechanisms cannot be effective without taking into account of the users (Wiedenbeck *et al.*, 2005b). At the end of the day, most pieces of software ultimately have a human user; therefore, attention to usability is always necessary to achieve true security (Yee, 2006).

Although usability is vital, overcompensating security for usability would also lead to downfalls. If the design of a system focuses solely on usability without much consideration of security, then the system becomes extremely vulnerable. For example, a network system without password authentication is usable, but not very secure. As a result, it is important to consider the balance of security and usability; with either one neglected can render a product useless (Yee, 2004).

2.2.2. Design goals

Traditionally, the primary interest of security research evolved on its technical and theoretical aspects, which has mainly focused on assuring the correctness of security systems. However, the fundamental problems about security are no longer about the technology, but instead they are about how the technology is used (Schneier, 2000). In recent years, the topic of usable security (or HCISec³) has raised awareness in both the security and the HCI research domains. Researchers and software designers have begun to realize a system designed with strong protection mechanisms is not enough; the system also needs to be manageable by users. Consequently, a new challenge arises as how to create systems that are not only security secure, but also usable and as well as useful.

³ HCISec is the term used for the study of HCI integrates with the study of information security. Its aim is to enhance usability of security in end-user applications.

In usable security, security is about restricting access to prevent undesirable effects, while usability is about improving access to produce desired effects (Yee, 2006). However, the design goals of security and usability conflict with each other (Sasse & Flechais, 2005; Sasse *et al.*, 2001). This is often seen as the case because many systems require tremendous effort from their users to cooperate with the security mechanisms. Yee (2004) argues that conflicts between the two goals can often be avoided if a different approach of the security design process was taken. Both, security and usability goals must be incorporated throughout the process, and they must be viewed as a common goal: fulfilling users' expectations (Yee, 2004). Therefore, the methodology used for designing the solution must aim to fulfil users' expectations.

2.2.3. Usable security needs user-centred design

From a security standpoint, the aims of a secure system are to eliminate illegitimate users from gaining entry and protecting users' possessions from being accessed (or altered) by others. For a system to protect its users' interest, the defence mechanisms must be implemented correctly and act consistent to what its users expect (Yee, 2006). The consistency is needed for the users to understand the system and to consider the system as secure. Therefore, designing for security systems requires an understanding of the users' mental model, i.e. the users' interpretation of how the system works, (Yee, 2006). Smetters and Grinter (2002) elaborate this concept: improving usability of security technology is only one part of the problem, what is missed is designing usable systems that provide security to the end-users in terms of what the users expected, required, and wanted. (Smetters & Grinter, 2002).

Attempting to add usability onto existing security technology is bound to be unsuccessful; instead, new security technologies need to be designed from bottom-up with the users in mind (Smetters & Grinter, 2002). Hence, the design methodologies should shift the spotlight away from traditional security design; instead they should focus around the question: "*if you put usability first, how much security can you get?*" (Smetters & Grinter, 2002, p82).

When users use a system, they do not focus on security, but rather on activity with goals (Renaud, 2005), so from the users' point of view, the main goals are at the centre of usability (Singh *et al.*, 2007). In other words, security goals should be integrated into users' normal

2. BACKGROUND

workflow to yield *implicit security* (Smetters & Grinter, 2002 cited in Yee, 2006), hence a shifting of emphasis from the system to the users. Therefore, usability-centred (or user-centred) security design is needed. Unfortunately, system security is one of last areas in information technology in which user-centred design is considered important (Adams & Sasse, 1999). Nevertheless, in the past ten years, HCI has shed some light on the research area of user-centred security design.

The lack of user-centred design in security mechanisms is the result of insufficient communication with users (Adams & Sasse, 1999). Smetters and Grinter (2002) recommend that instead of building and integrating usability into security systems as an afterthought, the underlying security technology must be changed and redesigned from the beginning with the users in mind. This allows designers to understand the users' requirements from an early stage and deliver systems that are compatible with the requirements (Smetters & Grinter, 2002).

Old technology is bound to be replaced; redesigning underlying technology can be applied to systems with obsolete security mechanisms. In such a case, user-centred design methodologies can be employed, and users should be involved throughout the process. However, redesigning the underlying technology requires tremendous amount of work. In cases where the underlying technology cannot be changed, usability and security mechanisms can only be applied as additions. Although this contradicts with the suggestions given by Smetters and Grinter, in reality, core systems often cannot be modified; therefore, unless the existing system contains major flaws or requires to be replaced by a newer version, else, the cheapest alternative approach for improvement is through patches.

Some security mechanisms, such as user authentication interfaces, can be considered as standalone modules. Those individual mechanisms can be designed independently from the entity. Once they are completed, those modules can be integrated into the whole system.

2.2.4. Usable security needs iterative design

Security systems that are designed using the conventional linear software development model, the waterfall model, are likely to experience usability failure. This happens because users and

designers lack communication during the process. Once the design process moves past the first step, requirement specification, users are not involved for the rest of the procedures. This means users and designers do not communicate well. Since users' expectations change frequently, without good communication with the users throughout the design process, designers would not fully understand the users' needs; therefore the designers cannot deliver a solution that conforms to the users' expectations. For this reason, designing security systems requires a discipline that allows the designers to intercommunicate ideas with the users. Iterative design is the suitable process for such a requirement. Both security and usability communities have advocated iterative design processes rather than linear processes (Yee, 2004). Given that users are involved since inception to completion, security and usability can be examined early and throughout the process. Iterative development processes based on repeated analysis, design, and evaluation cycles, offers the opportunity for designers to see how security and usability decisions affect each other (Yee, 2004); the effect can be seen as early as during the first cycle.

In addition, some systems have rapid changing requirements because of new demands. The technologies of these systems often require updates; iterative design is applicable for those systems, as each cycle produces a new solution that conforms to the new requirements.

2.2.5. Authentication interfaces need user-centred interaction design

Every authentication mechanism requires user interactions. When designing an authentication mechanism, the process should be considered as designing a user interface. However, unlike designing for an entire system, where requirements often change due to new demands, the requirements of a user interface are more static. Once an interface solution is found, the solution is likely to remain the same, at least for a long time. This is understandable because people take time to adjust, so they would prefer not to switch to another unfamiliar interface. Therefore, instead of applying the iterative design model that produces rapid changing solutions, a discipline for designing a single static user interface is needed.

When designing an interface, the aim is to design for good user experience. User experience is how users feel about a product and the pleasure and satisfaction of using it, looking at it, holding it, etc. (Sharp, Rogers & Preece; 2007). Every product used by someone has a user experience.

The overall impression is achieved when users find the product is useful. Nevertheless, an authentication mechanism is a product; users find good experience from its ease of use to achieve a goal, e.g. a successful login. Therefore, aiming for a good user experience is essential when designing an authentication mechanism.

In the case of designing an authentication interface, the aims of providing a good user experience are to increase accuracy and efficiency of user verification and to reduce the possibility of frustration during logins. The design process requires a method that defines an interface that behaves in ways users find intuitive. For this purpose, interaction design is a suitable discipline. Interaction design attempts to improve the usability and the user experience of a product by first researching into users' needs and then designing a solution to meet those needs. As a result, user-centred interaction design is most suitable for designing usable authentication.

Yee (2006) suggests a list of design guidelines for secure interaction design based on the aspects of controlling authorization and communicating with the users. In addition, Yee also introduced two strategies describing ways to design security software, through security by admonition and security by designation. However, the details of each of those guidelines and strategies are outside the scope of this thesis, and will not be addressed.

2.3. Trust

The concept of trust has been studied for many years across different fields, such as psychology, sociology, ethics, HCI, etc. Each field has its own interpretation of trust and its own theories of the concept. In this thesis, we are interested in how a user's trust in an application can affect his/her perception of the application.

2.3.1. Defining Trust

In many publications, trust is introduced as a rationalization of belief using incomplete evidence presented in a situation. Trust is a sentiment; it is subjective, and it varies from person to person. Different people have different views on trust. Everyone has to be an expert on trust, at least at

2. BACKGROUND

the level of interpreting trust in their own way. For this reason, it is very difficult to define trust in a general way that fits all contexts.

One of the most widely accepted definition of trust is proposed by Deutsch (1962, p. 303):

(a) The individual is confronted with an ambiguous path, a path that can lead to an event perceived to be beneficial (Va^+) or to an event perceived to be harmful (Va^-);

(b) He perceives that the occurrence of Va^+ or Va^- is contingent on the behaviours of another person; and

(c) He perceives the strength of Va^+ to be greater than the strength of Va^- . If he chooses to take an ambiguous path with such properties, he makes a trusting choice; if he chooses not to take the path, he makes a distrustful choice.

Using Deutsch's definition above, trust is interpreted as a perception that happens in situations where uncertainties are involved while multiple options are available; a negative, or a positive, outcome could arise depending on the option selected.

On the other hand, from a psychology view point, trust is interpreted not as an individual's choices, but as a psychological condition. An individual can use this condition to reason his/her action to take risk and accept vulnerabilities based upon his expectation of the trustee. This interpretation is defined as a general definition by Rousseau *et al.* (1998, p. 395) as:

Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another.

By merging the definitions by Deutsch and Rousseau *et al.*, we refine a definition of user trust in an application, specifically for this study, as:

The user perceives the risk of using the application and knowing the consequence of a negative outcome is greater than the benefit. Yet, the user is willing to accept the vulnerability in a transaction based on their positive expectations regarding the application's future behaviours (Kimery & McCord, 2002).

2. BACKGROUND

Based on this definition, we formalize the concept of user trust in authentication of mobile banking as: the users' willingness to use an authentication system for guarding their wealth, while they perceive the existence of a risk involved. The users are willing to use the system because they expect the system to behave according to their expectation.

2.3.2. Initial trust

Through-out all interpretations of trust, trust can be classified into two forms: *initial trust* and *long-term trust*. Initial trust is defined as the initial perception of trustworthiness perceived by the user, and long-term trust as the trust acquired over time through experience. The latter is a form of trust that requires the truster to repeat interactions with the trustee. After each successful interaction, the trustee appears more credible, because the experience of the interaction indicates the trustee is trustworthy.

In Mc Knight & Chervany (2006), they claimed almost every relationship begins with an initial phase. The initial phase is characterized by uncertainty and doubt. The trust generated in the initial phase may impact the effectiveness of a relation, and also how easy or difficult it will be for the parties to trust each other in the future. The parties are unfamiliar with each other in the beginning, and the truster has no prior experience with the trustee. This means, unlike in the case of long-term trust, experience is not a factor that influences initial trust. Instead, the truster must base his trust on relatively superficial cues (Egger, 2003). In other words, initial trust is influenced by the first appearance and the reputation of the trustee, along with the truster's experience during the first encounter. To get a better understanding of initial trust, we use an example that was presented in Marsh (1994, p.1):

“Suppose someone offers to help you fix your broken car on the motorway. You've never met them before, but they're wearing garage overalls, and they turned up in a pick-up truck which you saw a few minute ago at a service station. Do you accept their help? ... Now suppose the guy was in jeans and a T-shirt, and turned up in an old VW Beetle. You would probably take a lot more time in accepting help, asking lots of questions, such as who the man is, where he's from, and so on.”

2. BACKGROUND

Let us examine the example above. In the first instance, the driver (the truster) perceives a good initial trust on the strangers (the trustee) to fix the broken car. By judging based on the appearance, the trustee seems to dress in an outfit that appears to be consistent of a mechanic. Also, the first engagement at the service station with the trustee was at an environment where cars are fixed. These evidences increase the truster's perception of the trustee knows how to fix cars. Although, there is no direct evidence showing the strangers know how to fix a broken car (unless they attempt to fix it), there are enough superficial cues for the driver to perceive sufficient initial trust to accept help from the strangers. On the other hand, in the second instance, the strangers show up in an inconsistent outfit; as a result the appearance does not show enough cues for the driver to consider the strangers as trustworthy to fix the broken car.

In the case of attempting to introduce a new system to users, such as introducing mobile banking to the unbanked, the system must generate a good perception of initial trust to the users, so the users are willing to adopt the system. Similarly, in authentication, the system must show adequate relatively superficial cues for the user to create a good impression to perceive the system as secure.

2.3.3. Trust and risk

"Risk is a concept that denotes a potential negative impact to an asset or some characteristic of value that may arise from some present process or future event. In everyday usage, risk is often used synonymously with the probability of a known loss." (Project Smart, n.d.)

Luhmann (1988) identified a close relation between risk and trust. Trust is a mean of handling risk, or as a solution for specific problems of risk. In general, risk must exist for trust to arise. Trust would not be needed if there is complete certainty (or confidence); if there is complete certainty, a person will perceive no risk. Hence, without risk there is no need to trust (Luhmann, 1988). If we view from the opposite perspective, the absence of risk implies confidence (Egger, 2003). In other words, trust should be seen as confidence in the face of risk (Egger, 2003); except confidence does not require a person to consider alternatives, whiles trust requires a person to choose an action in preference to others (Luhmann, 1988).

In the case of mobile banking, from the users' viewpoint, there is always a risk in mobile transactions. The risk arises due to the fact that banking transactions are performed remotely. The users do not have direct person-to-person interaction with a bank representative, and, instead, interaction is mediated digitally. Especially for first time users, they risk using an unfamiliar system to perform banking transactions. What is essential is the designed interface must generate a good initial trust, so the users can place their trust in the application to handle their finances.

2.3.4. Trust in banking interfaces

In Kim & Moon (1998), an empirical study was undertaken that investigates which graphic design elements influence customer's perspective of trustworthiness in cyber-banking interfaces. Kim and Moon admitted there are flaws in their methodology. During their experiment, they requested their subjects to indicate the immediate feeling that was evoked by the interface; the result is therefore the reactive exposure to the visual interface, not the actual experience of cyber-banking. There study could be interpreted as a test for user initial trust, because the immediate evoked feeling is essentially the subjects' initial trust in the testing interfaces. The study results show users prefer cyber-banking interfaces to have colour tone that is "*cool hue*" in "*primary colours*". By using such properties, the user interface design can affect the perceived trustworthiness (Kim & Moon, 1998). Kim and Moon also admitted that their participants have a homogeneous social-cultural background. The factors that satisfied their subjects might not satisfy people with different social-cultural background. Furthermore, their study was conducted for electronic banking interfaces over a computer; it is questionable that some of their suggested properties might not apply in mobile banking interfaces.

2.4. Memory

Human beings have five senses (sight, hearing, smell, taste, and touch); people use their senses to capture information. The information is interpreted, filtered, processed, and translated into a form of data (or knowledge) which is stored in memory where it can be retrieved when needed. Memory can be considered as a placeholder where information is kept, and it is used for

remembering things. In cognitive psychology, memory is defined as an ability of storing, retaining, and retrieving of information.

People's memories belong to each individual. Unless there is an explicit communication between persons to disclose information, the information stored in an individual's memory is not shared. Hence, memory can be seen as a private placeholder where information can be kept secret, and the access to the information is controlled by the individual.

By exploiting this advantage, the concept of using password for verification is formed. If a legitimate user holds secret knowledge and assuming the knowledge is not shared, then only that user is able to present the correct secret for verification, and, hence, the user is authenticated.

2.4.1. How do people remember passwords?

A password is a secret used for user verification. Depending on the authentication scheme, a password could be represented in the form of text, images, or etc. However, no matter how a password is represented, the most important is that a user can remember it. Here, we identify the process of remembering a password as a two stage process: creating and learning; and storing.

The first stage of the process is creating and learning. The creation of a password depends on the policies adopted by the authenticating system; whilst some systems assign random passwords, others allow their users to select personalized passwords. Some systems assign passwords to their users because this guarantees the passwords are randomized, which also means the passwords are less susceptible to dictionary attacks. However, evidence from other research shows users remember passwords better if the passwords are chosen by the users themselves (Zviran & Haga, 1990). When people create a password, they attach meanings to the password or they select something that is deducible from their knowledge as the password (Renaud & De Angeli, 2004). Subsequently, the meanings or the knowledge are used as an index of the password.

2. BACKGROUND

During the process of password creation, a created password is briefly stored in the user's short-term memory⁴ (Renaud & De Angeli, 2004). If the meanings of the password do not have an impact on the user, or the user was distracted while processing the password, the password will most likely be forgotten. If a user is to memorize a password for a long period, the password must be encoded in the user's long-term memory⁵ (Renaud & De Angeli, 2004).

If a password is purely random, such as a password selected by a system, users would have to spend extra effort to learn the password. For a user to memorize a password without external memory aids, Sternberg (1999) (cited in Renaud & De Angeli, 2004, pp 1022-1023) claimed that one of the following must be true:

- The password must be meaningful or deducible; or
- The password must be based on some knowledge already encoded within the long-term memory; or
- The password must be rehearsed; or
- The user must have some special scheme for storing and recalling the password.

2.4.2. Password memorability issues

Some of the most important issues related to passwords memorability are identified by Sasse *et al.* (2001) as under the following headings (in *italic* font):

The capacity of working memory (or short-term memory) is limited. Miller (1956) identified that an average human memory can hold only seven (plus or minus two) perceptual items simultaneously in their working memory. Due to the limited capacity, with distraction (such as multitasking) or stress, users are bounded to forget some memory aids that help them to remember their passwords during the learning stage.

⁴ Short-term memory is the active or working memory. It holds a small amount of information for a short temporary period (about 20 to 30 seconds).

⁵ Long-term memory is the static persistent memory that can hold information for a few days or as long as decades.

2. BACKGROUND

Memory decays over time. Information stored in long-term memory may lose accuracy over time; this decay is modelled by the *Power Law of Forgetting* (Bahrick, 1984). Because of memory decays, people may not be able to recall a password, or not able to recall a password precisely, over time. This implies that less frequently recalled items are less likely to be recalled correctly; conversely, the inverse also applies, retrieval of frequently recalled items becomes automatic (Sasse *et al.*, 2001).

Distinct items can be associated with each other to facilitate recall. Passwords with distinctive meanings are easier to remember because there are less overlaps amongst the memory aids. Conversely, similar items compete against each other during recalls (Sasse *et al.*, 2001), and this happens because of within-list interference (Wickens, 1992).

People cannot forget on demand. Passwords will linger in memory even when they are no longer used. This means policies that enforce frequent password changes decrease password memorability; whilst the old password remains in the user's memory, a new password has to be remembered.

Recognition of a familiar item is easier than unaided recall. The concept of recognition rather than recall seeks to minimize users' memory load by making objects, actions, and options visible (Sharp *et al.*, 2007). The visual items are used as memory cues for retrieving and matching previously seen images from the users' memory. Unlike recognition, unaided recall is a two-step process; the memory aid of an item must first be recalled, and then used as an index to retrieve the wanting item from the user's memory.

2.4.3. Visual memory

The concept of recognition rather than recall leads to studies of visual memory performances. Prior cognitive studies have shown that people are much better at recognizing previously seen graphical information than at precisely recalling textual information (Paivio *et al.*, 1968; Madigan, 1983). Graphical images provide a rich and detailed representation in memory, which also makes them distinctive at the time of retrieval (Nelson, Reed, & Walling, 1976). In addition, people's visual memories are less likely to be affected by the decline of cognitive abilities, such

as ageing, which often occurs to other types of memory (Park, 1997 cited in Renaud & De Angeli, 2004). The increase in visual memorability is predicted by the *picture superiority effect* (Nelson *et al.*, 1976); it predicts concepts and information are more likely to be remembered if they are presented as images rather than as text. In other words, people can remember more images more accurately and far longer than semantic text.

Visual and verbal (or textual) information are processed differently; this is explained by a concept introduced by Paivio (1971), called *dual-coding theory*. The theory describes the human mind as having distinct channels to process information that are represented separately in different forms. For example, when people watch a movie, they can interpret both the visual and verbal information. This is possible because their processing channels do not interfere with each other. However, each channel has its limitations. If pictures and words are both presented in a visual format, such as watching a movie with subtitles, then the audience will experience difficulties attending to both sources of information simultaneously. This happens because people can only process one source of information from the same channel at a time, which means, multiple sources in one channel compete for attention. Furthermore, the theory explains information that forms a picture can be recorded in both visual and verbal memories, whilst abstract concepts, such emotions, can only be recorded in verbal form (Paivio, 1971).

Understanding of the dual-coding theory is important for authentication system designers. Users can use multiple channels to process a password if it can be represented in visual and verbal form; thus improves the password memorability. Also, if a password is represented visually, such as a graphical password, then it is important for the designer to ensure the sources of information are not competing for attention from one channel.

2.4.4. Kinesthetic memory

Kinesthetic memory (or muscle memory) is associated with human's ability to memorize motor skills, such as arm movements, within their neuro-muscular system. Before a motor skill is adopted, muscle movements require concentration in order to move in the correct way (Simlog, 2007). Through practice, the movements are shaped and inculcated into person's kinesthetic memory. Once the movements are consolidated within the kinesthetic memory, the person

2. BACKGROUND

becomes adapted to the action and requires less concentration to achieve precision of the movements. The movements become more natural and automatic (to a degree, without thinking) as they are reinforced through repetition. For example, a novice basketball player must calculate factors, such as the amount of throwing power; the body position; the aiming direction; etc. to throw for a basket, whilst the same action can be performed more naturally by a professional player. The skill of shooting a basket is directly associated with the player's muscle memory. The novice player has little experience to perform the action. The novice player's muscle movement of shooting a basket is not registered within his/her kinesthetic memory; therefore, the player's response system requires longer time to process the motor output. Conversely, the professional player has more practice and the throwing action registered within his/her memory allows the processing to become more efficient, and the shootings become more accurate.

A previous study by Chapman *et al.* (2001) suggests people's dominant hand plays an important role when it is used for targeting locations over time. Their study was conducted with right-handed participants, and the results show clear differences in the stability of target location over time. The right hand memory for target location did not decay overtime, but the pointing accuracy for the left hand did decrease. Their results suggest kinesthetic information stored within the memory is asymmetric and accuracy depends on the hand used. Furthermore, Chapman *et al.* state there are two memory stores for targeting locations, one based on kinesthetic information and the other based on visual information. The memory based on kinesthetic information is limb specific, while the one based on visual information is not. Another study by Khoshnoodi *et al.* (2005) discovered that for a kinesthetic-guided distance reproduction task, such as moving an object from point to point, the initial hand position is more important than the end position. The initial position can influence the user's ability and accuracy of performing the task. Khoshnoodi *et al.* also discovered that the presence of visual information can affect the accuracy of the task. Thus, the correct presentation of visual information is important for any kinesthetic reproduction tasks.

2.5. Security threats

Security threats of authentication systems can be classified into two categories: *malicious* and *non-malicious*.

Malicious security threat is a state when a system or a user deficiency is being exploited by illegitimate users with an intention to do harms. Phishing (or smishing⁶) attacks, for example, are a malicious activity made by attackers to trick legitimate users to give out their login passwords or personal information. The obtained information can be used to gain access into the users' accounts. Other common forms of malicious attacks against password systems are *dictionary attacks*, *keystroke logging*, and *shoulder-surfing*.

Dictionary attack is a type of password attack that uses words from dictionaries to crack a user's password. Users tend to choose weak passwords (Adams & Sasse, 1999); therefore this attack is most efficient against authentication systems that allow users to choose personalized passwords without policy restrictions. A more exhaustive version of dictionary attack is *brute force* attack; it attacks a password by trying all possible combinations of password elements (Yan *et al.*, 2004).

The other methods are more direct. Keystroke logging requires a Trojan horse program installed and running on the authenticating device. When the user enters his/her password, the program records the pressed keys. This type of attack is difficult to initiate on the mobile platform; this is because the attacker must first trick the user to explicitly install a key logging program onto the user's mobile device. Shoulder-surfing is the easiest method. The concept of shoulder-surfing refers to someone watching over the user's shoulder as the user enters a password, thereby capturing the password (Wiedenbeck *et al.*, 2006). With the correct recording equipments, shoulder-surfing becomes easy to achieve, especially when capturing passwords being entered into a fixed-location device. However, since mobile devices are movable, the attacker is required

⁶ Smishing is a form of criminal activity that sends phishing messages using SMS text messages.

to spend more effort to place the equipment or be at the right location to record the password entry.

Non-malicious security threat is a state when security information is exposed to non-malevolent personnel, such as friends or family members, but no harm is expected. People may divulge their passwords with someone their perceived trustworthy; ultimately, this action is sharing their authorization. From a security viewpoint, this is considered as an insecure practice; however, from a user perspective, sharing passwords helps users achieve the desired goal, i.e. retrieving the correct password when it is needed. Often, people share passwords because their passwords are too complicated or they have too many passwords to remember (Adams & Sasse, 1999). Users see the complexity of passwords as a mental workload, so, instead of spending effort to adapt to secure practices, people choose to share their passwords to shed the load.

Sasse *et al.* (2001) identified that some people share passwords because of *identity issues* and *social issues*. As identity issues, some people feel that exhibiting good password behaviour is often associated as ‘paranoid’ or ‘pedantic’. To an extreme, some people are proud to not follow regulations because they do not like following orders. Likewise, some people share passwords because of social issues. Sharing password is considered as a sign of trust; whilst refusing to share passwords with a person is effectively telling that person that he or she is not trustworthy.

There are cases where some people have no options but to share their passwords. Disabled people and illiterate users, for examples, are dependent on their helpers to operate an authentication system. Hence, those users are forced to disclose their login secret.

2.6. Authentication schemes

Authentication schemes can be grouped according to what the verification proofs are based on: *what the user knows*; *what the user is or does*; and *what the user holds* (Renaud, 2005). These are the three common factors that an authentication can use.

User authentication has traditionally centred on *what the user knows*. A secret knowledge, also known as a password, is only given to a legitimate user; this secret is shared only between the

2. BACKGROUND

user and the authentication system. During authentication, the user presents the secret, and the system verifies the user by checking the validity of the secret. In general, the system requires users to memorise knowledge items and recall the items during verification (Sasse *et al.*, 2001). This concept of verification is known as *knowledge-based* authentication. So far, this scheme is the most popular form of authentication, because it does not require exclusive devices and it is inexpensive to build (Renaud & De Angeli, 2004). Although knowledge-based schemes are the most common, there are downsides, such as memorability issues. In the search to resolve those problems, alternative techniques are identified.

