Computer Communications 32 (2009) 611–618

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Enhanced authentication scheme with anonymity for roaming service in global mobility networks

Chin-Chen Chang [a,b,*], Chia-Yin Lee [b], Yen-Chang Chiu [b]

[a] Department of Information Engineering and Computer Science Feng Chia University, 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan
[b] Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 62145, Taiwan

ARTICLE INFO

Article history:
Received 19 March 2008
Received in revised form 17 November 2008
Accepted 17 November 2008
Available online 6 December 2008

Keywords:
Authentication
Roaming
Key agreement
The forgery attack
Energy consumption

ABSTRACT

User authentication is an important security mechanism for recognizing legal roaming users. In 2006, Lee, Hwang, and Liao proposed an enhanced authentication scheme with user anonymity for roaming environments. This article shows that Lee–Hwang–Liao's scheme cannot provide anonymity under the forgery attack. Moreover, the heavy computation cost may consume battery power expeditiously for mobile devices. Therefore, we propose a novel authentication scheme to overcome these weaknesses that is efficient, secure, and suitable for battery-powered mobile devices in global mobility networks.

© 2008 Elsevier B.V. All rights reserved.

1. Introduction

Rapid development of wireless networks brings about many security problems in mobile communication. A special network environment provides personal communication users with a global roaming service called the global mobility network (GLOMONET) [1]. Through universal roaming technology, mobile users can access the services provided by the home agent in a foreign network.

How to authenticate mobile users in GLOMONET is an important security issue. Many user authentication schemes [1–8] have been proposed in recent years for the roaming environment. In 2004, Zhu and Ma [5] proposed a new authentication scheme using smart cards; Lin and Lee [6] later produced a possible attack to Zhu–Ma's scheme. In 2005, Lee, Chang, and Lin [7] proposed an improvement to overcome the weakness in Zhu–Ma's scheme. Recently, Lee, Hwang, and Liao [8] also pointed out some security weaknesses in Zhu–Ma's scheme and put forth an improved edition.

In this article, we show that Lee–Hwang–Liao's scheme suffers from the forgery attack, which is defined by Lin et al. [6,7]. Under this kind of attack, the real identity of roaming users will be exposed. Besides, mobile devices are powered by a battery and the constrained energy results in limited computation capability. In other words, asymmetric and symmetric cryptosystems are required to achieve the security requirement, which increases the computation cost and energy consumption of Lee et al.'s scheme. To improve these disadvantages, we propose an efficient authentication scheme with anonymity that uses low-cost functions such as one-way hash functions and exclusive-OR operations to achieve security goals. Having these features, it is more suitable for battery-powered mobile devices.

The remainder of this paper is organized as follows. In Section 2, we review Lee–Hwang–Liao's scheme and discuss its weakness. An efficient user authentication scheme is proposed in Section 3. Security discussions are described in Section 4. In Section 5, we compare the proposed scheme with previous. Finally, we make some conclusions in Section 6.

2. A review of previous works

In this section, we first briefly describe Lee–Hwang–Liao's scheme and then point out its weakness. This scheme cannot protect user privacy against all possible threats. Moreover, the communication between the mobile user and the foreign agent is vulnerable.

2.1. Lee–Hwang–Liao's scheme

In 2006, Lee, Hwang and Liao showed that Zhu–Ma's scheme has some security weaknesses and proposed an improved scheme. Table 1 lists all of the notations used in Lee et al.'s scheme.

There are three phases in their scheme: the initialization phase, the first phase, and the second phase. Three entities are involved:

* Corresponding author. Address: Department of Information Engineering and Computer Science Feng Chia University, 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan. Tel.: +886 4 24517250x3790; fax: +886 4 27066495.
E-mail addresses: ccc@cs.ccu.edu.tw (C.-C. Chang), licy@cs.ccu.edu.tw (C.-Y. Lee), cyc94@cs.ccu.edu.tw (Y.-C. Chiu).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.11.032

Table 1
Some notations of Lee–Hwang–Liao's scheme.

Notations	Descriptions
MN	A mobile user
PW_{MN}	A password of MN
T_X	The timestamp generated by an entity X
HA	The home agent of a mobile user
FA	The foreign agent of a foreign network
ID_X	The identity of an entity X
$Cert_X$	The certificate of an entity X defined in X.509
$(M)_K$	Encryption of a message M using a symmetric key K
$E_K(M)$	Encryption of a message M using an asymmetric key K
$h(.)$	A one-way hash function
$\|\|$	A concatenation operator
$\oplus$	A XOR operator

MN is a mobile user; FA is the agent of the foreign network; and HA is the home agent of the mobile user MN. When MN roams in a new foreign network, FA must authenticate the identity of MN through MN's home agent HA. We will now describe Lee–Hwang–Liao's scheme in detail.

We will now describe Lee–Hwang–Liao's scheme in detail. In the initialization phase, a mobile user MN registers with the home agent HA and obtains a smart card through a secure channel for future service. In the first phase, the foreign agent FA authenticates the mobile user MN and issues a temporary certificate. Additionally, a session key is established between the foreign agent FA and the mobile user MN. In the second phase, the foreign agent FA serves for the mobile user MN when MN roams in the foreign network, and they can modify their session key simultaneously. Detailed processes are given in the following sections.

