Password Authentication Schemes: Current Status and Key Issues

Chwei-Shyong Tsai[1], Cheng-Chi Lee[2], and Min-Shiang Hwang[1]
(Corresponding author: Min-Shiang Hwang)

Department of Management Information Systems, National Chung Hsing University[1],
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C. (Email: mshwang@isrc.nchu.edu.tw)
Department of Computer & Communication Engineering, Asia University[2],
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.

(Invited Paper)

Abstract

Password authentication is one of the simplest and the most convenient authentication mechanisms to deal with secret data over insecure networks. It is more frequently required in areas such as computer networks, wireless networks, remote login systems, operation systems, and database management systems. In this paper, we shall present the result of our survey through all currently available password-authentication-related schemes and get them classified in terms of several crucial criteria. To be critical, most of the existing schemes are vulnerable to various attacks and fail to serve all the purposes an ideal password authentication scheme should. In order to see how different password authentication schemes compare in different situations, we define all possible attacks and goals that an ideal password authentication scheme should withstand and achieve. We should hope that the attacks and goals we offer here can also help future researchers develop better schemes.

Keywords: Cryptography, ElGamal, one-way hash function, password authentication, RSA

1 Introduction

To access resources at remote systems, users should have proper access rights. One of the simplest and most convenient security mechanisms is the use of a password authentication scheme. Examples of password authentication applications include remote login systems, ATM, PDA, and database management systems, etc. To access these resources, each user should have an identifier (ID) and a password (PW). The ID and PW are maintained by the remote system. When a user wants to login to a remote server, he/she has to submit his/her ID and PW to the server. On receiving the login message, the remote server checks to see if it can identify the login message in the password (verification) table. The password table, also maintained by the remote system, covers all users' IDs and PWs. If the submitted ID and PW match the corresponding pair stored in the server's password table, the user will be granted to access the server.

Two problems are found in this traditional mechanism. One is that the revelation of the passwords can be seen by the administrator of the server because the password table is in plain-text format. The other problem is that an intruder can impersonate a legal user by stealing the user's ID and PW from the password table. To make things worse, the current Internet is vulnerable to various attacks such as denial of service attacks, forgery attacks, forward secrecy, server spoofing attacks, parallel session attacks, password guessing attacks, replay attacks, smart card loss attacks, and stolen-verifier attacks. These attacks will be defined and discussed in detail in Section 1.2.

1.1 Previous Researches

Hashed or encrypted passwords can solve the above two problems [14, 37]. That is why Lamport proposed his one-time password with one-way hash function against replay attacks [28]. However, Lamport's scheme has the three drawbacks as follows [31]: 1) it has high hash overhead. 2) it requires password resetting. 3) a password (verification) table should be stored on the server's side. Researchers later have aimed to mend the three drawbacks. To prevent the password table from being stolen or modified by attackers, solutions have been proposed where the password table is no longer required to be kept by the server [10, 18, 24]. To solve drawbacks 1 and 2 of Lamport's scheme, Shimizu proposed the so-called CINON protocol [43]. Later, Shimizu et al. proposed their PERM protocol [44] to solve the random number memorizing problem of the CINON protocol.

Inspired by Lamport's method, Haller developed the famous S/KEY one-time password for an Internet draft RFC 1760 [16, 17]. However, some researchers have pointed out that the security of the S/KEY scheme can be broken by replay attacks, server spoofing attacks, and password guessing attacks [35, 53, 54]. Sandirigama et al. and Lin et al. proposed the SAS [40] and OSPA protocol [33], respectively, which turn out superior to Lamport's protocol, the CINON protocol, and the PERM protocol, in terms of storage utilization, computing time, and transmission overhead. However, Chen and Ku later proved that the SAS and OSPA protocol can be broken by two stolen-verifier attacks [7].

Recently, quite a number of password authentication schemes with smart cards have been proposed [1, 2, 5, 6, 9, 10, 11, 15, 21, 22, 23, 24, 27, 29, 31, 32, 41, 42, 46, 47, 48, 51, 52, 55]. These smart-card-related schemes, exclusive of those in [5, 6, 24, 48, 49] which are based on cryptography, are classified into three types as follows.

RSA-based Password Authentication Schemes
Yang and Shieh [52] proposed two password authentication schemes with smart cards. The two schemes are based on RSA public key cryptosystem [39]. They do not store passwords or verification tables in the server, and let users freely change their own passwords. However, some papers [3, 15, 42, 45] pointed out that Yang and Shieh's schemes have a drawback in that an intruder is able to impersonate a legal user by constructing a valid login request out of an intercepted login request. In other words, Yang and Shieh's schemes are vulnerable to forgery attacks. Fan et al. [15] proposed a simple improved scheme to remedy the damage done by forgery attacks. The improved scheme puts a strict limit on the ID. In the authentication phase, the remote system will check the ID's form. However, Chen et al. [8] and Wang et al. [47] showed that Fan et al.'s scheme cannot seem to withstand forgery attacks either.

Shen et al. [42] also proposed an enhancement of the Yang-Shieh scheme. The proposed scheme can withstand forgery attacks and provide mutual authentication to withstand server spoofing attacks. However, Yang et al. [50] pointed out that Shen et al.'s scheme is still vulnerable to forgery attacks. Sun et al. [45] pointed out that the cryptanalysis in [3] was unreasonable and proposed their forgery attacks on the Yang-Shieh scheme. To resist Sun et al.'s attack, Yang et al. [51] proposed an improvement of the Yang-Shieh scheme.

ElGamal-based Password Authentication Schemes
Hwang and Li [23] proposed a ElGamal-based remote user authentication scheme using smart cards. This scheme is based on ElGamal's public key cryptosystem [13]. The Hwang-Li scheme does not need a password table to check the validity of the login request. Additionally, it can withstand replay attacks. However, some papers [1, 2, 4, 41] showed that the Hwang-Li scheme cannot withstand forgery attacks. Shen et al. [41] and Awasthi et al. [1] proposed an improved scheme to fight against forgery attacks. Besides, Awasthi et al.'s scheme can achieve forward secrecy, ensuring that the previously generated user's passwords are secure even if the system's secret key is stolen or has been revealed in public by accident. In the same year, Leung et al. [30] also showed that Shen et al.'s [41] scheme cannot withstand forgery attacks. Later, Kumar [27] proposed a new remote user authentication scheme using smart cards. This scheme is a modified form of Shen et al.'s scheme [41] and uses one more function C_K to generate the check digit for each registered identity.

