INFORMATICA, 2003, Vol. 14, No. 3, 289–294

Some Forgery Attacks on a Remote User Authentication Scheme Using Smart Cards

Chin-Chen CHANG
Department of Computer Science and Information Engineering, National Chung Cheng University
160, Sanhsing, Minhsiung, Chaiyi 621, Taiwan
e-mail: ccc@cs.ccu.edu.tw

Kuo-Feng HWANG
Department of Multimedia Desgin, National Taichung Institute of Technology
129, Sec. 3, Sanming Rd., Taichung 404, Taiwan
e-mail: kfhwang@mail.ntit.edu.tw

Received: July 2001

Abstract. Smart card has been adopted to various applications. In 2000, Hwang and Li proposed a remote user authentication scheme, which is also using smart card. Nine months later, Chan and Cheng pointed out that there is a weakness in the remote authentication scheme proposed by Hwang and Li. In this paper, we show that Chan and Cheng's attack does not work well because they did not consider the format of user's identity. In addition, we propose several ways to solve the problem of Chan and Cheng's attack.

Key words: cryptography, authentication, cryptanalysis.

1. Introduction

Smart card is an IC card which has the computation capability, and it has been adopted to various applications (Dhem and Feyt, 2001; Toji *et al.*, 2001). For instance, the SIM (Subscriber Identity Module) card, a special kind of smart card, is used in cellular phone. In 2000, Hwang and Li (2000) used smart card to authenticate the validity of a remote user. Their scheme is based on the ElGamal's public-key cryptosystem (ElGamal, 1985). Hwang and Li adopted a timestamp in the login message for resisting the replaying attack. In particular, the remote system does not need to store the password table and the user's identity table for authenticating in their scheme. The remote system only needs to maintain a secret key. And the security of Hwang and Li's scheme is based on the difficulty of computing the remote system's secret key from known messages.

In Hwang and Li's scheme, a user's password is registered to the remote system by submitting the user's identity. If the user's validity is certified, the remote system issues a smart card and passes the user's password to the user through a secure channel. To login to a remote system, the user has to attach their smart card into the reading device, then keys in his identity and the corresponding password. Because the identity table has

not been stored in the remote system, the remote system will check the validity of this identity according to the predefined format at the authentication stage. In November 2000, Chan and Cheng (2000) pointed out that Hwang and Li's scheme allowed any legitimate user to forge a valid identity and its corresponding password for login to the remote system illegally. However, they did not consider the condition of the identity format. In this paper, we show that Chan and Cheng's attack does not work always. Moreover, we propose several ways to accomplish Chan and Cheng's attack.

The rest of this paper is organized as follows. In Section 2, we review Hwang and Li's scheme and Chan and Cheng's attack. In Section 3, we propose several ways to obtain a valid identity and its corresponding password. Finally, Section 4 states the conclusions of our work.

2. Previous Work

2.1. *Hwang and Li's Scheme*

There are three stages in Hwang and Li's (Hwang and Li, 2000) remote user authentication scheme: Registration, login, and authentication. We review these stages as follows:

Registration. The remote system is referred to below as S and it uses the ElGamal's public-key cryptosystem (ElGamal, 1985). First, S chooses a large prime P and its secret key x_s. A user U_i registers his smart card and password PW_i to S by sending his identity ID_i. Here, the smart card records the pair (f, P), where f denotes a publicly known one-way function. Once the U_i's identity is verified, S computes his password PW_i as follows:

$$PW_i = ID_i^{x_s} \bmod P. \tag{1}$$

Afterwards, S delivers the smart card and the password PW_i to U_i secretly.

Login. In this stage, U_i attaches his smart card to the reading device, and then keys in his ID_i and PW_i. Afterwards, the smart card sends $C = (ID_i, C_1, C_2, T)$ to S for authentication. Here C_1, C_2, and T are computed as follows:

1. Generate a random number r.
2. Compute $C_1 = ID_i^r \bmod P$.
3. Compute $t = f(T \oplus PW_i) \bmod (P-1)$, where T denotes the current date and time (timestamp). Here $\oplus$ denotes the exclusive-or operation.
4. Compute $M = ID_i^t \bmod P$.
5. Compute $C_2 = M(PW_i)^r \bmod P$.

