Cryptanalysis of a Secure One-Time Password Authentication Scheme with Low-Communication for Mobile Communications

Hsien-Chu Wu[1], Chi-Yu Liu[2] and Shu-Fen Chiou[3]
(Corresponding author: Hsien-Chu Wu)

Department of Information Management, National Taichung Institute of Technology[1],
129 Sec. 3, San-min Rd., Taichung, Taiwan 404, R.O.C. (Email: wuhc@ntit.edu.tw)
Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology[2],
168 Gifeng E. Rd., Wufeng Taichung County, Taiwan 413, R.O.C.
Department of Computer Science, National Chung Hsing University[3],
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C.

(Received March 18, 2005; revised and accepted April 1, 2005)

Abstract

User authentication is a most important protocol in a distribution network. Those authentication schemes have been proposed for many years, and a one-time password authentication scheme is one of them. In 2004, Lin and Chang proposed a one-time password authentication scheme which is free from replay attacks, server spoofing attacks, off-line dictionary attacks, active attacks, and revelation of message contents. However, their scheme will suffer from guessing attacks which is proposed by us in this paper.

Keywords: Authentication, guessing attacks, one-time password, replay attacks, security

1 Introduction

The network service brings a great modern convenience. Users are able to request various services through the network, or obtain the most information about existence, etc. It is avoidable that people abuse those services, and the providers will establish some rules of the requirements such as authenticating the identity of a user who requests services. Those protocols can ensure that users are not deliberately using the services. There were many user identity authentication protocols proposed in the past. The user authentication scheme using passwords is one of the best-known protocols that could be easily implemented, and there are many books about that have been proposed such as [2, 4, 5, 6, 7, 8, 10, 12, 13, 14, 15, 16].

In 1981, Lamport [3] proposed a one-time password which could avoid replay attack conception in each communication. Afterward The Internet Engineering Task Force (IETF) proposed Haller's scheme [1] as S/Key one-time password system, which could ensure that it is not vulnerable to eavesdropping/replay attacks. However, Yeh et al. [17] demonstrated out that his scheme did not resist the server spoofing attacks. In addition, [11] also pointed out that Haller's scheme will suffer from off-line dictionary attacks, pre-play attacks, and a special form of replay attacks. In 2002, Yeh et al. [17] proposed an improvement scheme and claimed their scheme was suitable in a sensitive environment. But Lin and Chen [9] thought their scheme was unsuitable for lighter devices in a mobile environment. They designed a new algorithm to reduce the computation of a lighter device. In this article, we will show their scheme as having suffered from guessing attacks.

In Section 2, we will review Lin and Chang's scheme including two phases. Next, we will propose an attack for Lin and Chang's scheme. A brief conclusion is presented in Section 4.

2 Review of Lin-Chang Scheme

In this section, we review Lin and Chang's scheme. There are two phases in the scheme: registration, and login and authentication phases. The following is a brief description of each phase.

Initially, users will obtain a smart card containing a unique secret SEED from the server. When the user first wants to login the server, he/she should register at the server. User sends a request to the server, the server will replay $SEED \oplus SK$, where SK is a session key, that is,

$SK = D\|T$. And then, the user generates a secret key K, and computes $IK = K \oplus SEED$. Next, the user sends $IK \oplus SK$, and $N \oplus SK$ to the server, where N is that user decides the number of login. As the server obtains the information, it will compute $p_0 = H^N(IK)$, $p_1 = H^{N-1}(IK)$, and $p_2 = H^{N-2}(IK)$, and then it transmits $p_0 \oplus SK, p_1 \oplus SK, p_2 \oplus SK$ to the user. The user obtains p_0, p_1, p_2, and he/she stores three values in the smart card.

In login and authentication phase, the server receives the user's requirement of the tth time of login, it will compute $p_{t-1} = H^{N-t+1}$ and respond to $p_{t-1} \oplus SK$, $SEED \oplus SK$. The user can check the validity of the identity of the server according to the pre-shared value $SEED$. If the equation is equal, the user sends $p_t \oplus SK$ where p_t is original in the smart card. Next, the server compares $H(p_t)$ with p_{t-1}. If the two values are equal, the server is able to ensure the user's identity.

Above decryption is Lin and Cheng's scheme. Although they proposed an efficient algorithm for mobile devices, theirs is not secure. In the next section, we will reveal their scheme will force what the attack is.

3 Attack on Lin-Chang Scheme

In this section, we show that Lin and Chang's scheme cannot withstand a guessing attack. An attacker could scratch all the information transmitted on Internet. When he obtains a user communicating message in the registration phase, he could save those messages and proceed off-line guessing attacks to obtain the secret value SEED. The attack processes are described as follows.

1) When a valid user performs the registration to a server, the attacker could obtain the information $SEED \oplus SK$, $IK \oplus SK$, $N \oplus SK$, $p_0 \oplus SK$, $p_1 \oplus SK$, and $p_2 \oplus SK$ though the public network.

