LETTER

Cryptanalysis of an Improved User Authentication Scheme with User Anonymity for Wireless Communications

Eun-Jun YOON[†a)] ***and*** **Kee-Young YOO**[††b)], ***Members***

SUMMARY A user identity anonymity is an important property for roaming services. In 2011, Kang et al. proposed an improved user authentication scheme that guarantees user anonymity in wireless communications. This letter shows that Kang et al.'s improved scheme still cannot provide user anonymity as they claimed.
key words: *cryptanalysis, authentication, anonymity, wireless communications, security*

1. Introduction

In wireless communication environments, wireless roaming is rapidly becoming an important network feature because of the widespread use of mobile devices such as cellular phones or smart phones. To provide effective global roaming service for a legitimate mobile user between the home network and a visited foreign network, strong mobile user authentication measures are required. Moreover, anonymity of the mobile users should be also guaranteed to protect the privacy of mobile users.

In 2004, Zhu and Ma [1] proposed an authentication scheme with anonymity for wireless communication environments. Later, Lee et al. [2] showed several security flaws of Zhu-Ma's scheme and then improved it. However, in 2008, Wu et al. [3] showed that both Zhu-Ma's scheme and Lee et al.'s scheme still cannot provide anonymity and then proposed an improvement to preserve anonymity. Nevertheless, Zeng et al. [4] and Lee et al. [5] showed that Wu et al.'s scheme also cannot provide anonymity, respectively.

In 2011, Kang et al. [7] proposed an improved user authentication scheme based on both Wu et al.'s and Wei et al.'s schemes [3], [6] that guarantees strong user anonymity in wireless communications. However, this letter shows that the Kang et al.'s improved scheme also cannot provide user anonymity as they claimed.

2. Review of Kang et al.'s Scheme

Throughout the paper, notations are employed in Table 1. There are three phases in the Kang et al.'s scheme - initial phase, first phase, and second phase. In the initial phase, a mobile user MU sends his/her identity to his/her home agent HA and HA delivers a password and a smart card to MU through a secure channel. In the first phase, foreign agent FA authenticates MU and establishes a session. In the second phase, whenever MU visits FA, FA serves for MU. The detailed phases are shown in the following.

Table 1 Notations.

HA	Home Agent of a mobile user
FA	Foreign Agent of the network
MU	Mobile User
PW_{MU}	A password of MU
N	A strong secret key of HA
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 message X using symmetric key K
$E_{P_A}(X)$	Encryption of message X using public key of A
$S_{S_A}(X)$	Signature on message X using private key of A
$h(\cdot)$	A one-way hash function
$\|$	Concatenation
$\oplus$	Bitwise exclusive-or operation

2.1 Initial Phase

When an MU registers with his/her HA, the MU's identity ID_{MU} is submitted to the HA. After receiving ID_{MU} from MU, HA generates PW_{MU}, r_1 and r_2 as follows.

$$PW_{MU} = h(N\|ID_{MU}) \quad (1)$$

$$r_1 = h(N\|ID_{HA}) \quad (2)$$

$$r_2 = h(N\|ID_{MU}) \oplus ID_{HA} \oplus ID_{MU} \quad (3)$$

where N is a secret value kept by HA. HA stores ID_{HA}, r_1, r_2 and $h(\cdot)$ in the smart card of MU and then sends it with PW_{MU} to MU through a secure channel.

2.2 First Phase

Figure 1 illustrates the first phase of Kang et al.'s scheme. A foreign agent FA authenticates MU by interacting with HA as follows.

1. $MU \rightarrow FA$: $\{n, (h(ID_{MU})\|x_0\|x)_L, ID_{HA}, T_{MU}\}$
   If MU inputs ID_{MU} and 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.

$$n = h(T_{MU}\|r_1) \oplus r_2 \oplus PW_{MU} \quad (4)$$

$$L = h(T_{MU} \oplus PW_{MU}) \quad (5)$$

Manuscript received July 21, 2011.
[†]The author is with the Department of Cyber Security, Kyungil University, 33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712–701, South Korea.
[††]The author is with the School of Electrical Engineering and Computer Science, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702–701, South Korea.
a) E-mail: ejyoon@kiu.ac.kr
b) E-mail: yook@knu.ac.kr (Corresponding Author)
DOI: 10.1587/transinf.E95.D.1687