Authentication. Suppose that S receives C at the remote system's current time T'. S certifies the validity of U_i by the following steps:

1. Check the validity of ID_i. If the format of ID_i is incorrect, then the system will reject U_i's login request.
2. Check the authority of timestamp T, i.e., $(T' - T)$ must be less than or equal to $\triangle T$, where $\triangle T$ denotes the expected legal time interval caused by transmission delay.
3. If $C_2(C_1^{x_s})^{-1} \bmod P = ID_i^{f(T \oplus PW_i)}$ is satisfied, then S accepts the login request. Otherwise, U_i's request will be rejected.

2.2. *Chan and Cheng's Attack*

Chan and Cheng (2000) pointed out that there is a way to impersonate other legal user by a legal user in Hwang and Li's scheme. Chan and Cheng's attack is successful if a victim's identity satisfies a specific condition, i.e., $ID_v = ID_i \times ID_i \bmod P$. Here ID_i denotes the intruder's identity and ID_v denotes the victim's identity. Note that the identity ID_v may not represent a real user. However, S does not keep an authentication table. If the intruder has the corresponding password PW_i satisfying that $PW_v = ID_v^{x_s} \bmod P$, he still can successfully login to the system using the identity ID_v rather than his own identity ID_i. Chan and Cheng showed that the intruder had the capability to find out PW_v without knowing S's secret key x_s. We review their method as follows:

$$\begin{aligned} PW_v &= ID_v^{x_s} \bmod P \\ &= (ID_i \times ID_i)^{x_s} \bmod P \\ &= (ID_i^{x_s} \times ID_i^{x_s}) \bmod P \\ &= (PW_i \times PW_i) \bmod P. \end{aligned} \tag{2}$$

Here PW_i is the intruder's password and the modulo P is publicly known. Therefore, the intruder can obtain the valid password PW_v. Chan and Cheng concluded that the intruder can freely use the pair (ID_v, PW_v) to login to the remote system. However, we find that Chan and Cheng have made a mistake in their conclusion. Recalling Hwang and Li's scheme, in authentication stage, S first checks the format of the login user's identity. If the user's identity exhibits a wrong format, S will definitely reject the user's login request. Since Hwang and Li's method cannot guarantee that the specific format always fits the square of a legitimate identity, i.e., $ID_i^2 \bmod P$, their attack does not succeed always. In the next section, we extend Chan and Cheng's attack to make the forged identity possible.

3. The Extended Attacks

In this section, we present some ways which allow a legitimate user, say U_i, to obtain an acceptable identity and its corresponding password. We describe these possible ways to obtain a valid and acceptable pair (ID_v, PW_v) as follows:

Let $ID_v = ID_i^r \bmod P$, where r is an arbitrary integer. The corresponding password of ID_v can be obtained by

$$PW_v = PW_i^r \bmod P. \tag{3}$$

If ID_i is a primitive element of the modulus P, then U_i has the capability to compute all the valid identity ID_v's and its corresponding password PW_v's by Eq. 3. Otherwise, U_i still has possibility to obtain a valid identity. Note that the possibility highly depends on what the identity format is defined. Obviously, Chan and Cheng's attack is only a special case of this method, i.e., $r = 2$.

Example 1.

Let $P = 3571$, $x_s = 921$. Suppose a valid user's identity $ID = 1109$ and his corresponding password $PW = 1109^{921} \bmod P = 2766$. To check the identity format, we use the 2-LSBs (least significant bit) as the verification code, i.e., the 2-LSBs must be the same as its previous two bits. For instance, $ID = 1109$ satisfies the identity format because $1109 = (10001010101)_2$. Here we see that the verification code "01" is exactly the same as the pattern of its previous two bits. When Chan and Cheng's attack is applied, we can obtain $ID_v = ID^2 \bmod P = 1457$ and $PW_v = 2766^2 \bmod P = 1674$. Although $1674 = 1457^{x_s} \bmod P$, the impersonated identity $PW_v = 1457$ does not satisfy the identity format, because the verification code "01" is not equal to the pattern of its previous two bits "00" ($1457 = 10110110001_2$. Thus, Chan and Cheng's attack does not work in this case. Now, we apply the proposed scheme here. Let $r = 5$, and then we can obtain $ID_v = ID^5 \bmod P = 655$ as well as the corresponding password $PW_v = 2766^5 \bmod P = 659$. We can see that $655 = (1010001111)_2$, which satisfies the identity format.

