# SMART CARDS AND THE FINGERPRINT: A PROPOSED FRAMEWORK FOR THE AUTOMATIC TELLER MACHINE (ATM) SYSTEM

MOHD HASBULLAH BIN OMAR

UNIVERSITI UTARA MALAYSIA
2002

# SMART CARDS AND THE FINGERPRINT: A PROPOSED FRAMEWORK FOR THE AUTOMATIC TELLER MACHINE (ATM) SYSTEM

A thesis submitted to the Graduate School in full fulfillment of the requirements for the degree of Master of Science (Information Technology), Universiti Utara Malaysia

by
Mohd Hasbullah bin Omar

# PERMISSION TO USE

In presenting this thesis in full fulfillment of the requirements for a post graduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor(s) or, in their absence, by the Dean of Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Graduate School
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

# ABSTRACT

The need to control access to certain information and resources has been taken seriously nowadays due to fraud and other threats to current security systems. This research believes that no single security method, algorithm, key or procedure is entirely secure. Hence, a combination of multiple security components is mandatory to provide a high level of protection against fraud and other threats. This research combines three security components, which are, the smart card, fingerprint recognition and cryptography. It looks into the vulnerabilities of magnetic-stripe cards and personal identification numbers (PIN) or passwords widely used in systems today. As a result, the research proposed a framework for user identification and authentication in automatic teller machine (ATM) systems using fingerprints and smart cards as opposed to the PIN and magnetic-stripe cards. The cryptography is also implemented to further secure the data stored on the smart card. This robust method of user identification and authentication would hopefully reduce the vulnerabilities of ATM in the future.

# ABSTRAK

Keperluan mengawal akses kepada sesuatu sumber dan maklumat tertentu telah dititikberatkan sejak akhir-akhir ini disebabkan oleh keadaan sistem keselamatan sekarang yang terdedah kepada penipuan dan ancaman-ancaman seumpamanya. Penyelidikan ini percaya bahawa tiada satu pun pendekatan keselamatan, algoritma, kunci atau prosedur sahaja yang betul-betul selamat. Justeru, kombinasi pelbagai komponen keselamatan adalah mandatori atau perlu dalam menyediakan perlindungan bertahap tinggi bagi menentang atau mengawal daripada penipuan dan ancaman-ancaman lain. Penyelidikan ini menggabungkan tiga komponen keselamatan, iaitu kad pintar, pengesahan cap jari dan kaedah kriptografi. Ia melihat kelemahan yang terdapat pada kad pita magnetik dan nombor pengenalan diri atau kata laluan yang digunakan secara meluas dalam kebanyakan sistem pada hari ini. Hasilnya, penyelidikan ini mencadangkan satu rangka kerja untuk pengecaman dan pengesahan pengguna dalam sistem mesin teller automatik menggunakan cap jari dan kad pintar berbanding nombor pengenalan diri dan kad pita magnetik. Kaedah kriptografi juga digabungkan agar maklumat yang disimpan di atas kad pintar lebih selamat. Kekuatan pendekatan ini dalam pengecaman dan pengesahan pengguna secara langsung akan dapat mengurangkan kelemahan yang terdapat pada mesin teller automatik pada masa hadapan.

# ACKNOWLEDGEMENTS

In the name of Allah, the Most Gracious and the Most Merciful.

I would like to extend my thanks and gratitude to:

Allah the Almighty for giving me excellent health and mind for doing the research;

The Ministry of Science and Technology for the financial support;

Universiti Utara Malaysia and the School of Information Technology for the facilities and resources provided;

Both my supervisors, Mr. Roshidi Din and Mr. Hatim Mohamad Tahir for their wonderful support and effort in assisting me carry out this research and for the thesis to become a reality;

The ex-Dean, Professor Dr. Abu Talib Othman for his confidence and support, also for paving the way for MSc(IT) by Research at the School of Information Technology; staff members of the Graduate School and the School of Information Technology for their kind cooperation;

My beloved wife, Ms Juliana Aida Abu Bakar for her love and patience; my child, Ahmad Fathi who was born in the middle of the course duration; both my parents, parents-in-law and siblings for being there;

My colleagues, Mr. Ahmad Hisham Zainal Abidin, Mr. Amran Ahmad, Mr. Wan Hussain Wan Ishak, Mr. Mohamad Amir Abu Seman, Mr. Ahmad Hanis Mohd Shabli and others for their kindness, support and the wonderful series of discussions we had;

And last but not least, all individuals involved in the establishment of this research.