MU $(ID_{MU}, PW_{MU}$, SMART CARD$(ID_{HA}, r_1, r_2, h(\cdot)))$	FA $(Cert_{FA}, S_{FA}, P_{HA})$	HA $(ID_{HA}, N, Cert_{HA}, S_{HA}, P_{FA})$
Input ID_{MU} and PW_{MU} Generate two random x_0 and x Generate timestamp T_{MU} $n = h(T_{MU}\|r_1) \oplus r_2 \oplus PW_{MU}$ $L = h(T_{MU} \oplus PW_{MU})$		
$\{n, (h(ID_{MU})\|x_0\|x)_L, ID_{HA}, T_{MU}\}$ $\longrightarrow$		
	Check T_{MU} Generate random b Compute signature $S_{S_{FA}}(h(ID_{MU})\|x_0\|x)_L, T_{MU}, Cert_{FA}))$ Generate timestamp T_{FA}	
	$\{b, n, (h(ID_{MU})\|x_0\|x)_L, T_{MU}, S_{S_{FA}}((h(ID_{MU})\|x_0\|x)_L, T_{MU}, Cert_{FA})), Cert_{FA}, T_{FA}\}$ $\longrightarrow$	
		Check $Cert_{FA}$ and T_{FA} $ID_{MU} = h(T_{MU}\|h(N\|ID_{HA})) \oplus n \oplus ID_{HA}$ $L = h(T_{MU} \oplus h(N\|ID_{MU}))$ Decrypt $(h(ID_{MU})\|x_0\|x)_L$ Check $h(ID_{MU})$ $W = E_{P_{FA}}(h(h(N\|ID_{MU}))\|x_0\|x)$ Compute signature $S_{S_{HA}}(h(b, c, W, Cert_{HA}))$ Generate timestamp T_{HA}
	$\longleftarrow$ $\{c, W, b, S_{S_{HA}}(h(b, c, W, Cert_{HA})), Cert_{HA}, T_{HA}\}$	
	Check $Cert_{HA}$ and T_{HA} Generate temporary certificate $TCert_{MU}$ Decrypt W $k = h(h(h(N\|ID_{MU}))\|x\|x_0)$	
$\longleftarrow$ $(TCert_{MU}\|h(x_0\|x))_k$		
$k = h(h(PW_{MU})\|x\|x_0)$ Decrypt $(TCert_{MU}\|h(x_0\|x))_k$ Check $h(x_0\|x)$		

Fig. 1 First phase of Kang et al.'s scheme.

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

2. $FA \rightarrow HA$: $\{b, n, (h(ID_{MU})\|x_0\|x)_L, T_{MU}, S_{S_{FA}}((h(ID_{MU})\|x_0\|x)_L, T_{MU}, Cert_{FA})), Cert_{FA}, T_{FA}\}$
   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 $\{n, (h(ID_{MU})\|x_0\|x)_L, ID_{HA}, T_{MU}\}$, a certificate $Cert_{FA}$, timestamp T_{FA}, and the corresponding signature on the login message by using FA's private key S_{FA} to HA.
3. $HA \rightarrow FA$: $\{c, W, b, S_{S_{HA}}(h(b, c, W, Cert_{HA})), Cert_{HA}, T_{HA}\}$
   HA checks the validity of certificate $Cert_{FA}$ and timestamp T_{FA}. If they are valid, then HA computes MU's real identity ID_{MU} as follows.
   $$ID_{MU} = h(T_{MU}\|h(N\|ID_{HA})) \oplus n \oplus ID_{HA} \tag{6}$$
   HA computes $L = h(T_{MU} \oplus h(N\|ID_{MU}))$ with his/her secret N and decrypts $(h(ID_{MU})\|x_0\|x)_L$. 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 $\{h(ID_{MU})'\|x_0'\|x'\}$. If so, then HA computes $W = E_{P_{FA}}(h(h(N\|ID_{MU}))\|x_0\|x)$ 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 $S_{S_{HA}}(h(b, c, W, Cert_{HA}))$ to FA.
4. $FA \rightarrow MU$: $(TCert_{MU}\|h(x_0\|x))_k$
   FA checks whether or not the certificate $Cert_{HA}$ and timestamp T_{HA} are valid. If they are valid, then FA issues the temporary certificate $TCert_{MU}$, which includes a timestamp and other information to MU. To obtain $(h(h(N\|ID_{MU}))\|x_0\|x)$, 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 $(TCert_{MU}\|h(x_0\|x))$ with session key k and gives $(TCert_{MU}\|h(x_0\|x))_k$ to MU. Here, the session key is computed as follows.
   $$\begin{aligned} k &= h(h(h(N\|ID_{MU}))\|x\|x_0) \\ &= h(h(PW_{MU})\|x\|x_0) \end{aligned} \tag{7}$$
5. MU computes k and obtains $TCert_{MU}$. MU also authenticates FA by computing $h(x_0\|x)$ with the decrypted $h(x_0\|x)$. Therefore, MU can be sure that it is communicating with a legal FA.

2.3 Second Phase

When MU visits FA at the i-th session, MU sends the following login message to FA.

