A Forgery Attack on A Low Computation Cost User Authentication Scheme

Eun-Jun Yoon and Kee-Young Yoo
(Corresponding author: Eun-Jun Yoon)

Department of Computer Engineering, Kyungpook National University
Daegu 702-701, Republic of Korea (Email: ejyoon@infosec.knu.ac.kr)

(Received Aug. 9, 2005; revised and accepted Oct. 1, 2005)

Abstract

In 2005, Lee-Lin-Chang proposed a low computation cost user authentication scheme for mobile communication. However, the current paper demonstrates the vulnerability of Lee-Lin-Chang's scheme to a forgery attack, where an attacker can easily masquerade other legal users to access the resources at a remote system and then presents an simple solution to isolate such a problem.

Keywords: cryptanalysis, forgery attack, user authentication, smart card

1 Introduction

Remote user authentication is an important part of security, along with confidentiality and integrity, for systems that allow remote access over untrustworthy networks like the Internet. In 2003, Wu-Chieu [2] proposed a user-friendly remote authentication scheme with smart card through which the user can choose and change their password based on a secure channel. However, Yang-Wang [3] pointed out the scheme suffers from a forgery attack. Thereafter, in 2005, Lee-Lin-Chang [1] proposed an improvement on Wu-Chieu's scheme that can not only withstand a forgery attack, but also spend low computational cost suitable for mobile communication. They claimed that their scheme provided effective authentication and also eliminated the drawback of Wu-Chieu's scheme. However, Lee-Lin-Chang's scheme is still vulnerable to a forgery attack. Accordingly, the current paper demonstrates that Lee-Lin-Chang's scheme is susceptible to a forgery attack, where an attacker can easily masquerade other legal users to access the resources at a remote system and then presents an simple solution to isolate such a problem.

2 Review of Lee-Lin-Chang's Scheme

This section briefly reviews Lee-Lin-Chang's user authentication scheme, which has a registration, login, and authentication phase, as explained in the following:

2.1 Registration Phase

The user U_i submits their identifier ID_i and chosen password PW_i to the remote system. These private data must be sent in person or over a secure channel. Upon receiving the registration request, the remote system performs the following steps:

1) Compute $A_i = h(ID_i, x)$, where x is a secret key maintained by the system and $h(\cdot)$ is a collision resistant one-way hash function with an output sized 512 bits, e.g. SHA-512.

2) Compute $B_i = h(A_i||h(PW_i))$.

3) The remote system then personalizes the smart card with the secure information: $\{ID_i, A_i, B_i, h(\cdot)\}$.

2.2 Login Phase

If the user U_i wants to login, they attach their smart card to the card reader and key in their identifier ID_i and password PW_i^*, then the smart card performs the following operations:

1) Compute the following three integers:

   $B_i^* = h(A_i||h(PW_i^*))$, $C_1 = h(T \oplus B_i)$ and $C_2 = B_i^* \oplus A_i$, where T is the current date and time of the input device.

2) Send a message $m = \{ID_i, C_1, C_2, T\}$ to the remote system.

2.3 Authentication Phase

Upon receiving message m at time T', the remote system authenticates the user based on the following steps:

1) Verify the format of ID_i. If the format is incorrect, the system rejects the login request.

2) Verify the validity of the time interval between T and T'. If $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for a transmission delay, the remote system rejects the login request.

3) Compute $A_i = h(ID_i||x)$ and obtain B_i^* by computing $B_i^* = C_2 \oplus A_i$.

4) Compute $C_1^* = h(T \oplus B_i^*)$, and compare C_1 and C_1^*. If they are equal, this indicates that the password PW_i^* is equal to PW_i, then the system will accept the login request; otherwise the login request is rejected.

3 A Forgery Attack on Lee-Lin-Chang's Scheme

This section demonstrates that Lee-Lin-Chang's scheme is vulnerable to a forgery attack, where an attacker can easily masquerade as a legal user in order to access the resources of a remote system. In the login phase, the attacker can perform a forgery attack as follows:

1) Compute C_{2a} as follows:

$$\begin{aligned} C_{2a} &= T \oplus C_2 \oplus T_a \\ &= T \oplus B_i^* \oplus A_i \oplus T_a, \end{aligned}$$

where T_a is the attacker's current date and time for succeeding with Step 2 of the authentication phase.

