

Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

**An Empirical Study on the Relationship between Identity-
Checking Steps and Perceived Trustworthiness in Online
Banking System Use**

A Thesis

Presented to

The Academic Faculty

By

Yang (Kansi) Zhang

Under the supervision of

Dr. Hokyoung Ryu

Submitted in partial fulfilment

of the requirements for the Degree

Master of Information Sciences in Information Technology

Massey University

20th Feb. 2009

ABSTRACT

Online banking systems have become more common and widely used in daily life, bringing huge changes in modern banking transaction activities and giving us a greater opportunity to access the banking system anytime and anywhere. At the same time, however, one of the key challenges that still remain is to fully resolve the security concerns associated with the online banking system.

Many clients feel that online banking is not secure enough, and to increase its security levels, many banks simply add more identity-checking steps or put on more security measures to some extent to give users the impression of a secure online banking system.

However, this is easier to be said than done, because we believe that more identity-checking steps could compromise the usability of the online banking system, which is an inevitable feature in design of usable and useful online banking systems. Banks can simply enhance their security level with more sophisticated technologies, but this does not seem to guarantee the online banking system is in line with its key usability concern. Therefore, the research question raised in this thesis is to establish the relationships between usability, security and trustworthiness in the online banking system.

To demonstrate these relationships, three experiments were carried out using the simulation of an online banking logon procedure to provide a similar online banking experience. Post questionnaires were used to measure the three concepts, i.e.

usability, security and trustworthiness. The resulting analyses revealed that simply adding more identity-checking steps in the online banking system did not improve the customers' perceived security and trustworthiness, nor the biometric security technique (i.e., fingerprints) did enhance the subjective ratings on the perceived security and trustworthiness. This showed that the systems designer needs to be aware that the customer's perception of the online banking system is not the same as that conceived from a technical standpoint.

CONTENTS

ABSTRACT	II
STATEMENT OF ACADEMIC INTEGRITY.....	IX
ACKNOWLEDGEMENTS	X
CHAPTER ONE: INTRODUCTION AND BACKGROUND.....	1
1.1. INTRODUCTION TO THE STUDY	1
1.2. BACKGROUND TO THE STUDY	5
1.3. RESEARCH QUESTIONS AND POTENTIAL CONTRIBUTIONS	10
1.4. OUTLINE TO STUDY	12
CHAPTER TWO: LITERATURE REVIEW	14
2.1 SECURITY IN ONLINE BANKING	15
2.1.1 <i>Technical view of security in online banking systems.....</i>	<i>17</i>
2.1.2 <i>Customer view of security in online banking system</i>	<i>21</i>
2.2 RELATIONSHIP BETWEEN TRUSTWORTHINESS, USABILITY AND SECURITY	28
2.3 PERCEIVED SECURITY	29
2.3.1 <i>External factors of perceived security</i>	<i>30</i>
2.3.2 <i>Internal factors of perceived security</i>	<i>31</i>
2.4 CONCLUSION.....	32
CHAPTER THREE: METHODOLOGY.....	33
3.1 INTRODUCTION	33
3.2 EXPERIMENT INTERFACES.....	36
3.2.1 <i>Experiment I</i>	<i>36</i>
3.2.2 <i>Experiment II.....</i>	<i>41</i>
3.2.3 <i>Experiment III.....</i>	<i>43</i>
3.3 METHOD	44
3.3.1 <i>EXPERIMENTAL DESIGN</i>	<i>44</i>
3.3.2 <i>PARTICIPANTS.....</i>	<i>45</i>
3.3.3 <i>PROCEDURE.....</i>	<i>46</i>
3.3.4 <i>APPARATUS.....</i>	<i>48</i>
3.4 DATA COLLECTION	49
3.5 DATA ANALYSIS	49
CHAPTER FOUR: RESULT.....	50
4.1 EXPERIMENT I.....	50
4.2 EXPERIMENT II.....	56
4.3 ADDITIONAL ANALYSIS: SYSTEM-INITIATED (EXPT. II) AND USER-INITIATED (EXPT. I)	57
4.4 ADDITIONAL ANALYSIS: USER-INITIATED (EXPT. I) AND FINGERPRINT (EXPT. III)	59
CHAPTER FIVE: DISCUSSION	61

5.1	EXPERIMENT I.....	61
5.2	EXPERIMENT II.....	64
5.3	EXPERIMENT III	65
CHAPTER SIX: CONCLUSIONS		66
6.1	FINDINGS OF THE THESIS	66
6.2	LIMITATIONS OF THE THESIS.....	67
6.3	FUTURE WORK.....	68
REFERENCES.....		70
APPENDIX A		73

LIST OF FIGURES

Figure 1.1 Trade-off relationship between usability and security	4
Figure 1.2 Kiwibank online banking	7
Figure 1.3 Physiological characteristics. (a) Fingerprints; (b) Facial structure; (c) Iris configuration	9
Figure 1.4 Physical characteristics. (a) Handwriting; (b) Keystroke recognition.....	9
Figure 2.1 Secure Sockets Layer	18
Figure 2.2 Public-Key Infrastructures.....	19
Figure 2.3 Symmetric-Key Infrastructures	21
Figure 2.4 ASB Bank FastNet online banking.....	22
Figure 2.5 National Bank online banking	23
Figure 2.6 Kiwi Bank online banking.....	23
Figure 2.7 Bank of China online banking.....	24
Figure 2.8 E-Token device.....	25
Figure 2.9 Industrial and Commercial Bank of China's code card.....	26
Figure 2.10 The fingerprint scanner used for BRCB's online banking system	27
Figure 3.1 The Register Interface	36
Figure 3.2 Step 1 of Interface I	37
Figure 3.3 Step 2 of Interface I	37
Figure 3.4 The account information page	38
Figure 3.5 Step 3 in Interface II	39
Figure 3.6 Step 4 in Interface II	39
Figure 3.7 Step 5 in Interface III.....	40
Figure 3.8 Step 6 in Interface III.....	40
Figure 3.9 Step 7 in Interface IV	40
Figure 3.10 Step 8 in Interface IV	41
Figure 3.11 Step 1 in Interface V	41
Figure 3.12 Step 2 in Interface V	42
Figure 3.13 Step 3 in Interface VI	42
Figure 3.14 Step 4 in Interface VI	43
Figure 3.15 Fingerprint Registration.....	43
Figure 3.16 Fingerprint Logon System (Logon).....	44
Figure 3.17 Fingerprint register	47
Figure 3.18 Connection setup between fingerprint and customer account.....	48
Figure 4.1 Easy to use	51
Figure 4.2 Comfortable to use	52
Figure 4.3 Simple to use	53
Figure 4.4 Secure enough	54
Figure 4.5 Trustworthiness	55
Figure 5.1 Relationship between identity-checking steps and usability	62
Figure 5.2 Relationship between identity-checking steps and security	63

Figure 5.4 Expt. II vs. Expt.I	65
--------------------------------------	----

LIST OF TABLES

Table 2.1 Summary table of security	29
Table 3.1 Summary table of Experiment one	34
Table 3.2 Summary table of Experiment two	35
Table 3.3 Summary table of Experiment three	35
Table 3.4 Summary table of experimental settings.....	35
Table 3.5 Summary table of experimental design	45
Table 3.6 Summary table of participant.....	46
Table 3.7 Post-test questionnaire	49
Table 4.1 Average and standard deviation of rating for each question	50
Table 4.2 Paired sample test for Experiment II	57
Table 4.3 Univariate analysis of variance for order effect.....	58
Table 4.4 Average and standard deviation of ratings for each question.....	59
Table 4.5 Mean and standard deviation of ratings for each question	60
Table 5.1 Summary table of experiment hypothesis.....	61

STATEMENT OF ACADEMIC INTEGRITY

I declare that this research study is entirely my own work and that it has not been copied from the work of other people. If the work and ideas of others have been used in this study, they have been properly cited in the text.

Yang (Kansi) Zhang

ACKNOWLEDGEMENTS

I owe a great deal of gratitude to people who, in various ways, helped make this thesis possible. In particular, I would like to thank my supervisor, Dr. Hokyoung Ryu, for providing me with this opportunity; and my wife and my family for supporting me through this academic study.

CHAPTER ONE: INTRODUCTION AND BACKGROUND

1.1. Introduction to the study

Web-based technologies have been growing and are widely used in many business sectors for their instant and convenient interaction between stakeholders. For example, online banking is very common in our daily activities, giving us a great opportunity for easy access to our banking transaction activities.

Though the online banking system has certain benefits, many customers still seem to believe online banking is still not entirely safe. Several interviews (see interview transcripts below) of online-banking customers in New Zealand show that the security of the online banking system is one of their greatest concerns.

“In response to New Zealand banks being secured inadequately online, I'd like to say that there are plenty more steps the bank could take to up our security. I know StudyLink have one more step which requires a "pass phrase" - a sentence the customer sets and then StudyLink asks for certain letters in the pass phrase each time you log in. It's a simple step which would make it that much harder to hack into people's accounts.” (Cited in “Your say: Online banking security”, 25 March 2008)

“Internet banking has already taken off in most OECD countries. And banks in most of those countries offer security in the offer of 'identifiers' where it is necessary to enter data in offline utilities and copy this onto the website of the bank before being able to do any banking online. In New Zealand, however, one only needs to know a user name and password to do internet banking. That is very risky, as the security of the website is no more than that one of a dating site or any other website where you have to enter a few things. Okay, it is never okay when one manages to get hold of your user name and password but when it is in regard to an 'innocent' website, you take it for granted and move on. But when it is for your bank website you have a serious problem.”

(Cited in “Your say: Online banking security”, 25 March 2008)

Of course, these concerns may come from ignorance of the technical sophistication that the New Zealand banks are currently employing, but it is certainly indicative of the concern about the online-banking systems operating in New Zealand. To take on this security concern in the online banking system, a very simple solution adopted by many banks is to ask the clients more personal identification information. This can, at least, check that the client is legitimate and bona-fide. For instance, banks in some Asian countries (e.g. Korea and Japan) solicit six or seven client identity details in order to begin any banking transaction. Though this approach is simply applied without reservation, several practical studies have found that this was not the

case (Yang, 2007). Rather, the larger number of identity-checking steps implies a greater vulnerability of the system, and, as a consequence, this may signal decreased trust of the system due to its perceived risks. Also, it is thought that this onerous identity-checking procedure has some knock-on effects on the usability and trustworthiness of the system (Gang, 2001). This is definitely the other side of the telescope in relation to the increased security, because the larger number of logon steps will lead to a detrimental effect on usability. Hence, from the usability perspective, simply adding more security features that require extra user attention and interaction with the system would not be preferable. As a consequence, with more identity-checking steps, the trustworthiness of the system, which includes both usability and security, would be cancelled out. Central to this thesis is the idea that there should be a significant consideration of such security measures in developing online banking systems at the expense of usability or trustworthiness. (Joris, 2002).

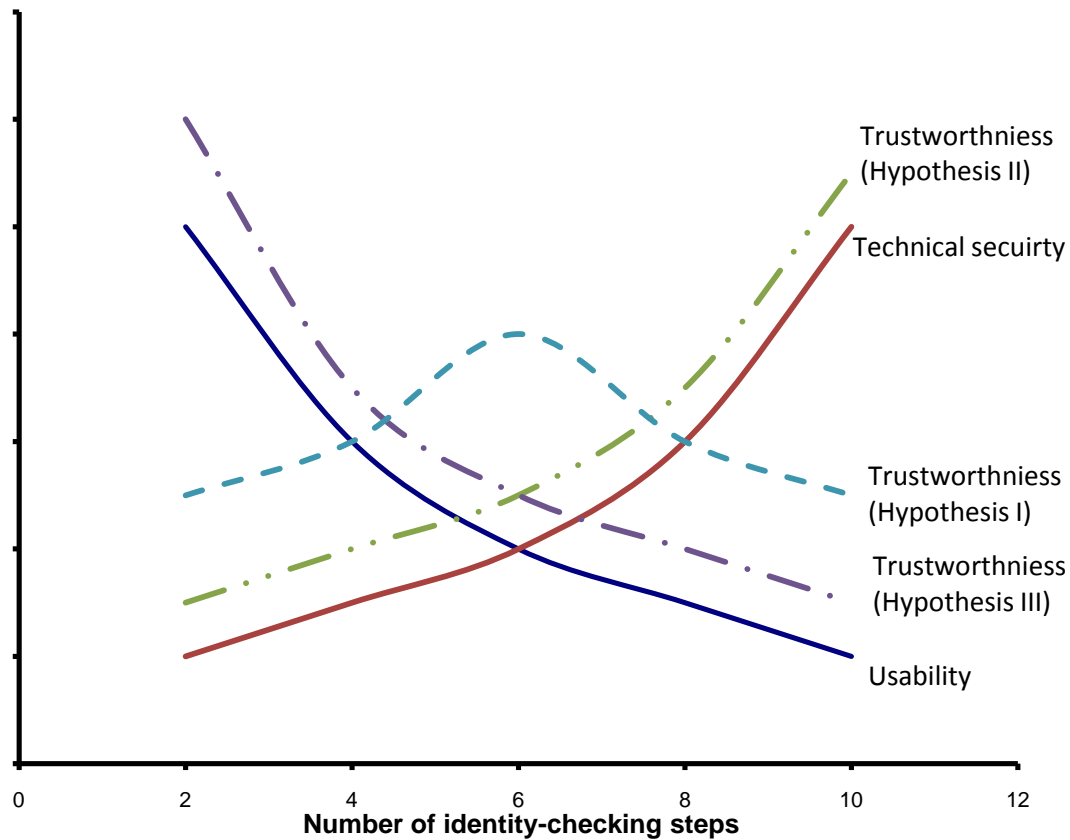


Figure 1.1 Trade-off relationship between usability and security

Having said as the above, there may be a solid relationship between the number of identity-checking steps and usability (and technical security). As shown in Figure 1.1, adding more security features to the online banking system might not benefit the clients at all (see the „Usability“ line). Of course, several methods have been proposed to increase both usability and security. Nasser *et al.* (2006) proposed that fingerprint biometric signatures be both secure and easy to use. However, their research did not provide any empirical data about the relationship between usability and security, which is the main research objective of this thesis.

By and large, in designing online banking systems, the primary concern is to make customers feel the systems be secure enough and easy to use, both of which

comprise the concept of “Trustworthiness” in HCI (Human-Computer Interaction). In HCI, both usability and security promote trustworthiness, but these two constructs are said to not be positively related, which was the impetus for carrying out the research (Al-Ghatani & King, 1999; Markus, 1983).

Consider Figure 1.1 again. The three dotted lines in the figure signify the potential relationships. For instance, if the security dominates usability, its likely relationship would be Hypothesis III. It may be the opposite, as usability is underscored (Hypothesis II). Otherwise, one can see these two would be compromised at some points, as shown in Hypothesis I. To answer this classic tit-for-tat question, three experiments are performed in this thesis. The first two analyse the relationship among the number of identity-checking steps, usability and perceived security. The last experiment tests a way to improve both usability and perceived security, building upon the results from the first two experiments.

