Dynamic Encryption Key based Smart Card Authentication Scheme

Ravi Singh Pippal
Radharaman Institute of
Research and Technology
Ratibad, Bhopal, M.P.

Pradeep Gupta
Gwalior Engineering College
Gwalior, M.P.

Rakesh Singh
Gwalior Engineering College
Gwalior, M.P.

ABSTRACT

In order to keep away from difficulties associated with traditional password based authentication methods, smart card based authentication schemes have been widely used. It has already been accepted worldwide due to its low computational cost. However, most of these schemes are vulnerable to one or the other possible attack. This paper describes a new smart card authentication scheme using symmetric key cryptography, which covers all the identified security pitfalls and satisfies the needs of a user. Its security is based on encrypting the contents of all the communicating messages exchanged between remote user and the server. Moreover, it provides users to choose and change their passwords freely, mutual authentication and session key generation. In addition, it uses nonce instead of timestamp to resist replay attack. Security analysis proves that this scheme is secure against impersonation attack, password guessing attack, replay attack, reflection attack, parallel session attack, insider attack, attack on perfect forward secrecy, stolen verifier attack, smart card loss attack and man-in-the-middle attack. The proposed scheme can be easily extended to Internet protocol television broadcasting, Multi-server authentication, Wireless communication and Healthcare, where the user needs to access data from server.

Keywords

Authentication, Encryption, Nonce, Session key, Smart card.

1. INTRODUCTION

In traditional password based remote user authentication schemes, server keeps a verification table secretly in order to verify the authenticity of a user. Based on one way hash function, a password authentication scheme has been proposed to authenticate remote users [1]. However, this scheme has a security pitfall as an intruder can penetrate the server and modify the contents of the verification table. A remote login authentication scheme based on a geometric approach has been offered [2] and claimed that the scheme eliminates the use of verification table, provides security against impersonation attack and replay attack. Nevertheless, this scheme is vulnerable to impersonation attack [3]. An ID based scheme using RSA cryptosystem has been given [4]. However, it is exposed to impersonation attack [5]. By making use of ElGamal’s cryptosystem, a remote user authentication scheme has been offered [6] and claimed that the scheme is free from replay attack and maintaining verification table. Though, it is shown that the scheme has security flaws as an unauthorized user can easily forge a valid login request [7]. To improve efficiency, a remote user authentication scheme using one way hash function has been proposed [8]. However, it is found that the scheme is weak against offline and online password guessing attacks [9]. An improved scheme has also been suggested [10] to eliminate password guessing attacks. It is claimed that the scheme does not require any verification table and user can choose the password by itself. In addition, it provides mutual authentication between remote user and the server. Though, it is proved that the scheme is susceptible to parallel session attack [9].

A nonce based scheme has been given to solve time synchronization problem [11] and claimed that the scheme has an additional merit of session key generation. Nevertheless, it is analyzed that this scheme is weak against insider attack and user is not allowed to change the password freely. A dynamic ID based remote user authentication scheme using one way hash function has been proposed [12]. The authors claimed that their scheme allows users to choose and change the passwords freely. Moreover, it provides security against ID theft and resists forgery attack, replay attack, insider attack, stolen verifier attack and guessing attack. Nevertheless, it is found that the scheme is weak against guessing attack, insider attack and fails to provide mutual authentication [13]. An improved scheme has also been suggested to preclude these weaknesses. It is demonstrated that the scheme mentioned in [12] shows inadequacy to resist impersonation attack, offline and online password guessing attacks and has insecure password change phase [14]. Further improvement has also been recommended to defend these attacks. An efficient smart card authentication scheme based on symmetric key cryptography has been given [15] and claimed that the scheme provides security against impersonation attack, parallel session attack, replay attack and modification attack. Moreover, it provides mutual authentication and shared session key. Though, it is shown that the scheme is inadequate to resist Denial-of-Service attack and fails to provide perfect forward secrecy [16]. Recently, a biometrics based remote user authentication scheme using smart cards has been proposed [17]. The security of the scheme relies on the one way hash function, smart card and biometrics verification. It is claimed that the scheme permits users to change their passwords freely and provides mutual authentication. Moreover, it does not require synchronized clocks and resists replay attack, parallel session attack and impersonation attack. However, it is found that the scheme is insufficient to provide proper authentication and fails to resist man-in-the-middle attack [18]. An improved scheme has also been suggested to prohibit these security pitfalls.