Hash-based Password Authentication Schemes
Recently, lots of password authentication schemes based on one-way hash function have been proposed because the computation cost is lower than those of RSA-based and ElGamal-based password authentication schemes. Sun [46] proposed an efficient and practical remote user authentication scheme. No password table is required to keep in his system and therefore the communication and computation costs are reduced. However, this scheme does not allow users to choose or change their passwords freely and cannot achieve mutual authentication [11]. Hwang et al. [22] and Chien et al. [11] respectively proposed their simple remote user authentication schemes. In those schemes, the authors claimed that their schemes could achieve the following goals: no verification or password table required on the server's side; low communication cost and the computation cost, the replay attack problem completely solved, and users' freedom to choose their passwords. However, the scheme in [22] cannot achieve mutual authentication, and the scheme in [11] cannot let users freely change their passwords. Furthermore, Yoon et al. [55] pointed out that the [22] scheme is insecure if the secret key of the server leaks out or is stolen. And Hsu [19, 20] showed that the [11] scheme is vulnerable to the parallel session attack. Later, Lee et al. [29] proposed an improved efficient scheme to remedy the parallel session attack problem.

Chen et al. [9] proposed two secure SAS-like password authentication schemes with lower storage, processing, and transmission overheads. The two schemes can withstand the stolen-verifier attack on SAS and OSPA prtocol. Nowadays, all password authentication schemes are based on the static login ID, which, however, can have partial information about the user's login message leaked out. Hence, Das et al. [12] proposed a dynamic ID-based remote user authentication scheme with smart cards. However, their scheme has some security flaws shown in [32]. Hence, Liao et al. [32] proposed an improved scheme to remedy these security flaws. Later, Liao et al. [31] further proposed a new scheme to achieve all of their proposed requirements. This scheme can agree on a session key to encrypt/decrypt the communicated messages using the symmetric cryptosystem.

Although so many schemes have been proposed to

authenticate a legitimate user, none of them can solve all possible problems and withstand all possible attacks. Now we define all the security requirements and all the goals an ideal password authentication scheme should satisfy and achieve.

1.2 Security Requirements and Definitions

In this section, we define the security requirements an ideal password authentication scheme should satisfy. In addition, we shall also introduce all of the attacks that an ideal password authentication scheme should withstand. We sort them as follows:

SR1. *Denial of Service Attacks*
An attacker can update false verification information of a legal user for the next login phase. Afterwards, the legal user will not be able to login successfully anymore.

SR2. *Forgery Attacks (Impersonation Attacks)*
An attacker attempts to modify intercepted communications to masquerade the legal user and login to the system.

SR3. *Forward Secrecy*
It ensures that the previously generated passwords in the system are secure even if the system's secret key has been revealed in public by accident or is stolen.

SR4. *Mutual Authentication*
The user and the server can authenticate each other. Not only can the server verify the legal users, but the users can also verify the legal server. Mutual authentication can help withstand the *server spoofing attack* where an attacker pretends to be the server to manipulate sensitive data of the legal users.

SR5. *Parallel Session Attacks*
Without knowing a user's password, an attacker can masquerade as the legal user by creating a valid login message out of some eavesdropped communication between the user and the server.

SR6. *Password Guessing Attacks*
Most passwords have such low entropy that it is vulnerable to password guessing attacks, where an attacker intercepts authentication messages and stores them locally and then attempts to use a guessed password to verifies the correctness of his/her guess using theses authentication messages.

SR7. *Replay Attacks*
Having intercepted previous communications, an attacker can impersonate the legal user to login to the system. The attacker can replay the intercepted messages.

SR8. *Smart Card Loss Attacks*
When the smart card is lost or stolen, unauthorized users can easily change the password of the smart card, or can guess the password of the user by using password guessing attacks, or can impersonate the user to login to the system.

SR9. *Stolen-verifier Attacks*
An attacker who steals the password-verifier (e.g., hashed passwords) from the server can use the stolen-verifier to impersonate a legal user to login to the system.

1.3 An Ideal Password Authentication Scheme

An ideal password authentication scheme should withstand all of the above attacks. Besides, it should achieve the following goals:

G1. The passwords or verification tables are not stored in the system.

G2. The passwords can be chosen and changed freely by the users.

G3. The passwords cannot be revealed by the administrator of the server.

G4. The passwords are not transmitted in plain text over the network.

G5. The length of a password must be appropriate for memorization.

G6. The scheme must be efficient and practical.

G7. Any unauthorized login can be quickly detected when a user inputs a wrong password.

G8. A session key is established during the password authentication process to provide confidentiality of communication.

G9. The ID should be dynamically changed for each login session to avoid partial information leakage about the user's login message.

G10. The proposed scheme is still secure even if the secret key of the server is leaked out or stolen.

To be called ideal, a password authentication scheme should be able to withstand all of the above attacks and achieve all of the above goals. Unfortunately, none of the existing password authentication schemes can. Comparisons among some important schemes are given in Section 4.

1.4 Organization

The remainder of this paper is organized as follows. In Section 2, we introduce the related theories, such as the RSA scheme, the ElGamal scheme, and the one-way hash function. In Section 3, we classify password authentication schemes into three types, which are RSA-based,

ElGamal-based, and Hash-based schemes. In Section 4, we shall compare schemes in terms of security requirements, goals, and performance. Finally, in Sections 5 and 6, we shall determine our future research directions and make some concluding remarks, respectively.

2 Related Theories

In general, password authentication schemes run on some basic concepts such as RSA [39], ElGamal [13], and one-way hash function [36, 38]. Let's check out these basic concepts as follows.

2.1 RSA Scheme

RSA public-key cryptosystem was proposed by Rivest, Shamir, and Adleman in 1978. The RSA scheme can be used on both digital signature and encryption schemes. Its security is based on the difficulty of factoring large numbers. A digital signature scheme based on RSA runs as follows: suppose p and q are two large primes. Compute $n = p \times q$ and choose e and d such that $e \times d \bmod (p-1)(q-1) \equiv 1$. Each user has a key pair, which includes a private key and a public key. Suppose d denotes the user's private key, and (e, n) denotes the user's public key. When Alice wants to sign a message M and sends it and its digital signature to Bob, Bob can verify whether the signed message was really signed by Alice as follows:

Sign:

1) Alice computes $s = M^d \bmod n$, where d is Alice's private key.
2) The value s is Alice's signature on M. Then Alice sends Bob (M, s).

Verify:
When Bob receives theses messages from Alice, he can verify whether s is Alice's signature on M by checking $s^e =? M \bmod n$, where e is Alice's public key.

2.2 ElGamal Scheme

ElGamal public-key cryptosystem is proposed by ElGamal in 1985. The ElGamal scheme can also be used to create both digital signature and encryption schemes. The security is based on the difficulty of calculating discrete logarithms in a finite field. ElGamal's digital signature schemes go as follows. For this scheme to work, each user has a key pair, which includes a private key and a public key. Firstly, choose a prime p and two random numbers, g and x, such that the two numbers are smaller than p. Here, x denotes user's private key, and y, g, and p denote user's public key, where $y = g^x \bmod p$. When Alice wants to sign a message M and send it and its digital signature to Bob, Bob can verify whether the signed message was really signed by Alice. The processes is as follows:

Sign:

1) Alice selects a random number $k \in Z_{p-1}$.
2) Alice calculates $r = g^k \bmod p$.
3) Alice solves the equation $M = xr + ks \bmod (p-1)$ and gets s, where x is Alice's private key.
4) The pair (r, s) is Alice's signature on M. Then Alice sends Bob (M, r, s).

