Cryptanalysis of Smart Card Based Remote User Authentication Scheme for Multi-Server Environment

Qimin Sun, Jongho Moon, Younsung Choi, Dongho Won*

College of Information and Communication Engineering Sungkyunkwan University
2066 Seobu-ro, Jangan-gu, Suwon-si, Gyeonggi-do, 16419, Korea

*Corresponding Author: dhwon@security.re.kr

Abstract

The traditional remote user authentication scheme is designed for single-server environment. However, with the increasing of network services, the user is not only required to severally register with each server, but also must store a mass of different identities and passwords. Therefore, a large number of password based remote user authentication scheme for multi-server environment have been proposed by researchers. Unfortunately, all the proposed remote user authentication scheme for multi-server environment have a big design defect in the login phase that user have to use the original static ID to login to server without encrypt. To fix this problem, Li et al. proposed a dynamic ID based remote user authentication scheme for multi-server environment. Recently, Shunmuganathan et al. pointed out that Li et al.'s scheme is vulnerable to off-line password guessing attack, stolen smart card attack and user impersonation attack. Later, they proposed an improved protocol to fix these problems. However, we found that Shunmuganathan et al.'s scheme is still vulnerable to off-line password guessing attack, off-line identity guessing attack and user impersonation attack.

Keywords: authentication, cryptanalysis, smart card, password, two-factor.

1. Introduction

With the rapid development of network technologies, network services gradually becomes a hot topic recently. Increasingly more services are being provided by internet such as on-line financial, bill payment, games, medical,

study, etc. When the user wants to inquire information or ask something from the server, he/she must login to the server first. Due to the openness of the internet, approach of guarding valuable information from unauthorized access is an essential part of network security infrastructure. If conventional smart card remote authentication methods are applied to multi-server environment, each user who wants to access server does not only need to log on various remote servers again and again, but also need to remember a large number of identities and passwords. It's lead to server needs to compute the exponentiation time for authentication and has a lot of security weakness. Therefore, conventional password authentication designed for single-server environment is not suitable for multi-server environment.

Recently, to enhance performance of traditional password authentication, as large the amounts of smart card based identity remote user authentication scheme have been proposed by researchers. These schemes can be divided into two types by cryptographic algorithms used, the one-way hash based authentication scheme and public key based authentication scheme. An efficient and secure remote user authentication scheme should have the ability of resisting all kinds of attacks such that it can be applied in the real world, the computation costs of the smart card must be low, user and server can authenticate each other and agree on a shared session key, allows the user to update his password freely after assuring the legality of user, no need for time synchronization and can avoid the delay-time problem. Moreover, users are required to register with the registration center only once to access all registered servers. The registered server does not store any password table or verification table and can provide two-factor security, maintain user anonymity, withstand masquerade attacks.

Table 1. Notations.

Notations	Description
U_i	The i-th user
ID_i	The identity of the U_i
PW_i	The password of the U_i
S_j	The j-th server
RC	The registration center
SK	Session Key shared between U_i and S_j
SID_j	The identity of the S_j
CID_i	The dynamic ID of U_i
b	A random number chosen by U_i
$h(\cdot)$	A one-way hash function
$\oplus$	Exclusive-OR operation
$\parallel$	Message concatenation operation

Nowadays, an enhanced smart card based remote user authentication scheme for multi-server environment was proposed by Shunmuganathan et al.[7]. They presented that their scheme have a secure session key, can protect anonymity of user, resist the off-line password guessing attack, user impersonation attack and spoofing attack. However, we found that their scheme is still vulnerable to same complex attacks such as off-line password guessing attack, stolen smart card attack and user impersonation attack. This paper is organized as follows. We begin by the introducing the existing research scheme about remote user authentication in section 2. We review Shunmuganathan et al.'s scheme in section 3. We describe the security weaknesses of Shunmuganathan et al.'s remote user authentication scheme for multi-server environment in section 4. Finally, we propose our further work and make a summing up of this paper in Section 5.

