I hereby declare that I have read this thesis and in my opinion this thesis issufficient in terms of scope and quality for the award of the degree of Master ofInformation security.

Signature : .....
Name of Supervisor : Dr. Mazdak Zamani
Date : 13/05/2013

A SECURE FRAMEWORK FOR E-BANKING SYSTEMS BASED ON HYBRID AUTHENTICATION SCHEMES

Shawnim Ikram Essa

A project report submitted in fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Center for Advanced Informatics School (AIS)
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

MAY 2013

I declare that this thesis entilted “A Secure Framework For E-Banking System Based on Strong Authentication” is the result of my own research except as cited in the references. The thesis has not been accepted of any degree and it’s not concurrently submitted in candidature of any other degree.

Signature : .....

Name : Shawnim Ikram Essa

Date : 13/05/2013

ACKNOWLEDGEMENTS

I would like to thank Advanced Informatics School (AIS) for the encouragement, I also would like to thank my family and friends whose assistance, support, and cooperation sustained me throughout the entire time.

First and foremost, I would like to express my sincere appreciation to my supervisor, Dr. Mazdak Zamani. I have been very lucky to have this opportunity to learn from him. I was overwhelmed by his knowledge, insightful, professionalism, and guidance during this thesis. He provided me with a role model of a professor and researcher that I wish to emulate in my future career. I also thank him for believing in my abilities with insightful patience. I am honored that I will graduate as his master student, and I hope that we can continue working together as collaborators.

Most importantly, I would like to thank my husband, Kaka, for his never ending support as I have pursued my educational goals. His support and encouragement mean the world to me. Also I want to thank my two beloved kids, Yar and Yara for their patience during my study.

Then, I would like to appreciate my dad and mum as well as my beloved sisters and brothers who supported me during my study and contacting me continuously.

Last not the least, I would like to thank my father in law, Mr Hayas for his continuously encouragement and advices regarding my study.

ABSTRACT

In recent years most banks offer online-banking to their customers. As banking activities are by nature more sensitive than most other Internet activities, higher security standards are required. Authentication is the first line of defense against compromising confidentiality and integrity, Internet banking systems must authenticate users before granting them access to particular services. The banking system must determine whether a user is, in fact, who he or she claims to be. The increase in use of online banking has given rise to an increase in attacks against banking institutions and their customers, such as phishing, shoulder surfing, eavesdropping, and dictionary attacks. It is widely accepted that without adequate controls, security threats are highly probable against transactions in electronic commerce, such as online banking transactions. For implementing a strong authentication technique, this project has introduced a secure framework for online banking authentication system, which is secure in public area and invulnerable to the common attacks and users can achieve the authentication process simply by selecting the appropriate mode according to the environment status (Safe or Unsafe).

ABSTRAK

Dalam tahun-tahun kebelakangan ini kebanyakan bank menawarkan perbankan dalam talian kepada pelanggan mereka. Disebabkan Aktiviti-aktiviti perbankan adalah lebih sensitif daripada aktiviti-aktiviti Internet yang lain, standard keselamatan yang lebih tinggi diperlukan. Pengesahan adalah barisan pertahanan pertama terhadap kerahsiaan berkompromi dan integrity, sistem perbankan internet mesti mengesahkan pengguna sebelum memberikan mereka akses kepada perkhidmatan tertentu. Sistem perbankan perlu menentukan sama ada pengguna adalah, sebenarnya, seperti yang dia sepatutnya menjadi. Peningkatan dalam penggunaan perbankan dalam talian telah menyebabkan peningkatan dalam serangan terhadap institusi perbankan dan pelanggan mereka, seperti as phishing, shoulder surfing, eavesdropping, and dictionary attacks. Ia adalah diterima secara meluas bahawa tanpa kawalan yang mencukupi, kemungkinan ancaman keselamatan terhadap transaksi dalam perdagangan elektronik adalah, seperti transaksi perbankan dalam talian. Untuk melaksanakan perbankan dalam talian dengan satu teknik pengesahan yang kukuh, projek ini telah memperkenalkan rangka kerja keselamatan bagi sistem pengesahan perbankan dalam talian, yang selamat dalam kawasan awam dan kebal daripada serangan biasa, yang pengguna boleh mencapai proses pengesahan hanya dengan memilih mod yang sesuai mengikut status persekitaran (iaitu Selamat atau tidak selamat). Daripada sistem disiasat dan dinilai, ia adalah jelas bahawa rangka kerja yang dicadangkan boleh hadir satu kaedah yang kukuh dan fleksibel dengan kebolehpercayaan untuk pengguna dalam sistem pengesahan perbankan dalam talian. Di mana pengguna boleh mencapai proses pengesahan hanya dengan memilih mod yang sesuai mengikut taraf alam sekitar (iaitu selamat atau tidak selamat).