1.2. Background to the Study

Security in the online banking system has various features, technically speaking, such as information encryption¹, communication layer protocol², firewall and digital

¹ For further details, please see Federal Information Processing Standard and Data Encryption Standard (DES). FIPS PUB 46-3, US Department of Commerce, National Institute of Standards and Technology, October 1999.

² For further details, please visit:

publib.boulder.ibm.com/infocenter/wasinfo/v1r0/index.jsp?topic=/com.ibm.websphere.ihs_2047.doc/9atssl.htm

signature³. Yet this thesis only focuses on the number of identity-checking steps in the logon procedure, partly because it is the most common method of authenticating genuine customers, and primarily because it is strongly related to the initial usability of the online banking system. Further to this last point, within the online banking system there are many other usability elements – how easy it is to learn, website structure, font colour, information structure, and so on – however it is the client logon procedure that initially determines whether or not this online banking system is easy to use. My negative personal experience of the six-logon procedure employed by a Chinese bank made me feel like I was doing all the work. Therefore, this thesis focuses on this „perhaps“ subtlety of the online banking system to further explore, in association with the security measures.

The term „identity-checking“ describes the whole process of checking the identity of a person or entity. In the online banking system, the identity-checking process begins with the logon procedure to control access to the customer accounts and personal information, normally including the customer’s user name, password and so on. It is not surprising that different banks use rather different identity-checking steps to secure their online banking systems, though the common identity-checking process in New Zealand consists of two steps: user ID and password. Of course, some banks in New Zealand, such as Kiwibank, use more than two identity-checking steps,

³ For further details, please see Federal Information Processing Standard and Digital Signature Standard (DSS). FIPS PUB 186-2, US Department of Commerce, National Institute of Standards and Technology, January 2000.

e.g., access number (or User ID), password and security code generated by the system (refer to “*dwc4*” in Figure 1.2).



Log in details:

Access number:

Password:

Security Step: [What's this for?](#)

Enter the following text in the space below:

dwc4

If you can't read the text, click [here](#) to have it read out to you

Sign on

Figure 1.2 Kiwibank online banking

In designing online banking systems, there also seems to be a cultural difference. As discussed above, in China, some banks use more thorough identity-checking procedures to verify authentic customers⁴, but banks in many Western countries have at most three identity-checking procedures. It would be fair to say that more thorough identity-checking procedures would increase customers' confidence in the security of an online banking system, but this has not been empirically tested.

As mentioned earlier, usability is also an important issue in the design of online banking systems. Good usability is believed to increase the efficiency, effectiveness and satisfaction with which banking customers achieve their intended goal with the online banking system. It is important to note that in terms of usability there are many diverse aspects to consider together. Ryu (2006) defined usability

⁴ The same applies to Korea and Japan.

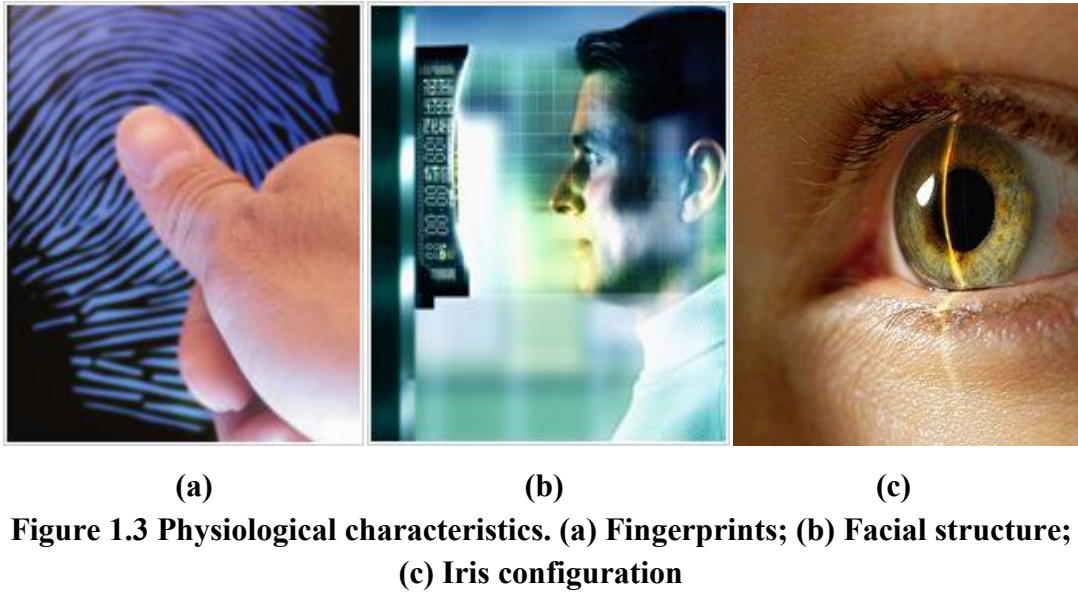
through the four analytic lenses: „easy to use“, „easy to learn“, „useful“ and „pleasant to use“. However, in that most online banking systems are simply “walk-up-and-use”⁵ and their functions are all but the same, and pleasure with banking activities would not be the main cause concern, this thesis considers “easy to use” as the main factor by which to define usability in online banking systems.

In this regard, on the one hand, when the online-banking system adds more identity-checking steps to the login, it makes the customer spend more time supplying information requested. This may, of course, affect the usability of the system. On the other hand, it will, accordingly increase, the customer’s confidence in the security of the online banking system being used. The main research question in this thesis is to identify the likely relationship between these two concepts.

To enhance both usability and security, there are new identity-checking techniques. Biometric identification technologies, based on individual’s physiological or physical characteristics, have recently been used in the online banking system. Physiological characteristics include fingerprints, facial structure, and iris configuration (see Figure 1.3). Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard (see Figure 1.3).⁶

⁵ Walk-up-and-use means the „learning process“ is minimised. An ATM is a walk-up-and-use system because the user does not need a service learning session to operate an ATM

⁶ Authentication in an Internet banking Environment. (2006). Please visit: <http://www.ffiec.gov>.



The most popular biometric data adopted in the online banking system is fingerprints. Fingerprints are unique and cannot be replicated, so they provide a robust template for identity checking (“Authentication in an Internet banking environment”. 2006). One of the benefits of fingerprints is that the customer does not need to recall information (e.g. password or User ID) to logon to the system. For instance, The Reserve Bank of Malawi developed a fingerprint-based online banking system.⁷ Though this seems to be a very effective way to avoid a potential usability problem of

⁷ Malawi bank to use fingerprints (2004). *Biometric Technology Today*, 12(10), 2-3.

the current online banking system, the cost involved would make this unrealistic for most of our online banking users, and handling huge volumes of fingerprint data would be another serious system-development cost.

To encompass usability and security in socio-technical systems, the HCI community has paid much attention to the concept of „trustworthiness“, which is also applied to the design of the online banking system. Gabriele (2007) suggested that trustworthiness means that the system does what is required – despite environment disruption, human and operator errors, and attacks by hostile parties. This concept is even more important in the online banking field than the offline banking environment, in the sense that in the online banking system, the customer cannot face the banking teller directly, so online banking is highly uncertain due to potential errors and attacks (Bomil & Ingoo, 2002). In order to make online banking systems more trustworthy, many banks use multi-step identity-checking procedures or employ more sophisticated technologies to avoid the hacking private information. Although the purpose of online banking-system design is to make the system safer and at the same time help customers ease of use, the conflict between the two may be greater than the banks’ expectations. Hence, this thesis will address this complicated issue bit by bit.

1.3. Research Questions and Potential Contributions

As discussed in the previous two sections, the purpose of this thesis is to explore the potential relationship between the security, usability and trustworthiness in the online-

banking system. Specifically, this thesis will empirically test the following four hypotheses:

Point 1: The relationship between the number of identity-checking steps and usability

The most important benefit of online banking systems is to save time and cost. In this regard, it is hypothesised that as the number of identity-checking steps increases, the customer needs to spend more time and effort, in particular, their cognitive efforts to recall the right information, and to supply the information requested by the system. Consequently, this would affect the usability of the online banking system.

Point 2: The relationship between the number of identity-checking steps and perceived security

Simply put, as the number of identity-checking steps increases, more logon information will be needed to log on to the system. It will probably make the online banking clients feel less concerned about identity theft or being hacked by malware. This hypothesis will be measured through the results of the post questionnaire administered.

Point 3: The relationship between usability (Point 1) and perceived security (Point 2)

Building upon the two hypotheses above, this hypothesis investigates the relationship between the perceived security and usability, in terms of the customer perception of security, rather than from a technical standpoint.

Point 4: Information types and their impacts on both usability and perceived security

There are various types of authentication techniques in the logon process. Some employ personal information, such as password, one-time password, fingerprint, date of birth, digital certificates or security codes created by the bank. It is hypothesised that the security code generated by the bank might be more secure than the user-generated information, so it may be a more reliable way to preserve the customer's perceived security.

1.4. Outline to study

Chapter 2 describes a literature review on the research questions outlined above, and the next chapter (chapter 3) introduces the research design and experimental methods to empirically investigate the research questions. In chapter 4, the results of the post-test questionnaire studies are statistically analysed. The interpretation and analysis of

results is described in chapter 5, and finally, a conclusion is drawn based on the results, and the limitations and future work are also discussed.

CHAPTER TWO: LITERATURE REVIEW

Building upon the ever-advancing Internet technologies, e-commerce has brought new dimensions to our daily lives. For example, online banking systems allow us to easily and conveniently carry out banking activities such as checking account balances, transferring money, transacting with credit cards, and so forth. Obviously, the online banking system provides people with a quick transaction activity and also helps banks increase their efficiency.

Many factors have affected the growth of online banking, including usability, trustworthiness, brand reputation, customer satisfaction, security and so on. In order to encourage customers to use online banking systems, a bank needs to build up a reputation for good customer satisfaction and maintain customer loyalty.

Among several factors, security is considered as paramount (Joris *et al*,2002). The main purpose of the online banking system is to provide a secure and remote delivery channel for banking services to allow customers to easily and quickly manage their bank accounts, so banks always put the security of online banking before other factors. A recent survey on the online banking system in America, showed that around half of Americans are worried about the vulnerability of their online banking, and around a third of the respondents do not completely trust online banking due to the lack of security measures. Another study, performed by TNS Sofres™, also shows that only a fifth of the study participants felt “positive” about the

security in any of the digital technology they use, indicating that the vast majority of Americans remain very wary.⁸ Winnie *et al.* (2002) agree with the idea that the security of online banking is the most important aspect, compared to other factors such as ease-of-use, up-to-date information, brand reputation and so forth. Therefore, it seems that the security of the online banking system is the most important issue that banks need to urgently address. In the following subsections, we review online banking security and its relationship to other contributors to trustworthiness, which are central to this thesis.

2.1 Security in Online Banking

Joris *et al.* (2002) summarised the security of the online banking system as follows:

- Confidentiality ensures that only authorised entities have access to the online banking system;
- Entity authentication allows the genuine customer to communicate with the bank, and the bank should know the identity of the customer before processing their banking activities;
- Data authentication ensures the data integrity.

Likewise, Warwick *et al.* (2002) described the security of e-commerce as the preservation of confidentiality, integrity, authorised use and availability of

⁸ US consumers wary of password security for eCommerce; smartcards to give peace of mind? (2008). *Card Technology Today*, 20(4), 1.

information. Preservation of confidentiality ensures only authorised online banking clients have the right to access their account information, e.g., an unexpected eavesdropper should not see information about a particular user. Hence, authorised use allows the bank to detect the operation by unauthorized users. Integrity means the data stored in the bank should be identically maintained during any operation, such as after transferring money, checking balances and so on. Availability ensures that the customer can access their account and check the information anytime and anywhere.

Yet, in this thesis, we see security from two viewpoints; one is the technical perspective and the other is the customer's perspective. Whilst these two viewpoints are mostly in line with each other, in the online banking field, the two stakeholders (i.e. the bank and the customer) may have different perceptions of security. The bank always tries to employ more secure and sophisticated techniques to protect its online banking system, which strongly implies the technical perspective; whereas, customers do not care what kind of techniques are used to protect their account, but are instead concerned with how they feel about whether or not the system is secure. Also, these sophisticated and technical security measures are mostly invisible to customers, so the customers may not be entirely sure of whether or not the technical sophistication is necessary. That is, security from the technical perspective is used to ensure the confidentiality, integrity, availability and authorized use of information. In contrast, security from a customer's view does not seem to be the same. Simply put, it is about

the perception of online banking security, regardless of the sophisticated security measures.

In this thesis, the most important disclosure is not understanding the technical perspective on security measures, but rather, it is looking at the user's perspective that is central to this thesis.

2.1.1 Technical view of security in online banking systems

From a technical standpoint, security measures in online banking systems are about using techniques to make online banking systems more secure and immune to harmful attacks. To do this, the five major commercial banks in New Zealand (i.e. ASB, ANZ-National, BNZ, Westpac and Kiwibank) offer a variety of services based on a 128 encryption security protocol called „Secure Sockets Layer“ (SSL). Data security between the customer browser and the bank web server is handled through this SSL, providing data encryption, server authentication, and message integrity for an Internet connection.⁹ SSL sets up a secure communication channel between the client and the bank (Juries *et al.*, 2002), using two keys that are a combination of public/asymmetric-key and secret/symmetric-key to secure data transfer. „Public-key“

⁹ Online Banking System Security. (2008). Data encryption is the most popular encryption method to ensure the confidentiality of sensitive information by using a private key, since it was standardized by the U.S National Institute of Standards and Technology (NIST) in 1977. It is used in almost every type of application, such as email and online banking truncations. Server authentication is used to provide authentication services to the clients. Message integrity is used to ensure that the contents of the message have not been damaged for any reason.

is used as cryptography based on pairs of keys known as public key and private key. The public key is published while the secret key is kept secret with the owner. Client and server need to share a secret key. The secret/symmetric key is used to encrypt and decrypt the message. To do so, before the data transfer occurs between the client and the bank, a “handshake” is created for initiating the connection to make the client and the bank agree on a set of cryptographic algorithms. Once the “handshake” has been completed, the connection is ready to transfer the data between the client and the bank. This is the most popular technique used by most banks (ANZ-National online banking systems explicitly shows this technique in use.) Figure 2.1 shows how the Secure Sockets Layer (SSL) works.