Alternative mechanisms that prove users' identity based on *what the user is or does* and *what the user holds* are *biometric-based* authentication and *token-based* authentication, respectively. Biometric-based techniques verify a user by examining the user's *physiological* and/or *behavioural* attributes through the direct measurement of certain properties (Jansen, 2003); these properties are known as *biometrics* (see Figure 0 for examples). And, token-based methods verify a user by validating the authenticity of an object that the user presents or holds, such as

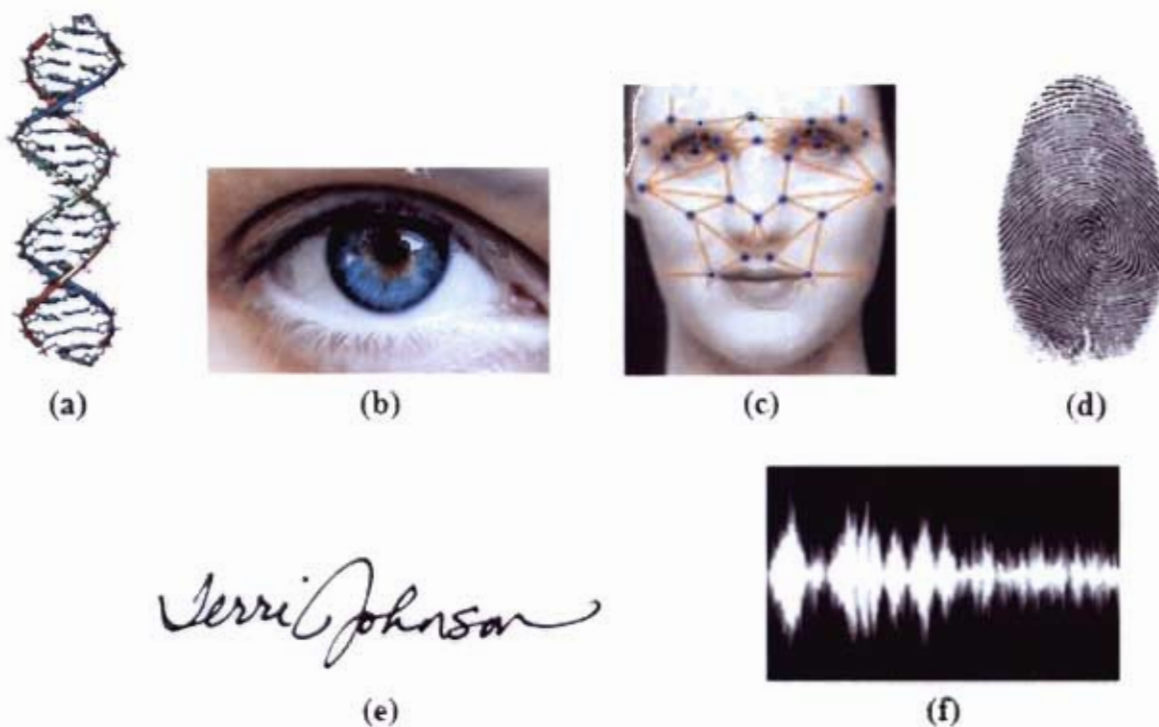


Figure 0. Examples of biometrics. Physiological: (a) DNA, (b) eye iris, (c) facial, (d) fingerprint; Behavioural: (e) signature, (f) speech

object is typically known as a *token* (Renaud, 2005).

A fourth-factor for authentication was proposed by Brainard *et al.* (2006), using the notion of “*Somebody you know*”. The technique makes use of human relationships for authentication. In social interactions, a person can be identified to another through an introduction by a common acquaintance. Therefore, the fourth-factor suggests the use of introduction by an authenticated user for verification. For example, if Bob wants to authenticate to a system called Cathy and Alice is a legitimate user of Cathy, then Bob can authenticate to Cathy through an introduction by Alice. This authentication technique could be very useful in a group environment where members trust each others. However, for individual login systems, such as mobile banking, the fourth-factor cannot be used; this is because a personal bank account belongs to an individual, not to a group of users. Hence, individual accounts are not interrelated.

2.6.1. Biometric-based authentication

Biometric authentication verifies a user based on the user’s properties; the system can only work if it recognizes the user. To do so, users are required to participate in an enrolment process beforehand. In which, the system captures the users’ biometric data to create a digital template and stores the template in a database. To authenticate, the user presents his/her biometrics. The verification is essentially pattern recognition by acquiring the user’s biometric data, extracting features from the collected data, and comparing the features against the template in the database (Jain *et al.*, 2004) (see Figure 0).

As biometrics are impossible to lose, there is no memorability requirement when using them. Biometrics are distinctive and intrinsic to each person; they are inherently more reliable and more capable than the other authentication techniques in differentiating people (Jain *et al.* 2000). As a result, biometrics scheme can be used for identification and verification, which is deemed as advantageous. Although biometrics are unique, not all biometric authentications are perfect; some biometrics can be forged. For example, if a system employs facial recognition, an attacker can use a photograph of the user to fool the system. Biometrics authentication, especially physiological biometrics, does not handle forgery well. If a biometric is forged, it remains stolen for life, and there is no changing back to a secure situation (Schneier, 1999). This is because



Figure 0. An ATM with fingerprint verification

biometrics have the property of being permanent, unlike passwords where they can be reset, biometrics cannot be replaced.

People believe facial recognition could work, as that is the natural way humans identify each other (Coventry *et al.*, 2003). People also perceive fingerprints must work because they are used as evidence in law enforcement (Coventry *et al.*, 2003). In fact, the general perceptions are wrong. Iris verification, using the complex visual texture of the iris for distinctive identification, is the most reliable biometric authentication (Coventry, 2005). The accuracy of iris verification is much greater than fingerprints. It is advantageous because iris images can be acquired from the individuals without physical contact (Coventry *et al.*, 2003), and forgeries, such as artificial irises (e.g. contact lenses), are easy to detect (Jain *et al.*, 2004). Iris scanners use a high resolution camera with a zoom lens to capture an image of the user's iris, and the patterns of the iris are then used for verification. Furthermore, the iris images must be acquired in a non-obtrusive manner, i.e. the system cannot expect the user to be standing with the eye in a predefined position (Coventry *et al.*, 2003); consequently, the sensor unit must cope with a wide range of angles and positions.

Biometric authentication has been adopted for banking interfaces. Integration of fingerprint authentication into ATMs is feasible. Although ATMs with fingerprint verification are not common, they have been put into practical use (see Figure 0). Besides fingerprints, other

biometrics have been proposed for ATM verification. Iris verification is one of the possibilities, and it has already been piloted in ATMs. Coventry *et al.* (2003) conducted usability studies of biometric verification at the ATM interface. Their initial study shows biometrics technology has usability issues, but successful login experiences can influence user opinion and confidence in using the technology in the future. Coventry *et al.* further conducted a field trial study, their results show over 90% of the interviewees were satisfied with iris verification, and would prefer it over PIN authentication. However, it is arguable their result may not apply in the developing world. Many people from the developing world are less experienced with biometric authentication; the lack of understanding of biometrics may influence those people's opinion of adoption.

Using biometrics for authentications appears to be a usable form of security, there are many valid reasons to adopt biometrics for authentication – such as memorability and acceptability; however this assumption is flawed. Every biometric device has its own usability issues (Coventry, 2005). On the surface, biometrics may seem to be beneficial because of their uniqueness; however, the current technology is susceptible to failure. When comparing biometric data, the algorithm must establish fault tolerance. Narrowing the limits increases security from false positive detection, but at the same time, the system becomes more restrictive which decreases usability. So, ultimately, biometric authentication suffers the security versus usability dilemma.

Furthermore, biometric authentication requires devices with a biometric sensor. Most mobile phones on the current market are not equipped with a biometric sensor; as a result, this verification scheme is not suitable for mobile banking authentication.

2.6.2. Token-based authentication

The concept of token-based authentication consists of two steps. Initially, the system assigns each legitimate user with a token, and the tokens are assumed to be used only by the assigned users. The system verifies a user based on the user's possession of a valid token. The system is not responsible for checking the legitimacy of the token holder; instead the responsibility of keeping the token protected belongs to the assignees. The process of key ignition for a vehicle

2. BACKGROUND

for example, regardless of the identity of the driver, as long as the person uses the correct key to start the vehicle, the engine will run.

A good example of a token-based payment system is Octopus card (Octopus Cards Limited, 2005) (see Figure 0) in Hong Kong. It is a contactless payment system where a user places an RFID⁷ card over the reader to conduct payment. The system employs the single-factor token authentication strategy, which is based on the presentation of the RFID card. Although using such strategy increases usability, as no prior enrolment and no memorability are required, however, the system cannot verify the user if the token is not presented. Therefore, the user has to remember to carry the token.

A token can be stolen and used by others. To reduce the possibility of illegal access, a system can employ a strategy called *two-factor authentication*; the system requires the user to perform multiple authentications during login. This strategy is most commonly used with the combination of a token and a password. The two-factor combination can still protect the user if one of the factors is compromised while the other factor remains secured (Renaud, 2005). ATMs use this strategy; an ATM user first uses his/her bank card as a token for identification, and then the

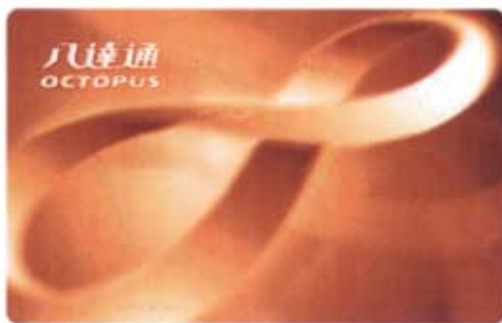


Figure 0. (Left) An image of Octopus card. (Right) A user using an Octopus card for payment.

system requires the user to enter a PIN for verification. While this strategy may seem to work well with token-based authentication, however it complicates usability because the second factor requires additional effort from the user.

In some mobile banking solutions, one can perceive a mobile phone as a token. For example, solutions that use the user's mobile number as identification are essentially using the SIM card as a token. However, this also indicates such applications are hardware dependent since the same SIM card must be used.

2.6.3. Knowledge-based authentication

The use of secret knowledge for authentication is not a new concept. Indeed, it was used before computers existed. In ancient times, Julius Caesar used a key cryptography technique, called *Caesar cipher*, to communicate with his generals. He used a key to cipher messages; the key is essentially the secret knowledge. Although the example above is for cryptography, the main concept of using a password for protection remains the same; without the correct secret knowledge, it is difficult to gain access to the system and its information.

Nevertheless, there are also flaws in knowledge-based authentication. Usability and security problems arise because passwords are expected to comply with two conflicting requirements, but meeting those requirements is almost impossible. The requirements are identified by Wiedenbeck *et al.* (2005b, p104):

Passwords should be easy to remember; authentication should be executable quickly and easily by humans.

⁷ **Radio frequency identification (RFID)** is an automatic identification tagging system which uses an integrated circuit to emit data, which allowing the receiver to retrieve the stored information for identification.

2. BACKGROUND

Passwords should be secure; they should look random and hard to guess; they should be changed frequently, and should be different on different accounts for the same user; they should not be written down or stored in plain text.

In computing systems, a secure authentication system requires strong passwords to prevent attacks (Yan *et al.*, 2004). Ideally, a strong password is highly randomized. However, “human beings being what they are, there is a strong tendency for people to choose relatively short and simple passwords that they can remember.” (Morris & Thompson, 1979, p.595). This means there is a conflict in satisfying those requirements. According to Yahoo! (2004), the most common passwords are “password”, “God”, “sex”, “money”, and “love”. Despite knowing it is not a good idea; people choose passwords based on memorability over security. As a result, password authentication is recognised as error-prone (Dhamija & Perrig, 2000; Sasse *et al.*, 2001).

To increase password memorability, Yan *et al.* (2004) suggest a method of using the pass phrase approach for password generations. For example, using the phrase “My sister Peg is 24 years old” and choosing the first letters of each word, the password would be “MsPi24yo”. Although this approach helps users to choose password that are harder to guess with a mnemonic phrase, this method is only suitable for alphanumeric passwords; the approach cannot be applied for PIN selections, as logical phrases are seldom made up of numbers only.

An alternative to simple passwords is cognitive passwords, also known as semantic passwords (Renaud & De Angeli, 2004). Instead of requesting a user to present a password, the system asks a set of questions and authenticates the user based on the semantic answers. This solution improves memorability by asking questions that the user has already known. However, this solution suffers the same problem as normal syntactic passwords: the user’s details are predictable, especially if the attacker knows the user well.

PIN authentication is currently used across all mobile banking applications. Yet, PINs are easily forgotten (Renaud & De Angeli, 2004). People find that remembering strong random PINs to be challenging (Yan *et al.*, 2004). To cope, people choose PINs that are memorable, yet easy to crack (e.g. “0000” and “1234”). Also, users adopt the same insecure behaviour as for passwords,

such as users write down their PINs (Sharp *et al.*, 2007); previous study has reported that up to 50% of users write their passwords down (Adams & Sasse, 1999). Furthermore, some passwords are recorded in obvious locations or near the authentication mechanism for easy access. To circumvent these problems, alternative solutions, such as graphical authentication solutions, have been proposed to increase memorability of the password through exploiting the users' visual memory.

2.7. Graphical Authentication

A graphical password is a secret in an imagery form. A human user inputs the secret into an authentication system with the aid of visual cues, graphical inputs, and output devices (Monrose & Reiter, 2005). The techniques of graphical authentication can be classified into three main categories: *Locimetric*, *Drawmetric* and *Cognometric* (De Angeli *et al.*, 2005). In the following subsections, each of the techniques is explained in detail and with examples.

2.7.1. Locimetric

Locimetric (or location-based) authentication is a technique where the system provides an image as a memory cue and relies on precise position recall to authenticate. This technique requires a user recalling a password by identifying a series of predefined points on a background image.

One of the earliest locimetric authentication techniques, called *graphical password*, is discussed by Blonder (1996). The technique is based on image cued recall; it requires a user to touch a set of predetermined areas on an image in a sequence to authenticate. An example of Blonder's graphical password is illustrated in Figure 0. A major problem of this scheme is identified by Wiedenbeck *et al.* (2005a); they identified that the number of predefined click regions are relatively small, so the password must be long to be considered secure. However, usability decreases as the length of a password increases. Wiedenbeck *et al.* (2005b) proposes a solution called *PassPoints* which overcomes this problem. The advantages of their solution are: (1) it allows users to submit their preferred images for visual cue, (2) users may choose any click points as a password, and (3) the tolerance size of the clickable region around the password click points can be varied.

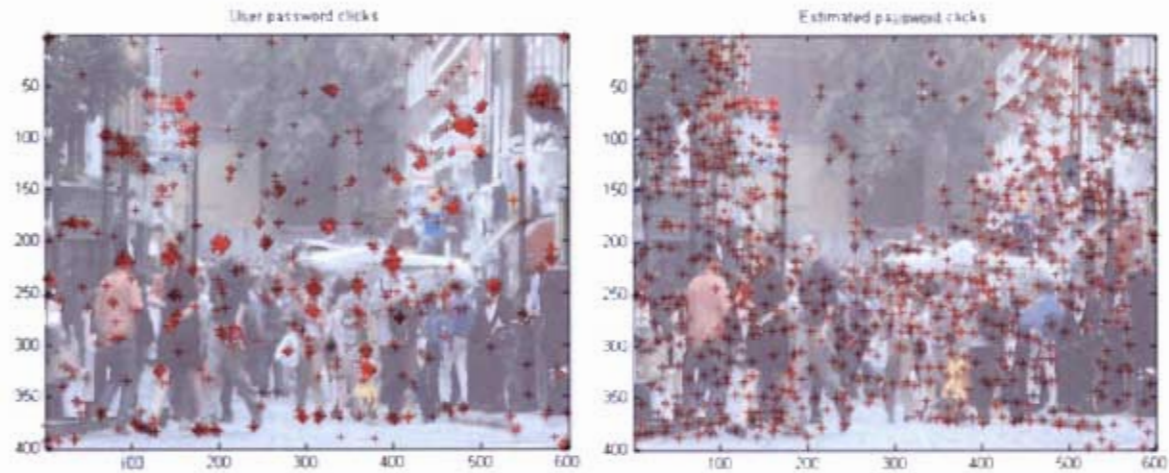


Figure 0. Actual (left) vs. predicted (right) click points (Dirik *et al.*, 2007)

Figure 0. An example of Bionuer's graphical password (Bionuer, 1990)

Although PassPoints is seen to improve the solution, its advantages are also its disadvantages. For PassPoints to be effective, it requires an intricate background image. Although users are allowed to submit their preferred images, but choosing a picture with enough visual salience and yet does not addle user selections is a difficult task. In other words, users might select images with merely few distinctive salient areas. Also, for simplicity, users are most likely to select click points that are easily distinguishable. Hence, both of these problems lead to passwords to become predictable. This is confirmed by Dirik *et al.* (2007); they developed a modelling system which predicts users' choice in PassPoints selection. Their study shows the modelling system can achieve 70% to 80% correct prediction (see Figure 0 for example).

Locimetric authentication relies on the users' ability to remember, to identify, and to click on specific positions on the screen with some level of precision (Renaud & De Angeli, 2004), i.e. the accuracy of finding and pointing at locations on the screen. However, the precision varies amongst users, which is why a tolerance region around the click point is needed. The size of the tolerance region can affect user inputs. Smaller region causes the system to reject more false-negatives, and, conversely, bigger region causes the system to accept more false-positives. This is further verified by Wiedenbeck *et al.* (2005b); they reported that tolerance regions of smaller than 10x10 pixels seriously impair users' memory and increase password input time.

2. BACKGROUND

PassPoints and Blonder's graphical password are based on the *method of loci*; these systems require an interactive interface where users can pick locations from an image, i.e. a touch-screen input interface. For mobile devices, locimetric authentication is suitable for PDAs and touch-screen smart phones; however, they are not suitable for standard mobile phones with a keypad



Figure 0. A user locating a password using a Jiminy template (Renaud & De Angeli, 2004)

interface.

Besides using locimetric for graphical authentication, Renaud & Smith (2001) propose a paper-based mechanism, called *Jiminy*, which augments the process of recording passwords securely. Jiminy uses humans' word searching puzzle ability to remind the users of their password. To record a password using Jiminy, the user chooses an image, selects a template, and picks a location inside the image to place the template, and then the system records the password characters, along with the random decoys characters. A grid of recorded characters is superimposed on the image and printed for a physical record. To retrieve the password, a corner of the template is aligned on the previously picked location in the image, and the characters of the password are revealed through the holes of the template (see Figure 0).

Jiminy has been reported to successfully help users to remember their passwords (Renaud & Smith, 2001). Renaud & De Angeli (2004) confirm that people remember spatial position better than simple password (passwords based on syntactic knowledge of a word), but worse than

2. BACKGROUND

semantic passwords (passwords based on answers of semantic questions). Furthermore, Jiminy suffers from several flaws. (1) During password retrieval, Jiminy requires the user to have the grid and the template; if any of the artefacts is missing, the system is useless. (2) Although Jiminy helps the user to retrieve his/her password characters, the user still needs to recall the exact sequence to form the password; eventually the solution becomes an anagram problem. (3) Jiminy shifts a knowledge-based authentication to become a token-based authentication (i.e. the template and the printed grid as tokens), but it requires extra effort from the user to remember the position and the sequence of the password characters.

2.7.2. Drawmetric

Drawmetric authentication involves the user drawing a simple outline of a password on a grid during enrolment, and the authentication is consisted of reconstruction of the enrolled sketch. For example, verifying the user's hand-written signature for authentication.

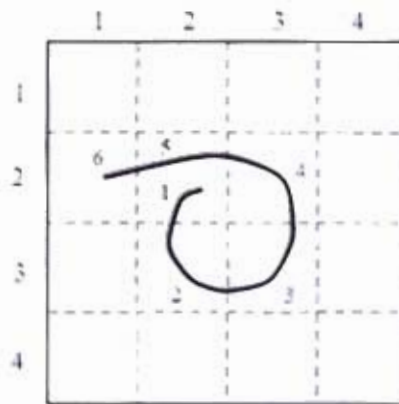


Figure 0. Input of a DAS password on a 4x4 grid (Jermyn *et al.*, 1999)

A well-known drawmetric authentication mechanism for mobile devices is *Draw-A-Secret (DAS)* (Jermyn, Mayer, Monroe, Reiter, & Rubin, 1999). DAS is intended for devices with stylus input, such as PDA's. The idea behind DAS is the user draws a sketch (the password) on a grid, and the system verifies the drawing by checking the drawn strokes. To verify the sketch, the system converts the user's input strokes into a sequence of coordinates, and then the system

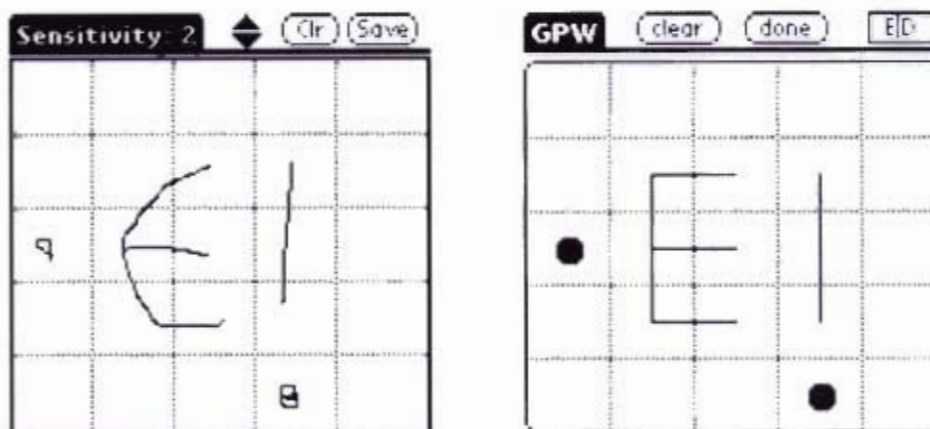


Figure 0. Hand drawn password (left) and system internal interpretation (right)
(Jermyn *et al.*, 1999)

validates by examining the position and the order of the coordinates. For example, the sketch in Figure 0 is translated to (2, 2), (3, 2), (3, 3), (2, 3), (2, 2), (2, 1), (5, 5); where the last coordinate, (5, 5), denotes a “Pen Up” event. Two secrets are considered equivalent if their encoding coordinates are the same, not the drawings themselves (Dunphy & Yan, 2007).

The advantage of this technique is that it allows a user to draw as many strokes as the user wants. Hence, as the number and the length of the strokes increase, the security also increases. However, increasing the number and the length of the strokes also indicates a longer password for the user, which increases password complexity. Also, problems arise when the user draws a sketch that contains strokes which are too close to the grid-lines. To avoid such a case, Jermyn *et al.* (1999) propose two solutions. One solution is letting the user view the system internal interpretation (see Figure 0 for example); whilst the other solution is having the system to reject any strokes that are too close to the grid-lines.

Jermyn *et al.* (1999) indicated that DAS delivers greater security than conventional textual passwords, because DAS has a large password space; this was confirmed by the modelling of user choices in their study. The model shows that, theoretically, the complexity of DAS is comparable to many textual password authentications. Thorpe & van Oorschot (2004) performed an analysis of exhaustive attacks on DAS using a 5 by 5 grid; their results show it is possible for an attacker to crack the user’s password if the number of strokes is relatively small. To increase

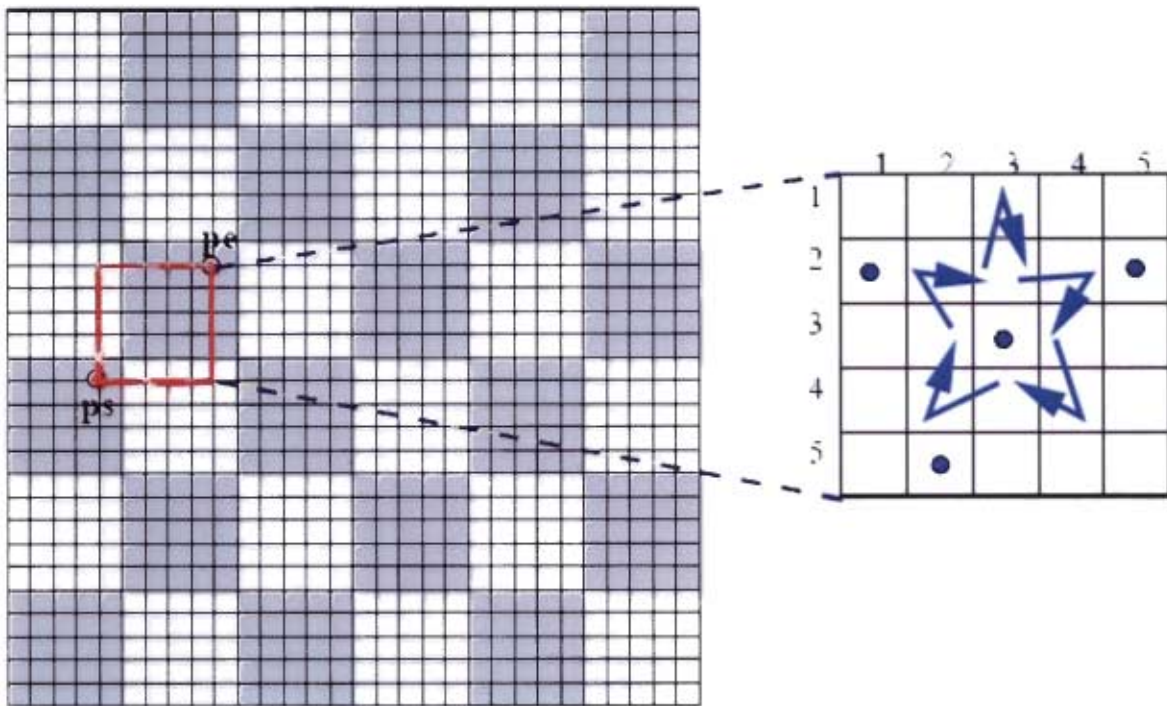


Figure 0. Grid selection (Thorpe & van Oorschot, 2004)

DAS security, the complexity must be increased, either by increasing the size of DAS password space or by increasing the length and the number of strokes. However, either of the solutions increases the difficulty for users to reproduce a password, thus none of the solutions are feasible. Instead, Thorpe and van Oorschot (2004) proposed a technique called *grid selection*. An initial fine-grained grid is displayed, from which the user selects a drawing grid where the user may enter his/her password (see Figure 0). This solution could add an additional of 16 bits to the password space, but with a trade off of minimal inconvenience to the users (Thorpe & van Oorschot, 2004).

A small number of usability studies were done to examine the memorability of DAS passwords. Nali and Thorpe (2004) discovered that 30% of the chosen passwords are symmetrical, 80% are composed of 1 – 3 strokes, 90% are with stroke counts of six or less, and 86% are centred or approximately centred within the grid; these factors show users' selections of DAS passwords are predictable. Another similar study by Goldberg *et al.* (2002) examined PassDoodles – a paper-based authentication using doodles. The results of their study show users could recall all the visual elements of their doodles, but could not perfectly redraw their selected password, like

stroke order, stroke direction, or number of strokes. In attempt to improve password memorability, Dunphy & Yan (2007) adopted the method of loci. They introduced a solution, called *Background DAS (BDAS)*, which adds an image to the background of DAS to aid users to recall their passwords. User studies in Dunphy and Yan (2007) show the effect of after adding a background image increases the complexity of the passwords chosen by the users; both the number of strokes and the length of the strokes have higher average values compare to original DAS. Thus, BDAS increases password security. Furthermore, Dunphy and Yan reported that BDAS passwords are just as memorable as the weaker, less complicated, DAS passwords.

Although studies of DAS have shown positive results, but drawmetric solutions suffer the same dilemma as locimetric mechanisms; they require devices that support a stylus input interface, which majority of the mobile phones on the current market do not support.

2.7.3. Cognometric

Cognometric authentication is by far the most researched area in graphical authentication, and it is widely recognized by its simplicity to design and to implement. The process requires a user to identify a series of recognized password images amongst a larger set of decoy images; if the set of correct images are identified the user is authenticated. Furthermore, cognometric authentication does not require an external interface for user input; it only requires standard button input and a display for output to show images. The strength of cognometric authentication is based on recognition rather than recall through exploiting the picture superiority effect of the human mind.

2. BACKGROUND

A variety of cognometric authentication mechanisms have been developed and many of them use different image types for mnemonics. Passfaces™ by Real User Corporation (2005) is a commercialized cognometric authentication mechanism which exploits peoples' proficient ability to recognize human faces. To authenticate, a user selects a recognised face from a grid of nine faces (see Figure 0), and the procedure repeats for several rounds with different faces each round. If the user correctly identifies all the password faces, then the user is authenticated.