Verify:
When Bob receives theses messages from Alice, he can verify whether (r, s) is Alice's signature on M using the following equation:

$$\begin{aligned} g^M &= g^{xr+ks \bmod (p-1)} \bmod p, \\ &= g^{xr} g^{ks} \bmod p, \\ &= y^r r^s \bmod p, \end{aligned} \quad (1)$$

where y is Alice's public key.

2.3 One-Way Hash Function Scheme

A one-way hash function $h : x \to y$ is a function $y = h(x)$ which takes an arbitrary-length message x as the input and returns a fixed-length hash value y. One-way hash functions have the following properties that make them one-way:

- Given x, it is easy to compute $h(x) = y$. However, given y, it is hard to compute $h^{-1}(y) = x$.
- Given x, it is computationally infeasible to find x' such that $x' \neq x$ but $h(x') = h(x)$.
- It is computationally infeasible to find any pair x and x' such that $x' \neq x$ but $h(x') = h(x)$.

Hash functions are aimed at high-speed software implementations and are currently widely used. In recent years, to strengthen the efficiency of cryptosystems, more and more cryptosystems have been constructed in a way the one-way hash function can be used to develop them.

3 Related Works

In this section, we review three types password authentication schemes, which are RSA-based, ElGamal-based, and hash-based password authentication schemes. Several important representative schemes will be reviewed for each type of password authentication scheme. First, some notations that will be used throughout this paper are defined in Table 1.

Each type of password authentication scheme is composed of three phases, including the registration phase, login phase, and authentication phase. In the registration phase, the user U sends a request registration to the

remote server. Then the server issues a smart card and a password to U through a secure channel. In the login phase, when U wants to login to S for using resources of S, he/she inserts his/her smart card to a terminal and keys in his/her identity ID and password PW to access services. In the authentication phase, S verifies the validity of the login request. Now, we review the three types of password authentication schemes below.

3.1 RSA-based Password Authentication Schemes

3.1.1 Yang-Shieh Scheme [52]

Yang and Shieh proposed two password authentication schemes with smart cards. One is a timestamp-based scheme, and the other is a nonce-based scheme. Here, we shall introduce the firs scheme. This scheme consists of three phases as follows:

Registration Phase
A Key Information Center(KIC) is necessary to issue a smart card to U. U submits his/her ID and a chosen PW to KIC. Then KIC performs the following steps:

1) Generate an RSA key pair, namely a private key d and a public key (e, n). KIC publishes (e, n) and keeps d privately.
2) Find an integer g, which is a primitive in both GF(p) and GF(q).
3) Calculate the user's secret information W as $W = ID^d \bmod n$.
4) Generate the smart card's identifier CID of U and compute V by $V = g^{PW \times d} \bmod n$.
5) Write n, e, g, ID, CID, W, V to the memory of the smart card and issue the card to U.

Login Phase
When U wants to login to S, he/she has to insert his/her smart card into a card reader and enters ID and PW. The smart card will perform the following steps:

1) Generate a random number r and calculate $X = g^{r \times PW} \bmod n$, and $Y = W \times V^{r \times h(CID,T)} \bmod n$.
2) Send the login request messages (ID, CID, X, Y, n, e, g, T) to S.

Authentication Phase
Upon receipt of the login request messages, S performs the following steps:

1) Check whether ID is a valid user identity and CID is a legal smart card identity.
2) Check whether T is a valid of timestamp.
3) Check whether the equation $Y^e = ID \times X^{h(CID \times T)} \bmod n$ holds.

If one of the above check results is no, the login request is rejected; otherwise, the login request is accepted.

Furthermore, the Yang-Shieh scheme allows users to freely change their passwords. A user can submit his/her smart card and a new PW' to KIC over a secure channel. KIC replaces V with $V' = g^{PW' \times d} \bmod n$ and sends the card to the user.

3.1.2 Fan-Li-Zhu Scheme [15]

The scheme is all the same as the Yang-Shieh Scheme except that this scheme put a strict limit on the ID.

3.1.3 Yang-Wang-Chang Scheme [51]

Registration Phase
This phase also needs a Key Information Center(KIC) to issue a smart card to U. U submits his/her ID and a chosen PW to KIC. Then KIC performs the registration steps. The only different steps with the Yang-Shieh scheme in this phase are Steps 3 and 4 as follows.

Step 3. Generate the smart card's identifier CID of U and calculate the user's secret information W as $W = ID^{CID \times d} \bmod n$.

Step 4. Compute V by $V = g^{PW \times d} \bmod n$.

Login Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1) Generate a random number r and calculate $X = g^{PW \times r} \bmod n$, and $Y = W \times V^{r \times T} \bmod n$.
2) Send the login request messages (ID, CID, X, Y, n, e, g, T) to S.

Authentication Phase
Upon receipt of the login request messages, S performs the following steps:

1) Check whether ID is a valid user identity and CID is a legal smart card identity.
2) Check whether T is a valid of timestamp.
3) Check whether the equation $Y^e = ID^{CID} \times X^T \bmod n$ holds.

If one of the above check results is no, the login request is rejected; otherwise, the login request is accepted.

3.2 ElGamal-based Password Authentication Schemes

3.2.1 Hwang-Li Scheme [23]

Registration Phase
U submits his/her ID to S for registration. S computes a password PW for the user as $PW = ID^x \bmod p$. S issues a smart card, which contains public parameters

Table 1: Notations

U	the user
S	the remote system
ID	the user's identity
PW	the password of U
$h(\cdot)$	a one-way hash function
$Red(\cdot)$	a shadowed identity of the device which is only possessed by the S
$C_K(\cdot)$	a function to generate the check digit for the registered identity, which is only possessed by the S
$\bigoplus$	XOR operation
x	the long secret key of S
y	S's secret number stored in each user's smart card
$\|\|$	Concatenation
p, q	large prime numbers
g	the primitive element in Galois field GF(p)
T, T'	time-stamps
T_{RT}	the user's registered timestamp
N, N'	nonce
r, r', a, w	random numbers

$(h(), p)$, and delivers PW to U through a secure channel.

Login Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1) Generate a random number r and calculate $C_1 = ID^r \bmod p$.

2) Compute $t = h(T \oplus PW) \bmod (p-1)$.

3) Compute $M = ID^t \bmod p$.

