Security Flaws in Authentication Protocols with Anonymity for Wireless Environments

Jing Xu and Dengguo Feng

ABSTRACT—The emerging wireless networks require the design of new authentication protocols due to their dynamic nature and vulnerable-to-attack structure. Recently, Wu and others proposed a wireless authentication protocol which is claimed to be an improvement of the authentication protocol proposed by Lee and others which provides user anonymity. In this letter, we show that these protocols have a common flaw and that these protocols fail to provide user anonymity. We also propose a modification method to solve this problem.

Keywords—Wireless security, roaming service, anonymity, authentication, key agreement, smart card.

I. Introduction

With the widespread use of mobile devices, wireless roaming is rapidly becoming an important network feature. To provide effective global roaming service for a legitimate mobile user between the home network and a visited foreign network, strong authentication measures are required. When a mobile user (MU) roams to a foreign network, it performs authentication and updates its registration information with its home agent (HA) in the home network, either directly or indirectly. A session key is set up to encrypt further communication in the session between the MU and its foreign agent (FA) in the visited foreign network if the authentication is successful.

Identity anonymity is an important property for roaming services. The disclosure of a user identity may allow unauthorized entities to track his movement history and current location. Any illegal access to information related to users' location without their permission can be a serious violation of privacy. In 2004, Zhu and others proposed an authentication protocol providing anonymity for wireless environments [1]. In 2006, Lee and others [2] pointed out the weakness of Zhu's protocol and proposed an improvement. Recently, Wu and others [3] showed that Lee's protocol does not provide identity anonymity and perfect backward secrecy. They also proposed an improved protocol to repair the security flaws. However, in this letter, we demonstrate that the improved protocol still cannot achieve perfect identity anonymity, contrary to some of the security claims which have been made concerning them. We then present a simple patch which fixes the security problem.

II. Review of Wu's Protocol

For convenience, the abbreviations and notations used in this letter are shown in Table 1.

Table 1. Notations.

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
$\|\|$	Concatenation operation
$\oplus$	XOR operation

Manuscript received Jan. 16, 2009; revised Apr. 7, 2009; accepted May 11, 2009.

This work was supported by the National Grand Fundamental Research (973) Program of China under Grant No. 2007CB311202 and the National Natural Science Foundation of China (NSFC) under Grant No. 60873197 and No.60673083.

Jing Xu (phone: +86 62661721, email: xujing@is.iscas.ac.cn) and Dengguo Feng (email: feng@is.iscas.ac.cn) are with the State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China.

doi:10.4218/etrij.09.0209.0026

Wu's wireless authentication protocol [3] is claimed to be an improvement of Lee's authentication protocol [2] and to provide user anonymity. The protocol includes three phases. In phase I, the HA delivers a password and a smart card for the MU through a secure channel. In phase II, mutual authentication between the MU and an FA is provided through his or her HA. After successful validation, a session key is established, and the MU can obtain service from the FA. In phase III, the MU renews his or her session key with the FA.

1. Phase I: Initiation

When an MU registers with his or her HA, the MU's identity ID_{MU} is submitted to the HA. Then, the HA delivers the password PW_{MU} and a smart card that contains ID_{HA}, r, and $h(\cdot)$ to the MU through a secure channel. We calculate PW_{MU} and r as $PW_{MU} = h(N \| ID_{MU})$ and $r = h(N \| ID_{HA}) \oplus h(N \| ID_{MU}) \oplus ID_{HA} \oplus ID_{MU}$, where N is a long random number kept secretly by the HA.

2. Phase II: Mutual Authentication

In this phase, a mutual authentication between an MU and an FA is performed. The steps of this phase are the following (see Fig. 1).

i) When an MU enters a new FA, the MU initiates a registration authentication process with the FA in order to identify him or herself to be a legal subscriber of his or her HA. The MU keys his or her password PW_{MU} to the device. Then, the device generates secret random numbers x_0 and x; computes $n = r \oplus PW_{MU}$ and temporary key $L = h(T_{MU} \oplus PW_{MU})$, where T_{MU} is a time stamp; and sends n, $(h(ID_{MU}) \| x_0 \| x)_L$, ID_{HA}, and T_{MU} to the FA.

ii) On receiving the message from the MU, the FA checks if the time stamp T_{MU} is valid. If it is valid; the FA generates a secret random number b; signs $(b, n, (h(ID_{MU}) \| x_0 \| x)_L, T_{MU}, Cert_{FA})$ using a private key PR_{FA} to generate s_1; and sends b, n, $(h(ID_{MU}) \| x_0 \| x)_L$, T_{MU}, s_1, $Cert_{FA}$, and T_{FA} to the HA.

