Security Enhancement for the Timestamp-Based Password Authentication Scheme Using Smart Cards*

Jau-Ji Shen[‡] Chih-Wei Lin[‡] Min-Shiang Hwang[†]

Department of Information Management[‡]
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

Graduate Institute of Networking and Communication Engineering[†]
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

September 19, 2012

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

[†]Responsible for correspondence: Min-Shiang Hwang

Security Enhancement for the Time-Stamp Based Password Authentication Scheme Using Smart Cards

Abstract

In 1999, Yang and Shieh proposed a timestamp-based password authentication scheme with smart cards. However, Chan and Cheng showed that it was insecure because the scheme was vulnerable to the *forged login attack*. In this paper, we propose a modified Yang-Shieh scheme to enhance the security. Our modification can help withstand the *forged login attack* and also provide a mutual authentication method to prevent the *forged server attack*.

Keywords: Authentication, cryptography, password, security, smart card.

1 Introduction

Password-based authentication schemes with smart cards are an important part of security for accessing remote servers. A variety of password-based authentication schemes with smart cards have been proposed [2, 3, 5, 6, 7, 8, 10]. These schemes allow a legitimate user to login to a remote server and access the resources.

In 2000, Hwang and Li [6] proposed a new remote user authentication scheme using a smart card based on ElGamal's cryptosystem [9]. However, this scheme has a drawback: the users cannot freely choose their passwords. A timestamp-based password authentication scheme was proposed by Yang and Shieh [10]. Their scheme allows the users to freely choose and change their passwords. In addition, the remote server does not need to store the passwords or verification tables for authenticating the users. Nevertheless, Chan and Cheng [2] launched the *forged login attack*, in which an intruder could impersonate legitimate users to login and accesses the remote server, on Yang and Shieh's scheme. In 2002, Fan et al. [4] also showed that Yang-Shieh scheme could not withstand the *forged login attack* and proposed a slight modification to resist this attack. However, their solution inefficient and impracticality because it limits the user ID_i with a strict form. The length of ID_i should be 1024 bits at least for satisfying the key length of RSA [9] in Fan et al.'s scheme. We will explain it in Section 4.

Several forged server attacks have been recently proposed [1]. The intruders can manipulate the sensitive data of the legitimate users via setting up fake servers. Therefore, a secure password-based authentication scheme with smart card must have the ability to work against such attacks.

In this paper, we shall propose a modified version of the Yang-Shieh scheme to enhance the security. A simple way to withstand the *forged login attack* will be proposed in our first modification. Our second modification can withstand the *forged login attack* and also provide mutual authentication to withstand the *forged server attack*.

This article is organized as follows: In Section 2, we review the Yang-Shieh scheme and discuss its weaknesses. Next, we propose two slightly modified versions of their scheme to enhance the security in Section 3. In Section 4, we analyze the security of our modified versions. Our conclusions are presented in Section 5.

2 Review of the Yang-Shieh Scheme

In this section, we will briefly review Chan and Cheng's *forged login attack* on Yang-Shieh's timestamp-based password authentication scheme. Yang-Shieh's scheme is composed of three phases; the registration phase, login phase and authentication phase. The detailed procedure of the Yang-Shieh scheme is as follows.

Registration phase: A user must be authenticated when she/he uses the resources provided by a remote server. Suppose a new user U_i wants to register with a key information center (KIC) for accessing services. The KIC does the following:

1. U_i securely submits her/his identity ID_i and a password PW_i to the KIC for registration.
2. Two large prime numbers p and q are renerated, and let $n = p \cdot q$. A prime number e is chosen at random as her/his public key, where e is relatively prime to $(p-1)(q-1)$. An integer d as a corresponding secret key that satisfies $ed \equiv 1(\text{mod}(p-1)(q-1))$. An integer g, which is a primitive element in both $GF(p)$ and $GF(q)$ is found, where g is KIC's public information.
3. Compute $S_i = ID_i^d \bmod n$ as U_i's secret information. Then compute h_i for U_i such that $h_i = g^{PW_i \cdot d} \bmod n$, and generate the smart card's identity CID_i.
4. Write $n, e, g, ID_i, CID_i, S_i, h_i$ into the smart card of U_i, and issue it through a secure channel.

