Journal of Information Security and Applications 38 (2018) 96–110

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

A secure and lightweight authentication scheme for roaming service in global mobile networks

R. Madhusudhan*, Shashidhara

Department of Mathematical and Computational Science, National Institute of Technology Karnataka, Surathkal 575025, India

ARTICLE INFO

Article history:

Keywords:
Global roaming
Mobility networks
User anonymity
Clock synchronization
Stolen-verifier attack

ABSTRACT

Global Mobile Network provides global roaming service to the users moving from one network to another. It is essential to authenticate and protect the privacy of roaming users. Recently, Marimuthu and Saravanan proposed a secure authentication scheme for roaming service in mobile networks. This scheme can protect user anonymity, untraceability, and is believed to have many abilities to resist a range of attacks in global mobile networks. In this paper, we analyse the security strength of their scheme and show that the authentication protocol is in fact insecure against insider attack, stolen-verifier attack, impersonation attack, denial-of-service attack, synchronization problem, lack of user anonymity and operational inefficiencies. Hence, we propose a secure and lightweight authentication scheme for Global Mobile Networks. In addition, the proposed scheme requires few message exchanges between the entities such as MU (Mobile User), FA (Foreign Agent) and HA (Home Agent). The scheme ensures both communication and computation efficiency as compared to the well-known authentication schemes. The performance analysis shows that the proposed authentication scheme is well suited for resource limited wireless and mobile environments.

1. Introduction

With the rapid development of mobile technologies, such as GSM (Global System for Mobile communications), GPRS (General Packet Radio Service), EDGE (Enhanced Data Rates for Global Evolution), UMTS (Universal Mobile Telecommunication Service) and HSPA (High Speed Packet Access), over the last couple of years, most of the electronic transactions are processed through mobile devices. A mobility network provides roaming service that permits mobile subscriber to access the services provided by the home agent in a foreign network [1,2]. To provide global roaming service for a mobile user, remote user authentication is an essential requirement and challenging task. A scenario of remote user authentication in global mobile network involves a Mobile User (MU), Foreign Agent (FA) and the Home Agent (HA) is shown in Fig. 1. A MU of a specific network can roam anywhere in the world and he/she can access the desired services through a foreign agent [3].

When a MU roams into a foreign network, the FA authenticates the roaming user (MU) with the assistance of home agent [3]. During roaming process in global mobile networks, privacy protection is challenging and essential requirement. The identity of mobile users should be protected, which is known as user anonymity and his/her location activities should be kept secret, which is known as user untraceability [4]. Mutual authentication is a very important security aspect. It requires that the MU, FA and HA prove their identities to each other before offering any application services between these entities. In order to achieve all security requirements, several authentication schemes [1–12] have been proposed for roaming services in global mobility networks. However, some of them have been proved to be insecure against known attacks.

1.1. Motivations and contributions

We studied many user authentication schemes in global mobile networks that provide roaming service for mobile users. It has been observed that the previous authentication schemes have the following problems: Most of them (1) are vulnerable to some known cryptographic attacks. (2) Make use of tamper-resistant devices such as smartcards, which does not ensure that an authentication protocol is safe and secure against all security risks. Because, the information stored in the smartcard can be extracted easily, either by analysing the leaked information or by monitoring its power consumption [13]. In addition, the smartcard based infrastructure required card reader terminals, which greatly increases the deployment cost. (3) Suffers from clock synchronization problem. (4) Uses static key agreement method to distribute secret

* Corresponding author.
E-mail address: madhurk96@gmail.com (R. Madhusudhan).

https://doi.org/10.1016/j.jisa.2017.12.002
2214-2126/© 2017 Elsevier Ltd. All rights reserved.

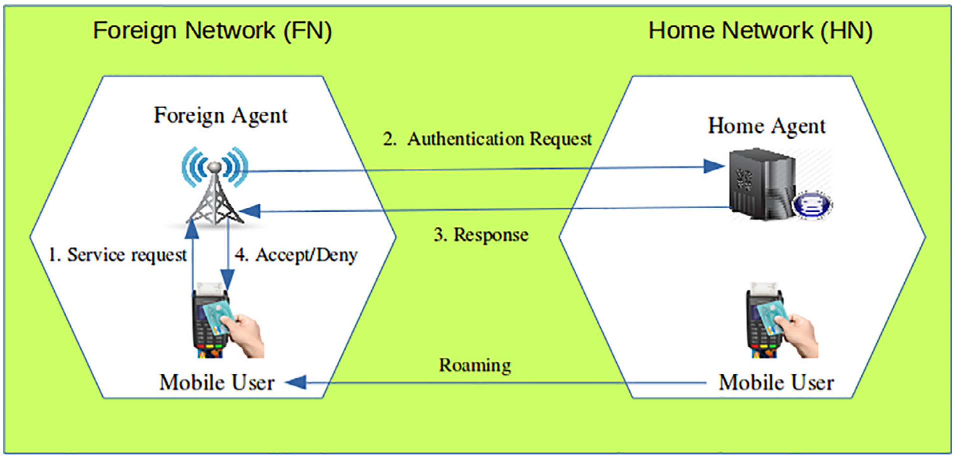

Fig. 1. Mobile user authentication for roaming service.

parameters between different entities. (5) Some of the existing authentication protocols do not have the secure password change and local password verification mechanisms. (6) Do not satisfy all the security requirements specified in Section 6.1.

