On the Anonymity of Some Authentication Schemes for Wireless Communications

Peng Zeng, Zhenfu Cao, Kim-Kwang Raymond Choo, and Shengbao Wang

Abstract—In 2004, Zhu and Ma proposed a new and efficient authentication scheme claiming to provide anonymity for wireless environments. Two years later, Lee et al. revealed several previously unpublished flaws in Zhu-Ma’s authentication scheme and proposed a fix. More recently in 2008, Wu et al. pointed out that Lee et al.’s proposed fix fails to preserve anonymity as claimed and then proposed yet another fix to address the problem. In this paper, we use Wu et al.’s scheme as a case study and demonstrate that due to an inherent design flaw in Zhu-Ma’s scheme, the latter and its successors are unlikely to provide anonymity. We hope that by identifying this design flaw, similar structural mistakes can be avoided in future designs.

Index Terms—Anonymity, authentication, wireless communications.

I. INTRODUCTION

WIRELESS communications technologies have undergone rapid development in recent years to meet the increasing needs of high-speed cordless connections in civil and military applications. In a wireless environment, the disclosure of a mobile user’s identity allows unauthorized entities to track his/her moving history and current location. This results in a compromise of the individual’s privacy [1] and potentially increases other risks of exploitation. Arguably, anonymity characteristics should be a feature to be considered in the design of wireless communications technologies. To provide anonymity service for wireless communications, Zhu and Ma proposed a new and efficient authentication scheme in which mobile users are allowed to perform only symmetric encryption and decryption operations [1]. Lee et al., however, showed that Zhu-Ma’s scheme is insecure and proposed an enhanced scheme to withstand identified weaknesses [2]. More recently in 2008, Wu et al. pointed out that Lee et al.’s enhanced scheme also fails to provide anonymity as claimed and then proposed a simple fix [3]. In this paper, we use Wu et al.’s scheme as a case study and demonstrate that due to an inherent design flaw in Zhu-Ma’s scheme, the latter and its successors are unlikely to provide user anonymity. We hope that by identifying this design flaw, similar structural mistakes can be avoided in future designs.

II. REVIEW OF WU ET AL.’S SCHEME

Wu et al.’s authentication scheme [3] consists of three phases: initial phase, first phase, and second phase. We briefly depict them in the following (the notations involved are listed in Table I).

A. Initial phase

When a new mobile user (MU) wants to register at his/her home agent (HA), he/she submits his/her identity ID_{MU} to the HA. Then HA delivers MU’s password PW_{MU} and a smart card, which contains ID_{HA}, r, and h, to MU through a secure channel. The PW_{MU} and r are calculated as follows:

\[
PW_{MU} = h(N||ID_{MU})
\]

and

\[
r = h(N||ID_{HA}) \oplus h(N||ID_{MU}) \oplus ID_{HA} \oplus ID_{MU},
\]

where N is a secret value kept by HA.

B. First phase

In this phase, the foreign agent (FA) authenticates MU and issues a temporary certificate to MU as follows, where the statement \(\{A \rightarrow B : M\}\) denotes that B receives a message M from A.

**Step 1.** \(MU \rightarrow FA: n, C, ID_{HA}, T_{MU}\)

MU computes

\[
n = r \oplus PW_{MU} = h(N||ID_{HA}) \oplus ID_{HA} \oplus ID_{MU} \tag{1}
\]

and

\[
C = (h(ID_{MU})||x_0||x), \text{ where } L = h(T_{MU} \oplus PW_{MU})
\]

is his/her temporary key, and \(x_0\) and \(x\) are two secret random numbers. A timestamp \(T_{MU}\) is also selected by MU to prevent from replay attacks.

**Step 2.** \(FA \rightarrow HA: b, n, C, T_{MU}, E_{SF_A}(h(b, n, C, T_{MU}, Cert_{FA})), Cert_{FA}, T_{FA}\)

FA passes the information received from MU with a certificate \(Cert_{FA}\), a secret random number \(b\), and the corresponding signature \(E_{SF_A}(h(b, n, C, T_{MU}, Cert_{FA}))\) to HA.

---

**TABLE I**

THE NOTATIONS USED IN WU ET AL.’S AUTHENTICATION SCHEME [3]

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 a message X using a symmetric key K</td>
</tr>
<tr>
<td>E_{K}(X)</td>
<td>Encryption of a message X using an asymmetric key K</td>
</tr>
<tr>
<td>h</td>
<td>A one-way hash function</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>⊕</td>
<td>XOR operator</td>
</tr>
</tbody>
</table>

Manuscript received October 30, 2008. The associate editor coordinating the review of this letter and approving it for publication was C.-K. Wu.

P. Zeng and Z. Cao (corresponding author) are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China (e-mail: zpengcmu021@gmail.com, zfcao@cs.sjtu.edu.cn).

K.-K. R. Choo is with the Australian Institute of Criminology and the ARC Centre of Excellence in Policing and Security, Regulatory Institutions Network, Australian National University’s College of Asia and the Pacific, Australia (e-mail: raymond.choo.au@gmail.com). Note that the views expressed in this article are those of the author alone and not the Australian Government or the organizations with whom the author are or have been associated. Research was carried out in the author’s personal capacity.

S. Wang is with New Star Research Institute of Applied Technology, China (e-mail: shengbaowang@gmail.com).

Digital Object Identifier 10.1109/LCOMM.2009.081821
HA, then he/she can derive its predecessors [1], [2] are unable to preserve user anonymity. Upon receiving messages from MU, FA decrypts unexpired previous secret knowledge secret random number generated by HA.

C. Second phase

We now demonstrate that both Wu et al.’s scheme [3] and its predecessors [1], [2] are unable to achieve the anonymity service too. Also applicable to the two schemes which causes them to fail if the attacker colludes with the FA, then FA can know the identity of mobile users and defeat the (claimed) anonymity service provided by Wu et al.’s scheme. Especially, if the attacker colludes with the FA, then FA can know the identity of all mobile users who shared the same HA with the attacker and are communicating with it.

Since Zhu-Ma’s and Lee et al.’s schemes have the same initial phase as Wu et al.’s scheme, and the same messages $n$ and $ID_HA$ need to be sent from MU to FA during Step 1 of the first phase (see [1], [2]), it is clear that the above attack is also applicable to the two schemes which causes them to fail in achieving the anonymity service too.

IV. CONCLUSIONS

We pointed out an inherent design flaw in the scheme of Zhu and Ma (2004), which enables an attacker registered as a user of some home agent (HA) to obtain the identity of other users registered with the same HA without authorization. As a result, we recommend that none of these three schemes identified in this paper should be deployed for real world applications and hope that by identifying this design flaw, similar structural mistakes can be avoided in future designs.

ACKNOWLEDGEMENT

This work was supported in part by the National Natural Science Foundation of China under Grant Nos. 60673079 and 60773086 and the National 973 Program of China under Grant No. 2007CB11201.

REFERENCES