Journal of Network and Computer Applications 62 (2016) 1–8

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks

Prosanta Gope, Tzonelih Hwang*

Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan, R.O.C

ARTICLE INFO

Article history:
Received 27 February 2014
Received in revised form
6 October 2015
Accepted 16 December 2015
Available online 26 December 2015

Keywords:
Privacy
Anonymity
Authentication
Smart card
Global mobility networks

ABSTRACT

User authentication is an imperative mechani sm, especially for recognizing legal roaming users in global mobility networks (GLOMONET). Therefore, it is highly desirable to have a secure mutual authentication and key agreement (MAKA) scheme which can guarantee both the communication security as well as fairness. Here, by communication security, we mean protection against any unauthorized alteration of intercepted data flow. Whereas a fair key agreement protocol specifies that the agreed key contains some contribution from each participant, so that nobody has an unfair advantage in controlling the session key. In 2011, He et al. proposed an enhanced authentication and key agreement scheme with the user anonymity for roaming in GLOMONET environments. In this article, however, we reveal that the authentication and key agreement protocol presented by He et al. can assure neither communication security, nor any fairness in key agreement. Because of that, He et al.'s scheme suffers from certain weaknesses. Accordingly, He et al.'s scheme cannot achieve desired security. Therefore, here we propose a novel authentication mechanism to overcome these weaknesses. Performance analysis shows that our proposed scheme is secure and even more efficient as compared to He et al.'s scheme in GLOMONET.

1. Introduction

Global mobility networks (GLOMONET) provide effective global roaming services for personal communication users. Through the universal roaming technology, legitimate mobile user can enjoy ubiquitous services.

However, in the rapid development of such environment, many security problems such as user's privacy have predominantly brought to researchers' attention. In this regard, it is always desirable to have a secure mutual authentication and key agreement scheme between a legitimate mobile user and a service provider of the visited network in GLOMONET, which can avoid illegal access from malicious intruders.

For achieving the several security goals (including user's privacy), many authentication and key agreement schemes have been proposed with user anonymity for roaming services in global mobile networks (Zhu and Ma, 2004; Lee et al., 2006; Wu et al., 2008; Cheng et al., 2009; Youn et al., 2009; Tang and Wu, 2008; Lu and Zhou, 2010; He et al., 2011). Particularly, in 2004, Zhu et al. proposed a wireless security protocol based on smart card and featuring user anonymity (Zhu and Ma, 2004). Unfortunately, Lee and Hwang (Lee et al., 2006) pointed out in 2006 that Zhu and Ma's protocol's (Zhu and Ma, 2004) does not achieve mutual authentication and is also subjected to the forgery attack. Lee et al. also proposed a slightly modified version of Zhu et al.'s protocol so as to remedy the identified shortcomings. However, in (Wu et al., 2008), it was shown that the Zhu et al.'s scheme and Lee and et al.'s scheme fails to provide user anonymity, and Wu, Lee and Tsaur proposed an enhanced scheme by providing an effective remedy. Independently, in (Cheng et al., 2009), Chang et al. showed that Lee et al.'s scheme cannot provide user anonymity under the forgery attack and also proposed an enhanced authentication scheme. Unfortunately, Youn et al. found that the scheme of (Cheng et al., 2009) fails to achieve user anonymity under four attack strategies (Youn et al., 2009). In 2008, Tang et al. proposed an authentication protocol for mobile network (Tang and Wu, 2008), and they claimed that their scheme is immune to all known types of attacks. However, Lu and Zhou (2010) showed that Teng et al.'s scheme (Tang and Wu, 2008) suffers from replication attack. Hereafter, He et al. (2011) proposed a mutual authentication and

* Corresponding author.
E-mail addresses: prosanta.nitdgp@gmail.com (P. Gope), hwangtl@ismail.csie.ncku.edu.tw (T. Hwang).

http://dx.doi.org/10.1016/j.jnca.2015.12.003

key agreement scheme, based on the symmetric/asymmetric key encryption. However, in this article, we show that the scheme has some serious weaknesses which have been overlooked during design.

Now, apart from (Zhu and Ma, 2004; Lee et al., 2006; Wu et al., 2008; Cheng et al., 2009; Youn et al., 2009; Tang and Wu, 2008; Lu and Zhou, 2010; He et al., 2011), there are few more interesting roaming authentication protocols have been proposed (Mun et al., 2012; Kim and Kwak, 2012; Zhao et al., 2014; Jiang et al., 2013; Wen et al., 2013; Gope and Hwang, 2015). Particularly, Mun et al. (2012) proposed an anonymous authentication scheme for roaming services in GLOMONET). However, Kim and Kwak (2012) and independently Zhao et al. (2014) pointed out that Mun et al. cannot withstand replay attacks, man-in-the-middle attacks, and insider attacks. Recently, Jiang et al. (2013) proposed an anonymous user authentication scheme, but Wen et al. (2013) showed that the protocol is vulnerable to several attacks like spoofing attacks, and replay attacks etc. and in order to resolve these security issues they proposed an improved protocol. However, Gope and Hwang (2015) pointed that Wen et al.'s protocol is insecure against offline guessing attack, forgery attacks, etc. and simultaneously they proposed an enhanced protocol based on Quadratic Residue Problem and Chinese Reminder Theorem, which certainly cannot ensure lower computation overhead. Besides, in their protocol, to resist synchronization problem, a MS requires to perform multiple registrations, which may not be relevant for mobile communication.

