CRYPTANALYSIS OF TYAGI ET AL.'S SMART CARD AUTHENTICATION SCHEME

Priyanka Sinha[1] and Akhilesh Bansiya[2]
Department of Computer Science & Engineering
Vedica Institute of Technology
RKDF University, Bhopal

Abstract :

A robust multi-server smart card authentication scheme has been proposed by Tyagi et al. using cryptographic one-way hash function and the discrete logarithm problem. The author claimed that this scheme eliminates the employment of verification table, permits users to settle on and alter the password firmly while not taking any help from the server or registration center, provides mutual authentication and establishes a typical session key between user and also the server. Additionally, the proposed scheme withstands server impersonation attack, user impersonation attack, reflection and parallel session attacks, replay attack, stolen verifier attack, password guessing attack, smart card loss attack and insider attack. However, it has been observed that the scheme proposed by Tyagi et al. is susceptible to impersonation attack.

Key words: Authentication, Encryption, Impersonation, Security, Smart Card

1. INTRODUCTION

Since last few years, electronic transactions carried out over the Internet are gaining popularity and are widely accepted in the world. To keep data secure during its transmission over insecure network, sufficient security measures are needed. One of the imperative key factors in security is authentication which is required for every transaction. It is the basic requirement prior to allow the user accesses the server. A lot of work has been done to secure the information from unauthorized access [1, 2]. One among various authentication schemes is password supported authentication scheme. In conventional password supported authentication schemes, server keeps verification table securely to verify the authenticity of a user. Every user has its own credentials, identifier (ID) and password (PW). Whenever a user desires to access resources from a server, he/she has to present ID and PW to pass the authentication phase. The server verifies the PW corresponding to the ID from verification table and authenticates the user if the submitted password matches with the stored password.

However, this technique is insecure since an attacker can access the contents of the verification table to break down the entire system. Storing the password in hashed format is one of the solutions [3]. The major drawback in this approach is the verification table size which is directly relative to the number of users; as a result security risk on the server increases. To resist potential attacks on the verification tables, smart card based password authentication scheme has been suggested [4]. In this authentication scheme, server needs not to preserve any verification table. It maintains only its own long term secret key(s).

Smart cards are similar to shape and size of credit cards embedded with microprocessors capable of holding important information of the person who holds them. They are safer than magnetic strip cards. Smart card provides authentication and identification for the users. Smart cards are widely accepted in Europe for the healthcare sector, compared to the rest of the world. In fact, Europe is the biggest consumer of smart card technology in the world and healthcare is the third-largest sector in the world to deploy smart cards, behind pay phones and Global System for Mobile Communications (GSM) applications. It has been suggested that a minimum level of security should be provided by the current European smart card legislation. To achieve this, a secure secret key storage is required. Smart cards are the perfect option to offer the necessary level of security.

Since last two decades, various smart card based authentication schemes have been proposed [5–7, 9, 10, 12–17]. To overcome the weaknesses in multi-server environment, a nonce based scheme using one-way hash function and symmetric cryptosystem was proposed [18]. It has all the previous advantages as well as server and user authenticate each other and generate a session key agreed between them. Nevertheless, it demonstrates insider attack and does not offer forward secrecy [19]. Further improvement was also proposed [20]. They claimed that their scheme provides mutual authentication between the remote server and the user, resists server spoofing attack, stolen-verified attack, replay attack, smart card loss attack and achieves forward secrecy.

A dynamic ID based remote user authentication scheme has been given to provide user anonymity using one way hash function [21]. It has been proved that the scheme fails to provide forward secrecy [22]. It has been pointed out that the scheme [21] does not oppose insider attack, server spoofing attack, impersonation attack, registration centre spoofing attack, not succeeds to afford mutual authentication and further improvement has been proposed [23]. Though, Sood et al. [24] showed that Hsiang-Shih's improved scheme fails to provide security against replay attack, impersonation attack, stolen smart card attack and has incorrect password change phase.

