Password Authentication Using Smart Card over Unsecure Channel

Sattar J. Aboud  
Department of Computer Science and Technology,  
University of Bedfordshire, UK  
Corresponding Author Email: sattar_aboud@yahoo.com

Edmond Prakash  
Department of Computer Science and Technology,  
University of Bedfordshire, UK

ABSTRACT

Password authentication is one of easiest and most appropriate authentication methods under unprotected channels. The problem of password authentication over unprotected channel is existed in various uses. Computing resources have increased considerably, password authentication is more often needed essential to login to computers, and wireless networks. Many authentication systems that rely on encryption schemes are proposed to solve some difficulties in the past. But, existing systems are vulnerable to different attacks and are neither efficient, nor user friendly. The user cannot select and alter its passwords regularly. In this research, we introduce a new password authentication system to meet all suggested requirements. The proposed system uses a Diffie-Hellman key agreement protocol under unprotected channels to encrypt and decrypt the communicated messages using asymmetric cryptography.

Keywords- Diffie-Hellman exchange key; wireless security; one-time password; password authentication system;

1. INTRODUCTION

Password authentication gives authorized user to employ the resources of a remote system. Various Internet applications are relying on password authentication, such as login. But, an existing Internet milieu is vulnerable to different attacks such as replay attack, guessing attack, modification attack, and stolen verifier attack. Thus, number of authors has introduced some password authentication systems for secure login of authorized users. In conventional password authentication systems, every user has identifier \( id \) and password \( w \). When the user needs to login to server, must insert the \( id \), and \( w \) to a server. The easiest authentication method is to save and to provide the password table including users \( id \) and passwords \( w \) in a server. Once accept a user \( id \) and password \( w \), a server searches a password table to check if the inserted \( id \) and \( w \) are identical with those in a password table or not. Upon \( id \) and \( w \) match a related pair kept in a server password table, a user is allowed access to a server services. As a user password is saved in document form in password table, this method is vulnerable to disclosure of passwords. The hacker can masquerade as the authorized user by theft a user \( id \) and \( w \) from a password table. This attack is so-called stolen-verifier attack. Another drawback in this method is that a system load is too high, when many users register in a system, a password table will become large and difficult to maintain. The hacker can intercept the \( id \), and \( w \) over Internet, and then replay later to login. Such attack is called a replay attack. To avoid a password table from theft, password must be encrypted inside a computer [1]. But, a broadcast of unencrypted password can be stolen. So, this system is weak to a replay attack. To overcome this difficulty, Lamport introduced one-time password using a one-way hash function [2]. Nevertheless there are three weaknesses in Lamport scheme. The first is a hash operating cost. The second is a need for password table. The third is the verification table must be saved in a server to check a validity of the user. When a hacker can somehow interrupt a server, the contents of a verification table can be altered easily. This is so-called modification attack. The attack also means that a hacker can pose as other authorized users by building the valid login demand from intercepted login demand. Authors have identified this difficulty and presented the solutions by which a verification table is no longer needed in a server.

2. RELATED WORKS

Since Lamport’s scheme, many researchers proposed other schemes to withstand various attacks, including offline password guessing attacks, replay attacks, denial of service attacks, stolen verifier attacks, and so on [3]. For example, in 1990, Yamaguchi et al. [4] introduced a simple scheme and they claimed that their scheme is efficient authentication scheme. Later, Hwang et al. indicated that the scheme is weak to a guessing attack [5]. In 1991, Chang and Wu [6] introduced the remote password authentication protocol with the smart card that relied on a Chinese Remainder Theorem. The system does not need to keep in verification table and is secure to anti-attacks of replaying before intercepted needs. But, a user password of this system cannot be selected and altered easily by a holder. In 1995, Wu [7] presented an efficient system that relied on a geometric Euclidean smooth. The merits of this system are its ease of geometry and a characteristic that user can easily select its own passwords. But, the scheme is insecure as shown in [8]. In 1999, Yang and Shieh [9] presented an approach to avoid replay attack. The system does not save passwords in a server, and allow user easily to alter its password. But Tzung et al. [10] indicated that Yang and Shieh approach has the weakness is that a hacker is able to impersonate the authorized user by building the authentic login request from intercepted login. Thus, Yang and Shieh scheme
cannot avoid modification attack. In 2000, Sandirigama et al. suggested a scheme [11], which was intended to be better compared with Lamport scheme, but this scheme was costly in terms of computing time and communication overhead. In 2002, Chien et al. [12] introduced a practical smart-card-typed scheme relied on secure one-way hash function. The researchers claimed that their system has the characteristics of verification table is not needed in a server, a communication and computing cost is very low, a replay attack problem is entirely solved and user can easily select its password. But, Altinkemer and Wang [13] indicate that the scheme is not allow user to alter its password easily. In 2005, Choo and McCullagh introduced a password authentication system using smart card [14]. In their system, a smart-card-oriented remote login authentication scheme is employed to validate authorized user. A smart card holds microprocessor that can achieve arithmetic processes rapidly, by which selected messages are kept. So, there is no need to keep the verification table in a server. In 2010, Li, et al. [15] proposed a two-factor user authentication scheme which provides mutual authentication and key agreement over insecure channels. But, in 2012 Jin Quyan et al., find that Li et al, scheme is vulnerable to some attacks [16]. There are many smart card systems suggested to validate the authorized user, none of them can solve all difficulties. The main problem is that when a user lost the smart card. The hacker can select the smart card lost by authorized user, then it can masquerade a user to login a scheme by offline guessing a password of a card holder. The aim of this research is to present the new password authentication system using smart card and illustrate that the proposed system can accomplish the requirements indicated below. The proposed scheme is better than other schemes in terms of storage space, time complexity, and communication overhead. The requirements to solve the problems in smart card typed systems are as follows:

