New Remote Mutual Authentication Scheme using Smart Cards

Rajaram Ramasamy*, Amutha Prabakar Muniyandi**

* Thiagarajar College of Engineering, Madurai, Tamil Nadu 625 015, India
E-mail: rrajaram@tce.edu

** Smart and Secure Lab, Thiagarajar College of Engineering, Madurai, Tamil Nadu 625 015, India

Abstract. Remote mutual authentication based on smart cards is the best practical solution for remote accessing. Most of the schemes are password based. In this paper we propose a new remote mutual authentication scheme using smart cards without maintaining the password table. This is based on ElGamal's. It provides high security and mutual authentication at a reasonable computational cost. Furthermore it restricts most of the current attacking mechanisms. It is simple and can be adopted in any kind of lightweight devices.

1 Introduction

To access resources from a remote system, users should have proper access rights. One of the simpler and more efficient mechanisms is the use of a password authentication scheme. To access the resources, each user should have an identity (ID) and a password (PW). In the existing traditional setup the ID and PW are maintained by the remote system in a verification table. If a user wants to log in a remote server, he has to submit his ID and PW to the server. The remote server receives the login message and checks the eligibility of the user by referencing the password or verification table. If the submitted ID and PW match the corresponding pair stored in the server's verification table, the user will be granted access to the server.

A remote password authentication scheme is used to authenticate the legitimacy of the remote user over an insecure channel. In such a scheme, the password is often regarded as a secret shared between the authentication server (AS) and the user, and serves to authenticate the identity of the individual login. Through knowledge of the password, the remote user can create a valid login message to the authentication server. AS checks the validity of the login message to provide the access right. Password authentication schemes with smart cards have a long history in the remote user authentication environment.

1.1 Problems in the Traditional Method

Two problems are found in this existing traditional mechanism.

1. The administrator of the server will come to know the password, because the server maintains the password table.
2. An intruder can impersonate a legal user by stealing the user's ID and PW from the password table.

To add to the woes, the current Internet is vulnerable to various attacks such as denial of service attack, forgery attack, forward secrecy attack, server spoofing attack, parallel session attack, guessing attack, replay attack, smart card loss attack, and stolen verifier attack. In this paper we propose a new remote mutual authentication scheme using smart cards without password table, which circumvents most of these attacks. In the proposed method the remote system does not maintain the password table, but instead maintains the one-time registration date and time of the users.

In this paper, we propose an improved remote user authentication scheme based on ElGamal, using smart cards. We have incorporated mutual authentication, which enhances the security mechanism further. Our proposed scheme resists most of the attacking mechanisms.

This paper is organized as follows, in section 2 we review the Hwang Li scheme [7] and Awasthi Lal scheme [14]. In section 3, we propose a new remote mutual authentication scheme without using password table. In section 4, we provide a security analysis of our proposed scheme. In Section5, we analyze the cost and functionality of the related scheme. Finally, in section 6, we conclude our paper.

2 Related Work

In 1981 Lamport [1] proposed a remote password authentication scheme using a password table to achieve user authentication. The Lamport [1] scheme is not secure, due to some vulnerabilities. A remote user authentication scheme using smart cards was proposed by Hwang–Li [7]. Hwang–Li's scheme is based on the ElGamal's [2] public key scheme. This scheme can withstand the replaying attack by including time stamp in the login message. Moreover, the remote system does not need to store a password table for verifying the legitimacy of the login users. The system only needs to maintain a secret key, which is used to compute user passwords, based on user submitted identities in the authentication phase. As the security of the scheme relies on the difficulty of computing discrete logarithms over finite fields, it is difficult for the users to compute the secret key of the system from known information. This scheme is breakable only by one of its legitimate users. A legitimate user can impersonate other legal users by constructing valid pairs of user identities without knowing the secure key of the system. Later, Shen [15] analyzed impersonation attack of Chan [8] on Hwang Li's [7] scheme, and suggested methods to repulse it.

Awasthi–Lal [14] presented a remote user authentication scheme using smart cards with forward security. Forward security ensures that the previously generated passwords in the system are secure even if the system's secret key is compromised. Yoon et al. [23] citing Awasthi Lal [14] proposed a hash based authentication scheme based on the work of Chien et al.[13]. In the authentication phase, the system cannot validate the login request message to compute the password of the user.

