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 Two years later, Lee *et al.* revealed several previously unpublished flaws in Zhu-Ma's authentication scheme and proposed a fix.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.

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: zpecnu021@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

TABLE I
THE NOTATIONS USED IN WU *et al.*'S AUTHENTICATION SCHEME [3]

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
$E_K(X)$	Encryption of a message X using an asymmetric key K
h	A one-way hash function
$\|\|$	Concatenation operator
$\oplus$	XOR operator

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

$$n = r \oplus PW_{MU} = h(N||ID_{HA}) \oplus ID_{HA} \oplus ID_{MU} \quad (1)$$

and $C = (h(ID_{MU})||x_0||x)_L$, 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}, $E_{S_{FA}}(h(b, n, C, T_{MU}, Cert_{FA}))$, $Cert_{FA}$, T_{FA}

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

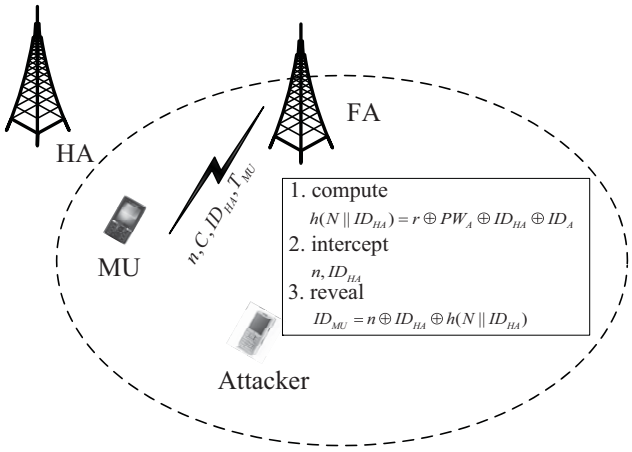

Fig. 1. Anonymity attack on Wu *et al.*'s authentication scheme [3].

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

HA computes the ciphertext

$$W = E_{P_{FA}}(h(h(N||ID_{MU}))||x_0||x)$$

and its signature $E_{S_{HA}}(h(b, c, W, Cert_{HA}))$, where c is a secret random number generated by HA.

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

With the response from HA, FA decrypts W with its secret key to obtain $h(h(N||ID_{MU}))$, x_0, and x. The session key $k = h(h(h(N||ID_{MU}))||x||x_0)$ between FA and MU is derived accordingly.

Upon receiving the message from FA, MU computes the session key k, and then decrypts $(TCert_{MU}||h(x_0||x))_k$ to obtain the temporary certificate $TCert_{MU}$.

C. Second phase

When MU visits FA at ith session, MU sends the following messages to FA:

MU $\rightarrow$ FA: $TCert_{MU}$, $(x_i||TCert_{MU}||OtherInformation)_{k_i}$

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

$$k_i = h(h(h(N||ID_{MU}))||x||x_{i-1}),\ i = 1, 2, \ldots, n.$$

Upon receiving messages from MU, FA decrypts $(x_i||TCert_{MU}||OtherInformation)_{k_i}$ and saves x_i for the next communication.

III. Anonymity of Wu *et al.*'s Scheme

We now demonstrate that both Wu *et al.*'s scheme [3] and its predecessors [1], [2] are unable to preserve user anonymity as claimed: an attacker who has registered as a user of HA, as shown in Fig. 1, can obtain the identity of other users as long as they registered at the same HA.

Assume that $\mathcal{A}$ is an attacker who has registered at some HA, then he/she can derive $PW_{\mathcal{A}}$, ID_{HA}, r, and h from the HA (see Sec. II-A), where

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

and

$$r = h(N||ID_{HA}) \oplus h(N||ID_{\mathcal{A}}) \oplus ID_{HA} \oplus ID_{\mathcal{A}}.$$

Consequently, $\mathcal{A}$ is able to compute $h(N||ID_{HA})$:

$$\begin{aligned} & r \oplus PW_{\mathcal{A}} \oplus ID_{HA} \oplus ID_{\mathcal{A}} \\ = \ & h(N||ID_{HA}) \oplus h(N||ID_{\mathcal{A}}) \oplus ID_{HA} \oplus ID_{\mathcal{A}} \\ & \oplus h(N||ID_{\mathcal{A}}) \oplus ID_{HA} \oplus ID_{\mathcal{A}} \\ = \ & h(N||ID_{HA}). \end{aligned}$$

Let MU be a mobile user who is registered at the same HA and is running the first phase with some FA. It is obvious that $\mathcal{A}$ can intercept ID_{HA} and $n = h(N||ID_{HA}) \oplus ID_{HA} \oplus ID_{MU}$ (see Eq. (1)) from Step 1 because wireless is broadcast in nature and anyone within range of a wireless device can intercept the packets being sent out without interrupting the flow of data [1]. Next, $\mathcal{A}$ can confirm that MU is a user of HA based on ID_{HA} and determine the identity of MU by executing the XOR operation to n, ID_{HA}, and $h(N||ID_{HA})$. That is, $\mathcal{A}$ is able to compute

$$\begin{aligned} & n \oplus ID_{HA} \oplus h(N||ID_{HA}) \\ = \ & h(N||ID_{HA}) \oplus ID_{HA} \oplus ID_{MU} \\ & \oplus ID_{HA} \oplus h(N||ID_{HA}) \\ = \ & ID_{MU}. \end{aligned}$$

The above attack shows that it is trivial for an attacker to obtain the identity of mobile users and defeat the (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. 2007CB311201.

References

[1] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Trans. Consumer 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. Industrial 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.