The usability of Passfaces was evaluated by Brostoff & Sasse (2000). They compared Passfaces with passwords. Their findings show: (1) after a long period between logins users made fewer login errors with Passfaces than passwords, (2) users took a long time to execute Passfaces, and (3) users are more reluctant to use Passfaces than passwords and Passfaces users logged into the system less often. A study by Davis *et al.* (2004) found the choices of faces chosen by users are highly predictable. Users choose faces that look most like themselves, based on appearance, gender, and race, or they choose faces that appeal to be most attractive, such as faces of models and celebrities. To overcome the predictability problem, the system should force users to select faces from both genders and from a mixture of racial groups, or alternatively the system can assign password faces.



Figure 0. A screenshot of Passfaces demo application (Real User Corporation, 2005)

2. BACKGROUND

A cognitive authentication concept called *Visual Identification Protocol (VIP)* was proposed by De Angeli *et al.* (2005). The concept is consisting of three types of mechanisms, namely VIP1, VIP2, and VIP3. VIP1 is the pictorial equivalent of PIN. It replaces numbers on the keypad with pictures (see Figure 0.a), and the users are required to identify a sequence of four previously selected pictures to authenticate. VIP2 uses the same interface as VIP1; it differs in that the pictures are displayed in random positions at each authentication attempt, except during authentication failure. VIP3 explores the concept of a combination lock, where the order of entry does not matter. Each user is assigned with a portfolio of eight images. During authentication, four of those pictures are displayed along with twelve other distractor images (see Figure 0.b); to login, the user selects his/her portfolio images in any order.

Results from De Angeli *et al.* (2005) show there is no significant difference in memorability performance between VIP1 and PIN, but the performance of VIP1 is significantly better than VIP2. The latter is expected, as pictures that are displayed in fixed positions are easier to locate and to remember. Besides picture recognition, people may remember a password using the images' locations. De Angeli *et al.*'s results also show fewer errors occurred when users use VIP3 than VIP1 or PIN. This can be explained, because VIP3 is based on pure recognition, which requires no additional memory challenge, such as the order of entry. However, the

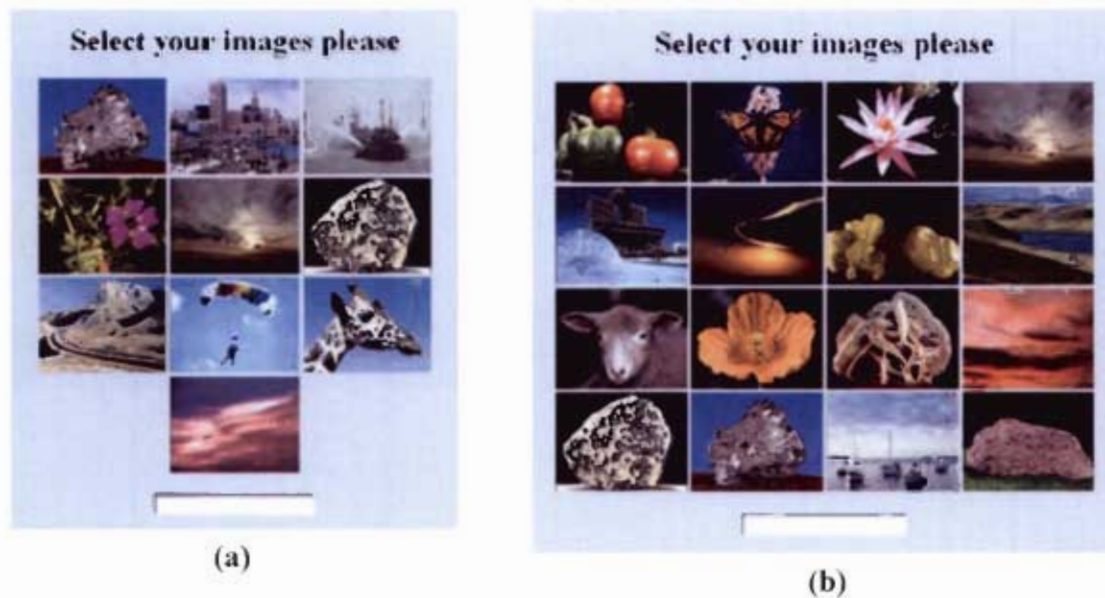


Figure 0. (a) Interface of VIP1 and VIP2, (b) VIP3 (De Angeli *et al.*, 2005)

2. BACKGROUND

downside of VIP3 is users take longer time to enter a password.

One of the problems with all knowledge-based authentication is users tend to have a risky habit of writing down passwords. Although it is difficult to draw the password images, users can describe the displayed objects in words for recording. To overcome this problem, Dhamija & Perrig (2000) proposed to replace photo images with abstract images, for which they created a prototype called *Déjà Vu*. *Déjà Vu* utilizes a technique called *visual hashes*; it converts text characters into graphical form to create password images. By using an algorithm called *Random Art* (Bauer, 1998), designers can hash textual strings into abstract images (see Figure 0). One of the advantages of using *Déjà Vu* is there are less probability of users transcribing their passwords since abstract images are difficult to describe verbally, yet they are recognisable.

Results from cognometric authentication studies (Brostoff & Sasse, 2000; De Angeli *et al.*, 2005; Dhamija & Perrig, 2000) show a commonality: users take a longer time to enter a password using pure recognition-based authentication than using recall-based authentication. In addition, Dhamija & Perrig (2000) also reported their participants take longer time to create a password portfolio using images than using textual characters. These can be expected because people take longer time to browse through each image before finding the recognized image. Hence, the process recognizing a visual password is slower than recalling a textual password.

A cognometric authentication for mobile phones called Awase-E was suggested by Takada & Koike (2003). Awase-E employs a similar strategy as Passfaces; the authentication is consist of multiple rounds, and the user is required to identify recognize images. The main difference of Awase-E is users use their personal images as their password images, and the distractor images are from other users. Takada and Koike argue the reason of using personalised pictures for



Figure 0. Sample images of Random Art (Bauer, 1998)

password is the images are closely related with the user's experience, thus, the users are subconsciously remembering those images. Although personal photos have the highest level of memorability, at the same time they are also the most predictable (Tullis & Tedesco, 2005), therefore, security wise, it is not a feasible option.

2.8. Movement-based authentication

Currently, research that investigates the use of kinesthetic memory to increase password memorability has not been found, but there is some work which exploits the use of gesture movements for authentication. In an attempt to create PIN-less authentication environments, researchers have designed methods that use gestures for pairing devices. Patel *et al.* (2004) suggest an authentication scheme by shaking a device. Their authentication scheme is based on a user authenticating his/her device when using a public terminal by mimicking a sequence of gestures that is generated by the device and displayed on the terminal. Similar work by Mayrhofer and Gellersen suggest a method which uses accelerometer data to pair two mobile devices (Mayrhofer & Gellersen, 2007). Their authentication method requires a user to hold the pairing devices tightly together and shake the devices for a short period. The built-in accelerometers within the devices are used for measuring the movement as the devices are shaken; the devices will only be paired if the accelerometers readings are similar.

2.9. Concluding remarks

So far we have been unable to find a research study that investigates the suitability of an authentication technique for mobile banking. Each of the existing authentication schemes has its advantages and limitations, especially for mobile devices.

At the moment password authentication is the most widely used method for banking systems to verify users; however, the technique is not foolproof. The problems of password authentication are generally caused by the limitations of people's memory. Consequently, users adopt non-secure behaviours to circumvent the memorability issues, and the adoption of those behaviours induces a problem of security weaknesses. To overcome this problem, alternative authentication

2. BACKGROUND

schemes have been suggested. Some are suggested at the cost of inconvenience and special hardware requirements. For example, biometric- and token-based authentications require special equipments to capture user information. Although there are schemes, such as cognometric authentication, that do not require extra hardware, but the use of those schemes are not common and they are unfamiliar to users. Furthermore, introducing a new system to users requires the system to generate a perception of positive initial trust, so the users will accept and adopt the system.

The following chapter outlines the research questions we aim to answer, and it describes the methods we used to conduct our research to find a usable login solution for mobile banking.

3. Methodology

3.1. Significance of research

The technique of using PIN for authentication has been shown to have memorability problems (Sasse *et al.*, 2001). Users adopt non-secure behaviours to circumvent those problems (Adams & Sasse, 1999). To improve the usability and the security of authentication, alternative techniques have been suggested. Although some of the techniques have shown better usability than PIN, so far designers have failed to employ any of those techniques for mobile banking. And, instead, PIN authentication remains as the primary login technique across many (or possibly all) implementations of mobile banking.

As introduced in the background chapter, there are three types of authentication schemes that can be used to verify users; however, two of those schemes (biometrics and tokens) are not suitable for mobile devices. For this reason, a decision was made to continue this research using the knowledge-based verification scheme. Many knowledge-based techniques have been suggested by previous research studies; however, none of the research we found had investigated user acceptance of using those techniques for m-banking.

In addition, this research pursues a new authentication technique that exploits kinesthetic memory for password retention. The prototypes developed as part of this research is for illustrating new authentication schemes to users. The purposes of this study are to identify the suitability of login techniques for mobile devices and to explore user preferences in password authentication systems. Overall, this research aims to find a technique that users accept to use for mobile banking authentication.

3.2. Research questions and hypotheses

The following questions (in **bold font**) drove our research design, and the answers are predicted to formalize our research hypotheses (in *italic font*):

- **Does social or physical context affect how people feel about using different authentication techniques for m-banking?** As indicated by Sasse *et al.* (2001) and Ashbourn (2000), the environment of use affects the user's perception of security. We speculate that when a user performs m-banking authentication, the user is aware of his/her surrounding environment. Since the user's password should be concealed at all times, the user should feel more comfortable to login in an uncrowded area (i.e. in private surroundings), as there is less of a chance of the password being exposed. For this reason, we conjecture that a user would feel more vulnerable to shoulder surfing attacks if authentication is performed in a public crowded area, thus we hypothesize:

H1: Users prefer to perform m-banking authentication in a private environment than in a public environment.

- **Which authentication technique do people perceive as the most trustworthy to use for m-banking?** One aspect of security not covered in any HCI studies we could find was an investigation into the users' perception of trustworthiness of the systems being evaluated. Currently, PIN authentication is the most commonly used verification scheme for m-banking; users have adapted to use PINs for authentication. Although alternatives, such as graphical passwords, have been proven to be more memorable (De Angeli *et al.*, 2005), it is arguable that users may prefer to use text-based passwords from the standpoint of familiarity. Therefore we hypothesize:

H2: Users perceive better initial trust in using PINs for m-banking authentication than using other authentication techniques.

- **Which authentication technique provides passwords that are the most memorable?** Due to the picture superiority effect, graphical authentication is predicted to be more memorable than textual authentication. Furthermore, previous research by Moncur & Leplâtre (2007) has found that retention of multiple graphical passwords is substantially better than multiple PINs. However, those results are from the findings of the comparisons between pictures and texts. People recall muscle movements based on their kinesthetic memory, thus it is arguable that the

memorability of kinesthetic passwords are different compared to textual or graphical passwords. Using the concept of recognition rather than recall as a standpoint, we predict passwords that make use of recognition have higher memorability than ones that make use of recall. As a result, we conjecture:

H3: Multiple graphical passwords are more memorable than multiple kinesthetic passwords or multiple PINs.

3.3. Methods

3.3.1. Participants

With the expansion of mobile banking, potential exists to transform the way people do banking in the developing world. To promote mobile banking for development (and ICT for development), the intended users of our prototypes are people from the low-income⁸ households living in developing countries. Even though people from this class are classified as low-income, many receive (small) wages, which means they have income. Hence, our target users potentially qualify for bank accounts.

For those reasons, we have decided to select our participants from South Africa, a country with a high rate of mobile adoption and banks have successfully established mobile banking services for their low-income populations. For the reasons of location accessibility and participant availability, we have decided to base our research in Cape Town; as a result, our user recruitment for studies is restricted within that region.

In addition, for a user to execute mobile banking and/or mobile authentication the user must have access to a mobile phone and have sufficient knowledge of using it; therefore, participants are expected to have prior experience of operating a mobile phone.

⁸ Different research/articles may have different definition for low-income in South Africa. Here, we assume the definition of low-income as monthly income of 4500.00 ZAR or less.

For the reasons of the restrictions above, we refined the user profile of our participants. In summary, users for this study are mobile users from the low-income household region in Cape Town who are potential qualify for bank accounts.

3.3.2. Procedure

This research is based on human-computer interaction (HCI) discipline; specifically, the user-centred mobile interaction design discipline is adopted. Interaction design is as a process of “designing interactive products to support the way people communicate and interact in the everyday and working lives.” (Sharp *et al.*, 2007, p.8). The process involves three main types of activity (Jones & Marsden, 2006):

- Understanding users (questionnaire and interview survey) – having a sense of people’s capabilities and limitations; gaining an insight into their lives, the things they do and use.
- Developing prototype designs (low-fidelity and high-fidelity prototypes) – representing a proposed interaction design in such a way that it can be demonstrated, altered and discussed.
- Evaluation (experimental evaluations) – Using evaluation techniques to identify the strengths and weaknesses of a design

3.3.3. Understanding users

In the background chapter, we explained the basic cognitive frameworks of how people trust and how they remember passwords. The frameworks provide a general understanding of what is needed for authentication. However, the frameworks are not enough. We also need an understanding of users’ behaviour, as well as their capabilities and limitations. For this reason, a field study is needed to gain an insight into our target users.

Unlike designing a product for a specific group of people, here we want to design for a broad range of people. Therefore, instead of conducting user study with a specific group, we are interested in speaking to various people from different backgrounds. We therefore need a method that allows us to recruit a variety of subjects. Jones & Marsden (2006) have categorized a list of

3. METHODOLOGY

methods of identifying people to study: *selecting people 'off the street', advertising, existing customers, employees of own organization, and referral*. Out of those methods only one, the *selecting people 'off the street'* method, fits our needs. This method has the advantage of allowing researchers to select whom to speak to. However, the method is time intensive in our case, since we are profiling people from different background. We adopt this method to conduct short surveys to get a general understanding of the users.

We recruited people from various locations, such as shopping malls; fuel stations; university campus; and so on; to conduct our survey. Since the profile of our target participants required diversity, we decided not to recruit university students. Instead, we interviewed various groups of people; our subjects were selected from different occupations and age groups. We selected people who were employed with a low- to middle-income employment; thus, we interviewed security guards, domestic workers, supermarket tellers, and so forth. Furthermore, potential mobile banking users are not restricted by employment; people who receive low-income wages but without formal employment, such as those who work part-time or those who are dependent on their family members, potentially qualify for bank accounts. Therefore, we also interviewed representatives from that group.

The choice of using employment status to classify our subjects may not seem to be the best option. Initially, we considered of using monthly income to differentiate the participants; however, we realized that to make such classification the researcher would need to find out the subjects' monthly income. Some people may deem such questions to be intrusive (or offensive), which is why we neglected this approach and decided to use employment status for classification instead.

To conduct the survey, we carried out ethnographic survey interviews with our participants. We first asked the interviewees a list of preset questions, and then followed by a discussion with some open-ended questions, which were based on the answers of the preset questions. After the survey, the data was analysed for an understanding of the target users.

3.3.4. Design and prototypes

In this project, we intend to design authentication interface for mobile devices. From the literature review, we came across different authentication schemes, and out of those schemes the most applicable one for mobile devices is knowledge-based authentication. Knowledge-based authentication is accessible (most mobile phones can support it) and affordable (requires no extra cost to implement). Therefore, the designs of our authentication systems are based on this authentication scheme.

Previous research studies have proposed different authentication techniques that have improved usability compare to existing employed techniques (passwords and PINs). Most of those proposed techniques suggest the use of memory aids to improve password memorability, such as graphical aids. For our design, we have derived our solutions from those proposed techniques for mobile devices. Furthermore, we designed an authentication technique that is based on kinesthetic memory for password retention.

The design ideas were implemented as prototypes. The purpose of prototyping is to demonstrate new ideas to users. Prototypes are a useful aid when discussing ideas, especially when conveying concepts to users; it encourages reflection in design and it is an effective way to test out ideas (Sharp *et al.*, 2007). Jones & Marsden (2006) discussed that prototyping can involve two stages: *low-fidelity* and *high-fidelity*.

A low-fidelity prototype is one that uses materials that are very different from the final product; it is intended to be cheap, simple, and quick to produce (Sharp *et al.*, 2007). The purpose of low-fidelity prototyping is for conceptual design, to explore new ideas, and it helps designers to decide the merits of new concepts. Here, we use low-fidelity prototyping to explore new ideas for login techniques.

Once we gained a clear idea of the basic design, the design is developed into high-fidelity prototypes. High-fidelity prototyping uses materials that are expected to be in the final product and produce a prototype that looks much like the final product (Sharp *et al.*, 2007). For our intention, we implemented software that simulates authentication systems based on the ideas from the low-fidelity prototypes.

A large part of prototyping is to decide what to test, and what not to test; therefore, prototyping requires intelligent compromises to be made (Jones & Marsden, 2006). The compromises lead to two types of prototyping: *horizontal* and *vertical*. A horizontal prototype provides a wide range of functionalities but with little details, while a vertical prototype provides a lot of details for a few functions (Sharp *et al.*, 2007). The objective of authentication requires only a single function, which is to verify users; therefore, we adopted vertical prototyping for our high-fidelity prototypes. After prototyping, the implementations were used for evaluation.

3.3.5. Evaluation

The reason for evaluation is to check that users can use the product efficiently, effectively, and satisfyingly. Furthermore, users also look for pleasing and engaging experience (Sharp *et al.*, 2007); therefore evaluation can be seen as a process to confirm user experience; though some may see evaluation as testing usability. Above all, the goal of evaluation is to assess whether a design (or a prototype) achieve its intended purpose(s).

Within the field of HCI, there are many approaches to evaluate systems. Some approaches evaluate design ideas, while some evaluate actual designs. For our evaluation, we were interested in techniques that allow us to evaluate our prototypes, hence our actual design. Jones and Marsden (2006) have identified a list of approaches that can be used for evaluation. Some of those approaches involve users, and some do not. Since part of our evaluation was to find our user trust in our authentication systems, therefore, real users must be involved; hence, non-user evaluation methods are excluded. On the other hand, not all approaches that involve users are suitable for our evaluation. For example, *direct observation* is a technique that evaluates a product by watching people using it. This technique is not suitable for our evaluation, as we needed to measure accuracy of memorability, user trust, as well as whether our prototypes offer any improvement over the existing authentication techniques. Therefore, we needed an approach that can give us both quantitative and qualitative results.

The approach we adopted for evaluating our prototypes is *experimental evaluation*. The underlying idea of this technique is “to bring the rigors of the scientific method to the field of interface evaluation.” (Jones & Marsden, 2006, p. 209). This technique evaluates prototypes with end-users (the profile of our end-users were defined previously in the participants section).

3. METHODOLOGY

Conducting experimental studies is essentially (dis)proving hypotheses, where in this research we are testing the hypotheses we have laid out earlier.

Two experimental studies were designed for evaluating our prototypes:

Experiment 1. From our hypotheses, H1 and H2 are both conjecturing user preferences based on the users' initial experience with the testing systems. We allocated an experimental study to test both of those hypotheses. The goal of this experiment is to compare user preferences between the testing authentication systems in different environments; we therefore selected the *within-group* study method. Since one of the hypotheses tests for user trust, we decided to conduct the experiment in an atmosphere where the users were comfortable and feel secure; thus we abandoned the use of laboratory environment, instead we brought the experiment to the participants. The experiment took place in a private context, and it began with a training of each user using the testing systems. To avoid learning effects, the order of introduction of each system was rotated (by using a Latin square design) for each new participant. After the subjects were familiar with the testing systems, we requested the subjects to perform tasks. Since our testing authentication systems are based on the knowledge-based login techniques, the systems authenticate passwords. The allocated tasks for this experiment were password entries.

The first task required the subjects to enter a list of given passwords. The time for each correct entry and the number of attempts were recorded for the measure of efficiency and effectiveness. Subsequently, a second task was given to the subjects; the task required the subject to perform password entries for each testing system in an open crowded environment. The idea of the second task is to allow the subjects to get a feel of password entries in a public environment. At the end of both tasks, a questionnaire took place to collect qualitative data about the testing systems.

Experiment 2. The aim of the second experiment is to test H3. A study by Moncur & Leplâtre (2007) compared subjects' retention of multiple PINs to multiple graphical passwords. Following on from their study, we investigate users' retention of multiple passwords of each of our password authentication prototypes. The goal of this experiment is find a type of passwords that is most memorable.

Having the users memorise different types of passwords can interfere password memorability. Hence, the within-group method cannot be used for this study; instead, the *between-groups* experiment approach was adopted. Each participant was allocated to one type of password. This means the order of introduction is not crucial; the important thing is that the number of participants in each group must be equal.

All participants first undertook a training session to familiarize themselves with the allocated password system. Once the subject was familiar with the system, he/she was given three randomly selected passwords; each password was made up of four elements. In Moncur & Leplâtre (2007), their participants undertook a rehearsal session by entering each of their assigned passwords correctly twice. However, we believe that entering the passwords twice is not sufficient for the subjects to register movements into their kinesthetic memory. Instead, our subjects were given a 24-hour rehearsal period to memorize their passwords. To enable the subjects to have access to the passwords during the rehearsal period, the passwords were given to the subjects on paper.

After the rehearsal period expired, a facilitator returned to the subjects and collected the papers that contain the passwords. Six days later, the facilitator returned again and requested the subjects to recall their given passwords. This was followed by a questionnaire session to determine the methods the subjects had applied to remember the passwords.

3.4. Constraints and anticipated problems

In this section, we lay out a list of constraints and anticipated problems of this research project:

Materials for prototypes – graphical authentication requires images. The images used must not violate copyright. Furthermore, the pictures lose quality after they are transformed to fit onto a mobile display; yet, the pictures must remain visible and distinctive.

Equipment and software (prototypes) – one of our login techniques requires its user to produce kinesthetic actions for verification. To do so, we require a device that can capture movements; a device with built-in accelerometer is suitable for this purpose.

3. METHODOLOGY

Availability of users – to understand users, the interview participants are selected randomly “off the street”. The subjects for our experiments are recruited and they need to be screened to ensure they fit the profile.

Dropout rate – there is a risk of losing subjects when running a longitudinal study. The study by Moncur & Leplâtre (2007) recruited volunteers to participate in their study, and they reported there was a high dropout rate. To avoid subjects dropping out, remunerations must be offered to encourage participation.

Physical context – one of the studies requires a comparison between private and public area; at the same time, the study is conducted in an environment where the subjects are most comfortable. However, it is difficult to find a location that fit both purposes because there is little control for the researcher to choose the environment.

Language translation – although English is the primary spoken language in South Africa, people from the developing community prefer to speak their native languages; thus a translator is needed. However, this also induces risks, as the translator could distort the information by misinterpretation or favouritism.

Financial resources – for our experiments, both subjects and a facilitator (who is also the translator) are recruited, therefore we need to have enough financial resources to provide compensation for their participation.

4. Understanding Users

In this research, we first focus on building a profile of the target users' habits and capabilities. From the literature review, we understood peoples' cognitive behaviour of how they remember passwords; whilst, in this part of the investigation, we want to find out the characteristics of our target users. We aim to acquire an understanding of the users' habits of using a mobile phone, their awareness and adoption of mobile banking, and their perception of trust in mobile services.

The target users for this research are people from the low-income sector, previously defined in the methodology chapter. The reason for selecting users from this division is that even though they are classified as low-income, they are receiving income; thus, they qualify for bank accounts. However, we do have one strict requirement: the target users must have access to a mobile phone and have sufficient knowledge of operating it. This is essential as m-banking requires the users to use a mobile phone to perform transactions, thus understanding the basic operations of a mobile phone is necessary.

Participants for this study were recruited randomly from various locations using the "*off the street*" method. Hence, no previous arrangement was made with the participants beforehand. This means ethnographic observation techniques cannot be used, as no individual would allow a stranger (or a researcher) to follow them for a period of time to observe their behaviours. So instead, our approach to understand our target users is through surveys. We designed an interview based survey (see Appendix A) for this study; the questions of the survey are categorized in two parts as follow:

- The first part of the survey focuses on the *mobile phone usage*. This part asks questions related to the subjects' perceived trustworthiness and reliability of mobile phones and mobile networks. Furthermore, we are interested in for which other applications besides communication the users use their mobile phones; knowing this, allows us to consider alternative applications for which mobile authentication could be used.

- The second part of the survey focuses on understanding *banking functions* that users use where authentication is needed. To start, we find out if the interview subject has a bank account. This is important as it can help us to identify whether the subject understands banking. If the subject has a bank account, we can assume the subject has sufficient understanding of banking functions; thus we can proceed with questions asking about their perceived trust in their banks. However, if the subject does not have a bank account, we compile a list of bank functions and explain the basic purposes of banking to the subject. Furthermore, we also ask questions about their awareness of different banking channels, such as internet banking and mobile banking.

At the end of the interview, unstructured open questions are asked. The topics of the questions relate to the answers given during the survey.

4.1. Interview results

In the methodology chapter, we identified two groups of low-income mobile users who potentially qualify for bank accounts: (1) there are those who are employed and receive low wages; and (2) those who work part-time or dependent on the income from their family members. These two groups cannot be considered as a same group; people from the former group are almost certainly financially independent from others, while people from the latter group are most likely dependent on their family members and/or friends. We speculate there are differences amongst their uses (or needs) of banking functions as people from the second group are more likely not to have a bank account. We therefore interviewed representatives from both groups; the results from each group are presented in separate subsections.

4.1.1. Survey 1: interviews with full-time employed users

The first group of interview subjects are representatives from the low-income division who are working full-time. To fulfil the requirement of subject diversity, subjects were selected from different occupations (security guard, cashier, receptionist, salesperson, waitron, etc.) and different age groups (from 20 to 53 with a mean age of 30). Seventeen subjects were

interviewed; the interview sessions took place at the subjects' work environments during working hours.

Part 1 – Mobile phone usage

Fifteen of the interviewed subjects reported that they own mobile phones; the other two subjects indicated that they do not have a mobile phone but have access to their spouses' mobile phones.

The majority of the subjects use mobile pre-paid accounts; the results show that the subjects have a habit of purchasing at least R30⁹ worth of airtime (and an average of R54) per week. Two thirds of the subjects claimed they purchase airtime for personal use only; the other third said they send airtime to family members and friends, sending an average of R15 to R30 worth of airtime per week.

Most of the subjects reported that they use the basic mobile applications such as calculator, alarm, clock and calendar. Seven of the subjects said they occasionally use their mobile phones to browse the internet. Eight of the subjects said they play games on their mobile phones. One subject indicated that she uses MXit¹⁰ (a mobile text-based chat application) on her phone. These results show that most of the subjects use the applications that were preloaded on their mobile phones, and they seldom download external applications. Furthermore, eleven of the subjects said they use their mobile phones to play music, and twelve subjects said they use the camera function of their phones. The subjects' habits of playing music and capturing pictures using mobile phones indicate that the subjects exchange media files. One of the common ways of exchanging media is via Bluetooth, a process which requires authentication. The authentication of Bluetooth connections does not require password retention, as the password (PIN) used is a one-time password for pairing devices. Thus, the password memorability issues do not apply in this case; the current PIN authentication is sufficient for such purpose.