All the schemes discussed so far have their pros and cons. This paper proposes a new smart card authentication scheme to resist all the identified attacks and satisfies the desires of a user. Its security depends on encrypting the contents of all the communicating messages exchanged between remote user and the server. The encryption key is generated dynamically for each session.

Rest of the paper is organized as follows. The proposed smart card authentication scheme is described in section 2. Section 3 demonstrates security analysis of the proposed scheme. Various applications where smart card is used are discussed in section 4, and at the end, section 5 concludes the paper.

2. PROPOSED SMART CARD AUTHENTICATION SCHEME

This section describes the proposed smart card authentication scheme. The notations used throughout this paper are summarized as follows.

U_i	:	remote user
ID_i	:	identity of U_i
PW_i	:	password chosen by U_i
S	:	authentication server
PW_i*	:	password guessed by the adversary
x	:	secret key of S
d	:	secret number of S
p	:	large prime number
g	:	primitive element
h(•)	:	cryptographic one way hash function
$\oplus$	:	bitwise XOR operation
$\|$	:	concatenation
N_1 (N_2)	:	random nonce generated by U_i (S)
$E_y/D_y[M]$	:	symmetric key encryption/decryption of 'M' with key 'y'
SKey	:	session key shared between U_i and S

The scheme consists of four phases: Registration phase, Login phase, Authentication phase and Password Change phase.

2.1 Registration Phase

In this phase, U_i selects ID_i and PW_i, computes $h(PW_i)$ and submits $\{ID_i, h(PW_i)\}$ to S over a secure channel. Once received the registration request from U_i, S computes $a_i = g^{h(PWi) \times h(d)} \bmod p$, $b_i = h(ID_i \| x)$ and issues a smart card over secure channel to U_i by storing $\{a_i, b_i, h(d), p, g, h(\bullet)\}$ into smart card memory.

2.2 Logic Phase

U_i inserts the smart card to the card reader and keys in ID_i and PW_i'. The reader computes $a_i' = g^{h(PWi') \times h(d)} \bmod p$ and checks whether computed a_i' equals stored a_i or not. If true, the card reader generates a random number r_s, computes $K_1 = r_s^{h(d)} \bmod p$, $K_2 = (r_s \times g^{IDi}) \bmod p$ and the encryption/decryption key $EDkey = h(K_1 \| h(d))$. The reader generates N_1, computes $y = g^{bi} \bmod p$, $c_i = y^{bi \times N1} \bmod p$, $d_i = y^{h(PWi) \times N1} \bmod p$, $e_i = (h(PW_i) + b_i \times h(ID_i \| a_i \| y \| c_i \| d_i \| N_1)) \bmod (p\text{-}1)$, $f_i = g^{h(PWi)} \bmod p$, $o_i = c_i \oplus d_i$, $M_1 = E_{EDkey}[e_i \| f_i \| o_i \| N_1]$ and sends the login request $\{ID_i, K_1, K_2, M_1\}$ to S.

2.3 Authentication Phase

Upon receiving the login request $\{ID_i, K_1, K_2, M_1\}$; S first checks the validity of ID_i to accept/reject the login request. If true, S computes

$$K_1' = (K_2^{h(d)})/(g^{IDi \times h(d)}) \bmod p. \quad \textbf{(1)}$$

$$K_1' = (((r_s \times g^{IDi}))^{h(d)})/(g^{IDi \times h(d)}) \bmod p. \quad \textbf{(2)}$$

$$K_1' = (r_s^{h(d)} \times g^{IDi \times h(d)})/(g^{IDi \times h(d)}) \bmod p. \quad \textbf{(3)}$$

$$K_1' = r_s^{h(d)} \bmod p. \quad \textbf{(4)}$$

Then, S verifies whether the received K_1 equals computed K_1' or not. If not, S rejects the login request otherwise, computes $EDkey = h(K_1 \| h(d))$, $[e_i \| f_i \| o_i \| N_1] = D_{EDkey}[M_1]$, $a_i = f_i^{h(d)} \bmod p$, $b_i = h(ID_i \| x)$, $y = g^{bi} \bmod p$, $c_i = y^{bi \times N1} \bmod p$, $d_i = c_i \oplus o_i$ and checks whether $g^{ei} = f_i \times y^{h(IDi \| ai \| y \| ci \| di \| N1)} \bmod p$ is true or not.