Login phase: In the login phase, U_i must insert her/his smart card into the login device when she/he wants to login to the remote server. The smart card will perform the following operations after U_i keys in her/his identity ID_i and password PW_i.

1. Generate a random number r_i and compute X_i and $Y_i$as follows.

$$
\begin{aligned}
X_i &\equiv g^{r_i \cdot PW_i} \bmod n, \\
Y_i &\equiv S_i \cdot h_i^{r_i \cdot f(CID_i, T)} \bmod n.
\end{aligned}
$$

   Here T is the current date and time on the login device and $f(x, y)$ is a one-way function.

2. Send a message $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$ to the remote sever as a login request message.

Authentication phase: Upon receiving the message M from U_i, the server will perform the following operations to identify the login user:

1. Check the validity of ID_i and CID_i. The remote server will reject the login request if ID_i or CID_i is incorrect. Then, check the validity of T. If $(T' - T) \geq \triangle T$, then the server rejects the login request. Here, T' is the current date and time on the remote server; $\triangle T$ is the expected legitimate time interval for transmission delay.
2. Check the equation $Y_i^e = ID_i \cdot X_i^{f(CID_i,T)}$. If it holds, then the remote server accepts the login request and access.

Recently, Chan and Cheng proposed an attack in which an intruder ID_f could actually masquerade as a legal user ID_i to login to the remote server. The login message $M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$ of the user ID_i could be intercepted by the intruder ID_f. The intruder sets $ID_f = Y_i^e \bmod n$ and $X_f = Y_i^e \bmod n$ and then $Y_f = ID_f^d \cdot X_f^{d \cdot f(CID_i,T_f)} = Y_i \cdot Y_i^{f(CID_i,T_f)} \bmod n$, where T_f is the current date and time from the intruder. Furthermore, the intruder modifies the login request message M to $M' = \{ID_f, CID_i, X_f, Y_f, n, e, g, T'\}$ and sends it to the remote server for forged login. The remote server will accept the login message because M' can pass the validity equation $Y_f^e = (ID_f^d \cdot X_f^{d \cdot f(CID_i,T')})^e = ID_f \cdot X_f^{f(CID_i,T')} \bmod n$. An intruder therefore could successfully masquerade as a user to login to the remote server and gain access.

3 Our Scheme

In Chan and Cheng's attack, they demonstrated that an intruder could modify the login request message $M = \{ID_i,\ CID_i,\ X_i,\ Y_i,\ n,\ e,\ g,\ T_1\}$ to $M' = \{ID_f,\ CID_i,\ X_f,\ Y_f,\ n,\ e,\ g,\ T_f\}$ and masquerade as a legitimate user U_i to access the remote server. The reason is that there is no direct relationship between ID_i and CID_i. As a result, the intruder's M' could pass the verification by the remote server.

In this section, we propose a modified scheme to withstand the *forged login attack* on the Yang-Shieh scheme proposed by Chan et al. [2] and Fan et al. [4] in 2002. We also provide mutual authentication in our modification.

Several steps in the Yang-Shieh scheme are modified in our method as follows.

Registration phase: In step 3 of the registration phase in the Yang-Shieh scheme, we make the CID_i satisfy

$$CID_i = f(ID_i \oplus d),$$

where $\oplus$ stands for an exclusive operation. We show the modified registration phase in Figure 1.