4) Compute $C_2 = M(PW)^r \bmod p$.

5) Send the login request messages (ID, C_1, C_2, T) to S.

Authentication Phase
Upon receipt of the login request messages, S performs the following steps:

1) Check whether ID is a valid user identity.

2) Check whether T is a valid timestamp.

3) Compute $PW = ID^x \bmod p$ and $t = h(T \oplus PW) \bmod (p-1)$.

4) Check whether the equation $C_2(C_1^x)^{-1} \bmod p = ID^t \bmod p$ holds.

If one of the above check results is no, the login request is rejected; otherwise, the login request is accepted.

3.2.2 Awasthi-Lal Scheme [1]

The scheme can provide forward secrecy which ensures the previously passwords in the system are secure even if the secret key of the system is stolen. This scheme is similar to the Hwang-Li scheme. The only different phase is the registration phase, which we briefly introduce as follows.

Registration Phase
U submits his/her ID to S for registration. S computes $m = h(ID \oplus T_{RT})$, and $PW = m^x \bmod p$, where T_{RT} is the user's registered timestamp. S issues a smart card which contains public parameters $(h(), p, T_{RT})$, and delivers PW to U through a secure channel.

Our New Attack
Awasthi and Lal pointed out that previous passwords in the system are secure even if x is public. When an attacker wants to obtain some previous password, he/she has to compute $PW = [h(ID \oplus T_{RT})]^x \bmod p$, where T_{RT} is a postdated timestamp that prevents him/her from computing PW. However, this scheme cannot provide forward secrecy if a smart card is lost or stolen. An attacker can derive T_{RT} from the smart card and then compute $PW = [h(ID \oplus T_{RT})]^x \bmod p$ if he/she also has x. Hence, all the previous passwords may be known to the attacker.

3.2.3 Kumar's Scheme [27]

Registration Phase
U submits his/her identity string J, which consists the name and a unique identification number of U, to S for registration. S computes $S_{ID} = Red(J), C_{ID} =$

$C_K(S_{ID})$, and $PW = (S_{ID})^x \bmod p$. S issues a smart card, which contains public parameters $(h(), p)$, and delivers $(S_{ID} \parallel C_{ID}, PW)$ to U through a secure channel.

Login Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in $S_{ID} \parallel C_{ID}$ and PW. The smart card will perform the following steps:

1) Generate a random number r and calculate $C_1 = (S_{ID})^r \bmod p$.
2) Compute $t = h(T \oplus PW) \bmod (p-1)$.
3) Compute $m = (S_{ID})^t \bmod p$.
4) Compute $C_2 = m(PW)^r \bmod p$.
5) Send the login request messages $(S_{ID} \parallel C_{ID}, C_1, C_2, T)$ to S.

Authentication Phase
Upon receipt of the login request messages, S performs the following steps:

1) Check whether S_{ID} is in the specific format.
2) Check whether the equation $C_{ID} = C_K(S_{ID})$ holds.
3) Check whether T is a valid timestamp.
4) Compute $PW = (S_{ID})^x \bmod p$ and $t = h(T \oplus PW) \bmod (p-1)$.
5) Check whether the equation $C_2 = (C_1^x)(S_{ID})^t \bmod p$ holds.

If one of the above check results is no, the login request is rejected; otherwise, the login request is accepted.

3.3 Hash-based Password Authentication Schemes

Due to their efficiency and one-way property, one-way hash functions have been used as the basis on which more and more cryptosystems including password authentication systems are developed. Recently, lots of password authentication schemes based on one-way hash function have been proposed because the computation cost is lower than those of RSA-based and ElGamal-based password authentication schemes.

3.3.1 Sun's Scheme [46]

Registration Phase
U submits his/her identity ID to S for registration. S computes a password $PW = h(ID, x)$. S issues a smart card, which contains public parameter $h(\cdot)$, and delivers PW to U through a secure channel.

Login Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1) Compute $C_1 = h(T \oplus PW)$.
2) Send the login request messages (ID, C_1, T) to S.

Authentication Phase
Upon receipt of the login request messages, S performs the following steps:

1) Check whether ID is the specific format.
2) Check whether T is a valid timestamp.
3) Compute $PW = h(ID, x)$ and $C_1' = h(T \oplus PW)$.
4) Check whether the equation $C_1 = C_1'$ holds.

If one of the above check results is no, the login request is rejected; otherwise, the login request is accepted.

3.3.2 Hwang-Lee-Tang Scheme [22]

Registration Phase
U chooses a PW freely and then computes $h(PW)$. U submits his/her identity ID and $h(PW)$ to S for registration over a secure channel. S computes $A = h(ID \oplus x) \oplus h(PW)$. S issues a smart card, which contains $(ID, A, h(\cdot))$, to U through a secure channel.

Login Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1) Compute $B = A \oplus h(PW)$ and $C_1 = h(B \oplus T)$.
2) Send the login request messages (ID, C_1, T) to S.

Authentication Phase
Upon receipt of the login request messages, S performs the following steps:

1) Check whether ID is the specific format.
2) Check whether T is a valid timestamp.
3) Compute $B' = h(ID \oplus x)$ and $C_1' = h(B' \oplus T)$.
4) Check whether the equation $C_1 = C_1'$ holds.

If one of the above check result is no, the login request is rejected; otherwise, the login request is accepted.

Furthermore, the Hwang-Lee-Tang scheme allows users to freely change their passwords. A user can insert his/her smart card and key in a new PW'. The smart card will compute $B = A \oplus h(PW) = h(ID \oplus x), h(PW')$, and $A' = B \oplus h(PW')$. Then the smart card replaces A with A'.

3.3.3 Chien-Jan-Tseng Scheme [11]

Registration Phase
U chooses a PW freely and submits his/her identity ID and PW to S for registration over a secure channel. S computes $R = h(ID \oplus x) \oplus PW$. S issues a smart card which contains $(R, h(\cdot))$ to U through a secure channel.

Login Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1) Compute $C_1 = R \oplus PW$ and $C_2 = h(C_1 \oplus T)$.
2) Send the login request messages (ID, C_2, T) to S.

Authentication Phase
Upon receipt of the login request messages, S performs the following steps:

1) Check whether ID is the specific format.
2) Check whether T is a valid timestamp.
3) Compute $C_1' = h(ID \oplus x)$.
4) Check whether the equation $C_2 = h(C_1' \oplus T)$ holds.

If one of the above check results is no, the login request is rejected; otherwise, the login request is accepted. Furthermore, the user can authenticate the system. S should compute $C_3 = h(C_1' \oplus T')$, where T' is the current timestamp. And then S sends back the message (T', C_3). Upon receiving the message, U can verify the system as follows:

1) Check whether T' is a valid timestamp.
2) Check whether the equation $C_3 = h(C_1 \oplus T')$ holds.