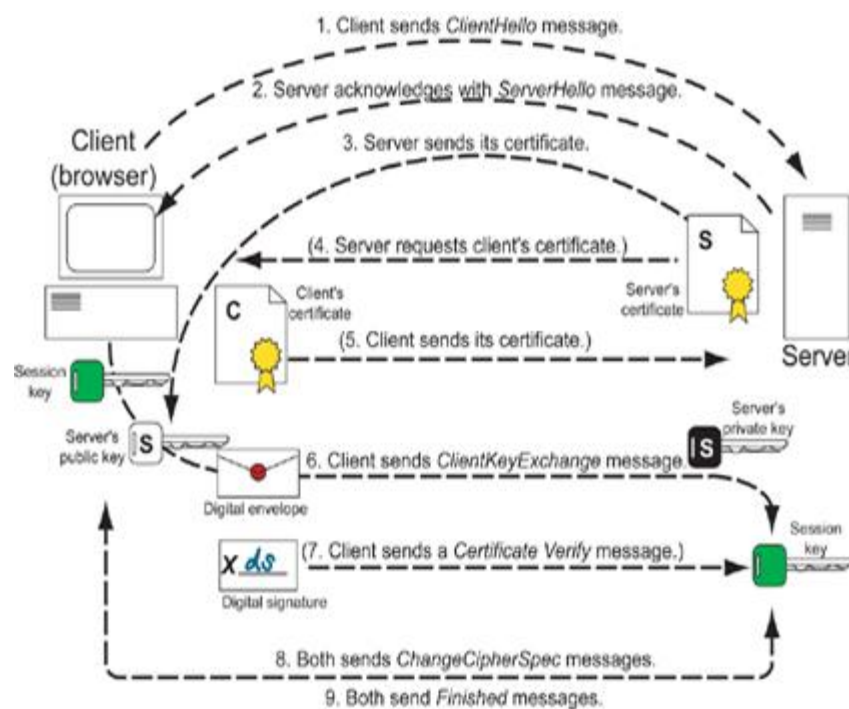


Figure 2.1 Secure Sockets Layer

In Figure 2.1, steps 1 to 5 depict the “handshake” process. A client sends a request to the server (1) and the server acknowledges the request (2). Then the server

requests the certificate from the client (3, 4). The client sends the certificate back to the server, as the server is genuine, and then the server also checks the certificate (5). After this “handshake” process, the client sends a session key seed that is encrypted with SSL public key to the server (6). After the server receives the session key seed, it indicates all future transmissions are encrypted (7), so both sides can communicate with the secure connection (8, 9).

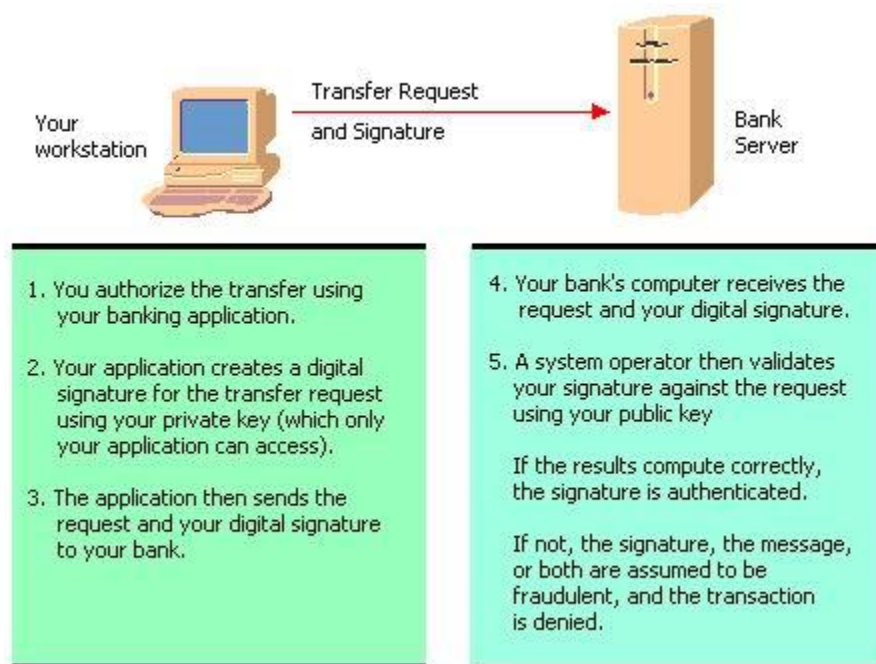


Figure 2.2 Public-Key Infrastructures

Another technique being widely adopted in the modern online banking system is message encryption. There are two kinds of message encryption, one is asymmetric and the other is symmetric. Public-Key Infrastructures (PKI) is one of the popular asymmetric cryptography techniques used to verify the identity of parties involved in a transaction, such as identifying the client and the server. Figure 2.2 illustrates how the PKI works. First, as the customer wants to communicate with the bank, he or she

sends an action request using the banking application (e.g. Shinhan™ bank in Korea uses this technique for Macintosh™ computers). The banking application creates an action request with the digital signature, which includes the customer's private key. Then the banking application sends the request along with the digital signature and a public key assigned to the bank server. The server verifies the request that actually comes from the customer by using the customer's public key. Whenever the verification process is successful, the signature is authenticated and the subsequent transaction is allowed. PKI tends to always be used together with SSL. First, the customer needs to set up a connection by using the SSL and then use PKI. In this case, the PKI is used to issue a digital certificate to the server to activate SSL to encrypt the data between the browser and server. For example, Scotia bank of Toronto, Canada, has deployed PKI with more than 100,000 users on the Internet for its online banking system (Wing, 1999). The Public-Key technology provides encryption to keep information confidential, and through digital signatures, it provides for authentication, data integrity, and no repudiation (Wing, 1999).

The other technique is the symmetric key technique, *a.k.a.*, “Secret Key Cryptography”. It keeps the information private by using the same key for the sender and receiver. This only differs slightly from the asymmetric encryption technique, which uses only one single key to encrypt and decrypt the message. The sender uses the key to encrypt the message and the receiver uses the same key to decrypt the

message. This technology is widely used and operates on a minimum 56-bit base key (Internet Banking-Comptroller's Handbook, 1999).

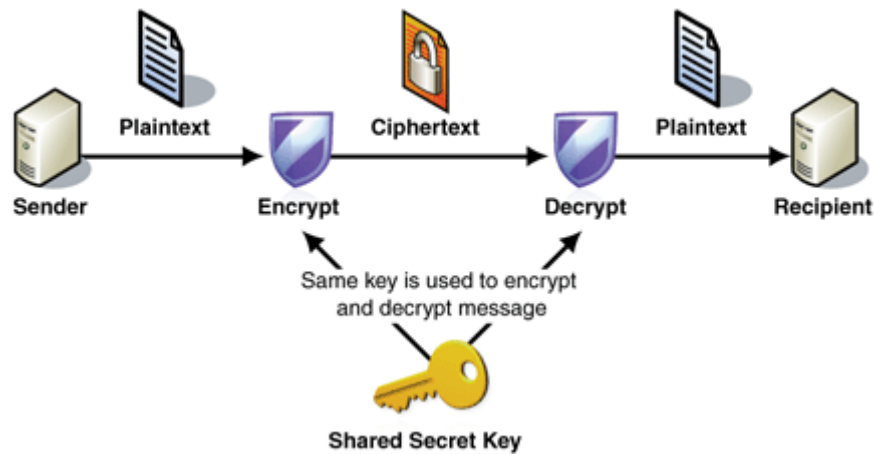


Figure 2.3 Symmetric-Key Infrastructures

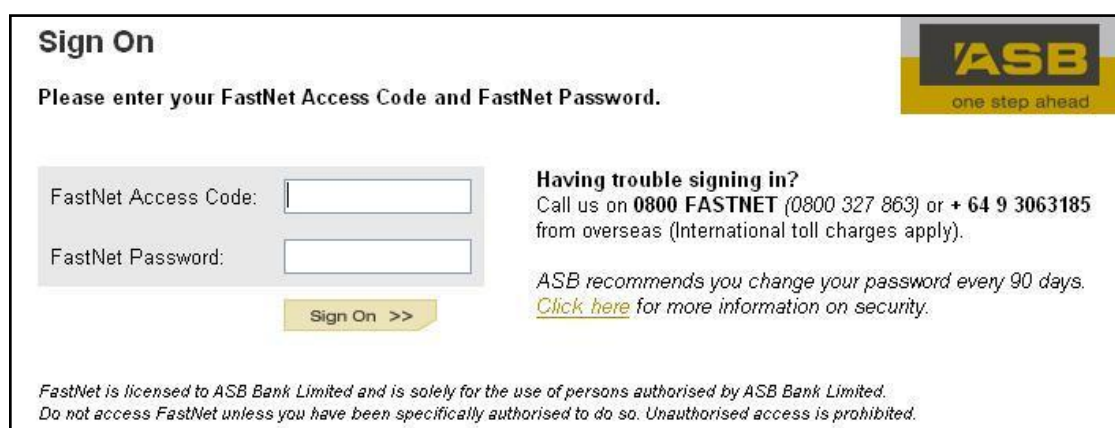
Figure 2.3 illustrates how this process works. The sender passes the secret key to encrypt the message and then sends it to the recipient, and the recipient uses the same secret key to decrypt the message. This is much simpler than Public-key encryption, which attracts many system developments based on this.

2.1.2 Customer view of security in online banking system

In terms of the sophisticated technologies discussed above, the user's perception of the security measures might not be the same. In other words, their perception on the sophisticated security measures would be minimal from these tech-savvy feelings. Perhaps they might be more concerned about identity theft, forgotten passwords, identification hacking and so on. Of course, the technologies discussed above would fulfill the customer's perceived security, but most customers would be still more concerned about whether the identity-checking step in initiating their connection with

the bank server could be more secure. In this light, the technical perspective of the online banking system here is not the major concern of the user's activity.

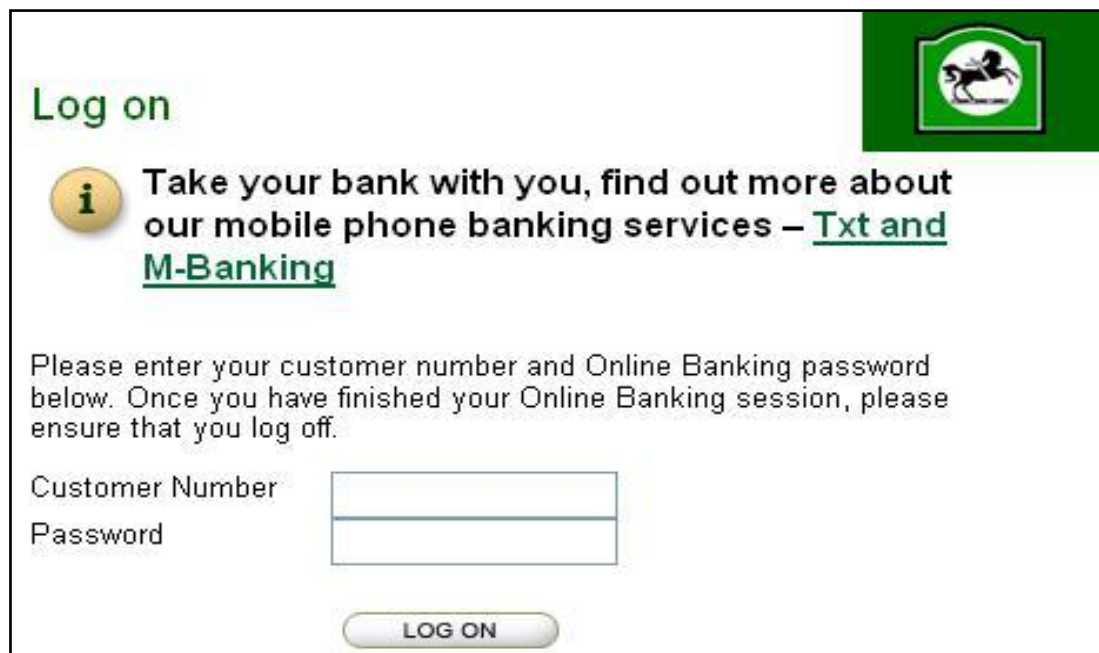
Identity checking in the online banking system can be divided into two categories. One is user-initiated; the other is system-initiated. The former indicates all the individual-oriented information entered, such as user name, password and date of birth; some banks even use the maiden name of the customer's mother. In contrast, some banks present the system-initiated information, such as customer number (please note that this is not the user name or ID specified by the user), dedicated security codes, and so forth. To exemplify the user initiated personal information, consider Figure 2.4. The Auckland Saving Bank (ASB) employs user-initiated data for its identity checking. It requires the „Access Code“ (i.e., FastNet Access Code in Figure 2.4, like user ID) that users create themselves, and the password, which is first given by the system and can later be changed by the user (see FastNet Password shown in Figure 2.4).



The screenshot shows the ASB Bank FastNet online banking sign-on page. At the top left, it says "Sign On" in bold. Below it, a message reads "Please enter your FastNet Access Code and FastNet Password." In the top right corner, there is an ASB logo with the tagline "one step ahead". The main content area contains two input fields: "FastNet Access Code:" and "FastNet Password:", each followed by a text box. Below these fields is a yellow button labeled "Sign On >>". To the right of the input fields, there is a section titled "Having trouble signing in?" which provides contact information: "Call us on 0800 FASTNET (0800 327 863) or + 64 9 3063185 from overseas (International toll charges apply)." Below this, it states "ASB recommends you change your password every 90 days." and includes a link: "Click here for more information on security." At the bottom of the page, there is a small disclaimer: "FastNet is licensed to ASB Bank Limited and is solely for the use of persons authorised by ASB Bank Limited. Do not access FastNet unless you have been specifically authorised to do so. Unauthorised access is prohibited."

Figure 2.4 ASB Bank FastNet online banking

In contrast, National Bank of New Zealand uses both the system-initiated identity “Customer Number” in Figure 2.5 and the password as the user-initiated identity checking (see Figure 2.5). Here, the customer number is printed on the customer’s bankcard so it does not need to be remembered, and the password is initially generated by the system, and the customer can change it later.



The screenshot shows the National Bank online banking login interface. At the top left, it says "Log on" in green. To the right is the National Bank logo, which is a green square with a white horse. Below the "Log on" text is a yellow circular icon with a lowercase 'i'. To the right of this icon is the text: "Take your bank with you, find out more about our mobile phone banking services – [Txt and M-Banking](#)". Below this is a paragraph: "Please enter your customer number and Online Banking password below. Once you have finished your Online Banking session, please ensure that you log off." There are two input fields: "Customer Number" and "Password". Below these fields is a green button with the text "LOG ON".

Figure 2.5 National Bank online banking



The screenshot shows the Kiwibank online banking login interface. At the top right is the Kiwibank logo, which is a green square with the text "kiwibank" in white. Below the logo is the text "Log in details:". There are two input fields: "Access number:" and "Password:". Below these fields is the text "Security Step: [What's this for?](#)". Below this is a paragraph: "Enter the following text in the space below:". There is a small input field containing the text "dwc4". To the right of this field is the text: "If you can't read the text, click [here](#) to have it read out to you". Below this is a black button with the text "Sign on".

