LETTER

An Enhanced User Authentication Scheme for Wireless Communications

Xinchun CUI[†a)], ***Student Member and*** **Xiaolin QIN**[†], ***Nonmember***

SUMMARY In this letter, anonymity problems of wireless communications are discussed. The weak points of previous studies is analyzed, then a user authentication scheme with anonymity enhanced for wireless communications is proposed.

key words: *user authentication, anonymity, wireless communications*

1. Introduction

User authentication is an important issue for wireless communication systems [1]–[8]. It is essential to keep user anonymity while accessing legitimate users and rejecting unauthorized users in wireless environments. Disclosure of a mobile user's real identity may lead to violations of the user's privacy, such as his roaming history, his current location and messages to/from him. Impersonation attacks that caused may give rise to data distortion, denial of service or even paralyze the whole communication system [5], [6], [8]. In recent years, various user authentication schemes have been proposed [5]–[8]. In 2004, Zhu and Ma proposed an authentication scheme to provide anonymity services for wireless communications [5]. However, Lee, Hwang, and Liao pointed out that that scheme has some security issues and then improved it in 2006 [6]. Two years later, Wu et al. pointed out that Lee et al.'s enhanced scheme also failed to provide anonymity as claimed and then proposed a modified scheme [7]. More recently in early 2009, Zeng et al. demonstrated that none of the above protocols can achieve the claimed anonymity due to an inherent design flaw in the initial phase [8].

In this letter, we take Wu et al.'s scheme as an example of the above schemes and analyze the anonymity problem. Then, we propose an improved user authentication scheme by encrypting some key parameters.

2. Review of Wu et al.'s Scheme

As an improvement of previous researches [5], [6], Wu et al.'s scheme consists of three phases: initial phase, first phase and second phase. The details are shown in [7], and notations used in this scheme are listed in Table 1.

Manuscript received April 2, 2010.
Manuscript revised September 13, 2010.

[†]The authors are with the College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, P.R. China.
a) E-mail: cuixc@nuaa.edu.cn

DOI: 10.1587/transinf.E94.D.155

Table 1 List of symbols.

Notations	Meaning
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

2.1 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

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

where N is a secret value kept by HA.

2.2 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

$$n = r \oplus PW_{MU} = h(N||ID_{HA}) \oplus ID_{HA} \oplus ID_{MU} \quad (2)$$

and $C = (h(ID_{MU})||x_0||x)_L$, is his/her temporary key, where $L = h(T_{MU} \oplus PW_{MU})$, 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.

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

HA computes the cipher text

$$W = E_{P_{FA}}(h(h(N||ID_{MU}))||x_0||x) \quad (3)$$

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

2.3 Second Phase

When MU visits FA at i-th session, MU sends the following messages to FA:
$MU \rightarrow FA : TCert_{MU}, (x_i||TCert_{MU}||OtherInformation)_{k_i}$
The new i-th session key k_i can be derived from the unexpired previous secret knowledge x_{i_1} and the fixed secret x as

$$k_i = h(h(h(N||ID_{MU}))||x||x_{i-1}), i = 1, 2, \ldots, n. \quad (4)$$

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

3. Security Weakness

As a successor of previous schemes [1], [2], Wu et al.'s scheme can't achieve perfect user anonymity due to some design flaws as explained in the following.
Anonymity as defined in [5] and [6] means that FA has no way of knowing MU's real identity. Yet, Wu et al.'s scheme and its predecessors [5], [6] are unable to preserve user anonymity as claimed [8]. Namely, an attacker may obtain the identity of other users as long as they registered at the same HA. Suppose that A is an attacker, he/she can firstly register at some HA, and get PW_A, ID_{HA}, r, and h from the HA, where $PW_A = h(N||ID_A)$, and

$$r = h(N||ID_{HA}) \oplus h(N||ID_A) \oplus ID_{HA} \oplus ID_A. \quad (5)$$

He/she then can get $h(N||ID_{HA})$ by computing:

$$\begin{aligned} &r \oplus PW_A \oplus ID_{HA} \oplus ID_A \\ &\quad = h(N||ID_{HA}) \oplus h(N||ID_A) \oplus ID_{HA} \oplus ID_A \\ &\qquad \oplus h(N||ID_A) \oplus ID_{HA} \oplus ID_A \\ &\quad = h(N||ID_{HA}). \end{aligned} \quad (6)$$

