Security Weaknesses of a Timestamp-Based User Authentication Scheme with Smart Card

Jaewook Jung, Younsung Choi, Donghoon Lee, Jiye Kim, and Dongho Won

***Abstract*—Remote User authentication scheme is commonly used for communication between authorized remote users over insecure network. Due to its simplicity and convenience, it is widely used in many environments such as E-commerce or remote host login. In recent years, several remote user authentication schemes using smart card have been proposed. Recently, Huang *et al.* proposed a timestamp-based user authentication scheme with smart card. They claimed that their scheme can resist off-line password guessing attack. However, there is some vulnerability Huang *et al.*'s scheme that we find their scheme cannot resist the off-line password guessing attack and it cannot detect the wrong password in login phase, and also insecure for changing the user's password in password change phase. In this paper, we conduct detailed analysis of flaws in Huang *et al.*'s scheme.**

***Index Terms*—Remote user authentication scheme, smart card, password, security.**

I. Introduction

With the rapid increasing need of the internet service and electronic commerce technology, user authentication schemes are an essential security requirement for protecting systems and networks. Especially, smart card authentication is that the most commonly used authentication method that authorized users can access the resources provided by remote servers. Due to its simplicity and efficiency, it is used many areas such as E-commerce environment or remote host login system.

Since Lamport [1] first proposed a remote password authentication protocol for the insecure channel in 1981, many remote user authentication schemes have been proposed [2]-[10]. However, most of these password authentication protocols have some flaws such as password guessing attacks, forgery attacks, replay attacks, insider attacks, impersonation attacks, stolen smart card attacks, parallel session attacks, etc.

Generally speaking, an outstanding smart card based password authentication scheme should satisfy some security requirements. Based on previous research, an ideal password authentication scheme using smart card should achieve the following goals such as

- The server does not need to maintain a password table or verification table.
- Allow users to freely choose and update password without communicating with the server.
- The remote user authentication schemes satisfy low communication cost and computation complexity.
- The remote user authentication schemes should withstand different types of attacks.
- Achieve mutual authentication between login users and remote servers.

In 1999, Yang and Sheih [2] proposed a timestamp-based password remote user authentication scheme using smart card. In their scheme, users are free to choose and change their password. In 2003, Shen *et al.* [3] proposed a modified Yang and Sheih scheme, which resist the forge login attack and provide a mutual authentication.

However, Liu *et al.* [4], Awasthi *et al.* [5] point out that Shen's scheme is still vulnerable to forged login attack. To surmount this shortcoming, Liu *et al.* [4] proposed a new improved scheme based on nonce. Also, Awasthi *et al.* [5] proposed an improved remote authentication scheme which still keeps the feature of the non-storage of data at server side.

Recently, Huang *et al.*'s [6] point out that Awasthi *et al.* 's scheme is vulnerable to impersonation attack and proposed a timestamp-based user authentication scheme with smart-card. In Huang *et al.*'s scheme, they claimed that the remote server does not require any verification information for the users.

However, after careful analysis, we find their scheme cannot resist the off-line password guessing attack and it cannot detect the wrong password in login phase, and also insecure for changing the user's password in password change phase. In this paper, we demonstrate this security problem with Huang *et al.*'s timestamp-based user authentication scheme.

The rest of the paper is organized as follows: In Section II, a brief review of the Huang *et al.*'s scheme [6] is given. In Section III, we show the vulnerabilities of the Huang *et al.*'s timestamp-based user authentication scheme. At the end, we draw our conclusion in Section IV.

II. Review of Huang *et al.*'s Scheme

In this section, we examine the timestamp-based user authentication scheme with smart-card proposed by Huang *et al.*'s in 2013. Huang *et al.*'s scheme consists of four phases: the initialization phase, the registration phase, the login and authentication phase, the password change phase.

The notations used throughout this paper are summarized in Table I.

A. Initialization Phase

In Huang *et al.*'s scheme, Key Information Centre (KIC) is a trusted authority which generates global parameters. KIC also computes user's secret information and distributes smart cards to the new users.

Manuscript received April 5, 2014; revised June 16, 2014.

The authors are with the School of Information and Communication Engineering, Sungkyunkwan University, Korea (e-mail: jwjung@security.re.kr, yschoi@security.re.kr, dhlee@security.re.kr, jykim@security.re.kr, dhwon@security.re.kr).

KIC performs the following steps:

1) Generate two large primes p, q and computes $n = pq$.
2) Choose a prime number e and an integer d such that $e \cdot d \bmod (p-1)(q-1) = 1$, where e is the system's public key, and d is the corresponding private key, respectively.
3) Find an integer g, which is a primitive element in both $GF(p)$ and $GF(q)$ and the public information of the system.