Figure 2.6 Kiwibank online banking

By comparison, Kiwibank employs an additional logon step with the dynamic security code (see Figure 2.6). The main difference with other online banking systems previously discussed is that Kiwibank uses a security code, e.g. “*dwc4*” in Figure 2.6, which allows this security code to guarantee SSL. Therefore, this online banking system has both “user-initiated” and “system-initiated” information.

In adopting either “user-initiated” or “system-initiated” information, there seems to be a cultural element. The banks in China employ more thorough identity-checking steps than the others do. For example, Bank of China, which is one of the largest commercial Chinese banks, has combined both the user-initiated and system-initiated approaches in its logon procedure. Firstly, it employs the “user-initiated” procedure, along with the user name (6-20 digits and letters in English) and password (8-20 digits and letters in English) (see Figure 2.7); and then it requires a further six-digit dynamic password generated by „E-Token“, which refreshes every 60 seconds.

The screenshot shows the Bank of China online banking login interface. It includes a 'LOGIN' title, the Bank of China logo, and input fields for 'User ID', 'Password', and 'E-Token'. Annotations on the left categorize the first two fields as 'User-initiated' and the third as 'System-initiated'. There are also links for recovering user ID/password and downloading security controls, and a 'Login' button at the bottom.

Figure 2.7 Bank of China online banking



Figure 2.8 E-Token device

„E-Token“ is passed through an electronic device (see Figure 2.8) with an embedded battery, a password-generation chip and a display screen, using an automatically generating dynamic passwords algorithm, *a.k.a.* One-Time-Pad (OTP) system. The password to be entered in the online banking system is different every single minute. Hence, it is widely thought that E-Token greatly enhances the logon and transaction security of online banking¹⁰.

Alternatively, the Industrial and Commercial Bank of China (ICBC) uses the „Code Card“ (see Figure 2.9). A matrix of character strings is printed on the Code Card. When a customer makes a transaction with ICBC, it asks for random coordinates, such as (I, 2), and the customer needs to key in the correct three digits at these coordinates (e.g. “135” in this example).

¹⁰ Security Mechanism – E-Token , please refer to <http://www.boc.cn/ebs/en/Logonfaqpsn3.html>

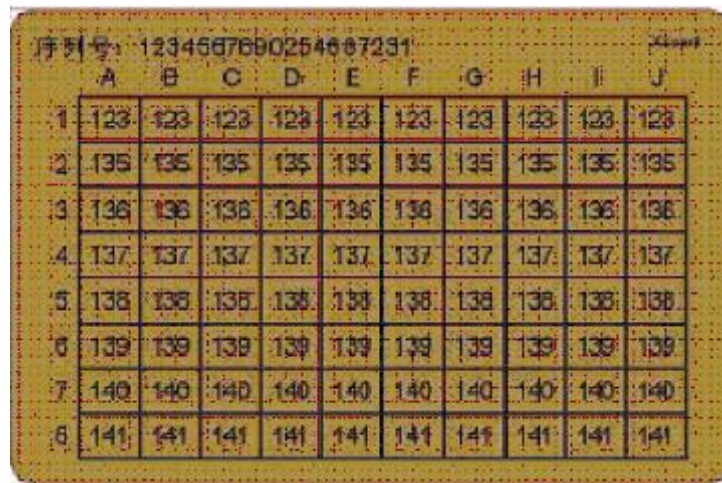


Figure 2.9 Industrial and Commercial Bank of China's Code Card

All the examples above show that most banks are currently employing either user-initiated or system-initiated or a combined approach to ensure security in their online banking system. Yet, as is evident in the previous examples, the logon procedure in the online banking system requires at least two interaction steps. Recently, another technology, biometric identity checking, has easily found its way into the online banking system in order to improve the limitations of the current online banking login interface. For instance, Beijing Rural Commercial Bank (BRCB) is the one of the first banks with the fingerprint technology for banking activities in China (see Figure 2.10). It provides a more convenient and faster way of logging on (i.e. virtually one-step logon), and no need for a bank card or Code Card. Instead, it scans the customer's fingerprint to log on to the system, which is connected to the terminal in the bank. However, this is not yet widely employed in China, because the service is not free of charge at this time.



Figure 2.10 The fingerprint scanner used for BRCB's online banking system

Compared with the Chinese online banking systems, most banks in New Zealand (and most of the banks in Western countries) use, at most, two or three identity-checking steps for their logon procedure. This is a relatively simple logon procedure and implies a cultural difference between China and New Zealand. Gurvinder *et al.* (2004) claimed that the ethical backgrounds of different countries affect online banking design, saying that compared with customers in the Asian group, customers in New Zealand held privacy in greater esteem. These findings implied that ethnic and cultural background plays another important role in influencing the design of online banking. However, this issue has not been thoroughly investigated in this thesis, which is beyond the scope of this study.

Also, population could be considered another important factor in determining the design considerations of an online banking system. In this regard, New Zealand has a population of around 4 million, while China has more than 1.4 billion people. The difference means that the Chinese online banking system employs more security measures than that of New Zealand.

2.2 Relationship between Trustworthiness, Usability and Security

The trustworthiness of online banking can be defined as an attitude of confident expectation that one's vulnerabilities will not be exploited. It can be considered that both security and usability are the constructs of trustworthiness (Cynthia *et al.*, 2003). Security in the online banking system provides protection against harmful threats and increases the customer's trust in the online banking system. Usability can also increase the trustworthiness of the system. Kubilus (2002) claimed that the implementation of a trustworthy e-commerce interface shares many of the general design features for effective interface usability when applied to e-commerce websites. Based on these studies discussed above, it may be said that both security and usability can increase the customer's trust in the online banking system.

Yet, it is evident that these two constructs for trustworthiness are in conflict in the online banking logon procedure. It is a common belief that to increase security with more logon steps will inevitably sacrifice the usability of the system, and fewer identity-checking steps would not be good for the perceived security of the online banking system. From the previous literature (e.g., Joris, 2002), it seems evident that usability is the cost of security on the client side. Technically speaking, it is always possible to continuously add more security features to the system. Yet, at the same time, this also raises the chance of reducing usability of the system, in terms of ease-of-use, ease-of-learning and comfort-of-use. It is the author's belief that additional

technologies to make the system more secure would not guarantee a user's "perceived security", which can be defined as the user's feeling about the security.

On the whole, the three elements of online banking system seem to rely on one another. And this is central to the research question in this thesis.

2.3 Perceived Security

Table 3.1 Summary table of security

	Object	Content	Attributes
Perceived security	Customer	User attitude	Honesty, Predictability
		Controllability	Control
		Usability	Easy to use and easy to learn
Technical security	System	Security technologies	Expertise
		Protection and efficiency	Reputation

As previously mentioned, this thesis focuses on the security from the customer perspective, so this kind of security can be considered as „perceived security“. Table 3.1 shows the differences between perceived security and technical security. Banphot *et al.* (2008) defined „perceived security“ as the perception that interactions are safe and secure. Also Flavián *et al.* (2006) defined it as the subjective probability with which consumers believe that their personal information (private and monetary) will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations. It is very true that all of the studies above emphasised that the security perception by the clients would not be the same as measures taken by the technical standards.

In perceived security, two main factors can impact on the customer's perception of security. These are external and internal factors.

2.3.1 External factors of perceived security

External factors refer to psychological issues (Cynthia *et al.*, 2003). These are the good or bad attitudes that come from the information customers receive from daily life, such as the credibility of the bank. Cynthia *et al.*, (2003) claimed that credibility could be measured in terms of: „honesty“, „predictability“, „credibility“ and „reputation“. Honesty is any truthful communication related to the truth of the event. For instance, the bank needs to be honest with its customers when security has been breached¹¹. Otherwise, customers will have suspicions about online banking security, which can eventually affect the customer's perceived security. Predictability is a client's expectation of trust, which acts consistently based on their past experience (Kee and Knox, 1970; Rotter, 1971; Barney and Hansen, 1994; Fogg *et al.*, 2001). For example, good past experience of the trustworthiness of the online banking system will create a good perception of the security of that online banking system. Ganesan (1994) identified reputation as a characteristic of credibility. For example, the public reputation of a trustworthy website captures the quality of recognised past performance, and therefore, credibility involves the public reputation of the website.

Fogg and Tseng (1999) pointed out that credibility is an important factor in a user's perceptions of online environments. It is the cue of a customer's trust. Hence,

¹¹ “Honesty the best online policy” please refer to <http://news.bbc.co.uk/1/hi/technology/6944435.stm>

good credibility will bring greater trust and greater trust will increase the customer's perceived security.

2.3.2 Internal factors of perceived security

Internal factors to increase perceived security are related to the controllability of online banking. In HCI, controllability is defined as the ability of the user to determine the nature and timing of the adaptation and interaction (Jameson & Schwarzkopf, 2002). Hence, as the customer can control the online banking interface and do whatever they want, they will feel comfortable and confident with the online banking system. It is my personal experience that the New Zealand online banking systems are not entirely compatible with the Safari™ web browser and its controllability is very limited. In this regard, Lewicki and Bunker (1996) rightfully pointed out that system controllability could enhance the customer's perception of security and increase a customer's confidence in this respect.

In the design of online systems, controllability is the key issue of usability. Norman (1994) pointed out that an important aspect of people's comfort with their activities is the feeling of control they have over these activities. For example, good navigation, ease-of-learning and comfort-of-use can help customers control the system and improve usability. Therefore, high controllability engenders more trust in a customer for a specific system, and also increases the perception of its security.

2.4 Conclusion

This chapter discusses the current security technologies in online banking systems and related issues with usability, security and trustworthiness. Three experiments are created to find answers to the research questions raised in the thesis. The next chapter discusses how the experiments are designed and what methods are used for the experiments to empirically examine the research questions in this thesis.

CHAPTER THREE: METHODOLOGY

In this chapter, we describe three experimental settings and procedures to test the relationship between the number of identity-checking steps and usability; the relationship between the number of identity-checking steps and perceived security; and the relationship between the number of identity-checking steps and trustworthiness, respectively. Section 3.1 introduces the purposes of each experiment. Section 3.2 describes the apparatus employed in the experiment. Section 3.3 shows the method and procedure of the experiments. Finally, sections 3.4 and 3.5 describe the data collection methodology and statistical analyses used in the three experiments.

3.1 Introduction

The first experiment is to investigate whether simply increasing the number of identity-checking steps would increase participants' perceived security. The relationship between the number of identity-checking steps and perceived security may not be a simple positive relationship. To empirically demonstrate this, four different interfaces are considered in the logon process.

Interface I has two identity-checking steps, with step 1 (user name and password) and step 2 (security code and date of birth). See Table 3.1 for further detail. Interface II has four identity-checking steps, which include the two steps in Interface I, plus registration email (step 3) and mobile number (step 4). Interface III has six identity-checking steps, which include the four steps of Interface II as well as a

security question (step 5) and the account number (step 6). Finally, Interface IV has eight identity-checking steps, which include all the identity-checking steps in Interface III, as well as the first four digits of the card number (step 7) and the last four digits of the card number (step 8). Table 3.1 summarises the differences between the four interfaces considered in this experiment. Of course, these four interfaces would not ensure the usability of the whole online banking system, but would be sufficient for one to see how the first impression of the user interface in the online banking system might dictate the other related issues. This will be described in more detail later.

Table 3.1 Summary table of Experiment one

Interface conditions	Base steps	Additional steps	
Interface I (2 steps)	User name, password	Security code, Date of birth	
Interface II (4 steps)	Interface I (2 steps)	Registration email	Mobile number
Interface III (6 steps)	Interface II (4 steps)	Security question	Last 4 digits of account number
Interface IV (8 steps)	Interface III (6 steps)	The first 4 digits of card number	The last 4 digits of card number

The second experiment explores whether the different types of identity-checking information would increase participants' perceived security. In this experiment, two interfaces are considered. Interface V has two identity-checking steps with the customer number and security code (see Table 3.2). Interface VI has four identity-checking steps, which include the identity-checking steps of Interface V, and the card number and another security code (see Table 3.2). Note that the identity-

checking information used in this experiment is all system-initiated, with nothing generated by the user of the system.

Table 3.2 Summary table of Experiment two

Interface conditions	Identity-checking steps (system initiated)			
Interface V (2 steps)	Customer number		Security code	
Interface VI (4 steps)	Customer number	Card number	Security code 1	Security code 2

The third experiment explores whether the biometric data would help participants to increase their perceived security, as many advocates of the technology have promised. This experiment consists of an interface with the fingerprint facility to logon into the system (see Table 3.3). Table 3.4 summarises all the experiment settings in this thesis.

Table 3.3 Summary table of Experiment three

Interface conditions	Identity-checking steps (biometric)
Interface VII	Fingerprint

Table 3.4 Summary table of all the experimental settings

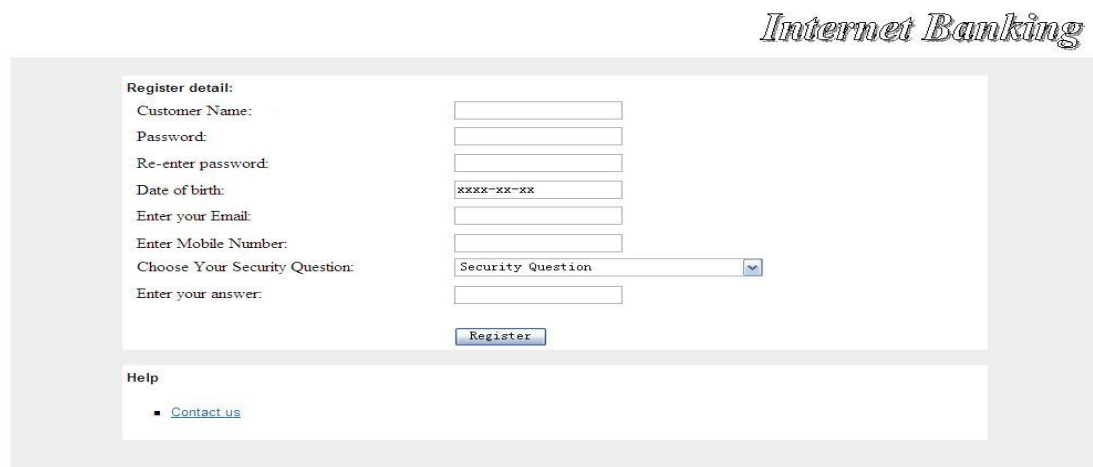
	Number of Interfaces	Number of Identity-checking steps	Identity-checking information
Experiment I	4	2, 4, 6, 8	User-initiated
Experiment II	2	2, 4	System-initiated
Experiment III	1	1	Biometric

3.2 Experiment Interfaces

All the interfaces used in the experiment are simulations of the online banking logon interface. Three experiments have similar interfaces but with different types of identity-checking steps and information to be filled in.