Yoon et al. [23] presents an enhancement to resolve the problems in the abovementioned scheme based on hash function. This scheme enables users to change their passwords freely and securely without the help of a remote server. It also provides secure mutual authentication

In 2004 Kumar [21] proposed a scheme, which is secure against forgery. To obtain this security, this scheme suggests some modification in login and authentication phases. This scheme is the modified form of the Hwang et al. [15] scheme and uses one more function C_K to generate the check digit of Kumar [21] for each registered identity. In this scheme, only the AS can generate a valid identity and the corresponding check digit.

Fan et al. [25] proposed a robust remote authentication scheme with smart cards. He claimed that his scheme satisfies the following properties: 1) low computation for smart cards; 2) no password table; 3) password chosen by the users themselves; 4) no need for clock synchronization and delay-time limitation; 5) withstand the replay attack; 6) server authentication; 7) withstand the offline dictionary attack without smart cards; 8) withstand the offline dictionary attack with smart cards; 9) revoking the lost cards without changing the user's identities. The major contribution of Fan et al. [25] scheme provides a method for preventing the offline dictionary attack even if the secret information stored in a smart card is compromised. The major drawbacks of his scheme are the higher computation and communication costs, because of using Rabin's public-key cryptosystem. Furthermore, his scheme does not provide a function for session key agreement and cannot prevent the insider attack.

Ku et al. [19] proposed an improvement to prevent the reflection attack mentioned by Mitchell [3] and an insider attack discussed by Ku et al. [16]. In addition, they showed that Chien [13] scheme is vulnerable and can be compromised. Furthermore, Ku et al. [19] proposed an improvement to Chien [13] scheme to prevent the above-mentioned weaknesses. However, the improved scheme is not only susceptible to parallel session attack proposed by Hsu [22], but also insecure for changing the user's password in password changing phase. Different types of password authentication schemes have been proposed by [4], [5], [6], [7], [9], [13], [11], [12], [10] and [20].

Hwang et al. [26] present the survey of all currently available password-authentication-related schemes and get them classified in terms of several crucial criteria. Tsai et al. pointed out that most of the existing schemes are vulnerable to various attacks and fail to serve all the purposes that an ideal password authentication scheme should, and define all possible attacks and goals that an ideal password authentication scheme should withstand and achieve.

Tian e.t al. [27] show that Yoon et al. scheme [23] is subject to forgery attacks if the information stored in the smart card is stolen. This violates the "two factor security" objective of the smart cards based remote user authentication schemes. Tian et al. propose an amendment to this problem and propose two new schemes, which are more efficient and secure than Yoon et al.'s scheme.

Liu Yongliang et al. [28] proposed a novel ECC-based wire-less authentication protocol.

3 New Remote Mutual Authentication Scheme Using Smart Cards

In this paper, we propose a new remote mutual authentication scheme using smart cards. Our proposed scheme is composed by an initial phase, a registration phase, a login phase and an authentication phase. Whenever a new user registers through the registration phase, the server issues the smart card and password, which holds the related information, and sends it through the secure channel. To access the remote server, user inserts his smart card into the device and keys the password. The server authenticates the user in the authentication phase.

Lee et al. [17] and Kumar [21] point out that Awasthi Lal fails to provide forward security because the registration time of the user is stored in the smart card itself. This does not apply to our scheme, as the registration time is stored in an encrypted form in the server.

The phases in our proposed scheme are explained below.

3.1 Initial Phase

The Authentication Server (AS) generates the following parameters

p : a large prime number

$f(.)$: A one-way function

x_s : the secret key of the system, maintained by the server

T_R : Registration Timestamp of every user, maintained by the server in an encrypted form, using the server's secret key.

3.2 Registration Phase

A user U_i who wants to register to access the server services, submits its ID_i to the AS. AS computes PW_i as

$$PW_i = (ID_i \oplus T_R)^{x_s} \bmod p$$

Here T_R is the one-time registration time and date of the user U_i as got from the system clock and maintained by the server. Registration center issues a password PW_i and a smart card, incorporated with the public parameters $(f(.), p)$.

