JOURNAL OF INFORMATION SECURITY AND APPLICATIONS 32 (2017) 15–26

Available online at www.sciencedirect.com

ScienceDirect

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

A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme

Ankita Chaturvedi [a], *Dheerendra Mishra* [b,*], *Srinivas Jangirala* [a], *Sourav Mukhopadhyay* [a]

[a] *Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India*
[b] *Department of Mathematics, LNM Institute of Information Technology, Jaipur 302 031, India*

ARTICLE INFO

Article history:
Available online 9 December 2016

Keywords:
Internet of Things
Authentication
Key agreement
Smart card
Biometric
Privacy

ABSTRACT

Advancement in Internet of Things (IOT) and remote user communication is facilitated, where a user need not be physically present. However, security and privacy challenges arrive as client–server communication is done via public network. To lower down the security and privacy threats, authentication and key agreement (AKA) protocols are being designed and analyzed. AKA protocols' goal is to ensure authorized and secure access of recourses. Recently, Li et al. proposed a biometric based three-factor remote user authentication scheme for client–server environment. Their scheme uses biometric identifier to resist guessing attacks. In this article, we discussed the security of Li et al.'s scheme, and show its vulnerability to known session specific temporary information attack. Additionally, it does not provide three-factor authentication and user's privacy. It also has some flows in authentication phase. We proposed a novel AKA protocol, which can overcome the weaknesses of Li et al.'s scheme without losing its original merits. Through the analysis, we show that our scheme is secure against various known attacks including the attacks found in Li et al.'s scheme. Furthermore, we demonstrate the validity of the proposed scheme using the BAN (Burrows, Abadi, and Needham) logic. Our scheme is also comparable in terms of computation overheads with Li et al.'s scheme and other related schemes.

1. Introduction

Rapid developments in the field of computer networks and communications have led to increase in the number of applications based on the Internet of Things (IOT) such as e-commerce, e-medicine, e-learning and so forth. In these applications, a user does not physically present at service center, however, he can access the remote server at anytime and from anywhere. A user interacts with the server via public channel, where an adversary may have full control over the public channel. This increases the user's privacy and data security threat. Thus, these applications need to be secure, and hence utilize security protocols. Security protocols determine the rules for communication, to achieve security objectives like authentication, confidentiality, integrity and privacy. Earlier methods of

* Corresponding author. Department of Mathematics, LNM Institute of Information Technology, Jaipur 302 031, India. Fax: +91-141-2689014.
E-mail address: dheerendra.mishra@lnmiit.ac.in (D. Mishra).
http://dx.doi.org/10.1016/j.jisa.2016.11.002
2214-2126/

ascertaining whether a protocol achieves its security objectives were by trial and error. The difficulty in detecting the flaws in security protocols by the above method is exemplified by the Needham–Schroeder public key based authentication protocol (Needham and Schroeder, 1978). In recent years, many smart card based remote user authentication schemes have been designed to achieve security and privacy goals (Amin and Biswas, 2015; Eldefrawy et al., 2010; He et al., 2013; Islam et al., 2015; Khan and Kumari, 2014). The advancement in computing power is also enabling the adversary to perform active or passive attacks on smart card based authentication schemes. Instead of adversary threat, a remote user authentication scheme should meet the following requirements: (i) Resistant to active and passive attacks; (ii) Protect user anonymity; (iii) Present efficient login phase; (iv) Present user-friendly and efficient password change phase; (iv) Support mutually authentication and session key agreement.