If the above checks turn out positive, U believes that S is a legal system and the mutual authentication is done; otherwise, U disconnects the connection.

3.3.4 Chen-Lee-Horng Scheme [9]

Registration Phase
U chooses a PW freely and computes $h^2(PW \oplus N)$. Then U submits his/her identity ID, $h^2(PW \oplus N)$, and N to S for registration over a secure channel. S stores $h^2(PW \oplus N)$ into the verification table. S computes $h(x \parallel ID)$ and issues a smart card which contains $(N, h(x \parallel ID))$ to U through a secure channel.

Login Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The login steps are as follows:

1) U sends ID and r' to S.
2) S checks the format of ID, and returns $r \oplus h(x \parallel ID)$ and $h(r \parallel r')$.
3) Upon receiving $r \oplus h(x \parallel ID)$ and $h(r \parallel r')$, U can extract r from $r \oplus h(x \parallel ID)$. Then, with r, U verifies whether $h(r \parallel r')$ contains r' in order to authenticate S.
4) With r, the smart card can compute $c_1 = h(PW \oplus N) \oplus h(h^2(PW \oplus N) \oplus r)$, $c_2 = h^2(PW \oplus N') \oplus h(PW \oplus N)$, and $c_3 = h^3(PW \oplus N')$.
5) U sends the login request messages (c_1, c_2, c_3) to S.

Authentication Phase
Upon receipt of the login request messages, S performs the following steps:

1) With r and $h^2(PW \oplus N)$, S can extract $h(PW \oplus N)$ from c_1.
2) Using $h(PW \oplus N)$, S can extract $h^2(PW \oplus N')$ from c_2.
3) Check whether the hash value of the extracted $h(PW \oplus N)$ is equal to that of the stored $h^2(PW \oplus N)$. If yes, this login request is accepted; otherwise, it is rejected.
4) Check whether the hash value of the extracted $h^2(PW \oplus N')$ is equal to the received c_3. If it is, S updates the verification table by replacing $h^2(PW \oplus N)$ with $h^2(PW \oplus N')$.

3.3.5 Liao-Lee-Hwang Scheme [32]

All the above schemes are based on static login identity. To make a difference, Liao, Lee, and Hwang proposed a dynamic ID-based remote user authentication scheme. The scheme is divided into three phases as follows: registration, authentication, and password change phase.

Registration Phase
U chooses a PW freely and computes $h(PW)$. Then U submits his/her identity ID and $h(PW)$ to S for registration over a secure channel. S computes $L = h(PW) \oplus h(x \parallel ID)$ and issues a smart card which contains $(L, y, h(\cdot))$ to U through a secure channel.

Authentication Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The steps to take are as follows:

1) The smart card computes a dynamic ID as $CID = h(PW) \oplus h(L \oplus y \oplus T)$, $B = h(CID \oplus h(PW))$, and $C = h(T \oplus L \oplus B \oplus y)$.
2) U sends the login request messages (CID, L, C, T) to S.
3) S checks whether T is a valid timestamp.
4) S computes $h(PW) = CID \oplus h(L \oplus y \oplus T)$, and $B = h(CID \oplus h(PW))$.

5) S checks whether the equation $C = h(T \oplus L \oplus B \oplus y)$ holds. If it holds, S accepts U's login request; otherwise, S rejects it.

6) S computes $D = h(T' \oplus L \oplus B \oplus y)$ and sends (D, T') to U.

7) Upon receiving (D, T'), U can check whether T' is a valid timestamp and compute $h(T' \oplus L \oplus B \oplus y)$. Then, U compares it with the received D. If positive, S is authenticated by U.

Password Change Phase
This scheme allows users to freely change their passwords. A user can insert his/her smart card and key in a new PW'. The smart card will compute $L' = L \oplus h(PW) \oplus h(PW')$. Then the smart card replaces L with L'.

3.3.6 Yoon-Ryu-Yoo Scheme [55]

Registration Phase
U chooses a PW freely and submits his/her identity ID and PW to S for registration over a secure channel. S computes $V = h(ID, T_{RT}, x)$ and $A = h(ID, T_{RT}, x) \oplus PW$. S issues a smart card which contains $(ID, V, A, h())$ to U through a secure channel.

Login Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card will perform the following steps:

1) Compute $B = A \oplus PW$ and verify whether B is equal to the stored V. If yes, compute $C_1 = h(B \oplus T)$.

2) Send the login request messages (ID, C_1, T) to S.

Authentication Phase
Upon receipt of the login request messages, S and the smart card perform the following steps for mutual authentication between U and S.

1) S checks whether ID is in the specific format.

2) S checks whether T is a valid timestamp.

3) S computes $B' = h(ID, T_{RT}, x)$ and $C_1' = h(B', T)$. S compares C_1 with C_1'. If they are identical, S accepts the login request; otherwise, S rejects it.

4) S computes $C_2 = h(B', C_1', T')$ and sends back the message (C_2, T').

5) Upon receiving (C_2, T'), U checks whether T' is a valid timestamp. Then, U computes $C_2' = h(B, C_1, T')$ and compares it with the received C_2. If they are identical, U believes that the responding part is the real system.

If one of the above check results is no, the login request is rejected; otherwise the login request is accepted.

Furthermore, the Yoon-Ryu-Yoo scheme allows users to freely change their passwords. A user can insert his/her smart card and key in a new PW'. The smart card will compute $B = A \oplus PW = h(ID, T_{RT}, x)$, and compare B with the stored V. If they are equal, it computes $A' = B \oplus PW'$. Then the smart card replaces A with A'.

3.3.7 Lee-Kim-Yoo Scheme [29]

The registration phase and login phase are the same as those of the Chien-Jan-Tseng scheme. The only difference between this scheme and the Chien-Jan-Tseng scheme is in the authentication phase as follows:

Authentication Phase
The only difference between this phase of this scheme and this phase of the Chien-Jan-Tseng scheme is in C_3. S computes $C_3 = h(h(C_1' \oplus T'))$, which is different from $C_3 = h(C_1' \oplus T')$ of the Chien-Jan-Tseng scheme. And S sends back the message (T', C_3). Upon receiving the message, U can verify the system as follows:

1) Check whether T' is a valid timestamp.

2) Check whether the equation $C_3 = h(h(C_1 \oplus T'))$ holds.

If the above checks turn out positive, U believes that S is the legal system and the mutual authentication is done; otherwise, U disconnects the connection.

Furthermore, the Lee-Kim-Yoo scheme allows users to freely change their passwords. A user can insert his/her smart card and key in a new PW'. The smart card will compute $R' = R \oplus PW \oplus PW'$. Then the smart card replaces R with R'.

