
UNIVERSITI PUTRA MALAYSIA

# AN AUTHENTICATION METHOD FOR SECURE INTERNET TRANSACTION USING SMART CARD AND SECURE COPROCESSOR

MUSTAFA ABDSALAM AYAD

FK 2002 4

# AN AUTHENTICATION METHOD FOR SECURE INTERNET TRANSACTION USING SMART CARD AND SECURE COPROCESSOR

By

MUSTAFA ABDSALAM AYAD

Thesis Submitted in Fulfillment of the Partial Requirement for the Degree of Master of Science in the Faculty of Engineering University Putra Malaysia
July 2002

UPM

## DEDICATION

*To my family….*

Abstract of thesis presented to the Senate of University Putra Malaysia in fulfillment of the partial requirement for the degree of Master of Science

**AN AUTHENTICATION METHOD FOR SECURE INTERNET TRANSACTION USING SMART CARD AND SECURE COPROCESSOR**

By

**MUSTAFA ABDSALAM AYAD**

**July 2002**

**Chairman : V. Prakash, Ph. D.**

**Faculty : Engineering**

Authentication is the process of confirming an identity. In the context of network interactions, authentication involves the confident identification of one party by another party. Authentication of users in distributed systems poses special problems because, users lack the ability to encrypt and decrypt. In most systems today, the user is forced to trust the node he wants to use. In a more satisfactory design, the user carries a smart card with sufficient computing power to assist him. This thesis deals with relatively new methods of authentication using a smart card and secure coprocessor. We analyze two cases to authenticate a client, depending on the smart card usage. The major attacks that affect the smart card and the server are applied to our proposed methods of authentication. The result shows that using the proper system preparation and proper authentication sequence for our methods the effects could be minimized.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia untuk memenuhi keperluan ijazah Master Sains

**KAEDAH AUTENTIKASI BAGI TRANSAKSI INTERNET YANG SELAMAT MENGGUNAKAN KAD PINTAR DAN PROSESOR BERSAMA YANG SELAMAT**

**Oleh**

**MUSTAFA ABDSALAM AYAD**

**Julai 2002**

**Pengerusi : V. Prakash,Ph.D.**

**Fakulti : Kejuruteraan.**

Pengesahan adalah suatu proses pemastian identiti. Di dalam konteks perhubungan menggunakan rangkaian, pengesahan melibatkan pemastian identiti suatu pihak oleh pihak yang dihubungi. Pengesahan oleh pengguna di dalam sistem teragih mempunyai masalah tersendiri disebabkan pengguna tidak boleh penyulitan dan menyah sulitan. Kebanyakan sistem pada masa ini terpaksa mempercayai pelayan yang ingin digunakan. Reka bentuk yang lebih memuaskan ialah pengguna menggunakan kad pintar untuk membantu membuat pengluomputan pengesahan. Tesis ini mengemukakan kaedah baru untuk pengesahan dengan menggunakan kad pintar dan pembantu pemproses keselamatan. Kami menganalisa dua kes untuk pengesahan pengguna, bergantung kepada penggunaan kad pintar. Serangan dilaksanakan ke atas kaedah ini yang cuba mengkompromi kad pintar dan pelayan. Keputusan menunjukkan bahawa dengan pengasingan serta turutan pengesahan yang betul, keberkesanan serangan boleh dikurangkan ke tahap yang minima.

## ACKNOWLEDGEMENTS

I wish to thank my supervisor, Dr. V. Prakash, for the guidance that he managed to extend to me during my Master study, and for his efforts to provide a good research environment, which made this thesis possible.

I am no less grateful to the other committee members Puan Wan Azizun, Puan Norkamariah Nordin, who were kind enough to read and comment on my work.

I am grateful to the researchers at Wireless Research Group, Department of Computer and Communication, for their helpful discussion

Last but certainly not least, I wish to thank my wife Hasna and my brother Khaled for having supported me in such a stable and loving environment, which has enabled me to come so far.