⁹ R = Rand, the South African currency

¹⁰ MXit is a popular mobile text instant messenger in South Africa - <http://www.mxit.com/>

4. UNDERSTANDING USERS

Here, we intend to learn if the users trust that mobile technology is secure and reliable. Questions on the subjects' perception of security were asked. The subjects were asked if they trust the information stored on their mobile phones cannot be accessed by a third party. Ten of the seventeen interviewees replied that they trust others cannot access their information. They indicated the reason for that is because they always carry their mobile phones with them. To the contrary, one of the common reasons indicated by those who do not trust their mobile phones is because their family and friends have access to their phones. Hence, the results show the subjects' perception of trust in mobile phones is associated to the phones being accessible by others.

We further asked questions related to the subjects' perception of reliability of their mobile service provider. Questions about if the subjects believe their sending or receiving message (or voice call) will deliver to the correct party were asked. Fourteen subjects indicated that they trust their mobile service provider as being reliable. However, a few subjects have mentioned that they have experienced call connections being rejected by the network or delays with sending text messages. Some subjects have pointed out that they use the delivery confirmation notification function to acknowledge message deliveries. Due to potential network delays, a comprehensible delivery confirmation service is a requirement for m-banking.

Part 2 – Banking functions

In the second part of the interview, we discovered an interesting result: all of the interviewees from this group have bank accounts. The interviewees explained that their salaries get paid directly into their bank accounts, which is the reason why each person has a bank account. A question of whether the subjects trust their banks to safeguard their money was asked. The majority (14 out of 17) responded yes. Some said they trust banks because their banks have good reputation; whilst, some said they have never experienced problem with their banks before. However, three of the interviewees did mention that they do not trust banks, and this is due to various reasons. One subject explicitly mentioned that her reason for not trusting banks is because some of the banking procedures can get too technical and sometime her money gets deducted without notifications. The former is understandable, as the service procedure becomes too complex, customers feel that they are not in control of the system and tend to lose trust with

4. UNDERSTANDING USERS

the service (Singh, 2006). However, the latter requires banks to change their communication methods to be more informative.

The results also show that people bank regularly and most people do banking at least once a month. The most popular banking features are *Checking Balance* and *Cash Withdrawal*, which two of the common functions of an ATM. When a client uses an ATM, the ATM system requires authentication. The topic of ATM password efficiency has been discussed by Moncur and Leplâtre (2007). Furthermore, based on the captured results, we suggest that the basic banking features (such as checking balance, peer-to-peer money transfer and bills payment) are required for m-banking solutions.

Eleven interviewed subjects indicated they have never come across the idea of mobile banking, and those who have heard of the service said they do not fully understand how the service works. This shows that banks in South Africa are not promoting m-banking services correctly; the majority from the low-income sector are not aware and do not understand the benefit of the service.

One person indicated that she uses internet banking and two persons said they use m-banking; whilst the others said they access their bank accounts in conventional ways (going to a bank teller or an ATM). A small portion (6 out of 17) of the interviewees indicated that they trust remote banking services to be secure. Those who remained conservative about remote banking reasoned they do not trust internet banking because they believe the internet is vulnerable; their perceptions were based on reputations of the internet learned from media reports. Whilst, some said they do not feel confident to use remote banking services because they have no experience of using such services and they prefer to do banking manually at the bank. From this survey, we learned that there are various reasons that cause people not trusting to use m-banking; the following list summarizes the reasons that we learned from our interviewees:

- Prefer to go to the bank to do banking with face-to-face interaction.
- Preference of cash transactions over digital transactions.
- No experience of using m-banking.
- A mobile phone does not give enough details

- A third party might have access into the account information.
- Easy to send money to a wrong account.

At the end of the survey, we asked the subjects if they send/receive money from other people, and if so we asked the methods that they use. The majority (14 out of 17) of the subjects said they prefer to leave their money in the bank because they believe that is the safer option. The survey results show eleven of the interviewees send money to other people, while seven of the seventeen receive money from others. To send/receive money, the subjects use one of the two common methods: money is either given to the receiver in cash or sent via the banking channel. The former is due to the subjects' preferences of giving money to the receiver in person; this is the most convenient method for both parties if they have direct access to each other. For those who do not have direct access to the receiver, they make use of the latter method; they prefer to use a reputable trusted third party, such as a bank, to send money. None of the interviewed subjects said they prefer asking a friend or using postal delivery service to send money. This is understandable because those approaches do not guarantee deliveries; as a result, the subjects prefer to use a paid service to assure deliveries.

4.1.2. Survey 2: interviews with part-time employed and unemployed users

For the second survey, the same questions in Appendix A were used; however, the difference in this survey is that we interviewed people who were not full-time employed. In our previous survey, the “*off the street*” method was used for identifying people to interview, and subjects were found at their work locations. However, the same method cannot be used for the second group. As we were interested in finding subjects who are unemployed, they do not have a specific location of work. Instead, interview subjects were recruited from a skills training centre in Khayelitsha, Cape Town. Total of fifteen subjects were interviewed (their age range from 17 to 49 with a mean age of 30); the interview sessions took place at the training centre during their break time.

All of the fifteen interviewed subjects were students at the training centre. Nine of them indicated to be unemployed, while the other six were part-time employed with occupations across different industry domains, such as fuel-station attending, cleaning, domestic work, waitressing, and street vending.

Part 1 – Mobile phone usage

Of the fifteen interviewed subjects, fourteen of them reported to own or have access to a mobile phone. One person responded that he does not own a mobile phone; he occasionally has access to his friends' mobile phones. He explained the reason for that is because he is unemployed, so he cannot afford a mobile phone. For people to contact him, he gives out his friends' phone numbers, so those people can contact his friends and then the message gets delivered to him.

The results of the second interview survey show the average amount of the subjects spent on airtime per week is R26, and only three subjects have indicated that they have a habit of sending airtime to other people.

Similar to the first survey, the subjects from the second survey also responded to use the basic functionalities of their mobile phones, such as calculator, alarm, clock, and calendar. Seven of them use their phones for entertainment, such as games and music; eight reported to use their phones for taking photos and videos. Surprisingly, none of the subjects from the second group reported to use their phones for browsing the internet.

Twelve subjects responded they trust mobile phones will not leak their private information. The general reasoning for their trust is because they have never experienced problems before, and they believed mobile phones provide sufficient privacy protection. Those who indicated not trusting mobile phones because they believe mobile phones are not secure or they believe their mobile service providers can make mistakes. The results show that the subjects' past experiences with mobile phones have much influence on their trust in using the technology.

The results from this survey are similar to the first survey; most of the subjects (13 out of 15) from this survey have responded that they trust their mobile service provider and they perceived their service providers as reliable. They trust their mobile phones and the networks to work as they expected; when a message is sent, they trust the service provider to deliver to the correct recipient if the receiver's telephone number was entered correctly.

Part 2 – Banking functions

The results of this part of the second survey are very different compared to the first survey. In the second survey, just over half of the group we interviewed (8 out of 15) had bank accounts. All the ones who indicated to be part-time employed had bank accounts, while there were also two who were unemployed but had bank accounts; they explained the reason they opened bank accounts was for their previous employments. From these results, we are confident to assume that peoples' (especially those who fit our participant profile) banking adoptions are closely related to their employment status. For reasons of security and convenience, many employers pay salaries (or wages) electronically; consequently, their employees are ought to open bank accounts. Therefore, we can consider employment as a force-factor which drives people to adopt banking. There are also other factors; some of our interviewed subjects explained that the reason they opened bank accounts is for others to transfer money to them. In other words, some people adopt the banking channel for remittance services.

The results show the subjects who have bank accounts prefer to do banking monthly (once or twice a month), and their bank account are used for savings and deposits. Of those eight subjects who have bank accounts, six indicated they trust their banks for safeguarding their money because they had never experienced any problems; while the other two subjects said that they do not trust banks because they had negative experiences, such as money goes missing without clear notification or mistakes were made by their banks. The results imply that the subjects' experiences with their bank influence their confidence in the system.

The majority of the subjects (14 out of 15) had never heard of m-banking. After we explained the basic concept of m-banking, eight subjects said they would be willing to try mobile banking services, six said they prefer not to try, and one said unsure. Those who responded willing to try m-banking said they are willing because the service seems convenient, and as they had never experienced problems with their mobile phones and banks, they see no problems with mobile banking. However, those who were not willing to try the service explained the reasons are because they do not have the experience of using the services or they rather prefer face-to-face interactions with bank personnel; these results show peoples' adoption of new banking services depends on their prior experience with the banks.

At the end of the survey, we also asked the subjects about the method they use to send/receive money. Seven of the subjects said they send money to other people. Five of them send money via the banking channel (direct bank transfer, or first withdraw cash then deposit into the receivers' accounts), one subject said she sends money to others through friends, and one said he sends money either via postal service or through a friend. The subjects have a habit of sending money in a monthly schedule, between R150 to R1000 each time. One of the subjects explained his method of notifying the receiver; after he sends money, he also sends a text message to the receiver. Another subject told us about how his grandmother retrieves the received amount. He explained his grandmother does not understand how to operate an ATM; therefore, when his grandmother goes to an ATM to withdraw cash, she asks a security guard to withdraw for her. During the process, she discloses her account PIN. Adopting this non-secure habit requires the grandmother to trust the third party. This could be explained by the following reasons: the grandmother sees the security guard as a bank employee, thus she sees enough superficial cues to generate initial trust to trust the security guard; or the grandmother does not understand the importance of PIN security, thus she does not see the needs of keeping her PIN private.

4.2. Summary and concluding remarks

Although the sample of the interviewed subjects was small, the data we collected from the interviews provided a sufficient understand of people's habits of using mobile phones and their perception of the security of mobile phones and banks.

Our results showed there is a high penetration rate of mobile phones in the low-income households in Cape Town, South Africa. A non-surprising result was discovered; given that the diversity of the current mobile phone market, every interviewed subject's mobile phone is of a different model. There are many different platforms and capabilities of mobile phones; hence, when designing solutions for m-banking, the solutions should aim to be deployable (or suitable) across many platforms.

The results from both survey studies showed peoples' adoption of mobile internet is relatively low. Based on this, it is arguable that m-banking services through the WAP (or mobile internet) channel may not be a good solution.

Most peoples' confidence in their banks depends on the reputation of the banks and their prior experience with the banks; with either one negated, people will dismiss their trust in the banking system. Furthermore, we discovered that most people trust using their phones and they also trust their banks; however, only a small portion of the subjects indicated to trust mobile banking. A broken link exists in that the subjects were hesitant to use mobile phones for remote banking. This could be explained by the subjects' unfamiliarity with m-banking; their lack of experience with the technology generated distrust in m-banking. We speculate that this was due to m-banking being a new concept, so people were not yet exposed to the benefits and the security of m-banking. Or ultimately, perhaps, people see mobile phones only as a tool for communication, but not as a tool for managing their finances.

5. Design and Prototypes

This chapter presents two design concepts of knowledge-based authentication for mobile devices. One exploits people's graphical memory for password retention, while the other exploits people's kinesthetic memory. The goal of the two is to find an optimal solution that is suitable to replace the usability-flawed PIN authentication.

5.1. Graphical authentication

From psychology, we have learnt that recognition of a previous seen item is easier than unaided recall. Following the same logic, graphical recognition-based authentication is predicted to provide better memorability than textual recall-based authentication.

The design of our graphical authentication follows the cognometric verification model. It follows the same design paradigm as Passfaces (Real User Corporation, 2005), Déjà Vu (Dhamija & Perrig, 2000), and VIP (De Angeli *et al.*, 2005), where users identify recognised images amongst decoys to login.

5.1.1. Design

Combination versus permutation

A PIN is a form of a permutation of numeric characters, where the characters and the order of the characters contribute to the correctness of the PIN. Remembering of a PIN requires recalling both; first recalling of the characters, then recalling of the sequence order. This decreases memorability, as the dual-recalling of the permutation increases the complexity of the PIN.

Monrose & Reiter (2005) confirm that a combination graphical password is easier than permutation. Their study shows the majority of their subjects who used a permutation graphical password can correctly identify password images but in an incorrect order. It shows people are efficient at recognizing images, but they are not efficient at remembering the order of the recognitions. This is expected, as the reconstruction of a sequence order is a form of unaided recall. This is further confirmed by De Angeli *et al.* (2005); their studies show it is more difficult

for people to remember visual sequence over long intervals between retrieval. From these studies, the concept of a combinational lock, where selection of a password element is unordered and no duplicates are used, seems promising for the design of a cognometric authentication. For this reason, we designed our graphical authenticator to be based on pure recognition, without any recall challenges.

Security

If N is the number of elements in a password and M is the total number of elements in the challenge set, then the security (or the guessability) of a PIN authenticator is 1 in M^N ; whilst the security of a combination authenticator is calculated using binomial coefficient:

$$1 \text{ in } {}_N C_M = \binom{M}{N} = \frac{M \cdot (M-1) \cdot \dots \cdot (M-N+1)}{N \cdot (N-1) \cdot \dots \cdot 1} = \frac{M!}{N! \cdot (M-N)!} \text{ where } M > N > 1 \quad (1)$$

For a combination authenticator, the guessability increases as the size of the challenge set (M) increases. To the contrary, increasing the number of password elements (N) does not necessarily increase the overall security. The system reaches highest security when $N = \frac{M}{2}$. Both N and M variables affect usability of the authentication. There is a trade-off of usability for security when either one is increased. The optimal values for both variables vary, and they depend on the level of security needed and the retention ability of the users.

Theoretically, for a combination authenticator to have equivalent security as a PIN authenticator, the former must have the same guessability as the latter. In this study, we are designing a graphical combination authenticator that has equivalent security as a four number PIN authenticator. Since the length of a PIN is 4 ($N_{PIN} = 4$, $M_{PIN} = 10$), the combination system requires to have guessability equals to or higher than 1 in 10000, therefore $\binom{M}{4} \geq 10000$, so $M \geq 24$ (i.e. the size of the challenge set must be equal to or larger than 24).

Furthermore, the security concern of shoulder surfing is presumed to be not an issue for mobile devices; given that mobile devices provide the freedom of mobility, users can choose a safe location to execute authentication.

Mobile input interface

Today, most mobile phones are designed with a standard 12 button keypad and along with other function keys (e.g. soft keys) for user commands (see Figure 0). In this study, our graphical authenticator is designed for mobile phones with this keypad layout.



Figure 0. An example of the standard mobile keypad

Display, layout, and choice selection

As discovered previously, the size of the challenge set must be equal to or greater than 24, which means 24 images must be displayed. However, due to the small sizes of mobile phone screens, not all images can be displayed at once, so the display of the images needs to be divided into multiple pages. The number of challenge set images is divided into the number of keys in a mobile keypad, i.e. twelve. Images are grouped into multiples of twelve called pages and only one page is displayed on the screen at a time. The displayed images of each page are further arranged in a 4×3 matrix grid; with each picture on the grid maps to a spatially related number key on the keypad. Hence, a user selects an image by selecting the corresponding number key.

5.1.2. Low-fidelity prototype

One of the advantages of prototyping is to work through design ideas. Often, designers make low-fidelity prototypes, such as paper-based prototypes, for them to be able to see whether their ideas make sense before discussing with others (Jones & Marsden, 2006). By carrying out ideas to paper, designers are able to see the interface of their design, and they are able to step through how their design can be used.

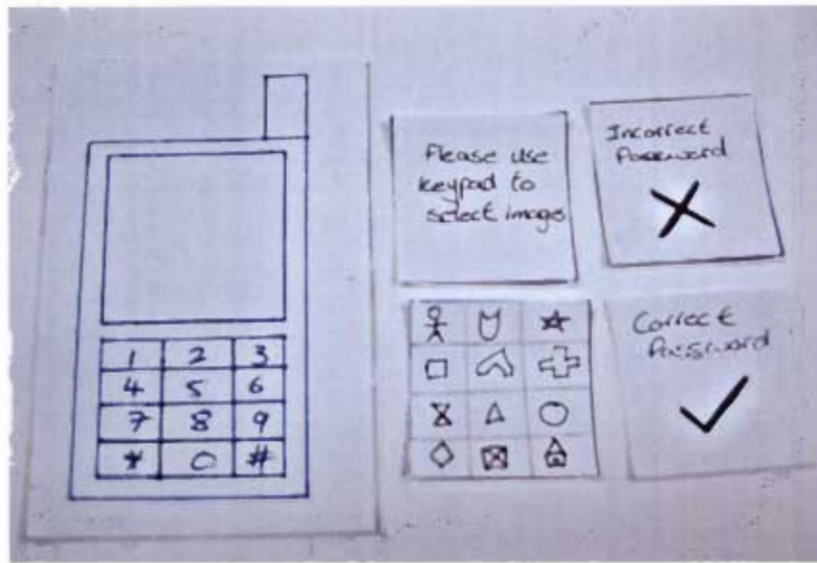


Figure 0. The paper-based prototype of our graphical authenticator

Figure 0 shows the sketches of the interface of our design; by using sketches, it allows us to outline the fundamental concept of our graphical authentication. The image on the left is used as an illustration of a mobile display, and the items on the right are the different screens; the display of each screen depends on the system status.

The paper-based prototype is for initial conceptualization; it is used as a mean for self-checking the design. The sketches show the look of the interface and moreover, we want to find out how people will interact with the interface. For this, slideshow software is used to demonstrate how the prototype can be used. We used PowerPoint to build a digital prototype (see Figure 0); the purpose of this prototype is to illustrate the interaction of the design; the interaction is achieved by linking different screens nonlinearly using hyperlinks.

To ensure that people can use our design, we presented the prototypes to our friends and colleagues to discuss possible flaws. The paper-based prototype failed to illustrate the authentication concept to our subjects. When the paper prototype was first shown, our subjects were sceptical because they failed to understand how the authenticator works. Only after the slideshow prototype was shown, the subjects were convinced that we are testing a new authenticator. Overall, people understand the concept of the prototype after a quick explanation and using the digital prototype. To test intuitiveness, we intended not to give a demo during the



Figure 0. A screenshot of the slideshow-based prototype

explanation; instead, we let the subjects to discover the operations themselves. Through this process, we found a usability flaw in our initial design. We discovered we have neglected the functionality of allowing users to correct a mistaken selection; only after discussions and testing, did this problem surface.

5.1.3. High-fidelity prototype

Images

In the research by Dhamija & Perrig (2000), they tested their graphical authentication system with both abstract art images and photographic images. Their findings show that users particularly prefer photographic images. Photographic images provide more realistic meanings than abstract images, which also provide better memory aids; therefore, abstract images are not used as the profile images for our graphical authentication.

Natural photographic images were initially considered. After resizing for mobile display, we discovered that most of the image details were lost; therefore, we abandoned the use of natural images. For alternatives, we considered using images of everyday objects, but later this idea was ignored; findings from Davis *et al.* (2004) have suggested that graphical password users are more efficient in using face images than object images. Consequently, we decided to pursue with using human faces as our authentication profile images.

People have an innate cognitive ability to remember human faces (Tari *et al.*, 2006). This was further confirmed by Valentine (1999); his study shows that Passfaces are very memorable over long periods. From our background investigation, it seems passwords that are made up of facial images are more memorable than alphanumeric passwords, even after long periods between logins.

In our prototype, we use a similar approach to Passfaces; we intend to use the advantage of people's ability of remembering faces. Images of people's faces are used as the profile images. Figure 0 shows the twenty four front-shot photographic images of human faces¹¹ used; twelve are males, and the other twelve are females.



Figure 0. Profile images for the graphical authenticator

User interaction

During authentication, the challenge images are displayed on the mobile screen. To authenticate, a user selects his/her recognized images (password images) by selecting the corresponding number keys, see Figure 0 for an example. Similarly, a user can press the same number key to cancel the selection.

¹¹ Images were downloaded from Computer Vision Laboratory, Computer Science Department, University of Massachusetts. The images are available at <http://vis-www.cs.umass.edu/lfw/lfw.tgz>. Last accessed: 2008-04-19

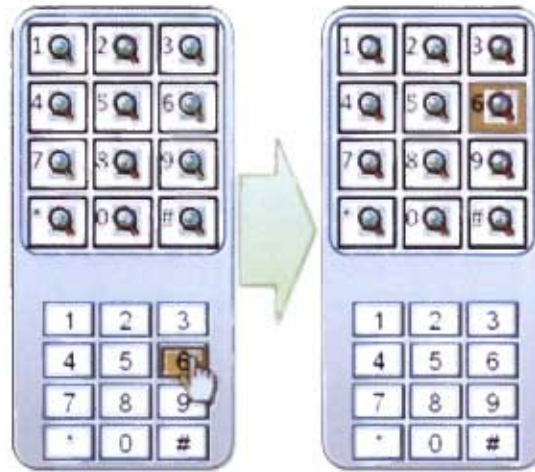


Figure 0. An example of a user input

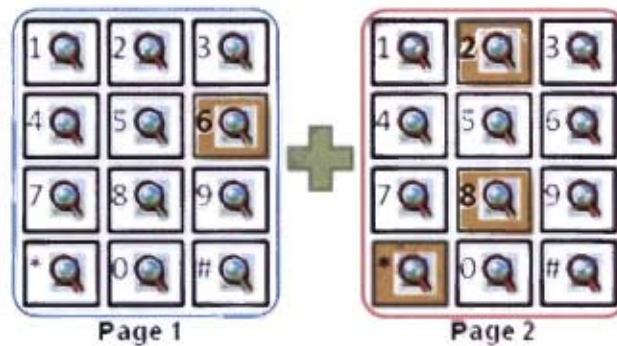


Figure 0. An example of a password entry

During the testing of our low-fidelity prototype, we discovered that if the system runs slowly the graphical feedback also runs slowly, so users often tapped the corresponding key more than once to make a selection. To improve user experience, we decided to implement a haptic feedback for user selection. After each key press, the software calls the vibrate function to shake the phone for a short period (100 milliseconds). By doing so, it helps the user to distinguish that an action is acknowledged by the system, thus preventing the user to press the same key multiple times. At the same time, we try to avoid setting the length of vibration for too long. If a user presses multiple buttons at once, the haptic feedback can turn into a senseless long vibration.

As described previously, not all images can fit onto the mobile screen at once; our twenty-four challenge set images are divided into two pages, twelve images per page. After a user has finished selecting his/her recognized images from the first page, the user scrolls to the next page

and selects the rest of the recognized images; Figure 0 demonstrate an example of a password entry.

Implementation

The graphical authentication prototype was written in Java programming language; it was implemented using Java Platform Micro Edition (J2ME or Java ME) for devices that support Connected Limited Device Configuration (CLDC) 1.1 and Mobile Information Device Profile (MIDP) 2.0. The prototype was deployed on a Sony Ericsson V630i mobile phone, with 176×220 coloured pixels display. The screen shots of the prototype are illustrated in Figure 0.

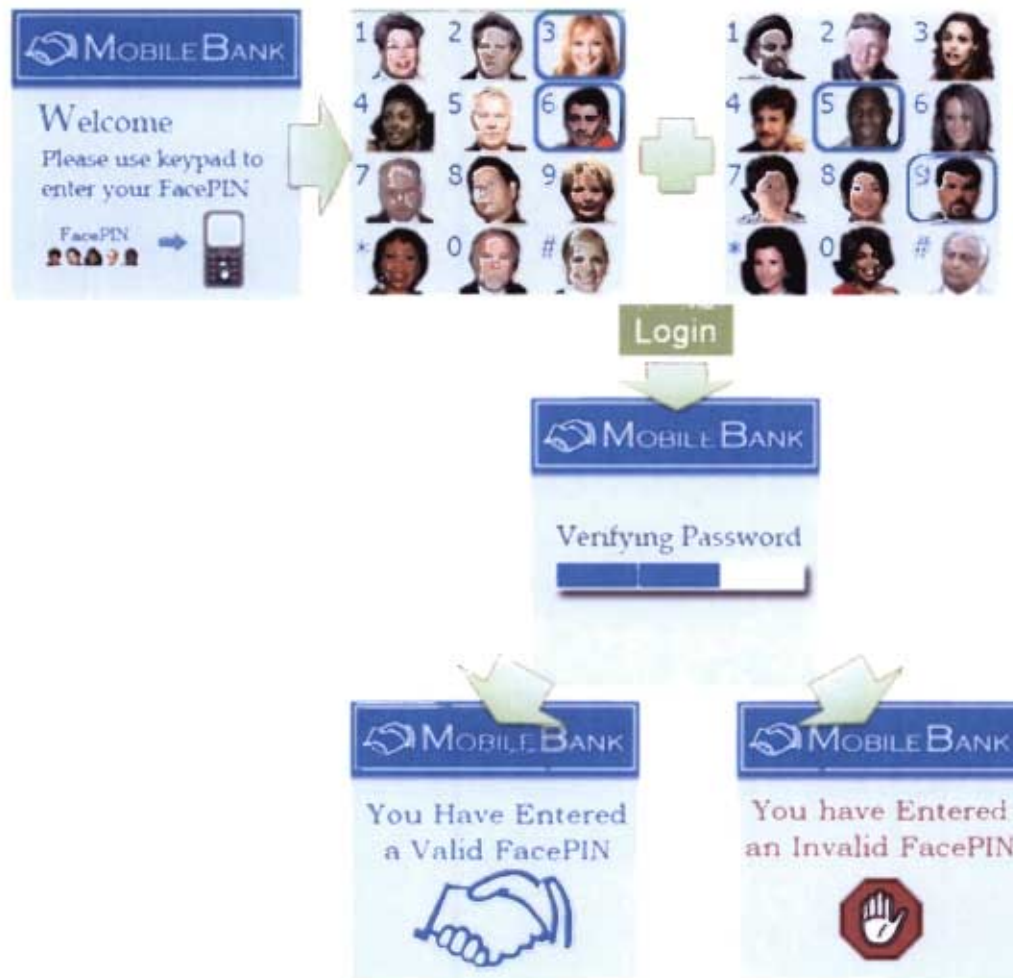


Figure 0. Screen shots of the graphical authentication prototype

5.2. Gesture authentication

In recent years, accelerometers have been increasingly integrated into mobile phones (such as Apple's iPhone, Nokia's N95, etc.). A built-in accelerometer allows the mobile device to sense users' movements and, as a result, it provides a new modality for user input. At the moment (2008), there are a small number of mobile applications which make use of this: for example, Williamson *et al.* (2007) introduced *Shoogle*, an interface for sensing data within a mobile device as the device is shaken. As more uses of accelerometers are being discovered, we confidently predict that more mobile phones will be equipped with built-in accelerometers in future.

In the design of this research, an accelerometer is used to detect directional movements as gesture inputs for user authentication for mobile devices. As a result, a novel gesture-based password authentication is created.

5.2.1. Design

Gesture password elements

The gestures used for this study are *discrete gestures*. A discrete gesture can be distinguished as a movement from a starting position to a stopping position. Here, a discrete gesture is defined as *a distinctive singular movement that can be perceived individually and not connected to, or part of another motion*. In other words, a motion that cannot be further decomposed as units of actions can be classified as a discrete gesture. Since it has the property of a discrete structure, multiple singular gesture units can be combined to form a string of discrete gestures.