3.2.1 Experiment I

For the first experiment, each participant fills in two parts. One part is the registration interface (see Figure 3.1); the other is the logon interface (see Figure 3.2).



The screenshot displays a web interface titled "Internet Banking" in a stylized font. Below the title is a registration form with the following fields and controls:

- Register detail:**
 - Customer Name:
 - Password:
 - Re-enter password:
 - Date of birth:
 - Enter your Email:
 - Enter Mobile Number:
 - Choose Your Security Question: (dropdown menu)
 - Enter your answer:
-
- Help**
 - [Contact us](#)

Figure 3.1 The Registration Interface

Figure 3.1 is the registration interface that all the participants must go through to complete the main experimental session. It is also necessary to guide each participant to a randomly designated experimental condition. This interface is only a one-off procedure before the participants set up their online banking account.

The screenshot shows a web page titled "Please sign on...". It contains a "Log in details:" section with input fields for "Customer Name" and "Password". Below this is a "Security Step 1:" section with the instruction "Enter the following text in the space below:". A box displays a security code "apsd". There is an input field for the code and a dropdown menu labeled "Select the logon interface:" with the option "----logon interface----". At the bottom of the form are "Next" and "Register" buttons. A "Help" section at the bottom left contains a link to "Contact us".

Figure 3.2 Step 1 of Interface I

Figure 3.2 depicts Interface I. With this interface, customers need to do two tasks. The first is to fill out „Customer Name“, „Password“ and „Security Code“, and then click „Next“, which leads to the second step in the logon procedure as shown in Figure 3.3. Therefore, Interface I has two logon steps, i.e. base information (ID and password), step 1 (Security code) and step 2 (Date of birth).

The screenshot shows a web page titled "Please sign on...". It contains a "Security Step 2:" section with the instruction "Enter your birthday:". Below this are three dropdown menus for "Day", "Month", and "Year". At the bottom of the form is a "Next" button. A "Help" section at the bottom left contains a link to "Contact us".

Figure 3.3 Step 2 of Interface I

Figure 3.3 depicts the second step of Interface I. In this page, participants select the date of birth from the drop-down list, the account information is shown as the participant clicks „Next“ (see Figure 3.4).

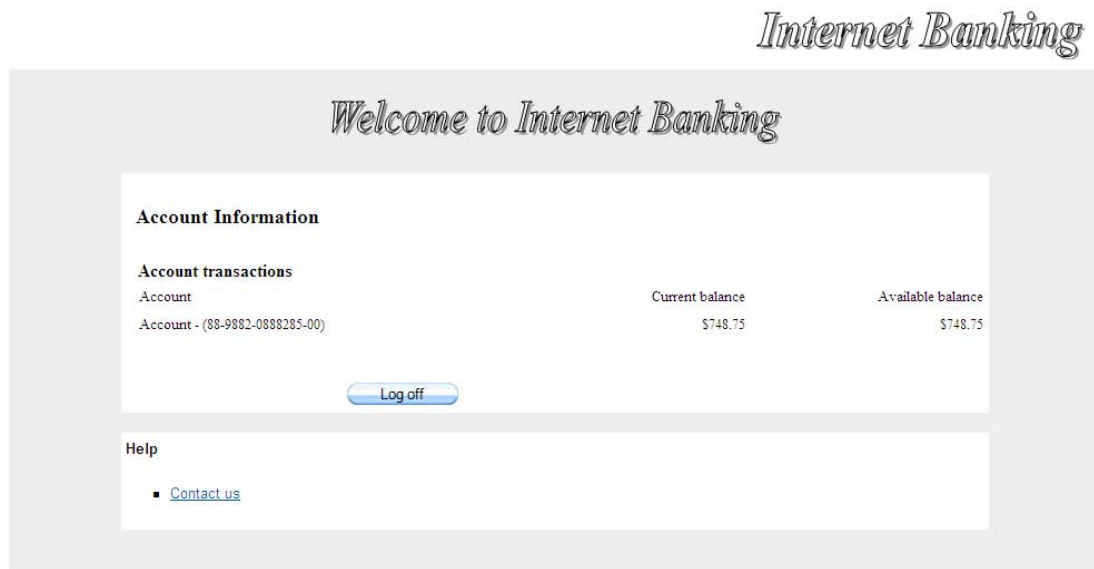


Figure 3.4 The account information page

The other interfaces used in this experiment have the same steps, except for the additional steps designated for each interface. For instance, both Figure 3.5 (step 3 of Interface II) and 3.6 (step 4 of Interface II) show the additional logon steps used in Interface II. Please note that Interface II also comes with both Figure 3.2 and 3.3 before completing Figure 3.5 and 3.6.

Please sign on...

Security Step 3:
Enter your registration Email:

Next

Help

- [Contact us](#)

Figure 3.5 Step 3 of Interface II, filling in the registration email as the third logon step

Please sign on...

Security Step 4:
Enter Mobile Number:

Next

Help


- [Contact us](#)

Figure 3.6 Step 4 of Interface II, asking participants to key in their mobile number, and then go to the account information page (please refer to Figure 3.4)

Likewise, both Figure 3.7 and 3.8 show the additional logon steps used in Interface III, and Figure 3.9 and 3.10 show the additional logon steps used in Interface IV.

Please sign on...

Security Step 5:

Choose Your Security Question: 

Enter your answer:

Help

■ [Contact us](#)

Figure 3.7 Step 5 of Interface III, filling in the security question that they submitted at the registration page

Please sign on...

Security Step 6:

Enter last four digits from your Account Number:

Help

■ [Contact us](#)

Figure 3.8 Step 6 of Interface III

Please sign on...

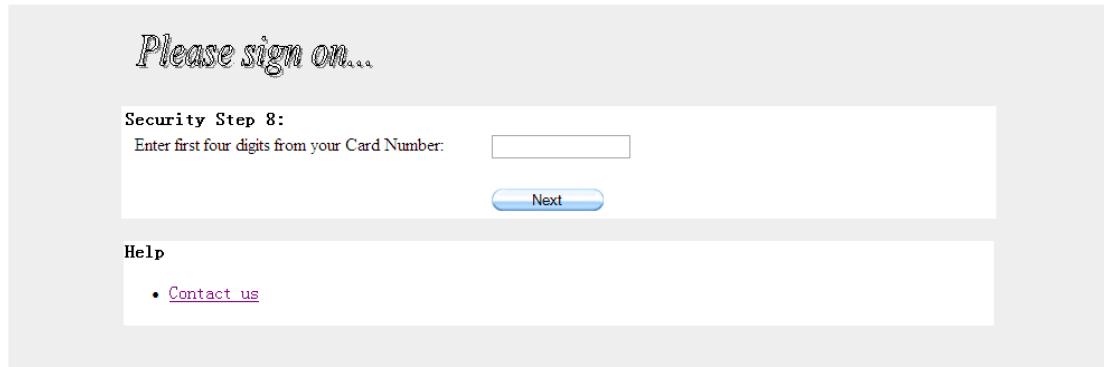
Security Step 7:

Enter last four digits from your Card Number:

Help

■ [Contact us](#)

Figure 3.9 Step 7 of Interface IV

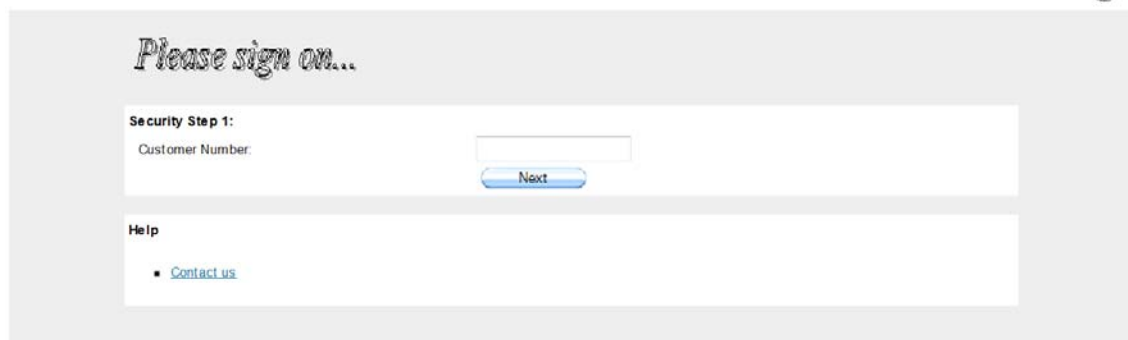


The screenshot shows a web interface for Internet Banking. At the top right, the text "Internet Banking" is displayed in a stylized, italicized font. Below this, the heading "Please sign on..." is centered. The main content area is divided into two sections. The top section, titled "Security Step 8:", contains the instruction "Enter first four digits from your Card Number:" followed by a text input field. Below the input field is a blue button labeled "Next". The bottom section, titled "Help", contains a single bullet point with the text "Contact us" in a blue, underlined font.

Figure 3.10 Step 8 of Interface IV

3.2.2 Experiment II

The simulated systems used for the second experiment are the same as the first experiment, except that the type of information is different. Experiment I used several pieces of user-initiated personal information (i.e., customer name, user ID, password, and date of birth). In contrast, Experiment II used only system-initiated personal information (e.g., customer number and security codes¹²). Experiment II employed two interfaces: Interface V and Interface VI.



The screenshot shows a web interface for Internet Banking. At the top right, the text "Internet Banking" is displayed in a stylized, italicized font. Below this, the heading "Please sign on..." is centered. The main content area is divided into two sections. The top section, titled "Security Step 1:", contains the instruction "Customer Number:" followed by a text input field. Below the input field is a blue button labeled "Next". The bottom section, titled "Help", contains a single bullet point with the text "Contact us" in a blue, underlined font.

Figure 3.11 Step 1 of Interface V

¹² Please note that this is not a password used in Experiment 1, see below for further detail.

Figure 3.11 depicts the first logon page of Interface V. In this page, customers need to key in the „Customer Number“ (not the „Customer Name“ as used in Interface I-IV). Clicking „Next“ leads to the second logon page of Interface V (see Figure 3.12).

Internet Banking

Please sign on...

Security Step 2:
Enter the security code: (Enter the number of 5F on your security card)

[Log on](#)

Help
▪ [Contact us](#)

Figure 3.12 Step 2 of Interface V

Figure 3.12 shows the second logon page of Interface V. In this page, participants need to use the matrix card (see Figure 2.9). Please note that this is not a password used in Experiment 1. After successfully completing these two logon steps, the account information is shown as Figure 3.4. Both Figure 3.13 and 3.14 show the additional logon steps used in Interface VI.

Internet Banking

Please sign on...

Security Step 3:
Enter your card number:

[Next](#)

Help
▪ [Contact us](#)

Figure 3.13 Step 3 of Interface VI



Figure 3.14 Step 4 of Interface VI

3.2.3 Experiment III

Experiment III was designed with a fingerprint logon system as shown in Figure 3.15 and 3.16. Firstly, participants need to register their fingerprint as shown in Figure 3.15. The pop-up window in Figure 3.15 is the software interface to register their fingerprint. After this registration step, the participants only need to scan their fingerprint on the fingerprint reader, and the system will automatically fill in the customer's number and password, and then log on to the system (see Figure 3.16).

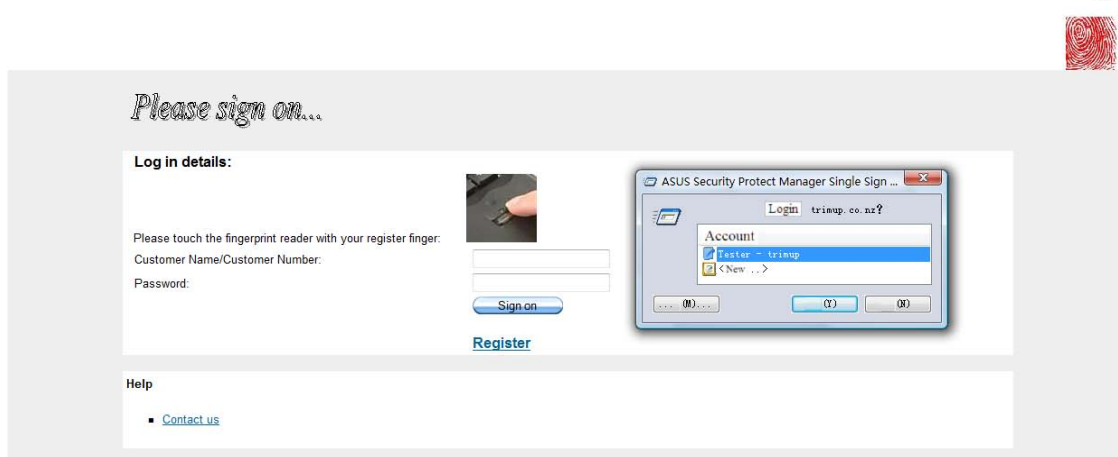


Figure 3.15 Fingerprint Registration



Figure 3.16 Fingerprint Logon System (Logon)

3.3 Method

3.3.1 Experimental design

The first experiment used a one-way between-subjects design. The independent variable was the system having the different number of identity-checking steps, and the dependent variables were the subjective ratings (on Likert scale) on the perceived security, trustworthiness and usability collected from the post questionnaire (see below for the questionnaire).

The second experiment employed a one-way within-subjects design where each participant used both interfaces (Interface V and VI). The independent variables were the system having the different types of identity-checking information and the number of logon steps. The dependent variables were the subjective ratings on perceived security, trustworthiness and usability that were measured with the post questionnaire study.

The third experiment used a one-way between-subjects design, compared with Interface II from Experiment I. The independent variable was the number of identity-checking steps, and the dependent variable was also the subjective ratings on perceived security, trustworthiness and usability that was also administered by the questionnaire. Table 3.5 summarises these experimental designs considered in this thesis.

Table 3.5 Summary table of experimental design

	Experiment design	Independent variable	Dependent variable	Measures of the study
Experiment one (Interface I/II/III/IV)	One-way between-subjects	Number of identity checking steps	Perceived security, Trustworthiness and Usability	Post questionnaire
Experiment two (Interface V & VI)	One-way within-subjects	Types of identity-checking information; Number of identity checking steps	Perceived security, Trustworthiness and Usability	Post questionnaire
Experiment three (Interface VII)	One-way between-subjects	Number of identity checking steps	Perceived security, Trustworthiness and Usability	Post questionnaire

3.3.2 Participants

For the first experiment, eighty participants were recruited from the students of Massey University. A random numbers table was used to assign the participants equally to four different interfaces.

For the second experiment, all of the twenty participants were collected from the same university, and were then randomly divided into two groups to do the

experiment in two different orders. It was designed to avoid any order effect or learning effect to be counterbalanced in the experimental design. Group A used Interface V first and then Interface VI, Group B used them in the other order.

