Vol.2 No. 1, 06-12 (2013)
Received: June 2012; Accepted: Feb.2013

A New Efficient and Secure Remote User Authentication Scheme Using Smart Cards

Swati Agariya

M. Tech, Department of Electronics & Communication Engineering,
Ajay Kumar Garg Engineering College, Ghaziabad UP India

Abstract

In the present Internet age, one of the main challenging tasks is to provide confidentiality for user's transaction. Various authentication schemes have been proposed to secure the information from unauthorized users. One of the most prominent schemes is smart card based authentication scheme used to withstand the possible attacks for verification table. From the user point of view, security and efficiency are the two main factors for any authentication scheme. But, none of these existing smart card based authentication schemes resist all the possible attacks. In this article, an efficient and secure smart card based authentication scheme is being proposed using cryptographic one-way hash function that resists all the possible attacks and satisfies the needs of a user. Security analysis proves that the proposed scheme is more secure and practical.

Keywords: Authentication, Denial-of-Service attack, denning-sacco attack, insider attack, perfect forward secrecy, smart card

Introduction

Network security is the primary requirement to provide data confidentiality, integrity, access control, etc. Data confidentiality during transmission over the public network/s requires some kinds of network security. Authentication is a technique designed to prove the identity of one entity with another entity. It is used to prevent unauthorized access. In order to authenticate the legitimate users, password based authentication schemes have been widely used in many remote login systems. In traditional password based authentication schemes, every user has an identity (ID) and a password (PW). Initially, each and every user has to register to the server by sending ID and PW. The server stores the PW corresponding to the ID in its verification table. Whenever a user wants to access resources from a server, user has to submit ID and PW to pass the server authentication phase. The server verifies the PW corresponding to the ID from verification table. If the received password matches the password stored in the verification table then server authenticates the corresponding user. However, an intruder can impersonate a valid user by intercepting the messages transmitted between user and the server and then login to the server later using the intercepted information. In addition, if an intruder penetrates the server; the contents of the verification table which are in plain text form can be easily modified. One of the solutions to deal with this problem is to encode the password using one way hash function and store the encoded pattern in a verification table [1]. Though, in this approach, size of the verification table increases as the number of users increases

which results in increasing burden to the server. Moreover, an attacker may still modify the contents of the verification table which result the entire system to collapse. To resist all possible attacks on the verification tables, smart card based password authentication scheme has been proposed. Smart card is a tamper resistant integrated circuit card with memory and processor capable of performing computations. The growth of smart cards by including more advanced algorithms for various cryptographic operations is driving their increased use in the field of mobile communication, banking & retail, health care, ID verification and access control, mobile payment, satellite and cable television, transportation etc. As of today, several smart card based authentication schemes have been proposed for these variety of application areas. In this scheme, server does not maintain a verification table to authenticate the legitimate user. Mainly, it is composed of three phases namely: Registration phase, Login phase and Authentication phase. The registration phase is invoked only once when a new user U_i registers in the server. Upon receiving registration request over secure channel, server issues a smart card to user by storing the computed parameters into smart card memory. The login phase and authentication phase are invoked, when a user wants to login the server. Upon receiving the login request, server checks the validity of the login request to authenticate the user. The rest of the paper is organized as follows. Major contributions in the field of smart card based authentication schemes are explained in section 2. Section 3 describes the proposed efficient and secure smart card based authentication scheme. Security analysis of the proposed scheme is discussed in section 4. Finally, section 5 concludes the paper.

Noteworthy Contribution

During the last decade, many well-designed remote user authentication schemes using smart cards have been proposed [4, 5, 6, 9, 10, 12-15]. An ID based scheme using RSA public-key cryptosystem has been proposed [2]. The security of the sche me is based on the difficulty of factoring a large number and the discrete logarithm problem. It was claimed that the scheme resists impersonation attack and replay attack. In addition, user can freely choose and change the password. Nevertheless, it reveals impersonation attack [2]. Based on ElGamal's public key cryptosystem, a remote user authentication scheme has been proposed [9]. It was claimed that the scheme does not maintain any verification table and it resists replay attack. However, it has been proved that the scheme is exposed to impersonation attack [1]. Moreover, user cannot choose and change the password freely as the password is issued by the server. There is only one-way authentication means it does not provide mutual authentication. Further improvement was suggested [6] which was not enough and hence, cryptanalyzed [7].

