On Security of An Efficient Nonce-based Authentication Scheme for SIP

Cheng-Chi Lee
Department of Information & Communication Engineering, Asia University
500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C. (Email: cclee@asia.edu.tw)
(Received July 30, 2008; revised and accepted Oct. 2, 2008)

Abstract

Recently, Tsai proposed an efficient nonce-based authentication scheme for session initiation protocol (T-SIP for short). However, the author shall show that T-SIP is vulnerable to perfect forward secrecy, password guessing attacks, and insider attacks.

Keywords: Authentication, guessing attacks, insider attacks, perfect forward secrecy, session initiation protocol

1 Introduction

The Session Initiation Protocol (SIP) was proffered as the application layer's protocol by IETF (Internet Engineering Task Force) in 1999 and was built in RFC2543 [1]. SIP is the signaling protocol that controls communication on the Internet, establishing, maintaining and terminating the sessions. SIP is a client-server protocol. User authentication is the most important technique for SIP. When a user wants to use SIP, the user must be authenticated by the server.

Recently, Tsai proposed an efficient nonce-based authentication scheme for SIP called T-SIP [7]. T-SIP is based on the random nonce. All messages exchange are encrypted/decrypted by using one-way hash function and exclusive-or operation. Thus, the computation cost of T-SIP is very low and is very suitable for low computation power equipment such as mobile device. However, this paper shall show that T-SIP is vulnerable to perfect forward secrecy, password guessing attacks, and insider attacks. I explain these security weaknesses in Section 3 in detail.

2 Review of Tsai's Scheme

In this section, I review Tsai's authentication scheme. In Table 1, I list the abbreviations and notations used in Tsai's scheme.

2.1 Registration Phase

When a user wants to register with his/her sever, the user first submits his/her username and password PW to the remote server. The username and password is used to verify the identity of the user and server. After receiving the username and password, the server stores the user's username and password PW into the verification table.

2.2 Authentication Phase

If a user wants to login remote server, he/she must enter username and password. The detailed steps are shown in the following and in Figure 1.

Step 1. U generates a random number N_C and sends Request (username, N_C) to S.

Step 2. After receiving these messages, S generates a random number N_S and computes $N_S \bigoplus H(PW||N_C)$ and $H(PW||N_S||N_C)$. Then S sends Challenge ($realm$, $N_S \bigoplus H(PW|| N_C)$, $H(PW|| N_S|| N_C)$) to U.

Step 3. After receiving these messages, U computes $H(PW||N_C)$ to derive N_S from $N_S \bigoplus H(PW||N_C)$. Then, U computes $H(PW||N_S||N_C)$ and compares it with the received $H(PW||N_S||N_C)$. If it is not the same, the user rejects the server request. Otherwise, the user computes $H(N_S||PW||N_C)$ and sends Response (username, realm, $H(N_S||PW||N_C)$) to S.

Step 4. After receiving these messages, S computes $H(N_S||PW||N_C)$ and compares it with the received $H(N_S||PW||N_C)$. If it is not the same, the server rejects the user request. Otherwise, the server accepts the user login. After that, the mutual authentication is done and the session key N_S is distributed between U and S.

3 Security Weaknesses

In this section, I shall show that T-SIP authentication scheme is vulnerable to perfect forward secrecy, password guessing attacks, and insider attacks.

Table 1: The notations

Notations	Description
U	the client user
S	the server
PW	the user's password
N_C	the nonce generated by U
N_S	the nonce generated by S, also the session key between U and S
$H()$	a one-way hash function
$\bigoplus$	the XOR operation
$\|\|$	the concatenation

3.1 Perfect Forward Secrecy

The perfect forward secrecy is when a party's long-term private key is compromised, it will never reveal any old short-term keys used previously [3, 8]. It is easily seen that Tsai's scheme cannot achieve the perfect forward secrecy. When a user's password PW is compromised, all the session keys N_Ss are known. I explain it as follows. Assume that we know PW. N_C is also known because we can intercept it from public channel. After that, we can compute the session key N_S from $N_S \bigoplus H(PW||N_C)$ because of $N_S \bigoplus H(PW||N_C) \bigoplus H(PW||N_C)$. Thus, if we know PW and N_C, any old short-term session keys are compromised. Therefore, Tsai's scheme cannot achieve the perfect forward secrecy.

