SHODH SANGAM - A RKDF University Journal of Science and Engineering
Volume 01, No. 01, 2018

Identifying Weak Spots of Three Provably Secure Smart Card Authentication Schemes

Ravi Singh Pippal
Vedica Institute of Technology, RKDF University, Bhopal
ravesingh@gmail.com

Abstract. With the development of networking technologies, authentication is becoming an essential security feature for systems that allow remote access over insecure channel. It determines the legitimacy of the communicating parties. Various elegant smart card authentication schemes have been proposed from time to time. However, most of these authentication schemes suffer from one or the other possible attack and fail to provide adequate security. Recently, Khan et al., Yeh et al. and Kim and Lee proposed their authentication schemes using smart card and claimed that their schemes are secure against well known attacks. This paper analyzes the security performance of these three authentication schemes and demonstrates that the schemes are vulnerable to identified attacks.

Keywords: Authentication, Cryptanalysis, Guessing, Impersonation, Smart card.

1 Introduction

Authentication is one of the vital challenging tasks to securely distribute or exchange information over insecure channel. It ensures the origin of a message correctly identified and gives an assurance that the identity is not a fake. To achieve this, password based authentication schemes have been widely used due to its convenience and usability. Lamport [1] first proposed a remote user authentication scheme using passwords for insecure communication. However, this scheme is inefficient as well as insecure. In this scheme, the size of the verification table is directly proportional to the number of users i.e. its size increases as the number of users increases. Maintaining such an enormous verification table increases burden to the server. Moreover, if an intruder breaks into the server; the contents of the verification table can be easily modified. To resist all the possible attacks on the verification tables, smart card based password authentication scheme has been proposed without verification table at the server [2]. It consists of three phases namely; registration phase, login phase and authentication phase. The registration phase is invoked whenever new user registers in the server. Upon receiving the registration request, server issues a smart card to user by storing the user as well as server credentials into smart card memory. The login phase and authentication phase are invoked at any time user login into the server. After receiving the login request, server checks the validity of the login request to authenticate the user.

1.1 Contribution of this paper

In view of the fact, most of the existing smart card authentication schemes have their pros and cons. This paper reviews recently proposed three smart card authentication schemes

(Khan et al. [16], Yeh et al. [13], Kim and Lee [19]). Each scheme consists of three phases namely Registration phase, Login phase and Verification phase. In this paper, it is proved that each scheme is vulnerable to one or the other attacks.

The remainder of this paper is organized as follows. Section 2 reviews related literatures. Section 3 describes cryptanalysis of Khan et al.'s scheme. Security flaws of Yeh et al.'s scheme are demonstrated in section 4. Section 5 shows the vulnerabilities of Kim and Lee's scheme. Finally, section 6 concludes the paper.

2 Literature Review

Many fascinating smart card authentication schemes have been proposed during the last decade [3, 5, 7, 9-17, 19]. Yang and Shieh [3] proposed an ID based scheme using RSA cryptosystem. They claimed that their scheme is free from replay attack and maintaining verification table. To avoid time synchronization problem, they suggested a nonce based scheme also. Nevertheless, it is vulnerable to impersonation attack [4]. Hwang and Li [5] gave a remote user authentication scheme using ElGamal's cryptosystem and claimed that their scheme provides security against replay attack and eliminates the use of verification table. However, this scheme has a security weakness as an unauthorized user can easily impersonate a legitimate user [6]. Moreover, it increases the computation and communication cost [7]. To improve efficiency, Sun [7] presented a remote user authentication scheme using one way hash function and claimed that the scheme resists impersonation and replay attacks. Its major drawbacks are i) Password is issued by the server which results the user not to choose and change the password freely. ii) No mutual authentication. In addition, Hsu [8] found that Sun's scheme is insecure against offline and online password guessing attacks.

