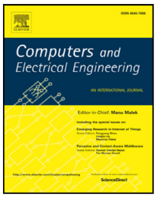
Computers and Electrical Engineering 000 (2017) 1–17

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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



An analytical study of biometric based remote user authentication schemes using smart cards[☆]

Trupil Limbasiya[a,*], Nishant Doshi[b]

[a] NIIT University, Neemrana, Rajasthan, India
[b] Pandit Deendayal Petroleum University, Gandhinagar, Gujarat, India

ARTICLE INFO

Article history:
Received 30 January 2016
Revised 27 January 2017
Accepted 27 January 2017
Available online xxx

Keywords:
Attack
Biometric
Remote user
Security
Session key
Smart card

ABSTRACT

In this digital era, any two entities can exchange messages, irrespective of their physical distance, via an authentication scheme on the Internet. A biometric identity is one of the unique parameters of each human being. A smart card stores such parameters based on the characteristics of an entity. Although a smart card cannot be tamper resistant, specific attacks have been identified by researchers in the context of remote user authentication schemes. Thus, motivated, we have conducted in this paper a state-of-art survey, the first of its type, on remote user authentication schemes from their inception. We have summarized and discussed distinct attacks that are likely to occur on a remote user authentication scheme and how such an attack makes a system vulnerable. Our aim is not only to document the history of findings on remote user authentication schemes but also to familiarize researchers with the list of attacks that have been identified to date.

1. Introduction

In a remote user authentication system, the remote user can access software or hardware components from different locations. A remote user authentication system is divided into two major modules, viz., verification and identification. In the verification phase, a system processes a one-to-one validation of the captured user information against a stored database. In a similar fashion, a system processes one to many validations of the captured user information with the stored database in the identification phase. There are sundry schemes for providing security in a remote user authentication scheme based on various authentication approaches. To date, many researchers have proposed various schemes based on biometric features for authentication by using a smart card. Most of these schemes are not fully secured from all attacks.

Remote user authentication schemes are helpful to provide authenticity to either a user or a server. Many scientists have proposed different types of authentication schemes based on requirements. A password-only-based authorization system is known as one-factor authentication. A password and smart card-based authorization scheme is called two-factor authentication. However, in this paper, we primarily discuss a three-factor authentication system in which three different factors are available, viz., a text password, a smart card, and a biometric identity. Remote user authentication system is employed at most of the places in today's life of networking. Automated Teller Machines (ATMs), Telecare Medicine Information Systems (TMIS), and Wireless Sensor Networks (WSNs) are examples of such applications.

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. A. Parakh.

[*] Corresponding author.
E-mail address: limbasiyatrupil@gmail.com (T. Limbasiya).

http://dx.doi.org/10.1016/j.compeleceng.2017.01.026
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

Please cite this article as: T. Limbasiya, N. Doshi, An analytical study of biometric based remote user authentication schemes using smart cards, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.01.026

There are various attacks on remote user authentication schemes such as dictionary, man-in-the-middle, plaintext, smart card lost, modification, denial of service (DOS), session key disclosure, impersonation, and insider. These attacks can be troublesome for a legitimate user when accessing a system for a specific purpose. A dictionary attack tries to guess common passwords based on the dictionary. A man-in-the-middle attack is implemented to recognize information. A plaintext attack is utilized when the cipher text is stolen. A smart card lost attack is introduced when a smart card is lost and then an attacker can apply procedures to acquire the information. A modification attack is implanted to modify information; in other words, the attacker modifies information and then retransmits the data again. These attacks can interrupt security or communication services [2,15,24,25,30].

