

Enhanced Password-Based Authentication Protocol

This dissertation is submitted to
The Faculty of Computer Science and Information Technology
University of Malaya
In partial fulfillment of the requirements for
Master Degree of Computer Science

By
LEE CHEE KIAM

July 2000

Perpustakaan Universiti Malaya



A510474927

DECLARATION

I hereby declare that this dissertation submitted for the degree of Masters in the result of my own research, except where otherwise acknowledged. This dissertation is not substantially the same as any that I have submitted or am currently submitting for a degree or diploma or other qualification at any other university.

Signed: 

Lee Chee Kiam

Date: 12 July 2000

ACKNOWLEDGEMENT

Many individuals have contributed to this project either directly or indirectly. First and foremost, I would like to express my deepest appreciation to my project supervisor, Mr. Omar Zakaria, for his guidance, encouragement, advice and most important of all, his trust in my capabilities in developing E-PAP System.

For special mention, I would like to express my sincere gratitude to Dr. Mazliza binti Othman and Mr. Woo Chaw Seng for sparing their precious time to be my moderator.

To all my friends at University of Malaya, I offer my heartiest thanks for their help and support in my study.

Last, but not least, I wish to thank my beloved family and Miss Teh Suet Ching who have been considerate and supportive during the project.

TABLE OF CONTENTS

	page
DECLARATION	ii
ACKNOWLEDGEMENT	iii
TABLE OF CONTENTS.....	iv
LIST OF FIGURES	ix
LIST OF TABLES.....	xii
ABSTRACT.....	xiii
CHAPTER 1 INTRODUCTION	1
1.1 Problem Statement.....	1
1.2 Objectives	2
1.3 Scope of The Dissertation.....	3
1.4 Significance of The Research	3
1.5 Methodology	4
1.6 Report Organization.....	4
CHAPTER 2 LITERATURE SURVEY	7
2.1 Introduction.....	7
2.1 What is Authentication?.....	7
2.1.1 ISO 7498.....	8
2.1.2 ISO/IEC 9798	8
2.1.3 Authentication Protocol Model.....	9
2.1.4 Cryptographic Mechanisms	11
2.1.5 Freshness Mechanisms	14
2.2 Terminology and Background	16
2.2.1 The Players	16
2.2.2 Password and Verifier.....	16
2.2.3 Known Plaintext and Verifiable Text.....	17
2.2.4 Poorly Chosen and Well Chosen	18
2.2.5 Symmetric and Asymmetric Cryptography	18
2.2.6 Public Key Infrastructure (PKI).....	18
2.3 Security Threat.....	21
2.3.1 Active, Passive and Replay Attack	21

TABLE OF CONTENTS

2.3.2	Brute-force Attack	21
2.3.3	Dictionary Attacks	22
2.3.4	Classification of Attacker	22
2.4	Interactive Proof and Zero Knowledge.....	23
2.5	The Best Authentication System.....	24
2.6	Why password is used?.....	25
2.7	Disadvantages of using Smartcard.....	27
2.7.1	Equipment's Physical Limitations.....	27
2.7.2	Mobility Problem.....	28
2.7.3	Expensive.....	28
2.7.4	Slower Performance.....	28
2.7.5	Physical attacks.....	29
2.7.6	Advanced Attack Techniques	30
2.7.7	Key compromise	31
2.7.8	Risks of PKI.....	31
2.7.9	Misbehavior of Certificate Authorities	31
2.8	Disadvantages of using Biometric.....	34
2.8.1	Accuracy Problem.....	36
2.8.2	Cost.....	38
2.8.3	Integrity.....	39
2.8.4	Ease of Use Problem.....	40
2.8.5	Ease of Development Problem	40
CHAPTER 3	SYSTEM ANALYSIS	42
3.1	Performance Requirements.....	42
3.1.1	Provide Mutual Authentication.....	42
3.1.2	Prevent On-Line Dictionary and Brute-Force Attack.....	42
3.1.3	Prevent Off-Line Dictionary and Brute-Force Attack	42
3.1.4	Integrated Key Exchange.....	43
3.1.5	No Persistent Recorded Secret or Sensitive Host-Specific Data	43
3.1.6	Forward Secrecy	43
3.2	Obsolete Password Method	43
3.2.1	Clear password.....	44
3.2.2	Scrambled password	45