Based on cryptographic one-way hash function, a remote user authentication scheme has been proposed [8]. It was claimed that the scheme is more efficient in terms of computation and communication cost. In addition, it resists replay and impersonation attacks. However, it does not provide mutual authentication, user cannot choose and change the password freely. Moreover, it

has been proved that the scheme is weak against offline and online password guessing attacks [3]. Further improvement was suggested to overcome these limitations [5]. It was claimed that the scheme does not require any verification table in the server, provides mutual authentication and an authorized user could choose password without any assistance from the server. Still, the scheme is vulnerable to the parallel session attack means fails to provide mutual authentication [3]. In addition, it does not provide security against insider attack, reflection attack and has insecure password change phase.A new remote user authentication scheme using one way hash function has been proposed [10] which was based on dynamic ID. They claimed that the scheme permits the users to choose and change their passwords freely, secure against ID-theft, and resists reply, forgery, guessing, insider and stolen verifier attacks. Nevertheless, it has been pointed out that the scheme is vulnerable to guessing attack, insider attack and fails to provide mutual authentication . All the schemes examined to this point do not solve the serious time synchronization problem. To overcome this limitation, an efficient nonce based scheme has been proposed [14]. It holds all the previous features. In addition, it provides session key generation agreed by the user and the server. However, in this scheme, user is not permitted to change the password freely; insecure against insider attack and uses symmetric key cryptography which makes it inefficient for smart cards with low computational capability. Based on one-way hash function and discrete logarithm, an efficient smart card authentication scheme has been proposed [12]. It was claimed that the scheme is secure against replay attack, impersonation attack, parallel session attack and modification attack. Moreover, it provides mutual authentication and shared session key generation. However, it has been proved that the scheme fails to resist Denial-of-Service attack and provide perfect forward secrecy [11]. To overcome all these drawbacks, this paper suggests an efficient and secure smart card based authentication scheme using cryptographic one-way hash function.

Proposed Scheme:

In this section, an efficient and secure authentication scheme is proposed which resists all the possible attacks and fulfills the security requirements. The notations used throughout this article are summarized as follows:

U_i → a remote user
ID_i → identity of U_i
PW_i → password chosen by U_i
S → authentication server
X_s → permanent secret key of S
$h(\bullet)$ → cryptographic one way hash function
$\oplus$ → bitwise XOR operation
$\|$ → concatenation
N_i, N_j → random nonces generated by U_i and S respectively The scheme consists of four phases: Registration phase, Login phase, Authentication phase and Password change phase.

Registration Phase

In this phase, user U_i selects ID_i and PW_i, computes $h(PW_i)$ and submits it to the server S over a secure channel. Upon receiving the registration request from user U_i, server S computes $A_i = h(X_s)$ and $B_i = A_i \oplus h(ID_i \| h(PW_i))$. The server S issues a smart card to user U_i by storing $\{A_i, B_i, h(\bullet)\}$ into smart card memory. The smart card is delivered to user U_i through a secure channel.

Login Phase

User U_i inserts the smart card to the card reader and keys in ID_i' and PW_i'. The card reader computes $B_i' = A_i \oplus h(ID_i' \| h(PW_i'))$ and checks whether B_i (stored in the smart card memory) and B_i' are equal or not. If yes, user U_i is a legitimate bearer of the smart card. Then the card reader generates a nonce N_i and computes $Z_i = N_i \oplus A_i$, $C_i = h(PW_i') \oplus h(A_i \| N_i)$, $D_i = h(PW_i') \oplus A_i$, $E_i = h(D_i \| N_i \| B_i)$ and sends the login request message $\{ID_i, C_i, E_i, Z_i\}$ to the server S.

