Further Improvement of An Authentication Scheme with User Anonymity for Wireless Communications

Jianbin Hu, Hu Xiong, and Zhong Chen
(Corresponding author: Hu Xiong)

Key Laboratory of Network and Software Security Assurance of the Ministry of Education, Institute of Software,
School of Electronics Engineering and Computer Science, Peking University, Beijing, P.R.China
No.5 Yiheyuan Road Haidian District, Beijing, 100085, China (Email: xionghu@pku.edu.cn)

(Received Nov. 29, 2005; revised and accepted Dec. 31, 2005)

Abstract

Seamless roaming is highly desirable for wireless communications, and security such as authentication and privacy preserving of mobile users is challenging. Recently, Wu *et al.* and Wei *et al.* proposed two authentication schemes that guarantee user anonymity in wireless communications, respectively. However, Kang *et al.* pointed out some security flaws of Wu *et al.*'s and Wei *et al.*'s authentication schemes and showed how to overcome the problems regarding anonymity and the forged login messages. In this paper, we will show that Kang *et al.*'s improved scheme still did not provide user anonymity as they claimed and give a further improvement to fix the problem without losing any features of the original scheme.

Keywords: wireless communication, user authentication, anonymity, cryptanalysis

1 Introduction

With the rapid development of mobile technologies, wireless communications have received a lot of concern from industry and academia. To transfer data anywhere and anytime, small mobile devices, such as mobile phones and personal digital assistance (PDA), has been widely used. In order to guarantee the security of mobile user's data transmission properly, user authentication is required to prevent the illegal use of resources. Furthermore, the privacy of the mobile users should be protected. To provide privacy-preserving authentication service for wireless communications, Zhu and Ma [10] proposed a wireless security protocol based on the smart card which is featured with user identity anonymity. After that, Lee *et al.* [4] pointed out several security flaws in Zhu-Ma's scheme and proposed a slightly modified version to remedy the identified deficiencies. Unfortunately, Wu *et al.* [8] and Chang *et al.* [1] showed that Lee *et al.*'s scheme also failed to preserve anonymity as claimed and then proposed improved scheme to address the problem respectively. However, Lee et al. [5] and Zeng *et al.* showed that [4, 8] are also incapable of providing user anonymity respectively. Furthermore, Lee *et al.* [6] pointed that [1] is also incapable of providing user anonymity. Recently, Kang *et al.* [3] pointed the security problems in [8, 7] and proposed an improved authentication scheme that guarantees the user anonymity in wireless environments. However, Kang *et al.*'s improvement cannot provide user anonymity in the authentication phase either: an attacker who has registered as a valid user of home agent (HA), can obtain the identity of other users assuming they registered at the same HA. As a suggestion to fix the problem, we present a slightly different authentication algorithm. Our fix does not cause any loss in efficiency or other features (such as high scalability) of the original scheme.

2 Registration and Authentication phases in the Kang *et al.*'s scheme

Kang *et al.*'s authentication scheme [3] consists of three phases: registration phase, authentication phase, and password change phase. We only review the registration and authentication phases in the following, for the password change part, readers may refer to [3] (the notations involved are listed in Table 1).

2.1 Registration Phase

After receiving identity ID_{MU} of a mobile user (MU), his/her home agent (HA) generates the following PW_{MU}, r_1 and r_2, and stores ID_{HA}, r_1, r_2 and a one-way hash function h in the smart card of MU.

Table 1: Notations

notation	description
HA	Home Agent of a mobile user
FA	Foreign Agent of the network
MN	Mobile User
PW_{MU}	A password of MU
ID_A	Identity of an entity A
T_A	Timestamp generated by an entity A
Cert_A	Certificate of an entity A
$(X)_K$	Encryption of a message X using a symmetric key K
(P_A, S_A)	public\secret key pair of entity A
$E_{P_A}(X)$	Encryption of a message X using a public key P_A
$S_{S_A}(X)$	Signature on a message X using a secret key S_A
$h(X)$	A one-way hash function
$\|$	Concatenation
$\oplus$	Bitwise exclusive-or operation

$PW_{MU} = h(N \parallel ID_{MU})$
$r_1 = h(N \parallel ID_{HA})$
$r_2 = h(N \parallel ID_{MU}) \oplus ID_{HA} \oplus ID_{MU}$
where N is a secret value kept by HA. HA then sends PW_{MU} and a smart card containing ID_{HA}, r_1, r_2 and h to MU through a secure channel.