For the third experiment, twenty participants from Massey University were recruited. All of the participants were required to have any type of online banking experience. Table 3.6 summarises the participants in the three experiments.

Table 3.6 Summary table of participants

	Number of Participants	Number of Groups
Experiment One	80	4
Experiment Two	20	2
Experiment Three	20	1

3.3.3 Procedure

In Experiment I, each participant was first provided with the instructions regarding the experiment. This included the general information about the experiment, the purpose of the study, and the data-protection policy.

Before the participants started the experiments, an information sheet (Appendix A) was provided. All information they used, such as the bank account number, the card number and so forth, was on the information sheet. Next, they opened the website (www.trimup.co.nz/mall/test). The participants first needed to register their account on the registration page with the information sheet given (see Figure 3.1). After registering, the participants were randomly assigned to one of the four experimental conditions. After the experimental session, the participants were

required to complete a post questionnaire. Seven questions used to collect the participant satisfaction in terms of usability, perceived security and trustworthiness.

In Experiment II, two different sessions were used, the difference between them being the order of interfaces. Group A (10 participants) used Interface V first and then Interface VI; Group B (10 participants) used them in the other order. The procedures were the same as with Experiment I.

In Experiment III, only one session and one interface was used. Each participant was first provided with the instructions regarding the experiment. This included the general information about the experiment, the purpose of the study, and the data-protection policy. As this experiment used fingerprints to logon, the participants needed to register their fingerprint data first (see Figure 3.17). To log on to the system, the participants only needed to scan their fingerprint on the fingerprint reader connected to the laptop computer. The post-questionnaire study was exactly the same as with the other two experiments.

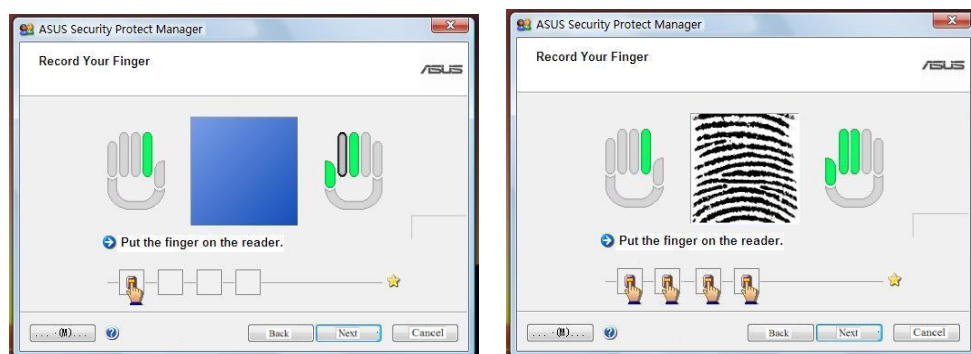


Figure 3.17 Fingerprint registration

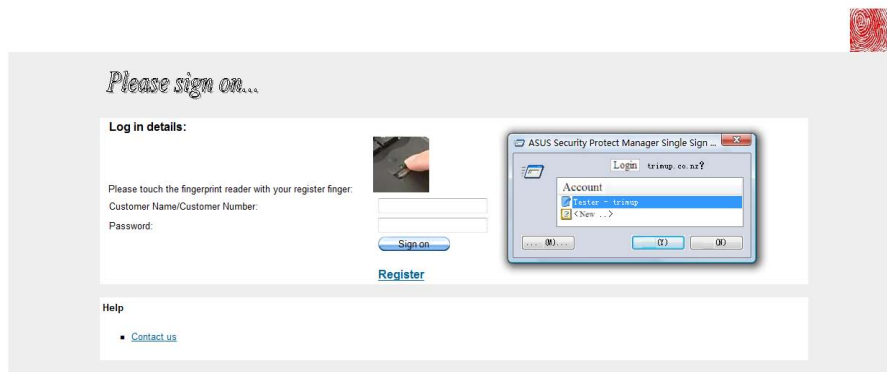


Figure 3.18 Connection set-up between fingerprint and customer account

3.3.4 Apparatus

An HP Laptop (HP Pavilion™ dv6700z) with high-speed broadband Internet connection was used to run Experiments I and II. For Experiment III, an HP laptop computer with a fingerprint reader was used instead. To make the experiments more realistic, the interfaces for Experiments I and II were uploaded to the internet (www.trimup.co.nz/mall/test). To make the participants more relax during the experiments, a chair and desk were set up in a computer laboratory.

Instructions were prepared for the three experiments and also the experiment procedure for both the participants and the person conducting the experiments. Questionnaires for the experiments were also prepared to see how the satisfied participants felt in terms of usability, perceived security and trustworthiness. The post-questionnaires (see Table 3.7 below) include seven questions on usability, perceived security and trustworthiness.

3.4 Data Collection

A post-questionnaire was created for data collection (see Table 3.7). Seven questions in the post-questionnaire focused on areas of usability, perceived security and trustworthiness. The first four questions in Table 3.7 (Post-test Questionnaire) were about usability issues, question six was about perceived security, and questions five and seven was about trustworthiness. All questions were answered on a Likert-scale of five points, and the ratings were recoded in SPSS.

Table 3.7 Post-test questionnaire

Question	Category
1. The interface for online banking logon is easy to use.	Usability
2. I feel comfortable using this interface.	Usability
3. The number of logon steps is appropriate.	Usability
4. It was simple to use this interface.	Usability
5. Overall, I am satisfied with this system.	Trustworthiness
6. The online banking logon system is secure enough.	Perceived security
7. Do you believe the online banking system is reliable and trustworthy?	Trustworthiness

3.5 Data Analysis

For the quantitative analyses, a statistical program SPSS™ 15 Windows was used. In particular, one-way ANOVA (ANalysis Of VAriance) and post-hoc analyses were employed throughout the result section. However, one analysis could not ensure the basic assumptions of ANOVA. In these cases, non-parametric analyses were employed instead.

CHAPTER FOUR: RESULT

4.1 Experiment I

The four different interfaces were tested in Experiment I. After using each interface, the post-test questionnaires were administered. Table 4.1 shows the average ratings for each question.

**Table 4.1 Average and standard deviation of rating for each question
(Interface I: 2 identity-checking steps; Interface II: 4 identity-checking steps;
Interface III: 6 identity-checking steps; Interface IV: 8 identity-checking steps.)**

Question	Interface I		Interface II		Interface III		Interface IV		Sig.
	Mean	S.D.	Mean	S.D.	Mean	S.D.	Mean	S.D.	
Q1 Easy to use	4.20	0.51	3.85	0.85	3.30	0.64	2.95	1.02	$p \leq 0.05$
Q2 Comfortable to use	3.90	0.67	3.70	0.63	2.50	0.79	2.45	0.82	$p \leq 0.05$
Q3 Steps are appropriate	3.20	1.14	3.00	1.25	2.40	0.84	2.30	1.06	$p \leq 0.05$
Q4 Simple to use	4.10	0.62	3.80	1.12	3.20	0.68	2.65	0.65	$p \leq 0.05$
Q5 Satisfied with system	3.90	0.70	3.95	1.16	3.00	0.45	2.15	0.91	$P \leq 0.05$
Q6 Secure enough	3.05	1.02	4.10	0.54	3.10	1.09	2.15	0.96	$p \leq 0.01$
Q7 Believe system is reliable and trustworthy	3.55	0.92	4.10	0.70	2.95	0.74	2.15	0.91	$p \leq 0.01$

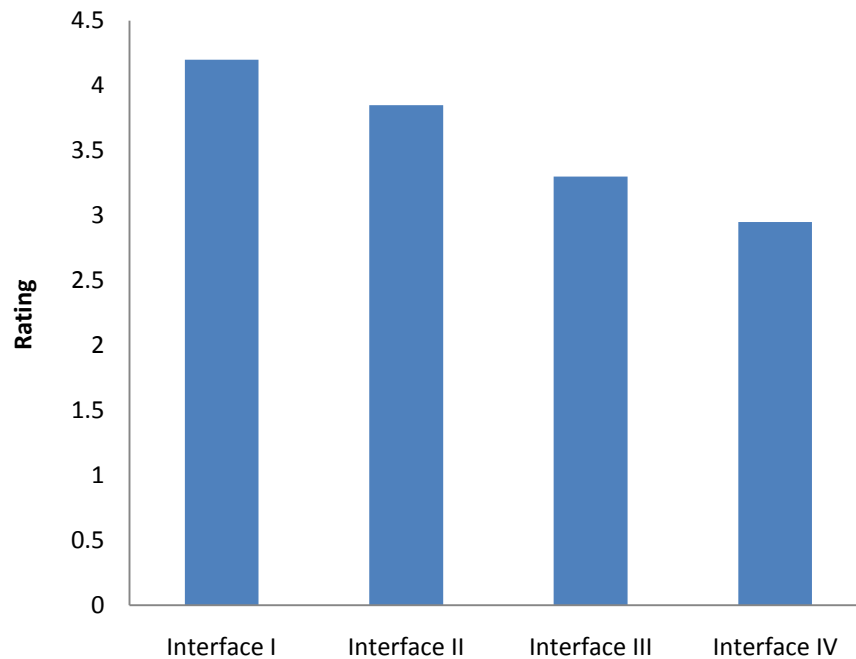


Figure 4.1 Easy to use

Again, for readability, Figure 4.1 shows the average ratings of “Easy-to-use” across the four different interfaces. The highest rating was 4.20 in Interface I, which implies Interface I was the easiest one could expect. The general trend of “Easy-to-use” decreases as more identity-checking steps are added (i.e., 3.85 for Interface II; 3.30 for Interface III; 2.95 for Interface IV).

One-way ANOVA test confirmed its significant difference ($F_{3, 76} = 9.66, p \leq .05$) and post-hoc analyses followed to show Interface I and Interface II were much easier to use than the other two interfaces, which were not significantly different from each other.

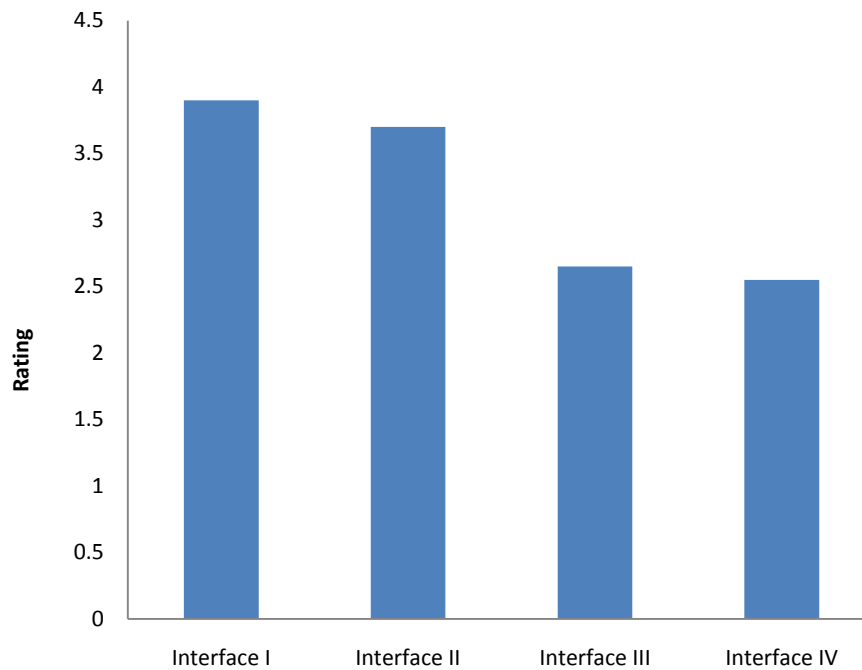


Figure 4.2 Comfortable to use

Likewise, Figure 4.2 shows the average ratings of “Comfortable to use” across the four different interfaces. The highest rating was 3.90 in Interface I, which implies Interface I was the most comfortable one.

One-way ANOVA test was used to test whether or not the “Comfortable to use” for each interface differed. It showed their significant difference among the four interfaces ($F_{3, 76} = 24.84, p \leq .05$). The post-hoc analyses further confirmed that both Interface I and II were in the higher level of “Comfortable to use” group, against Interfaces III and IV, which were not significantly different from each other.

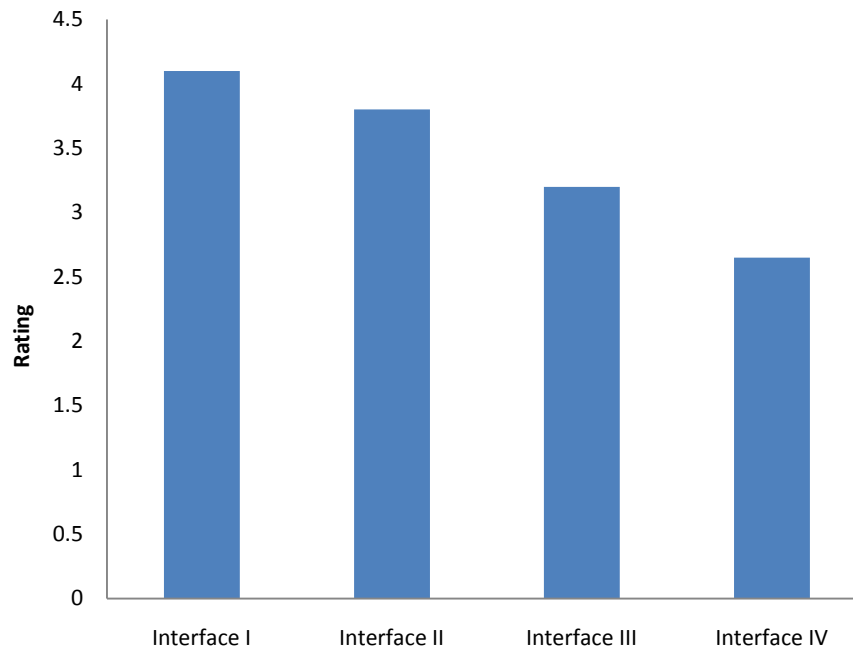


Figure 4.3 Simple to use

Similar to both Figure 4.1 and Figure 4.2, Figure 4.3 also shows the average ratings of “Simple to use” across the four interfaces. The highest rating was 4.10 in Interface I, which implies Interface I was the simplest one, and adding more logon procedures would be detrimental to usability.

One-way ANOVA test was applied to show their significant difference among the four interfaces ($F_{3, 76} = 12.44, p \leq .05$). The post-hoc analyses also supported the fact that Interface I was simpler to use than the other three, which were not statistically different from one another.

Reviewing all the questions above, one should be noted that they are all about usability issues. The analyses confirmed the common trend of the relationship between the number of logon steps and usability in the online banking logon

procedure. The possible explanation of these results is that usability and the number of logon steps seem to be a trade-off relationship.

Yet, question 6 (“Security satisfaction”) and question 7 (“Participants” Trustworthiness”) showed somewhat different patterns to the previous figures.

