On the Security of an Efficient Mobile Authentication Scheme for Wireless Networks

Jian-zhu Lu and Jipeng Zhou

Abstract

Tang and Wu proposed an efficient mobile authentication scheme for wireless networks, and claimed the scheme can effectively defend all known attacks to mobile networks including the denial-of-service attack. This article shows an existential replication attack on the scheme and, as a result, an attacker can obtain the communication key between a mobile user and the accessed VLR. Fortunately, we improve its security in this paper.

Index Terms

mobile authentication; digital signature; replication attack; elliptic-curve cryptosystem.

I. Introduction

Rapid development of wireless networks are gradually changing the way we live, and security such as authentication of mobile stations is a serious concern for many emerging application. Through roaming technology, mobile users can access the services provided by a foreign network. However, there is no trusted authentication server available to mobile users out of its home network.

How to achieve mutual authentication between a mobile user and a visited location register in wireless networks ia an important security issue. Many mobile authentication schemes [1,3,4,5,6] have been proposed in recent years for the roaming environment. In 2006, Jiang et al. proposed a mutual authentication and key exchange protocols using secret splitting principle in [4]. Lee and Yeh [3] proposed a delegation-based authentication protocol for use in portable communication system. In 2008, Tang and Wu [5] produced a possible attack to Lee-Yeh's scheme, and proposed an efficient mobile authentication to overcome this flaw.

In this article, we show that Tang-Wu's scheme suffers from the replication attack. Under this kind of attack, the communication key between a mobile user and the legal service provider will be exposed. Inevitably, there would be a serious accounting problem with their scheme. The above-mentioned weakness in Tang-Wu's scheme will be explained in Section 3. To improve this disadvantage, we proposed an improvement to achieve security goals.

The remainder of this paper is organized as follows. Section 2 reviews Tang-Wu's scheme, and we discuss its weaknesses in Section 3. Then in Section 4 a simple improvement is proposed to repair the security flaw in Section 3. Finally, we make some conclusions in Section 5.

II. Review of Tang-Wu's scheme

In this section, we review Tang-Wu's scheme. There are three entities in the scheme: a mobile station (MS), a home location register(HLR), and a visited location registers (VLR). The scheme consists of three phases, namely, trust delegation initialization (TDI), efficient mobile authentication (EMA), and HLR offline authentication (HOA). We assume that T is a generator of an additive group $\mathcal{G}$ on an elliptic curve and p is the largest prime factor of the order of T. Let $h : Z_p^* \mapsto Z_p^*$ be a collision resistant one-way hash function and $\prod : \mathcal{G} \mapsto Z_p^*$ be a point representation function. The symbol '$\biguplus$' denotes a point addition operator in $\mathcal{G}$, and $[X]_K$ denotes encrypting a message X with a key K using a symmetric encryption algorithm. The scheme works as follows:

A. TDI

Let $Y = xT$ be the public key of HLR whose private key is x, where T is the generator of a subgroup of elliptic group of order p. First, a new mobile station (MS) sends his/her real identity IDM to the home location register (HLR) or home network for registration. Then HLR sets key usage restrictions on IDM in m_w, and generates MS's public/delegation key pair (Γ, σ) by calculating $\Gamma = (h(IDM|m_w)T) \uplus (kT)$, $\sigma = -xh(\Pi(\Gamma)) - \kappa$ (in Z_p^*), where κ is a random number. Finally, HLR publishes (IDM, m_w, Γ) and delivers (σ, m_w) to MS through a secure channel. HLR always keeps the mapping relationship of IDM and σ.

MS accepts the delegation key σ if $h(IDM|m_w)T = (\sigma T) \uplus (h(\Pi(\Gamma))Y) \uplus \Gamma$.

J. Lu is with Department of Computer Science, University of Jinan, Guangzhou, Guangdong, China 510632. (e-mail: tljz@jnu.edu.cn).
J. Zhou is with Department of Computer Science, University of Jinan, Guangzhou, Guangdong, China 510632. (e-mail: tjpzhou@jnu.edu.cn).

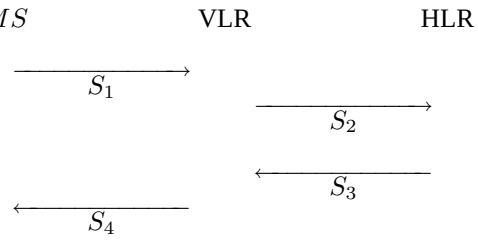

Fig. 1. Message exchange of EMA protocol in Tang-Wu's scheme

B. EMA

Suppose there is a secure channel to protect the traffic between a VLR and the HLR. The mutual authentication between a MS and a VLR is achieved as follows, where the statement $\{A \rightarrow B : M\}$ denotes that B receives a message M from A.