A stroke-based authentication system by De Luca *et al.* (2007) introduced a new concept of using directional strokes in a two-dimensional plane as passwords. They defined a stroke-based password as made up of many horizontal, vertical, and diagonal strokes; the strokes can form specific shapes, and the shapes are suggested as mnemonics. In this study, we apply a similar concept which uses gesture strokes in a three-dimensional space as passwords. Ten discrete gestures (illustrated in Figure 0) are defined as password elements. The elements were designed based on the spatial directions of a mobile phone, and the elements were designed with the intention that each gesture must have a symmetrical gesture in the mirror direction. The *forward*

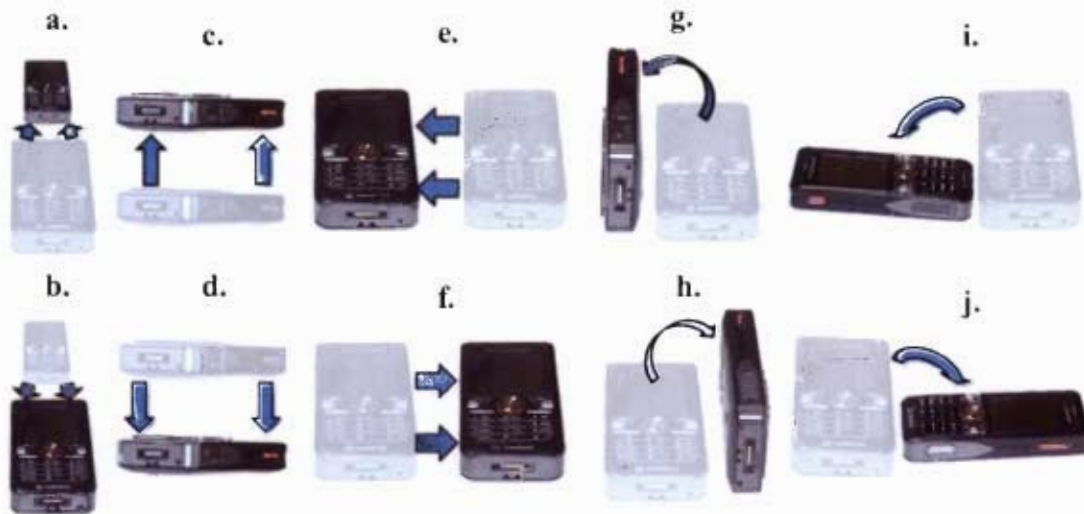


Figure 0. Gesture password elements. (a) Forward, (b) Backward, (c) Up, (d) Down, (e) Left, (f) Right, (g) Tilt Left, (h) Tilt Right, (i) Swing Left, (j) Swing Right



Figure 0. A string of tilt left gestures before adjustment. (a) Initial position, (b) Tilt left from position (a), (c) Tilt left from position (b)

gesture (Figure 0.a), for example, has a symmetrical gesture element *backward* (Figure 0.b) in the mirror direction. The symmetry is to ease the process of learning the gestures. As users learn a gesture element they can apply the reverse movement to learn the mirror gesture, thus simplifying the learning process for the users.

Due to the articulation structure of a human arm, motion is limited in certain ways. This implies that some strings of gestures could be impossible for people to reproduce. For example, when a

user holds a device perpendicular to the ground, the maximum tilting angle the user can rotate the device is about 180 degrees. Beyond that point it is uncomfortable or impossible to tilt further. Thus, a string of *tilt left* or *tilt right* is not replicable by a user (Figure 0 illustrates an example of a string of tilt left gestures. Tilting left beyond Figure 0.c is impossible). This problem manifested during our initial design stage, so a decision had to be taken that after each element entry, the device must be moved back to its starting position; hence the next element entry must start from the initial position. As a result, a valid password element entry is a string of paired discrete gestures, where a given pair is made up of a gesture element and its reverse.

User Interaction

A gesture entry is entered as a movement that starts and stops in the same position. A complete gesture is defined as the change of state from a motionless state to a moving state and then a motionless state to identify the end of the gesture. Consequently, for the system to register a motionless state, the user needs to pause between each gesture elements during password entry.

Security

A *string* is an ordered list of elements in which the same elements can appear multiple times at different positions. In this study, a *gesture password* is defined as a string of multiple gesture elements. For a user to authenticate, that user is required to produce a string of gesture password elements in the correct order, which means gesture passwords are permutation based. Since the system supports ten different gestures and it uses permutation, gesture passwords have the same password space as standard 10-digit PINs. Thus, in theory, both have the same security. However, gesture passwords have a weakness against shoulder-surfing; as a user enters a gesture password, his/her action can be recorded easily. For this reason, we recommend our gesture authentication to be used in a secure environment.

5.2.2. Low-fidelity prototype

In the design of our gesture authenticator, we used low-fidelity prototyping to test out our initial ideas. The objective of this prototype is to illustrate a new approach of interaction for password entry. Since the design is based on motions, we outlined the design through actions with aids of paper sketches; the images shown in Figure 0 are used as the paper aids.

In this prototype, we also tested with friends and colleagues. We first introduced the prototype as a motion-based authentication. At the start, our subjects failed to understand how motions can be used as a password system; only after we explained the design using the analogy of motion signature, the subjects began to understand the objective. For our testing, we provided a block of a rectangular object (we used our mobile phones), and we explained to the subject that the object represents a motion sensing device. We showed the subjects a list of gesture password elements (shown in Figure 0), and we requested the subjects to reproduce the listed elements. All of our subjects reproduced the single directional gesture elements (Figure 0.[a-f]) without problems, however some of the subjects had trouble interpreting the movements of the gestures that have turning motions. After illustrations, the subjects understood those motions.

To test the usability of password entries, we requested our subjects to enter gesture passwords; the passwords are chosen randomly by the illustrator, and each password is made up of four gesture elements. At first, the subjects experienced difficulties linking gesture elements; after a few practices, however, their movements became fluent. At the end of the session, most subjects can produce a string of gesture elements without much focus on the action.

5.2.3. High-fidelity prototype and implementation

Hardware and connectivity

Due to hardware availability, a Sony Ericsson V630i mobile phone was used for our prototype. However, this model does not support motion sensing function. To detect motions, we used a sensor called Sun SPOTTM (see Figure 0), manufactured by Sun Microsystems. As a result, we used the combination of the mobile phone and the Sun SPOT to simulate a mobile phone with a



Figure 0. Sun SPOT (Small Programmable Object Technology). Left: a base station (or a transceiver); right: a sensor board

built-in accelerometer. The Sun Spot is made up of two components: a sensor board, which has built-in accelerometers for motion sensing; and a base station, which is used for receiving data from the sensor.

According to the theory of operation document (Sun Microsystems, Inc., 2007), the Sun SPOT communicate via the wireless IEEE 802.15.4 protocol, and the base station communicates with a computer via the USB interface. There is no possible direct communication between a mobile phone and Sun SPOT components. Therefore, an external component is needed to bridge a connection. For this reason, we adopted a solution of using a computer with Bluetooth connectivity to bridge the connection. Figure 0 illustrates the setup of the connections. When a gesture is entered, a Sun SPOT sensor detects the motion data. The data is transmitted wirelessly to the base station and pushed onto the computer for processing. The computer translates the received data into one of the predefined gesture elements. Once it is translated, the result is sent via a Bluetooth connection to a mobile phone for display. Through this setup, the mobile phone and the sensor can be used as a single entity.

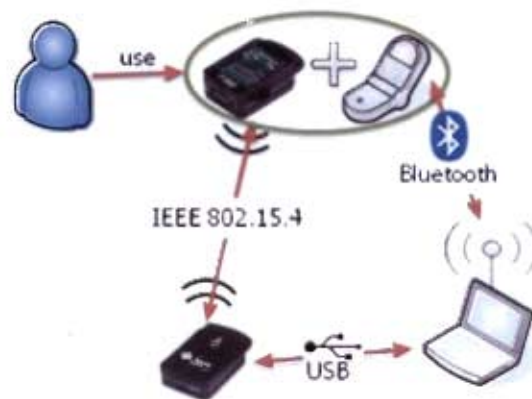


Figure 0. Connections between components

Sensor data acquisition

As described previously, the gesture motions are captured by a Sun SPOT sensor unit. The data transmissions between the sensor and the transceiver units require a communication protocol. In our prototype, we adapted the protocol from the *Telemetry* demo application written by Sun Microsystem for our purpose. Similar to Mayrhofer & Gellersen's (2007) pre-processing tasks,

sensor data is assumed to be available in the form of time series of acceleration values in three dimensions. The sensor samples acceleration data every 5 milliseconds (a sample rate of 200Hz), and the sampled data is broadcasted to the transceiver wirelessly.

Pre-processing

Human hands are never completely motionless; different joints such as fingers, wrists, and elbows often twitch unawares. Similarly, when a user holds a sensor, the sensor often detects slight movements from small twitches. For example, a slight body shiver can cause the sensor to detect unintended acceleration data. In general, the acceleration of an unintentional movement is either lesser than an intended motion, or the duration of the motion is shorter. To eliminate those unintended readings, a filter is used to pre-process the captured motion data. To do so, we used thresholds; each direction of the three axes is assigned a threshold (i.e. there are six threshold values). Acceleration values that are less than the preset thresholds are considered unintentional, thus it is ignored; conversely, values that exceed their thresholds are accepted.

To find the optimal values for the thresholds, we tuned the thresholds with people; for quick accessibility, we ran tests with our colleagues. We asked our colleagues to hold the sensor, and requested them to twitch their fingers or their wrists while holding the sensor; the idea of this is to simulate unintended movements. Although we cannot test for every possible twitches and shivers, at the end of the tests, the results show that the appropriate threshold values are between from 40% to 50% of the standard G-force (gravity).

Furthermore, from the results, we discovered that the duration of an unintended movement is relatively shorter than an intended movement; therefore, a filter was used to eliminate unwanted noise in the data.

Matching gesture features

The gestures used for this prototype are based on directional movements. When a user enters a gesture, he/she moves the sensor in the directions of the gesture; when the sensor is moved, the directions of acceleration are changed. The change of directions is used as movement features for matching gesture elements. For example, using the spatial orientation shown in Figure 0 as a reference, when an “Up” gesture is entered, the acceleration of the sensor changes; the direction



Figure 0. Spatial orientation representation of a mobile phone

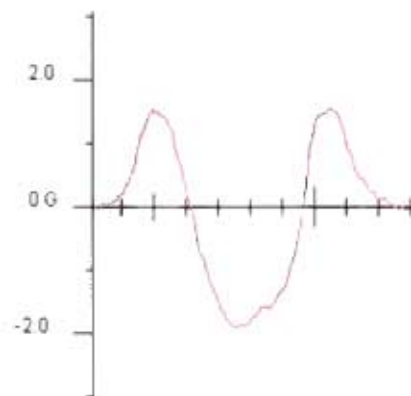


Figure 0. An acceleration wavelet representation of the “Up” gesture element

of the Z-axis acceleration fluctuates from positive to negative and then back to positive again (see Figure 0 for a wavelet representation).

The concept of matching the changes of acceleration is used to translate input data to gesture entries. For example, the change of direction of the “Up” gesture (see Figure 0) is “+ to – to +” on the Z-axis; if an input has the similar features, the input is classified as an “Up” gesture entry (refer to Appendix B for the list of features of the gesture elements). However, if the input data does not match any of the predefined entry, then the input is considered as an unknown input.

Display

For every gesture input, the computer processes the input data, and the results of the processed output are pushed onto the mobile phone for display. If the data matches one of the predefined

gestures, the corresponding image of the gesture (one of the images of Figure 0) is displayed. However, if the data does not match any of the predefined elements, then an “unknown gesture” sign is displayed on the mobile phone.

A mobile application is built for displaying the detected gesture inputs. The application is written in Java programming language, using the Java ME platform, and it runs on a Sony Ericsson V630i mobile phone which supports CLDC 1.1 and MIDP 2.0 environments. As shown in Figure 0, the mobile phone and the computer are communicated via a Bluetooth link; the Bluetooth connection is implemented using JSR 82 specification Bluetooth library, and we used the RFCOMM protocol to emulate a serial connection between the components.

Refined user interaction

In our initial design of the system, we displayed a notification on the screen to denote that a gesture had been detected. During preliminary user testing, however, we discovered that users often do not check the display information after inputting a gesture element. For this reason, a haptic feedback (i.e. a short pulse of vibration) is used to inform the user that the system has detected an input.

5.3. Chapter summary

Two mobile authenticators were introduced in this chapter; each of them exploits a human memory system for password memorability. The graphical authenticator uses combinations of visual images as passwords, and the gesture authenticator uses strings of motion elements as gesture passwords. In addition, prototypes of the authenticators were implemented and the details of the design and implementations were reported. The designed prototypes are used for evaluations; details of the evaluations are described in the next chapter.

Furthermore, the gesture password system is a novel design of password authentication. The design explored the use of accelerometer to detect discrete gestures as password elements. Gesture password is different compared to the systems in Patel *et al.* (2004) and Mayhofer & Gellersen (2007); while their authentication systems are for pair devices gesture password was designed for remote password authentication to a server.

6. Evaluation

Before we proceed further, we need to clarify what we mean by *usability*. In HCI, usability can be measured both quantitatively and qualitatively. However, the term “usability” is arguably vague and often misunderstood. ISO 9241-11 (1998) defines usability as “*the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.*” Usability can refer to the convenience of use of a product (i.e. quantitative – efficiency and effectiveness); whilst, the term can also refer to the enjoyment and the user experiences created from using a product (i.e. qualitative – satisfaction). In this chapter, the term usability is interpreted as the ease of use, the accuracy of use, and the user confidence in the product.

Having arrived at the stage of prototypes, it is time to ask the question of whether the prototypes offer any improvement over the existing system – PIN authentication.

In the previous chapters, we described the process of designing prototypes with usability in mind. However, the process can often mislead designers into thinking their prototypes are usable. Designers can create the most usable system and then expect users to use it in their most natural behaviours; however, users often do not do as expected and they are ingenious at doing the unexpected (Jones & Marsden, 2006). So, without testing with actual users, designers cannot be certain that their prototypes are indeed usable by the intended users. To confirm usability, evaluation is needed to understand how a product or a prototype is (or will be) used by its intended users. In other words, evaluation is a process of testing (or confirming) products’ usability. Evaluation is an essential part of the interaction design process; it collects information about users’ experiences when interacting with a prototype (Sharp *et al.*, 2007), and the information are analysed to understand the merits and the weaknesses of the prototype.

6.1. Background

Interaction design is a method of designing for a group of intended population. One of the key aspects in its evaluation process is involving the appropriate users that represent those for which the prototype was designed (Sharp *et al.*, 2007). Without involving the correct users, the entire

evaluation is invalid; thus, it is important to screen subjects before the evaluation takes place. This is to ensure the selected subjects are able to represent the intended population.

As previously mentioned in the methodology chapter (Chapter 3), the approach we adopt for evaluating is experimental evaluation. The intention of this approach is to determine objective truth, a truth that is independent of biases or prejudices (Jones & Marsden, 2006). Essentially, the approach involves finding the correct data that can represent the general outcomes as accurate as they possibly can be.

Experimental evaluation is essentially a method of measuring variables to find an answer to a question; it is important to know the questions to be answered beforehand. The questions are represented in the form of hypotheses. Through studies, hypotheses are (dis)proved by the results of those studies. The hypotheses we are answering were specified previously (in Chapter 3), and, as a recap, they are the following:

H1: Users prefer to perform m-banking authentication in private environment than in public environment.

H2: Users perceive better initial trust in using PINs for m-banking authentication than using other authentication techniques.

H3: Multiple graphical passwords are more memorable than multiple kinesthetic (gesture) passwords or multiple PINs.

Multiple graphical passwords have been shown to be more memorable than multiple PINs by Moncur and Leplâtre (2007); however, the type of password they used was permutation-based, where the order of password entry affects the correctness of the password. In this research, the type of graphical passwords examined was combinational, where the order of entry does not affect the password accuracy. As a result, H3 is further refined as:

H3: Multiple combinational graphical passwords are more memorable than multiple gesture passwords or multiple PINs.

Evaluating usability in terms of password memorability (i.e. H3) is through the measure of accuracy; this is determined by the number of passwords that are correctly remembered.

However, evaluating authentication systems designed for trust (i.e. H2) is challenging as success is not defined in terms of accuracy or efficiency, but in terms of satisfaction and confidence. Unlike time or correctness, trust and confidence cannot be quantified because there is no unit to indicate levels of trust. Instead, trust is measured on a referenced scale and through a comparison between the testing units. For example, it is valid for a user to claim that he/she (dis)trusts system A more than system B; in this case, system B was used as a reference to compare trust in system A. In this project, the most widely used authentication system – PIN authentication – is used as a reference system.

Experimental evaluations produce quantitative results (i.e. results that can be represented in numbers). Through analysing the results, comparisons amongst the testing systems can be made. Results from an experimental evaluation are scientific rigorous; they cannot represent qualitative measurements, such as user experiences. To reflect user experiences, a process of collecting qualitative data is required to evaluate how users feel about a product.

There are many methods that collect qualitative results; however, some of the methods cannot capture data such as user trust and confidence. For example, the direct observation technique collects qualitative results; however, researchers cannot analyse user trust by observing recorded data. Without speaking to the test subjects, the researchers are never able to understand how the subjects actually feel. What is needed is an approach that allows the researchers to ask questions that give results that can represent user trust. There are two techniques that suit this purpose: *questionnaire* and *interview*. The interview technique is a flexible approach – i.e. it covers more ground, but it also creates a risk of the interviewer pursuing the wrong issues, which can lead to critical information being missed (Jones & Marsden, 2006). The questionnaire technique is more suitable for the purpose of this research; this technique garners user opinion through a list of carefully designed questions. Unlike interviews, questionnaires are inflexible, so it is important to design good questionnaires which give results that are suitable for the study.

6.2. Study 1 – User experience

A banking system can be made as simple as possible; however, if users do not trust the security of the system, they would feel vulnerable to use it. Users perceive trust in a system by examining

its superficial cues; when adopting a new system, users need to see signs of protection for them to build initial trust in the system. Using the example in Marsh (1994, p.1) – the example with the broken car driver and the mechanic (refer to Chapter 2 page 18 for details), the driver requires enough superficial cues to accept help from a stranger. Likewise, in banking, users need sufficient superficial cues of security to generate trust to adopt a new remote banking system. Therefore, in this study, we are interested in finding an authentication system that demonstrates best superficial cues for users to accept it for mobile banking.

Another factor that influences trust is the physical environment where the authentication system is used. Sasse *et al.* (2001) have pointed out that users feel security mechanisms are meaningless if the surrounding environment has noticeable flaws. As a result, we are confident to predict that users would prefer to perform logins in a private environment, which limits the advantage of mobile banking – able to transact anywhere. Although we can safely assume private environment is the preferred atmosphere for mobile authentication, so far, there is no study that we found which confirms this conjecture. Therefore, we initiated a study of users' awareness of their surrounding context while conducting mobile logins.

The aim of this study is to understand user experience of using the designed authentication systems. In addition, we are particularly interested in finding a type of authentication system that generates best initial trust perceived by users. To test the above, a user study was conducted.

6.2.1. Method and procedure

Prior to the study, we anticipated there will be communication problems due to language differences. Although English is the primary official language in South Africa, it is not the native spoken language in most low-income households. In the Cape Town region, the most common native language is Xhosa. Unfortunately, the researcher of this study is not fluent in Xhosa; to overcome the expected language obstacle, a facilitator was hired to translate during the study. Before the experiment, the facilitator was trained and explained the procedures of the experiment, and during the experiment, the facilitator was the main communicator with the subjects, while the researcher supervised.

6. EVALUATION

To be consistent with the user profile of this research, participants were recruited from a low-income housing region in Cape Town. Learners from a skills training centre in Khayelitsha, Cape Town, were recruited as participants for this study. The study took part during their class hours; therefore each subject was offered R50¹² for remuneration. Before the subjects took part, they participated in a screening process; the purpose of the process is to ensure the subjects fit the user profile.

Participants' familiarity with PINs may influence their trust in the testing systems. For this reason, during recruitment, we aimed to balance between PIN and non-PIN users. However, due to the high mobile penetration rate, most participants we found already have the knowledge of using PINs.

The study was conducted with each participant individually. It began with an introduction explaining the purpose of this study to the subject, and during this period, consents from the subject were collected.

To compare user trust between each system, the participants are required to experience all the testing systems. To do so, the *within-group* study approach was adopted. The subject first undertook a training session to get familiarized with the three testing systems (see Figure 0). To counter learning effect, the order in which the systems were presented was rotated for each new participant. The training session ended when the participant indicated that he/she was comfortable of using all the authentication systems.

An unforeseen problem occurred during the training session. We noticed that many subjects were unable to enter a gesture password using our implemented prototype. This was not expected as during the preliminary testing with our colleagues they were able to enter gesture passwords. After an examination, we discovered the reason of failure was due to the speed of the gesture entries; the gesture movement speed of the experiment subjects was significantly slower than our colleagues (we suspect this was caused by the subjects' nervousness during the experiment and

¹² Rand, the South African currency.



Figure 0. One of the participants getting trained by our facilitator

their unfamiliarity of using a new interaction system). This deficiency forced us to abandon the use of our implemented prototype, and, instead, the validation of gesture password entries was performed manually by the facilitator; as a result, the “*Wizard of Oz*” method was adopted (Sharp *et al.*, 2007).

“*Wizard of Oz*” (or *OZ* paradigm) is a prototyping technique used in experiments. During an experiment, the user interacts with a prototype, while the facilitator (the “wizard”) simulates the processing and response of the prototype to the user. One could argue that the study is biased since the gesture passwords were not validated using a software system; however, whether using a person or software, the objective of the validation remains the same. The role of the authenticator was to capture and process the movement directions of gesture entries, and then give a binary response (correct or incorrect) of the validity of the entries to the user. Any invalid password elements were not revealed by the facilitator; it was up to the subjects to discover the invalid elements themselves.

Task 1

After the training session, the subject was given a task of entering passwords in a private area. In this task, the subject was given five passwords for each system, and the subject was requested to

6. EVALUATION

enter those passwords. To replicate existing PIN mechanism, the number of permit attempts was limited to three (Brostoff & Sasse, 2000), i.e. the “three strikes” policy; after a third failed login, the password was deemed as not enterable by the subject. During the password entries, the time taken to enter each password and the number of attempts were recorded. The data is later used for analysing the efficiency and the effectiveness of the testing systems. After accomplishing the task, a questionnaire (see Appendix C) was conducted to collect data on the subject’s first impression of using the systems.

Task 2

To test context awareness, we intended to let the subject experiences entering passwords in a public environment. As a result, the subject was moved to an open environment; the chosen location was the sewing workshop area in the training centre (see Figure 0). Prior to the study, the facilitator was instructed not to mention to the subject that they were moving to a public environment before/during the transit. This is crucial as we do not want the subject to be aware of their surroundings because he/she was explicitly told; instead, we want to find out if the subject acknowledges his/her surroundings autonomously.

For this task, a new set of passwords was given to the subject, and the subject entered the



Figure 0. The sewing workshop area

passwords in the new environment. Afterwards, the subject completed a second questionnaire (see Appendix C) which records the subject's experience of using the system in an open environment and his/her confidence of using the systems.

In one part of the questionnaire, the subject was given a scenario of using the authentication systems for mobile banking, and then the subject was asked to rank amongst the systems in the order of preferences and trust – 1st for the most preferred/trusted system, and 3rd for the least. In addition, to learn the level of trust perceived by the subject, the subject was requested to rate his/her trust in each of the systems on a 7-point Likert scale.

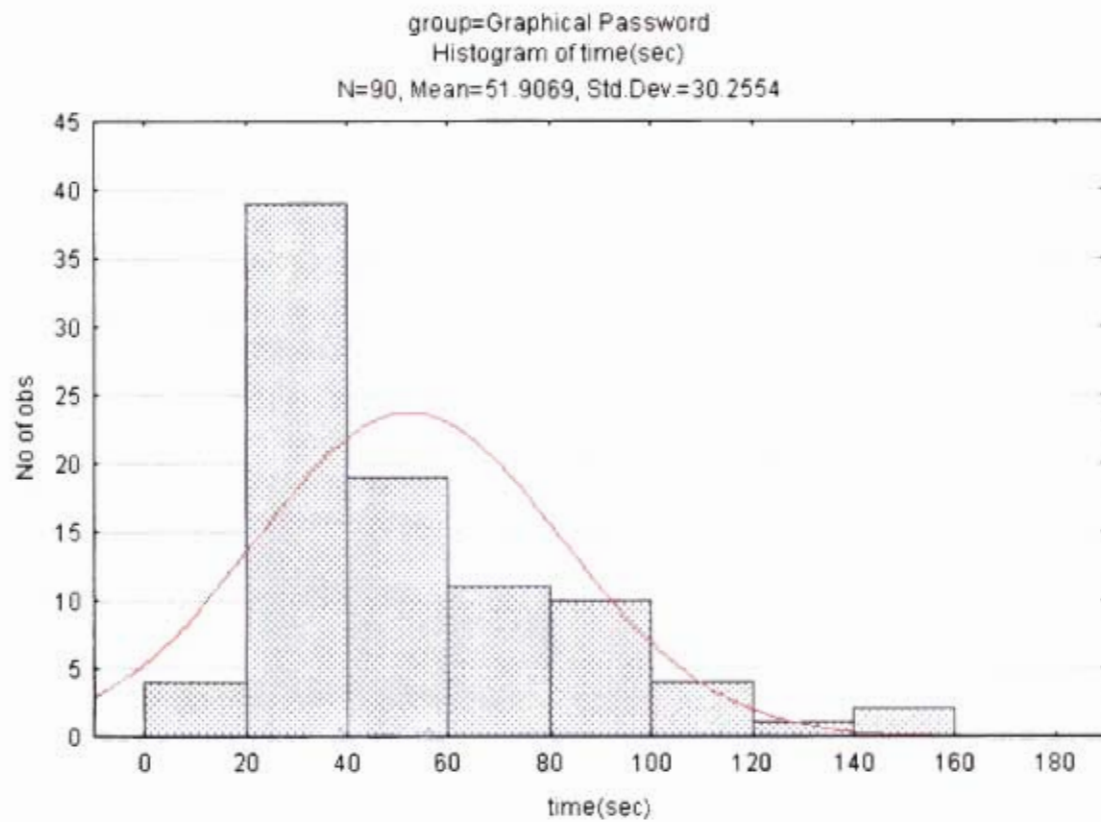
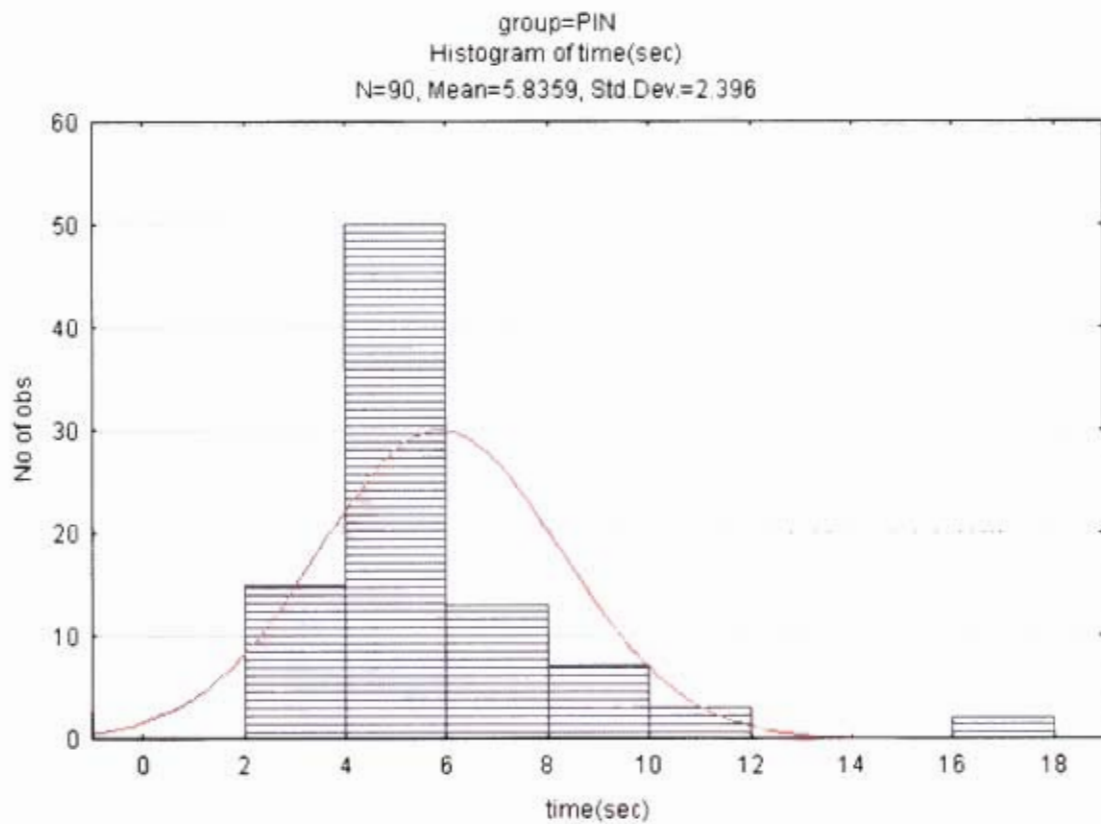
6.2.2. Results¹³

Eighteen participants were recruited to take part in this study. The demographics of the participants are adult learners from the skill training centre: two were male and sixteen were female (initially, we intended to balance the gender differences, but we were not able to recruit more male participants, as most of the learners from the woodwork class, which consist of male learners, were on leave). The age range of the participants is from 17 to 33, with a mean age of 24.4.