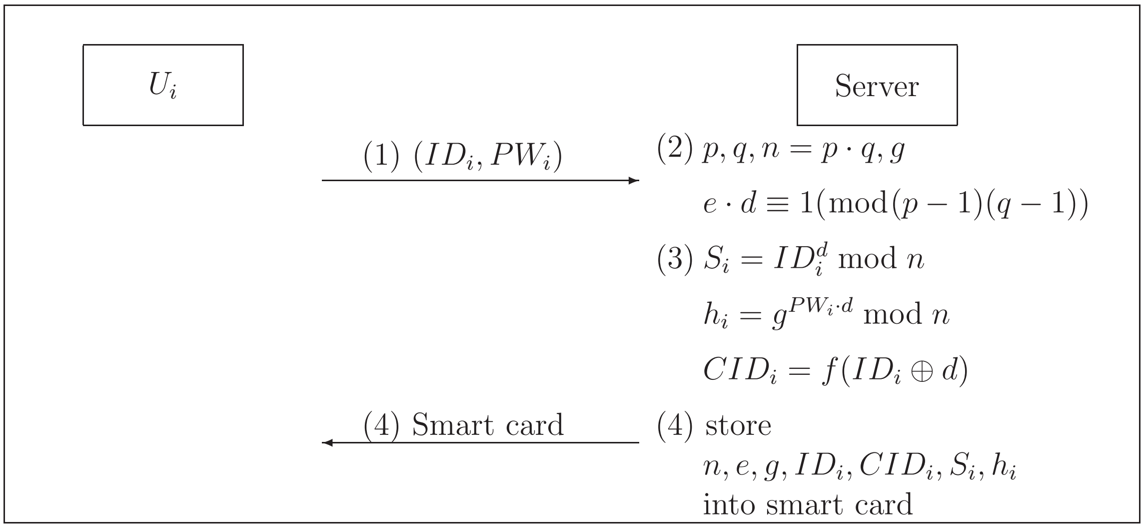

Figure 1: The modified registration phase

Authentication phase: After receiving the login request message M, the remote server checks the validity of ID_i. The remote server will reject this request if the ID_i format is incorrect. The user then checks the validity of CID_i by verifying $CID_i' =?CID_i$, where

$$CID_i' = f(ID_i \oplus d). \tag{1}$$

If the result is positive, the remote server performs the authentication steps of the Yang-Shieh scheme. The remote server then computes R for mutual authentication as follows:

$$R = (f(CID_i, T_2))^d \bmod n,$$

where T_2 is the timestamp showing the current date and time from the remote server. It returns $M' = \{R, T_2\}$ to the user U_i. Upon receiving the message M' from the remote server, the user verifies the message as follows:

1. Check the time interval between T_2 and T_3, where T_3 is the date and time when the remote server receives the message M'. If $(T_3 - T_2) \geq \triangle T$, then U_i rejects the remote server, where $\triangle T$ denotes the predetermined legitimate time interval of transmission delay.
2. Calculate R' using

$$\begin{aligned} R' &\equiv R^e \bmod n \\ &\equiv (f(CID_i, T_2)^d)^e \\ &\equiv f(CID_i, T_2). \end{aligned}$$

3. If $R' =?f(CID_i, T_2)$ does not hold, U_i then rejects the remote server and breaks the connection.

We show the modified authentication phase in Figure 2.

U_i		Server
(1) $X_i = g^{r_i \cdot PW_i} \bmod n$		
$Y_i = S_i \cdot h_i^{r_i \cdot f(CID_i, T_1)} \bmod n$		(3) check: ID_i, T_1
$M = \{ID_i, CID_i, X_i, Y_i, n, e, g, T\}$		$CID_i' = h(ID_i \oplus d)$
	(2) M $\longrightarrow$	$CID_i' =? CID_i$
(6) check:	$M' = \{R, T_2\}$	(4) $Y_i^e \equiv? ID_i \cdot X_i^{f(CID_i, T_1)} \bmod n$
$R' =? f(CID_i, T_2)$	$\longleftarrow$	(5) $R = (f(CID_i, T_2))^d \bmod n$

Figure 2: The modified authentication phase

4 Analysis

Our scheme is a modification of the Yang-Shieh scheme. The security and efficiency of Yang-Shieh was discussed. In this section, we discuss the difference between their scheme and ours.

Our modified scheme can withstand the *forged login attack* [2, 4] and also perform mutual authentication. By setting U_i's CID_i to be $CID_i = f(ID_i \oplus d)$, we can stop the *forged login attack* because d is the remote server's secret key. Any intruder cannot forge the valid CID_i and the login request message M. In addition, we added mutual authentication to the scheme to prevent the *forged server attack*. No intruder could create a fake mutual authentication request message because she/he cannot get the server's secret key.

