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

Eun-Jun YOON\(^{(*)}\) 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 as they claimed.

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.

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.

\[
PW_{MU} = h(N||ID_{MU})
\]
\[
r_1 = h(N||ID_{HA})
\]
\[
r_2 = h(N||ID_{MU}) \oplus ID_{HA} \oplus ID_{MU}
\]

where \(N\) is a secret value kept by HA. HA stores ID\(_{HA}\), \(r_1\), \(r_2\) and \(h()\) 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: \((n, (h(ID_{MU})||x_0)||x, ID_{HA}, T_{MU})\)

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.

\[
n = h(T_{MU}|r_1) \oplus r_2 \oplus PW_{MU}
\]
\[
L = h(T_{MU} \oplus PW_{MU})
\]

Table 1 Notations.

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA</td>
<td>Home Agent of a mobile user</td>
</tr>
<tr>
<td>FA</td>
<td>Foreign Agent of the network</td>
</tr>
<tr>
<td>MU</td>
<td>Mobile User</td>
</tr>
<tr>
<td>PW(_{MU})</td>
<td>A password of MU</td>
</tr>
<tr>
<td>N</td>
<td>A strong secret key of HA</td>
</tr>
<tr>
<td>ID(_A)</td>
<td>Identity of an entity A</td>
</tr>
<tr>
<td>(T_A)</td>
<td>Timestamp generated by an entity A</td>
</tr>
<tr>
<td>Cert(_A)</td>
<td>Certificate of an entity A</td>
</tr>
<tr>
<td>((X)_K)</td>
<td>Encryption of message X using symmetric key K</td>
</tr>
<tr>
<td>(E_{PA}(X))</td>
<td>Encryption of message X using public key of A</td>
</tr>
<tr>
<td>(S_{HA}(X))</td>
<td>Signature on message X using private key of A</td>
</tr>
<tr>
<td>(h())</td>
<td>A one-way hash function</td>
</tr>
<tr>
<td>(</td>
<td></td>
</tr>
<tr>
<td>@</td>
<td>Bitwise exclusive-or operation</td>
</tr>
</tbody>
</table>

Manuscript received July 21, 2011.

\(^{(*)}\) The author is with the Department of Cyber Security, Kyungil University, 33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangbuk-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
Input \( ID_{MU} \) and \( PW_{MU} \).
Generate two random \( x_0 \) and \( c \).

\begin{align*}
\text{Generate timestamp } T_{MU} \\
n &= h(T_{MU}) \oplus \epsilon_2 \oplus PW_{MU} \\
L &= h(T_{MU} \oplus PW_{MU})
\end{align*}

\[ n, (h(ID_{MU}))|x_0|L, ID_{HA}, T_{MU} \]

Check \( T_{MU} \).
Generate random \( b \).
Compute signature \( S_{FA}(h(ID_{MU}))|x_0|x_L, T_{MU}, Cert_{FA}) \).
Generate timestamp \( T_{FA} \).

\[ b, n, (h(ID_{MU}))|x_0|x_L, T_{MU}, \]

\[ S_{FA}(h(ID_{MU}))|x_0|x_L, T_{MU}, Cert_{FA}, Cert_{FA}, T_{FA} \]

Check \( T_{FA} \) and \( T_{HA} \).
Generate temporary certificate \( TCert_{FA} \).
Decrypt \( W \).

\[ k = h(h(N)|ID_{MU}||s|x_0) \]

\[ (TCert_{MU}||h(x_0||x))_k \]

\[ k = h(h(PW_{MU})|s|x_0) \]

\[ \text{Decrypt } (TCert_{MU}||h(x_0||x)_k \]

\[ \text{Check } h(x_0||x) \]

\begin{align*}
\text{Check } Cert_{FA} \text{ 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}) \\
\text{Decrypt } (h(ID_{MU}))|x_0|x_L \\
\text{Check } h(ID_{MU}) \\
W &= EP_{FA}(h(h(N)|ID_{MU})))|x_0|x_L \\
\text{Compute signature } S_{FA}(h(b, c, W, Cert_{HA})) \\
\text{Generate timestamp } T_{HA} \]

\begin{align*}
\text{[c, W, b, S_{SHA}(h(b, c, W, Cert_{HA}), Cert_{HA}, T_{HA})]}
\end{align*}

2. \( MU \rightarrow FA \): \[ (TCert_{MU}||h(x_0||x)_k \]

\[ \text{Decryt } (TCert_{MU}||h(x_0||x)_k \]

Check \( h(x_0||x) \)

4. \( FA \rightarrow MU \): \[ (TCert_{MU}||h(x_0||x)_k \]

\[ \text{FA checks whether or not the certificate } Cert_{HA} \]

Check \( T_{HA} \) and \( T_{HA} \).
Generate temporary certificate \( TCert_{HA} \).
Decrypt \( W \).

\[ k = h(h(N)|ID_{MU}||s|x_0) \]

\[ (TCert_{MU}||h(x_0||x))_k \]

\[ k = h(h(PW_{MU})|s|x_0) \]

\[ \text{Decryt } (TCert_{MU}||h(x_0||x)_k \]

Check \( h(x_0||x) \)

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. \( MU \rightarrow FA \): \[ TCert_{MU}, (x||TCert_{MU})|\text{Other Information}||k \]

\[ \text{Generate temporary certificate } TCert_{FA} \text{ and timestamp } T_{FA}. \]

\[ \text{Generate random } b, c, \text{ and } W. \]

\[ S_{FA}(h(b, c, W, Cert_{HA})) \]

\[ h(x_0||x) \]

\[ \text{Decrypt } (TCert_{MU}||h(x_0||x)_k \]

Check \( h(x_0||x) \)

2. \( FA \rightarrow MU \): \[ (TCert_{MU}||h(x_0||x)_k \]

\[ \text{FA checks whether or not the certificate } Cert_{HA} \]

Check \( T_{HA} \) and \( T_{HA} \).
Generate temporary certificate \( TCert_{HA} \).
Decrypt \( W \).

\[ k = h(h(N)|ID_{MU}||s|x_0) \]

\[ (TCert_{MU}||h(x_0||x))_k \]

\[ k = h(h(PW_{MU})|s|x_0) \]

\[ \text{Decryt } (TCert_{MU}||h(x_0||x)_k \]

Check \( h(x_0||x) \)

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 \( FA \).
The new $i$-th session key $k_i$ can be derived from the un-expired previous secret value $x_{i-1}$ and the fixed secret value $x$ as

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

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

2. Upon receiving a login message from $MU$, $FA$ decrypts $(x_i||T_{Cert_{MU}}||OtherInformation)_k$ with $k_i$ and newly saves $(T_{Cert_{MU}}, h(PW_{MU}, x_i)$ 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 $(n', (h(ID'_{MU})||x'_0||x'_1), ID_{HA}, T'_{MU})$ 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.

$$n' = h(T'_{MU}||r_1) \oplus ID_{HA} \oplus ID'_{MU}$$

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.

$$ID'_{MU} = n' \oplus ID_{HA} \oplus h(T'_{MU}||r_1)$$

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 solve 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**