TABLE I: THE NOTATIONS USED IN THIS PAPER

Notations	Description
p, q	Large prime numbers
e, d	system's public key and private key
U_i	The remote user
S	The authentication server
PW_i	Password corresponding to a registered identity ID
KIC	Key Information Center
CID	Smart card identifier
T_c	current timestamp in the user U_i
T_s	current timestamp in the server S
$f(\,)$	one way function
S	The server

B. Registration Phase

The registration phase is described in Fig. 1.

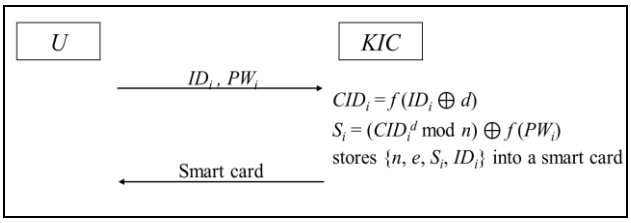

Fig. 1. Registration phase.

A new user Ui register with the server S by performing the following steps:

1) U_i sends his/her identifier ID_i and password PW_i to KIC through a secure channel.
2) Upon receiving the ID_i and PW_i, the KIC calculates smart card's identifier $CID_i = f(ID_i \oplus d)$, and secret information $S_i = (CID_i^d \bmod n) \oplus f(PW_i)$, where $f(\,)$ is a one way function.
3) KIC stores $\{n, e, S_i, ID_i\}$ into a smart card and then issues this smart card to user U_i through a secure channel

C. Login and Authentication Phase

The login and authentication phase is described in Fig. 2. When user U_i wants to login and authenticate to server S, the following operation will perform:

1) User U_i inputs his/her password PW_i and calculates X_i and Y_i as follows:
   $X_i = S_i \oplus f(PW_i)$ and $Y_i = X_i^{f(IDi, Tc)} \bmod n$, where T_c is the current date/timestamp in the user U_i.
2) User U_i sends the login request messages $M = \{ID_i, n, e, T_c, Y_i\}$ to the server S

After the message M is received at time T_s, the server S and the smart card execute the following operations:

1) Server S verifies whether the ID_i is a legitimate user or not, and then checks the timestamp T_s in the received message with the condition $|T_s - T_c| < \Delta T$, where ΔT is the expected transmission delay. If this condition holds, the login request is proceed. Otherwise, the login request is rejected.
2) Server S calculates $CID_i = f(ID_i \oplus d)$ and checks the equation $Y_i^e = f(ID_i \oplus d)^{f(IDi, Tc)} \bmod n$. if there are satisfied, the server S accepts the login request. Otherwise, the login request is rejected.
3) Then server S calculates $R = (f(ID_i, T_s'))^d \bmod n$, and send $M' = \{R, T_s'\}$ to user U_i, where T_s' is the current timestamp in the server S.
4) After receiving the reply message M' at time T_c', the user U_i checks the timestamp T_s' in the received message with the condition $|T_s' - T_c'| < \Delta T$, where ΔT is the expected transmission delay. If this condition holds, the user U_i accepts the login respond of S. Otherwise, terminates this procedure.
5) User U_i calculates $R' = R^e \bmod n$, and then checks the equation $R' = f(ID_i, T_s')$. If there are satisfied, the user U_i accepts the server S. Otherwise, rejects the server S.

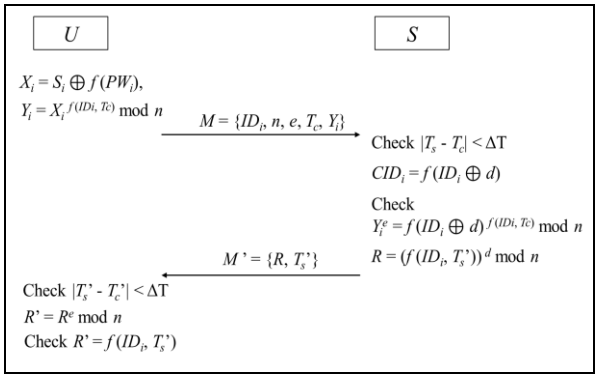

Fig. 2. Login and authentication phase of Huang *et al.*'s scheme.

D. Password Change Phase

The password change phase is described in Fig. 3. The password change phase is performed without communicating the remote server S.

