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.