According to the above mentioned mechanism, there are many various ways to obtain an acceptable identity and its password. For example, several users U_{i_j}'s can conspire to obtain a valid identity as well as its corresponding password in the following:

$$ID_v = \prod ID_{i_j} \bmod P. \tag{4}$$

If ID_v fits the identity format, then its corresponding password can be computed by

$$\begin{aligned} PW_v &= ID_v^{x_s} \bmod P \\ &= \left(\prod ID_{i_j} \right)^{x_s} \bmod P \\ &= \prod PW_{i_j} \bmod P. \end{aligned} \tag{5}$$

Besides, if ID_v is a primitive element of the modulus P, then these users U_{i_j} can conspire to compute all the passwords of the identities that exhibit valid format.

Although the above mentioned schemes have the capability to obtain a valid identity with its corresponding password, they do not provide an efficient way to find an arbitrary

valid identity's password. In other words, given an arbitrary valid identity, these schemes are still hard to obtain its corresponding password. However, because the remote system does not keep the valid users' identities, once a valid identity is computed, e.g, $ID_i^r \bmod P$, its corresponding password will be obtained easily, i.e., $PW_i^r \bmod P$.

Furthermore, there is a possible way to obtain the remote system's secret key x_s. If the equation $x_s \leqq \log_{ID_i}(P-1)$ is satisfied, then U_i can obtain x_s by computing $x_s = \log_{ID_i} PW_i$. In this case, Hwang and Li's authentication mechanism will be wholly impractical.

4. Conclusions

In this paper, we have presented that Chan and Cheng's attack does not always work well because they did not consider the condition of user's identity format (see Example 1). Furthermore, we proposed several ways that enable an attacker to obtain a really valid identity as well as its corresponding password.

References

Chan, C.K., and L.M. Cheng (2000). Cryptanalysis of a remote user authentication scheme using smard cards. *IEEE Transcations on Consumer Electronics*, **46**(4), 992–993.

Dhem, J.F., and N. Feyt (2001). Hardware and software symbiosis helps smart card evolution. *IEEE Micro*, **21**(1), 14–25.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, **31**(4), 469–471.

Hwang, M.S., and L.H. Li (2000). A new remote user authentication scheme using smard cards. *IEEE Transcations on Consumer Electronics*, **46**(1), 28–30.

Toji, R., Y. Wada, S. Hirata and K. Suzuki (2001). A network-based platform for multi-application smart cards. In *Proceedings of Fifth IEEE International Conference on Enterprise Distributed Object Computing*. pp. 34–45.

C.-C. Chang was born in Taichung, Taiwan, the Republic of China, on November 12, 1954. He received his BS degree in applied mathematics in 1977 and his MS degree in computer and decision sciences in 1979 from National Tsing Hua University, Hsinchu, Taiwan. He received his Phd in computer engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. From 1983 to 1989 he was among the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. Since August 1989, he has worked as a professor of the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Dr. Chang is a fellow of IEEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.

K.-F. Hwang was born in Changhua, Taiwan, the Republic of China, on October 11, 1970. He received his BS in construction engineering from National Lien-Ho College of Technology and Commerce, Taiwan, the Republic of China, in 1991 and received his MS degree in information management in 1999 from Chaoyang University of Technology, Taichung, Taiwan. He also studied information manager at Chaoyang University, Taiwan, from 1996–1997. In 2002, he received his Phd in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan. From July 1993 to September 1994, he was the associate manager at the Spiringfront Computer Co., Ltd, Taipei, Taiwan. From October 1994 to June 1995, he was a structural engineer at the Paoshan Construction Co., Ltd, Taichung, Taiwan. He also was a structural engineer at the Cahsin Corporation, Taichung, Taiwan, from 1995–1996. Since August 2002, he has worked as an assistant professor of the Department of Multimedia Design at National Taichung Institute of Technology, Taichung, Taiwan. His research interests include cryptography, image processing, and wireless communications.

Klastojimo atakos prieš mikroprocesorinę kortelę, naudojančią nutolusio vartotojo tapatumo nustatymo schemą

Chin-Chen CHANG, Kuo-Feng HWANG

Mikroprocesorinė kortelė buvo pritaikyta įvairiems taikymams. Hwang ir Li 2000 m. pasiūlė nutolusio vartotojo tapatumo nustatymo schemą, kuri naudoja mikroprocesorinę kortelę. Po 6 mėn. Chan ir Cheng surado, kad Hwang ir Li pasiūlyta schema turi trūkumų. Šiame straipsnyje mes parodome, kad Chan ir Cheng'o schema yra nepilnai patikima, nes ji neįvertina vartotojo identifikavimo formato. Be to, mes siūlome keletą būdų, kaip išspręsti Chan ir Cheng'o schemos patikimumo problemą.