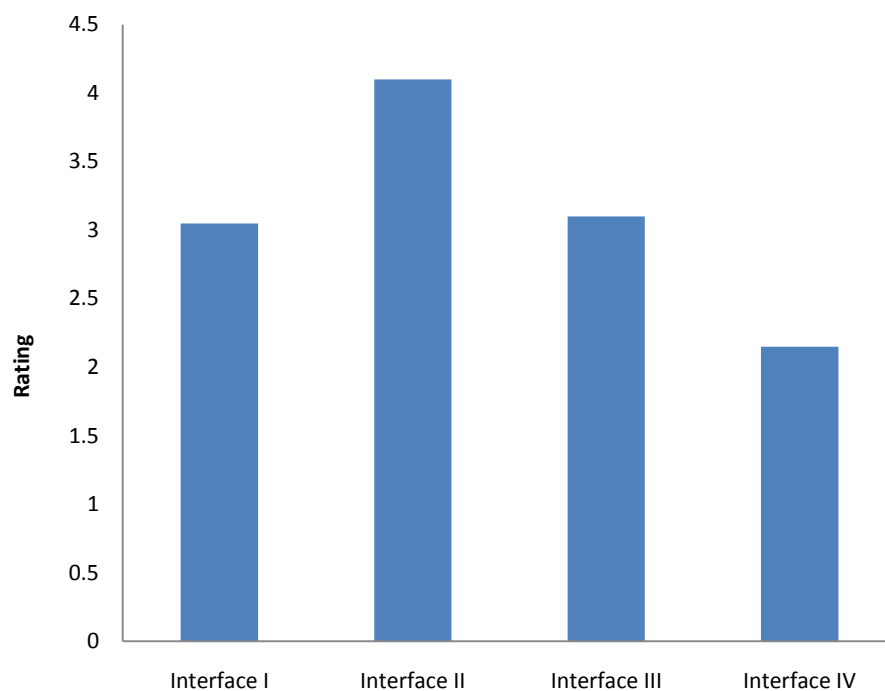


Figure 4.4 Secure enough

In Figure 4.4, Interface II had the highest rating (i.e., average score 4.1), which implies that most participants thought that Interface II was more secure than the others. Interestingly, more logon steps did not increase this rating (3.10 for Interface III and 2.15 for Interface IV)

One-way ANOVA test was not appropriate for these data, as Levene’s test for the heterogeneity of variance was found to be significant ($F_{3, 76} = 13.968, p \leq .05$). A Kruskal-Wallis test was performed, which identified the significant difference (K-

$W=27.20$, $p<0.01$). The pair-wise Mann-Whitney U tests showed Interface II was the most secure interface compared to the other three, which were not significantly different from one after another. This confirmed that simply adding more logon steps would not enhance the user's perceived security.

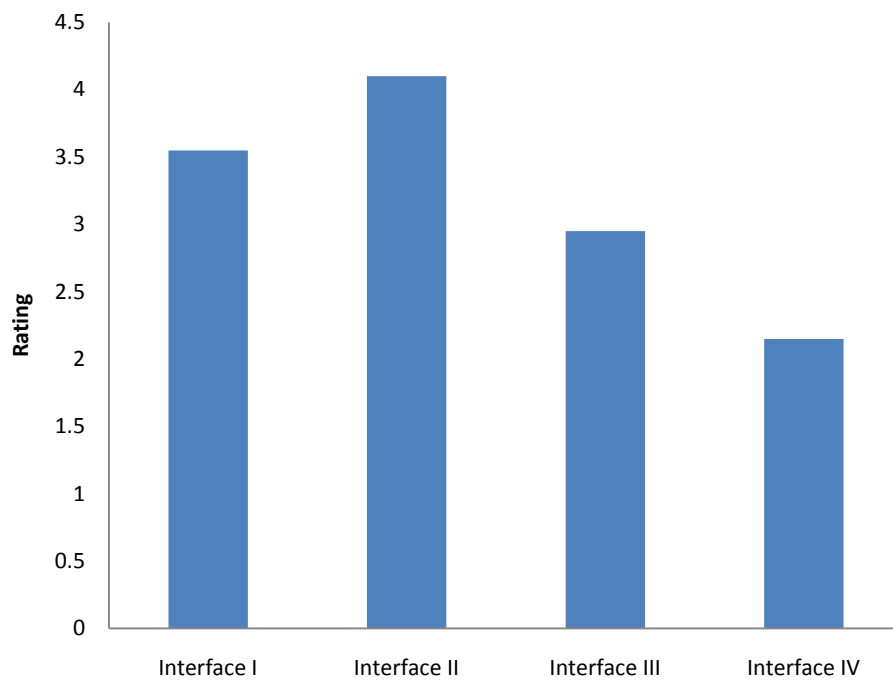


Figure 4.5 Trustworthiness

As with Figure 4.4, Figure 4.5 shows Interface II had the highest rating, 4.10, which means that most participants thought that Interface II was more trustworthy than the others.

One-way ANOVA test was also not appropriate for these data, as Levene's test for the heterogeneity of variance was found to be significant ($F_{3, 76} = 19.854$, $p \leq .05$). A Kruskal-Wallis test was performed, and it identified the significant difference ($K-W=35.09$, $p<0.01$). The pair-wise Mann-Whitney U tests showed the

Interface II was trustworthier than the other three, which are not significantly different from one after another. This also confirmed that simply adding more logon steps would not enhance the user's trust in the system. It also implies a positive relationship between the perceived security and trustworthiness.

On the whole, most participants felt Interface I, with two identity-checking steps, was more easy to use; and Interface II, with four identity-checking steps, was more secure and trustworthy.

4.2 Experiment II

From Experiment I, one can see that Interface I and II were better than the others in terms of usability, and that Interface II was better off for perceived security. To confirm this result, we performed another experiment with only the two conditions (two steps in Interface V and four steps in Interface VI). However, not to simply repeat the same experiment with Experiment 1, this experiment considered the different type of logon information; i.e., the system-initiated personal identity.

Table 4.2 Paired sample test for Experiment II
(Interface V: 2 identity-checking steps; Interface VI: 4 identity-checking steps.
Q1-Q5: Usability; Q6: Perceived security; Q7: Trustworthiness.)

Category			Means	Sig.
Usability (Question 1 – 5) ¹³	Pair1	Interface V Q1	4.45	n.s.
		Interface VI Q1	3.95	
	Pair2	Interface V Q2	4.00	n.s.
		Interface VI Q2	3.60	
	Pair3	Interface V Q4	4.25	p≤0.05
		Interface VI Q4	3.45	
	Pair4	Interface V Q5	3.10	n.s.
		Interface VI Q5	3.35	
Perceived Security	Pair5	Interface V Q6	2.40	p≤0.05
		Interface VI Q6	3.70	
Trustworthiness	Pair6	Interface V Q7	2.70	p≤0.05
		Interface VI Q7	3.60	

Table 4.2 shows the average ratings of the paired sampled test for each question in Interface V and VI. It shows that, in the usability category, only „Pair 3“ is significantly different, and Interface V is easier than Interface VI. But Interface VI is better than Interface V in terms of perceived security and trustworthiness. The results confirmed the findings from Experiment I.

4.3 Additional analysis: System-initiated identity information **(Expt. II) and User-initiated identity information (Expt. I)**

Experiment I showed that Interface II with the four user-initiated identity-checking steps was better than the others. Also, Experiment II confirmed that Interface VI with the four system-initiated identity-checking steps was more satisfactory to our participants. However, it is important to note that Interface II used user-initiated identity information (i.e. customer name, password and so forth), but Interface VI

¹³ Question 3 was not analysed in this experiment, like Experiment 1. It had almost the same outcomes as the other questions, questions 1, 2, 4 and 5.

used system-initiated identity information (i.e. customer number, security codes from the back of the security card). To further examine the potential difference between them, a one-way ANOVA test was then applied.

In this analysis, Interface II was the user-initiated four identity-checking steps system from experiment I, and Interface VI was the system-initiated four identity-checking steps from experiment II.

As Experiments I and II had different experimental designs, to make these comparisons possible, we first considered whether Experiment II had any order effect.

Table 4.3 Univariate analysis of variance for order effect

Source	Sig.
System	n.s.
Group	n.s.
System*Group	n.s.

Table 4.3 reveals that there is no order effect and interaction effect at all ($F_{1,38} = 0.811$, n.s.), so one can simply handle the data from Experiment II in the same way as Experiment I.

Table 4.4 recodes the average ratings for each question in both Interfaces (Interface II: 4 user-initiated identity-checking steps; Interface VI: 4 system-initiated identity-checking steps).

**Table 4.4 Average and standard deviation of ratings for each question
(Interface II: 4 user-initiated identity-checking steps;
Interface B: 4 system-initiated identity-checking steps)**

Questions	Interface II		Interface VI		Sig.
	Mean	S.D.	Mean	S.D.	
Q1 Easy to use	3.85	0.85	3.90	1.08	n.s.
Q2 Comfortable to use	4.10	0.63	3.60	0.75	n.s.
Q4 Simple to use	3.80	1.12	3.45	0.99	n.s.
Q5 Satisfied w/ system	3.95	1.16	3.35	0.93	n.s.
Q6 Secure enough	4.10	0.54	3.70	0.57	$p \leq 0.05$
Q7 Believe system is reliable and trustworthy	4.10	0.70	3.60	0.75	$p \leq 0.05$

One-way ANOVA test showed that for usability issues (Q1-Q5), there was not much different between Interface II and Interface VI. By contrast, for question 6, Interface II (mean 4.10) was significantly different from Interface VI (mean 3.70) ($F_{1, 38} = 5.067$, $p \leq .05$). For question 7, likewise, Interface II was better than Interface VI ($F_{1, 38} = 4.612$, $p \leq .05$). Both analyses support the user-initiated identity information (i.e., Interface II), which has not been empirically demonstrated in any other studies.

4.4 Additional analysis: User-initiated identity information (Expt. I) and Biometric identity information (Expt. III)

Based on the previous analyses, we found that the user-initiated identity information with the four logon steps were better in terms of usability, perceived security and trustworthiness. Experiment III would seek to confirm whether a biometric identity-checking system would heavily enhance its usability and, at the same time, its perceived security, which compared Interface II against the fingerprint logon system (Interface VII).

Table 4.5 shows the average ratings for each question in both Interfaces (Interface II: the user-initiated identity information with the four identity-checking steps; Interface VII: the fingerprint identity-checking system)

**Table 4.5 Mean and standard deviation of ratings for each question
(Interface II: 4 user-initiated identity-checking steps;
Interface VII: fingerprint identity checking.)**

Questions	Interface II		Interface VII		Sig.
	Mean	S.D.	Mean	S.D.	
Q1 Easy to use	3.85	0.85	4.60	0.50	$p \leq 0.01$
Q2 Comfortable to use	4.10	0.63	4.30	0.73	n.s.
Q4 Simple to use	3.80	1.12	4.40	0.50	$p \leq 0.05$
Q5 Satisfied w/ system	3.95	1.16	4.25	0.64	n.s.
Q6 Secure enough	4.10	0.54	4.05	0.69	n.s.
Q7 Believe system is reliable and trustworthy	4.10	0.70	4.15	0.88	n.s.

One-way ANOVA tests showed that the fingerprint was easy to use ($F_{1, 38} = 11.047$, $p \leq 0.01$), but did not enhance security (n.s), which arguably shows that the effectiveness of biometric data in e-commerce is not what the technology is promising.

CHAPTER FIVE: DISCUSSION

Table 5.1 summarises the findings from the three experiments, and how the findings would relate to the hypotheses discussed in Chapter 1

Table 5.1 Summary table of experiment hypothesis

Hypothesis		Result
1.	The number of identity-checking steps and usability would be trade-off.	Supported
2.	Simply adding more identity-checking steps would not help customers' perceived security.	Supported
3.	The relationship between usability (Point 1) and perceived security (Point 2) would not be a simple positive relationship.	Supported
4.	System-initiated identity information and biometric data would enhance perceived security.	Unsupported

5.1 Experiment I

In the first experiment, we empirically demonstrated the relationship of the identity-checking steps with usability, security and trustworthiness. The main outcomes were, firstly, that there is generally a trade-off between the number of identity-checking steps and usability. (Hypothesis 1 supported). Figure 5.1 depicts the plausible relationship between the number of identity-checking steps and ease-of-use in the online-banking logon process.

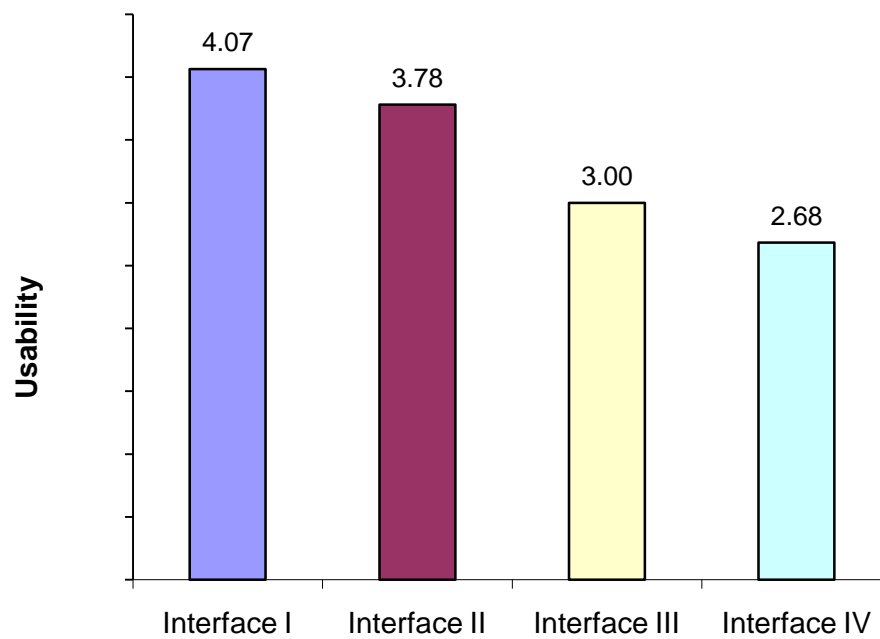


Figure 5.1 Relationship between identity-checking steps and usability

Secondly, as shown in Figure 5.2, simply adding more identity-checking steps (Interface III and IV in Experiment 1) would not enhance the customers' perceived security (Hypothesis 2 supported), positing a rather different stance on the security between the designer and the user.