Contribution of this Paper :

In 2012, Tyagi suggested robust multi-server authentication scheme using smart cards [25]. Its security is based on cryptographic one-way hash function and the discrete logarithm problem. This scheme permits remote users to access multiple servers while not singly registering with every server. Moreover, it eliminates the employment of verification table, permits users to settle on and alter the firmly while not taking any help from the server or registration center, provides mutual authentication and establishes a typical session key between user and the server. To boot, the proposed scheme withstands all the potential attacks. However, this paper demonstrates the weaknesses present in Tyagi et al.'s scheme.

The rest of the paper is structured as follows. Review of Tyagi et al.'s scheme is described in section 2. Security flaws of Tyagi et al.'s scheme are discussed in Section 3. At last, conclusion has been given by section 5.

2. REVIEW OF TYAGI ET AL.'S SCHEME

The scheme proposed by Tyagi et al. [25] has four phases: Registration phase, Login phase, Authentication phase and Password Change phase. Suppose, there are n servers with which the new user can communicate. The notations used throughout this paper are summarized as follows:

RC	→	registration center
U_i	→	i^{th} remote user
ID_i	→	identity of U_i
PW_i	→	password chosen by U_i
S_j	→	j^{th} authentication server ($1 \leq j \leq n$)
SID_j	→	identity of S_j
x	→	secret key of RC
d	→	secret number of RC
p	→	large prime number
g	→	primitive element
h(•)	→	cryptographic one way hash function
$\oplus$	→	bitwise XOR operation

$SKey_{ij}$ → session key shared between U_i and S_j

N_1 → random nonce generated by U_i

N_2 → random nonce generated by S_j

Registration Phase :

This phase is divided into two sub-phases: Server Registration phase and User Registration phase.

Server Registration phase: In this phase, S_j selects SID_j and submits it to RC over a secure channel. Once getting, RC computes the server secret parameter $SS_j = (g^{h(SID_j, h(x))} \bmod p) \oplus h(d)$ and sends $\{SS_j, h(d)\}$ to S_j through a secure channel.

User Registration phase: U_i selects ID_i and PW_i, computes $h(PW_i)$ and submits $\{ID_i, h(PW_i)\}$ to RC over a secure channel. Once the registration request is received, RC computes $x_i = (g^{h(PW_i)} \bmod p) \oplus h(x)$, $y_i = h(ID_i, h(d))$, $z_i = y_i \oplus h(PW_i)$ and issues a smart card over secure channel to U_i by storing $\{x_i, y_i, z_i, p, g, h(\bullet)\}$ into smart card memory.

Login Phase :

U_i inserts the smart card to the card reader and keys in ID_i and PW_i. The reader computes $z_i' = y_i \oplus h(PW_i')$ and checks whether computed z_i' equals stored z_i or not. If true, reader generates a random nonce N_1, computes $a_i = g^{y_i} \bmod p$, $b_i = a_i^{y_i \times N1} \bmod p$, $c_i = a_i^{h(PW_i) \times N1} \bmod p$, $d_i = g^{h(PW_i)} \bmod p$, $Q_j = g^{h(SID_j, (x_i \oplus d_i))} \bmod p$, $e_i = (h(PW_i) + y_i \times h(ID_i, a_i, b_i, c_i, d_i, N_1, Q_j)) \bmod (p-1)$ and sends the login request $\{ID_i, SID_j, d_i, e_i, N_1\}$ to S_j.

Authentication Phase :

Upon receiving the login request $\{ID_i, SID_j, d_i, e_i, N_1\}$; S_j first checks the validity of ID_i to accept/reject the login request. If true, S_j computes $y_i = h(ID_i, h(d))$, $a_i = g^{y_i} \bmod p$, $b_i = a_i^{y_i \times N1} \bmod p$, $c_i = d_i^{y_i \times N1} \bmod p$, $Q_j = SS_j \oplus h(d)$ and checks whether $g^{e_i} = d_i \times a_i^{h(ID_i, a_i, b_i, c_i, d_i, N1, Q_j)} \bmod p$ is true or not.

$$g^{e_i} = g^{(h(PW_i) + y_i \times h(ID_i, a_i, b_i, c_i, d_i, N1, Q_j))} \bmod p,$$

$$g^{e_i} = g^{h(PW_i)} \times g^{y_i \times h(ID_i, a_i, b_i, c_i, d_i, N1, Q_j)} \bmod p,$$

$$g^{e_i} = g^{h(PW_i)} \bmod p \times g^{y_i \times h(ID_i, a_i, b_i, c_i, d_i, N1, Q_j)} \bmod p,$$

$$g^{e_i} = d_i \times a_i^{h(ID_i, a_i, b_i, c_i, d_i, N1, Q_j)} \bmod p.$$

If this equation holds, S_j checks whether $a_i^{ei \times N1} = c_i \times b_i^{h(IDi, ai, bi, ci, di, N1, Qj)} \bmod p$ is true or not.