- The verification table is not kept inside a computer.
- The password is selected and altered easily by a holder.
- The password is not disclosed by a manager of a server.
- The password is not posted in message on channel.
- No entity can impersonate the authorized user to login to a server.
- The scheme should resist anti modification, stolen-verifier and guessing attacks.
- The size of the password should be suitable to remember.
- The scheme should be inexpensive and practical.
- The scheme can accomplish shared authentication.
- The password must not break by guessing attack even if a smart card is missing.

### 3. NOTATION USED

The notations used in this research are as follows:

- \( A \) : represents a user.
- \( S \) : represents an authentication server.
- \( Id \) : represents a user identity.
- \( w \) : represents a password of user \( A \).
- \( d \) : represents a private key of server \( S \).
- \( p \) : represents a prime number.
- \( a \) : represents a generator in Galois field \( GF(p) \).
- \( r \) : represents a service request. The request by a user to login a server.
- \( k \) : represents an arbitrary number.
- \( T \) : represents a time stamp.
- \( h \) : represents a secure one-way hash function.
- \( || \) : represents a concatenation.

### 4. THE DESCRIPTION OF THE PROPOSED SCHEME

The proposed system comprises three protocols. These are the registration protocol, the login protocol, and the authentication protocol. In a registration protocol, a server delivers a smart card to a user who requests registration. After a successful registration with the server, the server delivers the card to a user and verifies a validity of the card with the signature. We will not describe the server signature in this paper. If the user needs to use the card, should run this protocol first. The system is not accountable for verifying users except issuing smart card to the new user. The steps of the registration protocol are as follows:

**Step 1: The Server**

1. Chooses a prime number \( p \).
2. Selects a generator \( a \) in \( GF(p) \).
3. Chooses a secure one-way hash function \( h \).
4. Selects a long private key \( d \) and save it in safety location.

**Step 2: The User**

1. Selects \( Id \) and \( w \), \( w \) must be easy for remembering.
2. Computes \( h(w) \) using one-way hash function \( h \).
3. Posts a message \( Id \) and \( h(w) \) to a server \( S \) by an open channel.

**Step 3: The Server**

1. Computes \( v = a^{h(Id)} + h(w) \) mod \( p \).
2. Issues to the user A smart card which holds $Id, v, p, a$.
3. Posts this card to user A by the open channel.

### 4.2 The Login Protocol

After login, the user A inserts the smart card into the machine, and then he enter his $Id$ and his password $w$. Then, the server and the user will carry out the following steps:

1. The user A issues the login service request to server $S$.
2. The server $S$ finds $v' = a^{h(Id)k} \mod p$ and then computes $h(v')$ employing a one-way hash function $h$. The server then posts a message $h(v')$ and an arbitrary value $k$ to user $A$.
3. The smart card of user $A$ finds $v' = va^{h(w)k} \mod p$. Then the user checks a validity of server $S$ by verifying a received message $h(v')$ is identical to hashed $v'$. If yes, he finds $b = h(T || v')$; else, a server is rejected and repeats a login protocol. The time stamp $T$ of this login, and $k$ can accomplish a one-time password and avoid the replaying attack. The user $A$ passes a login request message $(Id, b, T)$ to server $S$.

### 4.3 The Authentication Protocol

This protocol is performed by a server $S$ to decide if user $A$ is allowed to login or not. Assume $T$ is the time if server $S$ accepts a login request message. A server $S$ performs the following steps to check a legality of user $A$.

1. Verify when a setup of $Id$ is true. If not, server $S$ rejects a login request message.
2. Compare $T$ with $T'$. When $T' = T \leq T''$, accept user $A$ login request; or reject it. The $T''$, is a legal time interval for broadcast delay, used to avoid replaying attack.
3. Find $b' = h(T || v')$ and then verify if $b$ is identical to $b'$. If not, then the server $S$ rejects a login request message; or the server $S$ receives a login request message.