1. $MU \rightarrow FA$: $TCert_{MU}, (x_i\|TCert_{MU}\|$Other Information$)_{k_i}$

The new i-th session key k_i can be derived from the unexpired previous secret value x_{i-1} and the fixed secret value x as

$$k_i = h(h(h(N \| ID_{MU})) \| x \| x_{i-1}) \tag{8}$$

where $i = 1, \ldots, n$.

2. Upon receiving a login message from MU, FA decrypts $(x_i \| TCert_{MU} \| \text{OtherInformation})_{k_i}$ with k_i and newly saves $(TCert_{MU}, h(PW_{MU}), x_i)$ for the next communication.

3. Anonymity Problem of Kang et al.'s Scheme

Kang et al. [7] improved Wu et al.'s scheme [3] and Wei et al.'s scheme [6] to provide anonymity. Based on the general interest of mobile users, user anonymity should be kept from any eavesdroppers including the foreign agents [5]. However, Kang et al.'s scheme still cannot provide anonymity. The main reason is that HA always computes r_1 for each MU with the same secret key N. The detailed anonymity broken attack scenario is as follows.

1. Any legal user MU can directly obtain $h(N \| ID_{HA})$ from r_1 in his/her smart card because $r_1 = h(N \| ID_{HA})$ from the Eq. (2).
2. The legal user MU can collect the messages $\{n', (h(ID'_{MU}) \| x'_0 \| x')_{L'}, ID_{HA}, T'_{MU}\}$ sent from any other legal mobile user MU' to FA at step (1) in the first phase (see Fig. 1). From the Eqs. (1)~(4), we can see that n' is equal to $h(T'_{MU} \| r_1) \oplus ID_{HA} \oplus ID'_{MU}$ as follows.

$$\begin{aligned} n' &= h(T'_{MU} \| r_1) \oplus r'_2 \oplus PW'_{MU} \\ &= h(T'_{MU} \| r_1) \oplus h(N \| ID'_{MU}) \oplus ID_{HA} \\ &\quad \oplus ID'_{MU} \oplus PW'_{MU} \\ &= h(T'_{MU} \| r_1) \oplus h(N \| ID'_{MU}) \oplus ID_{HA} \\ &\quad \oplus ID'_{MU} \oplus h(N \| ID'_{MU}) \\ &= h(T'_{MU} \| r_1) \oplus ID_{HA} \oplus ID_{MU} \end{aligned} \tag{9}$$

3. With obtained $r_1 = h(N \| ID_{HA})$ and collected messages $\{n', ID_{HA}, T'_{MU}\}$, MU can get the real identity ID'_{MU} of the other mobile user MU' as HA does at step (3) in the first phase as follows.

$$\begin{aligned} ID'_{MU} &= n' \oplus ID_{HA} \oplus h(T'_{MU} \| r_1) \\ &= h(T'_{MU} \| r_1) \oplus ID_{HA} \oplus ID'_{MU} \\ &\quad \oplus ID_{HA} \oplus h(T'_{MU} \| r_1) \\ &= ID'_{MU} \end{aligned} \tag{10}$$

As a result, legal mobile user MU''s anonymity cannot be preserved in Kang et al.'s scheme.

4. Conclusions

This letter demonstrated that recently published wireless authentication scheme by Kang et al. still cannot provide anonymity. Therefore, Kang et al.'s scheme did not solved the problem of user anonymity that was pointed out Zeng et al. [4] and Lee et al. [5].

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2010-0010106) and partially supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2012-H0301-12-2004) supervised by the NIPA (National IT Industry Promotion Agency).

References

[1] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environment," IEEE Trans. Consum. Electron., vol.50, no.1, pp.230–234, 2004.
[2] C.C. Lee, M.S. Hwang, and I.E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," IEEE Trans. Ind. Electron., vol.53, no.5, pp.1683–1687, 2006.
[3] C.C. Wu, W.B. Lee, and W.J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," IEEE Commun. Lett., vol.12, no.10, pp.722–723, 2008.
[4] P. Zeng, Z. Cao, K.R. Choo, and S. Wang, "On the anonymity of some authentication schemes for wireless communications," IEEE Commun. Lett., vol.13, no.3, pp.170–171, 2009.
[5] J. Lee, J.H. Chang, and D.H. Lee, "Security flaw of authentication scheme with anonymity for wireless communications," IEEE Commun. Lett., vol.13, no.5, pp.292–293, 2009.
[6] Y. Wei, H. Qiu, and Y. Hu, "Security analysis of authentication scheme with anonymity for wireless environments," ICCT (International Conference on Communication Technology), 2006.
[7] M. Kang, H. Rhee, and J. Choi, "Improved user authentication scheme with user anonymity forwireless communications," IEICE Trans. Fundamentals, vol.E94-A, no.2, pp.860–864, Feb. 2011.