$a_i^{ei \times N1} = a_i^{(h(PWi) + yi \times h(IDi, ai, bi, ci, di, N1, Qj)) \times N1} \bmod p,$

$a_i^{ei \times N1} = a_i^{h(PWi) \times N1} \times a_i^{yi \times h(IDi, ai, bi, ci, di, N1, Qj) \times N1} \bmod p,$

$a_i^{ei \times N1} = a_i^{h(PWi) \times N1} \bmod p \times a_i^{yi \times N1 \times h(IDi, ai, bi, ci, di, N1, Qj)} \bmod p,$

$a_i^{ei \times N1} = c_i \times b_i^{h(IDi, ai, bi, ci, di, N1, Qj)} \bmod p.$

If both the equations hold, S_j generates a nonce N_2, computes $X_1 = y_i \oplus N_1 \oplus N_2$, $X_2 = Q_j^{N2} \bmod p$ and sends the message $\{ID_i, X_1, X_2\}$ to U_i. After getting the message $\{ID_i, X_1, X_2\}$ from S_j, U_i computes $N_2 = y_i \oplus X_1 \oplus N_1$, $X_2' = Q_j^{N2} \bmod p$ and checks whether X_2 and X_2' are equal or not. If it holds, S_j is authentic otherwise terminate the session. Subsequently, U_i computes $X_3 = Q_j^{N1 \times N2} \bmod p$ and sends $\{ID_i, X_3\}$ to S_j. Once the message $\{ID_i, X_3\}$ is received, S_j computes $X_3' = Q_j^{N1 \times N2} \bmod p$ 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 $SKey_{ij} = h(ID_i, SID_j, Q_j, N_1, N_2)$.

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 $z_i' = y_i \oplus h(PW_i')$ and checks whether computed z_i' equals stored z_i or not.

If true, U_i enters a new password PW_{inew}. The card reader computes $z_{inew} = y_i \oplus h(PW_{inew})$, $x_{inew} = x_i \oplus g^{h(PWi)} \oplus g^{h(PWinew)} \bmod p$ and stores z_{inew}, x_{inew} instead of z_i, x_i respectively in the smart card memory. Thus, U_i can change the password without taking any assistance from S_j.

3. SECURITY FLAWS IN TYAGI ET AL.'S SCHEME :

This section describes the security weaknesses found in Tyagi et al.'s scheme under the assumption that the attacker is able to intercept all the messages exchanged between U_A and S. The proposed protocol is insecure and allows an attacker to impersonate a server to a user. The attack requires that the attacker observe a legitimate protocol run between the user and the server. From this, the attacker learns the nonce N_1 and the values X_1 and X_2, where $X_1 = y_i \oplus N_1 \oplus N_2$. Here, $X_2 = Q_j^{N_2}$. The attacker then runs a protocol with the user with the purpose of impersonating the server to the user. The user will send a new nonce N_1'. The attacker ignores the first message of the user and sends as the second message the values $\{ID_i, X_1' = X_1 \oplus N_1 \oplus N_1', X_2\}$. Now the user

computes $N_2^{'} = y_i \oplus X_1^{'} \oplus N_1^{'} = y_i \oplus X_1 \oplus N_1 = N_2$. Hence, $Q_j^{N_2^{'}} = Q_j^{N_2} = X_2$ and the protocol completes successfully at the user.