3.2 Password Guessing Attacks

Most passwords have such low entropy that it is vulnerable to password guessing attacks, where an attacker intercepts authentication messages and stores them locally and then attempts to use a guessed password to verifies the correctness of his/her guess using theses authentication messages [4, 5, 6]. In Tsai's scheme, an attacker can intercept N_C, $N_S \bigoplus H(PW||N_C)$, and $H(PW||N_S||N_C)$. Then, the attacker can guess a password PW' and computes $H(PW'||N_C)$. He/she derives N'_S from $N_S \bigoplus H(PW||N_C)$. Then, he/she computes $H(PW'||N'_S||N_C)$. If it is equal to $H(PW||N_S||N_C)$, the guessing password PW' is correct. Otherwise, the attacker repeatedly guesses a new PW'. Thus, Tsai's scheme is vulnerable to password guessing attacks.

3.3 Insider Attacks

The insider attacks is when the user's password is obtained by the server in the registration phase [2]. To prevent the insider attacks, the user must conceal his/her password from the server. It is easily seen that Tsai's scheme cannot prevent the insider attacks because the password PW is known to the server in the registration phase.

4 Conclusions

In this paper, I had pointed out that Tsai's scheme is vulnerable to perfect forward secrecy, password guessing attacks, and insider attacks.

Acknowledgments

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC97-2218-E-468-010. The authors are grateful to the anonymous reviewers for valuable comments.

References

[1] M. Handley, H. Schulzrinne, U. Columbia, E. Schooler, Cal Tech, J. Rosenberg, and Bell Labs, *SIP: Session Initiation Protocol*, IETF RFC2543, Mar. 1999.

[2] W. Ku, and S. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 204-207, 2004.

[3] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683-1687, 2006.

[4] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727-740, 2006.

[5] R. Lu, and Z. Cao, "Off-line password guessing attack on an efficient key agreement protocol for secure authentication," *International Journal of Network Security*, vol. 3, no. 1, pp. 35-38, 2006.

[6] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password authentication schemes: current status and key issues," *International Journal of Network Security*, vol. 3, no. 2, pp. 101-115, Sept. 2006.

[7] J. L. Tsai, "Efficient nonce-based authentication scheme for session initiation protocol," *International*

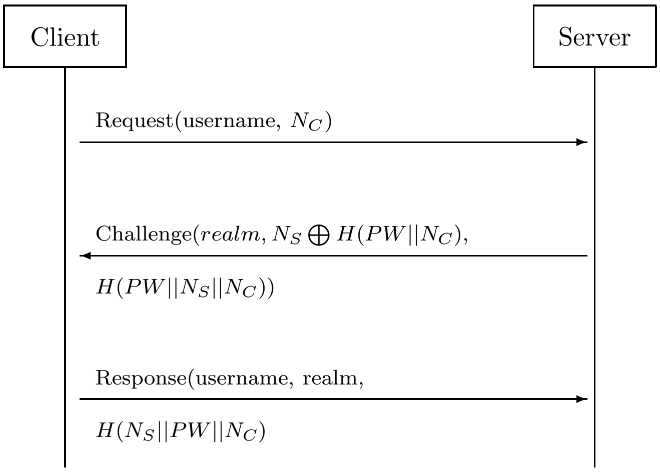

Figure 1: T-SIP authentication scheme

Journal of Network Security, vol. 8, no. 3, pp. 312-316, 2009.

[8] B. Wang, and Z. Q. Li, "A forward-secure user authentication scheme with smart cards," *International Journal of Network Security*, vol. 3, no. 2, pp. 116-119, Sept. 2006.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 1999 and in 2001. He researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He received the Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He was a Lecturer of Computer and Communication, Asia University, from 2004 to 2007. From 2007, he is a assistant professor of Computer and Communication, Asia University. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 30 articles on the above research fields in international journals.