2. Related Works

Rivest et al.[1] proposed a public-key cryptosystem for remote user authentication in 1978. However, their scheme needs high cost to encrypt and decrypt for public-key crypt-Tosystem. In 1990, Hwang et al.[2] proposed a non-interactive password authentication scheme and its improved version, which additionally uses smart cards. Since then, many password authentication schemes using smart cards have been proposed[3, 4, 5], and each has its advantages and disadvantages. In 2001, Juang[6] constructed an enhanced version of authentication scheme based on hash function and symmetric key cryptosystem.

Later, Lee and Chang[8] pointed out that Juang's scheme[6] is vulnerable to off-line dictionary attack, replay attack, server spoofing attack and proposed a new scheme that is based on hash function for multi-server environment.

However, a common characteristic among most of the remote user authentication schemes is the user's identity is static, which may leak some information about the user and create risk of ID during the message transmission, this gives the adversary a chance to monitor a legal user. In 2013, Li et al.[9] also proposed an enhance dynamic ID based remote user authentication scheme. However, in 2015, Shunmuganathan et al.[7] claimed that Li et al.'s protocol [9] has a flaw against the off-line password guessing attack, stolen smart card attack and forgery attack. They proposed an improved protocol to remedy the security weakness. Recently, we found that Shunmuganathan et al.'s scheme still cannot resist the off-line password guessing attack, stolen smart card attack and user impersonation attack.

3. Review Of Shunmuganathan et al.'s Scheme

In this section, we will show the detail of scheme that was proposed by Shunmuganathan et al. As same as all the basic requirements of smart card based remote user authentication for multi-server, Shunmuganathan et al.'s protocol also has four phases, i.e., the registration phase, the login phase, the authentication phase, and the password change phase. We show these phases as described below. The notations used in this paper are summarized as Table 1.

3.1 Registration phase

When the user U_i wants to access the server S_j , the user U_i needs to register with registration center RC first, when S_j has already been registered. The registration phase is the initial phase of the scheme. In this phase, the registration center provides secrets to the user as well as server.

(a) User U_i freely chooses his/her identity ID_i , password PW_i , and computes $A_i = h(b \parallel PW_i)$, where b is a random number generated by user U_i . After that, U_i sends ID_i and A_i to the registration center RC for registration.

(b) When receiving the registration request message, the registration center RC computes,

$$B_i = h(ID_i \parallel x) \quad (1)$$

$$C_i = h(ID_i \parallel h(y) \parallel A_i) \quad (2)$$

$$D_i = h(B_i \parallel h(x \parallel y)) \oplus A_i \quad (3)$$

$$E_i = B_i \oplus h(x \parallel y) \quad (4)$$

Fig. 1. Registration Phase.

where x is the master secret key maintained by RC and y is the secret number generated by RC .

(c) Then, the registration center creates a smart card with the following information $\{C_i, D_i, E_i, b, h(\cdot), h(y)\}$ and sends to user via a secure channel. Finally, User stores the random number b in the smart card to complete this phase.

3.2 Login phase

Whenever the user wants to login to the remote server, the user must first login to a specific terminal using smart card. The user inserts his/her smart card into card reader and inputs his/her identity ID_i , password PW_i . Then, the smart card executes the following sequence of operations.

(a) After that, the smart card computes $A_i = h(b || PW_i)$ and $C_i^* = h(ID_i || h(y) || A_i)$. Then, the smart card checks whether C_i^* is equal to the C_i stored in it. If holds, the smart card proves the user and goes to the next step. Otherwise, the smart card rejects this access.