I certify that an Examination Committee met on 15th July 2002 to conduct the final examination of Mustafa Abdsalam Ayad on his Master of Science thesis entitled "An Authentication Method for Secure Internet Transaction Using Smart Card and Secure Coprocessor" in accordance with Universiti Pertanian Malaysia (Higher degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:-

ABDUL RAHMAN RAMLI, Ph.D.
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

V. PRAKASH, Ph.D.
Faculty of Engineering,
Universiti Putra Malaysia
(Member)

WAN AZIZUN WAN ADNAN,
Faculty of Engineering,
Universiti Putra Malaysia
(Member)

NOR KAMARIAH NOORDIN,
Faculty of Engineering,
Universiti Putra Malaysia
(Member)

**SHAMSHER MOHAMAD RAMADILI, Ph.D,**
Professor/Deputy Dean
School of Graduate Studies,
Universiti Putra Malaysia

Date: 30 JUL 2002

This Thesis submitted to the Senate of Universiti Putra Malaysia has been was accepted as fulfillment of the partial requirements for the degree of Master of Science.

AINI IDERIS, Ph.D,
Professor/Dean
School of Graduate Studies,
Universiti Putra Malaysia

Date: 12 SEP 2002

## DECLARATION FORM

I hereby declare that the thesis is based on my original work except for quotation and citations, which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

Name: MUSTAFA ABDSALAM AYAD.

Date: 29/7/2002

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| ACL | Access Control List |
| ATM | Automatic Taller machine |
| CA | Certification Authority |
| CBC | Cipher Block Chaining |
| CC | Cryptographic Checksum |
| CIA | Central Intelligence Agency |
| CPU | Central Processing Unit |
| DES | Data Encryption Standard |
| DN | Distinguished name |
| DSA | Digital Signature Algorithm |
| DSS | Digital Signature Standard |
| ECB | Electronic Code Book |
| FAT | File Allocation Table |
| FIPS | Federal Information Processing Standard |
| FLs | Financial Institutions |
| H(M) | Hash Code for Message M |
| HTTP | Hyper Text Transport Protocol |
| IMAP | Internet Messaging Access Protocol |
| ISO | International Standard Organization |
| KDC | Key Distribution Center |
| KEA | Key-exchange algorithms |
| KGB | Russian Equivalent of the CIA |
| KLP | Key Loader Program |

| | |
|---|---|
| LDAP | Lightweight Directory Access Protocol |
| MD4 | Message-Digest Algorithm 4 |
| MD5 | Message-Digest Algorithm 5 |
| NCL | National Consumer's League |
| OI | Order Information |
| OIMD | Order Information Message Digest |
| PI | Payment Information |
| PIMD | Payment Information Message Digest |
| PKCS | Public key Cryptography Standard |
| PKI | Public Key Infrastructure Functions |
| ROM | Read only Memory |
| RSA | (Rivest, Shamir and Adleman) |
| RSA | A public key Cryptographic Algorithm Named for its Inventors |
| S/N | Serial Number |
| SET | Secure Electronic Transaction. |
| SHA | Secure Hash Algorithms |
| SSL | Secure Sockets Layer |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| VLSI | Very Large Scale Integration |

# CHAPTER 1

# INTRODUCTION

## 1.1 An Overview

Security in networks of computers is an important issue, although networks raise new issues in security, familiar topics appear in the list of solutions to network security problems. The problems are loss of confidentiality, integrity, and availability. The solutions to these technologies include, encryption, access controls, strong authentication, and protocols. In fact, networks can be viewed as more complex example of computing systems. Threats arise at different points based on different technologies, so that many program development and operating system security concepts and controls apply to networks as well. Computer networks offer several advantages over single-processor systems, such as:

1. **Resource Sharing.** Users of a network can access a variety of resources through the network. Sharing databases, data and program files, and other resources reduces maintenance and storage costs while providing each user with improved access.

2. **Distributing the Workload.** The use of single system varies as users join and leave a system. The degree of fluctuation of workload for a single user can be moderated in a network, so the workload can be shifted from a heavily loaded system to an underused one.

3. **Increased Reliability.** Because a computing network consists of more than one computing system, the failure of one system or just one component need not necessarily block users from continuing to compute. If similar systems exist, users can move their computing to other systems when one system fails.
4. **Expandability.** Network system can be expanded easily by adding new nodes. This expansion of user-base can occur without the manager of any single system having to take special action (Pfleeger 1997).

Computing networks have similar characteristics. The network must ensure integrity of data, secrecy of data and availability of services. Each user accesses the network through a single operating system, which also includes network interface responsibilities. Users still expect the operating systems to enforce the security policies of the network. However, in a network the operating systems at the two ends of the communication, as well as the operating systems of all computers in between, must cooperate to enforce security (Pfleeger 1997).