In the first task, a total of 270 password entries were tested (90 entries per system) (the results are shown in Table 1 of Appendix D). Within those entries, two gesture password entries were entered using more than 3 attempts, thus, under the three strikes rule, they were considered as invalid. Figure 0 illustrates the histograms of the time taken for the password entries of each system and Figure 0 illustrates the mean plot of the time.

¹³ See Appendix D for the raw data collected during the experiment

6. EVALUATION



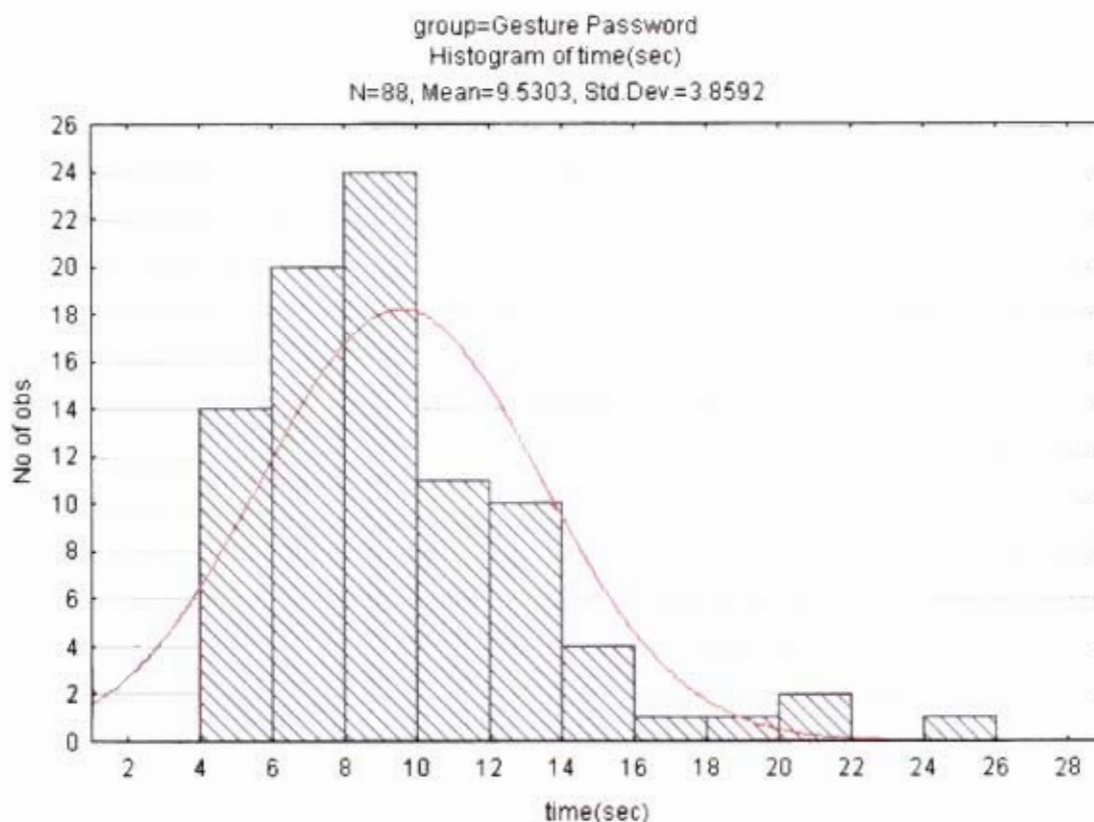


Figure 0. Histograms of password entry time

Efficiency

Efficiency of the password system was measured as the time taken to enter passwords (note: the time taken by the subjects to enter gesture passwords was captured by the facilitator, thus a slim margin of errors may be caused by human delays). A Repeated Measures of Analysis of Variance (ANOVA) was used to analyse the data; this kind of analysis is commonly used for repeated measures designs (Howell, 1982), i.e. within-group experimental designs. A Repeated Measures ANOVA across the three systems revealed a significant difference [$F(2, 174)=201.05$; $p<0.0001$]; this suggests that at least one mean is significantly different from the others (based on inspection of Figure 0, we can suspect the mean of the graphical password group shows a significantly difference). To further examine, a Newman-Keuls post-hoc comparison revealed that the differences between PIN/Graphical and Graphical/Gesture were significant ($p=0.000022$ and $p=0.000009$ respectively); however, the difference between PIN/Gesture was not significant ($p=0.156103$). In other words, the results indicated the participants took less time (i.e. more

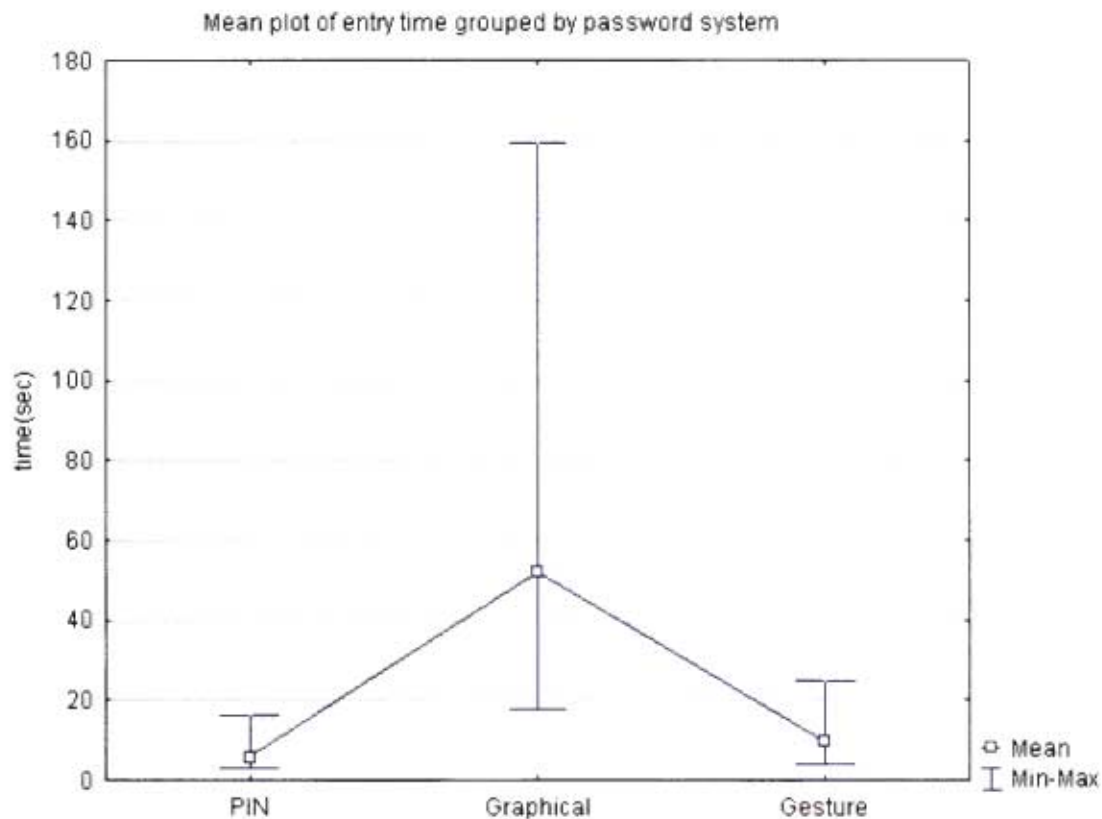


Figure 0. Mean plot of the password entry time

efficient) to enter PINs or gesture passwords than to enter graphical passwords; whilst, the time difference between entering PINs and gesture passwords is inconclusive.

Effectiveness

In this research, effectiveness is interpreted as the ability of reproducing passwords correctly, and it was measured as the number of attempts the participants took to enter passwords correctly, i.e. a system with lesser attempts indicates good effectiveness. The recorded data is represented in Figure 0. To analyse the data, Chi-square tests were used to confirm significances. An overall test on the results of the three systems showed a significant difference [$\chi^2=53.418$, $df=6$; $p<0.001$]. Further analysis revealed the differences between any two password systems were significant [PIN/Graphical, $\chi^2= 6.068$, $df=2$, $p <0.05$; Graphical/Gesture, $\chi^2= 22.789$, $df=3$, $p<0.001$; PIN/Gesture, $\chi^2= 42.841$, $df=3$, $p<0.001$]. In other words, the error rate is significantly

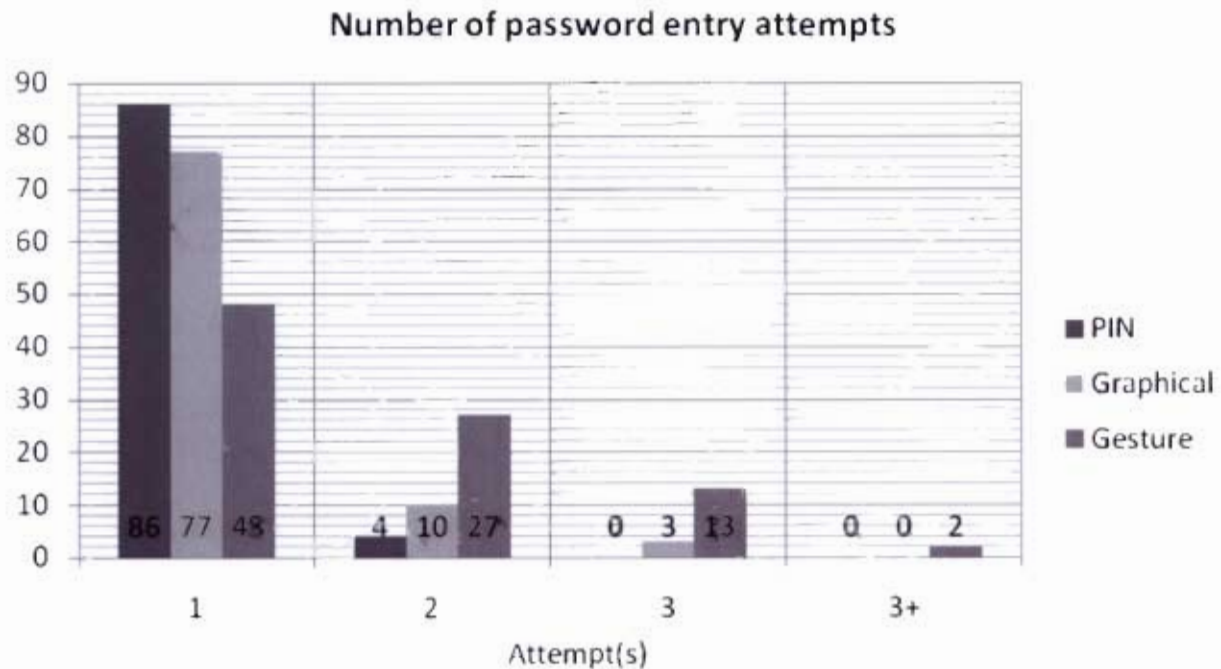


Figure 0. Histogram of password entry attempts

highest when the subjects entered gesture passwords, whilst they entering PINs achieved the least errors.

Satisfaction

Satisfaction was measured as the users' experiences of using the systems. To understand user experience, questions on the subjects' perceptions of the systems were asked in the questionnaire; those questions were categorized as the following: *first impression*; *ease of learning*; *comfort of use (in private area)*; and *ease of password entry*.

The participants were requested to indicate their perceptions on a 7-point Likert scale (7 as the most positive). The results showed that PIN has the highest mean scores across all categories (see Table 2 of Appendix D), whilst gesture password achieved the lowest. To analyse those data, a nonparametric alternative to Repeated Measures ANOVA, called Friedman ANOVA, was used. The analysis demonstrated not all the differences across the categories were significant (Table 0 presents the results of the analysis). The results revealed that the participants' first impressions of the PIN system were significantly better than their first impressions of the gesture

Table 0. Significance of differences of user experience between the password systems

Category	Friedman ANOVA	p	PIN/Gra.	PIN/Ges.	Gra./Ges.
First impression (UX1*)	(N=18, df=2) = 10.67	<i>p=0.00483</i>	p=0.05778	<i>p=0.00389</i>	p=0.08327
Ease of learning (UX2*)	(N=18, df=2) = 13.90	<i>p=0.00096</i>	<i>p=0.02535</i>	<i>p=0.00091</i>	p=0.05220
Comfort of use (UX3*)	(N=18, df=2) = 5.21	p=0.07375	-	-	-
Ease of entering password (UX5*)	(N=18, df=2) = 9.80	<i>p=0.00745</i>	<i>p=0.00815</i>	<i>p=0.00270</i>	p=0.76302

Significant values are shown in ***bold and italic***

*labels in brackets correspond to the labels in the questionnaire

password system. Furthermore, the participants perceived PINs were the easiest to learn, as well as the simplest to enter amongst the three systems. This outcome may be biased towards PIN, as most of the subjects were previously exposed to PIN authentication. Due to the high mobile penetration rate, it is rare to find users who were not exposed to PIN.

In addition, four subjects have indicated that they felt frustrated when learning/using the gesture system. The subjects explained the main causes of their frustrations were due to confusions of the directions as well as their unfamiliarity with the interactions of moving a mobile device. Two subjects indicated that they felt frustrated while using the graphical password system; they pointed out that their frustrations were caused by confusions amongst some of the pictures due to their similarities.

Overall, most of the subjects reported they enjoyed learning/using all three of the systems. One subject specifically indicated to the facilitator that she enjoyed using the gesture password system because “the experience was like playing a game”.

Context awareness

After the second task (entering passwords in an open environment), the subjects were asked to indicate their awareness of their surroundings. Seventeen out of the eighteen subjects indicated that they were aware that other people were watching them while they were entering passwords. This indicates that the subjects acknowledged their surrounding environment by themselves without the facilitator specifically describing their surroundings.

A question (CA3 of the questionnaire) on the subjects' perception of the difficulties for others to record the passwords was asked, and a 7-point Likert scale was used. The mean values of the responses (means: PIN=5.28, Graphical=6.33, Gesture=4.78) indicated that the subjects feel graphical passwords were the most difficult for other people to record, whilst gesture passwords were the easiest. A Friedman test showed that the differences between the groups were not significant [ANOVA Chi Sqr. (N=18, df=2) = 5.782609; p=0.05551]. Even though the averages appear to be that the subjects feel graphical passwords were more difficult to record the analysis showed the results were not significant enough to support the argument. However, the p-value of the calculation is marginally closed to 0.05, thus increased in the sample size may show a significant difference.

Surprisingly, the results showed that the subjects were more comfortable (or less awkward) entering gesture passwords in public environments than entering the other types of passwords (means: PIN=6.33, Graphical=5.89, Gesture=6.94). A Friedman test showed that there is one or more differences between the groups were significant [ANOVA Chi Sqr. (N=18, df=2) = 7.304348; p=0.02594]; further tests confirmed the differences between PIN/Gesture [ANOVA Chi Sqr. (N=18, df=1) = 4.0; p=0.0455] and Graphical/Gesture [ANOVA Chi Sqr. (N=18, df=1) = 6.0; p=0.01431] were indeed significant. It supports the assumption that the subjects felt more comfortable entering gesture passwords in public than using the other systems in public. Unfortunately, using the data that we have, we cannot confirm a reason. We speculate the reasons for this could be because the subjects prefer display-less login system when authenticating in public area, or perhaps the subjects prefer to use a movement-based application in public. For whatever the reason, further research is required to understand this anomaly.

Besides comfort (or awkwardness), we asked the subjects about their perceptions of whether the password systems are secure enough for logins in a public area (see CA4 of the questionnaire). The results show the subjects generally felt secure to use any of the systems, however, a Chi-square test [$\chi^2 = 5.147$, df=4; p=0.273] revealed that the data were not significant to support this argument. Similarly, the subjects were asked to identify their preferences of their locations for logins (a choice between "private", "public", or "either"). A majority responded "either" for the PIN (10 out of 18) and the graphical password (13 out of 18) systems; however, in the case of the

gesture password system, majority (11 out of 18) responded that they preferred to use it in a private location. A Chi-square analysis [$\chi^2=8.70$, $df=4$; $p=0.069$] revealed that the data is not significant enough to make an conclusion about the differences between the groups¹⁴.

User trust

This section of the questionnaire asked questions regarding the level of trust the subjects had in each of the testing password systems, specifically for mobile banking authentication. During the experiment, the facilitator explained a scenario of using the password systems for mobile banking; however, some of the subjects could not understand the concept of how a mobile phone connects to a bank. So, for those whom could not understand the concept, we used a new metaphoric scenario. Instead of mobile banking, we told them that the password systems was designed to be used for safeguarding a vault with valuable items; to gain access into the vault, he/she must use the password systems to authenticate him/herself. Subsequently, we asked the subjects to rank and rate their trusts in the systems (the results are shown in Table 6 of Appendix D).

The results showed that the subjects rated the PIN system as their most trusted, followed by the graphical password system, and lastly the gesture password system. The averages of the systems showed there were small differences. A Friedman ANOVA test showed the differences are not significant [ANOVA Chi Sqr. ($N=18$, $df=2$) = 3.00; $p=0.22313$].

Even though the results of the ratings of trust did not yield significant differences between the groups, this does not mean the subjects' confidences in the systems are the same. The results of the rankings showed that none of the subjects had chosen the gesture password system as their first choice of security system. In fact, a Chi-square analysis of the results showed an acute p -value [$\chi^2=18.667$, $df=4$, $p=0.001$]; whilst further test confirmed that the differences were

¹⁴ Although the analysis showed a p -value (0.069) that is bigger than the α -level (0.05), the p -value is just on the other side of 0.05. We can assume this p -value as a *marginal result* (Rumsey, 2007) caused by the small sample size ($N=18$). However, for this study, we follow the data that we captured.

significant between PIN/Gesture [$\chi^2=17.143$, $df=2$, $p<0.001$] and Graphical/Gesture [$\chi^2=12.00$, $df=2$, $p=0.002$]. As a result, it confirmed that the subjects considered PINs or graphical passwords as the more secure options than gesture passwords; however, the difference between PIN/Graphical was not significant, thus no conclusion for between those two systems can be made.

6.2.3. Discussion

The results of the password entries in task 1 showed that the subjects took significant amount of time to enter graphical passwords. This is consistent to the findings in De Angeli *et al.* (2005); users take longer time to enter VIP3 (recognition-based) passwords. This confirms that users are less time-efficient in using recognition-based passwords than recalled-based passwords; this is because users must examine every picture, thus it requires longer time to process the challenge set. Also, the design of the graphical authenticator for this study has divided images into pages; this has caused the users to spend extra effort to examine images within and/or between pages, i.e. the users must go back and forth between pages to ensure the correct images are selected. It is arguable that Passfaces may show better results; since Passfaces requires its users to identify only one face-image per page, the users do not have to cross-examine between pages.

Another factor that affects the time-efficiency of a graphical password entry is the input mechanism. The prototype was designed for mobile phones without touch screen ability. Thus, for a user to enter a selection, the user first needs to identify the selecting images and their related positions, and then maps the image positions to the number keypad. As a result, this induces an extra step of mapping between the screen and the keypad.

One variable that was not recorded was the time the subjects had taken to learn to use each of the systems correctly. The reason for not capturing this variable is because it is heavily biased due to the subjects' previous experience of PINs. The performance depends on many factors such as: the clarity of the explanations by the facilitator, the fatigue level of the subjects before and during the experiment, etc. Based on observation during the experiment, the subjects took the longest time to learn gesture passwords, and we also noticed some of the subjects struggled to learn the movements of the gesture elements. This suggests some people may have problems adopting discrete gesture interaction; this would be worth exploring in the future.

The study also explored the subjects' experience of using each of the password systems. It aims to (dis)prove hypotheses H1 and H2:

The first hypothesis (H1), "*Users prefer to perform m-banking authentication in private environment than in public environment*", was not confirmed. The results of question CA5 of the questionnaire addressed this hypothesis directly. The results revealed that a majority of the subjects had no preferences of their surrounding context when using PINs or graphical passwords, thus, it refuted the assumption that the environment of entry can affect user's sense of safeness of PINs or graphical passwords. However, the majority of the subjects preferred to use gesture passwords in private areas. This indicates that the subjects acknowledged the vulnerability of shoulder surfing; this was further supported by the low mean value of the gesture password achieved in question CA3, where the subjects felt other people can record their gesture passwords in public. Therefore, context is not a factor that affects user's perception of security when PINs or graphical passwords are used; however, it is an affective factor in the case of gesture passwords. In other words, surrounding context alone does not affect user's perception of security during logins; the factor also depends on the type of the security system used.

The second hypothesis (H2), "*Users perceive better initial trust in using PINs for m-banking authentication than using other authentication techniques*", was also not confirmed. Although the results of the subjects' first impression of the systems show the difference between PIN/Gesture was significant, statistical analysis showed the differences of the level of user trust (question UT1 of the questionnaire) between the systems were not significant. Surprisingly, the data suggests the subjects' previous knowledge of PINs did not favour their perceptions of trust towards the PIN system. One possible explanation is that the colour tones we used for the display were not appropriate. Another possible factor that could have influenced trust is the gesture password prototype used; since we had to abandon the digital prototype, the prototype may have not achieved the intended effect.

6.3. Study 2 – Retention of multiple passwords

In a real world situation, people often use different applications that require user authentication, which also means those people have to memorize multiple passwords, one for each system. With

multiple passwords, people sometime struggle to remember which password applies to which authentication system. Adams & Sasse (1999) identified that having users remember multiple passwords reduce memorability, which causes users to adopt insecure practices, such as writing passwords down. Therefore, from a research perspective, it is important to investigate memorability of multiple passwords when password systems are studied.

Human memory has a limited capacity to remember the arbitrary text and number strings that make up a password. This results in password retention deficiency, and to overcome this deficiency, people select passwords to which they can attach meaning. Although memory cues help users to memorize their passwords, the passwords can also become more guessable and raise security vulnerabilities. To avoid this weakness, many security systems disallow the use of personalized passwords, generating and enforcing random passwords for their users. By adopting this policy, those systems have restricted users to memorize passwords that are less likely to attach meanings; thus, security is increased through the compromises of usability and password memorability.

In this study, we therefore restrict ourselves to the issue of retention of multiple system generated passwords. As previously mentioned, a study by Moncur & Leplâtre (2007) compared subjects' retention of multiple passwords (PINs vs. graphical passwords). Following on from their study, we investigate users' retention of multiple passwords of PINs, combinational graphical passwords, and gesture passwords. We conducted a week-long study to measure passwords retention and the strategy they used to learn the passwords.

6.3.1. Method and procedure

The aim of this study is to find a type of password that is most memorable. To test for memorability, an experiment approach is adopted. In the design of this experiment, the independent variable is the authentication system used, and the dependent variable is the accuracy of the passwords reproduced after a specified period.

Participants for this study were selected from the location as the previous study (from the skills training centre in Khayelitsha), and new participants were used. Each person was offered R60 for remuneration for their participation. The participants were informed that they were required to

attend every study session. To ensure participation, the subjects were told the payment takes place after the final study session. Similar to the previous study, each participant undertook a screening process prior to the study to ensure they fit the profile.

In this experiment, the *between-groups* study approach was adopted. The eighteen subjects were divided amongst three groups: six subjects were assigned to a group using PINs (Group 1), another six were assigned to a group using combinational graphical passwords (Group 2), and the remaining six were assigned to a group using gesture passwords (Group 3). Hence, each subject is exposed to one authentication system only.

In this study, the focus is on password memorability, specifically multiple passwords, not the implemented prototypes. Therefore, to simplify the experiment process, the experiment was conducted without using the digital prototypes; instead passwords were given to the subjects on paper. For combination graphical passwords, the authentication display (see Figure 0) was simulated on a paper printout; the subject identifies password images manually from the images on the printout; whilst, for gesture passwords, the ten gesture elements (see Figure 0) were also printed on paper. During training, each gesture movement was illustrated to the subject by the facilitator.

All subjects first undertook a training session to familiarize themselves with the allocated password system. Once the subject was familiar with the system, he/she was given three randomly selected passwords (so far, there is no literature that suggests the number of passwords which challenges user's retention ability. We estimated the number of passwords based on the number of applications: one for a mobile phone, one for an ATM card, and one for mobile banking; thus, a total of three), and each password was made up of four elements. The subjects were required to rehearse each of their assigned passwords. In Moncur & Leplâtre (2007), their participants undertook a rehearsal session by entering each of their assigned passwords correctly twice. However, we believe that entering the passwords twice is not sufficient for the subjects to register the given passwords into their memory, especially for the subjects in Group 3 to register the gesture passwords into their kinaesthetic memory. Instead, our subjects were given a 24-hour rehearsal period to memorize the passwords. To enable the subjects to have access to the passwords during the rehearsal period, the printed passwords were given to the subjects.

After the rehearsal period expired, facilitators returned to the subjects and collected the papers that contain the passwords, and the subjects were informed that the facilitators will return after a six day period. Six days later, the facilitators returned again and requested the subjects to recall (or to reconstruct) their given passwords. This was followed by a questionnaire (see Appendix C) session with the subjects to determine the methods (or strategies) they adopted to remember the passwords.

6.3.2. Results

Eighteen subjects were recruited to participate in this study. The demographics of the recruited subjects are adults: eight were male and ten were female. Their ages range between 17 to 39 years old and with a mean age of 24.9.

Fourteen of the subjects reported to have a mobile phone; three of them reported they do not own a mobile phone but have access to a mobile phone; and one subject reported of neither having a mobile phone nor have access to one.

