New Cryptanalysis Paradigm on a Nonce-based Mutual Authentication Scheme

Da-Zhi Sun[1] and Zhen-Fu Cao[2]
(Corresponding author: Da-Zhi Sun)

School of Computer Science and Technology, Tianjin University[1]
No 92 Weijin Road, Nankai District, Tianjin 300072, China (Email: sundazhi1977@126.com)
Department of Computer Science and Technology, Shanghai Jiao Tong University[2]
1954 HuaShan Road, Shanghai 200030, China

(Received Feb. 7, 2006; revised and accepted May 7, 2006)

Abstract

In 2005, Lee, Kim, and Yoo proposed a nonce-based mutual authentication scheme using smart cards. However, this paper demonstrates that Lee-Kim-Yoo's scheme is vulnerable to an impersonation attack that the attacker without knowing the remote user's any secret can masquerade as him by obtaining the valid authentication message from any normal session between the remote user and the system. Our purpose is to emphasize that it is dangerous that the remote user and the system separately implement their authentication operations without any logical relation to achieve the mutual authentication. Furthermore, we suggest that the tool of matching conversations would be useful as a sanity check to find this kind of the security breach.

Keywords: Impersonation attack, matching conversation, mutual authentication, smart card

1 Introduction

Entity authentication [10] is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in the session of a scheme, and that the second has actually participated, i.e., is active at, or immediately prior to, the time the evidence is acquired. One of the primary purposes of entity authentication is to facilitate access control to a resource, when an access privilege is linked to a particular identity, e.g., local or remote access to computer accounts; withdrawals from automated cash dispensers; communications permissions through a communications port; physical entry to restricted areas or border crossings. In recent years, many scholars had proposed a lot of entity authentication schemes using smart card. A legal remote user can use his smart card to log in the system and access the value information provided by the system. According to the different cryptographic assumptions, we roughly classify such schemes into four categories: (1) the schemes based on the factorization and discrete logarithm problems, e.g., Yang-Shieh's scheme [12]; (2) the schemes based on the discrete logarithm problem, e.g., Hwang-Li's scheme [6]; (3) the schemes based on the factorization problem, e.g., Lu-Cao's scheme [9]; (4) the schemes based on the one-way cryptographic hash function, e.g., Sun's scheme [11], Hwang-Lee-Tang's scheme [5], and Chien-Jan-Tseng's scheme [2]. Certainly, the schemes based on the one-way cryptographic hash function are always more efficient than other types of schemes. Mutual authentication between the remote user and the system is indispensable to ensure the security in some application environments. A natural design idea is to use the same authentication structure in both the remote user and the system. We consider the mutual authentication following this idea is obtained by running any of the unilateral authentication schemes twice (once in each direction). Although this design idea is very simple and efficient, we believe the schemes derived from it are always insecure. For example, in the session period, Chien-Jan-Tseng's timestamp-based mutual authentication [2] can be treated as running Hwang-Lee-Tang's timestamp-based unilateral authentication scheme [5] twice. In fact, Chien-Jan-Tseng's scheme is vulnerable to the parallel session attack [4] and the reflection attack [7].

In 2005, Lee, Kim, and Yoo [8] also proposed a nonce-based mutual authentication scheme using smart cards. It also employs the same authentication structure in both the remote user and the system. Due to the random nonce, Lee-Kim-Yoo's scheme doesn't seem to suffer the parallel session attack and the reflection attack. However, this paper demonstrates that Lee-Kim-Yoo's scheme is vulnerable to an impersonation attack that the attacker without knowing the remote user's any secret can masquerade as him by obtaining the valid authentication message from any normal session between the remote user and the system. Through this cryptanalysis result, we aim to

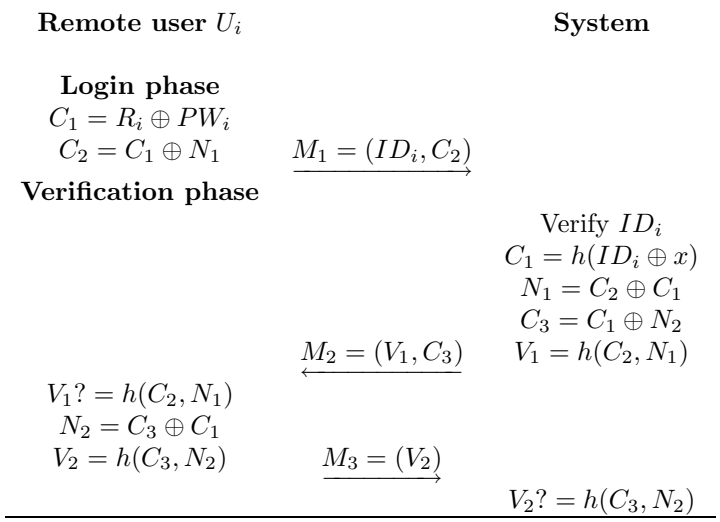

Figure 1: Challenge-response of Lee-Kim-Yoo's scheme

emphasize that such an ad-hoc combination idea cannot logically be associated with a secure mutual authentication scheme.

