A Modified Remote User Authentication Scheme Using Smart Cards

Jau-Ji Shen, Chih-Wei Lin, and Min-Shiang Hwang$_{Member,\ IEEE}$

***Abstract*— In 2000, Hwang and Li proposed a new remote authentication scheme using smart cards. Their scheme is based on the ElGamal's public key cryptosystem. However, Chan and Cheng pointed out that the scheme is vulnerable to the masquerade attack. In this article, we shall show a different attack on Hwang-Li scheme which is easier and simpler. Furthermore, we shall present a enhanced scheme for repairing the above attacks.**

***Index Terms*— Authentication, cryptography, password, security.**

I. INTRODUCTION

PASSWORD authentication schemes with smart card have a history in the remote user authentication environment. A wide variety of password authentication schemes with smart card [2], [3], [7], [8], [11], [10], [12], [13], [14], [15] have been proposed. These schemes can allow a legal user to login a remote server and access the data provided by the remote server.

In 1995, Wu proposed a new remote login authentication scheme based on simple geometric Euclidean plane [16]. His scheme allows users to freely choose passwords themselves. However, Hwang [6] has pointed out that the weakness of Wu's scheme lies in the security. In 2000, Hwang and Li [9] proposed a new remote user authentication scheme using smart card based on ElGamal's cryptosystem. Chen and Chang [1] pointed out a cryptanaylsis of Hwang-Li scheme's scheme.

In this article, we shall present a different attack on the Hwang-Li scheme that cannot withstand a masquerade attack; an attacker can derive a legal user's password and then masquerade as another legal user to login a remote server. For the above security flaw, we shall propose a enhance scheme to repair.

II. REVIEW OF THE HWANG-LI SCHEME

In this Section, we will briefly review Hwang-Li scheme [9]. The scheme is composed of three phases: the registration phase, the login phase, and the authentication phase. Each user sends his/her identity to the server in the registration phase. The server will issue a smart card and a password to every the legal user through a secure channel when the user is identified. When the user wants to access a remote server, he/she can insert his/her smart card into the login device and then key in the identity and password to access services. The server will verify the data in the authentication phase.

- **Registration phase:** The server prepares two system parameters p and x_s, where p is a large prime number and x_s is the secret key of the server. Besides, there is also a public one-way function $h(\cdot)$. Suppose a new user U_i wants to register the server for accessing services.
  First, U_i registers his/her identity ID_i to the server. The server computes the password $PW_i = ID_i^{x_s} \bmod p$ for the user U_i and stores $h(\cdot)$ and p into a smart card. Then the server issues the smart card and PW_i to the user U_i through a secure channel. Note that the data stored in the smart card is the same for all users, i.e., $h(\cdot)$ and p. The procedure is shown in Figure 1.
- **Login phase:** The user inserts his/her smart card into the login device when he/she wants to login the server. He/she keys in his/her identity ID_i and PW_i. The smart card provides $C_1 = ID_i^r \bmod p$ and $C_2 = M(PW_i)^r \bmod p$ for login, where r is a random number, and $M = ID_i^t \bmod p$. Here, $t = h(T \oplus PW_i) \bmod (p-1)$, where T is the current date and time by the input device, and $\oplus$ stands for an exclusive operation. The device sends a message $C = (ID_i, C_1, C_2, T)$ to the remote server.
- **Authentication phase:** The server first checks ID_i and T to make sure whether they are valid. If $(T'-T) \geq \triangle T$, then the server rejects the login request. Here, T' is the current date and time by the server; $\triangle T$ is the expected legal time interval for transmission delay. Second, the server checks $C_2(C_1^{x_s}) \bmod p = (ID_i)^{h(T \oplus PW_i)}$ to see if it holds before accepting the login request.

III. CRYPTANALYSIS OF THE HWANG-LI SCHEME

In 2000, Chan and Cheng pointed out Hwang-Li scheme cannot withstand the masquerade attack. However, we shall present an easier and simpler attack on Hwang-Li scheme. In this section, we shall briefly review Chan and Cheng's attack, and then show a different approach to attack on Hwang-Li scheme. We shall show that in the Hwang-Li scheme, it is possible for an illegal user to obtain a legal user's password and then masquerade as the legal user to login the server without being detected.

Manuscript received January 28, 2003. This work was supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E324-004..

Jau-Ji Shen and Chih-Wei Lin are with the Department of Information Management Chaoyang University of Technology 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.