### 4.4 The Change Password

The proposed scheme allows user to easily alter the password, and user does not want to register in a server again to alter the password. The proposed system is competitive with other schemes. In selected schemes, a password of the user has to be created by a server, and a user cannot alter his password unless he re-registers again. Every user must be allowed to alter his password regularly without he concerns about a possible disclosure of a password. When the user needs to alter the password, he can insert the smart card in the device and insert a new selected password $w$ according to the following steps:

1. Chooses the new password $w'$
2. Find $e = v^{-h(w)} \mod p$ with $w$ as the previous password of a user.
3. Find $f = e \mod p$
4. Substitute $v$ with $f$ in a smart card.
5. Once the password is altered, obtain updated smart card and use a new password $w'$.

### 5. Discussion

Some systems hide the password table in a server for keeping encoded passwords. For example, suppose there are $n$ users in a server. So, the amount of space required to save user identifiers and encrypted user passwords are $O(n)$. In the proposed system, a server requires to store only one private key. Thus, a computing time of the proposed system for a server is $O(1)$. The computing time of the proposed system is considered as follows. Assume $T_h$ is the time for running a one-way hash function $h$. In the registration protocol, the computing cost is (1 exponentiation +1 addition +1 modular operation). In the login protocol, the computing cost is $5T_h + 3$ exponentiations +2 multiplications +2 modular operations +1 ). In the authentication protocol, the computing cost is ( $2T_h +1$ comparison). Besides, the proposed system permits users to easily alter the passwords. The computing cost for altering password is (1 created new password +2 exponentiations +2 multiplications +2 modular operations).

The security of the proposed system is relied on both a discrete logarithm assumption and a secure one-way hash function. Many schemes are relied on one-way hash function [17]. The computing cost is less with a discrete logarithm problem. But, a proposed system is more secure than those relied on one of two problems. Comparing with other systems that have the verification table for keeping encrypted user passwords, the proposed system allows a server securely save only one value. When a value is known to others, the proposed system will be destroyed. So, a server must continue and store this value securely.

### 6. The Properties of the Proposed Scheme

In this section, we describe the properties of the proposed scheme as follows.

- No password table is stored in the computer. There is just one private key $x$ known and kept securely by a server. This characteristic can withstand the stolen-verifier attack and modification attack since no one can steal and alter user password.
- The user password is selected easily by a user, not given by a server. Also, a user can alter the password.
- The password of a user is not known to the manager of the server, because it is protected by one-way hash function $h(w)$.
• The password of a user is not send on a channel. Instead \( h(B^x) \) and \( C \) are sent on channel. While these values contain \( x \), they are protected by discrete logarithms and one-way hash function. If hacker knows \( B \) and intercepts \( R \) provided \( B^x, R, g \) and \( p \), but it is difficult to determine \( x \), since the security relies on intractability of computing discrete logarithm over \( GF(p) \).

• The password parameter \( (h(B^x), C) \) is employed one time in login protocol. These messages cannot be intercepted for reprocess since they are created by \( R \) and \( T \) with different result for every login. However, a server can test when \( T' - T \leq \Delta T \) to avoid a replay attack.

• The user can select the small password for easy remembrance in the registration protocol. Then a server will create the long password parameter \( B \) using \( x, ld \) and put \( (ld, B, p, g) \) into a smart card supplied to a user. A user requires only remembering a small password for employing a smart card. The computing time for a smart card is not much. It requires only two exponential operations and one hashing operation.

• When the impersonated server desires to fraud a requesting user, the server should prepare the valid message \( (h(B^x), R) \). But, it is difficult to find \( h(B^x) \) since there is no way to get a value \( h(x||ld) \), because of a one-way hash function and discrete logarithm problem are used. Also, \( x \) is the long private key kept by a server, without knowing \( x \), no entity can forge the server to fraud a user. In the proposed scheme, not only a server can validate a user, but also user can validate a server.

• Guessing attacks are categorized as online or offline. The online guessing attacks can be avoided easily by restricting the number of failed login. (In the proposed scheme, when a hacker intercepts \( h(B^x), R, C \), and \( T \)). It cannot break \( w \) by making offline guessing attacks since \( w \) is protected by both one-way hash function and the discrete logarithm problem. Also, even if a smart card is missing, it is still difficult for offline guessing attacks to determine \( w \). The individual, who chosen a missing smart card, can attempt to get a password \( w \) from \( B = g^{h(x||ld)+h(w)} \mod p \). While it knows \( B, g, p, h \), and \( ld \), it cannot get \( w \) without knowing \( x \).

7. CONCLUSIONS

In this paper, we have introduced a new password system under unprotected channel. The requirements for gauging the new password system presented into Section 4, the proposed system is a sound scheme compare with other systems. The main value of the proposed system is in its ease and realism for application over an unprotected communication channel. The drawback of the proposed system is that a server has to save the private value securely. When a value is known to others, the proposed system will break. In order to give the advanced security of password system, combining three kinds of uniqueness authentication approaches.

ACKNOWLEDGEMENT

The authors would like to thank the Department of Computer Science and technology at the University of Bedfordshire for its support this project.

REFERENCES


