Cryptanalysis of A User Friendly Remote Authentication Scheme with Smart Card

[1]Min-Shiang Hwang, [2,3]Jung-Wen Lo, [4]Chi-Yu Liu, [5]Shu-Chen Lin

[1]Department of Management Information System
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
http://isrc.nchu.edu.tw
Email: mshwang@nchu.edu.tw
Fax: 04-22857173

[2]Department of Computer Science
National Chung Hsing University

[3]Department of Information Management
National Taichung Institute of Technology
129 Sec. 3, San-min Rd., Taichung, Taiwan 404, R.O.C

[4]Graduate Institute of Networking and Communication Engineering
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.

[5]Department of Information Management
Chaoyang University of Technology

Abstract

Recently, Wu-Chieu proposed an efficient and friendly remote authentication scheme with smart card. This scheme is very elaborate since no password table in the remote system, and could keep as well as low communication and low computation costs. In addition, freely choosing and changing password is very friendly for users. However, their scheme could not withstand the forged attack. Flaw is proposed in this study.

Keywords: Cryptography, password, remote login, smart card, user authentication.

Introduction

At present, if we desires any service, we just remote login to a server which provides the service. The password authentication schemes are the well known and the most accepted mechanisms. These schemes use the correct password to authenticate the right user who wants to login the system. Only a legal user who has registered in system with corresponding password can use the system resources.

There are varieties of the password remote authentication schemes with smart card [1-10]. These schemes can allow a legal user to login the remote system with his/her password and identity. In 2000, Sun proposed a scheme which authenticates user's validity without storing a password table and ensures the low communication and low computation [9]. However, Sun's method was not friendly, the fixed and unknown password could not satisfy user's request. Then, Wu and Chieu proposed an improved scheme in 2003 [11]. Their scheme allows users to choose a password randomly.

In this article, it is pointed out that Wu-Chieu's scheme could not withstand forge attack. An attacker can login the remote system without knowing anyone's password.

Wu-Chieu's scheme

There are three phases in this scheme: registration phase, login phase, and authentication phase. The following is the brief description of each phase.

Registration phase:

Firstly, a user submitted his/her identity $\mathrm{ID_i}$ and a chosen password $\mathrm{pw_i}$ to the system through a secure channel. Then, the system performs the following steps:

- Step 1: Compute $A_i = h(ID_i, x)$, where x is a secret key of the system and h(.) is a one-way hash function.
- Step 2: Compute $B_i = g^{Aih(pwi)} \mod p$, where p is a large prime number, and g is a primitive element in $GF(p)$.
- Step 3: The messages $\{ID_i, A_i, B_i, h(.), p, g\}$ are stored in a smart card.

Login phase:

When a user wants to login the system, he/she must insert his/her smart card into a device. Then, the user keys in his/her ID_i and pw_i, and the input device with smart card will perform the following steps:

- Step 1: Compute two integers $B_i^* = g^{A_i h(pw_i^*)}$ and $C1 = h(T \oplus Bi)$, where T is the current date and time of the input device.
- Step 2: Send the message $m = \{ID_i, B_i^*, C_1, T\}$ to the remote system.

Authentication phase:

After received the message m, the system performs the following steps to verify the user's identity.

- Step 1: Check the format of the ID_i. If the format is not correct, the login request will be rejected.
- Step 2: Verify the validity of the time interval between T and T'. If $(T' - T) \geqq \Delta T$ where the ΔT is the expected valid time interval for transmission delay, then the login request will be rejected.
- Step 3: Compute $\mathrm{C_1^* = h(T \oplus B_i^*)}$, and compare $C1$ and $\mathrm{C_1^*}$. If they are equal, the system accepts the login request.

Attacks on Wu-Chieu's scheme

In this section, we show that Wu-Chieu's scheme cannot withstand a masquerade attack. In this scheme, an illegal user could login the server without obtain any password.

We suppose that an attacker wants to login a remote server. He performs the following steps before goes into the authentication phase, and he will login the remote server successfully.

- Step 1: The attacker forges an ID_i with applicable format or tries to obtain a legal user's ID_i by using any way, such as intercepting from the network flows.
- Step 2: He randomly chooses a $B_i^{'}$ and, computes $\mathrm{C}_1^{'} = \mathrm{h}(\mathrm{T} \oplus \mathrm{B}_\mathrm{i}^{'})$, where T is the current time.
- Step 3: He sends the message $m' = \{ID_i, B_i^{'}, C_1^{'}, T\}$ to the remote system.
- Step 4: When the remote system receives the message m, it will go into the authentication phase and performs the following checks.
    - It checks the format of the IDi. Of course, it is correct.
    - Then, it checks the time is valid or not. Because $T' - T \leqq \Delta T$, where T' is the arrived time of message m, the system will accept this check.
    - It computes $\mathrm{C}_\mathrm{s} = \mathrm{h}(\mathrm{T} \oplus \mathrm{B}_\mathrm{i}^{'})$, and compares with the $\mathrm{C}_1^{'}$. No doubt, C_s is the same as $\mathrm{C}_1^{'}$, so this step is satisfied.

Therefore, the remote system will accept the login request, because the attacker could pass through the all authentication checks of the system.

Conclusion

In this study, we have shown that Wu-Chieu's scheme is not secure. We forge the B_i, and it's could be approved by the system authentication phase. In the future, if we want to develop a remote authentication scheme with smart card, we should achieve the following two goals in order to guarantee the security.

1. When a user's smart card is lost, he/she will not worry about the information which are stored in the smart card would be divulge.
2. The smart card could store the user's password. When a user wants to login a remote system, he/she must have the correct password to use this smart card.

References

[1] Chang C. C., and Hwang S. J., 1993. Using smart cards to authenticate remote passwords. Computers and Mathematics with Applications, vol. 26, no. 7, pp. 19-27.

[2] Chang C. C., and Wu T. C., May 1991. Remote password authentication with smart cards. IEE Proceedings-E, vol. 138, pp. 165-168.

[3] Hwang M. S., 1999. A remote password authentication scheme based on the digital signature method. International Journal of Computer Mathematics, vol. 70, pp. 657-666.

[4] Hwang M. S., Lee C. C., and Tang Y. L., 2001. An improvement of SPLICE/AS in WIDE against guessing attack. International Journal of Informatica, vol. 12, no. 2, pp. 297-302.

[5] Lee C. C., Hwang M. S., and Yang W. P., 2002. An exible remote user authentication scheme using smart cards. ACM Operating Systems Review, vol. 36, no. 3, pp. 46-52.

[6] Lee C. C., Li L. H., and Hwang M. S., 2002. A remote user authentication scheme using hash functions. ACM Operating Systems Review, vol. 36, no. 4, pp. 23-29.

[7] Li L. H., Lin I. C., and Hwang M. S., 2001. A remote password authentication scheme for multi-server architecture using neural networks. IEEE Transactions on Neural Networks, vol. 12, no. 6, pp. 1498-1504.

[8] Peyravian M., and Zunic N., 2000. Methods for protecting password transmission. Computers & Security, vol. 19, no. 5, pp. 466-469.

[9] Sun H. M., 2000. An e_cient remote use authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 958-961.

[10] Tang Y. L., Hwang M. S., and Lee C. C., 2002. A simple remote user authentication scheme. Mathematical and Computer Modelling, vol. 36, pp. 103-107.

[11] Wu S. T., and Chieu B. C., 2003. A user friendly remote authentication scheme with smart card. Computers & Security, vol. 22, no. 6, pp. 547-550.