Min-Shiang Hwang is with the Graduate Institute of Networking and Communication Engineering Chaoyang University of Technology 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C. (Fax: 886-4-23742337; Email: mshwang@cyut.edu.tw)

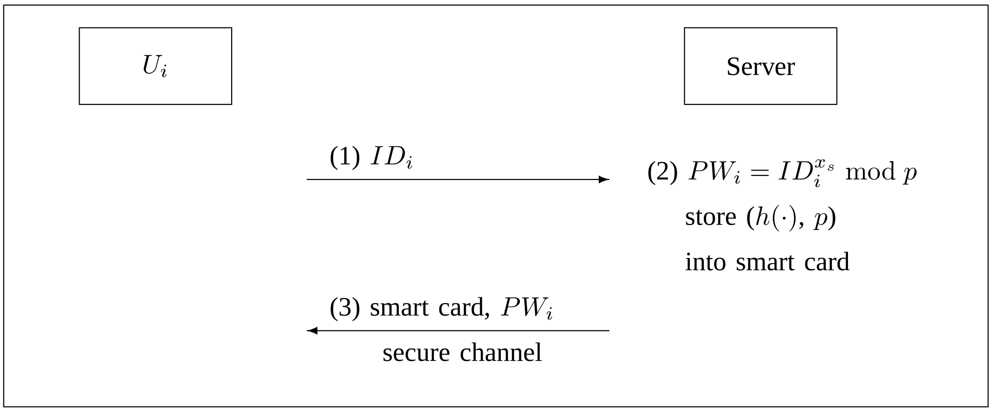

Fig. 1. The Registration Phase

A. Chan-Cheng's attack

Suppose that a user U_a wants to masquerade other legal users. She/he submits her/his ID_a to the remote server for registering to be a legal user. The remote server will responses PW_a and a smart card for U_a after the identity is identified. Now, U_a wants to create a legal user U_f and corresponding a valid pair of (ID_f, PW_f). Now, she/he computes $ID_f = (ID_a \cdot ID_a) \bmod p$ and $PW_f = ID_f^{x_s} = (PW_a \cdot PW_a) \bmod p$. Thus, U_a can successfully login in the remote server via forged (ID_f, PW_f).

B. Different Attack

Suppose a user U_a is an attacker who wants to masquerade as another user U_i to login a remote server and gain access privilege.

The attacker can make his/her ID_a equal to $ID_i^k \bmod p$ because ID_i is public, where k is a random number chosen by the attacker and $\gcd(k, p) = 1$. The attacker summits his/her identity ID_a and registration request to the server in the registration phase.

The server will verify the identity attached to the registration request and compute $PW_a = ID_a^{x_s} \bmod p$ for the attacker to store $h(\cdot)$ and p into his/her smart card. Finally, the server will issue the smart card and PW_a to the attacker through a secure channel. Now, the attacker can derive U_i's password as follows:

$$\begin{aligned}(PW_a)^{-k} \bmod p &= (ID_j^{x_s})^{-k} \bmod p, \\ &= (ID_i^{k \cdot x_s})^{-k} \bmod p, \\ &= (ID_i^{x_s}) \bmod p, \\ &= PW_i.\end{aligned}$$

Next, the attacker can successfully use U_i's password to masquerade as the user U_i to login the remote server.

IV. Security Enhancement for the Hwang-Li Authentication Scheme

In this section, we present a modification of the Hwang-Li scheme to enhance the security flaw described in Section 3 and analysis the security of our enhanced scheme.

A. The Enhanced Scheme

Here, we propose a enhanced scheme that can amend the security flaw of the Hwang-Li scheme. It employs the concept of hiding identity to prevent from masquerading attack. We only modify the registration phase which issue a ”shadowed” identity [4], [5] for every legal user. The steps of login and authentication phase are retained except that replace (ID_i, ID_i') by ”shadowed” identity (SID_i, SID_i'), respectively. The modified registration phase is presented as follows.

- **Registration Phase:** Assume that this phase is executed over a secure channel. First, U_i submits her/his identity string J_i to the remote server for registration, where J_i is U_i's identity string that includes name, unique number etc. which are unique. The remote server computes (SID_i, SID_i', PW_i) for the registering user after her/his identity J_i is identified.

$$\begin{aligned} SID_i &= Red(J_i), && (1)\\ SID_i' &= SID_i^{x_{s_1}} \bmod p, && (2)\\ PW_i &= SID_i'^{x_{s_2}} \bmod p. && (3)\end{aligned}$$

Where, $Red(\cdot)$ is a ”shadowed” identity of the device which only is possessed with the remote server; SID_i and SID_i' are U_i's ”shadowed” identity which can be disclosed. Furthermore, the remote server issues the smart card and (SID_i, PW_i) to U_i, which $(f(\cdot), p)$ is stored into the smart card.