(b) The smart card generates two random numbers N_i and N_k and computes as following,

$$P_{ij} = E_i \oplus h(h(SID_j || h(y)) || N_i) \quad (5)$$

$$F_i = D_i \oplus A_i \quad (6)$$

$$Al_i = h(A_i || N_k) \quad (7)$$

$$CID_i = Al_i \oplus h(F_i || SID_j || N_i) \quad (8)$$

$$M_i = h(P_{ij} || CID_i || F_i || N_i) \quad (9)$$

(c) Then, the smart card sends the login request message $\{P_{ij}, CID_i, M_i, N_i\}$ to the server S_j over a public channel for mutual authentication and computing session key.

3.3 Authentication phase

After receiving the login request messages, the server S_j performs the following set of operations to authenticate each other and generate the same session key with user U_i . After receiving the login request messages, the server S_j performs the following set of operations to authenticate each other and generate the same session key with user U_i .

(a) The server S_j computes the following information with $\{P_{ij}, CID_i, M_i, N_i\}$ received from U_i ,

$$E_i = P_{ij} \oplus h(h(SID_j || h(y)) || N_i) \quad (10)$$

$$B_i = E_i \oplus h(x || y) \quad (11)$$

$$F_i = h(B_i || h(x || y)) \quad (12)$$

$$Al_i = CID_i \oplus h(F_i || SID_j || N_i) \quad (13)$$

(b) Before sending any messages, the server must verify the authenticity of user. Thus, server S_j uses the above derived information and verifies whether M_i is equal to the computed value $h(P_{ij} || CID_i || F_i || N_i)$ or not. If holds, the server generates a random number N_j and goes to next phase. Otherwise, the phase is simply terminated.

(c) The server S_j uses the user's information, nonce N_j and SID_j to compute the following:

$$M_2 = h(F_i || Al_i || N_j || SID_j) \quad (14)$$

$$M_3 = Al_i \oplus N_i \oplus N_j \quad (15)$$

Then, server S_j sends the message $\{M_2, M_3\}$ to user U_i via public channel for mutual authentication.

(d) Once the message is received, the user U_i gets N_j from it as $N_j = Al_i \oplus N_i \oplus M_3$ and verifies whether M_2 is equal to the computed value $h(F_i || Al_i || N_j || SID_j)$. If this holds, U_i successfully authenticates S_j . Then, user computes $M_4 = h(F_i || Al_i || N_i || SID_j)$ and transmits it to server S_j use the message $\{M_4\}$ over a public channel.

(e) After receiving message $\{M_4\}$, the server computes $h(F_i || Al_i || N_i || SID_j)$ and verifies it with the received message $\{M_4\}$. If M_4 is correct, server S_j successfully authenticates the user U_i and the mutual authentication is completed. And they use the information from receiving message to

Fig. 2. Login Phase.

compute session key as $SK = h(F_i || A_i || N_i || N_j || SID_j)$. It is to be noted that both session keys are the same.

3.4 Password change phase

This mechanism is simple enough, if a user wants to change his/her password of smart card, it can be done without informing the registration center.

(a) The user U_i inserts his/her smart card into card-reader and inputs his/her identity ID_i , password PW_i .

(b) Smart card checks the entered information. If the user is the authentic one, then the smart card prompts the user to inputs a new password PW_i^* and generates a new random number b^* computes,

$$A_i^* = h(b^* || PW_i^*) \quad (16)$$

$$C_i^* = h(ID_i || h(y) || A_i^*) \quad (17)$$

$$D_i^* = D_i \oplus A_i \oplus A_i^* \quad (18)$$

(c) Finally, the smart card replaces C_i^* , D_i^* and b^* in the place of C_i , D_i and b . Now, the updated smart card has $\{C_i^*, D_i^*, E_i, b^*, h(\cdot), h(y)\}$. The smart card can be used as before.

4. Security Analysis

Shunmuganathan et al.[7] claimed that their protocol can resist all known attack such as off-line password guessing attack, user impersonation attack and stolen smart card attack. After careful analysis, we found that their scheme is still vulnerable to off-line password guessing attack. If an adversary is able to obtain the smart card of user U_i ,

he/she can extract user's identity ID_i and password PW_i from stolen smart card. Therefore, it's easy for him/her to impersonate user U_i to login to the server. Moreover, their scheme has a big design defect in the session key agreement phase by which the session key can be easily obtained by the adversary after extracting the secret value password PW_i . Thus, the protocol proposed by Shunmuganathan et al. is still insecure. The details of these flaws are described as follows.