2.2 Authentication Phase

A foreign agent (FA) authenticates MU by interacting with HA as follows.

Step 1. $MU \rightarrow FA : [n, (h(ID_{MU}) \parallel x_0 \parallel x)_L, ID_{HA}, T_{MU}]$.

1) If MU inputs PW_{MU} to MU's mobile device, then MU's mobile device chooses secret random values x_0 and x and computes n and L as follows.

   $n = h(T_{MU} \parallel r_1) \oplus r_2 \oplus PW_{MU}$.

   $L = h(T_{MU} \oplus PW_{MU})$.

2) MU's mobile device sends MU's login message $[n, (h(ID_{MU}) \parallel x_0 \parallel x)_L, ID_{HA}, T_{MU}]$ to FA, where T_{MU} is a current timestamp.

Step 2. $FA \rightarrow HA : [b, n, (h(ID_{MU}) \parallel x_0 \parallel x)_L, T_{MU}, S_{S_{FA}}((h(ID_{MU}) \parallel x_0 \parallel x)_L, T_{MU}, Cert_{FA}), Cert_{FA}, T_{FA}]$.

3) FA checks the validity of T_{MU}. If it is valid, then FA chooses secret random number b. FA then sends b, the MU's login message containing $[n, (h(ID_{MU}) \parallel x_0 \parallel x)_L$ and $T_{MU}]$, a certificate $Cert_{FA}$, timestamp T_{FA}, and the corresponding signature on the login message by using FA's private key S_{FA}.

Step 3. $HA \rightarrow FA : [c, W, b, S_{S_{HA}}(h(b, c, W, Cert_{HA})), Cert_{HA}, T_{HA}]$.

4) HA checks the validity of certificate $Cert_{FA}$ and timestamp T_{FA}. If they are valid, then HA computes MU's real identity as follows.

   $ID_{MU} = n \oplus h(T_{MU} \parallel h(N \parallel ID_{HA})) \oplus ID_{HA}$

   HA can compute $L = h(T_{MU} \oplus h(N \parallel ID_{MU}))$ with his secret value N and decrypts $(h(ID_{MU}) \parallel x_0 \parallel x)_L$. Then, HA verifies if MU is a legal user by checking $h(ID_{MU}) = h(ID_{MU})'$ where $h(ID_{MU})$ is computed with ID_{MU} on the login message and $h(ID_{MU})'$ of the decrypting result $[h(ID_{MU})' \parallel x_0' \parallel x']$.

5) If so, then HA computes $W = E_{P_{FA}}(h(h(N \parallel ID_{MU})) \parallel x_0 \parallel x)$ and generates its signature using his/her private key S_{HA}. Then, HA sends random number c, W, the certificate of HA, $Cert_{HA}$, current timestamp T_{HA}, and signature $S_{S_{HA}}(h(b, c, W, Cert_{HA}))$.

Step 4. $FA \rightarrow MU : (TCert_{MU} \parallel h(x_0 \parallel x))_k$.

6) FA checks the validity of certificate $Cert_{HA}$ and timestamp T_{HA}. If they are valid, then FA issues the temporary certificate $TCert_{MU}$, which includes a timestamp and other information, to MU.

7) To obtain $(h(h(N \parallel ID_{MU})) \parallel x_0 \parallel x)$, FA decrypts W with the secret key corresponding to P_{FA}. To establish session key k_i for the i-th session, FA first saves $(TCert_{MU}, h(PW_{MU}), x_0)$. FA encrypts $(TCert_{MU} \parallel h(x_0 \parallel x))$ with session key k and gives $(TCert_{MU} \parallel h(x_0 \parallel x))_k$ to MU. Here, the session key is computed as follows.