$$g^{ei} = g^{(h(PWi) + bi \times h(IDi \| ai \| y \| ci \| di \| N1))} \bmod p. \quad \textbf{(5)}$$

$$g^{ei} = g^{h(PWi)} \times g^{bi \times h(IDi \| ai \| y \| ci \| di \| N1)} \bmod p. \quad \textbf{(6)}$$

$$g^{ei} = g^{h(PWi)} \bmod p \times g^{bi \times h(IDi \| ai \| y \| ci \| di \| N1)} \bmod p. \quad \textbf{(7)}$$

$$g^{ei} = f_i \times y^{h(IDi \| ai \| y \| ci \| di \| N1)} \bmod p. \quad \textbf{(8)}$$

If equation (8) holds, S checks whether $y^{ei \times N1} = d_i \times c_i^{h(IDi \| ai \| y \| ci \| di \| N1)} \bmod p$ is true or not.

$$y^{ei \times N1} = y^{(h(PWi) + bi \times h(IDi \| ai \| y \| ci \| di \| N1)) \times N1} \bmod p. \quad \textbf{(9)}$$

$$y^{ei \times N1} = y^{h(PWi) \times N1} \times y^{bi \times h(IDi \| ai \| y \| ci \| di \| N1) \times N1} \bmod p. \quad \textbf{(10)}$$

$$y^{ei \times N1} = y^{h(PWi) \times N1} \bmod p \times y^{bi \times N1 \times h(IDi \| ai \| y \| ci \| di \| N1)} \bmod p. \quad \textbf{(11)}$$

$$y^{ei \times N1} = d_i \times c_i^{h(IDi \| ai \| y \| ci \| di \| N1)} \bmod p. \quad \textbf{(12)}$$

If both the equations (8) and (12) hold, S generates a nonce N_2, computes $X_1 = b_i \oplus N_1 \oplus N_2$, $X_2 = y^{N2} \bmod p$, $M_2 = E_{EDkey}[X_1 \| X_2]$ and sends the message $\{ID_i, M_2\}$ to U_i. After getting the message $\{ID_i, M_2\}$ from S, U_i computes $[X_1 \| X_2] = D_{EDkey}[M_2]$, $N_2 = b_i \oplus X_1 \oplus N_1$, $X_2' = y^{N2} \bmod p$ and checks whether X_2 and X_2' are equal or not. If it holds, S is authentic otherwise terminate the session. Subsequently, U_i computes $X_3 = y^{N1 \times N2} \bmod p$, $M_3 = E_{EDkey}[X_3]$ and sends $\{ID_i, M_3\}$ to S. Once the message $\{ID_i, M_3\}$ is received, S computes $[X_3] = D_{EDkey}[M_3]$, $X_3' = y^{N1 \times N2} \bmod p$ and checks whether X_3 and X_3' are equal or not. If it holds, mutual authentication is achieved. Both the parties agree upon a common shared session key $SKey = h(EDkey \| N_1 \| N_2)$.

2.4 Password Change Phase

This phase is invoked when U_i wants to change the password. U_i inserts the smart card to the card reader and keys in ID_i and PW_i'. The reader computes $a_i' = g^{h(PWi') \times h(d)} \bmod p$ and checks whether computed a_i' equals stored a_i or not. If true, U_i enters a new password PW_{inew}. The card reader computes $a_{inew} = g^{h(PWinew) \times h(d)} \bmod p$ and stores a_{inew} instead of a_i in the smart card memory. Thus, U_i can change the password without taking any assistance from S.

3. SECURITY ANALYSIS

This section presents an in-depth security analysis of the proposed smart card authentication scheme based on the following possible attacks.

3.1 Impersonation Attack

The login request contains $\{ID_i, K_1, K_2, M_1\}$ where $K_1 = r_s^{h(d)} \bmod p$, $K_2 = (r_s \times g^{IDi}) \bmod p$ and $M_1 = E_{EDkey}[e_i \| f_i \| o_i \| N_1]$. Therefore, attacker needs to guess the correct value of d to get the key ‘EDkey’ to masquerade as U_i. Let’s assume attacker guesses the correct value of d and succeeds in computing EDkey. It is difficult to derive $h(PW_i)$ from f_i because of discrete logarithm problem. In addition, it is not possible to extract the nonce value from the eavesdropped response message as the value of b_i is unknown. Moreover, S verifies the validity of login request by comparing equation (8) and (12) and accepts the login request only when both of them are equal else rejects the login request. If an attacker modifies any of the login request parameters, S easily detects them as both the equations are unsatisfied. Hence, attacker is unable to forge the login request to impersonate a valid U_i.