iii) On receiving the messages from the FA, the HA first checks if the signature and time stamp T_{FA} are valid. If they are valid, the HA gets the MU's real identity by computing $ID_{MU} = h(N \| ID_{HA}) \oplus n \oplus ID_{HA}$. Then, the HA computes $h^* = h(ID_{MU})$. Next, the HA calculates $L = h(T_{MU} \oplus h(N \| ID_{MU}))$ and uses it to decrypt $(h(ID_{MU}) \| x_0 \| x)_L$. If the decrypted $h(ID_{MU})$ is equal to h^*, the legal identity of the MU is authenticated. Subsequently, the HA generates a secret random number c; encrypts $(h(h(N \| ID_{MU})) \| x_0 \| x)$ with the public key PU_{FA} to generate e_1; signs $(b, c, e_1, Cert_{HA})$ using his or her private key PR_{HA} to generate s_2; and sends c, e_1, s_2, $Cert_{HA}$, and T_{HA} to the FA.

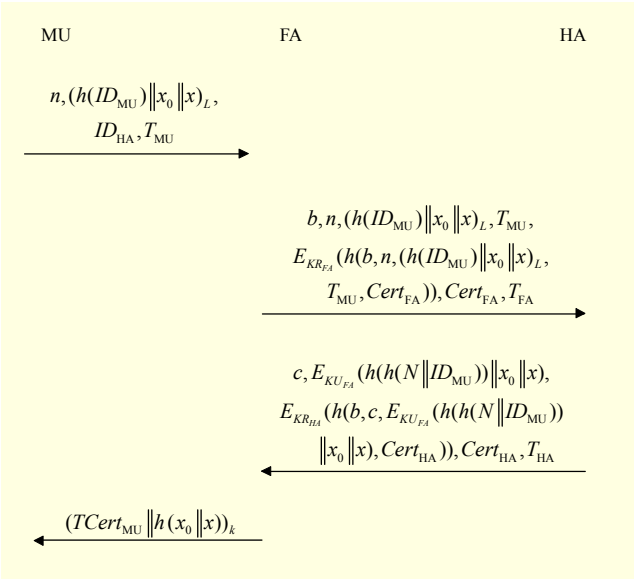

Fig. 1. Wu's improvement.

iv) On receiving the message from the HA, the FA first checks if the signature and time stamp T_{HA} are valid. Next, the FA checks if the received b is the same as its original b. If so, the FA issues to the MU the temporary certificate $Tcert_{MU}$, which includes lifetime and other information. Next, the FA decrypts e_1 with his or her own private key PR_{FA} to obtain $h(h(N \| ID_{MU}))$, x_0, and x. Then, the FA computes the session key $k = h(h(h(N \| ID_{MU})) \| x \| x_0)$ and sends $(TCert_{MU} \| h(x_0 \| x))_k$ to the MU.

v) Since $PW_{MU} = h(N \| ID_{MU})$, the MU also computes the session key $k = h(h(PW_{MU}) \| x \| x_0)$. Then, the MU decrypts $(TCert_{MU} \| h(x_0 \| x))_k$ using k. If the decrypted $h(x_0 \| x)$ is equal to its original value, the legal identity of the FA is authenticated.

3. Phase III: Session Key Renewal

Suppose that the MU needs to renew his or her session key k_{i-1} with the FA for the i-th time, then the new session key k_i can be obtained as follows.

The MU chooses x_{i-1} randomly and sends $TCert_{MU}$ and $(x_{i-1} \| TCert_{MU})_{k_{i-1}}$ to the FA. On receiving the messages from the MU, the FA checks if the certificate $TCert_{MU}$ is valid. If it is valid, the FA decrypts $(x_{i-1} \| TCert_{MU})_{k_{i-1}}$. If the decrypted $TCert_{MU}$ is the same as the original $TCert_{MU}$, the integrity of x_{i-1} is verified. Then, the new session key k_i is calculated as $k_i = h(h(h(N \| ID_{MU})) \| x \| x_{i-1})$.

III. Security Weakness in Wu's Protocol

In mobile networks, to prevent unauthorized entities from tracking a mobile user's movements and current whereabouts (which may be a serious violation of privacy), it is important to assure user anonymity so that the user's real identity can only be recognized by the user's HA, while others can only refer to the user by a pseudonym.