All the schemes previously discussed do not provide mutual authentication between remote user and the server. Chien et al. [9] suggested an improved scheme to get rid of password guessing attacks and claimed that their scheme avoids verification table, provides users to choose the password and mutual authentication. However, Hsu [8] proved that Chien et al.'s scheme is weak against parallel session attack. Moreover, user is not allowed to change the password freely. To withstand insider attack and reflection attack, Ku and Chen [10] proposed an improvement over Chien et al.'s scheme and claimed that their scheme allows users to change the password freely without any assistance from the server. Yoon et al. [11] found that Ku and Chen's scheme is weak against parallel session attack and it has insecure password change phase. They suggested further improvement also to get rid of these drawbacks. Later on, Hsiang and Shih [12] demonstrated that Yoon et al.'s scheme is vulnerable to parallel session attack, offline password guessing attack and masquerading attack. They gave their improved scheme to overcome these security pitfalls. Recently, Yeh et al. [13] found that Hsiang and Shih's scheme is still under the threat of masquerading attack and password guessing attack. To preclude these security pitfalls, they presented an efficient scheme and claimed that their scheme is free from masquerade attack and password guessing attack.

Das et al. [14] proposed a dynamic ID based remote user authentication scheme using one way hash function. They claimed that the scheme allows users to choose and change their passwords freely. Moreover, it provides security against ID theft, replay attack, forgery attack, guessing attack, insider attack and stolen verifier attack. However, Wang et al. [15]

pointed out that Das et al.'s scheme does not provide mutual authentication and is password independent. To rule out these security flaws, they proposed an enhanced scheme. Though, Khan et al. [16] found that Wang et al.'s scheme does not allow users to choose the password and it is insecure against insider attack. Also, it fails to provide user anonymity, revocation of lost or stolen smart card and no provision for session key establishment. To preclude these security pitfalls, they also suggested an improved scheme over Wang et al.'s scheme. Song [17] presented a secure smart card authentication scheme based on symmetric key cryptography and claimed that the scheme is secure against impersonation attack, parallel session attack, replay attack and modification attack. In addition, it provides mutual authentication and shared session key. However, Pippal et al. [18] demonstrated that Song's scheme is not good enough to resist Denial of Service attack and provide perfect forward secrecy. To improve efficiency, Kim and Lee [19] proposed their scheme based on one way hash function.

3 Cryptanalysis of Khan et al.'s Scheme

This section briefly reviews Khan et al.'s scheme and shows the possible attacks for it. The notations used rest of paper is summarized in Table 1.

Table 1. Notations used in this paper.

Symbols	Description
U_i	Remote user
S	Authentication Server
U_a	Attacker
ID_i	Identity of U_i
PW_i	Password chosen by U_i
x	Secret key of S
T_u	U_i's current system timestamp
T_s	S's current system timestamp
T_a	U_a's current system timestamp
S_K	Shared session key between U_i and S
h(•)	Secure one way hash function
||	Message concatenation operation
⊕	Exclusive-or operation

3.1 Review of Khan et al.'s scheme

The scheme consists of three phases: Registration phase, Login phase and Verification phase. The Server 'S' maintains two secrets named as 'x' and 'y'.

3.1.1 Registration phase

In this phase, U_i selects ID_i, PW_i, generates a random number r to compute $RPW = h(r||PW_i)$ and submits $\{ID_i, RPW\}$ to S over secure channel. Upon receiving the registration request from U_i, S checks whether the received ID_i is already in the database or not. If not, S checks the registration record of U_i. S sets value of $N = 0$ if U_i is a new user else sets $N = 1$ and stores ID_i and N in the database. S computes $J = h(x||IDU)$, $L = J \oplus RPW$ to store into smart card memory and issues it over a secure channel, where $IDU = (ID_i||N)$. U_i stores random number 'r' into the smart card memory. After completion of storing operation, smart card is ready to use at time.

3.1.2 Login phase

U_i inserts the smart card to the card reader and keys in ID_i and PW_i. Smart card computes $RPW = h(r||PW_i)$, $J = L \oplus RPW$, $C_1 = h(T_u||J)$, where T_u is current timestamp, $AID_i = ID_i \oplus h(y||T_u||d)$, where AID_i is anonymous identity and sends the login request $m = \{AID_i, T_u, d, C_1\}$ to S.