   $k = h(h(h(N \parallel ID_{MU})) \parallel x \parallel x_0) = h(h(PW_{MU}) \parallel x \parallel x_0)$

MU computes k and obtains $TCert_{MU}$. MU also authenticates FA by computing $h(x_0 \parallel x)$ with the decrypted $h(x_0 \parallel x)$. Therefore, MU can be sure that it is communicating with a legal FA.

3 A Security Flaw in Authentication phase

Below we describe a serious security flaw in the authentication phase of the Kang *et al.*'s scheme. Assume that an attacker $\mathcal{A}$ who has registered as a valid user of HA, then he can obtain the identity of other users assuming they registered at the same HA.

Note that $\mathcal{A}$ can obtain ID_{HA}, r_1, r_2 and h from the HA (see Sec. 2.1), where

$PW_{\mathcal{A}} = h(N \parallel ID_{\mathcal{A}})$

$r_1 = h(N \parallel ID_{HA})$

$r_2 = h(N \parallel ID_{\mathcal{A}}) \oplus ID_{HA} \oplus ID_{\mathcal{A}} = PW_{\mathcal{A}} \oplus ID_{HA} \oplus ID_{\mathcal{A}}$

Next, $\mathcal{A}$ can collect the messages $[n, (h(ID_{MU}) \parallel x_0 \parallel x)_L, ID_{HA}, T_{MU}]$ sent from any other legal mobile user MU to FA at step 1 in the authentication phase (As a matter of fact, wireless is broadcast and anyone within range of a wireless device can intercept the packets being sent out without interrupting the data flow [10]). After that, $\mathcal{A}$ can confirm that MU is a user of HA based on ID_{HA}. With computed $h(T_{MU} \parallel r_1)$, $\mathcal{A}$ can determine the real identity of MU as HA does at step 3 in the authentication phase. That is,

$$\begin{aligned} & n \oplus ID_{HA} \oplus h(T_{MU} \parallel r_1) \\ = \ & h(T_{MU} \parallel r_1) \oplus r_2 \oplus PW_{MU} \oplus ID_{HA} \oplus h(T_{MU} \parallel r_1) \\ = \ & PW_{MU} \oplus ID_{HA} \oplus ID_{MU} \oplus PW_{MU} \oplus ID_{HA} \\ = \ & ID_{MU} \end{aligned}$$

The above attack shows that it is trivial for an attacker to obtain the identity of mobile users and defeat the anonymity claimed by Kang *et al.*'s scheme. The basic reason of this attack is that HA computes r_1 for each MU with the same secret number N.

4 A Suggestion on Registration and Authentication algorithms

To resolve the problem, we suggest to slightly modify the authentication algorithm as follows:

In the registration phase: instead of defining $r_2 = h(N \parallel ID_{MU}) \oplus ID_{HA} \oplus ID_{MU}$, we redefine $r_2 = h(N \parallel ID_{MU}) \oplus ID_{HA} \oplus (ID_{MU} \parallel m)_N$, where m is a secret random value chosen by HA.

In the step 1 of authentication phase, MU computes $n = h(T_{MU} \parallel r_1) \oplus r_2 \oplus PW_{MU} = h(T_{MU} \parallel r_1) \oplus ID_{HA} \oplus (ID_{MU} \parallel m)_N$.

In the step 3 of authentication phase, after checking the validity of certificate $Cert_{FA}$ and timestamp T_{FA}, HA computes MU's real identity as follows.

$(ID_{MU} \parallel m)_N = n \oplus h(T_{MU} \parallel h(N \parallel ID_{HA})) \oplus ID_{HA}$

Then, HA decrypts $(ID_{MU} \parallel m)_N$ by using the secret value N to obtain the MU's real identity ID_{MU}.

Note that the other steps of authentication algorithm are the same as those in the Kang *et al.*'s original scheme.

4.1 Security analysis

In the improved scheme, the anonymity of MU is obtained by the symmetric encryption technique. In the step 1 of authentication phase, the identity of MU is submitted to HA in a secure channel, thus the attacker cannot obtain the identity of MU. Only HA, who knows the secret key N, can get the real identity of MU. Assume that the attacker (including a valid foreign agent and any other users except MU) has extracted the secrets ID_{HA}, r_1, r_2 and h stored in MU's smart card and recorded the used messages transmitted between MU, FA and HA. However, the attacker cannot derive the real identity of MU without knowing the secret key N.