3.3.8 Liao et al.'s Scheme [31]

Registration Phase
U chooses a PW freely and then computes $h(PW)$. U submits his/her identity ID and $h(PW)$ to S for registration over a secure channel. S computes $B = g^{h(x \| ID) + h(PW)} \bmod p$. S issues a smart card which contains $(ID, B, p, g, h())$ to U through a secure channel.

Login Phase
When U wants to login to S, he/she inserts his/her smart card into a card reader and keys in ID and PW. The smart card and S will perform the following steps:

1) U sends ID to S to login to the system.

2) After receiving the login ID, S computes $B" = g^{h(x \| ID) r} \bmod p$. Then S computes $h(B")$ and sends back the message $(h(B"), r)$ to U.

3) Upon receiving $(h(B"), r)$, U computes $B' = (Bg^{-h(PW)})^r \bmod p$. Then U can verify the validity of S by checking whether the received $h(B")$ is equal to the hashed B'. If it is, U computes $C = h(T \| B')$; otherwise, S is rejected. To prevent attackers from replaying $(h(B"), r)$ and break the system, in point 8 of Section 2.5, they point out that a timestamp can be added to it.

4) U sends the login request messages (ID, C, T) to S.

Modified Login Phase to Key agreement
The steps of the login phase have been modified as follows:

1) U sends ID to S to login to the system.

2) After receiving the login ID, S computes $B" = g^{h(x\|ID)r} \bmod p$ and $A = g^a \bmod p$. Then S computes $h(B"\|A)$ and sends back the message $(h(B"\|A), r, A)$ to U.

3) Upon receiving $(h(B"\|A), r, A)$, U computes $B' = (Bg^{-h(PW)})^r \bmod p$. Then U can verify the validity of S by checking whether the received $h(B"\|A)$ is equal to the hashed $(B'\|A)$. If it is, U computes $W = g^w \bmod p$ and $C = h(T\|B'\|W)$; otherwise, S is rejected. To overcome the $(h(B"\|A), r, A)$ replaying attack, in point 8 of Section 2.5, they point out that a timestamp can be added to it.

4) U sends the login request messages (ID, C, W, T) to S.

Finally, U and S can agree on the session key $K = A^w \bmod p = W^a \bmod p = g^{aw} \bmod p$.

Authentication Phase
Upon receipt of the login request messages (ID, C, T), S performs the following steps:

1) Check whether ID is in the specific format.

2) Check whether T is a valid timestamp.

3) Compute $C' = h(T\|B")$.

4) Check whether the equation $C = C'$ holds.

If one of the above check results is no, the login request is rejected; otherwise, the login request is accepted.

Furthermore, Liao et al.'s scheme allows users to freely change their passwords. A user can insert his/her smart card and key in a new PW'. The smart card will compute $Y = g^{h(PW')} \bmod p$, $Z = Bg^{-h(PW)} \bmod p$, and $\beta = YZ \bmod p$. Then the smart card replaces B with β.

4 Comparisons

In this section, we compare the schemes in terms of security requirements satisfied, goals achieved, and performance. Checking out all the security requirements and goals we listed in the Introduction Section, we can judge if a scheme deserves the title of an ideal password authentication scheme.

4.1 Security Requirements

Tables 2, 3, and 4 show how the three types of schemes compare in security requirements. In Table 2, Yang et al.'s scheme turns out the best scheme because their scheme can withstand most of the attacks. In Table 3, Awasthi-Lal and Kumar's scheme are the best schemes for the same reason. In Table 4, most schemes prove to be good, capable of withstanding most of the attacks. However, we can seen that none of the password authentication schemes from any of the three types is an ideal password authentication scheme.

4.2 Goals

Tables 5, 6, and 7 show how the three types of schemes compare in terms of the goals they achieve. In Table 5, unfortunately, none of the schemes can achieve most goals. These schemes are not good. In Table 6, the schemes are also not good because they cannot achieve most goals. In Table 7, Liao's scheme is the best scheme because it can achieve most goals. However, we can see that none of the password authentication schemes from the three types is an ideal password authentication scheme.

4.3 Performance

The performance evaluation here mainly concerns the time complexity. To evaluate the three types of schemes, the symbols used to analyze the computational complexity have been defined and shown in Table 8. For simplification, we skip the registration phase and password change. Tables 9, 10, and 11 show how the performances of the three types of schemes compare. The tables clearly reveal why more and more password authentication schemes are based on one-way hash function.

5 Future Works

In general, there are three types of identity authentication tasks [26]:

1) identity authentication for something known, such as a password;

2) identity authentication for something possessed, such as a smart card;

3) identity authentication for some personal characteristics, such as fingerprints.

Most existing schemes use the first two methods to identify a user. In the future, we can enhance the security level of a system by combing the three types, trying to come up with an ideal password authentication scheme. The procedures of designing an ideal password authentication scheme are shown in Figure 1.

In addition, most password authentication schemes currently available are only designed for the single-server environment. However, since the scales of computer networks are becoming larger and larger, password authentication schemes which only support single-server environment will soon fall behind users' needs. Therefore,

Table 2: Security requirement comparisons among the RSA-based schemes

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9
Yang-Shieh[52]	Y	N	Y	N	Y	Y	Y	Y	Y
Fan et al.[15]	Y	N	Y	N	Y	Y	Y	Y	Y
Yang et al.[51]	Y	Y	Y	N	Y	Y	Y	Y	Y

SRi: Proposed Security Requirements in Section 1, Y: Supported, N: Not supported.

Table 3: Security requirement comparisons among the ElGamal-based schemes

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9
Hwang-Li[23]	Y	N	N	N	Y	Y	Y	Y	Y
Awasthi-Lal[1]	Y	Y	Y	N	Y	Y	Y	Y	Y
Kumar[27]	Y	Y	Y	N	Y	Y	Y	Y	Y

Table 4: Security requirement comparisons among the hash-based schemes

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8	SR9
Sun[46]	Y	Y	N	N	Y	Y	Y	Y	Y
Hwang et al.[22]	Y	Y	Y	N	Y	Y	Y	N	Y
Chien et al.[11]	Y	Y	Y	Y	N	Y	Y	N	Y
Chen et al.[9]	Y	Y	Y	Y	Y	Y	Y	N	Y
Liao et al.[32]	Y	Y	Y	Y	Y	Y	Y	N	Y
Yoon et al.[55]	Y	Y	Y	Y	Y	Y	Y	N	Y
Lee et al.[29]	Y	Y	Y	Y	Y	Y	Y	N	Y
Liao et al.[31]	Y	Y	Y	Y	Y	Y	Y	N	Y

Table 5: Goals comparisons among the RSA-based schemes

	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
Yang-Shieh[52]	Y	N	N	Y	Y	Y	N	N	N	N
Fan et al.[15]	Y	N	N	Y	Y	Y	N	N	N	N
Yang et al.[51]	Y	N	N	Y	Y	Y	N	N	N	N

Gi: Proposed Goals in Section 1, Y: Achieved, N: Not Achieved.