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	x
	LIST OF FIGURES	xi
	LIST OF APPENDICES	xiii
1	**INTRODUCTION**	**1**
	1.1 Introduction	1
	1.2 Background of the problem	3
	1.3 Problem Statement	5
	1.4 Research Questions	6
	1.5 Project Aim	6
	1.6 Project Objectives	6
	1.7 Scope of the Study	7
	1.8 Summary	8
2	**LITERATURE REVIEW**	**9**
	2.1 Introduction	9
	2.2 Authentication	9
	2.3 Authentication in E-Banking	12
	2.4 Authentication Approaches	14
	2.4.1 The one-time password approach	15
	2.4.2 The certificate based approach	17

2.4.3 The timer based (short) password approach 18
2.4.4 The certificate - smart card based approach 19
2.5 The Usage of Online Banking 19
2.6 Security and Usability of Online Banking Websites 21
2.7 User ID and Passwords 24
2.8 Biometrics 25
2.9 Biometric Characteristics 26
2.10 Previous Works 27
2.10.1 Traditional Passwords 28
2.10.2 Graphical Password 30
2.10.3 Virtual password 33
2.10.4 PIN entry scheme 35
2.10.5 Formula Based Password (FBA) 38
2.11 Summary 42
3 METHODOLOGY 43
3.1 Introduction 43
3.2 Research Methodology 43
3.2.1 Planning phase 43
3.2.2 Analysis phase 44
3.2.3 Designing phase 44
3.2.4 Implementation phase 46
3.2.5 Evaluation phase 46
3.3 Summary 46
4 **IMPLEMENTATION 47**
4.1 Introduction 47
4.2 Proposed Framework 48
4.3 Transaction Modes (Modes of Authentication) 48
4.3.1 Safe Area 50
4.3.2 Unsafe Mode 53
4.4 Summary 63
5 **ANALYSIS AND DISSCUSSION 64**
5.1 Introduction 64

5.2 Comparison of Proposed System with Existing Schemes 65
5.3 Summary 66
6 **CONCLUSION AND FUTURE WORKS** **67**
6.1 Introduction 67
6.2 Research findings 67
6.3 Main contributions 68
6.4 Conclusion 68
6.5 Recommendation and Future Work 70
6.6 Limitations 71
APPENDIX A-B **72**
REFERENCES **84**

LIST OF TABLES

TABLE NO. **TITLE** **PAGE**

Table 2-1: Summery of related work..... 41

Table 4-1: An analysis testing for Safe Mode..... 52

Table 4-2: An analysis testing for Seen-Unsafe Mode..... 56

Table 4-3: An analysis testing for Heard-Unsafe Mode..... 58

Table 4-4: An analysis testing for TAC-Unsafe Mode..... 62

Table 5-1 Comparison between Proposed Hybrid Scheme and Other Techniques..... 65

LIST OF FIGURES

FIGURE NO. TITLE PAGE

Figure 2-1: A schematic of the basic vouching process(Brainard et al., 2006)..... 11

Figure 2-2: Factor of authentication, something you process (Shah & Minhas, 2009) 12

Figure 2-3: Offline credential-stealing attack scenarios(Hiltgen et al., 2006) 13

Figure 2-4: Online channel-breaking attack scenarios (Hiltgen et al., 2006)..... 14

Figure 2-5: TAN and iTAN approaches (Hoebl, 2007). 15

Figure 2-6: Existing OTP Generation Mechanism(Prakash & Shobana, 2010)..... 17

Figure 2-7: The certificate-based solution(Hiltgen et al., 2006). 18

Figure 2-8 : The short-time password approach (Hiltgen et al., 2006). 19

Figure 2-9: Selection panel in graphical step(Oorschot & Wan, 2009). 31

Figure 2-10 : Enrollment process (Joshi et al., 2012)..... 32

Figure 2-11: Login time for Different Users(Rekha et al., 2011). 34

Figure 2-12: Average Login time for a User(Rekha et al., 2011). 35

Figure 2-13: The Spinlock graphical user interface(Bianchi et al., 2011). 36

Figure 2-14: Colored Patterns in Display Tables (Lashkari et al., 2009)..... 37

Figure 2-15: Architecture and information flow of the Mobile Devices and Browser Extensions (Shi et al., 2010)..... 38