4.2 Efficiency

It is obvious to see that our modified authentication algorithm is slightly more expensive than the original algorithm given by Kang *et al.* due to the extra symmetric encryption operation. Also, since the other steps in authentication protocol is not changed, our modified scheme is at least as efficient as the original scheme.

5 Conclusions

We showed that an inherent design flaw in the scheme of Kang *et al.*, in which an attacker registered as a user of some HA can obtain the identity of other users registered with the same HA without authorization. Furthermore, the basic reason resulted in this flaw has also been analyzed. We also presented a fix to resolve the problem without sacrificing any desirable feature of the original scheme.

6 Acknowledgement

The authors thank the editors and the anonymous referees for their valuable comments and suggestions. This work is partially supported by National Natural Science Foundation of China under Grant No. 61003230, State Key Laboratory of Information Security under Grant No.01-02-4, China Postdoctoral Science Foundation under Grant No. 20100480130, Chongqing Key Lab of Computer Network and Communication Technology under Grant No. CY-CNCL-2010-01 and National Research Foundation for the Doctoral Program of Higher Education of China under Grant No. 200806140010.

References

[1] C.C. Chang, C.Y. Lee, Y.C. Chiu, Enhanced authentication scheme with anonymity for roaming service in global networks, Computer Communications, vol. 32, no. 4, pp. 611-618, 2009.

[2] C.-W. Chen, M.-C. Chuang, and C.-S. Tsai, An Efficient Authentication Scheme between MANET and

WLAN on IPv6 Based Internet, International Journal of Network Security, Vol. 1, No. 1, pp. 14-23, 2005.

[3] M. Kang, H. S. Rhee, J.-Y. Choi, Improved User Authentication Scheme with User Anonymity for Wireless Communications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 94-A(2): 860-864, 2011.

[4] 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.

[5] J.S. Lee, J.H. Chang, D.H. Lee, Security flaw of authentication scheme with anonymity for wireless communications, IEEE Communications Letters, vol. 13, no. 5, pp. 292-293, 2009.

[6] C.C. Lee, R.X. Chang, T. Williams, On the anonymity of an enhanced authentication scheme for a roaming service in global mobility networks, International Journal of Secure Digital Information Age, Vol II, No. 1, June 2010.

[7] Y. Wei, H. Qiu, Y. Hu, Security analysis of authentication scheme with anonymity for wireless environments, International Conference on Communication Technology (ICCT), Guilin, China, pp. 1-4, 2006.

[8] C.-C. Wu, W.-B. Lee, and W.-J. Tsaur, A secure authentication scheme with anonymity for wireless communications, IEEE Communications Letters, vol. 12, no. 10, pp. 722-723, 2008.

[9] J. Zhan, L. Chang, and S. Matwin, Privacy Preserving K-nearest Neighbor Classification, International Journal of Network Security, Vol. 1, No. 1, pp. 46-51, 2005.

[10] J. Zhu, and J. Ma, A new authentication scheme with anonymity for wireless environments. IEEE Transactions on Consumer Electronics. vol. 50, no. 1, pp. 230-234, 2004.

[11] P. Zeng, Z. Cao, K.K.R. Choo, S. Wang, On the anonymity of some authentication schemes for wireless communications, IEEE Communications Letters, vol. 13, no. 3, pp. 170-171, 2009.

Jianbin Hu is an associate professor in Peking University. He received her Ph.D degree from Peking University, China, 2004. His research interests include: cloud computing and information security.

Hu Xiong is an Assistant Professor at University of Electronic Science and Technology of China. He received his Ph.D degree in University of Electronic Science and Technology of China, 2009. His research interests include: cryptographic protocol, and network security.

Zhong Chen is a professor of Peking University, and director of the Network and Information Security Research Group of the Software Institute. He received his B.S. and Ph.D. degrees from Peking University in 1983 and 1988, respectively. He has wide interests in network and information security, system software and embedded system.