TABLE OF CONTENTS

3.2.3	Challenge/Hashed-Random Response (CHRAP).....	45
3.2.4	Kerberos Logon	46
3.2.5	S/Key	47
3.2.6	SecurID	48
3.2.7	Clear Password Over An SSL Signed Channel	49
3.3	Key-Exchange Algorithms	52
3.3.1	Diffie-Hellman.....	52
3.3.2	Station-to-Station Protocol	54
3.3.3	Encrypted Key Exchange (EKE).....	54
3.4	Simple Password-Authenticated Exponential Key Exchange	56
3.4.1	The Protocol.....	56
3.4.2	Why is SPEKE used?.....	58
CHAPTER 4	DESIGN AND IMPLEMENTATION	59
4.1	Introduction.....	59
4.2	Files Distribution	59
4.3	Basic Concept	60
4.4	E-PAP spekebn.dll Library	61
4.5	E-PAP spekekit.dll Library.....	62
4.6	E-PAP Server.....	65
4.6.1	Requirements	66
4.6.2	checkIP.....	67
4.6.3	processChangePw	67
4.6.4	doServerHandshake	68
4.6.5	processAuthenticatedRPC	69
4.6.6	processNewConnection	69
4.6.7	runServer.....	70
4.7	E-PAP Client.....	70
4.7.1	Requirements	71
4.7.2	changePw	72
4.7.3	detectBadPw	72
4.7.4	doClientHandshake.....	73
4.7.5	authenticatedRPC.....	74
4.7.6	doClient.....	75

TABLE OF CONTENTS

4.7.7	runClient	75
4.8	Procedure Sequence Flow Chart.....	76
4.9	E-PAP Server Implementation.....	84
4.10	E-PAP Client Implementation	85
CHAPTER 5	TESTING AND RESULTS.....	87
5.1	Purpose and Assumptions.....	87
5.1.1	Purpose.....	87
5.1.2	Assumptions.....	87
5.2	Participants and Venue	87
5.3	Procedures.....	88
5.4	Testing and Result	88
5.4.1	Phase I: Generating a Credential	89
5.4.2	Phase II: Starting E-PAP Server	89
5.4.3	Phase III: Starting E-PAP Client	90
5.4.4	Phase IV: Starting Authentication	93
5.4.5	Phase V: Changing Password	96
5.4.6	Phase VI: Other Tests	101
5.5	Discussion.....	102
5.5.1	Provide Mutual Authentication Without Revealing The Password..	102
5.5.2	Prevent Off-Line Dictionary Or Brute Force Attack.....	103
5.5.3	Prevent On-Line Dictionary And Brute-Force Attack.....	104
5.5.4	Integrated Key Exchange.....	104
5.5.5	No Persistent Recorded Secret Or Sensitive Host-Specific Data	104
5.5.6	Forward Secrecy	105
5.6	Strengths of E-PAP.....	105
5.6.1	Fulfill All Strong Authentication Requirements.....	105
5.6.2	Upgraded Existing Network Logon System	105
5.6.3	Multi-Factor Authentication	106
5.6.4	Numeric-Keypad-Only System.....	106
5.6.5	Diskless Workstations.....	106
5.6.6	Bootstrapping.....	106
5.7	Limitations of E-PAP.....	107
5.7.1	Operating System Integration Problem.....	107

TABLE OF CONTENTS

5.7.2 Single-threaded Server.....107

CHAPTER 6 EVALUATION AND CONCLUSION.....108

6.1 Achievements.....108

6.1.1 Theoretical Knowledge on Network.....108

6.1.2 Theoretical Knowledge on Network Security108

6.1.3 Theoretical Knowledge on Windows Socket.....109

6.1.4 Practical Knowledge.....110

6.2 Future Enhancement.....110

6.2.1 Multithreaded Server110

6.2.2 Internet Standard for E-PAP System110

6.3 Conclusion.....111

References.....112

Appendix A.....117

LIST OF FIGURES

	page
Figure 1-1: Overall Thesis Process	6
Figure 2-1: An authentication protocol model	10
Figure 2-2: Ali Baba's Cave [7].	24
Figure 2-3: Removing a smartcard plastic cover. [64].	29
Figure 2-4: Read-out attack modifications with a FIB workstation [64].	30
Figure 2-5: Forged Certificate [33].	32
Figure 2-6: Exchanged Message [33].	33
Figure 2-7: Register same user id and key in different domain [33].	33
Figure 2-8: Examples of different biometric characteristics [46].	35
Figure 2-9: Variability is inherent in all signal readings, whether from (a) signature, (b) face or (c) fingerprint [46].	37
Figure 2-10: Pass Rate of Biometric [62].	38
Figure 2-11: Cost versus accuracy [46].	39
Figure 2-12: Usable, marginal and unusable fingerprint [46].	40
Figure 3-1: Basic Authentication	44
Figure 3-2: SecurID	48
Figure 3-3: SSL icon for Netscape Communicator	50
Figure 3-4: An expired certificate for Internet Explorer 5	51
Figure 4-1: E-PAP System files distribution.	60
Figure 4-2: E-PAP Client	71
Figure 4-3: Change password module	77
Figure 4-4: Authentication module.	77
Figure 4-5: Change password procedure flow between E-PAP Server and Client	78
Figure 4-6: Detailed processChangePassword() and changePassword().	79

