Journal of Network and Computer Applications 34 (2011) 73–79

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards

Xiong Li [a,*], Jian-Wei Niu [b,**], Jian Ma [a], Wen-Dong Wang [a], Cheng-Lian Liu [c]

[a] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] State Key Laboratory of Software Development Environment, Beihang University, Beijing 100191, China
[c] Department of Mathematics and Computer Science, Fuqing Branch of Fujian Normal University, Fuqing 350300, China

ARTICLE INFO

Article history:
Received 4 May 2010
Received in revised form
19 August 2010
Accepted 5 September 2010

Keywords:
Cryptanalysis
Biometrics
Authentication
Smart card
Security

ABSTRACT

Recently, Li and Hwang proposed a biometrics-based remote user authentication scheme using smart cards [Journal of Network and Computer Applications 33 (2010) 1–5]. The scheme is based on biometrics verification, smart card and one-way hash function, and it uses the nonce rather than a synchronized clock, so it is very efficient in computational cost. Unfortunately, the scheme has some security weaknesses, that is to say Li and Hwang's scheme does not provide proper authentication and it cannot resist the man-in-the-middle attacks. If an attacker controls the insecure channel, she/he can easily fabricate messages to pass the user's or server's authentication. Besides, the malicious attacker can impersonate the user to cheat the server and can impersonate the server to cheat the user without knowing any secret information. This paper proposes an improved biometrics-based remote user authentication scheme that removes the aforementioned weaknesses and supports session key agreement.

1. Introduction

Network identity authentication is an important mechanism in network security that provides the conformation of two communication parties' identity under the public environment. Lamport (1981) first proposed a remote password authentication scheme for the insecure communication. However, in their scheme, the server must store a password list and cannot resist interpolation attacks. Since then there have been other enhanced password authentication schemes (Chang and Wu, 1991; Haller, 1994; Wang and Chang, 1996), which made certain improvement over Lamport's scheme. In 2000, Hwang and Li (2000) proposed a remote user authentication scheme using smart cards based on ElGamal's (1985) public key cryptosystem. But there exist some security flaws in Hwang et al.'s scheme (Chan and Cheng, 2000; Chang and Hwang, 2003; Yeh et al., 2004). Until now, there have been many proposed remote user authentication schemes based on smart cards (Lee et al., 2005; Liu et al., 2008; Shen et al., 2003; Sun, 2000; Wu and Chieu, 2003). In generally, a secure and efficient remote user authentication scheme should meet the following conditions (Fan et al., 2005; Liao and Wang, 2009; Lin et al., 2003):

- Compatibility with a multi-server network architecture without repetitive registration.
- Low computational workload of the smart card.
- No need of password table or verification table.
- Resistance to different kinds of attacks.
- Allow the user to choose her/his ID, password and update her/his password freely.
- Allow the users and servers to authenticate each other and then negotiate a session key to security communication.
- No requirement on time synchronization and delay-time limitation.

Traditional methods of the user authentication usually depend on IDs and passwords that can be forgotten, disclosed, lost or stolen. In addition, traditional authentication systems cannot discriminate an impostor who fraudulently obtains the access privileges (e.g., IDs, Passwords) from the genuine users. For example, if a user's ID and password are shared with a colleague there is no way for the system to tell who the actual user is. In such distributed system environments, the traditional authentication protocol based on a combination of user ID and password has become inadequate (Ratha et al., 2001). On the contrary, the distinguishing feature of biometrics, such as fingerprints, faces and irises, provides the opportunity for a more reliable and automated method of identity verification based on measurable physiological or behavioral characteristics. These biometric characteristics are usually universal, unique and cannot be duplicated, lost or forgotten.

In a generic biometric authentication system, feature information is extracted from the scanned biometric data and compared with the pre-stored template. The similarity between the inputted

* Corresponding author. Tel.: +86 15010249305.
** Corresponding author. Tel.: +8610 82317601.
E-mail addresses: lixiongzhq@163.com (X. Li), niujianwei@buaa.edu.cn (J.-W. Niu).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.09.003