3.3 Login Phase

User Ui inserts the smart card to the smart card reader and keys ID_i and PW_i. The smart card will perform the following operations,

1. Generate a random number r
2. Compute $C_1 = PW_i^r \bmod p$
3. Compute $t = f(T \oplus PW_i) \bmod (p-1)$, where T is the current date and time of the smart card reader.
4. Compute $M = PW_i^t \bmod p$
5. Compute $C_2 = M(C_1^t) \bmod p$
6. Sends a login request $C = (ID_i, C_1, C_2, T)$ to the remote system (Authentication Server AS).

3.4 Authentication Phase

Assume AS receives the message C at time T_c, where T_c is the current date and time of the AS. Then AS takes the following actions,

1. Check the format of ID_i. If the identity format is correct, then AS will accept the login request. Otherwise, the request will be rejected.
2. Check the validity of the time interval between T and T_c.
3. Check whether the following equation, $C_2(C_1^t)^{-1} = (PW_i)^{f(T \oplus PW_i)} \bmod p$ is satisfied. It is difficult for

user U_i to compute the secret key x_s and find the registration time T_R of the system from the equation,

$$PW_i = (ID_i \oplus T_R)^{x_s} \bmod p$$

Now mutual authentication message is composed as follows,

$t = f(T_s \oplus PW_i)$ Here T_s is the current time of the remote system.

$$C_3 = C_1^t \bmod p$$

4. Send the mutual authentication message $C^* = (C_3, T_s)$ to user U_i.
5. User U_i receives the mutual authentication message C^* and checks the validity of the message. putes $C_3^* = C_1^t \bmod p$ and checks with the received C_3 value. If it is valid then accepts, otherwise rejects and generates a new login request.

4 Security Analysis of the Proposed Scheme

In this section we discuss the enhanced security features of the proposed scheme. Our proposed scheme withstands most of the attacking methods.

4.1 Denial of Service Attack

In our proposed scheme, the login request is generated based on a password and the current time. The login request generation does not depend on any previous information: every time it is a new one with current time. The attacker cannot create or update the false information to login

4.2 Forgery Attack

The attacker cannot create a valid password without knowing the registration time T_R and the secret key of server x_s. So the attacker cannot create a valid login request and act as a legal user

4.3 Password Guessing Attack

In our scheme, the password is computed as follows $PW_i = (ID_i \oplus T_R)^{x_s} \bmod p$. Suppose an adversary intercepts the login request $C = (ID_i, C_1, C_2, T)$ of a user U_i. It is not possible to recover the original password from the login request message. The T_R value is unique and x_s is the secret key of the remote system.

4.4 Parallel Session Attack

Suppose an adversary intercepts the login message $C = (ID_i, C_1, C_2, T)$, the adversary cannot create a valid new login message. Here C_1 and C_2 values are fresh for every time. The adversary cannot find the value of r and $t = (T \oplus PW_i)$.

4.5 Smart Card Loss Attack

Suppose user U_i loses his smart card, the adversary cannot use this card without knowing the password of the user U_i. Suppose an adversary wants to change the password, he must know the original password. Thus his attempt to impersonate user U_i fails.

4.6 Mutual Authentication

The user U_i wants to log on to the remote system S and sends a login request to S. Suppose an adversary intercepts the login request and attempts to impersonate as remote system S. The adversary cannot calculate the valid $C_3 = C_1^t \bmod p$ without knowing the value PW_i, and cannot get the PW_i value from the login message. The adversary again fails to impersonate the remote system S.

5 Analysis of Cost and Functionality

In this section, we present a comparison between our scheme and three other schemes. All the 4 schemes are based on ElGamal's, but only the proposed scheme facilitates mutual authentication. Table 1 illustrates the computational cost for each phase.