LIST OF FIGURES

Figure 4-7: Detailed detectBadPw() routine.	80
Figure 4-8: Authentication procedure flow between E-PAP Server and Client	81
Figure 4-9: Detailed handshake flow between Server and Client.	82
Figure 4-10: Detail Authenticated RPC flow between Server and Client	83
Figure 4-11: Windows restrict logon access.	85
Figure 4-12: Client for Microsoft Logon	85
Figure 4-13: Microsoft Family Logon	86
Figure 5-1: A message box alerted the user to provide a server name.	91
Figure 5-2: A message box alerted the user to provide a logon name.	92
Figure 5-3: A message box alerted the user to provide a port number.	92
Figure 5-4: A message box alerted the user to provide a port number between 49152 to 65535.	92
Figure 5-5: A message box alerted the user to provide correct server name or port number.	92
Figure 5-6: A message box alerted the user's logon name or password is wrong.	94
Figure 5-7: logxuser.txt file	94
Figure 5-8: logxpw.txt file	95
Figure 5-9: A message box notified the user is verified and enquire if the user want to send a message.	95
Figure 5-10: A dialog box for sending authenticated message.	95
Figure 5-11: A message box notified the message has been successfully sent and enquire the user want to send other message again.	96
Figure 5-12: A message box alerted the user that only a maximum of 3 messages is allowed.	96
Figure 5-13: A message box alerted the user to provide other new password.	100
Figure 5-14: A message box alerted the user to provide new password with minimum eight characters.	100
Figure 5-15: A message box alerted the user to re-input password.	100

LIST OF FIGURES

Figure 5-16: A message box alerted the user to choose an other password.	100
Figure 5-17: A message box alerted the user to choose an other password.	101
Figure 5-18: A message box alerted the user to choose an other password.	101
Figure 5-19: A message box notified user about password has been successfully changed.	101
Figure 5-20: A message notified user that he / she was blocked from server.	102

LIST OF TABLES

	Page
Table 2-1: Dramatis Personae	16
Table 2-2: Password search time with respect to the password and charset size [51].	26
Table 3-1: Notation for EKE protocol.	54
Table 3-2: Notation of SPEKE protocol	56
Table 4-1: Technical Specification for E-PAP System	59
Table 4-2: FreeSPEKE Routines	63
Table 4-3: Installation Requirement for E-PAP Server	66
Table 4-4: Installation Requirement for E-PAP Client	71
Table 5-1: IP address, host name and user.	88
Table 5-2: Logon name, password and credential (1)	103
Table 5-3: Logon name, password and credential (2)	103

ABSTRACT

This dissertation introduces Enhanced Password-Based Authentication Protocol (E-PAP) System. E-PAP System combines asymmetric (public-key) and symmetric (secret-key) cryptography that allow two parties sharing a small shared secret to provide authentication service, exchange confidential and authenticated information over an insecure network like Internet. E-PAP System also provides authentication service by using *something you know* concept. It has some advantages over biometric which uses *something you are* concept and smartcard that uses *something you have* concept, as it is free of equipment's physical limitations, accuracy and cost problem as well as other constraints. The core for E-PAP System is FreeSPEKE SDK, a free open source development's toolkit for Simple Password-Authenticated Exponential Key Exchange (SPEKE), which can prove knowledge of a small secret without revealing anything else about it by using zero-knowledge proof. E-PAP System has the properties that the password is protected against off-line "dictionary" and brute-force attacks that can crack hash-based challenge/response methods, such as Microsoft's LAN Manager for Windows NT4, Point-to-Point Protocol Challenge-Handshake Authentication Protocol (PPP CHAP), Kerberos version 5 for UNIX family platforms and Windows 2000, which have been the dominant forms of password protocol to date. E-PAP System was developed using Visual C++ version 6. It consists of E-PAP Client and E-PAP Server. E-PAP Server will handle all client authentications and process authenticated Remote Procedure Call (RPC). Two simple audit log files (E-PAP System Invalid Password Log and E-PAP System Invalid User Log) and a blocking IP file had been added to increase E-PAP Server performance and security. E-PAP Client is used to authenticate itself to E-PAP Server and to change user password. A bad password detector has been built to avoid bad-chosen password. The testing had been carried out in three sessions and the results could be used for future authentication protocol enhancement.