In this section, we demonstrate that Wu's improved protocol [3] does not provide identity anonymity. Similarly, Lee and Zhu's original authentication protocols [1], [2] also fall to our attacks.

Assume that $MU_{\mathfrak{A}}$ is a malicious mobile user registered with an HA. This $MU_{\mathfrak{A}}$ can obtain the identity of any other mobile user MU_i registered with the same HA. The attack proceeds as follows.

i) In the mutual authentication phase, the attacker, $MU_{\mathfrak{A}}$, overhears all the communication flows between MU_i and the FA and obtains n_i.

ii) Since $PW_i = h(N \| ID_i)$, $n_i = r_i \oplus PW_i$, and $r_i = h(N \| ID_{\mathrm{HA}}) \oplus h(N \| ID_i) \oplus ID_{\mathrm{HA}} \oplus ID_i$, we have $n_i = h(N \| ID_{\mathrm{HA}}) \oplus ID_{\mathrm{HA}} \oplus ID_i$. Similarly, $n_{\mathfrak{A}} = h(N \| ID_{\mathrm{HA}}) \oplus ID_{\mathrm{HA}} \oplus ID_{\mathfrak{A}}$. Thus, $MU_{\mathfrak{A}}$ can obtain the identity of mobile user MU_i from $ID_i = ID_{\mathfrak{A}} \oplus n_{\mathfrak{A}} \oplus n_i$.

Furthermore, we show that a malicious outsider $\mathfrak{A}$, who compromises a mobile user MU_i's identity, can reveal the identity of any other mobile user MU_j registered with the same HA as MU_i. In particular, $\mathfrak{A}$ overhears the messages n_i and n_j from MU_i and MU_j, respectively. Since $n_i = h(N \| ID_{\mathrm{HA}}) \oplus ID_{\mathrm{HA}} \oplus ID_i$ and $n_j = h(N \| ID_{\mathrm{HA}}) \oplus ID_{\mathrm{HA}} \oplus ID_j$, $\mathfrak{A}$ can obtain MU_j's identity by computing $ID_j = ID_i \oplus n_j \oplus n_i$.

IV. Countermeasure

Our attack exploits the fact that the same random number N is chosen by the HA for different mobile users registered with the HA. Thus, the patch is fortunately simple.

In the initiation phase, the HA generates a different random number N_{MU} for each mobile user and computes PW_{MU}, r_{MU}, and n_{MU} as

$$PW_{\mathrm{MU}} = h(N_{\mathrm{MU}} \| ID_{\mathrm{MU}}),$$

$$r_{\mathrm{MU}} = h(N_{\mathrm{MU}} \| ID_{\mathrm{HA}}) \oplus h(N_{\mathrm{MU}} \| ID_{\mathrm{MU}}) \oplus ID_{\mathrm{HA}} \oplus ID_{\mathrm{MU}},$$

$$n_{\mathrm{MU}} = PW_{\mathrm{MU}} \oplus r_{\mathrm{MU}}.$$

Then, the HA delivers the password PW_{MU} and a smart card, which contains ID_{HA}, r_{MU}, and $h(\cdot)$, to the MU through a secure channel. The HA also records the mapping relation of the MU's n_{MU} and N_{MU} ($n_{\mathrm{MU}} \leftrightarrow N_{\mathrm{MU}}$). In the mutual authentication phase, the HA gets the MU's real identity by computing $ID_{\mathrm{MU}} = h(N_{\mathrm{MU}} \| ID_{\mathrm{HA}}) \oplus n_{\mathrm{MU}} \oplus ID_{\mathrm{HA}}$.

With this modification, the message n_{MU} sent by the MU in each run of the protocol becomes bounded to the identity ID_{MU} and N_{MU} of the MU; therefore, such an attack as that previously presented would be impossible.

V. Conclusion

In this letter, we demonstrated that Wu's wireless authentication protocol [3] fails to provide perfect identity anonymity, and it is easy to extend the result to the original versions [1], [2]. We have also demonstrated how to fix the protocol to ensure that it is robust against attacks.

References

[1] J. Zhu and J. Ma, "A New Authentication Scheme with Anonymity for Wireless Environments," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, Feb. 2004, pp. 231-235.

[2] C.C. Lee and M.S. Hwang, "Security Enhancement on a New Authentication Scheme with Anonymity for Wireless Environments," *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, Oct. 2006, pp. 1683-1686.

[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, Oct. 2008, pp. 722-723.