IEICE Electronics Express, Vol.8, No.8, 536–541

Anonymous authentication with unlinkability for wireless environments

Li Kun[a)], **Xiu Anna**[b)], **He Fei**[c)], **and Dong Hoon Lee**[d)]
Korea University, Republic of Korea
a) *lijunyantc@hotmail.com*
b) *19840317xiu@korea.ac.kr*
c) *hefei1986@gmail.com*
d) *donghlee@korea.ac.kr*

Abstract: With the development of wireless networks and the use of mobile devices, mobile user's privacy issue is becoming more and more important. In order to protect mobile user's privacy, the previous works in the literature mainly considered anonymous authentication of mobile users. Unfortunately anonymity only is not sufficient to guarantee the intended privacy if messages are identified to belong to one specific user. In this paper, we propose an anonymous authentication scheme with unlinkability for wireless environments. The analysis results show that all the previous anonymous schemes are linkable while our scheme is anonymous and unlinkable. The scheme is still efficient when compared with the previous schemes providing anonymity only.

Keywords: anonymity, authentication, unlinkability, wireless environments, security, key agreement
Classification: Wireless circuits and devices

References

[1] M. G. Rahman and H. Imai, "Security in wireless communication," *Wireless Personal Communications*, vol. 22, no. 2, pp. 213–228, 2002.
[2] J. Zhu and J. Ma, "A new Authentication scheme with anonymity for wireless environments," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 231–235, 2004.
[3] 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.
[4] J. Xu and D. Feng, "Security flaws in authentication protocols with anonymity for wireless environments," *ETRI Journal*, vol. 31, no. 4, pp. 460–462, 2009.
[5] 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.

DOI: 10.1587/elex.8.536
Received October 27, 2010
Accepted January 03, 2011
Published April 25, 2011

Table I. Notations

Notations	Descriptions
HA	Home Agent of a mobile user
FA	Foreign Agent of the network
MU	Mobile User
PW_{MU}	A password of MU
ID_A	Identity of 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
$h(X)$	A one-way hash function

1 Introduction

Cellphones are daily necessity, RFID (Radio Frequency Identification) is embedded in daily life applications, and laptops are used everywhere. We live in the mobile and wireless environments. Since the broadcast nature of wireless networks, the data being transferred can be intercepted by any attacker as long as she is within the coverage of the wireless information launcher. Given this inherent nature of wireless networks, the concern on user's privacy is increasing. User authentication is considered as one of best practices to keep private data private in wireless networks. Since hardware resources in mobile devices are quite limited, authentication with high security and low computation properties is required.

Related Work: Several authentication protocols in wireless networks have been proposed [1, 2, 3, 4, 5]. In [2], Zhu et al. proposed an anonymous authentication scheme. In 2006, Lee et al. [3] found a security flaw in Zhu's scheme and improved it. Wu et al. [5] improved Lee's scheme again in 2008. Finally, Xu and Feng [4] pointed out that Wu's scheme still fails to provide anonymity and improved the scheme to provide anonymity.

Our Contribution: All the schemes mentioned above did not consider a very important factor for user's privacy: unlinkability. When data packages are recognized to be from one specific (even anonymous) user, an attacker can easily identify the trajectory of the mobile user. In this paper we improve Xu and Feng's scheme to provide not only identity anonymity but also unlinkability. We also show that the proposed scheme is secure, compared to the previous schemes in the literature providing anonymity only. The paper is organized as follows. In Section 2 we review Xu and Feng's scheme and point out the weakness in Section 3. We propose our countermeasure scheme in Section 4 and conclusion follows in Section 5.

2 Review of Xu and Feng's scheme

The notations used in this scheme are listed in Table I.

DOI: 10.1587/elex.8.536
Received October 27, 2010
Accepted January 03, 2011
Published April 25, 2011

Xu and Feng's scheme, which is an improvement of Wu's scheme [5], provides user anonymity. There are 3 phases in this scheme and the details are shown as follows (See Figure 1).