Step 1. MS $\rightarrow$ VLR: $S_1 = \{R, s, \text{IDH}, m_w, C, N\}$
MS computes

$$C = [ck, ts, T_{exp}, N]_\sigma \tag{1}$$

and

$$R = kT, \tag{2}$$
$$s = \sigma - kh(\Pi(R)|N) \text{mod} p \tag{3}$$

where ck is the communication key between MS and VLR, T_{exp} is the expiration time of communication key, and k and N are two random numbers. IDH is the identity of HLR. A timestamp ts is also selected by MS to counter replay attacks.

Step 2. VLR $\rightarrow$ HLR: $S_2 = \{\text{IDM}, C\}$
On receipt of message from MS, VLR checks the warrant m_w for restrictions, and authenticates MS by using the attached digital signature (R, s).

$$(sT) \biguplus \Gamma \biguplus (h(\prod(\Gamma))Y) \biguplus (h(\prod(R)|N)R) = h(\text{IDM}|m_w)T \tag{4}$$

HLR passes the information from MS with the identity IDM in m_w and certificate C to HLR.

Step 3. HLR $\rightarrow$ VLR: $S_3 = \{C_{V,H}, [T_{V,M}]_\sigma\}$
Let $K_{V,H}$ be the session key between VLR and HLR, and IDV is the identity of VLR. VLR obtains the delegation key σ from the mapping database, and then decrypts decrypt C to obtain IDM, T_{exp}, ts, ck and N. Afterwards, HLR can compute $C_{V,H} = [\text{IDM}, T_{exp}, ts, ck, N]_{K_{V,H}}$ and $[T_{V,M}]_\sigma$, where $T_{V,M} = \{\text{IDV}, N\}$. .

Step 4. VLR $\rightarrow$ MS: $S_4 = \{[\text{IDV}, N, [T_{V,M}]_\sigma]_{ck}\}$
With the response from HLR, VLR can decrypt $C_{V,H}$ with the session key $K_{V,H}$ to obtain IDM, T_{exp}, ts, ck and N. After checking the validity of expiration timestamp T_{exp} and consistence of N, VLR can send $[\text{IDV}, N, [T_{V,M}]_\sigma]_{ck}$ to MS for authentication.

MS decrypts the received message and $[T_{V,M}]_\sigma$ using ck and σ, respectively. By the consistence of IDV and N, MS can authenticate VLR.

C. HOA

In order to enhance the efficiency, while ck is not expired based on ts and T_{exp}, MS who stays with the same VLR picks two new random numbers k', $\tilde{N}$ to compute

$$R' = k'T, \tag{5}$$
$$s' = \sigma - k'h(\Pi(R)|\tilde{N}) \text{mod} p \tag{6}$$

Whereafter, MS sends $\{m_w|R'|s'|\text{IDH}|\tilde{N}\}$ to VLR for authentication.

III. The request replication attack

In this section we point out that the EMA protocol in Tang-Wu's scheme suffers from the request replication attack.

In EMA, communication key ck depends only on ts, T_{exp} and N; therefore, it is determined after S_1 is sent. An adversary with a compatible radio receiver/transmitter can easily eavesdrop ongoing radio communication link from the MS to a VLR

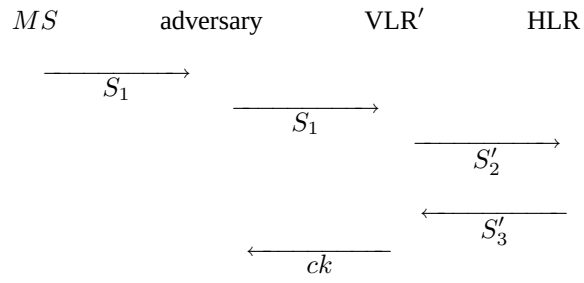

Fig. 2. Message exchange in the request replication attack for Tang-Wu's scheme

to gain the MS's request S_1. The request replication attack takes place when the adversary puts a replica of S_1 in a controlled VLR, and we denote this controlled VLR by VLR′ with identification IDV′.