Furthermore, our modified scheme is more practical than [4] because there is no limits the user ID_i with strict form. In Fan et al's protocol, the length of ID_i should be 1024 bits at least for satisfying the key length of RSA. Even the ID_i selected by the user is not enough 1024 bits which must be filled with 0 to 1024 bits. Therefore, the computations of remote server will be increased in the registration phase and authentication phase, when calculates S_i $(= ID_i^d \bmod n)$ and checks whether the equation holds $(Y_i^e \bmod n = ID_i \times X_i^{f(CID_i \times T)} \bmod n)$ for all users, respectively. The performance of remote server will be decrease because the length of ID_i always equal to the key length of RSA. The computation cost of remote server is heavy because the security is depending on the key length of RSA.

However, our protocol is practicality that doesn't need to restrict the ID_i within strict form which must be filled with 0 to 1024 bits if not enough 1024 bits. In the modified scheme, the remote server uses one exclusive operation and one one-way hash function to calculate CID_i as Equation (1) to enhance the original protocol. The user can freely choose his/her memorable and short identity ID_i without increasing the computations of remote server too much. Therefore, the modified scheme is more efficient than [4].

5 Conclusion

A modified version of the Yang-Shieh scheme was proposed in this paper. The proposed scheme can withstand the *forged login attack* [2, 4]. Our modified scheme can withstand the *forged login attack* and also provide mutual authentication to protect itself from the *forged server attack*. Moreover, our modified scheme is practical and more efficient than Fan et al.'s scheme [4].

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC91-2213-E-324-003.

References

[1] N. Aoskan, H. Debar, M. Steiner, and M. Waidner, "Authenticating public terminals," *Computer Networks*, vol. 31, pp. 861–970, 1999.

[2] Chi-Kwong Chan and L. M. Cheng, "Cryptanlysis of timestamp-based password authentication scheme," *Computers & Security*, vol. 21, no. 1, pp. 74–76, 2002.

[3] C. C. Chang and W. Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," *Compupers & Security*, vol. 13, no. 2, pp. 137–144, 1994.

[4] Lei Fan, Jian-Hua Li, and Hong-Wen Zhu, "An enhancement of timestamp-based password authentication scheme," *Computers & Security*, vol. 21, no. 7, pp. 665–667, 2002.

[5] Min-Shiang Hwang, "A remote password authentication scheme based on the digital signature method," *International Journal of Computer Mathematics*, vol. 70, pp. 657–666, 1999.

[6] Min-Shiang Hwang and Li-Hua Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[7] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang, "A flexible remote user authentication scheme using smart cards," *ACM Operating Systems Review*, vol. 36, no. 3, pp. 46–52, 2002.

[8] Chih-Wei Lin, Jau-Ji Shen, and Min-Shiang Hwang, "Security enhancement for optimal strong-password authentication protocol," *ACM Operating Systems Review*, vol. 37, no. 2, pp. 7–12, 2003.

[9] Bruce Schneier, *Applied Cryptography, 2nd Edition.* New York: John Wiley & Sons, 1996.

[10] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computers & Security*, vol. 18, no. 8, pp. 727–733, 1999.

BIOGRAPHIES

Jau-Ji Shen received the B.S. in Mathematics from Fu-Jen University, Taipei county, Taiwan, Republic of China, in 1982. Two years after, he received M.S. in information science program of Applied Mathematics from National Chung-Shing University, Taichung, Taiwan. In 1988, he received Ph.D. in Information Engineering and Computer Science from National Taiwan University, Taipei, Taiwan. From 1988 to 1994, he was the leader of the software group in Institute of Aeronautic, Chung-Sung Institute of Science and Technology, ROC. He is currently an Associate professor and Associate Dean of the Management College, Chaoyang University of Technology, Taiwan, ROC. His current research interests include database technjques, algorithms and software engineering.

Chih-Wei Lin received the B.S. in Management Information System Engineering from Kun Shan University of Technology, Taiwan, Republic of China, in 2001. He is currently pursuing his master degree in Information Management at Chaoyang University of Technology. His research interests include cryptography, mobile communications, and Information Management.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China (ROC), in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He obtained the 1997, 1998, 1999, 2000, and 2001 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Graduate Institute of Networking and Communications, CYUT. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 70 articles on the above research fields in international journals.