Figure 2-16: original stroke on the interface (Zheng et al., 2009) 38

Figure 2-17: General interface for login (Shakir & Khan, 2010)..... 40

Figure 2-18: Sequence of User Login (Shabih ul Hasan Naqvi & Afzal, 2010)..... 39

Figure 3-1: Research Methodology Phases 45

Figure 4-1: Flowchart of the Proposed Approach 49

Figure 4-2: Main Authentication Page 49

Figure 4-3: Login Page / Safe Mode 51

Figure 4-4: Successful Login Page 52
Figure 4-5: Unsuccessful Login Page 53
Figure 4-6: Unsafe Mode Page 54
Figure 4-7: Seen Area Flowchart 55
Figure 4-8: Seen Page Scheme 56
Figure 4-9 Heard Area Flowchart 57
Figure 4-10: Heard Page Scheme 58
Figure 4-11: Heard Page Scheme 59
Figure 4-12 Flowchart of TAC Method 59
Figure 4-13: TAC Page Scheme 61
Figure 4-14: TAC Page 62

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Programming Codes …….....	71
B	Gant Chart ……	82

CHAPTER 1

INTRODUCTION

1.1 Introduction

Online banking is a new phase in retail banking services. With the help of online banking several types of services through which customers can request information and carry out their banking transaction such as balance inquiry, inter account transfers, utility bills payment, request check book etc., via a telecommunication network or internet without physically visit the branches(Daniel, 1999).

The Internet is an integral part of our daily lives, and the proportion of people who expect to be able to manage their bank accounts anywhere, anytime is constantly growing. As such, Internet banking has come of age as a crucial component of any financial institution's multichannel strategy. Information about financial institutions, their customers, and their transactions is, by necessity, extremely sensitive, thus, doing such business via a public network introduces new challenges for security and trustworthiness.

Security of a customer's financial information is very important, without it, online banking could not operate. Financial institutions have set up various security processes to reduce the risk of unauthorized online access to a customer's records, but there is no consistency to the various approaches adopted.

The beginning of the twenty first century has brought a dramatic increase in the use of the online channel for financial institutions. The number of users taking

advantage of the services offered online by financial institutions continues to increase each year(Sullivan, 2005).

The growth and popularity of the Internet through recent years has resulted in it becoming a tool that is used in everyday life. With the growth in Internet usage, new ways of conducting financial transactions, through online banking, have also grown in usage and popularity. Online banking provides the ultimate convenience to the consumer, in the ability at anytime and anywhere to manage one's bank accounts.

It is evident that online crime and fraud against online banking is not going away and will only continue to grow and adapt. Financial institutions see the Internet as the banking channel of the future and will continue to move more products to it to help reduce their costs and increase convenience for the customer. Fraudsters know this and see the opportunity to steal information and money without ever leaving their computer desk.

Any Internet banking system must solve the issues of authentication, confidentiality, integrity, and nonrepudiation, which means it must ensure that only authorized people can access an Internet banking account, that the information viewed remains private and can't be modified by third parties, and that any transactions made are traceable and verifiable(Hiltgen, Kramp, & Weigold, 2006).

For implementing a strong authentication technique, this project has introduced a secure framework for online banking authentication system, which is secure in public area and invulnerable to the common attacks suffered by other authentication schemes. The contribution of this study was to provide two modes of authentication for the user. The two modes were designed depending on whether the transaction environment will be safe or not.

The main purpose of this hybrid system is to offer multi choice for user authentication, the choice of a specific scheme is based on the environment status, weather its safe area or unsafe. The presented analysis showing that, this hybrid system is ease of use, user acceptance a person's willingness to offer this trait for

authentication and determining if the system is easier, faster, friendlier, and more convenient than the alternatives.

1.2 Background of the problem

Security is the primary concern for all organizations. Organizations are worried about the security of their stored and transported data. Electronic commerce and electronic banking have their own special security problems, due to the remote access granted to their important information (Mohammadi & Abedi, 2008).

The positive development of e-banking over the last decades has left banks with the quest for secure e-banking systems, including effective countermeasures against financial fraud, cybercrime and their related malicious attacks (Mockel, 2011).