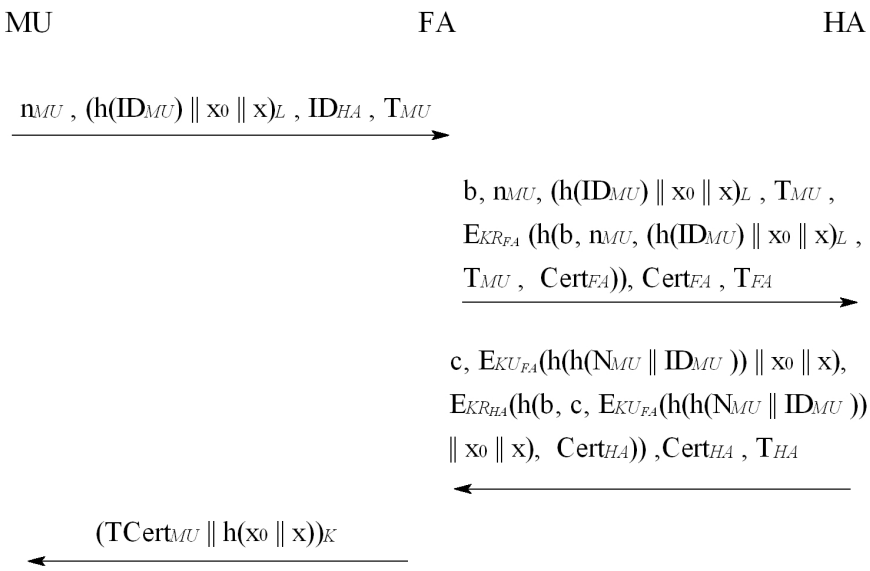

Fig. 1. Xu and Feng's Scheme

- **Phase 1: Initiation** HA generates a different long random number N_{MU} for each MU which is kept secretly and computes PW_{MU}, r_{MU} and n_{MU} as $PW_{MU} = h(N_{MU}||ID_{MU})$, $r_{MU} = h(N_{MU}||ID_{MU}) \oplus h(N_{MU}||ID_{HA}) \oplus ID_{HA} \oplus ID_{MU}$, $n_{MU} = PW_{MU} \oplus r_{MU}$. Then HA sends PW_{MU} and a smart card, which includes ID_{HA}, r_{MU}, to the MU through a secure channel. The HA also records the mapping relation between the MU's n_{MU} and N_{MU}.

- **Phase 2: Mutual Authentication** The mutual authentication between MU and FA is done in this phase.

  (1) MU generates secret random numbers x, x_0 and computes $n_{MU} = r_{MU} \oplus PW_{MU}$, the symmetric key $L = h(T_{MU} \oplus PW_{MU})$, where T_{MU} is a time stamp. Then MU sends $n_{MU}, (h(ID_{MU}||x_0||x))_L$, ID_{HA}, T_{MU} to FA.

  (2) After receiving the message from MU, FA first checks whether T_{MU} is valid or not. If it is valid, FA generates a random number b which is kept secretly and a signature $E_{KRFA}(b, n_{MU}, (h(ID_{MU})||x_0||x)_L, T_{MU}, Cert_{FA})$ with his private key KR_{FA}. Then FA sends $b, n_{MU}, (h(ID_{MU})||x_0||x)_L, T_{MU}, Cert_{FA}$, $E_{KRFA}(h(b, n_{MU}, (h(ID_{MU})||x_0||x)_L, T_{MU}, Cert_{FA}))$ and T_{FA} to HA.

  (3) After receiving the message from FA, HA first checks whether FA's signature and T_{FA} are valid. If they are both valid, HA com-

DOI: 10.1587/elex.8.536
Received October 27, 2010
Accepted January 03, 2011
Published April 25, 2011

putes $ID_{MU} = h(N_{MU}||ID_{HA}) \oplus n_{MU} \oplus ID_{HA}$. And after computing $h' = h(ID_{MU})$ and $L = h(T_{MU} \oplus h(N_{MU}||ID_{MU}))$, HA decrypts $(h(ID_{MU}||x_0||x))_L$ with L and compares the decrypted $h(ID_{MU})$ with h'. If they are the same, HA is convinced that the identity of MU is legal. Then HA generates a secret number c and a ciphertext $E_{KU\,FA}(h(h(N_{MU}||ID_{MU}))||x_0||x)$ with the public key KU_{FA}. Then HA generates a signature $E_{KR\,HA}(h(b, c, E_{KU\,FA}(h(h(N_{MU}||ID_{MU}))||x_0||x), Cert_{HA}))$ with his private key KR_{HA} and sends c, $E_{KR\,HA}(h(b, c, E_{KU\,FA}(h(h(N_{MU}||ID_{MU}))||x_0||x), Cert_{HA}))$, $Cert_{HA}$ and T_{HA} to FA.