Authentication Phase

Upon receiving the login request message $\{ID_i, C_i, E_i, Z_i\}$; server S first checks the validity of ID_i to accept/reject the login request. If it is true, then the server S computes $A_i = h(X_s)$, $N_i = Z_i \oplus A_i$, $h(PW_i') = C_i \oplus h(A_i \| N_i)$, $D_i' = h(PW_i') \oplus A_i$, $B_i' = A_i \oplus h(ID_i' \| h(PW_i'))$, $E_i' = h(D_i' \| N_i \| B_i')$ and checks whether E_i and E_i' are equal or not. If they are not equal then rejects the login request. If true then the server S generates a nonce N_j and computes $Z_j = N_j \oplus A_i$, $F_i = h(A_i \| B_i' \| N_i \| N_j)$ and sends the message $\{F_i, Z_j\}$ to the user U_i. After receiving the message $\{F_i, Z_j\}$ from server S, user U_i computes $N_j = Z_j \oplus A_i$, $F_i' = h(A_i \| B_i' \| N_i \| N_j)$ and checks whether F_i and F_i' are equal or not. If yes, server S is authentic otherwise terminate the session. Then the user U_i computes $G_i = h(A_i \| N_j \| B_i')$ and sends the message $\{G_i\}$ to the server S. After receiving the message $\{G_i\}$ from user U_i, server S computes $G_i' = h(A_i \| N_j \| B_i')$ and checks whether G_i and G_i' are equal or not. If yes, the user U_i is authentic and mutual authentication is achieved otherwise terminate the session. After mutual authentication, both the parties compute the session key $SK = h(D_i \| N_i \| N_j \| B_i')$.

Password Change Phase This phase is invoked whenever user U_i wants to change the password PW_i with a new password PW_{inew}. User U_i inserts the smart card to the card reader and keys in ID_i' and PW_i' and requests to change password. Then the card reader computes $B_i' = A_i \oplus h(ID_i' \| h(PW_i'))$ and checks whether B_i and B_i' are equal or not. If yes, user U_i is a legitimate bearer of the smart card otherwise reject the request. Then the reader
asks the user U_i to input new password PW_{inew}. After entering the new password, the reader calculates $B_{inew} = A_i \oplus h(ID_i' \| h(PW_{inew}))$ and replaces B_i with B_{inew} in the smart card memory.

Security Analysis

In this section, the security of the proposed scheme is examined through considering the security requirements and all the possible attacks. It is clear that the proposed scheme is efficient and practical as it uses only the one-way hash function instead of any symmetric or asymmetric encryption-decryption technique. So, the computational workload of the smart card as well as the server will be low. The given scheme resists the following possible attacks and provides the essential security requirements.

Forgery Attack (Impersonation Attack)

The proposed scheme(Fig-1) resists impersonation attack. In this scheme, the login request message contains $C_i = h(PW_i') \oplus h(A_i \| N_i)$, $Z_i = N_i \oplus A_i$ and $E_i = h(D_i \| N_i \| B_i')$. Hence, the attacker needs the value of A_i, N_i and B_i' to forge which are not a part of any of the transmitted messages between user U_i and the server S.
Online and Offline Password Guessing Attacks