Table 6: Goals comparisons among the ElGamal-based schemes

	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
Hwang-Li[23]	Y	N	N	Y	N	Y	N	N	N	N
Awasthi-Lal[1]	Y	N	N	Y	N	Y	N	N	N	N
Kumar[27]	Y	N	N	Y	N	Y	N	N	N	N

Table 7: Goals comparisons among the hash-based schemes

	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
Sun[46]	Y	N	N	Y	Y	Y	N	N	N	N
Hwang et al.[22]	Y	Y	Y	Y	Y	Y	N	N	N	N
Chien et al.[11]	Y	N	N	Y	Y	Y	N	N	N	N
Chen et al.[9]	N	N	Y	Y	Y	Y	N	N	N	N
Liao et al.[32]	Y	N	Y	Y	Y	Y	N	N	Y	N
Yoon et al.[55]	Y	Y	N	Y	Y	Y	Y	N	N	Y
Lee et al.[29]	Y	Y	N	Y	Y	Y	N	N	N	N
Liao et al.[31]	Y	Y	Y	Y	Y	Y	N	Y	N	N

Table 8: Symbols

T_{mexp}	the time for executing a modular exponentiation operation
T_{mmul}	the time for executing a modular multiplication operation
T_{xor}	the time for executing a XOR operation
T_h	the time for executing a one-way hash function
T_{ck}	the time for executing a function $C_k()$

Table 9: The performance analysis of the RSA-based schemes

	Login Phase	Authentication Phase
Yang-Shieh[52]	$2T_{mexp} + 3T_{mmul} + 1T_h$	$2T_{mexp} + 1T_{mmul} + 1T_h$
Fan et al.[15]	$2T_{mexp} + 3T_{mmul} + 1T_h$	$2T_{mexp} + 1T_{mmul} + 1T_h$
Yang et al.[51]	$2T_{mexp} + 3T_{mmul}$	$3T_{mexp} + 1T_{mmul}$

Table 10: The performance analysis of the ElGamal-based schemes

	Login Phase	Authentication Phase
Hwang-Li[23]	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$
Awasthi-Lal[1]	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$
Kumar[27]	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h$	$3T_{mexp} + 1T_{mmul} + 1T_{xor} + 1T_h + 1T_{ck}$

Table 11: The performance analysis of the hash-based schemes

	Login Phase	Authentication Phase
Sun[46]	$1T_{xor} + 1T_h$	$1T_{xor} + 2T_h$
Hwang et al.[22]	$2T_{xor} + 2T_h$	$2T_{xor} + 2T_h$
Chien et al.[11]	$2T_{xor} + 1T_h$	$2T_{xor} + 2T_h$
Chen et al.[9]	$5T_{xor} + 8T_h$	$3T_{xor} + 3T_h$
Liao et al.[32]	x	$19T_{xor} + 9T_h$
Yoon et al.[55]	$2T_{xor} + 1T_h$	$4T_h$
Lee et al.[29]	$2T_{xor} + 1T_h$	$2T_{xor} + 4T_h$
Liao et al.[31]	$3T_{mexp} + 2T_{mmul} + 3T_h$	$1T_h$

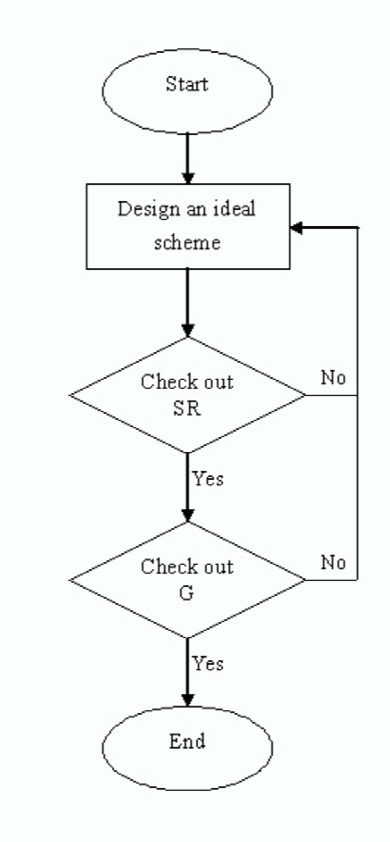

Figure 1: The procedures of designing an ideal password authentication scheme

some schemes [25, 34] have tried multi-server architectures, where users can register at the register center only once and access resources from different servers efficiently. In the future, expert researchers can also attempt to develop an ideal password authentication scheme with a multi-server architecture.

6 Conclusions

In this study, we have surveyed all currently available password authentication schemes and analyzed how they work over insecure networks. Unfortunately, none of the schemes can solve all possible problems and withstand all possible attacks. We have defined all the security requirements and all of the goals an ideal password authentication scheme should satisfy and achieve. In the future, we hope an ideal password authentication scheme which meets all the security requirements and achieves all the goals can be developed.

References

[1] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1246–1248, 2003.

[2] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, vol. 46, pp. 992–993, 2000.

[3] C. K. Chan and L. M. Cheng, "Cryptanlysis of timestamp-based password authentication scheme," *Computers & Security*, vol. 21, no. 1, pp. 74–76, 2002.

[4] C. C. Chang and K. F. Hwnag, "Some forgery attack on a remote user authentication scheme using smart cards," *Infomatics*, vol. 14, no. 3, pp. 189–194, 2003.

[5] C. C. Chang and W. Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," *Compupers & Security*, vol. 13, no. 2, pp. 137–144, 1994.

[6] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, pp. 165–168, May 1991.

[7] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," *IEICE Transactions on Communications*, vol. E85-B, pp. 2519–2521, November 2002.

[8] K. F. Chen and S. Zhong, "Attacks on the (enhanced) Yang-Shieh authentication," *Computers & Security*, vol. 22, no. 8, pp. 725–727, 2003.

[9] T. H. Chen, W. B. Lee, and G. Horng, "Secure SAS-like password authentication schemes," *Computer Standards & Interfaces*, vol. 27, pp. 25–31, 2004.

[10] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "A modified remote login authentication scheme based on geometric approach," *Journal of Systems and Software*, vol. 55, pp. 287–290, 2001.

[11] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers & Security*, vol. 21, pp. 372–375, 2002.

[12] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamid ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[13] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

[14] A. Jr. Evans, W. Kantrowitz, and E. Weiss, "A user authentication scheme not requiring secrecy in the computer," *Communications of the ACM*, vol. 17, pp. 437–442, August 1974.

[15] L. Fan, J.H. Li, and H. W. Zhu, "An enhancement of timestamp-based password auhentication scheme," *Computers & Security*, vol. 21, pp. 665–667, 2002.