The numbers of malicious attacks on e-banking and related fraud cases have risen accordingly, accounting for £ 46.7 million in the year 2010 only in the UK(Moeckel, 2011). Computer crime, especially internet crime is growing fast every year. For example: In 2009, more than 336,655 complaints of internet crime had been investigated by law enforcement and regulatory agencies nationwide were processed by the Internet Crime Complaint Center (Jebriel & Poet, 2011).

Moreover, with the rapid growth of internet based financial transactions, the need for strong authentication has drastically increased. Financial institutions in the world are facing a fast approaching deadline to improve user authentication for online banking and other financial institutions. Not only in these fields but the authentication process secures banking, ATM, security entrances, networks, defense forces, top secret projects, personal data of individuals and general websites(Shabih ul Hasan Naqvi & Afzal, 2010).

Authentication is a significant issue for security when using different computer applications. Human actors play a major role in authentication. Usually, two stages have been divided for authentication procedures which are identification and authentication. The term identification normally uses the (User ID) to identify the user whereas the authentication stage is used to verify that the user is the legitimate owner of the ID (Adams & Sasse, 1999).

Password authentication is one of the most simple and effective approaches for authentication in a client/server environment. It has been widely deployed in banking and payment systems, computer networks.(Mohammadi & Hosseini, 2010).

However with the increase in the number of online services, the users need to register with each service separately and must remember many sets of ID's and passwords to access the respective services. This is considered insecure as most of the users tend to use same password on various servers leading to compromise of their accounts by means of guessing attack and insider attack(Shabih ul Hasan Naqvi & Afzal, 2010).

Attackers have to break the first and last line of defense that is the password. Passwords remain the dominant means of authentication in today's systems because of their simplicity, legacy deployment and ease of revocation. People either choose a password which is easy to remember but can also easily be hacked and the difficult password is usually forgotten. This leads to the weak security and the loss of important data or information (Shabih ul Hasan Naqvi & Afzal, 2010).

There are many techniques that are used by attackers to obtain and exploit passwords. Among these techniques, phishing has been one of the most popular and effective approaches. It is widely adopted by attackers all over the world, partially because it is easy to launch: a forged website and/or a fake e-mail is usually enough to trick novice users and acquire their passwords and/or other sensitive information.

In addition to phishing, key logging programs are also widely used by adversaries in order to collect sensitive information. Sometimes, people have to enter

their sensitive information using untrusted machines (e.g., using public PCs in Internet cafes), which makes them particularly vulnerable to key loggers. While computers in public places have a higher probability of being infected by key logging programs, home computers can also be infected by such programs due to the flooding of spywares and botnets(Shi, Zhu, & Youssef, 2010).

When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual's authentication session. This is referred to shoulder surfing attack and it is a known risk, of special concern when authenticating in public places. As well as when a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user's password credentials. This is a problem that has been difficult to overcome(Lashkari, Farmand, Zakaria, Bin, & Saleh, 2009).

1.3 Problem Statement

The need for stronger user authentication in online banking systems has become necessary to ensure customer security, confidence, and acceptance of this widely used channel for financial institutions. The standard means of user authentication, such as username and textual password, are no longer strong enough to ensure appropriate access control to customer's accounts and personal information(Zhao & Li, 2007).

Fraud and identity theft account for large financial loses each year, hackers can use many techniques to steal passwords, such as shoulder surfing, Hidden Camera, Eavesdroppers, dictionary attack, Phishing, etc., and as a result of attacks targeting passwords, different authentication methods have been proposed by previous research in recent years in the field of online banking.

The traditional passwords mechanisms achieve all benefits on deploy ability, and one scheme achieves all in security, but no scheme achieves all usability

benefits. So there was a great demand of having strong authentication system, which wills not going to allow, the unauthorized user to access the cloud(Saxena, 2008). For implementing a strong authentication technique, this project has proposed a secure framework for internet banking authentication system, Which is a hybrid of several different mechanisms, in order to offer multi choice for user authentication, the choice of a specific scheme is based on the environment status, weather its safe area or unsafe.

1.4 Research Questions

The main questions this research motivates to answer are as follows:

I. What techniques used to eliminate common attacks in online banking authentication?
II. How to introduce a method for securing the password between users and banking system.
III. How to evaluate the security of proposed method against common attacks.

1.5 Project Aim

The aim of this study is to make the authentication system between users and banks over the Internet as much secure as possible for public places, user friendly, and robust against shoulder surfing, eavesdropping, dictionary, and phishing attacks.