2) Send a forged message $m_a = (ID_i, C_1, C_{2a}, T_a)$ to the remote system.

When the remote system receives the message m_a, the remote system will go into the authentication phase and perform the following checks:

1) The remote system will check the format of the ID_i. Of course, it is correct.

2) Then, the remote system will check whether the time is valid, because $(T' - T_a) \geq \Delta T$, where T' is the received timestamp of message m_a, the remote system will accept this check.

3) Then, the remote system will compute $A_i = h(ID_i||x)$ and obtain B_a^* by computing the following:

$$\begin{aligned} B_a^* &= C_{2a} \oplus A_i \\ &= T \oplus B_i^* \oplus A_i \oplus T_a \oplus A_i \\ &= T \oplus B_i^* \oplus T_a. \end{aligned}$$

4) Finally, the remote system will compute C_1^* as follows:

$$\begin{aligned} C_1^* &= h(T_a \oplus B_a^*) \\ &= h(T_a \oplus T \oplus B_i^* \oplus T_a) \\ &= h(T \oplus B_i^*), \end{aligned}$$

and compare C_1^* and receive C_1. It is easy to check whether the remote system will accept this forged message m_a, as $C_1 = C_1^* = h(T \oplus B_i^*)$. Finally, the remote system accepts the attacker's login request, making Lee-Lin-Chang's scheme insecure.

4 Simple Improvement

This section proposes an simple solution to overcome the above mentioned problem inherent in Lee-Lin-Chang' scheme. We only modify the login phase. That is, in Step 1 of the login phase, user U_i computes $C_1 = h(T||B_i)$ instead of $C_1 = h(T \oplus B_i)$, where $||$ is concatenation operation, and sends a message $m = \{ID_i, C_1, C_2, T\}$ to the remote system. In the improved scheme, the attacker cannot masquerade as a legal user U_i by using above mentioned forgery attack in order to access the resources of a remote system. Because C_1 is not equal to $C_1^* = h(T||B_a^*)$, where $B_a^* = T \oplus B_i^* \oplus T_a$, the remote system can easily detect the attacker's forged login request.

5 Conclusion

The current paper demonstrated that an attacker can easily masquerade other legal users to access the resources at a server in Lee-Lin-Chang's user authentication scheme and then presented an simple solution to isolate such a problem.

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

References

[1] C. Y. Lee, C. H. Lin, and C. C. Chang, "An improved low computation cost user authentication scheme for mobile communication," in *Proceedings of the 19th Advanced Information Networking and Applications (IEEE AINA'05)*, vol. 2, pp. 249–252, Taipei, Taiwan, Mar. 2005.

[2] S. T. Wu and B. C. Chieu, "A user friendly remote authentication scheme with smart cards," *Computers & Security*, vol. 22, no. 6, pp. 547–550, Sept. 2003.

[3] C. C. Yang and R. C. Wang, "Cryptanalysis of a user friendly remote authentication scheme with smart cards," *Computers & Security*, vol. 23, no. 5, pp. 425–427, July 2004.

Eun-Jun Yoon received his BS in the School of Textile and Fashion Technology from the Kyung Il University, South Korea in 1995, and his MS in the Computer Engineering from the same University in 2003. He is now working toward the Ph.D. degree in the Kyungpook National University, South Korea. His current research interests are cryptography and network security. E-mail address: ejyoon@infosec.knu.ac.kr

Kee-Young Yoo received his BS degree in education of mathematics from Kyungpook National University in 1976; the MS degree in Computer Engineering from Korea Advanced Institute of Science and Technology in 1978 and the PhD degree in the Computer Science from Rensselaer Polytechnic Institute, New York, U.S.A., in 1992. He is now a Professor at the Department of Computer Engineering, Kyungpook National University. His current research interests are wireless security and cryptography. E-mail address: yook@knu.ac.kr