Recently, Marimuthu and Saravanan [2] proposed a secure authentication scheme for roaming service. This scheme can protect user anonymity, untraceability and is believed to have many abilities to resist a range of attacks in global mobile networks. However, this paper presents a brief review of Marimuthu and Saravanan scheme and we identify that their scheme has some security pitfalls. Compared with previous related authentication schemes, the proposed scheme has many advantages. Firstly, the scheme enjoys important security attributes including prevention of various attacks. The scheme ensures user anonymity, local password verification, user friendliness, no password-verifier in HA to maintain secret key and so on. Secondly, the scheme makes use of common memory devices such as USB (Universal Serial Bus) sticks, PDAs (Digital Assistant) and mobile phones without a tamper resistant property to store authentication information issued by the home agent. Finally, the performance and cost analysis of the scheme shows that there are only few encryption and decryption primitives. Also, the proposed scheme does not require additional clock synchronization mechanisms. Therefore, the proposed scheme is simple, secure, lightweight and more suitable for wireless and mobile environments.

1.2. Organization of the paper

The rest of the paper is organized as follows: Section 2, covers related work. Section 3, provides some mathematical preliminaries such as Diffie–Hellman problem, discrete logarithm problem and one-way hash function. These preliminaries form basis of the proposed security model and useful for a security analysis. Section 4, reviews Marimuthu and Saravanan's scheme. Section 5, shows security weaknesses in this scheme and points out its computational inefficiencies. Section 6, proposes a Secure and Lightweight Authentication Scheme and corresponding scheme analysis are presented in Section 7. The performance analysis and security requirement comparisons are presented in Section 8. Section 9, concludes the paper.

2. Related work

To support the roaming facility, in 2004, Zhu et al. [14] established an efficient two-factor authentication scheme. However, Lee et al. [8] showed that Zhu et al.s. scheme does not achieve mutual authentication and is vulnerable to impersonation attack. In 2006, the authors also proposed an improved scheme, to overcome the weakness of Zhu et al.'s authentication scheme. In 2008, Wu et al. [15] proved that the proposed scheme of Lee et al.s still fails to provide strong user anonymity and perfect backward secrecy. Wang et al. [16] also introduced the new authentication scheme, later, Jeon et al. [17] pointed out that Wang et al.s. authentication scheme cannot withstand against forgery attacks and fails to achieve anonymity. Independently, Chang et al. [9] proved Lee et al.s. authentication scheme fails to achieve user anonymity. Then, Chang et al. proposed a new authentication scheme. Unfortunately, Youn et al. [10] found that, their scheme cannot provide anonymity. In 2010, He et al.s. [12] pointed that Wu et al.'s authentication scheme is vulnerable to forgery and replay attacks. Then, they come up with a robust authentication mechanism for mobile and wireless communications.

After, in 2011, Li et al.'s [11] also points that, Wu et al.'s protocol is unlikely to provide anonymity due to an inherent design weakness and also cannot withstand against impersonation attack and replay attack. Then they proposed an enhanced authentication scheme using smartcards, which provides both computation and communication efficiency as compared to some well known authentication schemes. Recently, Mun et al. [18] reanalysed Wu et al.'s [15] authentication scheme, they pointed that Wu et al.'s authentication scheme fails to provide forward secrecy and reveals the legitimate mobile users password. Then they come up with an enhanced scheme for roaming service, which has several advantages: (1) It can provide several security properties such as providing perfect forward secrecy and preventing disclosure of users password. (2) It is more efficient regarding performance compared with some previous known schemes that use public key cryptosystem with certificates. (3) It does not use timestamps, thus it is not required to synchronize the time. Zhao et al. [7] in 2014, proved that Mun et al.'s [18] authentication scheme does not provide mutual authentication, local password verification and user friendliness. Also, the scheme cannot withstand against forgery attacks. Further, they designed an enhanced user authentication scheme. Later on, some new remote user authentication schemes have been proposed [7,19–21].

Recently, in 2015, Marimuthu and Saravanan's [2] proposed a secure authentication scheme with user anonymity for roaming service in global mobility networks. This scheme can protect user anonymity, untraceability, and is believed to have many abilities to resist a range of attacks in global mobile networks. However, this paper presents a brief review of Marimuthu and Saravanan's scheme [2] and we identify that their scheme has some security