Assume MU is a registered mobile user of the same HA, A can get n by intercepting the packets being sent out without interrupting the flow of data. Then A is able to get ID_{MU} by computing:

$$\begin{aligned} &n \oplus ID_{HA} \oplus h(N||ID_{HA}) \\ &\quad = h(N||ID_{HA}) \oplus ID_{HA} \oplus ID_{MU} \oplus ID_{HA} \oplus h(N||ID_{HA}) \\ &\quad = ID_{MU}. \end{aligned} \quad (7)$$

That is to say, by launching above attacks, it is easy to get the identity of mobile users and defeat the claimed anonymity service provided by Wu et al.'s scheme [3]. Furthermore, after A get a user's real ID, he/she can then launch an impersonation attack.

4. Improved Scheme

An improvement is made to Wu et al.'s scheme to enhance the security of the user authentication scheme.
From the above analysis we know that an attacker can deduce a legal user's ID by XOR operation. To deter this, we just set

$$r = h(N||ID_{HA}) \oplus h(N||ID_{MU}) \oplus E_{P_{HA}}(ID_{HA}||ID_{MU}) \quad (8)$$

and accordingly, in the initial phase, we set

$$n = r \oplus PW_{MU} = h(N||ID_{HA}) \oplus E_{P_{HA}}(ID_{HA}||ID_{MU}) \quad (9)$$

So that HA can deduce ID_{MU} from parameter n.

5. Security Analysis

In this section, we will demonstrate how the proposed scheme can achieve perfect anonymity.
Theorem 1: The proposed scheme achieves user anonymity.
Proof: In initial phase of the improved scheme, when an attacker A registers to a HA, he/she obtains PW_A, ID_{HA}, r, and h from HA, even $h(N||ID_{HA})$ (see Eq. (6)). So that he/she may get $E_{P_{HA}}(ID_{HA}||ID_{MU})$, yet he/she can't decrypt it without the private key of HA. So the value of ID_{MU} can't be deduced by an anonymity attack (see Sect. 3). Thus, user anonymity can be achieved in this scheme.

6. Conclusion

In this paper, we identified a security weakness of Wu et al's scheme and proposed a user authentication scheme which can achieve perfect user anonymity.

Acknowledgements

This study is partially supported by the Natural Science Foundation of China under grant Number 60673127, 10771120, National High Technology Research and Development Program (Project 863) of China under grant number 2007AA01Z404, and Key Technology Research and Development Program of Jiangsu Province of China under grant number BE2008135.

The authors would like to give their sincere gratitude to the anonymous reviewers of this paper for their constructive comments.

References

[1] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., vol.46, no.1, pp.28–30, 2000.

[2] K.C. Leung, L.M. Cheng, A.S. Fong, and C.K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., vol.49, no.4, pp.1243–1245, Nov. 2003.
[3] J.J. Shen, C.W. Lin, and M.S. Hwang, "A modified remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., vol.49, no.2, pp.414–416, May 2003.
[4] S.J. Wang, "Yet another login authentication using N-dimensional construction based on circle property," IEEE Trans. Consum. Electron., vol.49, no.2, pp.337–341, May 2003.
[5] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," IEEE Trans. Consum. Electron., vol.50, no.1, pp.230–234, 2004.
[6] 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.
[7] 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.
[8] P. Zeng, Z. Cao, K. Choo, et al, "On the Anonymity of Some Authentication Schemes for Wireless Communications," IEEE Commun. Lett., vol.13, no.3, pp.170–171, 2009.