CHAPTER 1 INTRODUCTION

1.1 Problem Statement

Authentication is the most important of the security services because all other security services, such as access control, confidentiality, integrity and non-repudiation, depend upon it. In order to achieve secure data communication, participants should be authenticated when setting up a communication session. How to authenticate participants is a critical problem of computer network security.

In many cases, people are typically authenticated by their passwords. Users tend to select password that can be easily guessed, and this lead to the choosen password being vulnerable to attacks due to copying of information and experimenting off-line. A common remedy to this risk is to encourage people to choose password that are obscure, thus difficult to guess. However, these passwords are likely difficult to remember and inconvenient to the users. Therefore, many authentication protocols have been developed to protect user password from guessing attacks. Many people belief that using smartcard and biometric to provide authentication may overcome the above problems. Nevertheless, in some scenarios, smartcard [1] and biometric [2] are not the security panacea that some people believe them to be.

The problem of how to prove and verify a password without revealing it is a longstanding open problem in cryptography. In recent years, researchers have developed a new class of methods (Simple Password-Authenticated Exponential Key Exchange (SPEKE) [39], Secure Remote Protocol (SRP) [19], Augmented Encrypted Key Exchange (AEKE) [15], Open Key Exchange (OKE) [60] and other variants) using secret public keys to achieve what was previously impossible. For example, using just a small password over an insecure network can:

- provide mutually authenticate,
- stop network attack,
- create a strong session key.
- prevent off-line dictionary attack,

- prevent on-line dictionary attack,
- integrated key exchange,
- user needs no persistent recorded secret data or sensitive host-specific data

These methods safely and directly verify a password, requiring

- no stored user keys and
- no public-key infrastructure (PKI) or certificates.

1.2 Objectives

All methods of authentication fall into three broad categories:

- Something the user is (voiceprint identification, retinal scanners)
- Something the user has (identity cards, smartcards)
- Something the user knows (PIN code, password, passphrase, or other secret knowledge)

This dissertation deals with a particularly important subset of the last category known as direct password authentication that combines techniques of zero-knowledge with asymmetric key exchange protocol.

The objectives of this dissertation are to:

1. survey any terminology and background regarding to authentication service,
2. determine possible attacks on authentication service,
3. investigate requirements for strong authentication protocol,
4. distinguish three main types of authentication methods, (something you have, you know and you are)
5. analyse vulnerabilities of authentication methods,
6. examine obsolete authentication protocols,
7. select appropriate authentication method that can provide strong authentication protocol,
8. develop an Enhanced Password-Based Authentication Protocol, and
9. provide a report on the above protocol.

1.3 Scope of The Dissertation

This dissertation focuses on providing an enhanced password-based authentication protocol for Windows family platform:

- Windows 95, 98, 98 SE
- Windows NT,
- Windows 2000

The main purpose for this dissertation is to provide an enhanced password-based authentication protocol that may be used to replace current authentication methods. The discussion regarding

- authentication service,
- other types of authentication methods,
- class of attacks, and
- obsolete authentication protocols

can be found in Chapter 2 and Chapter 3.

1.4 Significance of The Research

Enhanced Password-Based Authentication Protocol (E-PAP) in this dissertation is not only suitable to replace obsolete password methods which are discussed in Section 3.2, it also can be used for upgrading Kerberos authentication system, personal-computer remote banking and general computer logon over the Internet for E-Commerce. E-PAP can be used in systems where only a numeric keypad is available, such as cellular phones, phone-banking or set-top boxes. Other applications such as diskless workstations, bootstrapping, user-to-user authentication as well as multi-factor authentication also can exploit E-PAP for a more secure environment. For further detail about strengths of E-PAP, please refer to Section 5.6.

This dissertation will certainly offer great benefits to people who are in charge of organisations or corporates security. The target audiences of this dissertation are system administrators and operators of the system.

1.5 Methodology

The center of action taken in carrying out this dissertation is depicted in the Figure 1-1. The figure shows how this system was built up, started from Section 1.1 Problem Statement until the usability testing phase.

A survey regarding of authentication protocols standard from ISO-7498, authentication protocol model, cryptographic mechanisms and freshness mechanisms for authentication, as well as terminologies, background and class of attacks related to authentication service was carried put.