# CONTENTS

**CHAPTER THREE : RESEARCH METHODOLOGY**



**CHAPTER FOUR : ANALYSIS AND DESIGN**



**CHAPTER FIVE : RESULTS AND DISCUSSION**

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **AES** | - Advanced Encryption Standard |
| **AFIS** | - Automatic Fingerprint Identification System |
| **APDU** | - Application Data Protocol Unit |
| **API** | - Application Programming Interface |
| **ATM** | - Automatic Teller Machine |
| **BSI** | - British Standards Institute |
| **CEN** | - European Committee of Standardization |
| **DES** | - Data Encryption Standard |
| **DF** | - Dedicated File |
| **DSN** | - Data Source Name |
| **DSS** | - Digital Signature Standard |
| **EEPROM** | - Electrically Erasable Programmable Read Only Memory |
| **EF** | - Elementary File |
| **EMV** | - Europay, MasterCard and Visa |
| **EPROM** | - Erasable Programmable Read Only Memory |
| **ETSI** | - European Telecommunications Standards Institute |
| **FAR** | - False Acceptance Rate |
| **FRR** | - False Rejection Rate |
| **GMPC** | - Government Multi-Purpose Card |
| **GPK** | - Gemplus Public Key |
| **GSM** | - Global Standard for Mobile Communications |
| **ICC** | - Integrated Circuit Card |
| **ICT** | - Information Communication Technology |
| **IDEA** | - International Data Encryption Algorithm |
| **IEC** | - International Electrotechnical Commission |
| **IFD** | - Interface Device |
| **ISO** | - International Standards Organization |
| **IT** | - Information Technology |
| **MF** | - Master File |
| **MFC** | - Microsoft Foundation Classes |

| | |
|---|---|
| **MULTOS** | - Multi-applications Operating System |
| **OCF** | - OpenCard Framework |
| **ODBC** | - Open Database Connectivity |
| **PC/SC** | - Personal Computer Smart Card |
| **PIN** | - Personal Identification Number |
| **PKI** | - Public Key Infrastructure |
| **RAM** | - Random Access Memory |
| **ROM** | - Read Only Memory |
| **RSA** | - Rivest-Shamir-Adleman |
| **SDK** | - Software Development Kit |
| **SPI** | - System Programming Interface |
| **SQL** | - Structured Query Language |

# CHAPTER ONE

# Introduction

Computer security plays an important role in identifying and authenticating users in this information and communication technology (ICT) era. Organizations are becoming increasingly aware of computer security as all form of computer networks (Janson *et al.*, 1991) are deployed in business and government critical operations (Lampson *et al.*, 1992). Computer security is required as a prerequisite for reliable information systems (Graff, 1995). This calls for more trustworthy forms of user identification and authentication than password or Personal Identification Number (PIN).

To date, most information systems authenticate their users by the use of passwords or PINs (Fritzner *et al.*, 1991). This use of the password or PIN schemes was introduced in the early days of multi-user (time-sharing) machines and its use has continued into today's highly networked and distributed systems (Woo *et al.*, 1992). The system does not further identify users if the password or PIN is correctly entered because the password or PIN is meant to be known only to the authorized user. This allows anybody related or unrelated to the user who knows the user's password or PIN to make illegal access or withdrawal.

The contents of the thesis is for internal user only

# REFERENCES

American Biometric Company (1999). Biometric and Smart Card User Authentication. Discussion Paper.

Anderson, R. (1994), "Why Cryptosystems Fail", *Communications of the ACM*, November 1994, Volume 37, Issue 11.

Anderson, R. and Kuhn, M (1996). Tamper Resistance – A Cautionary Note. In *Proceeding of Workshop on Electronic Commerce*, pp. 1 – 11.