1.6 Project Objectives

The objectives of this study are as below:

I. To investigate existing methods of authentication in E-Banking against possible attacks.

II. To propose and develop a secure framework for e-banking based on strong authentication.

III. To evaluate the proposed framework against shoulder surfing, eavesdropping, dictionary, and phishing attacks, by comparing with other methods.

1.7 Scope of the Study

This study focuses on authentication in online banking system against common attacks. Also it is focusing on protecting passwords from being stolen by adversary attack in online banking environment, especially in public places such as coffee shop, shopping mall, library, etc., when user doing financial transaction. This study introduced a framework for online banking system; the proposed framework is a hybrid of various schemes of authentication which depend on user's environment. The various techniques introduced in this authentication framework are including of the traditional password authentication scheme, graphical password approach, and one time password technique in online banking authentication system that uses the Transaction Authentication Code (TAC). The proposed framework is free hardware and software installing devices, only the software that used is the voice-recognition software programmer which is built in windows system.

1.8 Summary

Online banking has become a popular service through most banking institutions. As a result, security of the online banking sites is becoming increasingly important. This chapter began with an introduction about online banking system and followed by the background of the problem. Then the statement of problem has been explained, and a description of project objectives, research questions, the aim of the study, and scope, has been explained respectively.

The support for this study is provided in Chapter 2, which describes the foundation literature regarding the background and relevance for the study. Chapter 3 provides a description of the methodology that was followed for the study. The results of the study are discussed in Chapter 4. Chapter 5 illustrates the evaluation of proposed framework. The conclusions, implications, and recommendations resulting from this study are provided in Chapter 6.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Alghathbar, K., & Mahmoud, H. A. (2009). *Noisy password scheme: A new one time password system.* Paper presented at the Electrical and Computer Engineering, 2009. CCECE'09. Canadian Conference on.

Alsaleh, M., Mannan, M., & van Oorschot, P. C. (2012). Revisiting defenses against large-scale online password guessing attacks. *Dependable and Secure Computing, IEEE Transactions on, 9*(1), 128-141.

AlZomai, M., AlFayyadh, B., & Josang, A. (2010). *Display security for online transactions: SMS-based authentication scheme.* Paper presented at the Internet Technology and Secured Transactions (ICITST), 2010 International Conference for.

Auclair, J. R., Green, K. M., Shandilya, S., Evans, J. E., Somasundaran, M., & Schiffer, C. A. (2007). Mass spectrometry analysis of HIV-1 Vif reveals an increase in ordered structure upon oligomerization in regions necessary for viral infectivity. *Proteins: Structure, Function, and Bioinformatics, 69*(2), 270-284.

Beuster, G., Henrich, N., & Wagner, M. (2006). Real world verification—experiences from the Verisoft email client. *Proc. ESCoR, 192*, 112-115.

Bianchi, A., Oakley, I., & Kwon, D. (2011). Spinlock: a single-cue haptic and audio PIN input technique for authentication. *Haptic and Audio Interaction Design*, 81-90.

Bicakci, K., Atalay, N. B., & Kiziloz, H. E. (2011). *Johnny in internet café: user study and exploration of password autocomplete in web browsers.* Paper presented at the Proceedings of the 7th ACM workshop on Digital identity management.

Bidgoli, H. (2006). *Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations* (Vol. 2): Wiley.

Blonder, G. E. (1996). Graphical password: Google Patents.

Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2006). *Fourth-factor authentication: somebody you know.* Paper presented at the Conference on Computer and Communications Security: Proceedings of the 13 th ACM conference on Computer and communications security.

Cheng, F. (2011). Security Attack Safe Mobile and Cloud-based One-time Password Tokens Using Rubbing Encryption Algorithm. *Mobile Networks and Applications, 16*(3), 304-336.

Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. C. (2008). *Influencing users towards better passwords: persuasive cued click-points.* Paper presented at the Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1.

Council, F. F. I. E. (2011). Authentication in an internet banking environment.

Cranor, L. F., & Garfinkel, S. (2008). *Security and usability: Designing secure systems that people can use*: O'reilly Media.

Daniel, E. (1999). Provision of electronic banking in the UK and the Republic of Ireland. *International Journal of Bank Marketing, 17*(2), 72-83.

Datta, S. K. (2010). Acceptance of E-banking among adult customers: An empirical investigation in India. *Journal of Internet Banking and Commerce, 15*(2).