Seventeen of the total eighteen reported to have knowledge and/or have used PIN authentication. One subject stated that she does not understand PIN authentication, and interestingly, we asked her about the security mechanism she uses to protect her phone, she said she uses the on/off button as a protection, i.e. the phone is considered secure when it is off.

Although eighteen subjects were initially recruited for this study, one subject from Group 1 had dropped out. Therefore a total of fifteen PINs, eighteen graphical passwords, and eighteen gesture passwords were tested (the results are listed in Table 8 of Appendix D). Figure 0 shows the average scores of the participants from each group.

Statistic analysis

Given the chosen experiment setup, one may be thinking of using a one-way ANOVA to analyse the data. However, the data from each population does not form normal distributions, and hence the data is nonparametric, which made this type of analysis problematic. Consequently, the equivalent of ANOVA for nonparametric data, called the Kruskal-Wallis ANOVA by ranks test, was used to establish whether the differences amongst the groups were significant.

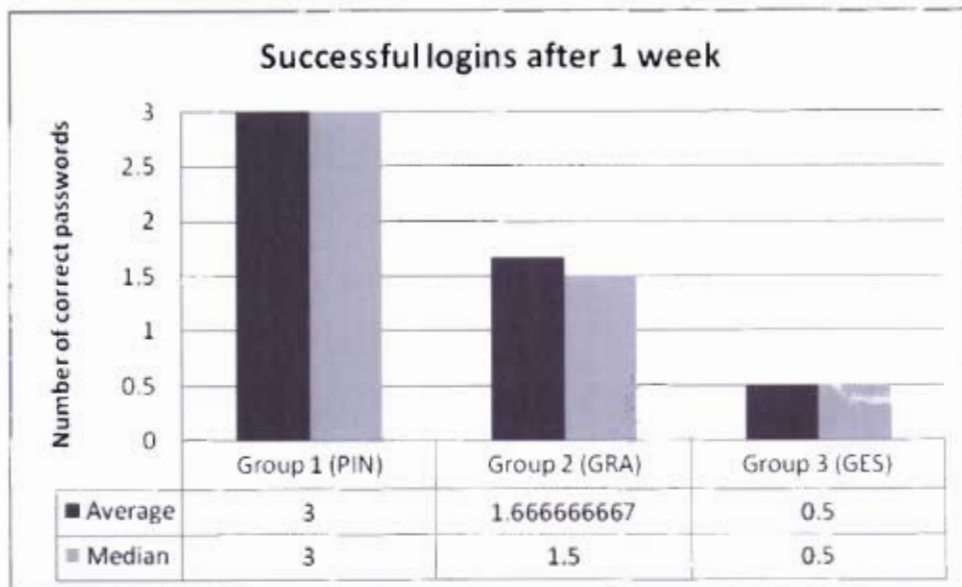


Figure 0. Correctness of passwords after 1 week

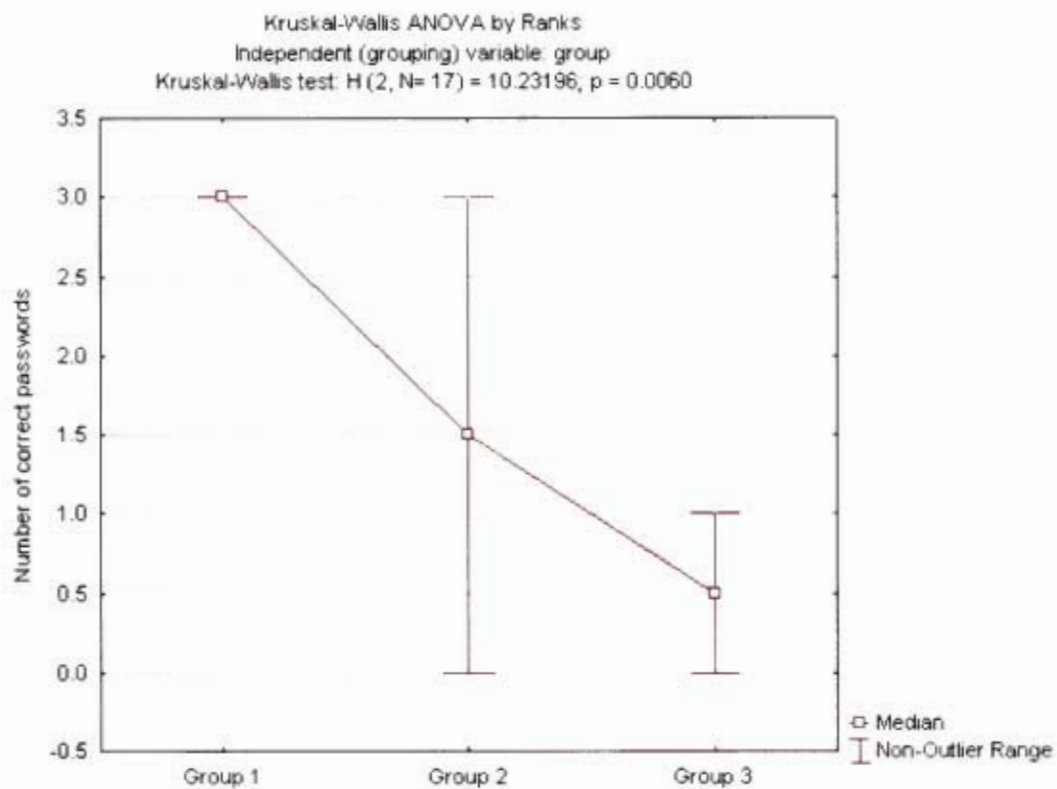


Figure 0. The results of the Kruskal-Wallis ANOVA by ranks analysis

Figure 0 shows an overall analysis on the three groups, the analysis shows an output of an acute p-value [$H(2) = 10.23196$; $p < 0.01$]; this demonstrates that the data of at least one group shows a significant difference.

Further tests reveal the difference of retention between Group 1 and Group 3 was significant [$H(1) = 8.593750$; $p < 0.01$]. This indicates that PINs were effectively more memorable than gesture passwords. The difference between Group 1 and Group 2 was also significant [$H(1) = 4.498978$; $p < 0.05$]. However, the difference between Group 2 and Group 3 was not significant [$H(1) = 3.170588$; $p > 0.05$]. These results indicate that combinational graphical passwords were not remembered more effectively than PINs nor gesture passwords, thus H3 is invalidated.

Overall, the statistic analysis of this study shows the retention of PINs is superior to the retention of both combinational graphical passwords and gesture passwords.

Errors

To understand the causes of retention failures, we analysed the data of erroneous password entries for each group. Moncur and Leplâtre (2007) classified an erroneous password could involve any of the three errors:

- *Order confusion: correct components select, but wrong order*
- *Component selected twice (or double click)*
- *Wrong component(s) selected*

The “component selected twice” factor is not relevant in this study, as the input interface used was paper-based. In addition, the type of passwords used by Group 2 is combinational, so the “order confusion” factor will never turn up in that group.

The collected data shows Group 1 achieved 100% correctness, hence, no error was made (the result excludes the data of the subject who dropped out).

The data of Group 2 shows most of the erroneous passwords (seven of the eight erroneous passwords) were caused by one wrong component, while the remaining one was caused by two wrong components. This indicates most of the password images are remembered; however,

occasional misidentifications occur which cause the passwords to be incorrect. This result implies that distinctive images are necessary for graphical password.

Whilst, the data of Group 3 indicates only three of the eighteen tested passwords were correctly remembered. Out of the fifteen erroneous passwords one was caused by order confusion; six were caused by one wrong component, three were caused by two wrong components, three were caused by three wrong components; and one was caused by four wrong components. This result shows that most of the errors were caused by wrong component(s) selected, which means users have difficulties remembering directional gesture elements.

Retention strategies

To understand the methods that the subjects had used to remember their passwords, a questionnaire on users' retention strategy was conducted.

Three subjects from Group 1 indicated that they remembered PINs through visualizing the images of the numbers. One subject said he adopted a strategy by grouping the PINs' digits into groups of two numbers. He memorizes a PIN by remembering the first two digits and then the next two digits. Two subjects from Group 1 adopted a strategy of rehearsing the numbers audibly in their mind. None of the subjects adopted the strategy of constructing a story using the given PINs, and neither did they adopt the strategy of memorising the PINs through the mnemonic of the numbers' position on a keypad. The former can be explained by the difficulty of constructing a story using only numbers, and the latter is because the PINs were given on paper, thus the subjects never entered the PINs on a number pad.

Results of Group 2 show all six subjects have adopted the strategy of remembering their password images through visualizing them in their minds. This result is expected since graphical authentication exploits people's graphical memory for password retention. Five of the six subjects indicated they tried to create mental stories using the password images. In addition, the prototype uses human faces as password images, so we asked the subjects if they have used the facial characteristics to remember their passwords. The results show race and gender are major factors that influence memorability. This is similar to the findings in Davis *et al.* (2004); users choose face images based on race and gender. Surprisingly, the questionnaire results show age is

not an influential factor. Also, four of the subjects have reported to memorise their password faces by remembering the hair-styles shown in the images. These results imply that people adopt a strategy of remembering passwords by identifying the most distinctive physical characteristics of the faces; whilst in contrast, factors that require judgement, such as age, are not applied.

The questionnaire with Group 3 reported that all six participants have practised their gesture passwords by moving their hands in the passwords' directions. Five subjects reported to have adopted the strategy of rehearsing the gesture passwords audibly by speaking the directions, and three subjects memorized the passwords by visualising the directions, i.e. the arrows of the gestures. The results show that participants attempted to use their kinesthetic memory to memorise gesture passwords through practices, in addition, some participants also adopted to use their audio and graphical memory for gesture passwords.

6.3.3. Discussion

Given the participants with the defined periods, the results show that retention in Group 1 was superior to retention in Group 2 and Group 3. The result of Group 1 could be influenced by the subjects' familiarity with PINs. Hence, the subjects have already adopted an effective strategy to remember PINs beforehand. The low scores archived by Group 3 are suspected to have been caused by the subjects' unfamiliarity of the system and not having enough time to practise their passwords. One of the subjects had explicitly mentioned to the facilitator that she needed more time to memorize the passwords. The results of Group 2 are suspected to be influenced by the choice of faces; one subject from Group 2 told us that while she was identifying the password images she found that all the faces look alike. This result shows that users require distinctive facial features to recognize password images.

Although multiple graphical passwords have been proven to be more memorable than multiple PINs, however, in this research, the use of combinations caused a negative effect. The use of combinations (while maintaining the equivalent password space as other systems) requires a large challenge set of images. As the number of pictures increases, users spend more effort examining the challenge set during logins, hence usability is decreased.

In addition, the use of non-distinctive images has caused the users to mistake their selections, which increases the number of errors. Each of the images should therefore contain uniqueness for it to be identifiable by the users. However, the images for our graphical authenticator were resized to a resolution that is suitable for a small mobile screen. In the process, much of the pictures' details were lost; thus, the images became less distinctive and less identifiable (or less recognizable).

This study explored one of the defined hypotheses, H3. The hypothesis H3, "Multiple combinational graphical passwords are more memorable than multiple gesture passwords or multiple PINs", was not confirmed. Although people remember images better than text (words or numbers), our conjecture of the superiority of combinational graphical password is debunked.

6.4. Summary and concluding remarks

In this chapter, two experimental studies and their results were discussed. The first study investigated user experience amongst the three testing password systems, and the second study investigated the memorability of passwords and the retention strategies the subjects had used to remember those passwords. The results of the studies were used to test three hypotheses; however, none of the hypotheses could be confirmed using the data collected from the studies.

Due to the limited resources, we were not able to recruit as many subjects as we have wanted. The sample size (N=18) was relatively small for user experiments; especially for the second study, the number of participants was preferably to be at least 10 per group, which means at least 30 people were needed. With larger sample size, the results of the statistic analyses may vary.

7. Conclusion

This research aimed at finding an authentication solution that is most suitable for mobile banking. Currently, PIN authentication is the most prevalent form of verification technique for mobile banking, but the background literature survey had unveiled numerous limitations related to PIN authentication. One of those limitations is password memorability, which has been investigated in many cognitive and HCI research studies; solutions were proposed to exploit the picture superiority effect to overcome the memorability issue. Studies have found that people remember graphical passwords substantially more accurate over time than passwords or PINs. To adapt graphical passwords for mobile system, we have designed and implemented a cognometric graphical authenticator for mobile phones.

Although peoples' graphical memory has been proven to be proficient at remembering graphical passwords, alternative memory schemes are also possible for password retention. In this research, we have proposed the use of kinesthetic memory (or muscle memory) for password retention, and we have found no research that has investigated the use of kinesthetic memory to increase password memorability. To explore this possibility, we have designed a password system that requires users to produce certain gestures as password elements to authenticate, and we have developed the designed system into a prototype which allows users to enter gesture elements using a mobile phone. In order to confirm password memorability, we designed an experiment to test for users' ability and their strategies to remember different types of passwords.

One research area of authentication that has seldom been investigated is users' perception of trustworthiness of the systems. Without users trusting the authenticator, the users would not accept to adopt it for mobile banking to protect their wealth. Thus, we have designed an experiment to learn in which authentication system(s) users perceived most trust.

As a result, in this research, two studies were conducted: one for testing users' experience of using different authenticators, and the other one for testing password memorability. The two empirical studies were conducted in the aims of answering our research questions. In each of the studies, the three authentication systems (PIN, graphical, and gesture) were tested with eighteen

users. Data was collected during the studies, and the data was analysed to understand users' acceptance and their performances of using our proposed authenticators.

7.1. Research questions

The studies conducted were aimed to answer the following questions:

Does social or physical context affect how people feel about using different authentication techniques for m-banking?

From the evaluation, it appears that social and physical context does not affect how people feel about the authentication technique used as long as the technique does not reveal their actions. Inputs into the PIN and the graphical password authenticators require small discreet actions; however the gesture password prototype requires actions that are more exposed. Thus, the latter is more susceptible to shoulder surfing. From examining the data of our experiment, users seemed to be comfortable with using PINs and graphical passwords in both private and public environments; however, many of the subjects were reluctant to use gesture passwords in public and prefer to use them in a private environment.

Which authentication technique do people perceive as the most trustworthy to use for m-banking?

Initially, we thought users' previous knowledge of PINs would favour their trust in using PINs for mobile banking authentication. The data from the experiment shows there were no significant differences between users' trust in the authentication systems. However, the data did show that the subjects considered gesture passwords as the least secure option for mobile banking; whilst, the difference between PINs and graphical passwords was not distinguishable. Thus, users have no preference of choice between PINs and graphical passwords.

Which authentication technique provides passwords that are the most memorable?

A test on the retention of multiple passwords was conducted for this question. The results of the test show users remember PINs more accurate than combinational graphical passwords or gesture passwords. Although the study by Moncur & Leplâtre (2007) confirmed that multiple

graphical passwords were easier to remember than PINs, by adding the combinational effect to graphical passwords has negatively influenced the memorability of the passwords.

7.2. Contributions

Our research focused on mobile authentication, specifically for mobile banking. During the study, two types of authentication systems for mobile phones were suggested: one system explored the use of facial images in combinational form as passwords, while the other one explored an innovative approach of using strings of 3-dimensional discrete motions as passwords. From the literature survey, it seems kinesthetic memory has never been pursued for password retention before, and to the best of our knowledge, the gesture password system proposed in this research is the first of its kind. Furthermore, we acknowledged the password memorability issue is not the only aspect that influences user adoption of an authentication system; we suggested that users' experience and their perceived trustworthiness of using the authenticator must also be considered. Overall, our research provides an insight into alternatives to PINs for remote mobile authentication. From this project, it seems PIN authentication is the still most desirable option for mobile banking. However, the result does not limit any future work of developing a new and more suitable authentication for mobile banking. Furthermore, as mobile banking is becoming more popular, we encourage more research to be conducted in the related field.

7.3. Future work

There are number of areas in which our work could be extended, and the followings explain some of the areas.

7.3.1. Experiment participants

In both experiments, the numbers of participants were relatively low. It would be of interest to repeat the studies with larger sample sizes, especially for the retention test as the between-groups participatory method was adopted. With larger sample sizes, we can analyse more data and look for unexpected patterns. Furthermore, the subjects recruited for the experiments were from a

homogenous background; to generalise the findings across different people, subjects with different backgrounds are needed.

7.3.2. Biometric movement signatures

In this research, data from accelerometers was used to match discrete gestures. However, the technique can further be extended for kinesthetic biometric authentication. Users can wave a sensor device in a specific pattern in mid-air to enter a 3D-signature, and the data of the sensor can be analysed to detect biometric features.

7.3.3. Beyond mobile phones

From the literature survey, most of the research we found discussed about authentication systems for computers or mobile phones. Although those are the most common devices that require authentication, we should not limit ourselves in researching for suitable authentication solutions for those devices only. As ubiquitous computing is becoming more popular, many new types of devices also require authentication. We are certain to assume PIN authentication is suitable for systems that have a number pad input interface, such as mobile phones; our gesture password system is ideal for devices that are equipped with an accelerometer. Using Apple's fourth generation iPod for an example, instead of using its click-wheel to enter PINs, the system can adopt gesture passwords for authentication. One can argue that graphical authentication may also be a good option for iPods. From the experiences of this project, we realize the small resolution screen of mobile devices cannot display full details of pictures; therefore, some pictures of a graphical authenticator may not be displayed properly.

Appendix A: Understanding Users - Survey Questions

1st Preface: [*Researcher explains research objectives to the subject*]

Researcher explains reasons for conducting this survey and informs the subject that this survey is only for academic purpose. The subject's information is always remained confidential.

General Questions

Subject Description: M / F _____

Age: _____

Occupation: _____

Contact Details [*Optional, ask the subject if he/she wants to leave his/her contact details*]:

Part 1 – Mobile Phone Usage

1. Do you own a mobile phone?

(a) Yes, which model? (b) No, do you have access to a mobile phone?

2. How often do you change or buy a new mobile phone?

3. How long do you normally leave you phone switched on?

(a) Always on (b) Switch phone off at night (c) Switch phone off during weekend

(d) Only switch phone on when it is needed (e) Others _____

4. How much airtime (mobile pre-paid credit) do you use per week? (estimate)

5. Do you send airtime (top-up) to family members, friends or other people?

(a) Yes, how often and how much? (b) No

6. Do you trust your mobile phone? E.g. trust that other people cannot access the information on your phone?

(a) Yes, what makes you trust your phone? (b) No, why?

7. If you send a message, do you trust that your message will be delivered to the correct phone number/receiver?

(a) Yes, what makes you trust it? (b) No, why?

8. Do you think you will always receive the message that was sent to you?

(a) Yes, why? (b) No, why?

9. Besides communications, what else do you use you mobile phone for? (*Can select multiple options*)

(a) Games (b) Camera (photo/video) (c) WAP Browser (d) Play Music

(e) Calculator (f) Alarm/Clock/Calendar (g) Others, please specify

Part 2 – Banking Functions

10. Do you have a bank account?

(a) Yes, which bank do you bank with? (b) No, jump to (#)

11. How often do you do banking?

(a) Daily (b) Weekly (c) Once in 2 Weeks (d) Monthly (e) Once in 2 Months

12. What do you do with a bank account? *(Can select multiple options)*

(a) Check Balance (b) Withdraw Cash (c) Account Payment (d) Buy Airtime

(e) Shopping (f) Transfer Money (g) Others, please specify

13. Which banking services do you use/like? (e.g. Loan, Saving, etc.)

14. Do you trust banks? E.g. Do you trust that your money will not be stolen from your bank account?

(a) Yes, Why? (b) No, Why?

15. Do you use a computer?

(a) Yes, what do you use a computer for? (b) No

16. Do you have access to the internet?

(a) Yes, do you use internet banking (e-banking)? (b) No

17. Do you trust internet banking?

(a) Yes, why? (b) No, why?

(#) *[Show a list of banking functions and explain each function to the subject]*

18. Which of the shown functions do you think can help you to manage your money?

19. Do you (i) understand or (ii) use mobile banking (m-banking)?

(a) If (i), please explain your understanding of m-banking

(b) If (ii), which m-banking service do you use? And why do you use m-banking?

(c) No [*Researcher explains the concept of m-banking to subject*]


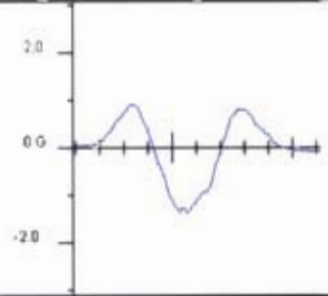

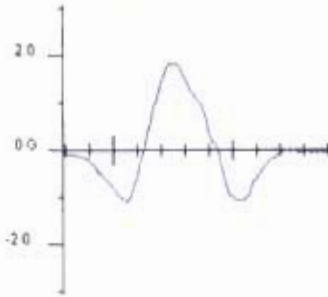

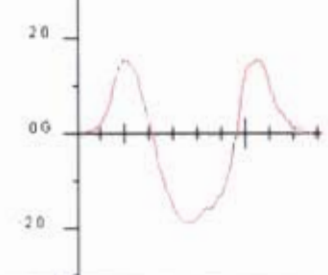

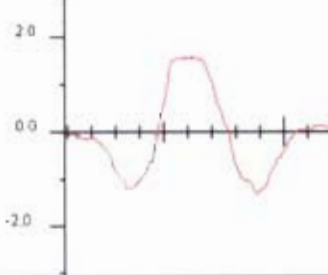
20. Do you trust banking with your mobile phone?


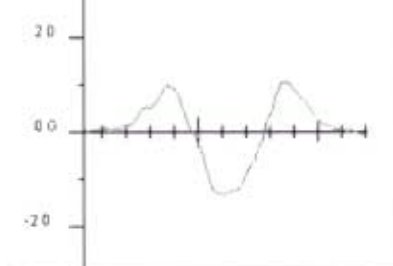

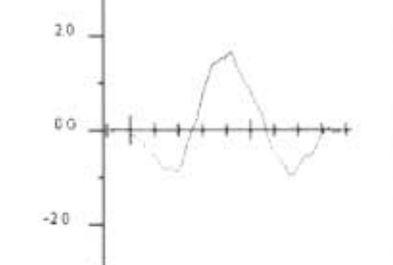

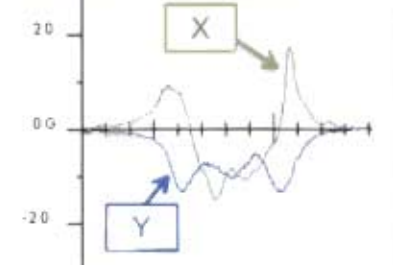

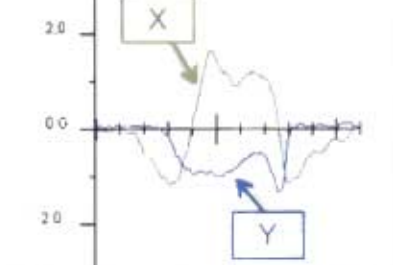

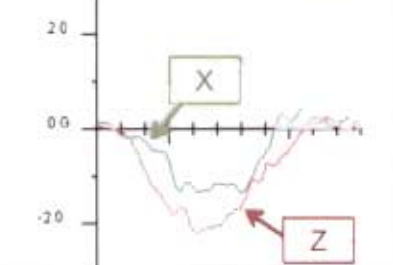
(a) Yes, why? (b) No, why?


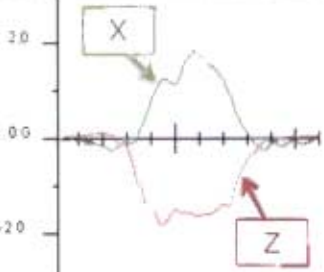
21. *Open questions*

[Express appreciations to the subject for his/her participation and ask the subject if he/she has any questions]

Appendix B: Features of Gesture Elements

Gesture	Motion	Axis	Change of directions	
			directions	Wavelet
Forward		Y-axis	+ to - to +	
Backward		Y-axis	- to + to -	
Up		Z-axis	+ to - to +	
Down		Z-axis	- to + to -	

<p>Left</p>		<p>X-axis</p>	<p>+ to - to +</p>	
<p>Right</p>		<p>X-axis</p>	<p>- to + to -</p>	
<p>Swing Left</p>		<p>X-axis</p>	<p>+ to - to +</p>	
		<p>Y-axis</p>	<p>-</p>	
<p>Swing Right</p>		<p>X-axis</p>	<p>- to + to -</p>	
		<p>Y-axis</p>	<p>-</p>	
<p>Tilt Left</p>		<p>X-axis</p>	<p>-</p>	
		<p>Z-axis</p>	<p>-</p>	

Tilt Right		X-axis	+	
		Z-axis	-	

Appendix C: Experiment Questionnaires

Study 1

*** On the Likert scale, small numbers represent negative response and large numbers represent positive response. Boxed *Italic texts* indicate actions for the facilitator

Introduce and explain the purpose of this study to subject.

Subject's information

- **Name:** _____ **Age:** _____
- **Gender:** M / F **Education (Grade):** _____
- **Occupation:** _____
- **Have a mobile phone:** YES / NO
 - If *NO*, does the subject have access to a mobile phone: YES / NO
- **Income (per month):** R0 – R500 / R500 – R1000 / R1000 – R2000 / R2000 – R3000 / R3000+
- **Have a bank account:** YES / NO
 - If the subject has a bank account, does the subject use his/her bank card to withdraw cash or pay with the bank card? WITHDRAW / SWIPE / BOTH
- **Use cellphone banking (m-banking):** YES / NO
 - If *NO*, experimenter explains m-banking to the subject
- **PIN/Non-PIN user:** YES / NO

Familiarize the subject with the testing systems (Alternate order of introduction to prevent learning effect)

Order

- _____ PIN
- _____ Graphical Password
- _____ Gesture Password

APPENDIX C

Reason: _____

Gesture: **YES, SECURE / NO, INSECURE / UNSURE**

Reason: _____

CA5: Would you prefer to perform logins in a private area or a public area

PIN: PRIVATE / PUBLIC / EITHER

GRAPHICAL: PRIVATE / PUBLIC / EITHER

GESTURE: PRIVATE / PUBLIC / EITHER

User Trust

Provide subject a scenario of using prototypes for authentication

UT 1: Rate: "I Trust PIN for cellphone banking"						
1	2	3	4	5	6	7
Strongly Disagree						Strongly Agree
UT 1: Rate: "I Trust Graphical Password for cellphone banking"						
1	2	3	4	5	6	7
Strongly Disagree						Strongly Agree
UT 1: Rate: "I Trust Gesture Password for cellphone banking"						
1	2	3	4	5	6	7
Strongly Disagree						Strongly Agree
UT 2: Which system do you think is the most secure for cellphone banking logins? (Rank: 1, 2, or 3)						
PIN: _____						
Graphical: _____						
Gesture: _____						

/ END OF STUDY 1

Study 2

Introduction

Subject's information

- Name: _____
- Allocated Passwords: _____

Train the subject to use the allocate password system.

Present the paper with a set of passwords to the subject and inform the subject that he/she has a 24-hour rehearsal period to memorize the given passwords.

*The facilitator returns **one day** later.*

Request the subject to present the given paper with the allocated passwords and collect the paper.

How many times did you open the envelope? _____

When was the last time you checked the envelope? _____

On average, how long did you have to take to check the passwords?

*The facilitator returns **six days** after
Request the subject to recall passwords*

PASSWORD 1 _____

PASSWORD 2 _____

PASSWORD 3 _____

What methods (or strategies) did you use to remember the passwords?