4.1 Off-line Password Guessing Attack

Stolen smart card attack means that an adversary who possessed of smart card performs any operation which obtains any information from smart card. If an adversary steals the smart card of legitimate user U_i and obtains the parameters $\{C_i, D_i, E_i, b, h(\cdot), h(y)\}$, then, he/she can easily compute out the hash value of the password PW_i of the user. Now, an adversary performs an off-line password guessing attack to get the current password PW_i of the user U_i .

(a) The adversary extracts $\{C_i, D_i, E_i, b, h(\cdot), h(y)\}$ from stolen smart card and intercepts one of the previous authentication message $\{P_{ij}, CID_i, M_1, N_j\}$.

(b) The adversary speculates the value of a candidate password to be PW_i^* from the password space D .

(c) Then, computation is shown as follows:

$$\begin{aligned} M_1^* &= h(P_{ij} || CID_i || F_i || N_i) \\ &= h(P_{ij} || CID_i || D_i \oplus A_i || N_i) \\ &= h(P_{ij} || CID_i || D_i \oplus h(b || PW_i^*) || N_i) \end{aligned} \quad (18)$$

verifies the correctness of PW_i^* by checking if M_1^* equals the revealed M_1 .

(d) Goes back to the step (b) of this phase until the true value of PW_i is found. Since the size of the password dictionary D is very limited in fact, the above attack procedure can be completed in short time. Moreover, the above attack is very effective because it only needs the abilities of an eavesdropping attacker, i.e., a passive attacker, and involves no special cryptographic operations.

4.2 Off-line Identity Guessing Attack

In Shunmuganathan et al.'s scheme, a user U_i is allowed to choose his/her own identity ID_i during the registration phase. The user usually like to select a simple identity such as his/her e-mail or his/her phone number. Therefore, these easy-to-remembered identities have low entropy and cannot resist off-line identity guessing attack. Let's think about this,

Fig. 3. Authentication Phase.

a legitimate user U_i 's smart card is somehow obtained by an adversary. Then, he/she can calculate the user U_i 's password PW_i through the above process, and extract the stored secret values like C_i , D_i from smart card so that it's easy for him/her to speculate the user's identity ID_i by performing the following malicious attack procedure:

(a) The adversary can compute $A_i = h(b||PW_i)$ with secret value b from stolen smart card, then, compute out password PW_i by above attack. Then, computes $F_i = D_i \oplus A_i$ with secret value D_i .

(b) The adversary calculates $Al_i = CID_i \oplus h(F_i||SID_j||N_i)$ using CID_i and N_i extracted from the intercepted authentication request message $\{P_{ij}, CID_i, M_i, N_{ij}, SID_j\}$ which is known to all registered users.

(c) After that, the adversary guesses the value of a candidate identity to be ID_i^* from the identity space E . He/she calculates $C_i^* = h(ID_i^*||h(y)||A_i)$ and verifies whether C_i^* is equal to C_i or not.

(d) Repeat step (c) until C_i^* is equal to C_i .

4.3 User Impersonation Attack

An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol. If the secret value identity ID_i and password PW_i are obtained by adversary from smart card, he/she can successfully impersonate as user U_i to access the remote server because he/she knows everything about user U_i .

(a) The adversary extracts the secret value identity ID_i and password PW_i through the above attack process.

(b) Lastly, the adversary can successfully login to the server like the legitimate user U_i with identity ID_i and password PW_i . Therefore, Shunmuganathan et al.'s scheme fails to provide proper authentication.