(4) After receiving the message from HA, FA first checks the validity of HA's signature and time stamp. Then FA checks whether the received b equals to the original one, if it does, FA issues a temporary certificate $TCert_{MU}$ to MU. Then FA gets $h(h(N_{MU}||ID_{MU}))$, x_0 and x by decrypting $E_{KU\,FA}(h(h(N_{MU}||ID_{MU}))||x_0||x)$ with its private key KR_{FA}. FA also computes the session key k as $k = h(h(h(N_{MU}||ID_{MU}))||x||x_0)$ and sends $(TCert_{MU}||h(x_0||x))_k$ to MU.

(5) MU computes the session key $k = h(h(PW_{MU})\ ||\ \mathrm{x}||x_0)$ and decrypts $(TCert_{MU}||h(x_0||x))_k$ with k. Then MU checks whether the decrypted $h(x_0||x)$ equals to the original one, if it does, MU is convinced that the message is authentic.

- **Phase 3: Session Key Renewal** In the i_{th} time when MU wants to communicate with FA, he needs to renew the session key. The process is as follows. MU sends $TCert_{MU}$ and $(x_{i-1}||TCert_{MU})_{k_{i-1}}$ to FA, where x_{i-1} is chosen randomly. After receiving the message from MU, FA checks whether the $TCert_{MU}$ is valid or not, if it is, FA decrypts $(x_{i-1}||TCert_{MU})_{k_{i-1}}$ and checks whether the decrypted $TCert_{MU}$ equals to the original one, if it does, then FA is convinced that x_{i-1} is valid and the new session key is computed as $k_i = h(h(h(N_{MU}||ID_{MU}))||x||x_{i-1})$.

3 Weakness of Xu and Feng's scheme

Xu and Fengs scheme improved Wu et al.'s scheme [5] to provide identity anonymity. But it does not provide unlinkability which means that any data package sent by a same mobile user should not be linked by other entities except HA. That is, entities except HA should not be able to know that several certain data packages are originated from a same MU. In fact, Lee et al.'s scheme [3] and Zhu and Mas scheme [2] also fail to provide unlinkability for the same reason. The reason is as follows. Because different MU has a different but permanent value n_{MU} which has to be sent to FA every time MU wants to visit FA (Step (1) of Phase 2), so data packages that contain

DOI: 10.1587/elex.8.536
Received October 27, 2010
Accepted January 03, 2011
Published April 25, 2011

a same n_{MU} can be linked by FA. Another reason for data packages being linked by FA is the permanent certificate $TCert_{MU}$ which it issues to MU by FA. As a result, FA is able to track a specific MU by simply analyzing data packages that contain a same $TCert_{MU}$.

4 Our countermeasure scheme

In order to provide unlinkability property, N_{MU} should be changed to a new value which is never used previously when MU wants to visit FA. Furthermore, the session key renewal process should also be modified. We know that the $TCert_{MU}$ is issued by FA for the purpose of authentication and key renewal. But this can cause linkability because FA records the mapping relation $TCert_{MU}$ and the corresponding k_{i-1} of every MU. And thus once a specific MU sends a data package which contains $TCert_{MU}$ to FA for session key renewal, this package can be linked by FA. For this reason, we will not use $TCert_{MU}$ in step (5) of Phase 2. The details of our countermeasure scheme are as follows (See Figure 2). The notations are shown in Table I.