Anderson, R. and Kuhn, M. (1997). Low Cost Attacks on Tamper Resistant Devices. In Lomas, M. *et al.*, editors, *Proceedings of the fifth International Workshop on Security Protocols*, LNCS 1361, pp. 125 – 136. Springer-Verlag.

Anonymous (2000). Digital 21: Knowledge Corner: Smart Card. [On-Line] Available http://www.info.gov.hk/digital21/eng/knowledge/smart.html

Braghin, C. (2000). Biometric Authentication. Department of Computer Science, University of Helsinki.

Bank Negara Malaysia (2000). Unauthorised ATM Withdrawals. [On-Line] Available http://www.bnm.gov.my/en/News/releases.asp?yr=2000&sid=0408.

Bechelli, L., Bistarelli, S. and Vaccarelli, A. (2002). Biometrics Authentication with Smartcard. Technical Report, Istituto di Informatica e Telematica, CNR Pisa. [On-Line] Available ftp://ftp.di.unipi.it/pub/Papers/bista/impronte-IIT_TR-08_2002.pdf.gz

Castle, T. (2001). Online Authentication Using Combined Smart Card And Fingerprint Recognition. Centre for Applied Research into Education Technology, University of Cambridge. [On-Line] Available http://www.caret.ac.uk/pdfs_ppts/fingerprint.pdf.

Chan, S. C. (1997). An Overview of Smart Card Security. [On-Line] Available http://home.hkstar.com/~alanchan/papers/smartCardSecurity/index.html.

Consumer Biometric Applications (1999). Consumer Biometric Applications: A Discussion Paper [On-Line] Available http://www.ipc.on.ca/english/pubpres/papers/cons-bio.htm. 23/8/2000.

Corcoran, D., Sims, D., and Hillhouse, B., (2000), "Smart Cards and Biometrics: Your Key To PKI", Retrieved on August 22, 2000 from the World Wide Web at http://noframes.linuxjournal.com/lj-issue59/3013.html.

Daemen, J., Rijmen, V. (2000). The Block Cipher Rijndael. *Smart Card Research and Applications, LNCS 1820,* J.-J. Quisquater and B. Schneier, Eds., Springer-Verlag, pp. 288-296.

Dreifus, H. and Monk, J. T. (1998), *Smart Card. A Guide to Building and Managing Smart Card Applications*, Wiley Computer Publishing, John Wiley and Sons Inc, Canada.

FIPS-197 (2001). Announcing the Advanced Encryption Standard (AES). National Institute of Standard and Technology (NIST), US [On-Line] Available http://csrc.nist.gov/encryption/aes.

Fritzner, C., Nilsen, L., and Skomedal, A. (1991), Protecting Security Information in Distributed Systems. In *Proceedings of the IEEE Computer Society Symposium in Security and Privacy*, pages 245-254. IEEE Computer Society, IEEE Press.

Ganger, G. R. (2001), Authentication Confidences [On-Line] Available http://reports-archive.adm.cs.cmu.edu/cs2001.html

Gaskell, G. I. (2000). *Integrating Smart Cards into Kerberos*. Master dissertation, Faculty of Information Technology, Queensland University of Technology.

Gemplus (2001). GemPC-Touch Series Software Development Kit. Installation and Programming Guide Version 1.0. France.

Gollmann, D. (1999). *Computer Security*. West Sussex, England: John Wiley and Sons, Ltd.

Gong, L., Lomas, M. A., Needham, R. M. and Saltzer, J. H. (1993), Protecting Poorly Chosen Secrets From Guessing Attacks. *IEEE Journal on Selected Areas in Communications*, 11(5):648-656.

Graff, M. G. (1995), Great Unsolved Problems in Applied Computer Security. In *National Information Systems Security Conference*, volume 18, pages 63-72, National Information System Security Center – US Government.

Gulachenski, B. D. and Costa, M. J. (1994), Taxonomy of Threats and Security Services for Information Systems, working paper, MITRE Corporation.

Hachez, G., Koeune, F. and Quisquater, J.J. (2000). Biometrics, Access Control, Smart Cards: A Not So Simple Combination. [On-Line] Available http://www.dice.ucl.ac.be/crypto/publications/ 2000/Biometrics.pdf

ISO/IEC (1997). Information Technology – Identification Cards – Integrated Circuit(s) Cards With Contacts, 1995. Part 4 – Inter-Industry Commands for Interchange. An amendment was issued in 1997.