Therefore, the contribution of this article is to reveal the weaknesses of the He et al.'s scheme, which have not been revealed yet. Besides, this article also demonstrates that the existing approaches for accomplishing anonymity property in mobile communication are impractical. Hence, we propose a novel mutual authentication and key agreement scheme based on symmetric key crypto-system, which can accomplish the aforesaid goals in a decent way and even can offer secure and expeditious roaming services in the GLOMONET environment with the reasonable computational, communication, and storage overhead.

The remainder of this article is organized as follows. Section 2 reviews the protocol of He et al. (2011) and whose weaknesses are pinpointed in Section 3. Thereafter, we present our proposed scheme in Section 4, whose security and performance are analyzed in Sections 5 and 6 respectively. Finally, a concluding remark is given in Section 7. The abbreviations and cryptographic functions used in this article are defined in Table 1.

Table 1
Notations and cryptographic functions.

Symbol	Definition
MU	Mobile user
FA	Foreign agent
HA	Home agent
ID_M	Identity of the mobile user
AID_M	One-time-alias identity of the MU
PID	Pseduo identity of MU
ID_h	Identity of the HA
ID_f	Identity of the FA
SK	Session key between FA and MU
K_{uh}	Shared key between MU and HA
K_{fh}	Secret key shared between the FA and HA
Tr_{seq}	Track sequence number (maintain both MU and HA)
$h(.)$	One-way hash function
$\oplus$	Exclusive-OR operation
$\|$	Concatenation operation

2. Review of He et al.'s scheme

In this section, we briefly describe He et al.'s scheme, which consists of four phases: the registration phase, mutual authentication and key agreement phase, password renewal phase, and the authentication phase when a mobile user located in his/her home network.

2.1. ***Phase I:*** *Registration phase*

When a mobile user (MU) desires to register at the home agent, the user needs to request to the home agent, and then the home agent will issue a smart card with related information to the user. In this regard, MS at first selects a password PSW_M, a random number d and computes $h(PSW_M \oplus d)$. Hereafter, MU submits his/her identity ID_M to the home agent (HA) through a secure channel. After receiving the request from MU, HA generates three random numbers N, x_{HA}, m and computes $TK_M = h(ID_M \| x_{HA})$, $SK_M = h(ID_M \| N)$, and $r = TK_M \oplus ID_{HA} \oplus (ID_M \| m)_N$. Finally, HA stores $\{TK_M, SK_M, h(.), r\}$ into a smart card, and sends it to the mobile user MU through a secure channel. After receiving the smart card, the MU calculates $SK_M^* = h(ID_M \| h(PSW_M) \oplus SK_M$ and replaces SK_M with SK_M^*.Subsequently, MU computes $V_M = TK_M \oplus h(ID_M \| h(PSW_M \oplus d))$, $H_M = h(TK_M)$ and replaces TK_M with $\{V_M, H_M\}$. Finally, the smart card contains $\{V_M, H_M, SK_M^*, h(.), d, r\}$.

2.2. ***Phase II:*** *Mutual authentication and key agreement phase*

Once enrolled by HA, when MU visits a foreign network managed by the FA, then he/she needs to authenticate himself/herself to FA. In this case, they take assistance of the HA, who issued the smart card to MU. The steps of this phase are outlined in Fig. 1. and explained as follows.

Step 1 $\mathbf{M_{A_1}}$: $\{n, E, ID_{HA}, T_M\}$.

MU inserts his/her smart card into the device and enters the identity ID_M and password PSW_M and then generates two random numbers x_0, x_1 and computes $SK_M = h(ID_M \| h(PSW_M) \oplus SK_M^*$, $L = h(T_M \oplus SK_M)$, $E = (h(ID_M) \| ID_{FA} \| x_0 \| x_1)_L$, $n = r \oplus TK_M = ID_{HA} \oplus (ID_M \| m)_N$, where T_M denotes the timestamp generated by MU. Finally, MU forms a login message $M_{A_1} = \{n, E, ID_{HA}, T_M\}$ and sends it to FA.

Step 2 $\mathbf{M_{A_2}}$: $\{b, n, E, T_M, E_{S_{FA}}(h(b, n, T_M, Cert_{FA})), Cert_{FA}, T_{FA}\}$.

After receiving the request message from MU, the FA checks the timestamp whether the message is valid or not. If so, the FA generates a random number b and computes its signature using the private key S_{FA}. Thereafter, FA sends a message $M_{A_2} = \{b, n, E, T_M, E_{S_{FA}}(h(b, n, T_M, Cert_{FA})), Cert_{FA}, T_{FA}\}$, to the mobile user's home agent (HA), where T_{FA} denotes the timestamp generated by the foreign agent FA.

Step 3 $\mathbf{M_{A_3}}$: $\{c, W, E_{S_{HA}}(h(b, c, W, Cert_{HA})), Cert_{HA}, T_{HA}\}$.

Upon receiving the message from the MU, HA at first checks that the timestamp T_{FA} and the certificate$Cert_{FA}$, whether they are valid or not. If they are invalid, HA immediately terminates the connection. Otherwise, HA computes $n \oplus ID_{HA} = (ID_M \| m)_N$and then decrypts $(ID_M \| m)_N$ and subsequently verifies whether the mobile user is legal or not. After the successful verification, HA computes $L = h(T_M \oplus h(N \| ID_M)$ and decrypts the E to obtain the random numbersx_0, andx_1. Thereafter, the HA computes $W = E_{P_{FA}}(h(h(N \| ID_M)) \| x_0 \| x_1)$,$E_{S_{HA}}(h(b, c, W, T_{HA}, Cert_{HA}))$,where c is