One of the functions performed by authentication protocols is to verify the correctness of each other and commutate the secret session key among participants. To enhance the security of designs, many password based authentication schemes using smart card have been designed and analyzed (Byung-Gi and Hong, 2005; Chen et al., 2013; Farash, 2014; He, 2012; Hsieh and Leu, 2014; Lee and Chiu, 2005; Lee et al., 2005; Li et al., 2013; Park, 2012; Song, 2010) which are widely employed because of their efficiency and applicability. In 2009, Xu et al. (Xu et al., 2009) presented a password based authentication scheme using smart card to overcome the weaknesses of Lee and Chiu (2005) and Lee et al. (2005). Xu et al. also claimed that their proposed scheme satisfies all desirable security attributes. In 2010, Sood et al (Sood et al., 2010) demonstrated that Xu et al.'s scheme is vulnerable to off-line password guessing and forgery attacks. They also presented an improvement of Xu et al.'s scheme. In the same year, Song (2010) also demonstrated that an adversary can extract the parameters from the legitimate user's smart card and perform user's impersonation attack. Furthermore, he presented an improvement of Xu et al.'s scheme. In 2012, Chen et al. (Chen et al., 2014) pointed out that the presented improvements by Song and Sood et al. are not secure. Chen et al. (2014) pointed out that Sood et al.'s scheme supports one way authentication, but not mutual authentication where only server verifies the user's authenticity. In addition, they identified the inefficiency of Sood et al.'s scheme to detect incorrect input. Chen et al. also demonstrated the off-line password guessing attack on Song's scheme. They also proposed an efficient scheme. Recently, Li et al. (2013) analyzed Chen et al.'s scheme and showed that Chen et al.'s scheme fails to maintain efficient login and user-friendly password change phase. Li et al. (2013) also presented a password based authentication scheme using smart card to overcome the weaknesses of existing schemes. Unfortunately, Li et al.'s scheme does not resist off-line password guessing attack and insider attack (Kumari and Khan, 2014). Moreover, Li et al. (2015) discussed the failure of Chang et al.'s scheme (Chang et al., 2014) to satisfy security attributes. Ramasamy and Muniyandi (2009) also came up with a novel smart card based authentication scheme. Later, Karuppiah and Saravanan (2015) identified that Ramasamy and Muniyandi's scheme is vulnerable to off-line password guessing and impersonation attacks. Additionally, they proposed an improved authentication scheme. Their scheme can resist impersonation attack and off-line password guessing attack, but does not provide anonymity.

Most of the existing password based authentication schemes are unable to resist guessing attacks or have unfriendly or inefficient password change phase. Moreover, the password cannot be considered a unique identifier of a user. On the contrary, biometric keys (irises, fingerprints, hand geometry and palm-prints, etc.) are considered to be a unique identifier of a user. The adoption of biometric keys in authentication schemes also enhances the security against guessing attacks (Khan, 2009). The advantages of biometric keys can be summarized as follows: (i) Biometric keys cannot be lost or forgotten; (ii) Biometric keys are extremely difficult to forge or distribute; (iii) Biometric keys maintain uniqueness property; (iv) Biometric keys are hard to guess. It is clear that biometric-based remote user authentications are more secure and reliable rather than traditional password-based remote user authentication. Adoption of biometric keys may also provide three-factor authentication while password based authentication schemes can only achieve two factor authentication. Thus, the biometric-based remote user authentication schemes with password have attracted significant research attention. Recently, many biometric based authentication schemes have been proposed (An, 2012a; Das, 2011; Go et al., 2014; Jaspher et al., 2012; Lee et al., 2011; Li and Hwang, 2010; Li et al., 2011, 2014; Truong et al., 2012; Wang and Ma, 2012; Yoon and Yoo, 2013).

In 2010, Li and Hwang presented a biometric based remote user authentication scheme (Li and Hwang, 2010) in which user biometric identification is used to verify the correctness of user. In 2011, Das (Das, 2011) pointed out the security flaws in login and password change phase of Li and Hwang's scheme. Das also proposed an efficient biometric based authentication scheme to erase the pitfalls of Li and Hwang's scheme. His scheme presents efficient login and password change phases where incorrect input can be quickly detected. Li et al. (2011) also demonstrated that Li and Hwang's scheme does not resist man-in-the middle attack. Moreover, they presented an improved authentication scheme using smart card and biometrics along with password which is proven to be insecure to resist off-line password guessing attack, forgery attack, and insider attack by An (2012b). Recently, Li et al. (2014) showed that Das's scheme is vulnerable to forgery and stolen smart card attack. Additionally, they presented an improved scheme to overcome the weaknesses of Das's scheme. Unfortunately, their scheme is vulnerable to replay attack and known session specific temporary information attack. In 2014, Karuppiah and Saravanan (Karuppiah and Saravanan, 2014) proposed dynamic ID based authentication scheme. Their scheme ensures unlinkability, but it is vulnerable to off-line password guessing attack. Moreover, these biometric based authentication schemes (An, 2012b; Das, 2011; Karuppiah and Saravanan, 2015; Li and Hwang, 2010; Li et al., 2011, 2014) do not protect user privacy.

1.1. *Our contribution*

The contribution of the paper is twofold. First, we point out the security flaws in Li et al.'s user authentication scheme,