2 Lee-Kim-Yoo's Scheme

In order to make our attack easier to understand, we review the main points of Lee-Kim-Yoo's scheme. The precise technical description appears in [8].

2.1 Registration Phase

Let x be the only secret key maintained by the system, and $h(\cdot)$ be a one-way cryptographic hash function. Assume a remote user U_i registers his identifier ID_i and password PW_i to the system in a secure channel. The system computes $R_i = h(ID_i \oplus x) \oplus PW_i$, where $\oplus$ denotes the bit-wise exclusive-OR operator, stores $h(\cdot)$ and R_i into the memory of a smart card, and issues the smart card to U_i.

2.2 Login Phase

When U_i wants to log into the system, he inserts his smart card into the terminal, and enters his identifier ID_i and password PW_i. The smart card then performs the following operations:

1) Compute $C_1 = R_i \oplus PW_i$ and $C_2 = C_1 \oplus N_1$, where N_1 is a random nonce.

2) Send the message $M_1 = (ID_i, C_2)$ to the system.

2.3 Verification Phase

After the authentication request message M_1 is received, the system and the smart card execute the following operations to achieve mutual authentication.

1) The system checks the validity of ID_i. Then the system computes $C_1 = h(ID_i \oplus x)$, $N_1 = C_2 \oplus C_1, V_1 = h(C_2, N_1)$, and $C_3 = C_1 \oplus N_2$, where N_2 is a random nonce.

2) The system sends the message $M_2 = (V_1, C_3)$ to U_i.

3) Upon receiving the message M_2, U_i verifies whether $V_1? = h(C_2, N_1)$. If equals, U_i believes that the system is authenticated. Then the smart card computes $N_2 = C_3 \oplus C_1$ and $V_2 = h(C_3, N_2)$.

4) The smart card sends the message $M_3 = (V_2)$ to the system.

5) The system verifies whether $V_2? = h(C_3, N_2)$. If equals, the system believes that U_i is authenticated.

Figure 1 highlights the authentication session of this scheme, which is important for our security discussions.

3 Impersonation Attack on Lee-Kim-Yoo's Scheme

Assume an attacker wants to impersonate a target remote user U_i. The impersonation attack can be described as follows:

1) When U_i sends the message $M_1 = (ID_i, C_2 = C_1 \oplus N_1 = h(ID_i \oplus x) \oplus N_1)$ to the system, the attacker also initiates a session with the system and sends the message $M_{a1} = (ID_i, C_{a2})$, where the parameter C_{a2} is a random number.

2) After receiving the message M_1 and M_{a1}, the system respectively generates and sends $M_2 = (V_1 = h(C_2, N_1), C_3 = C_1 \oplus N_2)$ and $M_{a2} = (V_{a1} = h(C_{a2}, N_{a1}), C_{a3} = C_1 \oplus N_{a2})$ in two sessions, where $N_{a1} = C_{a2} \oplus C_1$. After the attacker intercepts and

Remote user U_i		**Attacker**		**System**
Login phase				
$C_1 = R_i \oplus PW_i$	$M_1 = (ID_i, C_2) \longrightarrow$		$M_1 = (ID_i, C_2) \longrightarrow$	
$C_2 = C_1 \oplus N_1$				
			$\overset{M_{a1}=(ID_i, C_{a2})}{- - - - - \dashrightarrow}$	
Verification phase				
				Verify ID_i
				$C_1 = h(ID_i \oplus x)$
				$N_1 = C_2 \oplus C_1$
				$C_3 = C_1 \oplus N_2$
			$M_2 = (V_1, C_3) \longleftarrow$	$V_1 = h(C_2, N_1)$
				Verify ID_i
				$C_1 = h(ID_i \oplus x)$
				$N_{a1} = C_{a2} \oplus C_1$
				$C_{a3} = C_1 \oplus N_{a2}$
				$V_{a1} = h(C_{a2}, N_{a1})$
			$\overset{M_{a2}=(V_{a1}, C_{a3})}{\dashleftarrow - - - - -}$	
	$M_{f2} = (V_1, C_{a3}) \longleftarrow$			
$V_1? = h(C_2, N_1)$				
$N_{a2} = C_{a3} \oplus C_1$				
			$\overset{M_{a3}=(V_{a2})}{- - - - - \dashrightarrow}$	
$V_{a2} = h(C_{a3}, N_{a2})$	$M_3 = (V_{a2}) \longrightarrow$			$V_{a2}? = h(C_{a3}, N_{a2})$

$\longrightarrow$: U_i's session $\dashrightarrow$: Attacker's session

Figure 2: Impersonation attack on Lee-Kim-Yoo's scheme

blocks the messages M_2 and M_{a2}, he sends the fabricated message $M_{f2} = (V_1, C_{a3})$ to U_i just like the step 2 of the verification phase.

