UNIVERSITI PUTRA MALAYSIA

ENHANCEMENT OF SECURITY ARCHITECTURE FOR SMARTCARD-BASED AUTHENTICATION PROTOCOLS

LAWAN AHMED MOHAMMED.

ENHANCEMENT OF SECURITY ARCHITECTURE FOR SMARTCARD-BASED AUTHENTICATION PROTOCOLS

LAWAN AHMED MOHAMMED

DOCTOR OF PHILOSOPHY
UNIVERSITI PUTRA MALAYSIA

June, 2004

ENHANCEMENT OF SECURITY ARCHITECTURE FOR SMARTCARD-BASED AUTHENTICATION PROTOCOLS

By

LAWAN AHMED MOHAMMED

Thesis Submitted to the School of Graduate Studies,
Universiti Putra Malaysia, in Fulfilment of the
Requirements for the Degree of Doctor of Philosophy

June, 2004

DEDICATION

This thesis is dedicated to my parents whose selfless sacrifices and dedications have made it possible for me to reach this stage of my studies.

Abstract of thesis presented to the Senate of the Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

ENHANCEMENT OF SECURITY ARCHITECTURE FOR SMARTCARD-BASED AUTHENTICATION PROTOCOLS

By

LAWAN AHMED MOHAMMED

June, 2004

Chairman: Associate Professor Haji. Dr. Abdul Rahman Ramli, Ph.D.

Faculty: Engineering

Currently computer systems and software used by the average user offer less security due to rapid growth of vulnerability techniques. This dissertation presents an approach to increase the level of security provided to users when interacting with otherwise unsafe applications and computing systems. It provides a general framework for constructing and analyzing authentication protocols in realistic models of communication networks. This framework provides a sound formalization for the authentication problem and suggests simple and attractive design principles for general authentication protocols. The general approach uses trusted devices (specifically smartcards) to provide an

area of secure processing and storage. The key element in this approach is a modular treatment of the authentication problem in cryptographic protocols; this applies to the definition of security, to the design of the protocols, and to their analysis. The definitions are drawn from previous ideas and formalizations and incorporate several aspects that were previously overlooked. To identify the best cryptographic algorithm suitable for smartcard applications, the dissertation also investigates the implementation of Elliptic Curve encryption techniques and presents performance comparisons based on similar techniques. The findings discovered that the proposed Elliptic Curve Cryptographic (ECC) method provides greater efficiency than similar method in terms of computational speed.

Specifically, several aspects of authentication protocols were studied, and new definitions of this problem were presented in various settings depending on the underlying network. Further, the thesis shows how to systematically transform solutions that work in a model of idealized authenticated communications into solutions that are secure in the realistic setting of wired communication channels such as access control, and online transactions involving contact communication schemes.

As with all software development, good design and engineering practices are important for software quality. Rather than thinking of security as an add-on

feature to software systems, security should be designed into the system from the earliest stages of requirements gathering through development, testing, integration, and deployment. In view of this, a new approach for dealing with this problem in an object-oriented approach is presented. Some practical illustrations were analyzed based on the *Unified Modeling Language* (UML) as it applies to modeling authentication/access control schemes in online transactions. In particular, important issues such as how smartcard applications can be modeled using UML techniques and how UML can be used to sketch the operations for implementing a secure access using smartcard has been addressed.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia bagi mendapatkan ijazah Doktor Falsafah

SUATU KAJIAN DAN PEMANTAPAN SENIBINA KESELAMATAN UNTUK PROTOKOL PENGESAHAN BERASASKAN KAD PINTAR

Oleh

LAWAN AHMED MOHAMMED

Jun, 2004

Pengerusi: Profesor Madya Prof. Haji. Abdul Rahman Ramli, Ph.D.

Fakulti: Kejuruteraan

Sistem komputer dan perisian yang digunakan oleh pengguna kini mempunyai ciri keselamatan yang semakin tumpul disebabkan peningkatan dalam teknik-teknik pendedahan dalam ciri keselamatan *(vulnerability techniques)*. Disertasi ini cuba mengenengahkan satu kaedah untuk meningkatkan tahap keselematan untuk pengguna apabila berinteraksi dengan aplikasi dan sistem komputer yang kurang selamat. Ia juga memberikan satu garis panduan untuk membina dan menganalisa protokol pengesahan di dalam model rangkaian komunikasi yang realistik. Garis panduan memberikan satu susun atur yang rapi bagi permasalahan pengesahan dan mencadangkan prinsip rekabentuk yang mudah

dan menarik untuk protokol pengesahan umum. Kaedah umum menggunakan peranti yang dipercayai (khususnya kad pintar) untuk memberikan kawasan selamat bayi elemen utama di dalam kaedah ini ialah dengan menggunakan rawatan modular terhadap permasalahan pengesahan dalam protokol kriptografi. Kaedah ini juga diterapkan kepada definisi keselamatan hinggalah kepada rekabentak protokol dan analisis protokol tersebut. Definisi yang dimaksudkan telah di ambil dari idea-idea dan perancangan terdahulu dan melibatkan beberapa aspek yang sebelum ini telah diabaikan. Untuk mengenal pasti algoritma kriptografi yang terbaik sesuai untuk aplikasi kad pintar, disertasi ini juga mengkaji perlaksanaan teknik enkripsi *'Elliptic Curve Cryptography'* (ECC), dan membuat perbandingan berasaskan pada teknik-teknik yang serupa. Penemuan yang dijumpai bahawa ECC yang dicadangkan memberikan kecekapan yang lebih tinggi berbanding kaedah ECC yang serupa.

