A Secure and Robust Three-Factor Based Authentication Scheme Using RSA Cryptosystem

Rifaqat Ali, Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, India
Arup Kumar Pal, Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, India

ABSTRACT

In remote user authentication, a server confirms the authenticity of a user via unreliable channel. Several authentication protocols are devised in the literature relied on the identity, password and biometric of a user. But, most of the authentication protocols are either computationally expensive or not-secure from several kinds of malicious threats. In this document, the authors have suggested a secure and robust three-factor (such as password, smartcard and biometric) based authentication scheme by using RSA cryptosystem. The proposed protocol is validated through BAN logic. Then, formal security analysis using random oracle model shows that the identity, password, biometric and session key are highly secure from an adversary. Besides, the informal security analysis of our protocol proves that it withstands to several kinds of malicious attacks. In addition, performance comparison of presented scheme with respect to other schemes is comparatively suitable in the context of communication and computation costs.

KEYWORDS

Authentication, BAN Logic, Random Oracle Model, RSA, Security Analysis

1. INTRODUCTION

By the speedy growth of Internet technology, several Internet based applications such on-line shopping, Internet banking, e-learning, e-health are widely used and popular among computer users. But, Internet inherently is not able to provide any kinds of security to prevent several malicious attacks during accessing these on-line services. In most of these on-line applications, authentication is one of the essential security methods to verify the legality of the remote client to prevent forgery. The traditional authentication scheme (Lamport, 1981) was designed based on password and identity of a user. This kind of authentication scheme is also known as two factor authentication scheme. The deficiency of such kind of authentication scheme is that the authentication information is possible to forge by an attacker. To remedy this weakness, several authors have devised biometric based authentication schemes (Hwang et al., 1990), those are much more efficient and secure than traditional authentication schemes.

Lamport (1981) firstly projected the password based authentication scheme. In this scheme, the verification table is stored at the server end. As a result, the scheme will not work when any kind of alteration will take place on verification table by an attacker. Hwang et al. (1990) also suggested a password based authentication scheme without keeping the verification table at the server end.
But, in their scheme, password change is not an easy process. Later, Hwang and Li (2000) proposed two-factor based authentication protocol using ElGamal public key cryptosystem. But, the user was restricted to change the password in their scheme. Some other authors (Fan et al., 2005; Lee et al., 2005; Tsai, 2008) have also devised some smartcard based remote user authentication schemes to obviate the earlier issues at some certain level of extent. Khan et al. (2013) suggested a smart-card based authentication scheme for accessing healthcare services in secure way. Xie et al. (2013) designed a secure anonymous preserving authentication scheme to remove their vulnerability even if an attacker knows all confidential parameters kept in the smart-card. Dictionary attack is possible on these traditional remote user authentication schemes. Another, major issue is to protect the security even if the password and smart card are stolen or misplaced. Chen et al. (2014) presented authentication protocol which is capable to resist the smart card stolen or misplacement attack. However, biometric based authentication schemes are more robust in the context of authentication because only authorized users are allowed to access the system.

Generally, remote user authentication using biometrics is essentially high safe and trustworthy than the traditional authentication scheme because biometric keys such as face, iris and finger print cannot be stolen or forgotten, difficult to copy or share. Several biometric using remote user authentication protocols are designed (Ku et al., 2005; Das, 2011; Li and Hwang, 2010; Khan and Zhang, 2007). These algorithms were developed in various cryptographic environments like RSA cryptosystem (Das and Bruhadeshwar, 2013; Giri et al., 2015), ElGamal cryptosystem and ECC (Zhang et al., 2014). RSA is one of the famous public-key cryptosystem and broadly used in various applications in field of security. So, in this paper, our objective is to design a three key factor based authentication scheme in RSA environment which is maintaining high security along with comparatively less communication and computation overheads.

After this introduction, the rest of manuscript is arranged as follows: The proposed scheme is described in Section 2. The security using BAN logic is explained in Section 3 and the formal security analysis by the help of random oracle model is done in Section 4. And then the informal security analysis is presented in Section 5. The performance comparison is demonstrated in Section 6 and finally the conclusion and future scope is explained in Section 7.

2. PROPOSED SCHEME

This section clarifies the proposed work of five phases namely initialization; registration; login; authentication and key agreement; and password change. The description of all phases is elaborated in the following forthcoming subsections.

2.1. Initialization Phase

To initialize the system or organization, the server S uses RSA algorithm (Chandrakar et al., 2015) for generating the public key (e, n) and private key (d).

2.2. Registration Phase

When the user $U_i$ wants to registration or re-registration to the server S then following steps are performed.

1. Firstly, the user $U_i$ touches own biometric $B_i$ at the device and also chooses identity $ID_i$, password $PW_i$, and random number r. Then, $U_i$ evaluates $pwb_{i} = h \left( PW_i \parallel r \right)$, $F_i = H \left( B_i \right)$,
Compact and Efficient Reconfigurable Antennas for Flexible Radio Front-End in Cognitive Radio Systems
www.igi-global.com/chapter/compact-and-efficient-reconfigurable-antennas-for-flexible-radio-front-end-in-cognitive-radio-systems/123582?camid=4v1a

Renewable Energy Sources for Power Supply of Base Station Sites
www.igi-global.com/article/renewable-energy-sources-for-power-supply-of-base-station-sites/95723?camid=4v1a