Scheme	E1	E2	E3
Our Scheme	1 Dis–Log	1 Hash + 2 Dis-log	2 Hash + 3 Dis-log
Hwang–Li's [7]	1 Dis-log	1 Hash + 2 Dis-log	1 Hash + 2 Dis-log
Awasthi [17]	1 Dis-log	1 Hash + 2 Dis-log	1 Hash + 2 Dis-log

Kumar [24]	1 Dis–Log	1 Hash + 2 Dis–log	1 Hash + 2 Dis–Log

Table 1: Cost comparison between Our Scheme and Related Schemes

Computational cost comparison between our scheme and related schemes. Here, E1 stands for the computation cost of the Registration phase, E2 stands for the computational cost for the login phase, E3 stands for the computation cost for the authentication phase, Dis-log for discrete logarithm, and Hash for hash function. Obviously due to inclusion of mutual authentication, our scheme entails a higher computational cost.

6 Security Comparison

Table 2 shows the security requirements of the related schemes. Hwang's, Awasthi–Lal and Kumar's scheme are based on the public key ElGamal scheme.

Schemes	S1	S2	S3	S4	S5	S6	S7	S8	S9
Hwang–Li [7]	Y	N	N	N	Y	Y	Y	Y	Y
Awasthi [17]	Y	Y	Y	N	Y	Y	Y	Y	Y
Kumar [24]	Y	Y	Y	N	Y	Y	Y	Y	Y
Our Scheme	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 2: Security Comparison with related schemes

In this table we consider all the attacks identified and defined by Tsai-Lee-Hwang [24]. They are the ones described below. In the table, Y stands for achieved and N for non-achieved.

S1 – 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

S2 – Forgery Attacks (Impersonation Attacks): An attacker attempts to modify intercepted communications to masquerade the legal user and log in the system

S3 – 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 has been stolen

S4 – 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

S5 – Parallel Session Attack: 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

S6 – Password Guessing Attack (Offline dictionary attack): Most passwords have such low entropy that the system is vulnerable to password guessing attacks, where an attacker intercepts authentication messages, stores them locally and then attempts to use a guessed password to verify the correctness of his/her guess using these authentication messages

S7 – Replay Attacks: Having intercepted previous communications, an attacker can impersonate the legal user to log in the system. The attacker can replay the intercepted messages

S8 – 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 log in the system

S9 – 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 log in the system

7 Conclusion

Hwang Li [7] proposed a remote user authentication scheme using smart cards. Awasthi Lal [14] proposed a remote user authentication scheme with forward security. Both schemes suffer different types of attacks. In this paper we propose a new remote mutual authentication scheme using smart cards. Our proposed scheme withstands most of the current attacking mechanisms.

Awasthi Lal's scheme suffers from stolen verifier attack. In our method, stolen verifier attack will not work. The user password is not related to any information stored in the smart card and the server will not maintain any password table. The server maintains the registration time of all the users in the encrypted format by using its secret key. It is difficult for the attacker to find the password without knowing the registration time of the user and the secret key of the remote system.

Acknowledgment

This work was supported by grants from National Technical Research Organization, of Government of India. The authors thank the Principal and Head of the Department of Computer Science and Engineering of Thiagarajar College of Engineering, Madurai, India, for the support and encouragement.

References

[1] L. Lamport (1981), Password authentication with insecure communication, Communication of the ACM, Vol. 24, No. 11, pp. 770-772.

[2] T. ElGamal (1985), A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, Vol. 31, No. 4, pp. 469-472, July.

[3] C. Mitchell (1989), Limitation of challenge–response entity authentication, Electronics Letters, Vol. 25, No.17, pp. 1195–1196, Aug.

[4] C. C. Chang and T. C. Wu (1993), Remote password authentication with smart cards, IEE Proceedings-E, Vol. 138, No. 3, pp. 165-168.

[5] C. C. Chang and S. J. Hwang (1993), Using smart cards to authenticate remote passwords, Computers and Mathematics with applications, Vol. 26, No. 7, pp. 19-27.

[6] T. C. Wu (1995), Remote login authentication scheme based on a geometric approach, Computer Communication, Vol. 18, No. 12, pp. 959-963.

[7] M. S. Hwang and L. H. Li (2000), A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28-30, February.

[8] C. K. Chan and L. M. Cheng (2000), Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, Vol. 46, pp. 992-993.

