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

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

LIST OF FIGURES

LIST OF TABLES

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.