Rehearsal by speaking the passwords out loud YES / NO

Visualise the image(s) of the passwords in mind YES / NO

Construct stories using the passwords YES / NO

(PIN) By visualising the position of the number on a key pad YES / NO

(Graphical) By the gender of the faces YES / NO

(Graphical) By the race of the faces YES / NO

(Graphical) By the age of the faces YES / NO

(Gestures) By practising the movements YES / NO

(Gestures) By remembering the directions YES / NO

Other: _____

Were there any difficulties that you encountered while remembering the passwords?

Do you think it was easy (or difficult) to remember all three passwords?

1	2	3	4	5	6	7
Very Difficult						Very Easy

/END OF STUDY 2

Appendix D: Experiment Data

Study 1

Table 1. Results of the password entries in Study 1

Subject ID	PIN		Graphical Password		Gesture Password	
	<i>Time (sec.)</i>	<i>Attempt</i>	<i>Time (sec.)</i>	<i>Attempt</i>	<i>Time (sec.)</i>	<i>Attempt</i>
Subject 1	9.07	1	91.31	1	6.43	3
	5.14	1	38.28	3	8.28	2
	5.96	1	21.95	1	7.42	1
	4.63	1	40.84	2	7.60	1
	4.58	1	37.48	1	6.70	1
Subject 2	6.98	1	39.58	1	9.76	1
	6.04	1	43.87	1	9.67	2
	5.24	1	64.05	1	9.63	1
	6.10	1	69.20	1	8.23	1
	5.09	1	50.63	1	8.10	1
Subject 3	7.53	1	48.95	1	9.40	1
	4.33	1	24.96	1	5.13	1
	3.61	1	18.61	1	4.50	1
	4.38	1	34.19	1	4.27	2
	3.90	1	29.39	1	4.63	1
Subject 4	7.37	1	85.66	1	7.42	2
	4.21	1	94.51	1	5.58	1
	6.95	1	18.75	1	5.53	2
	5.25	1	39.82	3	6.57	1
	5.00	1	24.95	1	4.81	2
Subject 5	16.40	1	71.80	1	-	3+
	11.70	1	34.26	1	10.80	1
	16.40	1	43.60	1	9.90	2
	11.56	1	40.50	1	6.70	2
	8.11	1	30.18	1	6.43	3
Subject 6	4.12	1	24.54	1	-	3+
	3.43	1	21.30	1	8.50	1
	3.62	1	18.39	1	7.60	1
	5.22	1	17.64	1	8.00	1
	3.27	1	24.78	1	9.72	3
Subject 7	7.43	1	84.05	1	16.78	3
	5.05	1	52.29	1	13.45	1
	5.73	1	30.89	1	13.32	1
	5.32	1	67.98	1	12.51	2
	5.31	1	37.27	1	10.30	1
Subject 8	5.71	2	45.02	2	8.55	2
	5.24	1	57.19	1	13.77	1
	3.70	1	27.58	1	6.84	2

APPENDIX D

	4.67	1	26.26	2	6.21	2
	4.78	1	22.37	2	6.97	1
Subject 9	9.34	1	100.92	2	8.59	3
	5.19	1	64.48	1	10.12	2
	5.80	1	32.47	1	10.21	2
	4.38	1	85.03	1	15.43	2
	4.20	1	39.86	1	9.85	1
Subject 10	7.48	1	108.21	1	10.00	2
	6.73	1	85.96	1	11.88	3
	5.92	1	81.92	1	13.54	2
	5.72	1	39.41	1	12.42	3
	5.49	1	42.93	1	9.94	1
Subject 11	7.91	1	89.61	1	5.76	2
	5.00	1	75.90	1	9.90	1
	5.23	1	39.23	1	8.01	1
	5.22	1	159.59	1	6.61	2
	3.99	1	86.64	1	5.67	2
Subject 12	10.65	1	152.34	1	20.74	1
	8.36	1	67.67	1	18.18	1
	8.26	1	54.20	1	14.62	1
	7.97	1	45.20	2	20.92	1
	8.06	1	31.58	1	15.30	1
Subject 13	7.05	1	105.15	1	5.87	3
	4.67	1	21.86	1	6.34	3
	4.81	1	27.2	1	5.49	3
	4.95	1	20.86	1	4.68	2
	4.61	1	20.05	1	5.26	1
Subject 14	4.90	1	102.60	1	24.66	1
	3.91	1	29.00	1	10.98	3
	3.27	1	78.01	1	8.14	1
	3.33	1	38.51	1	6.88	3
	3.80	1	52.14	1	9.81	1
Subject 15	8.42	1	61.82	1	11.34	1
	5.69	1	83.94	1	8.86	2
	5.44	2	39.48	1	8.37	2
	4.39	1	22.23	2	10.35	1
	4.87	1	29.26	1	7.15	1
Subject 16	5.76	1	129.75	1	12.46	3
	5.39	1	54.71	1	13.18	2
	3.87	1	40.03	1	12.51	1
	4.70	1	75.70	3	12.28	2
	3.40	1	51.78	1	14.17	2
Subject 17	5.02	1	79.23	1	10.62	1
	3.85	2	24.02	1	11.52	1
	3.37	1	59.17	1	10.12	1
	4.96	1	56.03	1	9.94	1
	4.06	1	25.17	2	9.54	1

Subject 18	7.40	1	57.20	1	9.40	1
	4.80	1	34.87	2	6.39	1
	5.75	2	26.66	1	6.52	1
	4.90	1	24.27	1	6.79	1
	4.86	1	22.90	2	5.35	2

Table 2. Results of the user experience questionnaire

Subject ID	UX1			UX2			UX3			UX5		
	PIN	Gra.	Ges.	PIN	Gra.	Ges.	PIN	Gra.	Ges.	PIN	Gra.	Ges.
Subject 1	7	5	6	7	6	5	7	7	7	7	5	7
Subject 2	7	7	6	7	7	6	7	7	7	7	5	7
Subject 3	7	7	7	7	7	7	7	7	7	7	7	7
Subject 4	7	7	7	7	7	7	7	7	6	7	6	6
Subject 5	7	7	4	7	7	3	7	7	7	7	7	4
Subject 6	6	7	6	7	7	6	7	7	7	7	7	7
Subject 7	6	5	4	6	6	5	5	6	5	7	7	5
Subject 8	7	6	6	7	7	6	7	6	7	7	6	7
Subject 9	7	6	7	7	6	7	7	5	7	7	5	7
Subject 10	7	4	5	7	4	5	7	7	7	7	7	4
Subject 11	7	6	6	7	3	7	7	5	6	7	4	6
Subject 12	5	7	6	7	7	6	7	7	6	7	7	6
Subject 13	6	6	5	7	7	6	7	7	6	7	7	6
Subject 14	7	6	4	7	6	5	7	6	6	7	7	5
Subject 15	7	6	5	7	7	7	7	7	7	7	5	5
Subject 16	7	7	5	7	7	6	7	7	6	7	7	7
Subject 17	3	3	3	7	7	7	7	7	7	7	7	7
Subject 18	7	7	7	7	7	7	7	7	7	7	7	7
<i>Mean</i>	<i>6.5</i>	<i>6.05</i>	<i>5.5</i>	<i>6.94</i>	<i>6.39</i>	<i>6</i>	<i>6.89</i>	<i>6.61</i>	<i>6.56</i>	<i>7</i>	<i>6.28</i>	<i>6.11</i>

Table 3. Results of the context awareness questionnaire

Subject ID	CA1	CA2			CA3			CA4			CA5		
		PIN	Gra.	Ges.	PIN	Gra.	Ges.	PIN	Gra.	Ges.	PIN	Gra.	Ges.
Subject 1	Yes	7	1	7	5	6	7	no	unsure	yes	either	either	either
Subject 2	Yes	7	7	7	7	7	7	yes	yes	yes	either	either	private
Subject 3	Yes	7	7	7	7	7	7	yes	yes	yes	either	either	either
Subject 4	Yes	1	7	7	7	7	1	yes	yes	no	private	private	private
Subject 5	Yes	7	7	7	7	7	7	no	yes	yes	either	either	private
Subject 6	Yes	6	5	7	7	6	5	yes	yes	no	public	public	private
Subject 7	Yes	4	5	7	3	7	4	unsure	unsure	unsure	private	either	private
Subject 8	Yes	7	7	7	2	2	5	no	unsure	yes	either	either	either
Subject 9	No	7	1	7	7	5	5	yes	yes	no	private	private	private

APPENDIX D


Subject 10	Yes	7	7	7	7	7	3	yes	yes	yes	either	either	either
Subject 11	Yes	7	5	7	2	5	2	yes	unsure	no	private	either	private
Subject 12	Yes	6	6	7	6	7	6	no	no	unsure	either	public	private
Subject 13	Yes	7	7	7	3	7	6	no	yes	no	private	either	private
Subject 14	Yes	7	7	7	6	6	5	unsure	unsure	yes	private	either	either
Subject 15	Yes	6	6	6	4	7	7	yes	yes	yes	either	either	either
Subject 16	Yes	7	7	7	7	7	7	yes	unsure	yes	either	either	either
Subject 17	Yes	7	7	7	7	7	1	unsure	no	no	public	private	private
Subject 18	Yes	7	7	7	1	7	1	yes	yes	no	either	either	private
<i>Mean</i>		6.33	5.89	6.94	5.28	6.33	4.78						

Table 4. Two-way table of CA4 in Table 3

	PIN	Graphical	Gesture
Yes	10	10	9
No	5	2	7
Unsure	3	6	2

Table 5. Two-way table of CA5 in Table 3

	PIN	Graphical	Gesture
Private	6	3	11
Public	2	2	0
Either	10	13	7

Table 6. Results of the trust questionnaire

Subject ID	UT1: Trust rating			UT2: Trust ranking		
	PIN	Gra.	Ges.	PIN	Gra.	Ges.
Subject 1	7	4	7	1	3	2
Subject 2	5	7	7	3	1	2
Subject 3	7	7	7	2	1	3
Subject 4	7	7	7	3	1	2
Subject 5	7	7	6	2	1	3
Subject 6	7	7	6	1	2	3
Subject 7	7	5	5	1	2	3
Subject 8	7	7	7	1	3	2
Subject 9	4	4	4	1	3	2
Subject 10	7	5	4	1	2	3
Subject 11	7	6	1	1	2	3
Subject 12	5	4	5	1	2	3
Subject 13	1	7	7	2	1	3
Subject 14	3	7	6	2	1	3
Subject 15	5	6	5	1	3	2
Subject 16	7	7	7	2	1	3
Subject 17	7	1	1	1	2	3
Subject 18	7	7	1	2	1	3
<i>Mean</i>	5.94	5.83	5.17			

Table 7. Two-way table of UT1 in Table 6

	PIN	Graphical	Gesture
1	10	8	0
2	6	6	6
3	2	4	12

Study 2

Table 8. Individual scores of the password retention test in Study 2

Group1: PIN		Group 2: Graphical Password		Group 3: Gesture Password	
<i>Subject ID</i>	<i>Score (out of 3)</i>	<i>Subject ID</i>	<i>Score (out of 3)</i>	<i>Subject ID</i>	<i>Score (out of 3)</i>
PIN1	3	GRA1	3	GES1	0
PIN2	3	GRA2	2	GES2	1
PIN3	3	GRA3	3	GES3	1
PIN4	3	GRA4	0	GES4	0
PIN5	3	GRA5	1	GES5	0
PIN6	<i>dropped out</i>	GRA6	1	GES6	1

References

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communication of the ACM*, 42 (12), 41-46.
- Ashbourn, J. (2000). *Biometrics - Advanced Identity Verification*. London, UK: Springer-Verlag.
- Bahrick, H. P. (1984). Semantic memory content in permastore: Fifty years of memory for Spanish learned in school. *Journal of Verbal Learning and Verbal Behavior*, 14, 1-24.
- Bauer, A. (1998). Random Art Gallery. [WWW document]. Retrieved October 17, 2008, from <http://www.random-art.org/>
- Bishop, M. (2006). Psychological acceptability revisited. In L. F. Cranor, & S. Garfinkel, (Eds), *Security and Usability* (pp. 1-11). Sebastopol, CA: O'Reilly.
- Blonder, G. E. (1996). Graphical Password. *Patent No. 5559961*. United States.
- Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2006). Fourth-factor authentication: Somebody you know. In CCS '06: *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 168-178, New York: ACM Press.
- Brostoff, S., & Sasse, M. A. (2000). Are passfaces more usable than passwords? A field trial investigation. In *Proceedings of the HCI 2000 Conference on People and Computers XIV – Usability and System Evaluation*, pp. 405-424, Springer.
- Chapman, C. D., Heath, M. D., Westwood, D. A., & Roy, E. A. (2001). Memory for kinesthetically defined target location: Evidence for manual asymmetries. *Brain and Cognition*, 46 (1-2), 62-66.
- Coventry, L. (2005). Usable biometrics. In L. F. Cranor, & S. Garfinkel, (Eds), *Security and Usability* (pp. 175-197). Sebastopol, CA: O'Reilly.

REFERENCES

- Coventry, L., De Angeli, A., & Johnson, G. (2003). Usability and biometric verification at the ATM interface. In CHI '03: *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 153-160, New York: ACM Press.
- Davis, D., Monrose, F., & Reiter, M. K. (2004). On user choice in graphical password schemes. In SSYM '04: *Proceedings of the 13th conference on USENIX Security Symposium*. Berkeley, CA: USENIX Association.
- De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*, 63 (1-2), 128-152.
- De Luca, A., Weiss, R., & Hussmann, H. (2007). PassShape: Stroke based shape passwords. In OZCHI'07: *Proceedings of the 19th Australasian conference on Computer-Human Interaction*, pp. 239-240, New York: ACM Press.
- Deutsch, M. (1962). Cooperation and Trust: Some Theoretical Notes. In M. Jones, *Nebraska Symposium on Motivation* (pp. 275-318). Lincoln, NE: University of Nebraska Press.
- Dhamija, R. & Perrig, A. (2000). Déjà Vu: A user study using images for authentication. In SSYM'00: *Proceedings of the 9th USENIX Security Symposium*. Berkeley, CA: USENIX Association.
- Dirik, A. E., Memon, N., & Birget, J.-C. (2007). Modeling user choice in the PassPoints graphical password scheme. In SOUPS '07: *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pp. 20-28. New York: ACM Press.
- Dunphy, P., & Yan, J. (2007). Do background images improve "draw a secret" graphical passwords? In CCS '07: *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 36-47. New York: ACM Press.
- Egelman, S., King, J., Miller, R. C., Ragouzis, N., & Shehan, E. (2007). Security user studies: Methodologies and best practices. In CHI '07: *CHI '07 extended abstracts on Human factors in computing systems*, pp. 2833-2836. New York: ACM Press.

REFERENCES

- Egger, F. N. (2003). *From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce*. Eindhoven: Technische Universiteit Eindhoven. PhD Thesis. [Electronic version ISBN 90-386-1778-X].
- GSM Association. (2007). Global money transfer pilot uses mobile to benefit migrant workers and the unbanked. [WWW document]. Retrieved October 6, 2008, from http://www.gsmworld.com/news/press_2007/press07_14.shtml.
- GSM Association. (2008a). Subscriber connections - Q2 2008. [Electronic document] Retrieved October 6, 2008, from http://www.gsmworld.com/news/statistics/pdf/gsma_stats_q2_08.pdf.
- GSM Association. (2008b). 20 facts for 20 years of mobile communications. [Electronic document]. Retrieved October 6, 2008, from http://www.gsmworld.com/documents/20_year_factsheet.pdf.
- Howell, D., C. (1982). *Statistical methods for psychology*. Boston, MA: Duxbury Press.
- Integrat. (2008). Mobile marketing: Uncovering the myth. [WWW document]. Retrieved October 6, 2008, from <http://www.itweb.co.za/sections/telecoms/2008/0805260807.asp?A=CEL&S=Cellular&O=FPIN>.
- ISO 9241-11 (1998). Ergonomic requirements for office work with visual display terminals (VDTs) - part 11: Guidance on usability.
- Ivantury, G., & Pickens, M. (2006). *Mobile Phone Banking and Low-Income Customers Evidence from South Africa*. Washington DC: Consultative Group to Assist the Poor (CGAP).
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14 (1), 4-20.

REFERENCES

- Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, 43 (2), 90-98.
- Jansen, W. A. (2003). Authenticating users on handheld devices. In *Proceedings of the Canadian Information Technology Security Symposium*.
- Jansen, W., Gavrilla, S., Korolev, V., Ayers, R., and R., S. (2003). Picture password: A visual login technique for mobile devices. [NIST Report - NISTIR7030].
- Jermyn, I., Mayer, A., Monroe, F., Reiter, M. K., & Rubin, A. D. (1999). The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX Security Symposium* (pp. 1-14). Washington, D.C.: USENIX Association.
- Jones, M., & Marsden, G. (2006). *Mobile Interaction Design*. Chichester, West Sussex: John Wiley & Sons.
- Kayle, A. (2008). Mobile banking on the rise. [WWW document]. Retrieved January 9, 2009, from <http://www.itweb.co.za/sections/telecoms/2008/0811051500.asp?A=HOME&O=FPMN>.
- Khoshnoodi, M. A., Motiei-Langroudi, R., Omrani, M., Ghaderi-Pakdell, F., & Abbassian, A. H. (2005). Kinesthetic memory in distance reproduction task: Importance of initial hand position information. *Experimental Brain Research*, 170 (3), 312-319.
- Kim, J., & Moon, J. Y. (1998). Designing Emotional Usability in Customer Interfaces - Trustworthiness of Cyber-banking System Interfaces. *Interacting with Computers*, 10, 1-29.
- Kimery, K. M., & McCord, M. (2002). Third-party assurances: Mapping the road to trust in e-retailing. *Journal of Information Technology Theory and Application (JITTA)*, 4 (2), 63-82.

REFERENCES

- Luhmann, N. (1988). Familiarity, Confidence, Trust: Problems and Alternatives. In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations* (pp. 94-107). New York, NY: Basil Blackwell.
- Madigans, S. (1983). Picture memory. In Yuille J. C. (Ed.), *Imagery, memory, and cognition: Essays in honor of Allan Paivio* (pp. 65-89). Hillsdale, NJ: Erlbaum.
- Marsh, S. P. (1994). *Formalising Trust as a Computational Concept*. Stirling: University of Stirling. PhD Thesis. [Electronic version]
- Mayrhofer, R. & Gellersen, H. (2007). Shake well before use: Authentication based on accelerometer data. In Proc. Pervasive 2007: *5th International Conference on Pervasive Computing*, pp. 144-161. London, UK: Springer-Verlag.
- Mc Knight, H., & Chervany, N. L. (2006). Reflections on an Initial Trust-Building Model. In R. Bachmann, & A. Zaheer (Eds), *Handbook of Trust Research* (pp. 29-51). Cheltenham: Edward Elgar Publishing.
- Miller, G. (1956). The magic number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63, 81-97.
- Moncur, W., & Leplâtre, G. (2007). Pictures at the ATM: Exploring the usability of multiple graphical passwords. In CHI '07: *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 887-894. New York: ACM Press.
- Monrose, F., & Reiter, M. K. (2005). Graphical Passwords. In L. F. Cranor, & S. Garfinkel, (Eds), *Security and Usability* (pp. 157-174). Sebastopol, CA: O'Reilly.
- Morris, R., & Thompson, K. (1979). Password security: A case history. *Communication of the ACM*, 22 (11), 594-597.
- Nali, D., & Thorpe, J. (2004). Analysing user choice in graphical passwords. *Technical Report TR-04-01*, School of Computer Science, Carleton University.

REFERENCES

- Nelson, D. L., Reed, U. S., & Walling, J. R. (1976). Picture superiority effect. *Journal of Experimental Psychology: Human Learning & Memory*, 2 (5), 523-528.
- Nielsen, J. (2005). Ten Usability Heuristics. [WWW document]. Retrieved January 9, 2008 from http://www.useit.com/papers/heuristic/heuristic_list.html.
- Octopus Cards Limited. (2005). Welcome to Octopus. [WWW document]. Retrieved October 22, 2008, from <http://www.octopuscards.com/consumer/en/index.jsp>.
- Paivio, A. (1971). *Imagery and verbal processes*. New York: Holt, Rinehart, and Winston.
- Paivio, A., & Csapo, K. (1973). Picture superiority in free recall: Imagery or dual coding? *Cognitive Psychology*, 5 (2), 176-206.
- Paivio, A., Rogers, T. B., & Smythe, P. C. (1968). Why are pictures easier to recall than words? *Psychonomic Science*, 11, 137-138.
- Patel, S., Pierce, J., & Abowd, G. (2004). A gesture-based authentication scheme for untrusted public terminals. In *UIST '04: Proceedings of the 17th annual ACM symposium on User interface software and technology*, pp. 157-160. New York: ACM Press.
- Patrick, A. S., Long, A. C., & Flinn, S. (2003). HCI and security systems. In *CHI '03: CHI '03 Extended abstracts on Human factors in computing systems*, pp. 1056-1057. New York: ACM Press.
- Porteous, D. (2006). *The Enabling Environment for Mobile Banking in Africa*. London: Department for International Development (DFID).
- Project Smart. (n.d.) Risk Management. [WWW document]. Retrieved October 19, 2008, from <http://www.projectsmart.co.uk/risk-management.html>.
- Real User Corporation. (2005). Welcome to the Passfaces Demonstration. [WWW document]. Retrieved October 16, 2008, from http://www.passfaces.com/enterprise/demo/try_passfaces.htm.

REFERENCES

- Renaud, K. (2005). Evaluating authentication mechanisms. In L. F. Cranor, & S. Garfinkel, (Eds), *Security and Usability* (pp. 103-128). Sebastopol, CA: O'Reilly.
- Renaud, K., & De Angeli, A. (2004). My password is here! An investigation into visuo-spatial authentication mechanisms. *Interacting with Computers*, 16 (6), 1017-1041.
- Renaud, K., & Smith, E. (2001). Jiminy: Helping users to remember their passwords. In SAICSIT '01: *Proceedings of South African Institute for Computer Scientists and Information Technologists*, pp. 73-80. Pretoria: UNISA Publishers.
- Rousseau, D., Sitkin, S., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23 (3), pp. 393-404.
- Rumsey, D. (2007). *Intermediate statistics for dummies*. Indianapolis, IN: Wiley Publishing, Inc.
- Sasse, M. A. & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In L. F. Cranor, & S. Garfinkel, (Eds), *Security and Usability* (pp. 13-30). Sebastopol, CA: O'Reilly.
- Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19 (3), 122-131.
- Schneier, B. (1999). Inside risks: The uses and abuses of biometrics. *Communications of the ACM*, 42 (8), pp. 136.
- Schneier, B. (2000). *Secret and Lies*. John Wiley & Sons.
- Sharp, H., Rogers, Y., & Preece, J. (2007). *Interaction Design: Beyond Human-Computer Interaction* (2nd ed.). Chichester, West Sussex: John Wiley & Sons.
- Simlog. (2007). Muscle Memory. [WWW document]. Retrieved October 20, 2008, from <http://www.simlog.com/muscle-memory.html>.

REFERENCES

- Singh, S. (2006). The Social Dimensions of the Security of Internet Banking. *Journal of Theoretical and Applied Electronic Commerce Research*, 1 (2), 72-78.
- Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., & Furlong, M. (2007). Password sharing: Implications for security design based on social practice. In CHI '07: *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 895-904. New York: ACM Press.
- Smetters, D. K., & Grinter, R. E. (2002). Moving from the design of usable security technologies to the design of useful secure applications. In *Proceedings of the 2002 workshop on New security paradigms*, pp. 82-89. New York: ACM Press.
- Sternberg, R. J. (1999). *Cognitive Psychology* (2nd ed.). London: Harcourt Brace.
- Sun Microsystems, Inc. (2007). *Sun™ Small Programmable Object Technology (Sun SPOT) Theory of Operation*. Retrieved November 18, 2008, from <http://www.sunspotworld.com/docs/Purple/SunSPOT-TheoryOfOperation.pdf>. [Electronic version].
- Takada, T., & Koike, H. (2003). Awase-E: Image-based authentication for mobile phones using user's favorite images. In *Mobile HCI 2003: Proceedings of the 5th International Symposium on Human Computer Interaction with Mobile Devices and Services*, pp. 347-351. Springer.
- Tari, F., Ozok, A. A., & Holden, S. H. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *SOUPS '06: Proceedings of the 2nd Symposium on Usable Privacy and Security*, pp. 56-66. New York: ACM Press.
- Thorpe, J., & van Oorschot, P. C. (2004). Towards secure design choices for implementing graphical passwords. In *ACSAC '04: Proceedings of the 20th Annual Computer Security Applications Conference*, pp. 50-60. Washington, DC: IEEE Computer Society.

REFERENCES

- Tognazzini, B. (2005). Design for usability. In L. F. Cranor, & S. Garfinkel, (Eds), *Security and Usability* (pp. 31-46). Sebastopol, CA: O'Reilly.
- Tullis, T. S., & Tedesco, D. P. (2005). Using personal photos as pictorial passwords. In CHI '05: *CHI '05 extended abstracts on Human factors in computing systems*, pp. 1841-1844. New York: ACM Press.
- Valentine, T. (1999). *Memory for Passfaces after a Long Delay*. Technical Report, Goldsmiths College, University of London.
- Weirich, D., & Sasse, M. A. (2001). Persuasive password security. In CHI '01: *Extended abstracts on Human factors in computing systems*, pp. 139-140. New York: ACM Press.
- Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *SSYM'99: Proceedings of the 8th conference on USENIX Security Symposium*. Berkeley, CA: USENIX Association.
- Wickens, C. D. (1992). *Engineering Psychology and Human Performance* (2nd ed.). New York: Harper Collins.
- Wiedenbeck, S., Waters, J, Birget, J.-C., Brodskiy, A., & Memon, N. (2005a). Authentication using graphical passwords: Effects of tolerance and image choice. In *SOUPS '05: Proceedings of the 2005 Symposium on Usable Privacy and Security*, pp. 1-12. New York: ACM Press.
- Wiedenbeck, S., Waters, J, Birget, J.-C., Brodskiy, A., & Memon, N. (2005b). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63 (1-2), 102-127.
- Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J.-C. (2006). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *AVI '06: Proceedings of the working conference on Advanced visual interfaces*, pp. 177-184. New York: ACM Press.

REFERENCES

- Williamson, J., Murray-Smith, R., & Hughes, S. (2007). Shoogle: Excitatory multimodal interaction on mobile devices. In CHI '07: *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 121-124. New York: ACM Press.
- Yahoo! (2004). What's the most popular password? [WWW document]. Retrieved October 23, 2008, from <http://ask.yahoo.com/20041022.html>.
- Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security and Privacy*, 2 (5), 25-31.
- Yee, K.-P. (2004). Aligning Security and Usability. *IEEE Security and Privacy*, 2 (5), 48-55.
- Yee, K.-P. (2006). Guidelines and strategies for secure interaction design. In L. F. Cranor, & S. Garfinkel, (Eds), *Security and Usability* (pp. 247-273). Sebastopol, CA: O'Reilly.
- Zviran, M., & Haga, W. J. (1990). Cognitive passwords: The key to easy access control. *Computers and Security*, 9 (9), 723-736

Plagiarism Declaration

I know the meaning of plagiarism and declare that all of the work in the document, save for that which is properly acknowledged, is my own.