De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies, 63*(1), 128-152.

Dhamija, R., & Perrig, A. (2000). *Deja vu: A user study using images for authentication.* Paper presented at the Proceedings of the 9th USENIX Security Symposium.

Di Giandomenico, F., Kwiatkowska, M., Martinucci, M., Masci, P., & Qu, H. (2010). Dependability Analysis and Verification for Connect ed Systems. *Leveraging Applications of Formal Methods, Verification, and Validation*, 263-277.

Drimer, S., Murdoch, S., & Anderson, R. (2009). Optimised to fail: Card readers for online banking. *Financial Cryptography and Data Security*, 184-200.

Flechais, I., Mascolo, C., & Sasse, M. A. (2007). Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics, 1*(1), 12-26.

Florêncio, D., & Herley, C. (2010). *Where do security policies come from?* Paper presented at the Proceedings of the Sixth Symposium on Usable Privacy and Security.

Hiltgen, A., Kramp, T., & Weigold, T. (2006). Secure internet banking authentication. *Security & Privacy, IEEE, 4*(2), 21-29.

Hoebl, M. (2007). Authentication approaches for online-banking. *Council of European Professional Informatics Societies, Legal and Security Special Interest Network, LSI SIN (07), 2*.

Hollien, H. F. (2002). *Forensic voice identification*: Academic Press.

Howell, J., & Wei, J. (2010). Value increasing model in commercial e-banking. *Journal of Computer Information Systems, 51*(1), 72.

Jebriel, S. M., & Poet, R. (2011). *Preventing shoulder-surfing when selecting pass-images in challenge set.* Paper presented at the Innovations in Information Technology (IIT), 2011 International Conference on.

Jones, S., Johnson-Yale, C., Millermaier, S., & Perez, F. S. (2009). Everyday life, online: US college students' use of the Internet. *First Monday, 14*(10).

Joshi, A., Kumar, S., & Goudar, R. (2012). *A More Multifactor Secure Authentication Scheme Based on Graphical Authentication.* Paper presented at the Advances in Computing and Communications (ICACC), 2012 International Conference on.

Karaca, K., & Levi, A. (2008). *Towards a framework for security analysis of multiple password schemes.* Paper presented at the Proceedings of the 1st European Workshop on System Security.

Kuo, C., Romanosky, S., & Cranor, L. F. (2006). *Human selection of mnemonic phrase-based passwords.* Paper presented at the Proceedings of the second symposium on Usable privacy and security.

Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder Surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951*.

Lei, M., Xiao, Y., Vrbsky, S. V., Li, C. C., & Liu, L. (2008). *A virtual password scheme to protect passwords.* Paper presented at the Communications, 2008. ICC'08. IEEE International Conference on.

Li, S., Shah, S., Khan, M., Khayam, S. A., Sadeghi, A.-R., & Schmitz, R. (2010). *Breaking e-banking CAPTCHAs.* Paper presented at the Proceedings of the 26th Annual Computer Security Applications Conference.

Mannan, M., & van Oorschot, P. C. (2007). Using a personal device to strengthen password authentication from an untrusted computer *Financial Cryptography and Data Security* (pp. 88-103): Springer.

Mannan, M., & van Oorschot, P. C. (2008). *Security and usability: the gap in real-world online banking.* Paper presented at the Proceedings of the 2007 Workshop on New Security Paradigms.

Markowitz, J. (2007). The many roles of speaker classification in speaker verification and identification *Speaker Classification I* (pp. 218-225): Springer.

Mihajlov, M., & Jerman-Blažič, B. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. *Interacting with Computers, 23*(6), 582-593.

Mockel, C. (2011). *Usability and Security in EU E-Banking Systems-Towards an Integrated Evaluation Framework.* Paper presented at the Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on.

Moeckel, C. (2011). Human-computer interaction for security research: the case of EU E-banking systems. *Human-Computer Interaction–INTERACT 2011*, 406-409.

Mohammadi, S., & Hosseini, S. Z. (2010). *Virtual password using Runge-Kutta method for internet banking.* Paper presented at the Communication Software and Networks, 2010. ICCSN'10. Second International Conference on.

Möller, S., Ben-Asher, N., Engelbrecht, K.-P., Englert, R., & Meyer, J. (2011). Modeling the behavior of users who are confronted with security mechanisms. *Computers & Security, 30*(4), 242-256.