Jain, A. K., Hong, L., Pankanti, S. and Bolle, R. (1997). An Identity Authentication System Using Fingerprints. *Proceedings of IEEE*. Vol. 85, No. 9, pp. 1365-1388.

Jain, A.K., Prabhakar, S. and Pankanti, S. (2001). Matching and Classification: A Case Study in Fingerprint Domain. *In Proceedings of Indian National Science Academy (INSA-A)*. Vol. 67, No. 2, pp. 67 – 85.

Janson, P. and Molva, R. (1991), Security in Open Network and Distributed Systems, *Computer Networks and ISDN Systems*, 22:323-346.

Keating, G. (1999). Performance Analysis of AES Candidates on the 6805 CPU core. [On-Line] Available http://members.ozemail.com.au/~geoffk/aes-6805/paper.pdf.

Kocher, P., Jaffe, J. and Jun, B. (1998a). Introduction to Differential Power Analysis and Related Attacks. [On-Line] Available http://www.cryptography.com/resources/whitepapers/DPA-technical.html.

Kocher, P., Jaffe, J. and Jun, B. (1998b). Q&A on Differential Power Analysis. [On-Line] Available http://www.cryptography.com/resources/whitepapers/DPA-qa.html

Kommerling, O. and Kuhn, M. (1999). Design Principles for Tamper-Resistant Smartcard Processors. In *Proceeding of the Usenix Workshop on Smart Card Technology (Smartcard 99)*, pages 9-20.

Lampson, B., Abadi, M., Burrows, M. and Wobber, E. (1992), Authentication in Distributed Systems: Theory and Practice, *Association of Computing Machinery Transactions on Computer Systems,* 10(4):265-310.

Morris, R. and Thompson, K. (1979). Password Security: A Case History. *Communications of the ACM*, Vol.22, No.11, November, 1979, pp.594-597.

National Institute of Standards and Technology (NIST), U.S. Department of Commerce (1995), "An Introduction to Computer Security: The NIST Handbook", Special Publication 800-12.

Nunamaker, J. F., Chen, M., and Purdin, T. (1991). Systems Development in Information Systems Research. *Journal of Management Information Systems*, Vol. 7, No. 3, pp. 89 – 106.

Omar, M. H., Din, R. and Mohamad Tahir, H. (2001). Smart Card and Fingerprint: An Alternative for Users Identification and Authentication. *Persidangan Kebangsaan Penyelidikan dan Pembangunan (P&P) IPTA 2001.*

Rankl, W. and Effing, W. (2000). *Smart Card Handbook.* West Sussex, England: John Wiley and Sons, Ltd.

Ratha, N., Karu, K., Chen, S., and Jain, A. K. (1996). A Real-Time Matching System for Large Fingerprint Database. *IEEE Trans. On Pattern Anal. Machine Intell.*, Vol. 18, No. 8, pp. 799-813.

Rubin, J. (1994). *Handbook of Usability Testing: How to Plan, Design and Conduct Effective Tests.* John Wiley & Sons.

Schneier, B. (1996). *Applied Cryptography Second Edition: Protocol, Algorithms and Source Code in C.* Canada: John Wiley and Sons Inc..

Smith, R. (2001). Deciphering the Advanced Encryption Standard. [On-Line] Available http://www.networkmagazine.com/article/NMG20010226S0010 Retrieved on 9/3/2002.

Thieme, M. (2000). Smart Cards and Biometrics. Biometrics In Human Services User Group. [On-Line] Available http://www.biometricgroup.com/a_press/bhsugmar99.html.

Villiot, J. M. (2001). "Fingerprint Identification", [On-Line] Available http://c3iwww.epfl.ch/projects_activities/jmv/fingerprint_identification.html

Woo, T. Y. C. and Lam, S. S. (1992), Authentication for Distributed Systems. *IEEE Computer*, pages 39-52.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2002). The Memorability and Security of Passwords – Some Empirical Results. [On-Line] Available http://www.cl.cam.uk/ftp/users/rja14/tr500.ps Retrieved on 14/03/2002.