### 1.1.1 Motivation

The security of credit card transactions remains the number one concern both for Internet users who have yet to make an online purchase, and for those who have performed an online transaction. The US National Consumer 's League Internet Fraud Watch (NCL) has reported that American consumers

lost over $3.2 million to online scams in 1999, a 38 percent increase over the previous year. The vast majority of cases reported to the NCL involved payments by cheque or money order, with credit card transactions accounting for only three percent of cases. An online survey in January, March 2000 found that 41 percent of regular Internet users had shopped online two to four times, while 22 percent had made one online purchase. Significantly, 19 percent had made over 10 online transactions. Due to continued strong growth in the number of Internet users, it seems likely the total number of people shopping online and the proportion of frequent shoppers will continue to increase. Internet-related fraud is certainly a matter for concern, and authorities around the world are active in combating a range of illegal activities being conducted over the Internet. One of the most widely publicized cases of credit card fraud occurred in the US, where a group of web-based companies made small, recurrent charges to hundreds of thousands of credit cards (Phantom Menace 2001, Meridien Research 2001).

Improvements in security and encryption technology will make it more difficult for criminals to intercept online transactions. Both Netscape Navigator and Microsoft Internet Explorer use Secure Sockets Layer (SSL) to encrypt data before sending it over the Internet. SSL scrambles personal data and provides an unbroken key or lock that appears in the bottom of the browser window. This technology provides a secure connection that keeps data private during transmission over the Internet, however it does not authenticate the parties at either end of the transaction.

Table 1: Credit Card Statistics- VISA and MasterCard.

| As at Fiscal Year Ending Oct. 31. | No. of Cards in Circulation (Millions). | No. of Accounts with balance (Millions). | # Of Cards Reported Lost or Stolen. | No. of Cards Fraudulently used. | $ Amount of Fraudulent Accounts written off (millions). |
|---|---|---|---|---|---|
| 1985 | 14.0 | 7.3 | 330,380 | 21,026 | $17.54 |
| 1986 | 15.5 | 7.9 | 378,239 | 22,326 | $18.61 |
| 1987 | 17.6 | 8.8 | 408,239 | 23,913 | $15.78 |
| 1988 | 19.4 | 9.5 | 460,348 | 25,773 | $15.63 |
| 1989 | 20.4 | 10.3 | 522,204 | 30,919 | $19.20 |
| 1990 | 23.2 | 11.1 | 520,716 | 32,851 | $28.90 |
| 1991 | 24.3 | 11.8 | 623,946 | 53,968 | $44.60 |
| 1992 | 24.4 | 12.2 | 650,088 | 61,234 | $63.50 |
| 1993 | 25.0 | 12.4 | 674,988 | 63,442 | $75.20 |
| 1994 | 27.5 | 13.2 | 731,052 | 63,635 | $70.60 |
| 1995 | 28.8 | 13.6 | 648,824 | 66,109 | $72.64 |
| 1996 | 30.2 | 14.1 | 794,996 | 77,740 | $83.63 |
| 1997 | 31.9 | 15.0 | 858,625 | 89,982 | $88.08 |
| 1998 | 35.3 | 16.0 | 895,817 | 126,384 | $104.80 |
| 1999 | 37.7 | 17.3 | 823,934 | 132,836 | $134.10 |
| 2000 | 40.1 | 18.5 | 805,580 | 112,070 | $156.38 |
| 2001 | 44.1 | 19.6 | 813,624 | 116,139 | $142.27 |

VISA International and MasterCard International, with support from many of the world's top financial institutions, are presently working to develop a more advanced encryption process called Secure Electronic Transaction (SET). SET involves a system of digital certificates provided by card issuers, and encryption. It enables the identity of both merchant and cardholder to be authenticated, and also ensures that neither the merchant or cardholder 's bank sees the purchaser 's credit card number (Konrad et al. 2000).

As shown in Table 1, the number of cards in circulation, the number of accounts with balance, the number of cards reported lost or stolen and the numbers of cards fraudulently used are increased as the years going on from

1985-2001. The number of cards fraudulently used at 1985 is 21,026 cards, while it is 116,139 at 2001 (Canadian Bankers Association 2001).

Enhancement of authentication protocols and encryption technology improved the security and makes it more difficult for hackers to intercept or tamper with online transactions. We propose the use of smart card and secure coprocessor to provide a highly secure environment for the Internet transactions. Two methods of authentication are proposed in this thesis, which can provide a secure environment for handshaking and secure transaction processing.