1.1. Guidelines for biometric-based schemes

In the last decade, the use of the Internet and information technology has swiftly expanded. We frequently store most of the information in soft-copy form, which is a convenience and a problem at the same time. We must afford sufficient level of security to the saved data; otherwise, attackers have knowledge concerning several techniques to extract confidential information quickly. Consequently, we should implement a strong authentication scheme before making any type of transaction to protect users/servers with respect to information security. A biometric authentication scheme is an automated process predicated on behavioral or physiological characteristics. The word “biometric” is derived from the two Greek words ‘*bios*’ and ‘*metric*’. *Bios* indicates life, and *metric* denotes measurement. There are biometric identities such as hand geometry, palm print, fingerprint, signature verification, facial recognition, voice recognition, ear recognition, retinal scan and so on. A biometric identity has various merits such as has unique security, has permanency, cannot be misplaced or forgotten, is quite tough to generate an exact replica, is hard to distribute exceptionally, cannot be predicted effortlessly, and is not easy to break compared with others. At the same time, a biometric identity has different demerits; for example, it does not provide 100% perfect matching, it is not modifiable, and it fails if body component(s) are lost. Due to its pluses, the biometric-based schemes are finding vital roles in many applications such as attendance systems, unique identity cards, crime detection, visas & passports, and digital locking techniques. A biometric identification is helpful to manage credible security at highly secured places such as military systems, database security, government sectors, private sectors, education institutions, medical systems, legal agreements and so on [26–35]. In such cases, it is infeasible to achieve 100% security, but we can try to ensure security as much as possible. Usage of biometric identifications will increase in forthcoming systems because we access increasing numbers of facilities through a network. Several countries have started using biometric identifications in different applications, for example, national identity cards, passports, border security, airport security, and payment systems.

Paper Organization: In Section 2, we present a brief survey concerning various remote user authentication schemes proposed by different researchers to address related attack vulnerabilities. In Section 3, we describe possible attacks against the remote user authentication schemes. Finally, we conclude our paper in Section 4. References are at the end. Thereafter, Appendix A includes referenced figures.

2. Literature survey

Leslie Lamport introduced a remote user authentication scheme for the first time in 1981 [1]. In 1995, Wu proposed that two attacks are possible against Lamport’s scheme, viz., a reply attack and an impersonation attack. Hwang et al. introduced cryptanalysis concerning a replay attack, an impersonation attack and a masquerade attack into Wu’s scheme in 1999. In 2000, Hwang et al. suggested a new scheme. In 2003, Lin et al. proposed that the scheme of Hwang et al. is vulnerable and susceptible to a replay attack, a modification attack, and an impersonation attack [2]. In 2000, Sun found Attack-1 issue in the scheme of Hwang et al. A password key length was too long causing users to have more difficulty in memorizing the password key [3]. In 2003, Shen et al. introduced the masquerade attack against the scheme of Hwang et al. [4].

In 2004, Juang proposed Attack-2 against the scheme of Lin et al. [2], in which a session key agreement and the time synchronization are issues. But, Lee et al. proposed Attack-5 against Juang’s scheme, in which a verification table is stored on the verifier side. Secret keys of the users are stored in the verification table. Thus, there is an issue related to the verification table. In 2011, Chang et al. proposed that the scheme of Lee et al. was insecure against a forgery attack [7]. Liao et al. [5] thereafter advanced their own system as, stating that their proposed model was secure against different attacks (e.g., server spoofing, insider, replay, stolen verifier) in 2007 and then comparing it with different schemes (Lin et al. and Juang). Two years later, Hsiang et al. determined in 2009 that scheme [5] cannot resist an insider attack, a masquerade attack or a server spoofing attack [6].

In 2003, Wu et al. proposed Attack-3 against Sun’s scheme [3], in which a password is generated by the system automatically. The users do not have rights to change the password. Thus, there are issues related to the password change phase [8]. In 2002, Chien et al. proposed Attack-4 against Sun’s scheme [3], in which a mutual authentication issue existed, suggesting that problems arise in communication in both user and server side authentication [9]. In 2005, Lee et al. proposed that the scheme of Wu et al. [8] is vulnerable to a forgery attack. In 2005, Lee at el. proposed via another scheme that the scheme of Chien et al. [9] is insecure against a parallel session attack. In 2009, Xu et al. proposed that the scheme of Lee et al. is insecure against a forgery attack and that the scheme of Lee et al. is additionally insecure against a password guessing attack [10]. In 2010, R. Song proposed that the scheme of Xu et al. [10] was vulnerable and susceptible to an internal attack and to an impersonation attack [11].

Please cite this article as: T. Limbasiya, N. Doshi, An analytical study of biometric based remote user authentication schemes using smart cards, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.01.026