Under control of the adversary, VLR′ establishs a session key $K_{V',H}$ with the HLR of MS, and sends the message, S_2, with the identity IDM in m_w and certificate C to the HLR at the same time that the accessed VLR does (After the EMA protocol shown in Fig.1, the share communication key ck between MS and the accessed VLR is established).

$$\textbf{Step 2'}.\ \text{IDV}' \rightarrow \text{HLR} : S'_2 = \{\text{IDM}, C\}.$$

It is obvious that the HLR can decrypt the ck and N encapsulated in C by using σ, and then send $C'_{V,H} = [\text{IDM}, T_{exp}, ts, ck, N]_{K_{V',H}}$ and $[T'_{V,M}]_\sigma = [IDV', N]_\sigma$ to VLR′.

$$\textbf{Step 3'}.\text{HLR} \rightarrow \text{VLR}' : S'_3 = \{C'_{V,H}, [T'_{V,M}]_\sigma\} \tag{7}$$

After VLR′ receives S'_3 (from HLR), which is defined as in (7), it successfully obtains the communication key ck by decrypting $C'_{V,H}$ with the session key $K_{V',H}$. Subsequently, the adversary can get the services from the VLR by impersonating the MS. Note that VLR′ is unable to transmit HLR's acknowledgment $[T'_{V,M}]_\sigma$ to the MS. It is straightforward to see that the accessed VLR, MS and HLR cannot know the fact that the communication key ck is compromised.

IV. Modification

In this section, we show a simple but possible solution by slightly modifying the original protocol.

A. Simple Idea

Because the original certificate $C = [ck, ts, N, T_{exp}, N]_\sigma$ can be used as an evidence to assure whether the MS's identity is correct, this value needs to be modified in a way to bind ck with the VLR. To do so, we set $C = [ck, ts, N, T_{exp}, N, \text{IDV}]_\sigma$ instead of old one in Step 1 of EMA phase. Moreover, in order to protect against replay attacks, MS sends a one-time digital signature in S_1 to the VLR. During the digital signature generation, we replace N with IDH$||m_w||C||N||ts$ in (3). Here, the request message of MS is $S_1 = \{R, s, \text{IDH}, m_w, C, N, ts\}$.

B. Analysis

We will describe how our proposed scheme can resist the impersonation attacks in this subsection.

Proposition 1: Our proposed improved scheme can resist the impersonation attacks.

Proof: In our improved scheme, HLR obtains $[ck, ts, N, T_{exp}, N, \text{IDV}]_\sigma$ instead of $[ck, ts, N, T_{exp}, N,]_\sigma$. Therefore, HLR can verify whether the VLR identity is consistent with the designated IDV in C. Thus, The request of adversary is refused by HLR. Besides, altering the identity IDV in $[ck, ts, N, T_{exp}, N, \text{IDV}]_\sigma$ is also intractable if the symmetric encryption algorithm is secure such as AES. Therefore, the impersonation attack cannot succeed. ■

V. Conclusions

In this paper, we discuss the properties of security in the mobile authentication scheme for wireless networks. The analysis has shown that the security issues in the previous schemes can be solved in a very simple way.

Acknowledgment

We would like to thank the professor Kefei Chen at Shanghai Jiaotong university for careful reading the paper. His useful suggestions improved the quality of the paper.

REFERENCES

[1] R. Molva, D. Samfat, G. Tsudik, “Authentication of mobile users,” IEEE Network Special Issue on Mobile Communications vol.8, no. 2, pp.26-34, 1994.
[2] T. Okamoto, M. Tada, E. Okamoto, Extended proxy signature for smart card, in LNCS 1729. Spinger-Verlag, 1999, pp. 247-258.
[3] W.-B. Lee, C.-K. Yeh, A new delegation-based authentication protocol for use in portable communication systems, IEEE Transactions on Wireless Communications, vol.4, no.1, pp.57-64, 2005.
[4] Y. Jiang, C. Lin, X.Shen, and M. Shi, Mutual authentication and key exchange protocols for roaming services in wireless mobile networks, IEEE Transactions on Wireless Communications, vol.5, no. 9, pp.2569-2577, 2006.
[5] C. Tang and D. O. Wu, An efficient mobile authentication for wireless networks, IEEE Transactions on Wireless Communications, vol.7, no.4, pp.1408-1416, 2008.
[6] C. Tang and D. O. Wu, Mobile privacy in wireless networks revisited, IEEE Transactions on Wireless Communications, vol.7, no.3, pp.1035-1042.
[7] J. van der Merwe, D. Dawoud, S. Mcdonald, A survey on peer-to-peer key management for mobile ad hoc networks, ACM Computing Surveys, vol.39, no.1, pp.1-45, 2007.