2.1.1. Initialization phase

First, a new mobile user MN submits his identity ID_{MN} to the home agent HA. Then, HA generates a password for MN by calculating $PW_{MN} = h(N||ID_{MN})$, where N is a long-term secret key of HA. Finally, HA delivers PW_{MN} and a smart card, which contains ID_{HA}, r and a one-way hash function $h(.)$, to MN through a secure channel. Note that $r = h(N||ID_{HA}) \oplus h(N||ID_{MN}) \oplus ID_{HA} \oplus ID_{MN}$, where ID_{HA} is the identity of HA. Fig. 1 illustrates the initialization phase.

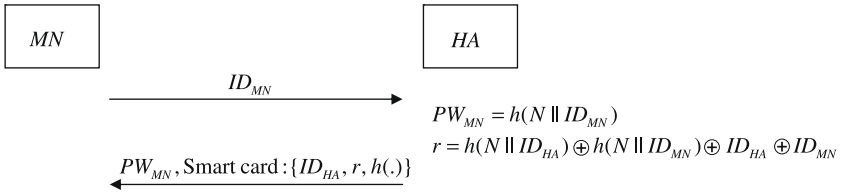

Fig. 1. Initialization phase of Lee–Hwang–Liao's scheme.

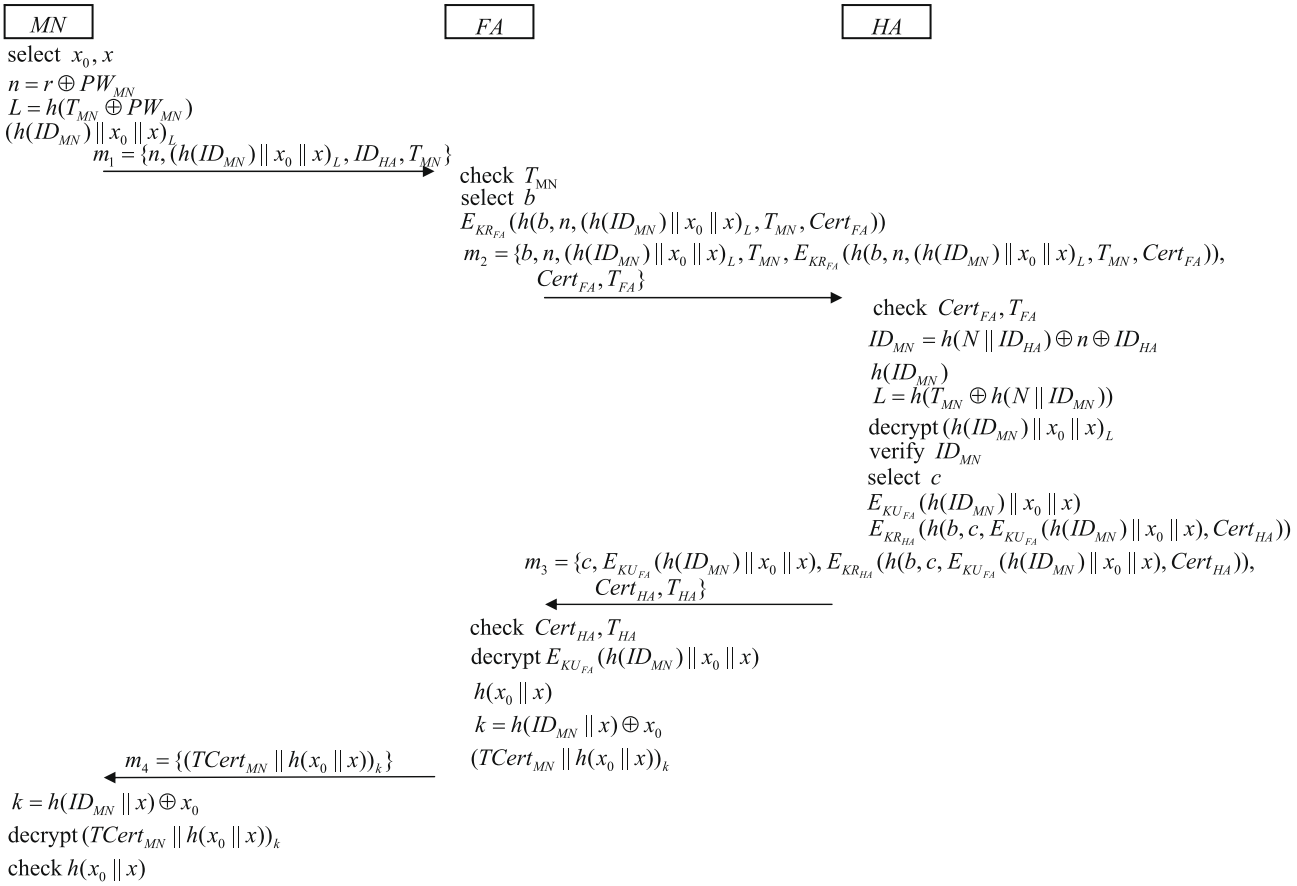

Fig. 2. First phase of Lee–Hwang–Liao's scheme.

Download English Version:

https://daneshyari.com/en/article/448411

Download Persian Version:

https://daneshyari.com/article/448411

Daneshyari.com