3.1.3 Verification phase

Upon receiving the login request $m = \{AID_i, T_u, d, C_1\}$; S first checks the validity of T_u to accept/reject the login request. If true, S computes $ID_i = AID_i \oplus h(y||T_u||d)$ and checks the validity of ID_i. If ID_i is valid, gets the value of N from its database, computes $IDU = (ID_i||N)$, $J = h(x||IDU)$ and checks whether $h(T_u||J)$ equals received C_1 or not. If equal, U_i is authentic otherwise rejects the login request. S gets the current timestamp T_s, computes $C_2 = h(C_1 \oplus J \oplus T_s)$ and sends the message $\{C_2, T_s\}$ to U_i for mutual authentication. After receiving, U_i checks the validity of T_s. If true, computes $h(C_1 \oplus J \oplus T_s)$ and checks whether it is equal to received C_2 or not. If it holds, both U_i and S compute the session key $S_K = h(C_2 \oplus J)$ for further operations.

3.2 Vulnerabilities of Khan et al.'s scheme

Khan et al.'s scheme has the following security vulnerabilities, i.e. server impersonation attack, weak session key generation and undetectable wrong password in the login phase.

3.2.1 Server impersonation attack

Attacker U_a intercepts the login request $m = \{AID_i, T_u, d, C_1\}$ transmitted from U_i to S. U_a guesses the value of J', computes $C_1' = h(T_u||J')$ and checks whether $C_1' = C_1$ or not. If not, U_a tries all the combinations for J'. After successful guessing, U_a gets current timestamp T_a, computes $C_2' = h(C_1' \oplus J' \oplus T_a)$ and sends the message $\{C_2', T_a\}$ to U_i for mutual authentication. Once the message is received, U_i checks the validity of T_a, computes $h(C_1' \oplus J' \oplus T_a)$ and checks whether it is equal to received C_2' or not which is obviously true. Hence, attacker U_a can easily masquerade as a legitimate server S.

3.2.2 Weak session key generation

Session key is used to secure communication between user and server and it must be different from session to session. This scheme shows inadequacy to generate session key securely. After successful guessing of J' (as discussed above), attacker intercepts mutual authentication message $\{C_2, T_s\}$ and computes the session key $S_K = h(C_2 \oplus J')$.

3.2.3 Lack of early wrong password detection

To check whether the requested user is a legitimate bearer of smart card, password needs to be verified at the user side prior to login request creation. In this scheme, attacker can create invalid login request by entering wrong password which will be detected only at the server side not at the user side. Hence, it leads to Denial of Service attack.

4 Cryptanalysis of Yeh et al.'s Scheme

Yeh et al. demonstrates security vulnerabilities of Hsiang and Shih's scheme. To overcome the identified security flaws, enhanced scheme is also proposed. This section briefly reviews Yeh et al.'s enhanced scheme over Hsiang and Shih's scheme and then demonstrates the possible weaknesses.

4.1 Review of Yeh et al.'s scheme

4.1.1 Registration phase

In this phase, U_i selects ID_i, PW_i, generates a random number 'b' to compute $h(b \oplus PW_i \oplus ID_i)$ and submits $\{ID_i, h(PW_i), h(b \oplus PW_i \oplus ID_i)\}$ to S over a secure channel. Upon receiving the registration request from U_i, S creates a new entry with a value $m = 0$ for U_i in its database or sets $m = m+1$. S computes $EID = (ID_i \| m)$, $P = h(EID \oplus x)$, $R = P \oplus h(b \oplus PW_i \oplus ID_i)$, $V = h(P \oplus h(PW_i))$ and issues smart card to U_i by storing $\{V, R, h(\bullet)\}$ into smart card memory over secure channel. The random number 'b' generated by U_i also stored into the smart card memory.

4.1.2 Login phase

U_i inserts the smart card to the card reader and keys in ID_i and PW_i. The smart card gets the current timestamp T_u, computes $C_1 = R \oplus h(b \oplus PW_i \oplus ID_i)$, $C_2 = h(C_1 \oplus T_u)$ and sends the login request $\{h(ID_i), C_2, T_u\}$ to S.

