Cryptanalysis of Threshold Password Authentication Against Guessing Attacks in Ad Hoc Networks

Chun-Ta Li[1,2] and Yen-Ping Chu[3]
(Corresponding author: Chun-Ta Li)

Department of Information Management, Tainan University of Technology[1]
529 Jhong Jheng Road, Yongkang, Tainan, Taiwan 710, R.O.C.
Department of Computer Science and Engineering, National Chung Hsing University[2]
250 Kuo Kuang Road, Taichung, 402 Taiwan, R.O.C. (Email: phd9307@cs.nchu.edu.tw)
Department of Computer Science and Information Engineering, Tunghai University[3]
181 Taichung Harbor Road, Taichung, 407 Taiwan, R.O.C.

(Received Aug. 8, 2007; revised and accepted Oct. 23, 2007)

Abstract

Recently, Chai et al. proposed a threshold password authentication scheme that t out of n server nodes could efficiently carry out mutual authentication with a user while preserving strong security requirements in the mobile ad hoc networks. In this article, we will show that their scheme suffers from a number of security vulnerabilities by passive attacks.

Keywords: Ad hoc network, authentication, cryptanalysis, passive attack, security

1 Introduction

Due to rapid advancement of wireless and mobile communication technologies, mobile ad hoc networks have received a great deal of attention over the past years. In an ad hoc network, it provides the advantages of easily connect nodes as long as they are within the radio transmission range and increasing flexibility for communications. However, if a user node wants to request some services from other server nodes, there might cause some security issues that should be taken into consideration. For example, how to prevent an unauthorized user to access the resources? How to enhance the availability of the system in the mobile ad hoc network if some server nodes are compromised?

Recently, Chai et al. [1] proposed a (t, n) threshold password authentication scheme [2, 3] to address above issues. Moreover, their scheme provides the following advantages: (1) mutual authentication between user and server node; (2) user can freely change the password without registration again; (3) no password tables stored in server nodes; (4) attacker cannot derive the password even if user's mobile device is lost; (5) attacker cannot impersonate the legal user to login the server. However, in this article, we show that Chai et al.'s scheme suffers from a number of security problems by passive attacks.

The organization of this article is as follows. In Section 2, we will briefly review the Chai-Cao-Lu scheme. In Section 3, we will show our attacks on Chai-Cao-Lu scheme. Finally, Section 4 is our conclusions.

2 Review of Chai-Cao-Lu Scheme

This section briefly reviews the main ideas of Chai-Cao-Lu scheme. The notations used throughout this article are the same as Chai et al. used in the original scheme and shown in Table 1.

Before the threshold authentication, a set up process would be performed by a trusted authority TA. Firstly, TA selects a random polynomial $f(\cdot)$ over Z_q of degree $t-1$ that satisfying $f(0) = x$ and computes $f(i) = x_i$, where x is the primary shared secret and $i = 1, \cdots, n$. Then, TA sends x_i to the corresponding S_i over a secret channel and discards x. After being set up, there are three phases in Chai-Cao-Lu scheme, registration phase, login phase and authentication phase, respectively. The detailed phases are briefly described as follows.

- Registration phase – U_i first sends his ID_i and $h(PW_i)$ to ℓ over a secret channel. Then, the server computes $B_i = h(ID_i)^{x_i} \bmod p$ and sends B_i to the dealer (one of the servers and assume that it is an honest server). After collecting all the B_i, the dealer

Table 1: Notations used in this article

U_i	User
ID_i	U_i's identity
PW_i	U_i's password
ℓ	A collection of n servers
S_i	A server in ℓ, $i = 1, \cdots, n$
x	Primary secret key shared by all servers in ℓ
x_i	Secret key hold by S_i
p, q	Two secure large primes, where $p = 2q + 1$
T	Timestamp
$h(\cdot)$	A public and secure one-way hash function
ϕ	$\phi \subset \{1, \cdots, n\}$, $\|\phi\|$=t
L_i^z	L_i^z=$\prod_{j \in \phi, j \neq i} \frac{z-j}{i-j}$ is the Lagrange coefficients
$\|\|$	Concatenation symbol

can compute:

$$\begin{aligned} \beta &= (\prod_{i \in \phi} B_i^{L_i^0}) + h(PW_i), \\ &= h(ID_i)^{\sum_{i \in \phi} L_i^0 x_i} + h(PW_i), \\ &= h(ID_i)^x + h(PW_i) \bmod p, \end{aligned}$$

where $x = f(0) = \sum_{i \in \phi}(x_i L_i^0)$. Subsequently, the dealer issues the ticket (contains ID_i, β, p, q, $h(\cdot)$) to U_i through a secure channel and U_i can store the ticket in his login device.

- Login phase – In this phase, U_i inputs his ID_i and PW_i and the login device will compute these values, B, E, D and C, as follows:

$$\begin{aligned} B &= \beta - h(PW_i) \bmod p, \\ E &= B^r = h(ID_i)^{xr} \bmod p, \\ D &= h(ID_i)^r \bmod p, \\ C &= h(T||E||B) \bmod p, \end{aligned}$$

where r is a random number $\in Z_q^*$ and T is the current timestamp of the login device. Next, U_i sends the login message $M = (ID_i, T, D, C)$ to ℓ.