Khususnya, beberapa aspek protokol pengesahan telah di kaji dan penakrifan baru bagi masalah ini telah dibentangkan dalam pelbagai persekitaran bergantung kepada rangkaian asasnya. Selanjutnya, tesis ini menunjukkan bagaimana untuk menukar secara sistematik penyelesaian yang berfungsi di dalam model komunikasi disahkan yang unggul, kepada penyelesaian yang selamat dalam persekitaran saluran komunikasi yang realistik seperti di dalam sistem kawalan laluan, dan urusniaga dalam talian yang melibatkan skema-skema komunikasi secara terus.

Sebagaimana dalam pembangunan perisian, rekabentuk dan amalan kejuruteraan yang baik adalah penting bagi memastikan kualiti perisian. Daripada memikirkan ciri keselamatan sebagai satu ciri tambahan kepada system perisian, ciri-ciri keselamatan sepatutnya diterapkan ke dalam sistem dari peringkat permulaan pengumpulan keperluan sehinggalah pembangunan, ujian, integrasi dan perlaksanaan. Dengan ini, satu pendekatan baru bagi menangani masalah ini dengan menggunakan pendekatan berorientasikan objek diunjurkan. Beberapa contoh praktik telah dianalisa berdasarkan kepada *'Unified Modeling Language (UML)'* seperti mana ia dilaksanakan kepada model pengesahan/skema kawalan laluan di dalam urusniaga melalui Internet. Secara khususnya, perhatian dapat diberikan kepada isu-isu penting seperti bagaimana aplikasi kad pintar dapat dilaksanakan menggunakan teknik UML dan bagaimana UML dapat digunakan untuk melakarkan operasi bagi melaksanakan laluan selamat berasaskan kad pintar .

ACKNOWLEDGMENTS

First of all I would like to thank All Mighty Allah for everything (Alhamdulillah). I am extremely grateful to my supervisor Associate Professor Haji AbdulRahman Ramli for the technical, financial and moral support he provided throughout my study. He has opened my mind to research in the field of computer and network security. I am also very grateful to the other members of the dissertation committee - Professor Mohamad Daud and Dr V. Prakash for their support and feedback in many ways. I had the opportunity to work with them and it has helped my research work immensely. Further, I would like to acknowledge Professor Mohamad Daud for his financial support.

Several people have helped and supported me in writing this dissertation. I would like to acknowledge Abdulkarim Mohd and Salisu Garba for there contribution in processing and delivering the thesis to the authority concern while I was away. Special thank goes to Mohammad Fadzilli for his efforts and comments especially in translating the abstract. Many thanks to all my lab mates who contributed in one way or the other toward successful completion of the thesis. Last but not least, I would like to thank my parents and my wife for being patient with me and for their encouragement during my studies.

Thanks everyone!
Lawan Ahmed.

TABLE OF CONTENTS

List of Tables

LIST OF FIGURES

GLOSSARY OF TERMS

ACLU	American Civil Liberties Union
ATR	Answer to Reset
BBS	Blum-Blum-Shub
BWT	Block Waiting Time
CA	Certification Authorities
CRT	Chinese Remainder Theorem
CWT	Character Waiting Time
COSng	Next Generation Smartcard Operating Systems
CDMF	Commercial Data Masking Facility
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DNS	Domain Name System
ECC	Elliptic Curve Cryptosystem
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECKAS-DH	Elliptic Curve Key Agreement Scheme (Diffie-Hellman)
ECSSA	Elliptic Curve Signature Scheme
ECSVDP-DH	EC Secret Value Derivation Primitive (Diffie-Hellman)
ECSP-NR	Elliptic Curve Signature Primitive, Nyberg-Rueppel
ECVP-NR	Elliptic Curve Verification Primitive, Nyberg-Rueppel
EMSA	Encoding Method for Signatures with Appendix
ECDSA	Elliptic Curve Digital Signature Algorithm
ECES	Elliptic Curve Encryption Scheme
ETU	Element Time Unit
FAR	False Acceptance Rate
FRR	False Rejection Rate
GSM	Global System for Mobile Communication
GUI	Graphical User interface
IDEA	International Data Encryption Algorithm
ICC	Integrated Circuit Card
KDF	Key Derivation Function
LCG	Linear Congruential Generators
LFSR	Linear Feedback Shift Register
MAC	Message Authentication Code
MEPS	Malaysian Electronic Payment Systems
MISC	Miscellaneous procedures
MOV	Menezes-Okamoto-Vanstone
NBS	National Bureau of Standard
NTP	Network Time Protocol
ODL	Online Distance Learning
PCBC	Propagating CipherBblock Chaining
PGP	Pretty Good Privacy

PRNG	Pseudo-random number generator
RBAC	Role based access control
RSA	Rivest-Shamir-Adleman Algorithm
SHA-1	Secure Hash Algorithm, Version1
SG-LFSR	Shrinking Generator Linear Feedback Shift Register
SSL	Secure Sockets Layer
STS	Station-to-Station Protocol
SNMP	Simple Network Management Protocol
RNG	Random number generation
TFTP	Trivial File Transfer Protocol
TGS	Ticket Granting Server
TGT	Ticket-Granting Ticket
TTP	Trusted Third Party
UML	Unified Modeling Language