3.2 Password Change Phase

In the proposed scheme, $h(PW_i)$ is used to compute $e_i = (h(PW_i) + b_i \times h(ID_i \| a_i \| y \| c_i \| d_i \| N_1)) \bmod (p-1)$ and $f_i = g^{h(PWi)} \bmod p$. Let us assume that the adversary intercepts login request $\{ID_i, K_1, K_2, M_1\}$ during the transmission from U_i to S. It is hard to guess the key ‘EDkey’ to decrypt M_1 in order to get e_i, f_i and check whether each of the guessed passwords is correct or not. Moreover, to derive PW_i from f_i, adversary needs to solve the discrete logarithm problem and break the security of one way hash function. Therefore, the scheme is secure against password guessing attack.

3.3 Password Change Phase

An adversary may try to act as an authentic user by resending previously intercepted messages. This scheme uses random nonces N_1 and N_2 which are different from session to session. As a result, attackers cannot enter the system by resending the previously transmitted messages to impersonate legal users. Assume that the intercepted login request $\{ID_i, K_1, K_2, M_1\}$ is replayed to pass the authentication phase. Attacker is unable to retrieve N_2 correctly from the response message $\{ID_i, M_2\}$ to compute the correct message $\{ID_i, M_3\}$ for mutual authentication. Consequently, S rejects the message by comparing X_3 with X_3'.

3.4 Password Change Phase

To resist reflection and parallel session attacks, the given scheme employs asymmetric structure of communicating messages, i.e., $\{ID_i, K_1, K_2, M_1\}$, $\{ID_i, M_2\}$ and $\{ID_i, M_3\}$. There is no symmetry in the values of $M_1 = E_{EDkey}[e_i \| f_i \| o_i \| N_1]$, $M_2 = E_{EDkey}[X_1 \| X_2]$ and $M_3 = E_{EDkey}[X_3]$. Hence, attacker is unable to launch parallel session attack by replaying server response message as the user login request or reflection attack by resending user login request as the server response message.

3.5 Password Change Phase

When a smart card is lost or stolen, unauthorized user, who obtains U_i’s smart card, can guess the password of U_i by using password guessing attacks or impersonate U_i to login into S. In the proposed scheme, if U_i’s smart card is lost or stolen, no one can impersonate the smart card owner to login into S without knowing the correct ID_i and PW_i of U_i.

3.6 Password Change Phase

U_i’s secret information stored at S is under extensive threat from the attackers. In the proposed scheme, S keeps secret key ‘x’ and secret number ‘d’ to avoid maintaining verification table used to verify U_i’s login request. Hence, the scheme is secure against stolen verifier attack.

3.7 Password Change Phase

An insider of S can obtain U_i’s password during the registration phase and then impersonate U_i to access other servers if same password is used to access several servers. In this scheme, $h(PW_i)$ is sent to S instead of PW_i to resist insider attack. So, any insider of S cannot get U_i’s password PW_i.

3.8 Password Change Phase

In the proposed scheme, attacker is unable to find out the present session key or any of the previously used session keys from the eavesdropped messages as the values of EDkey, N_1 and N_2 are unknown to the attacker and it is infeasible to guess all these values simultaneously.

3.9 Password Change Phase

If an attacker intercepts the communicating messages between U_i and S, it does not generate any useful information as they are encrypted using encryption/decryption key ‘EDkey’. Attacker cannot pretend as U_i or S to authenticate each either of them since ‘EDkey’ is unknown. Moreover, to calculate the key, one needs to know the value of secret number ‘d’. Hence, the proposed scheme is secure against man-in-the-middle attack.