- Authentication phase – After receiving the message M, $S_i (i \in \phi)$ checks ID_i and T, if the format of ID_i is incorrect or time interval between T and receiving time is invalid, the login request will be rejected. Otherwise, S_i computes $E_i' = D^{x_i} \bmod p$ and $B_i' = h(ID_i)^{x_i} \bmod p$ and sends (E_i', B_i') to the dealer. After collecting all (E_i', B_i'), the dealer can compute $E' = \prod_{i \in \phi} E_i'^{L_i^0} \bmod p = h(ID_i)^{xr} \bmod p$ and $B' = \prod_{i \in \phi} B_i'^{L_i^0} \bmod p = h(ID_i)^x \bmod p$ and checks the validity of $C \stackrel{?}{=} h(T||E'||B')$. If it does not hold, the login request is terminated. Otherwise, the login request is accepted and the dealer will send (ID_i, C', T') to U for achieving mutual authentication, where $C' = h(B'||E'||T')$ and T' is the current timestamp of the dealer. Finally, U_i can check the validity of ID_i and T' and further check the validity of $C' \stackrel{?}{=} h(B||E||T')$. If it holds, mutual authentication between U_i and ℓ is achieved. Otherwise, a new login request will be restart by the login device.

3 Cryptanalysis of Chai-Cao-Lu Scheme

In this section, we will show the cryptanalysis of Chai-Cao-Lu scheme. Their scheme could not withstand the passive attack that an attacker could monitor on the communication channel between dealer and $S_i (i \in \phi)$ and discovers some valuable information about the messages transmitted over the communication channel. Then, the attacker can derive user's secret token and easily impersonate a legal user to login the server. We describe the cryptanalysis as follows.

In authentication phase, after $S_i (i \in \phi)$ checks the validity of ID_i and T, S_i will compute B_i' and E_i' and sends them to the dealer. Meanwhile, an attacker can un-intrusively monitor on the communication channel between dealer and S_i to collect S_i's secret token B_i' without disturbing the communication. After that, as long as there are at least t out of n secret token B_i' are obtained to the attacker, the attacker could easily derive the user's secret token $h(ID_i)^x$ by computing $\prod_{i \in \phi} B_i'^{L_i^0}$. Unfortunately, since the attacker knows $h(ID_i)^x$, he can impersonate a legal user to login the server. Besides, if a victim user's mobile device is lost, the attacker can easily derive the password $h(PW_i)$ by computing $\beta - h(ID_i)^x$ and even the victim user's password can be changed freely by the attacker.

Also, in their scheme, assume there are only $t-1$ server nodes send their B_i' to the dealer and the dealer would compute the last B_i' to perform the authentication with a registered user. Thus, the attacker cannot derive the secret value $h(ID_i)^x$ from collecting these $t-1$ secrets in first authentication process. But it is still insecure to resist passive attack because the value of S_i's B_i' is changeless in every authentication process. So, when the user login to the system again, the attacker would continually collect the secret token B_i' until to t secrets are collected and the secret value $h(ID_i)^x$ would be derived. Due to this kind of attacks, the simple solution is that all messages transmitted between dealer and S_i should be encrypted for achieving integrity in ad hoc networks, that is, there must establish a secure tunnel between dealer and S_i so that the former can securely get all the piece of secret information sent by the latter participants.

4 Conclusions

In this article, we have shown the Chai-Cao-Lu scheme is vulnerable to the passive attack that the attacker could collect secrets by monitoring the communication channels

between nodes in an ad hoc network and further derives the legal user's secret token to damage the security of system.

Acknowledgements

This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grants NSC 96-2219-E-001-001, and NSC 96-2219-E-009-013.

References

[1] Z. Chai, Zhenfu Cao, and R. Lu, "Threshold password authentication against guessing attacks in ad hoc networks," *Ad Hoc Networks*, vol. 5, no. 7, pp. 1046-1054, Sep. 2007.

[2] M. S. Hwang, and T. Y. Chang, "Threshold signatures: Current status and key issues," *International Journal of Network Security*, vol. 1, no. 3, pp. 123-137, Nov. 2005.

[3] 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, June 2006.

Chun-Ta Li received the M.S. degree in Information Management from Chaoyang University of Technology, Taichung county, Taiwan, in 2004, and the Ph.D. degree in Computer Science and Engineering from National Chung Hsing University, Taichung, Taiwan, in 2008. Currently, he has been assistant professor of the Department of Information Management, Tainan University of Technology, Tainan county, Taiwan. His research interests include information security, wireless sensor networks, and security protocols for ad hoc networks.

Yen-Ping Chu is a Professor in the Computer Science and Information Engineering and the library director at Tunghai University, Taichung, Taiwan. His research interests include high-speed networks, operating systems, neural networks, and computer-assisted learning.