3) Upon obtaining the message M_{f2}, U_i computes and sends the message $M_3 = (V_{a2} = h(C_{a3}, N_{a2}))$. The attacker can send the message $M_{a3} = (V_{a2})$ to finish his session and pass the system's authentication.

Note that U_i should compute the parameter $V_{a2} = h(C_{a3}, N_{a2})$, because he successfully verifies $V_1? = h(C_2, N_1)$ in the step 3 of the verification phase. As a result, although U_i authenticates the system after U_i's session, the system mistakenly believes that the attacker is U_i after the attacker's session. Since the attacker without knowing any secret information can impersonate U_i to cheat the system, Lee-Kim-Yoo's scheme fails to provide the mutual authentication service. Figure 2 illustrates our impersonation attack on Lee-Kim-Yoo's scheme.

4 Further Discussions and Conclusions

Herein, we have pointed out an impersonation attack on Lee-Kim-Yoo's nonce-based mutual authentication scheme. The attacker skillfully makes use of the legal remote user's session to help own session find the authentication message for the system. Using this attack paradigm, our purpose is to demonstrate that it is dangerous that two parties, i.e. the remote user and the system, separately implement their authentication operations without any logical relation in a session, to obtain the mutual authentication.

To design the secure mutual authentication mechanism, we suggest that one of the main tools is a notion of matching conversations. Diffie, Oorschot, and Wiener [3] first introduced the notion of matching runs. This idea is to a level of precision adequate to help them separate out what are and what are not meaningful attacks on the authentication scheme. But they did not provide any formal definition or proof. Bellare and Rogaway [1] formally defined matching conversations. In fact, under Bellare-Rogaway's definition, Lee-Kim-Yoo's scheme and Chien-Jan-Tseng's scheme [2] are all insecure. As a matter of fact, matching conversations may be useful as a sanity check. If the mutual authentication scheme fails the sanity check, it should be insecure.

Security authentication scheme designers often face the difficult task of reconciling security, functionality, and efficiency requirements and sometimes must make design decisions that appear well motivated but have unintended consequences. A lesson learned with respect to above Lee-Kim-Yoo's scheme illustrates this point. What we hope our cryptanalysis paradigm will aid is the development of secure and efficient schemes that are more suitable for real-life cryptographic applications than previous versions.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant Nos. 60225007 and 60572155, and the Science and Technology Research Project of Shanghai under Grant Nos. 04JC14055 and 04DZ07067.

References

[1] M. Bellare and P. Rogaway,"Entity authentication and key distribution," in *Advances in Cryptology (Crypto'93)*, LNCS 773, pp. 232-249, Springer-Verlag, 1994.

[2] H. Y. Chien, J. K. Jan, and Y. M. Tseng,"An efficient and practical solution to remote authentication: Smart card," *Computer and Security*, vol. 21, no. 4, pp. 372-375, 2002.

[3] W. Diffie, P. van Oorschot, and M. J. Wiener,"Authentication and authenticated key exchanges," *Designs, Codes and Cryptography*, vol. 2, no. 2, pp. 107-125, 1992.

[4] C. L. Hsu,"Security of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 26, no. 3, pp. 167-169, 2004.

[5] M. S. Hwang, C. C. Lee, and Y. L. Tang,"A simple remote user authentication scheme," *Mathematical and Computer Modelling*, vol. 36, no. 1-2, pp. 103-107, 2002.

[6] M. S. Hwang and L. H. Li,"A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28-30, 2000.

[7] W. C. Ku and S. M. 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.

[8] S. W. Lee, H. S. Kim, and K. Y. Yoo,"Efficient nonce-based remote user authentication scheme using smart cards," *Applied Mathematics and Computation*, vol. 167, no. 1, pp. 355-361, 2005.

[9] R. X. Lu and Z. F. Cao,"Efficient remote user authentication scheme using smart card," *Computer Networks*, vol. 49, no. 4, pp. 535-540, 2005.

[10] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997.

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

[12] W. H. Yang and S. P. Shieh,"Password authentication schemes with smart cards," *Computer and Security*, vol. 18, no. 8, pp. 727-733, 1999.

Da-Zhi Sun received the B.E. in Electronic Engineering from Nanchang Institution of Aeronautical Technology, Jiangxi, in 1999, the M.E. in Control Science and Engineering from Nanchang University, Jiangxi, in 2002, and the Ph.D. in Computer Science and Technology from Shanghai Jiao Tong University, in 2006. He now is a lecturer in Tianjin University. His current research interests include applied number theory, applied cryptography, and information security.

Zhen-Fu Cao received his Ph.D. in Applied Mathematics from Harbin Institution of Technology, Heilongjiang, in 1999. He is now a professor at Shanghai Jiao Tong University. His research interests include cryptography, information security, and e-topics.