4. APPLICATIONS OF SMART CARDS

In addition to ID verification and access control, smart cards are currently used for a vast array of applications. The main promising uses of smart cards are as follows:

4.1 Internet Protocol Television Broadcasting

In Internet Protocol Television (IPTV) broadcasting, service providers scramble the program with conditional access system (CAS) after charging a subscription fee to the user. This avoids unauthorized users to receive the programs. A smart card (CA card) is used to decrypt the control words (CWs) and transfer them back to the set-top box (STB) to descramble the scrambled program. Therefore, it is necessary to develop a secure authentication scheme so that both the STB and CA card can achieve mutual authentication.

4.2 Wireless Communication

Wireless communication technology is experiencing fast growth, with the prospective to offer high-speed and high quality data exchange between mobile devices. Mobile users get the services from their home network through universal roaming technology in wireless networks. Before providing services, it is obvious that the foreign agent needs to authenticate the mobile users. Hence, a proper authentication scheme is needed to verify the legitimacy of a user. Due to the security and computational power, smart cards are used to provide authentication to the registered users while on roaming.

4.3 Healthcare

The use of smart cards is increasing in the healthcare sector due to their portability, robustness, flexibility and reliability. Smart cards store the information for a patient's history safely. Authorized persons can immediately access this information when needed and update the content also. Rapid patient verification allows instant insurance processing, refund and improving the treatment. It is a convenient way to carry data and helps in reduction of records maintenance cost.

5. CONCLUSION

This paper enlightens a more secure smart card authentication scheme. It has been shown that the proposed scheme provides stronger security as the contents of all the communicating messages exchanged between user and server are encrypted with a key generated by the user itself. An attacker cannot extract these contents from an eavesdropped message. The scheme provides security against impersonation attack, password guessing attack, replay attack, reflection attack, parallel session attack, insider attack, attack on perfect forward secrecy, stolen verifier attack, smart card loss attack, man-in-the-middle attack and solves time synchronization problem. Moreover, to accomplish user's needs, the proposed scheme has the following merits (i) user can choose and change the password without taking any assistance from the server. (ii) provides mutual authentication and common shared session key.

6. REFERENCES

[1] Lamport L.: Password authentication with insecure communication. Communications of the ACM, 24, 770-772 (1981).

[2] Wu T.C.: Remote login authentication scheme based on geometric approach. Computer Communications, 18, 959-963 (1995).

[3] Hwang M.S.: Cryptanalysis of a remote login authentication scheme. Computer Communications, 22, 742-744 (1999).

[4] Yang W.H., Shieh S.P.: Password authentication schemes with smart cards. Computers & Security, 18, 727-733 (1999).

[5] Chan C.K., Cheng L.M.: Cryptanalysis of timestamp-based password authentication scheme. Computers & Security, 21, 74-76 (2002).

[6] Hwang M.S., Li L.H.: A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46, 28-30 (2000).

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

[8] Sun H.M.: An efficient remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46, 958-961 (2000).

[9] Hsu C.L.: Security of two remote user authentication schemes using smart cards. IEEE Transactions on Consumer Electronics, 49, 1196-1198 (2003).

[10] Chien H.Y., Jan J.K., Tseng Y.M.: An efficient and practical solution to remote authentication: smart card. Computers & Security, 21, 372-375 (2002).

[11] Juang W.S.: Efficient password authenticated key agreement using smart cards. Computers & Security, 23, 167-173 (2004).

[12] Das M.L., Saxena A., Gulati V.P.: A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics, 50, 629-631 (2004).

[13] Liao I.E., Lee C.C., Hwang M.S.: Security enhancement for a dynamic ID-based remote user authentication scheme. International Conference on Next Generation Web Services Practices (2005).

[14] Giri D., Srivastava P.D.: Cryptanalysis and improvement of a remote user authentication scheme using smart cards. International Symposium on Electronic Commerce and Security, 355-361 (2008).

[15] Song R.: Advanced smart card based password authentication protocol. Computer Standards & Interfaces, 32, 321-325 (2010).

[16] Pippal R.S., Jaidhar C. D., Tapaswi S.: Comments on symmetric key encryption based smart card authentication scheme. 2nd International Conference on Computer Technology and Development, 482-484 (2010).

[17] Li C.T., Hwang M.S.: An efficient biometrics-based remote user authentication scheme using smart cards, Journal of Network and Computer Applications, 33, 1-5 (2010).

[18] Li X., Niu J.W., Ma J., Wang W.D., Liu C.L.: Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards, Journal of Network and Computer Applications, 34, 73-79 (2011).