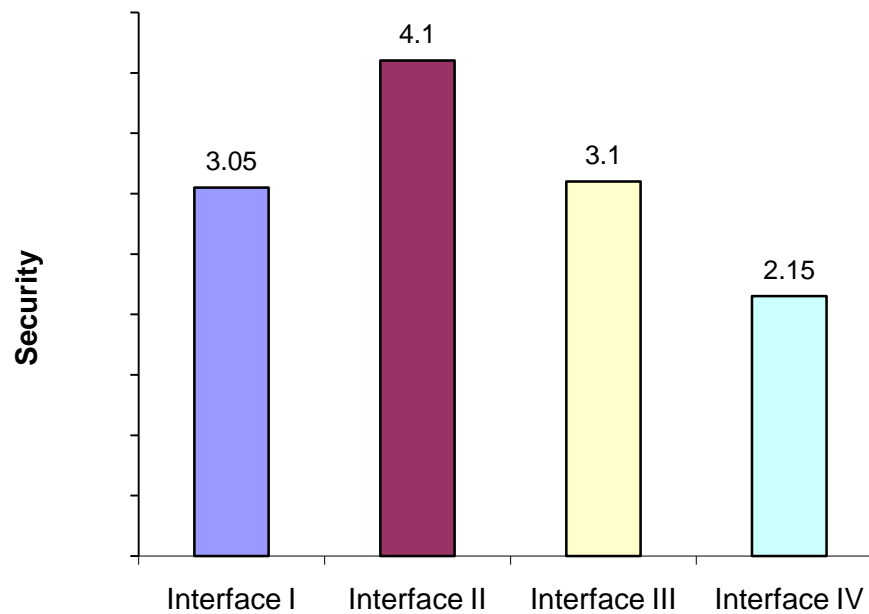


Figure 5.2 Relationship between identity-checking steps and security

Trustworthiness could be interpreted in the same way – that trustworthiness would not be proportional to the level of difficulty. This result can also be interpreted that usability and security will be compromised in a certain way. As mentioned before, Hypothesis I in Figure 1.1 shows the relationship is compromised at some levels. The general trend of Figure 5.2 is similar to that of Hypothesis I as shown in Figure 1.1. Hence, it can be said that Hypothesis I in the Figure 1.1 is supported.

Indeed, Experiment I proved too many identity-checking steps would make the logon interface less usable and even would not help customers’ perceived security and trustworthiness.

5.2 Experiment II

The second experiment used different types of identity-checking information to perform the same procedure as in Experiment I. It was originally hypothesised that the system-initiated identity information would be perceived as more secure than the user-initiated ones. However, Figure 5.4 clearly showed that this was not the case of our participants.

There can be two possible explanations for this. Firstly, our participants might find it easier to use their personal information rather than searching for the system-initiated identity information from the security code card or others. Therefore, the usability of the system-initiated identity information might be poor, which, as a consequence would affect its trustworthiness. Secondly, the system-initiated identity information might be easily lost in practice, and our participants might be less prone to forgetting user-initiated information. Hypothesis 4 was not supported.

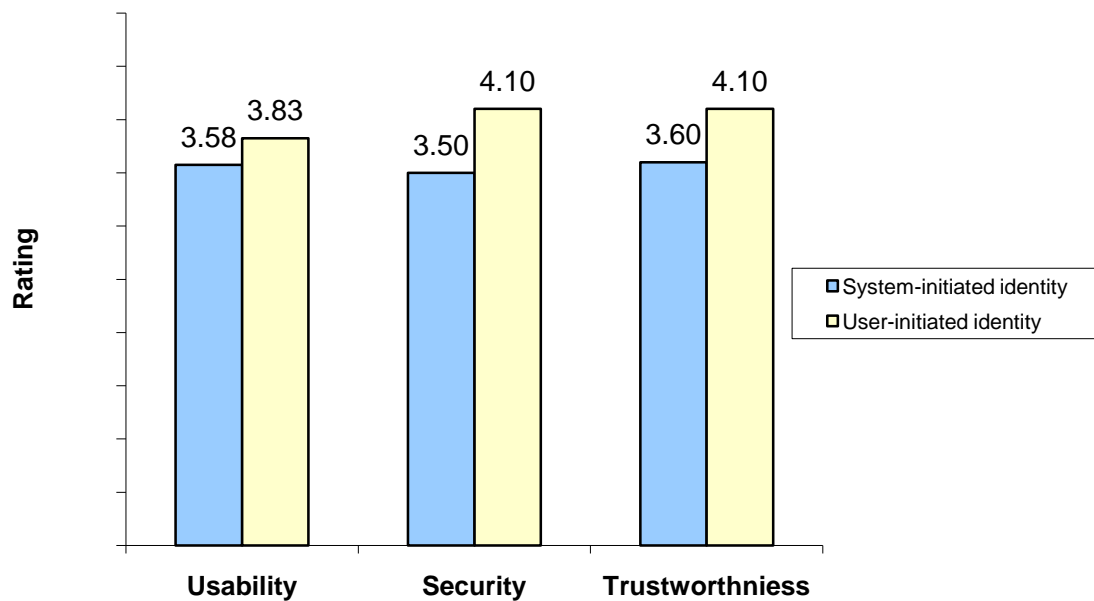


Figure 5.3 Expt. II vs. Expt.I

5.3 Experiment III

Experiment III was used to compare Interface II with the fingerprint interface (Interface VII). As one can see, this one-step logon procedure was welcomed by our participants, but not in terms of security and trustworthiness (Hypothesis 4 was not supported, either). That is, contrary to what the advocates of the technology are promising, the idea itself does not seem to present any enhancement of security. Another potential problem of this new biometric technology is the cost of devices. Although it seems to be very easy to use, it is not possible to incorporate it into common online banking transactions in daily life.

CHAPTER SIX: CONCLUSIONS

6.1 Findings of the Thesis

We take online banking for granted in our daily financial or monetary life, however, it has been the focus of concerns over security and trustworthiness. From the three experiments performed in this thesis, we found that, in terms of usability, perceived security and trustworthiness, the online banking logon system preferred by our participants incorporated four identity-checking steps. Of course, based on this limited study, we cannot say that all the online banking systems should have four identity-checking steps. However, it does indicate that the designers of online-banking systems need to be sensitive to the fact that adding more logon steps does not necessarily guarantee success. Furthermore, the presupposed benefit of biometrical security measures (i.e., fingerprints), is not empirically supported. Although our experimental outcomes did not reveal all the issues related to security in online banking systems, none of the findings above have been empirically demonstrated.

The main conclusion one can draw from the three experiments is that simply adding more identity-checking steps to the online banking log-on procedure does not improve the customer's perceived security and trust in the system. The number of identity-checking steps and the trustworthiness would be compromised at some point (Hypothesis I in Figure 1.1). This demonstrates that the designers need to understand

that the customer's perception of a system being secure is not due to the technical measures put in place. This is the main conclusion drawn from this study.

We also identified that while newly developing technologies, such as biometric identity-checking techniques, greatly improve the usability of the online banking system, they do not necessarily improve the perception of security. Biometric identity checking appears to be superior and more practical in application than traditional logon procedures; however, this thesis found that it did not really improve the customer perceived security and trust. Biometric identity checking techniques require extra devices, such as fingerprint readers, to work properly, which is another obvious limitation as a common interaction technique in the online-banking system.

6.2 Limitations of the Thesis

Despite the logic of the above conclusions, this study has several limitations, which lead to the need for future work.

The main limitation is the number of participants and their cultural backgrounds. Experiment I had 80 participants, while Experiments II and III only had 20 participants each. Therefore, all the experiments could be improved by recruiting more participants to make the data more representative of the population. In addition, the majority of participants were selected from Massey University and were therefore young students. The interpretations discussed above may have been skewed as a result of the participants all belonging to one particular age group. Therefore, a range of

participants is essential for any future work. Likewise, we did not consider the cultural background of the participants in this thesis, something that is widely acknowledged as pivotal (Gurvider *et al.*, 2004). In all likelihood, adding more participants from different age groups and different cultural backgrounds would fine-tune the interpretations above. These issues will be considered in the future work.

The experimental apparatuses were not highly professional, which could result in a potential bias with regard to the use of simulated online banking systems, as opposed to real-life online banking systems.

Finally, the usability measures only focussed on „ease-of-use“, whereas the concept of usability is wider in scope. Therefore, one cannot avoid thinking this may have some effect on our interpretations.

6.3 Future Work

In order to address the above limitations, we plan to run some more experiments with a larger number of participants recruited from different age groups (e.g., the elderly) and those with different cultural backgrounds, such as Asian participants.

With these multiple efforts, we would like to update our experimental apparatus, in order to be able to create finer interpretations. For example, we are redesigning the simulated online banking system more professionally and putting it on the Internet so that it more closely resembles a real online banking system. Also, in order to measure different usability dimensions of the online banking system, other

aspects of usability will be considered in subsequent work. This will allow one to potentially draw a complete structure of the relationships between the usability, security and trustworthiness.

REFERENCES

- Al-Ghatani, S. S., & King, M. (1999). Attitudes, satisfaction and usage: Factors contributing to each in the acceptance of information technology. *Behaviour & Information Technology*, 18 (4), 277-297.
- Barney, J.B., & Hansen, M.B. (1994). Trustworthiness as a source of competitive advantage. *Strategic Management Journal*, 15 (1), 175–190.
- Banphot, V., Magid, I., Antonis, C., S., & Waymond, R. (2008). Information systems continuance intention of web-based applications customers: The case of online banking. *Information and Management*, 45 (7), 419-428.
- Bomil, S., & Ingo, H. (2002). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, 7(3), 135-161.
- Cynthia, L., Corritore, B. K., & Susan, W. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, 58(6), 737-758.
- Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems*, 106(5), 601-602.
- Donald A., N. (1994). How might people interact with agents? *Communications of the ACM*, 37(7), 68-71.
- Fogg, B.J., Marshall, J., Kameda, T., Solomon, J., Rangnekar, A., et. al. (2001). *Web credibility research: a method for online experiments and early study results*. Paper presented at The Conference on Human Factors in Computing Systems. ACM Press, New York, pp. 295–296.
- Fogg, B.J., Tseng, H. (1999). *The elements of computer credibility*. Paper presented at The Conference on Human Factors in Computing Systems. ACM Press, New York, pp. 80–87.
- Ganesan, S. (1994). Determinants of long-term orientation in buyer–seller relationships. *Journal of Marketing*, 58(2), 1–19.

- Gang L. (2001). Telecommunications Software and Multimedia. *Customer Confidence and Security*. Retrieved June 4, 2008 from <http://www.tml.tkk.fi/Studies/T-110.501/2001/papers/ganglian.pdf>
- Gurvinder, S.S., & Bing, L. (2004). Internet banking: an empirical investigation of customers' behaviour for online banking in New Zealand. *Journal of E-Business*, 5(1), 1-17.
- Comptroller of the Currency Administrator of National Banks. (1999). *Internet Banking Comptroller's Handbook*. Retrieved from <http://www.occ.treas.gov/handbook/intbank.pdf>
- International Organization for Standardization. (1998). *Ergonomic requirements for office work with visual display terminals (VDTs) Part II: Guidance on Usability*. Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=16883
- Joris, C., Valentin, D., Danny D., C., Bart, P., & Joos, V., (2002). On the Security of Today's Online Electronic Banking Systems, *Computers & Security*, 21(3), 253-265.
- Karvonen, K. (2000). *The beauty of simplicity*. Paper presented at The Proceedings of the ACM Conference on Universal Usability. Arlington, VA: The Association of Computing Machinery.
- Kee, H.W., & Knox, R.E. (1970). Conceptual and methodological considerations in the study of trust and suspicion. *Conflict Resolution*, 14 (3), 357–366.
- Kubilus, N. J. (2002). Designing an e-commerce site for users. ACM Crossroads [online serial], August. Available: <http://www.acm.org/crossroads/xrds7-1/ecuser.html>.
- Lewicki, R.J., & Bunker, B.B. (1996). Developing and maintaining trust in work relationships. In: Kramer, R., Tyler, T. (Eds.) *Trust in Organizations: Frontiers of Theory and Research*. Sage, Newbury Park, CA, 114-139
- Industrial and Commercial Bank of China. (2008). *Online Bank Help*. Retrieved July 3, 2008, from <http://www.icbc.com.cn>
- Sara, N, S. D., Gregory Vert. (2006). *User Interface Design of the Interactive Fingerprint Recognition (INFIR) System* [electronic version] Retrieved from <http://ww1.ucmss.com/books/LFS/CSREA2006/SAM8023.pdf>

- Rotter, J.B. (1971). Generalized expectancies for interpersonal trust. *American Psychologist* 26(5), 443–452.
- Scheffelmanier, G. W., & Vinsonhaler, J. F. (2002). A synthesis of research on the properties of effective Internet commerce web sites. *Journal of Computer Information Systems*, 43(2), 23–31.
- Warwick, F., & Michael S., B. (2002). *Secure Electronic Commerce* (2nd Ed.). New Jersey: Prentice Hall PTR.
- Winne Chung, J. P. (2002). *An Evaluation of Internet Banking in New Zealand*. Paper presented at the Proceedings of the 35th Hawaii International Conference on System Science.
- Wing, P.O.H., B. (1999). Using public-key infrastructures for security and risk management. *IEEE Communications Magazine*, 37(9), 71-73.
- “Your say: Online banking security”. (2008). Retrieved July 3, 2008, from <http://www.stuff.co.nz/4414962a4621.html>
- Zhang, Y. & Ryu, H. (2008). *An Empirical Study on the Relationship between identity-checking Steps and Perceived Trustworthiness in Online Banking System Use*. Paper presented at The 7th International Conference on Applications and Principles of Information Science.

Appendix A

Information sheet

Thank you for taking part in this experiment to demonstrate the relationships among usability, perceived security and number of identity checking step, three experiments were carried out using the simulation of an online banking logon procedure to provide a similar online banking experience. The main purpose of the experiments is not to assess you, but to improve the current system specifications in terms of your response. Once again, it is not to stigmatise you, but to develop a user-friendly system.

Also, at any time you can withdraw from this evaluation without any further disadvantage of you. All the data obtained from this survey will be made anonymous before being published.

CONSENT

I have read the introduction, and consent to take part in this survey. I am aware that if I have any difficulty to proceed this evaluation, I can withdraw this session at any time.

Full Name: _____

Contact (email/telephone): _____

Signature: _____

Date: _____

If you have anything to ask about the experiment, you can contact Hokyoung Ryu (h.ryu@massey.ac.nz, ext. 9140) or Yang (Kansi) Zhang (garnett2002@hotmail.com) at

any point.

1. Customer Number: 71262668

2. Card Number: 25467231

3. Security code card

	A	B	C	D	E	F	G	H	I	J
1	123	123	123	123	123	123	123	123	123	123
2	135	135	135	135	135	135	135	135	135	135
3	137	137	137	137	137	137	137	137	137	137
4	138	138	138	138	138	138	138	138	138	138
5	139	139	139	139	139	139	139	139	139	139
6	140	140	140	140	140	140	140	140	140	140
7	142	142	142	142	142	142	142	142	142	142
8	145	145	145	145	145	145	145	145	145	145