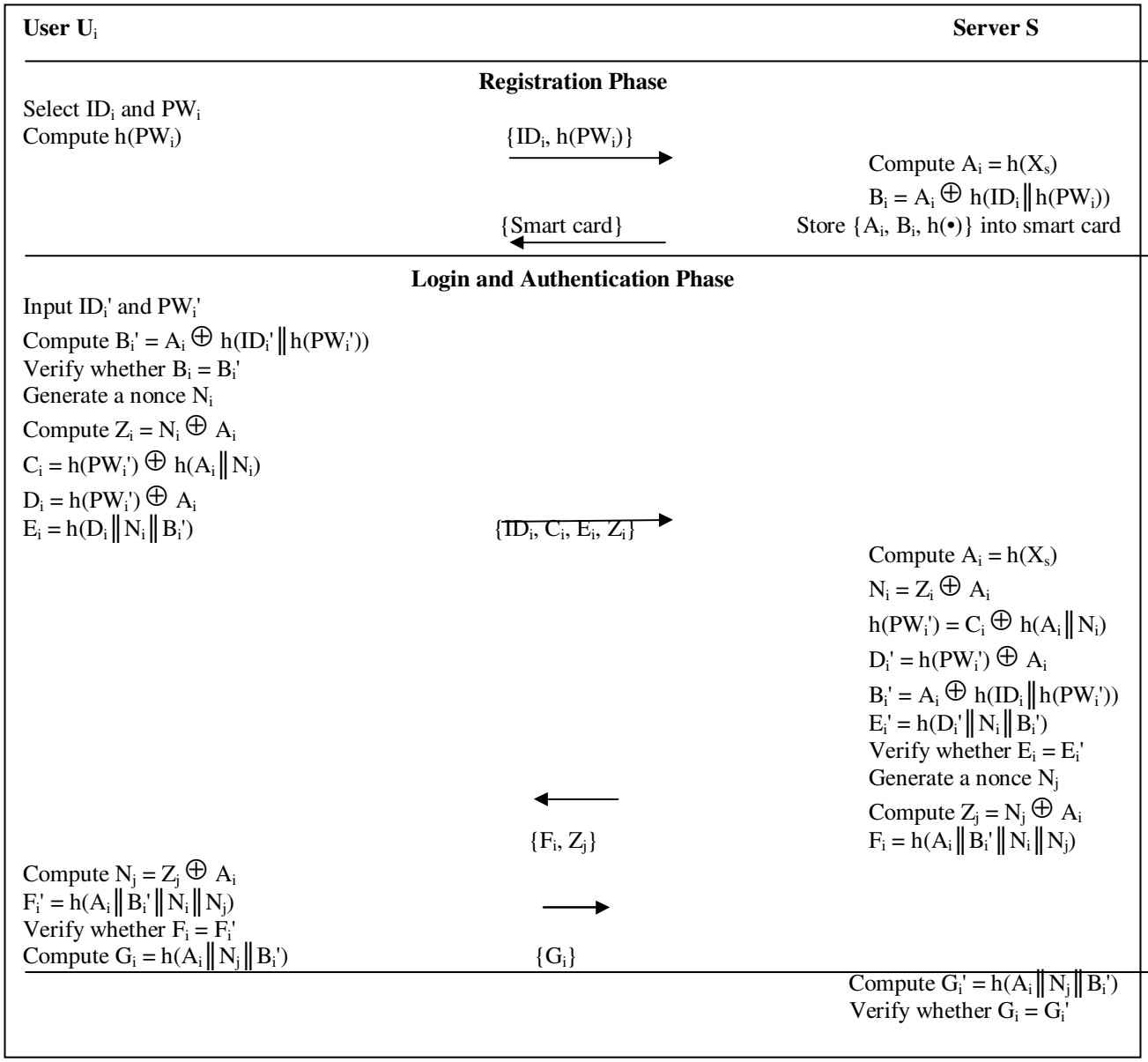

Figure1. The Proposed Scheme

Replay Attack

The scheme resists replay attack. Instead of timestamps, this scheme uses randomly generated nonces N_i and N_j which are not a part of login request message and their values differ among sessions. Thus, attackers cannot enter the system by resending messages previously transmitted by legal users.

Insider Attack

In the proposed scheme, during the registration phase, $h(PW_i)$ is sent to server S instead of PW_i. So, any insider of S cannot get user password PW_i. Hence, this scheme resists insider attack.

Reflection And Parallel Session Attack

Reflection and parallel session attacks are possible due to the symmetric

structure of messages transmitted between user U_i and the server S. This scheme employs asymmetric computations of communicating messages to resist reflection and parallel session attacks.

Attack On Perfect Forward Secrecy

In the scheme, the session key $SK = h(D_i \| N_i \| N_j \| B_i')$ is calculated using randomly generated nonces N_i and N_j which are different for each login session and are not a part of any of the transmitted messages between user U_i and the server S. Even if an attacker gets X_s, server's secret key, there is no way to get any information about present session key or previous session keys. Hence, the scheme provides perfect forward secrecy.

Smart Card Loss Attack

If due to an accident, someone lost their smart card, no one can impersonate the smart card owner to login the server. Without knowing the correct ID_i and PW_i of the user, an intruder cannot prepare a valid login request message even if he has a valid smart card.