[16] N. Haller, "The S/KEY one-time password system," in *Proceedings of Internet Society Symposium on Network and Distributed System Security*, pp. 151–158, 1994.

[17] N. Haller, "The S/KEY one-time password system," *RFC1760*, Feb. 1995.

[18] G. Horng, "Password authentication without using password table," *Information Processing Letters*, vol. 55, pp. 247–250, 1995.

[19] C. L. Hsu, "Security of two remote user authentication schemes using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1196–1198, 2003.

[20] C. L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 26, no. 3, pp. 167–169, 2004.

[21] M. S. Hwang, "Cryptanalysis of remote login authentication scheme," *Computer Communications*, vol. 22, no. 8, pp. 742–744, 1999.

[22] M. S. Hwang, C. C. Lee, and Y. L. Tang, "A simple remote user authentication scheme," *Mathematical and Computer Modelling*, vol. 36, pp. 103–107, 2002.

[23] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[24] J. K. Jan and Y. Y. Chen, "'paramita wisdom' password authentication scheme without verification tables," *The Journal of Systems and Software*, vol. 42, pp. 45–57, 1998.

[25] W. S. Juang, "Efficient multi-server password authentication key agreement using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 251–255, 2004.

[26] H. J. Kim, "Biometrics, is it a viable proposition for identity authentication and access control," *Computers & Security*, vol. 14, pp. 205–214, 1995.

[27] M. Kumar, "New remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 597–600, 2004.

[28] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, pp. 770–772, November 1981.

[29] S. W. Lee, H. S. Kim, and K. Y. Yoo, "Improved efficient remote user authentication scheme using smart cards," *IEEE Transactions on Communications*, vol. 50, pp. 565–567, May 2004.

[30] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1243–1245, 2003.

[31] I-En Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *accepted in Journal of Computer and System Sciences*, 2005.

[32] I-En Liao, C. C. Lee, and M. S. Hwang, "Security enhancemento for a dynamic id-based remote user authentication scheme," in *IEEE CS Press, International Conference on Next Generation Web Services Practices (NWeSP'05)*, pp. 437–440, Seoul, Korea, August 2005.

[33] C. L. Lin, H. M. Sun, and T. Hwang, "Attacks and solutions on strong-password authentication," *IEICE Transactions on Communications*, vol. E84-B, pp. 2622–2627, September 2001.

[34] I. C. Lin, M. S. Hwang, and L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, pp. 13–22, 2003.

[35] C. J. Mitchell and L. Chen, "Comments on the S/KEY user authentication secheme," *ACM Operating Systems Review*, vol. 30, pp. 12–16, Oct. 1996.

[36] NIST. "Secure hash standard,". Tech. Rep. FIPS 180-1, NIST, US Department Commerce, April 1995.

[37] G. B. Purdy, "A high security log-in procedure," *Communications of the ACM*, vol. 17, pp. 442–445, Aug. 1974.

[38] R. Rivest. "The MD5 message digest algorithm,". Tech. Rep. RFC 1321, IETF, April 1992.

[39] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[40] M. Sandirigama, A. Shimizu, and M. T. Noda, "Simple and secure password authentication protocol (sas)," *IEICE Transactions on Communications*, vol. E83-B, pp. 1363–1365, June 2000.

[41] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414–416, 2003.

[42] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards," *Computers & Security*, vol. 22, no. 7, pp. 591–595, 2003.

[43] A. Shimizu, "A dynamic password authentication method by one-way function," *IEICE Transactions on Information and System*, vol. J73-D-I, pp. 630–636, July 1990.

[44] A. Shimizu, T. Horioka, and H. Inagaki, "A password authentication method for contents communication on the Internet," *IEICE Transactions on Communications*, vol. E81-B, pp. 1666–1763, Aug. 1998.

[45] H. M. Sun and H. T. Yeh, "Further cryptanalysis of a password authentication scheme with smart cards," *IEICE Transactions and Communications*, vol. E86-B, no. 4, pp. 1412–1415, 2003.

[46] H. M. Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958–961, 2000.

[47] B. Wang, J. H. Li, and Z. P. Tong, "Cryptanalysis of an enhanced timestamp-based password authentication scheme," *Computers & Security*, vol. 22, no. 7, pp. 643–645, 2003.

[48] T. C. Wu, "Remote login authentication scheme based on a geometric approash," *Computer Communications*, vol. 18, no. 12, pp. 959–963, 1995.

[49] S. Yamaguchi, K. Okayama, and H. Miyahara, "Design and implementation of an authentication system in WIDE Internet environment," in *Proceedings of IEEE Region Conference on Computer and Communication System*, 1990.

[50] C. C. Yang, H. W. Yang, and R. C. Wang, "Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 578–579, 2004.

[51] C. C. Yang, R. C. Wang, and T. Y. Chang, "An improvement of the Yang-Shieh password authentication schemes," *Applied Mathematics and Computation*, vol. 162, pp. 1391–1396, 2005.

[52] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computers & Security*, vol. 18, no. 8, pp. 727–733, 1999.

[53] T. C. Yeh, H. Y. Shen, and J. J. Hwang, "A secure one-time password authentication scheme using smart cards," *IEICE Trans. on Communications*, vol. E85-B, pp. 2515–2518, Nov. 2002.

[54] S. M. Yen and K. H. Liao, "Shared authentication token secure against replay and weak key attacks," *Information Processing Letters*, vol. 62, pp. 77–80, 1997.

[55] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "An improvement of Hwang-Lee-Tang's simple remote user authentication schemes," *Computers & Security*, vol. 24, pp. 50–56, 2005.

Chwei-Shyong Tsai was born in Changhua, Taiwan, Republic of China, on September 3, 1962. He received the B.S. degree in Applied Mathematics in 1984 from National Chung Hsing University, Taichung, Taiwan. He received the M.S. degree in Computer Science and Electronic Engineering in 1986 from National Center University, Chungli, Taiwan. He received the Ph.D. degree in Computer Science and Information Engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. From August 2002, he was an associate professor of the Department of Information Management at National Taichung Institute of Technology, Taichung, Taiwan. Since August 2004, he has been an associate professor of the Department of Management Information Systems at National Chung Hsing University, Taichung, Taiwan. His research interests include image watermarking, image authentication, information hiding, bio-information and computer networks.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from the Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and in 2001. He researched in Computer and Information Science from the National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He is currently pursuing his Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, Republic of China. He is a Lecturer of Computer and Communication, Taichung Healthcare and Management University (THMU), from 2004. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 25 articles on the above research fields in international journals.

Min-Shiang Hwang received the B.S. in Electronic Engineering from the National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from the National Tsing Hua University, Taiwan, in 1988; and a Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at the National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also the chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of National Science Council of the Republic of China. He is currently a professor and chairman of the department of Management Information Systems, National Chung Hsing University, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 100 articles on the above research fields in international journals.