B. The Security Analysis of the Enhanced Scheme

Our enhanced scheme is modification of the Hwang-Li scheme. The security analysis have been already discussed and demonstrated in [6]. Therefore, we shall only discuss the enhanced scheme how to resist the masquerade attack which proposed by [1] and us.

The masquerade attack on the Hwang-Li scheme is described in Section 3. The attack works because the evil user can successfully register a new ID_e via ID_i. In our enhanced scheme, we propose a modification of the login phase as the equations (1), (2) and (3) to withstand the attack.

As the Section 3, assume that an evil user U_e can intercepts $C = (PID_i, C_1, c_2, T)$ from a public network. Now, U_e submits her/his

$$J_e = (PID_i)^k \bmod p,$$

to the remote server to register for masquerading as U_i. Upon receiving the registration message J_e from U_e, the remote server will rejects the registration request because the format of J_e is incorrect which must includes name, unique number etc. for identifying. J_i is maintained by the user U_i and the remote server, secretly. Thus, U_e cannot masquerades as U_i to login and access the remote server because cannot intercepts J_i from the public network. For this reason, our enhanced scheme can withstand the masquerading attack. As same reason, our enhanced scheme also can withstand the Chan-Cheng's attack.

V. Conclusions

In this article, we have shown a that the Hwang-Li scheme is vulnerable to the different masquerade attack from [1]. An evil user can masquerades as another legal user to login a remote server via derive a legal user's password. For the above attacks, we shall present a enhanced scheme to repair the security flaw of the Hwang-Li scheme.

Acknowledgment

This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E324-004.

References

[1] Chi-Kwong Chan and L. M. Cheng. Cryptanalysis of a remote user authentication scheme using smart cards. *IEEE Transaction on Consumer Electronics*, 46:992–993, 2000.

[2] C. C. Chang and S. J. Hwang. Using smart cards to authenticate remote passwords. *Computers and Mathematics with Applications*, 26(7):19–27, 1993.

[3] C. C. Chang and T. C. Wu. Remote password authentication with smart cards. *IEE Proceedings-E*, 138(3):165–168, May 1991.

[4] L. Guillou and J. J. Quisquater. Efficient digital public-key signatures with shadow. In *Advances in Cryptology, CRYPT'87*, page 233, Lecture Notes in Computer Science, 293, 1987.

[5] L. Guillou and J. J. Quisquater. A "Paradoxical" identity-based signature scheme resulting from zero-knowledge. In *Advances in Cryptology, CRYPT'88*, pages 216–231, Lecture Notes in Computer Science, 430, 1988.

[6] Min-Shiang Hwang. Cryptanalysis of remote login authentication scheme. *Computer Communications*, 22(8):742–744, 1999.

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

[8] Min-Shiang Hwang, Cheng-Chi Lee, and Yuan-Liang Tang. An improvement of SPLICE/AS in WIDE against guessing attack. *International Journal of Informatica*, 12(2):297–302, 2001.

[9] Min-Shiang Hwang and Li-Hua Li. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(1):28–30, 2000.

[10] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang. A flexible remote user authentication scheme using smart cards. *ACM Operating Systems Review*, 36(3):46–52, 2002.

[11] Cheng-Chi Lee, Li-Hua Li, and Min-Shiang Hwang. A remote user authentication scheme using hash functions. *ACM Operating Systems Review*, 36(4):23–29, 2002.

[12] Li-Hua Li, Iuon-Chung Lin, and Min-Shiang Hwang. A remote password authentication scheme for multi-server architecture using neural networks. *IEEE Transactions on Neural Networks*, 12(6):1498–1504, 2001.

[13] Yuan-Liang Tang Min-Shiang Hwang, Cheng-Chi Lee. A simple remote user authentication scheme. *Mathematical and Computer Modelling*, 36:103–107, 2002.

[14] M. Peyravian and N. Zunic. Methods for protecting password transmission. *Computers & Security*, 19(5):466–469, 2000.

[15] M. Udi. A simple scheme to make passwords based on one-way function much harder to crack. *Computers & Security*, 15(2):171–176, 1996.

[16] T. C. Wu. Remote login authentication scheme based on a geometric approash. *Computer Communications*, 18(12):959–963, 1995.

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 techniques, 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; 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 project leader for research in computer security at TL in July 1990. 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 Communication Engineering, Chaoyang University of Technology, Taiwan, ROC. He is a

member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile computing.