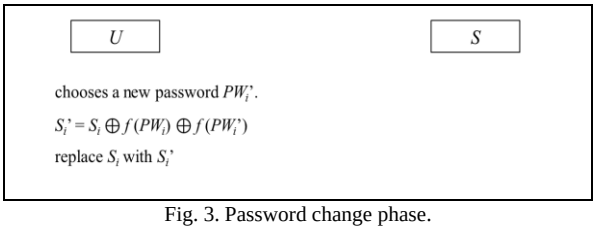

Fig. 3. Password change phase.

In this phase, the user U_i wants to his/her password PW_i with as new password PW_i' by performing the following steps:

1) First, the user U_i chooses a new password PW_i'.
2) Calculate $S_i' = S_i \oplus f(PW_i) \oplus f(PW_i')$.
3) Smart card replaces S_i with S_i', which completes the password change.

III. CRYPTANALYSIS OF HUANG *ET AL.*'S SCHEME

In this section, we will discuss the flaws of Huang *et al.*'s

timestamp-based user authentication scheme with smart card. After careful analysis, we find that their scheme cannot resist the off-line password guessing attack and it has its inherent design flaws in the login phase that if the user U_i inputs a wrong password, the login and authentication phased are still performed until it checked by the server S. Besides, their scheme has a weakness in password change phase. The details of these flaws are described follows.

A. Off-Line Password Guessing Attack

Offline password guessing attack [7]-[10] is that an attacker repeats a trial of a password candidate for all candidates until finding the correct password. In general, the attacker can easily obtain a user's password through off-line password guessing attack within a reasonable time limit, because users tend to set simple and brief passwords for their convenience.

In Huang *et al.*'s scheme, attacker can obtain the secrets $\{n, e, S_i, ID_i\}$ in smart card after the attacker has stolen the smart card, and intercept Login request message $\{ID_i, n, e, T_c, Y_i\}$ between a user and the server. And then, the attacker tries to off-line password guessing attack by performing the following steps:

1) Attacker selects a password candidate PW^*.
2) In login phase, Using $X_i^* = S_i \oplus f(PW^*)$, $Y_i^* = X_i^{f(IDi, Tc)} \bmod n$, attacker can compute $Y_i^* = S_i \oplus f(PW^*)^{f(IDi, Tc)} \bmod n$.
3) The attacker repeats above steps from 1 to 2 until the computed result Y_i^* equals the breached secret Y_i.

If they are equal, $PW^* = PW_i$, this means that attacker successfully obtain user's password by off-line password guessing attack.

B. Wrong Password Cannot Be Quickly Detected

In the login phase of Huang *et al.*'s scheme, if the user U_i inputs his/her ID_i and PW_i, the smart card does not verify the validity of user's password in itself. Therefore, even if the user U_i inputs his/her password incorrectly by mistake, the login and authentication phased are still performed until it checked by the server S. This leads to unnecessary waste a lot of communication and computation costs during the login and authentication phases. The detailed description is as follows:

Assume that the user U_i inputs a wrong password PW_i^* in the login phase, then the smart card computes $X_i^* = S_i \oplus f(PW_i^*)$ and $Y_i^* = X_i^{*\, f(IDi, Tc)} \bmod n$, where T_c is the current date/timestamp in the user U_i. Then, user U_i sends the login request messages $M = \{ID_i, n, e, T_c, Y_i^*\}$ to the server S

After receiving the login request message $M = \{ID_i, n, e, T_c, Y_i^*\}$, the server S checks whether the ID_i is a legitimate user or not, and then checks the timestamp T_s in the received message with the condition $|T_s - T_c| < \Delta T$, where ΔT is the expected transmission delay. Then, the server S calculates $CID_i = f(ID_i \oplus d)$ and checks the equation $Y_i^{*e} = f(ID_i \oplus d)^{f(IDi, Tc)} \bmod n$. if there are satisfied, the server S accepts the login request. Otherwise, the login request is rejected.

It is obvious that $Y_i^{*e} \neq f(ID_i \oplus d)^{f(IDi, Tc)} \bmod n$ since $X_i^* \neq X_i$ and $Y_i^* \neq Y_i$, therefore, the server S will reject U_i's login request.

From above demonstration, if the user U_i inputs a wrong password in the login phase, it cannot be quickly detected. However, if the verification of the password change phase can be quickly checked in the beginning of the login phase, this situation will not happen and it will not lead to unnecessary waste a lot of communication and computation costs.

C. Weakness in Password Change Phase

When the smart card was stolen, unauthorized user can easily change new password of card in password change phase because of there is no validation of the old password.

In password change phase, au unauthorized user inserts U_i's smart card into a smart card reader, and then inputs the ID_i and PW^*, where PW^* is unauthorized user's arbitrary new password, and requests to change the password.