4.1.3 Verification phase

After receiving the login request $\{h(ID_i), C_2, T_u\}$; S checks the validity of $h(ID_i)$ and T_u to accept/reject the login request. If true, S computes $h(h(EID \oplus x) \oplus T_u)$ and compares it with the received C_2. If both of these values are equal, U_i is authentic otherwise rejects the login request. S gets the current timestamp T_s, computes $C_3 = h(h(EID \oplus x) \oplus h(T_s))$ and sends the message $\{C_3, T_s\}$ to U_i in order to achieve mutual authentication. Once the message is received, U_i checks the validity of T_s. If true, computes $h(C_1 \oplus h(T_s))$ and checks whether it is equal to received C_3 or not. If it holds, both U_i and S compute the session key $S_K = h(h(EID \oplus x) \oplus ID_i \oplus ID_s \oplus T_s) = h(C_1 \oplus ID_i \oplus ID_s \oplus T_s)$ to securely communicate with each other.

4.2 Vulnerabilities of Yeh et al.'s scheme

Yeh et al.'s improved scheme over Hsiang and Shih's scheme is exposed to user and server impersonation attacks. The details of these security weaknesses are as follows.

4.2.1 User impersonation attack

Attacker U_a intercepts the login request $\{h(ID_i), C_2, T_u\}$. U_a guesses the value of C_1', computes $C_2' = h(C_1' \oplus T_u)$ and checks whether $C_2' = C_2$ or not. After successful guessing, U_a

gets current timestamp T_a, computes $C_2'' = h(C_1' \oplus T_a)$ and sends the login request $\{h(ID), C_2'', T_a\}$ to S. This will clearly pass the authentication phase and U_a mimics as legitimate user U_i.

4.2.2 Server impersonation attack

After guessing the correct value of C_1', U_a gets current timestamp T_a, computes $C_3' = h(C_1' \oplus h(T_a))$ and sends the message $\{C_3', T_a\}$ to U_i for mutual authentication. Upon receiving, U_i checks the validity of T_a, computes $h(C_1' \oplus h(T_a))$ and checks whether it is equal to received C_3' or not which is obviously true. In this way, U_a can easily masquerade as legitimate server S.

5 Cryptanalysis of Kim and Lee's Scheme

This section briefly reviews Kim and Lee's scheme and then demonstrates the possible security weaknesses. In Kim and Lee's scheme, S maintains two secrets 'x' and 'r'.

5.1 Review of Kim and Lee's scheme

5.1.1 Registration phase

In this phase, U_i selects ID_i, PW_i, generates a random number b to compute $APW_i = h(b \oplus PW_i)$ and submits $\{ID_i, APW_i\}$ to S over a secure channel. After receiving the registration request, S computes $T_i = h(ID_i||x)$, $V_i = T_i \oplus h(ID_i||APW_i)$, $H_i = h(T_i)$, $A_i = h(ID_i \oplus x \oplus r)$, $B_i = A_i \oplus APW_i$ and issues smart card over secure channel to U_i by storing $\{V_i, H_i, B_i, h(\bullet)\}$ into smart card memory. The random number 'b' generated by U_i also stored into the smart card memory.

5.1.2 Login phase

U_i inserts the smart card to the card reader and keys in ID_i and PW_i. The smart card computes $APW_i = h(b \oplus PW_i)$, $T_i = V_i \oplus h(ID_i||APW_i)$, $H_i' = h(T_i)$ and checks whether H_i' is equal to the stored H_i or not. If true, U_i is the legitimate bearer of smart card. The smart card gets the current timestamp T_u to compute $A_i = B_i \oplus APW_i$, $C_1 = h(A_i \oplus T_u)$ and sends the login request $\{ID_i, C_1, T_u\}$ to S.

5.1.3 Verification phase

Upon receiving the login request $\{ID_i, C_1, T_u\}$; S checks the validity of T_u. If it does not hold, S rejects the login request otherwise computes $A_i' = h(ID_i \oplus x \oplus r)$, $C_1' = h(A_i' \oplus T_u)$ and compares it with the received C_1. If both are equal, U_i is authentic. S gets the current timestamp T_s, computes $C_2 = h(A_i' \oplus T_s)$ and sends the message $\{C_2, T_s\}$ to U_i for mutual authentication. After receiving, U_i checks the validity of T_s. If true, computes $C_2' = h(A_i \oplus T_s)$ and compares it with the received C_2. If both are equal, mutual authentication is achieved between U_i and S.