Denning-Sacco Attack

If an attacker captures a session key then there is no way to get any information about nonces N_i and N_j or server's secret key X_s due to the property of one-way hash. As PW_i is not involved directly in the calculation of session key, no one can get user's password from the eavesdropped session key.

Stolen Verifier Attack

Here the server does not maintain any password or verification table to verify the user's login request, so the scheme is free from stolen verifier attack.

Denial-Of-Service Attack

If the user U_i inputs a wrong password by mistake, this password will be quickly detected by the card reader since reader compares $B_i' = A_i \oplus h(ID_i' \| h(PW_i'))$ with the stored B_i during the login phase. Hence, the scheme resists this type of Denial-of-Service attack.

Man-In-The-Middle Attack

In the proposed scheme, if an attacker intercepts the communicating messages between the user and the server then it will not generate any useful information because nonces N_i and N_j (used in the calculation of session key) are not a part of the communicating messages. Moreover, to alter Z_i or Z_j, one needs the value of A_i. Hence, the proposed scheme resists man-in-the-middle attack.

User Can Choose and Change the Password Securely Without Any Assistance from the Server

In the scheme, the card reader verifies the old password first in the password change phase. So, unauthorized users cannot change the authorized user's password even if they get the corresponding smart card.

The Scheme Solves Serious Time Synchronization Problem

The proposed scheme uses randomly generated nonces (different for each login session) instead of time-stamps to avoid time synchronization problem.

The Scheme Provides Session Key Generation

The scheme generates a session key $SK = h(D_i \| N_i \| N_j \| B_i')$ during the authentication phase which will be different for each login session.

Conclusion

This paper describes a new efficient and secure remote user authentication scheme using smart cards. It has been shown that the proposed scheme is more efficient, in terms of computational cost as it uses cryptographic one-way hash function only, and at the same time provides strong security. It prevents impersonation attack, online and offline password guessing attacks, replay attack, insider attack, reflection and parallel session attacks, attack on perfect forward secrecy, smart card loss attack, denning-sacco attack, stolen verifier attack, Denial-of-Service attack and man-in-the-middle attack. Moreover, the proposed scheme provides the following properties: user can choose and change the password securely without any assistance from the server, solves serious time synchronization problem, mutual authentication and establish a session key.

References

1. C. K. Chan and L. M. Cheng. (2000). "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, **46**, (4), 992-993.
2. C. K. Chan and L. M. Cheng(2002). "***Cryptanalysis*** of ***timestamp-based password authentication scheme",*** Computer & Security, 21 (1): 74-76.
3. Chien-Lung Hsu (2003). Security of two remote user authentication schemes using smart cards", IEEE Transactions on Consumer Electronics, 49(4): 1196-1198.
4. H.M. Sun (2000). An efficient remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, 46 (4): 958-961.
5. Hung-Yu Chien, Jinn-Ke Jan and Yuh-Min Tseng (2002). An efficient and practical solution to remote authentication: smart card", Computers & Security.21(4): 372-375.
6. J. J. Shen, C. W. Lin and M. S. Hwang (2003). A modified remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics.49(2):414-416.
7. Kai-Chi Leung, L. M. Cheng, Anthony S. Fong and Chi-Kwong Chan (2003). Cryptanalysis of a modified remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics.49(4): 1243-1245.
8. Leslie Lamport (1981). Password authentication with insecure communication", Communications of the ACM. 24(11): 770-772.
9. M. S. Hwang and L. H. Li (2000) A new remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics46(1): 28-30.
10. Manik Lal Das, Ashutosh Saxena and Ved P. Gulati (2004). dynamic ID-based remote user authentication scheme", IEEE Transactions on Consumer Electronics, 50(2):629-631.
11. Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi (2010). Comments on symmetric key encryption based smart card authentication scheme", 2nd International Conference on Computer Technology and Development (ICCTD-2010), November 2-4, Cairo, Egypt, pp. 482-484.
12. Ronggong Song (2010). Advanced smart card based password authentication protocol", Computer Standards & Interfaces.32(5-6): 321-325.
13. Wen-Her Yang and Shiuh-Pyng Shieh (1999). Password authentication schemes with smart cards", Computers & Security.**18**(8): 727-733.