4. CONCLUSION

Tyagi et al. proposed multi-server authentication scheme using cryptographic one-way hash function and the discrete logarithm problem. The author claimed that this scheme eliminates the employment of verification table, permits users to settle on and alter the password firmly while not taking any help from the server or registration center, provides mutual authentication and establishes a typical session key between user and also the server. Additionally, the proposed scheme withstands server impersonation attack, user impersonation attack, reflection and parallel session attacks, replay attack, stolen verifier attack, password guessing attack, smart card loss attack and insider attack. It is clear that the scheme proposed by Tyagi et al. is susceptible to impersonation attack.

References

[1] Needham, R. M. & Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. Communications of the ACM, 21(12), 993-999.

[2] Booth, K. S. (1981). Authentication of signatures using public key encryption. Communications of the ACM, 24(11), 772-774.

[3] Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM, 24(11), 770-772.

[4] Chang, C. C. & Wu, T. C. (1991). Remote password authentication with smart cards. IEE Proceedings on Computers and Digital Techniques, 138(3), 165-168.

[5] Hwang, M. S. & Li, L. H. (2000). A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46(1), 28-30.

[6] Sun, H. M. (2000). An efficient remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46(4), 958-961.

[7] Chien, H. Y., Jan, J. K. & Tseng, Y. M. (2002). An efficient and practical solution to remote authentication: smart card. Computers and Security, 21(4), 372-375.

[8] Hwang, M. S., Lee, C. C. & Tang, Y. L. (2002). A simple remote user authentication scheme. Mathematical and Computer Modeling, 36(1-2), 103-107.

[9] Ku, W. C. & Chen, S. M. (2004). Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 50(1), 204-207.

[10] Yoon, E. J., Ryu, E. K. & Yoo, K. Y. (2004). Further improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 50(2), 612-614.

[11] Yoon, E. J., Ryu, E. K. & Yoo, K. Y. (2005). An improvement of Hwang-Lee-Tang's simple remote user authentication scheme. Computers and Security, 24(1), 50-56.

[12] Wang, X. M., Zhang, W. F., Zhang, J. S. & Khan, M. K. (2007). Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards. Computer Standards and Interfaces, 29(5), 507-512.

[13] Das, M. L., Saxena, A. & Gulati, V. P. (2004). A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics, 50(2), 629-631.

[14] Liao, I. E., Lee, C. C. & Hwang, M. S. (2005). Security enhancement for a dynamic ID-based remote user authentication scheme. In Proceedings of the NWeSP, pp. 437-440, Seoul, Korea, 2005.

[15] Wang, Y. Y., Liu, J. Y. Xiao, F. X. & Dan, J. (2009). A more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, 32(4), 583-585.

[16] Hao, Z. & Yu, N. (2010). A security enhanced remote password authentication scheme using smart card. In Proceedings of the 2nd ISDPE, pp. 56-60, Buffalo, New York, USA, 2010.

[17] Song, R. (2010). Advanced smart card based password authentication protocol. Computer Standards and Interfaces, 32(5-6), 321-325.

[18] Juang, W. S. (2004). Efficient multi-server password authenticated key agreement using smart cards. IEEE Transactions on Consumer Electronics, 50(1), 251-255.

[19] Ku, W. C. & Chuang, H. M. (2005). Weaknesses of a multi-server password authenticated key agreement scheme. National Computer Symposium, 1-5.

[20] Chang, C. C. & Lee, J .S. (2004). An efficient and secure multi-server password authentication scheme using smart cards. Proceedings of International Conference on Cyberworlds, 417-422.

[21] Liao, Y. P. & Wang, S. S. (2009). A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, 31(1), 24-29.

[22] Chen, T. Y., Hwang, M. S., Lee, C. C. & Jan, J. K. (2009). Cryptanalysis of a secure dynamic ID based remote user authentication scheme for multi-server environment. Fourth International Conference on Innovative Computing, Information and Control, 725-728.

[23] Hsiang, C. & Shih, W. K. (2009). Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, 31(6), 1118-1123.

[24] Sood, S. K., Sarje, A. K. & Singh, K. (2011). A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications, 34(2), 609-618.

[25] Tyagi, J. K., Srivastava, A. K. & Patwal P. S. (2012). Remote user authentication scheme in multi-server environment using smart card. International Journal of Computer Applications, 57(12) 1-5.