After requesting a password change, unauthorized user inputs arbitrary new password PW^* and then the smart card calculates $S_i^* = S_i \oplus f(PW_i) \oplus f(PW^*)$, which yields $CID_i{}^d \oplus f(PW^*)$. Finally, smart card successfully replaces S_i with S_i^* without any checking.

If an illegal user stole user U_i's smart card and change an arbitrary new password as above mentioned, then legal user U_i succeeding login request will be rejected unless re-register with the remote server again. Therefore, Huang *et al.* 's password change phase is insecure.

IV. Conclusion

In 2013, Huang *et al.*'s proposed a timestamp-based user authentication scheme using smart card and demonstrated its resistance to off-line password guessing attack. However, in this paper, we point out their scheme cannot resist the off-line password guessing attack and it cannot detect the wrong password in login phase, and also insecure for changing the user's password in password change phase. We are working to improve the scheme by including suitable changes to surmount the shortcomings, which leads to the insecurity of the authentication scheme.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2014R1A1A2002775).

References

[1] L. Lamport, "Password authentication with insecure communication," *Communications of ACM*, no. 24, pp. 770-772, 1981.
[2] W. W. Yang and S. P. Shieh, "Password authentication scheme with smart cards," *Computers and Security*, vol. 18, no. 8, pp. 727-733, 1999.
[3] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security enhancement for the timestamp-based password authentication," *Computers and Security*, vol. 22, no. 7, pp. 591-595, 2003.
[4] J. Y. Liu, A. M. Zhou, and M. X. Gao, "A new mutual authentication scheme based on nonce and smart cards," *Computer Communications* , vol. 31, pp. 2205-2209, 2008.
[5] K. Awasthi, K. S. Srivastava, and R. C. Mittal, "An improved timestamp-based remote user authentication scheme," *Computers and Electrical Engineering*, vol. 37, pp. 869-874, 2011.
[6] H. F. Huang, H. W. Chang, and P. K. Yu, "Enhancement of timestamp-based user authentication scheme with smart card," *International Journal of Network Security*, vol. 16, no. 6, pp. 463-467, Nov. 2014.

[7] J. Nam, K. K. R. Choo, J. Kim, H. K. Kang, J. Kim, J. Paik, and D. Won, "Password-Only authenticated three-party key exchange with provable security in the standard model," *Sensors 2014*, vol. 14, no. 4, pp. 6443-6462, April. 2014.
[8] J. Jung, W. Jeon, and D. Won, "An enhanced remote user authentication schemeusing smart card," *ICUIMC*, 2014.
[9] J. Nam, K. K. R. Choo, M. Kim, J. Paik, and D. Won, "Dictionary attacks against password-based authenticated three-party key exchange protocols," *Ksii Transactions on Internet and Information Systems*, vol. 7, no. 12, pp. 3244-3260, Dec. 2013.
[10] E. Yoon, E. Ryu, and K. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 612-614, May. 2004.

Jaewook Jung received the B.S. degree in electrical and computer engineering from Korea Aerospace University, Korea, in 2010 and the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2012. He is currently undertaking a Ph.D. course on electrical and computer engineering in Sungkyunkwan University. His current research interests include cryptography, forensic, authentication protocol, and mobile security.

Younsung choi received the B.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2005 and the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2007. He is currently undertaking a Ph.D. course on electrical and computer engineering in Sungkyunkwan University. His current research interests include digital forensic, cyber-crime, cryptography, forensic, authentication protocol, and mobile security.

Donghoon Lee received the B.S. degree of computer science from National Institute for lifelong education (NILE), Korea, in 2009 and the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2011. He is currently undertaking a Ph.D. course on electrical and computer engineering in Sungkyunkwan University. His current research interests include digital forensic, cryptography, forensic, authentication protocol, and mobile security.

Jiye Kim received the B.S. degree in information engineering from Sungkyunkwan University, Korea, in 1999 and the M.S. degree in computer science education from Ewha Womans University, Korea, in 2007. He is currently undertaking a Ph.D. course on electrical and computer engineering in Sungkyunkwan University. His current research interests include cryptography, forensic, authentication protocol, and information security.

Dongho Won received his B.E., M.E., and Ph.D. from Sungkyunkwan University in 1976, 1978, and 1988, respectively. After working at ETRI (Electronics & Telecommunications Research Institute) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently a professor of the School of Information and Communication Engineering. In the year 2002, he served as the President of KIISC (Korea Institute of Information Security & Cryptology). He was the Program Committee Chairman of the 8th International Conference on Information Security and Cryptology (ICISC 2005). His current research interests include cryptology and information security.