[9] L. H. Li, L. C. Lin and M. S. Hwang (2001), A remote password authentication scheme for multi-server architecture using neural networks, IEEE Transactions Neural Networks, Vol. 12, No. 6, pp. 1498-1504.

[10] Y. L. Tang, M. S. Hwang and C. C. Lee (2002), A simple remote user authentication scheme, Mathematical and Computer Modeling, Vol. 36, pp. 103-107.

[11] C. C. Lee, M. S. Hwang and W. P. Yang (2002), A flexible remote user authentication scheme using smart cards, ACM Operating Systems Review, Vol. 36, No. 3, pp. 46-52.

[12] C. C. Lee, L. H. Li, and M. S. Hwang (2002), A remote user authentication scheme using hash functions, ACM Operating Systems Review, Vol. 36, No. 4, pp. 23-29.

[13] H. Y. Chien, J. K. Jan, and Y. M. Tseng (2002), An efficient and practical solution to remote authentication: smart card, Computers & Security, Vol. 21, No. 4, pp. 372–375.

[14] A K. Awasthi and Sunder Lal (2003), A Remote User Authentication Scheme using Smart Cards with Forward Security, IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp. 1246-1248, 2003.

[15] J. J. Shen, C. W. Lin and M. S. Hwang (2003), A modified Remote User Authentication Scheme using Smart Card, IEEE Transactions on Consumer Electronics, Vol. 49, No. 2, pp. 414-416.

[16] W. C. Ku, C. M. Chen, and H. L. Lee (2003), Cryptanalysis of a variant of Peyravian–Zunic's password authentication scheme, IEICE Transaction on Communication, Vol. E86–B, No. 5, pp. 1682–1684, May.

[17] Sung-Woon Lee, Hyun-Sung Kim, and Kee-Young Yoo (2004) Comment on a Remote User Authentication Scheme using Smart Cards with Forward Secrecy. IEEE Transactions on Consumer Electronics, Vol 50. No 2. May.

[18] M. Kumar (2004), Some Remarks on a Remote User Authentication Scheme Using Smart Cards with Forward Secrecy. IEEE Transactions on Consumer Electronics, Vol 50. No 2. May.

[19] W. C. Ku, and S. M. Chen (2004), Weakness and improvement of an efficient password based user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 204-207, Feb.

[20] A. K. Awasthi and S. Lal (2004), An enhanced remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, pp. 583-586, May.

[21] M. Kumar (2004), New remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, pp. 597-600. May.

[22] C. L. Hsu (2004), Security of Chien et al's remote user authentication scheme using smart cards, Computer Standards and Interfaces, Vol. 26, No. 3, pp. 167-169.

[23] Eun–Jun Yoon, Eun–Kyung Ryu, and Kee–Young Yoo (2004), Further Improvement of an Efficient password based Remote Authentication Scheme using smart cards, IEEE Transaction on Consumer Electronics, Vol. 50, No. 2, pp. 612–614, May.

[24] Eun–Jun Yoon, Eun–Kyung Ryu, and Kee–Young Yoo (2004), Efficient remote user authentication scheme based on generalized ElGamal signature scheme, IEEE Transaction on Consumer Electronics, Vol. 50, No. 2, pp. 568–570, May.

[25] C. Fan, Y. Chan, and Z. Zhang (2005), Robust remote authentication scheme with smart cards, Computers and Security, Vol. 24, No. 8, pp. 619–628, Nov.

[26] C.S. Tsai, Cheng Chi Lee, and Min-Shiang Hwang (2006), Password Authentication Schemes: Current Status and Key Issues, International Journal of Network Security, Vol.3, No.2, PP.101–115, Sept. 2006

[27] X. Tian, Robert W. Zhu, and Duncan S. Wong (2007), Improved Efficient Remote User Authentication Schemes, International Journal of Network Security, Vol.4, No.2, PP.149–154, Mar.

[28] Liu Yongliang, Wen Gao, Hongxun Yao and Xinghua Yu (2007), Elliptic Curve Cryptography Based Wireless Authentication Protocol, International Journal of Network Security, Vol.5, No.3, PP.327–337, Nov.