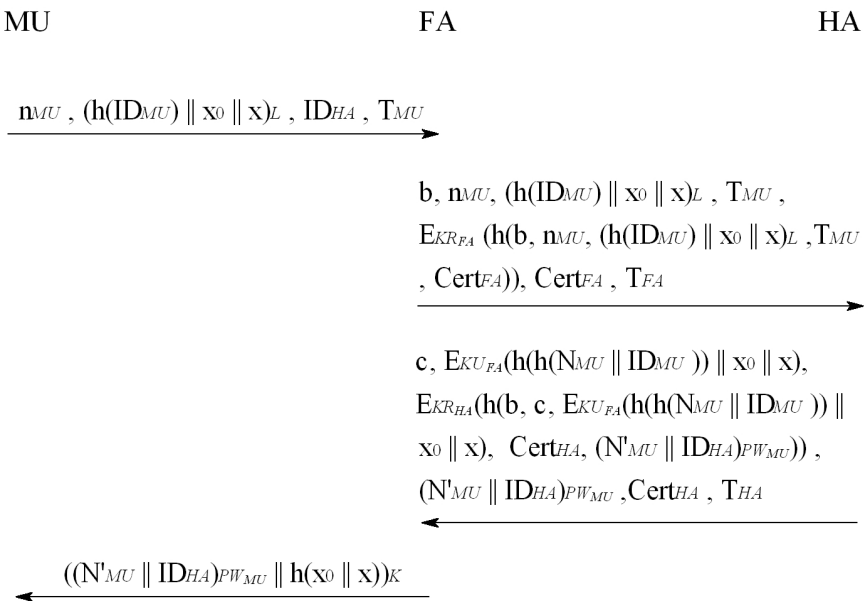

Fig. 2. Our countermeasure scheme

The initiation phase is the same with Xu and Feng's scheme. The differences between our scheme and Xu and Feng's scheme are step (3) and step (5) of phase 2 as well as phase 3.

In step (3) of phase 2, HA has to generate a new N'_{MU} for MU and encrypt N'_{MU} and ID_{HA} with PW_{MU} which is only known to HA and MU. Then HA sends c, $E_{KU\,FA}(h(h(N_{MU} \,||\, ID_{MU})) \,||\, x_0 \,||\, x)$, $E_{KR\,HA}(h(b,\ c,\ E_{KU\,FA}(h(h(N_{MU} \,||\, ID_{MU})) \,||\, x_0 || \,x),Cert_{HA}$, $(N'_{MU}||ID_{HA})_{PW\,MU}))$, $(N'_{MU}||ID_{HA})_{PW\,MU}$, $Cert_{HA}$, T_{HA} to FA.

DOI: 10.1587/elex.8.536
Received October 27, 2010
Accepted January 03, 2011
Published April 25, 2011

In Step (5) of phase 2, FA sends $((N'_{MU}||ID_{HA})_{PW_{MU}}||h(x_0||x))_k$ to MU. In phase 3, MU repeats step (1) to step (5) of phase 2 for session key renewal.

Since the new value N'_{MU} is sent to MU at the end of phase 2, PW_{MU}, r_{MU}, and n_{MU} should also be recomputed as,

$$PW'_{MU} = h(N'_{MU})||ID_{MU},$$

$$r'_{MU} = h(N'_{MU}||ID_{HA} \oplus h(N'_{MU}||ID_{MU}) \oplus ID_{HA} \oplus ID_{MU}),$$

$$n'_{MU} = PW'_{MU}||r'_{MU}.$$

In phase 2, no entities except HA can trace a specific MU by simply analyzing data packages because n_{MU} is changed to a new value which is never used previously every time MU wants to visit FA (step (1) of phase 2). So phase 2 provides unlinkability. The process of phase 3 is the same with that of phase 2 where unlinkability is guaranteed as explained above. So the FA has no useful information which can be used to identify the trajectory of the MU, and thus unlinkability is also guaranteed in phase 3. As we can see, our scheme provides both anonymity and unlinkability.

5 Conclusion

In this paper, we showed that Xu and Feng's Scheme does not provide unlinkability and proposed a countermeasure scheme which not only holds all the merits in Xu and Feng's scheme but also provides unlinkability property. The previous schemes proposed by Zhu and Ma and Lee et al. also failed to provide unlinkability for the same reason as well.

Acknowledgments

This work was supported by the IT R&D program of MKE/KEIT [KI002113, Development of Security Technology for Car-Healthcare]

DOI: 10.1587/elex.8.536
Received October 27, 2010
Accepted January 03, 2011
Published April 25, 2011