Monrose, F., & Reiter, M. (2005). Graphical passwords. *Security and Usability*, 147-164.

Mulligan, J., & Elbirt, A. (2005). Desktop security and usability trade-offs: An evaluation of password management systems. *Information Systems Security, 14*(2), 10-19.

Nilsson, M., Adams, A., & Herd, S. (2005). *Building security and trust in online banking.* Paper presented at the CHI'05 extended abstracts on Human factors in computing systems.

Oorschot, P., & Wan, T. (2009). TwoStep: An authentication method combining text and graphical passwords. *E-Technologies: Innovation in an Open World*, 233-239.

Peng, Y., Chen, W., Chang, J. M., & Guan, Y. (2010). *Secure online banking on untrusted computers.* Paper presented at the Proceedings of the 17th ACM conference on Computer and communications security.

Prakash, M. V., & Shobana, S. J. (2010). *Eliminating Vulnerable Attacks Using One-Time Password and PassText Analytical Study of Blended Schema}.* Paper presented at the IJCA Proceedings on International Conference on VLSI, Communications and Instrumentation (ICVCI)}.

Rekha, N. R., Rao, Y. V. S., & Sarma, K. (2011). *Enhanced Key Life in Online Authentication Systems Using Virtual Password.* Paper presented at the Information Technology: New Generations (ITNG), 2011 Eighth International Conference on.

Saxena, A. (2008). *Dynamic authentication: Need than a choice.* Paper presented at the Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on.

Shabih ul Hasan Naqvi, S., & Afzal, S. (2010, 9-11 July 2010). *Operation Code Authentication preventing shoulder surfing attacks.* Paper presented at the Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on.

Shah, S. U., & Minhas, A. A. (2009). *New Factor of Authentication: Something You Process.* Paper presented at the Future Computer and Communication, 2009. ICFCC 2009. International Conference on.

Shakir, M., & Khan, A. (2010). *S3TFPAS: Scalable shoulder surfing resistant textual-formula base password authentication system.* Paper presented at the Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., . . . Cranor, L. F. (2010). *Encountering stronger password requirements: user attitudes and behaviors.* Paper presented at the Proceedings of the Sixth Symposium on Usable Privacy and Security.

Shi, P., Zhu, B., & Youssef, A. (2009). *A PIN Entry Scheme Resistant to Recording-Based Shoulder-Surfing.* Paper presented at the Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on.

Shi, P., Zhu, B., & Youssef, A. (2010). *A framework to strengthen password authentication using mobile devices and browser extensions.* Paper presented at the Signal Processing and Information Technology (ISSPIT), 2010 IEEE International Symposium on.

Simons, D. J., & Levin, D. T. (1997). Change blindness. *Trends in cognitive sciences, 1*(7), 261-267.

Stebila, D. J., Udupi, P. V., & Shantz, S. C. (2008). Multi-Factor Password-Authenticated Key Exchange: Google Patents.

Stuttard, D., & Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*: Wiley.

Sullivan, B. (2005). Click! Online banking usage soars. *Online Banking special*.

Tanapichet, P., Cooharojananone, N., & Lipikorn, R. (2011). *Automatic comic strip generation using extracted keyframes from cartoon animation.* Paper presented at the Intelligent Signal Processing and Communications Systems (ISPACS), 2011 International Symposium on.

Tatroe, K., MacIntyre, P., & Lerdorf, R. (2013). *Programming Php*: O'Reilly Media.

Thorpe, J., & van Oorschot, P. C. (2007). *Human-seeded attacks and exploiting hot-spots in graphical passwords.* Paper presented at the 16th USENIX Security Symposium.

Vivekanandan, L., & Jayasena, S. (2012). Facilities offered by the banks and expectations of IT savvy banking customers. *Procedia-Social and Behavioral Sciences, 40*, 576-583.

Weir, C. S., Douglas, G., Richardson, T., & Jack, M. (2010). Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers*, *22*(3), 153-164.

Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J.-C. (2006). *Design and evaluation of a shoulder-surfing resistant graphical password scheme.* Paper presented at the Proceedings of the working conference on Advanced visual interfaces.

Zhao, H., & Li, X. (2007). *S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme.* Paper presented at the Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on.

Zheng, Z., Liu, X., Yin, L., & Liu, Z. (2009). *A stroke-based textual password authentication scheme.* Paper presented at the Education Technology and Computer Science, 2009. ETCS'09. First International Workshop on.