5.2 Vulnerabilities of Kim and Lee's scheme

Kim and Lee's scheme could be better influenced after resolving the security flaws which are user impersonation attack, server impersonation attack and absence of session key generation. The details of these security drawbacks are as follows.

5.2.1 User impersonation attack

U_a intercepts the login request $\{ID_i, C_1, T_u\}$, guesses the value of A_i', computes $C_1' = h(A_i' \| T_u)$ and checks whether $C_1' = C_1$ or not. After successful guessing of A_i', U_a gets current timestamp T_a, computes $C_1'' = h(A_i' \| T_a)$ and sends the login request $\{ID_i, C_1'', T_a\}$ to S for authentication. This will clearly pass the authentication phase.

5.2.2 Server impersonation attack

Once the value of A_i' is successfully guessed (as previously discussed), U_a gets current timestamp T_a, computes $C_2' = h(A_i' \oplus T_a)$ and sends the message $\{C_2', T_a\}$ to U_i in order to achieve mutual authentication. After receiving, U_i checks the validity of T_a, computes $h(A_i' \oplus T_a)$ and checks whether it is equal to received C_2' or not which is obviously true. Hence, U_a can easily mimic as legitimate server S.

5.2.3 No session key generation

Moreover, this scheme does not support session key generation used to secure further communication between U_i and S.

In timestamp based authentication schemes, the clock of server and all registered users need to be synchronized. In addition, transmission delay of the login request has to be limited which is inefficient for real world applications. All the three schemes discussed (Khan et al. [16], Yeh et al. [13], Kim and Lee [19]) fail to solve this issue.

6 Conclusion

This paper pointed out the imperfection of three provably secure remote user authentication schemes using smart cards. It is clear that all the schemes discussed (Khan et al. [16], Yeh et al. [13], Kim and Lee [19]) show inadequacy to resist the identified attacks. The steps used to show the security vulnerability lends to design a secure and efficient smart card authentication scheme which will be used for practical applications.

Acknowledgements

The author would like to thank Vedica Institute of Technology, RKDF University, Bhopal, India for providing the academic support.

References

1. Lamport L.: Password authentication with insecure communication. Communications of the ACM, 24, 770-772 (1981).
2. Chang C.C., Wu T.C.: Remote password authentication with smart cards. IEE Proceedings E: Computers and Digital Techniques, pp. 165-168 (1981).
3. Yang W.H., Shieh S.P.: Password authentication schemes with smart cards. Computers & Security, 18, 727-733 (1999).
4. Chan C.K., Cheng L.M.: Cryptanalysis of timestamp-based password authentication scheme. Computers & Security, 21, 74-76 (2002).
5. Hwang M.S., Li L.H.: A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46, 28-30 (2000).
6. 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).
7. Sun H.M.: An efficient remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46, 958-961 (2000).
8. Hsu C.L.: Security of two remote user authentication schemes using smart cards. IEEE Transactions on Consumer Electronics, 49, 1196-1198 (2003).
9. 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).
10. Ku W.C., Chen S.M.: Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 50, 204-207 (2004).
11. Yoon E.J., Ryu E.K., Yoo K.Y.: Further improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 50, 612-614 (2004).
12. Hsiang H.C., Shih W.K.: Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards. Computer Communications, 32, 649-652 (2009).
13. Yeh K.H., Sub C., Loa N.W., Li Y., Hung Y.X.: Two robust remote user authentication protocols using smart cards. The Journal of Systems and Software, 83, 2556-2565 (2010).
14. 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).
15. Wang Y.Y., Liu J.Y., Xiao F.X., Dan J.: A more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, 32, 583-585 (2009).
16. Khan M.K., Kim S.K., Alghathbar K.: Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'. Computer Communications, 34, 305-309 (2011).
17. Song R.: Advanced smart card based password authentication protocol. Computer Standards & Interfaces, 32, 321-325 (2010).
18. 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, pp. 482-484 (2010).
19. Kim H.S., Lee S.W.: Robust remote user authentication scheme using smart cards. Journal of Security Engineering, 7, 495-502 (2010).