4.4 Violation of the Session Key Security

In the part of weakness analysis of Shunmuganathan et al.'s paper, they proposed the session key SK generated by five parameters $(F_i, Al_i, N_i, N_j, SID_j)$. F_i consists of the user's ID information protected by hash function and master keys. Most importantly, F_i is not directly stored in the smart card. They said that it's impossible for adversary to know (F_i, Al_i, N_j) , but the adversary have already obtained the value F_i and Al_i from the stolen smart card through the above process. Therefore, if he/she have already extracted the value N_j from stolen smart card or authentication message, he/she can extract the session key. Then, the adversary computes $N_j = M_3 \oplus N_i \oplus Al_i$ with M_3

from intercepted authentication message $\{M_2, M_3\}$. Finally, the adversary can easily calculate the secret session key $SK = h(F_i||Al_i||N_i||N_j||SID_j)$ without problem.

5. Conclusions

Remote User authentication scheme is widely used for communicating between authorized remote users over insecure network. In this paper, we have indicated that Shunmuganathan et al.'s scheme is still vulnerable to stolen smart card attack, off-line password guessing attack, and user impersonation attack, and dose not provide perfect forward secrecy. Finally, our further research will focus on proposing a secure user authentication scheme which can solve these problems.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.R0126-15-1111, The Development of Risk-based Authentication·Access Control Platform and Compliance Technique for Cloud Security)

References

- (1) R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun. ACM, vol. 21, pp. 120-126, Feb. 1978
- (2) T. Hwang, Y. Chen, C. S. Lai, "Non-interactive password authentication without password tables," IEEE Region 10 Conference on Computer and Communication System, vol.1, pp. 429-431, Sept. 1990
- (3) C. I. Fan, Y. C. Chan, Z. K. Zhang, "Robust remote authentication scheme with smart cards," Computers and Security, 24.8, 619-628, Mar. 2005
- (4) M. K. Khan, J. S. Zhang, "Improving the security of A flexible biometrics remote user authentication scheme," Computer Standards and Interfaces, 29, 82-85, Feb. 2006
- (5) C. T. Li, M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, 33, 1-5, Aug. 2009
- (6) W. S. Juang, "Efficient multi-server password authentication key agreement using smart cards," IEEE

Transactions on Consumer Electronics, vol.50. No.1.
Pp. 251-255, Mar. 2001

- (7) S. Shunmuganathan, R. D. Saravanan, "Secure and Efficient Smart-Card-Based Remote User Authentication Scheme for Multiserver Environment," CANADIAN JOURNAL OF ELECTRICAL AND COMPUTER ENGINEERING, VOL. 38, NO. 1, Mar. 2015
- (8) C. C. Chang, J. S. Lee, "An efficient and secure multi-server password authentication protocol using smart cards," Proceedings of the Third International Conference on Cyberworlds, pp. 417-422, Nov. 2004
- (9) X. Li, J. Ma, W. Wang, Y. Xiong, J. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments," Computer Standards and Interfaces, 58. 85-95, Jun. 2012
- (10) Y. S .Choi, J. H. Nam, D. H. Lee, J. Y. Kim, J. W. Jung, D. H. Won, " Security Enhanced Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics," The Scientific World Journal, Article ID 281305, Sep. 2014
- (11) Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, D. Won, " Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography,"Sensors, 14(6), 10081-10106, Jun. 2014
- (12) J. Kim, D. Lee, W. Jeon, Y. Lee, D. Won, "Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks," Sensors, Vol.14, No.4. 6443-6462, Apr. 2014
- (13) J. Nam, K. K. R. Choo, S. Han, M. Kim, J. Paik, D. Won, "Efficient and Anonymous Two-Factor User Authentication in Wireless Sensor Networks: Achieving User Anonymity with Lightweight Sensor Computation," PLOS ONE, Vol.10, No.4 1-21, Apr. 2015
- (14)Y. Chung, S. Choi, D. Won "Anonymous Authentication Scheme for Intercommunication in the internet of Things Environments", International Journal of Distributed Sensor Networks, ID 305785, Sep. 2015