The three main categories of authentication methods were also analysed: something you have, something you are and something you know. The properties of strong authentication protocol also have been discussed in Section 3.1.

The third perspective is in analyzing some obsolete authentication protocols to understand their advantages. After that, this dissertation introduces an Enhanced Password-Based Authentication Protocol (E-PAP).

The final part in the Figure 1-1 is the implementation part whereby the coding and testing have been conducted.

1.6 Report Organization

This report is divided into six chapters. The following is a brief description of each chapter.

- Chapter 1 Introduction

  An overview of the project which includes problem statement, project objective, project scope and development strategy.
- Chapter 2 Literature Survey

  Explains details of the research required for the system development.
- Chapter 3 System Analysis

Describes the system analysis and requirements specifications of the system.

- Chapter 4 System Design and Implementation

  Highlights the implementation aspect of this dissertation, illustrates the development environment and coding process.

- Chapter 5 Testing and Results

  This chapter looks into the usability testing of the Enhanced Password-Based Authentication Protocol (E-PAP). The system's strength, weaknesses and analysis of finding vulnerabilities also has been carried out.

- Chapter 6 Evaluation and Conclusion

  Summarizes the entire development process through achievements, some opinions in expanding the research and finished with an overall conclusion.

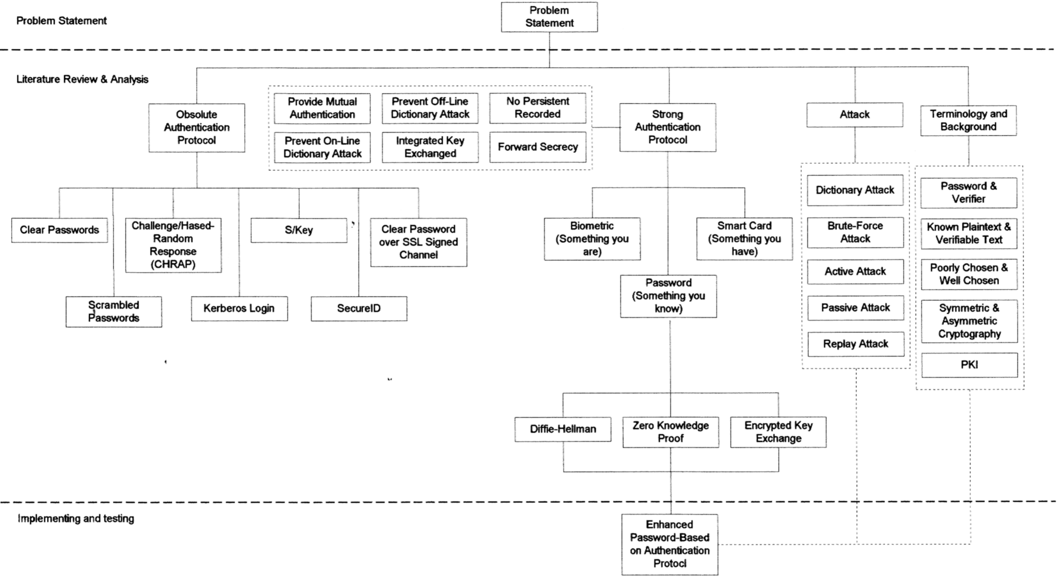
Problem Statement
Problem Statement
Literature Review & Analysis
Obsolute Authentication Protocol
Provide Mutual Authentication
Prevent Off-Line Dictionary Attack
No Persistent Recorded
Prevent On-Line Dictionary Attack
Integrated Key Exchanged
Forward Secrecy
Strong Authentication Protocol
Attack
Terminology and Background
Clear Passwords
Challenge/Hased-Random Response (CHRAP)
S/Key
Clear Password over SSL Signed Channel
Scrambled Passwords
Kerberos Login
SecureID
Biometric (Something you are)
Smart Card (Something you have)
Password (Something you know)
Dictionary Attack
Brute-Force Attack
Active Attack
Passive Attack
Replay Attack
Password & Verifier
Known Plaintext & Verifiable Text
Poorly Chosen & Well Chosen
Symmetric & Asymmetric Cryptography
PKI
Diffie-Hellman
Zero Knowledge Proof
Encrypted Key Exchange
Implementing and testing
Enhanced Password-Based on Authentication Protocl

Figure 1-1: Overall Thesis Process