2) The attacker could utilize the information to proceed off-line guessing attacks. First, he assumes the number of decided logins by the user N', and performs the following equations:

   E1: $SK' = N' \oplus (N \oplus SK)$

   E2: $p'_0 = SK' \oplus (SK \oplus p_0)$

   E3: $p'_1 = SK' \oplus (SK \oplus p_1)$

   E4: $H(p'_1) \stackrel{?}{=} p'_0$

   If the equation E4 is not equal, the attacker will select the other N' and computes above equations until E4 is equal. If E4 is equal, that is denoted the attacker guesses correctly N'. And then, he could obtain the correct section key SK, and compute $SK \oplus (SEED \oplus SK)$. Finally, he could get the user's pre-shared secret $SEED$ with the server.

The conception of our attacking method is that the scheme allows a user to choose the number of login N. Generally, the login times N is not a big value, and it is easily guessed. As the attacker gets the correct secret $SEED$, he could forge the valid user to login the server, and request any services which is provided by the server.

4 Conclusion

In 2004, Lin and Chang proposed an efficient one-time password authentication scheme. Their scheme is more suitable in mobile network than others, but the scheme is insecure. In this article, we explain their scheme unable to withstand guessing attacks. When an attacker utilizes some messages sent by the user in registration phase, he could easily guess right N which is selected by the user himself. And then, he could obtain all secret values. Because the user decides on the number of logins N which is easily guessed, and the scheme protects it with SK, the attacker could easily guess correctly. There is one suggestion that the security of login times N is not imperative, and it could be sent with a plaintext. There will be no affect from the attack.

References

[1] N. M. Haller. "A one-time password system,". Tech. Rep. RFC 1938, May 1996.

[2] M. S. Hwang, J. W. Lo, C. Y. Liu, and S. C. Lin, "Cryptanalysis of a user friendly remote authentication scheme with smart card," *Pakistan Journal of Applied Sciences*, vol. 5, no. 1, pp. 99–100, 2005.

[3] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, pp. 770–772, November 1981.

[4] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart cards," *ACM Operating Systems Review*, vol. 36, no. 3, pp. 46–52, 2002.

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

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

[7] C. W. Lin, J. J. Shen, and M. S. Hwang, "Security enhancement for optimal strong-password authentication protocol," *ACM Operating Systems Review*, vol. 37, no. 2, pp. 7–12, 2003.

[8] I. C. Lin, M. S. Hwang, and L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13–22, 2003.

[9] M. H. Lin and C. C. Chang, "A secure one-time password authentication scheme with low-computation for mobile communications," *ACM SIGOPS Operating Systems Review*, vol. 38, no. 2, pp. 76–84, Apr. 2004.

[10] W. P. Yang, M. S. Hwang, C. C. Lee, "An improvement of mobile users authentication in the integration environments," *International Journal of Electronics and Communications*, vol. 56, no. 5, pp. 293–297, 2002.

[11] C. J. Mitchell and L. Chen, "Comments on the S/KEY user authentication scheme," *ACM Operating System Review*, vol. 30, no. 4, pp. 12–16, 1996.

[12] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414–416, 2003.

[13] J. J. Shen, C. W. Lin, and M. S. Hwang, "Security enhancement for the timestamp-based password authentication scheme using smart cards," *Computers & Security*, vol. 22, no. 7, pp. 591–595, 2003.

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

[15] C. C. Yang, T. Y. Chang, and M. S. Hwang, "The security of the improvement on the methods for protecting password transmission," *Informatica*, vol. 14, no. 4, pp. 551–558, 2003.

[16] C. C. Yang, T. Y. Chang, J. W. Li, and M. S. Hwang, "Security enhancement for protecting password transmission," *IEICE Transactions on Communications*, vol. E86-B, no. 7, pp. 2178–2181, 2003.

[17] T. C. Yeh, H. Y. Shen, and J. J. Hwang, "A secure one-time password authentication scheme using smart cards," *IEICE Transactions on Communications*, vol. E85, no. 11, pp. 2515–2518, 2002.

Hsien-Chu Wu was born in Tainan, Taiwan, Republic of China, on October 26, 1962. She received the B.S. and M.S. degrees in Applied Mathematics in 1985 and 1987, respectively, from the National Chung Hsing University, Taichung, Taiwan. She received her Ph.D. in Computer Science and Information Engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. From 1987 to 2002, she was a lecture of the Department of Information Management at National Taichung Institute Technology, Taichung, Taiwan. Since August 2002, she has worked as an associate professor of the Department of Information Management at National Taichung Institute Technology, Taichung, Taiwan. Her research interests include image authentication, digital watermarking, image processing and information security.

Chi-Yu Liu see page 73.

Shu-Fen Chiou received a B.B.A degree in Information Management from National Taichung Institute of Technology, Taichung, Taiwan, Republic of China in 2004. She is currently pursuing her M.S. degree in Computer Science from National Chung Hsing University. Her current research interests include information security, 2-D Electrophoresis Image analysis and DNA microarray image analysis.