## 1.2 Threats in Networks

In the following sections we look to network security issues and reasons for network security problems, and security threats considering damage to confidentiality, integrity and availability, and then looking to many ways to accomplish threats to the network.

### 1.2.1 Network Security Issues

Networks have several security problems for several reasons. In the next sections we will explain each of the reasons, which are causing the network security problems.

#### 1.2.1.1 Sharing

Because of the resource sharing of networks, more users have the potential to access networked systems than single computers. Perhaps worse access is afforded to more systems, therefore access controls for single systems may be inadequate in the networks.

#### 1.2.1.2 Complexity of System

As we know that an operating system is the most complicated piece of software ever produced. Reliable security is difficult if not possible on large operating system, especially one not designed for security. A network combines two or more dissimilar operating systems. Therefore, a network operating system/control system is likely to be more complex than an operating system for single computer system. This complexity limits confidence in the security of a network.

#### 1.2.1.3 Unknown Perimeter

The expandability of a network also implies uncertainly about the network boundary. One host may be a node on two different networks, so that resources on one network are accessible to the users of other networks as well. Although wide accessibility is an advantage, this unknown or uncontrolled group of possibly malicious users is a security disadvantage. A similar problem occurs when new hosts can be added to the network. Every

network node must be able to react to the possible presence of new, untrustable hosts. Figure 1.1 points out the problems in defining the boundaries of a network. Notice that, users on a host in network D may be unaware of the potential connections from users of networks A and B.

#### 1.2.1.4 Many Points of Attack

A simple computing system is a self-contained unit. Access controls on one machine preserve the secrecy of data on that processor. However, when a file is stored in a network host remote from the user, the file may pass through many hosts to get to the user. Although the administrator of one host may enforce rigorous security policies, that administrator has no control over other hosts in the network. The user has to depend on the access control mechanism of all of these systems.

#### 1.2.1.5 Anonymity

An attacker can mount an attack from thousands of miles away and thus never have to touch the system attacked or come into contact with any of its administrators or users. The attack can be passed through many other hosts, in an effort to disguise from where the attack originated. Finally, computer-to-computer authentication is not the same as for humans to computers; secure distributed authentication requires thought and attention to detail.

#### 1.2.1.6 Unknown Path

There may be many paths from one host to another. Suppose that a user on one host wants to send a message to user on another host, that message might be routed through different hosts before arriving at destination host. Source host may provide acceptable security, but not intermediate nodes. Network users seldom have control over the routing of their messages.

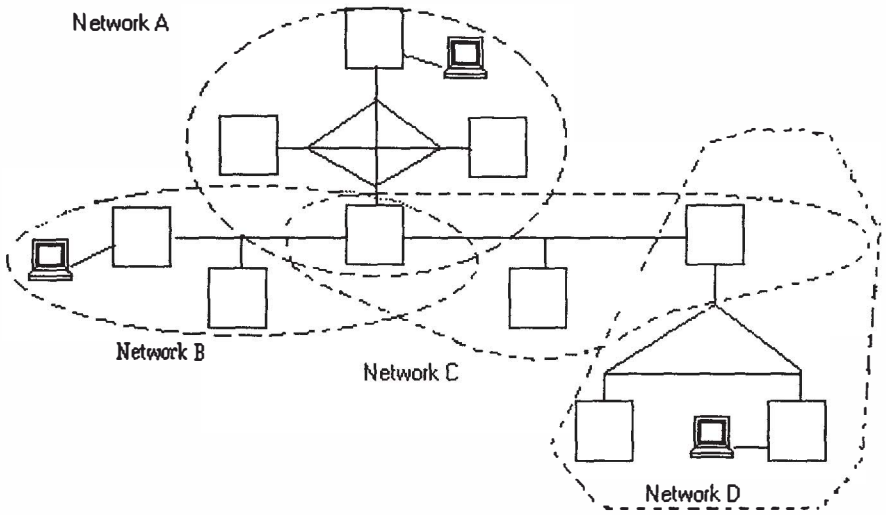


Figure 1.1: Unclear Network Boundaries

### 1.2.2 Security Threats

We looked at all the parts of a network; considered damage to confidentiality, integrity, and availability; and hypothesized the kinds of attack that could cause this damage.