Computers and Electrical Engineering 000 (2018) 1–14

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Advanced formal authentication protocol using smart cards for network applicants[☆]

Trupil Limbasiya[a,*], Mukesh Soni[b], Sajal Kumar Mishra[a]

[a] NIIT University, Neemrana, Rajasthan, India
[b] Smt. S. R. Patel Engineering College, Unjha, Gujarat, India

ARTICLE INFO

Article history:
Received 15 April 2017
Revised 23 December 2017
Accepted 26 December 2017
Available online xxx

Keywords:
Attack
Authentication
Key agreement
Remote user
Security

ABSTRACT

The rapid growth of internet technologies has provided various functions that allow easy remote user or customer access to its many systems. However, the responsibility of the system does not end after providing access to such remote users. The framework must consummate a precise level of security, because otherwise, an adversary may be able to disrupt the system or use its resources without authorization. This affects the system and its clients directly or obliquely, and to restrict access, an authentication scheme must be implemented. Recently, Nikooghadam et al. proposed an authentication and key agreement protocol and illustrated how it would be secure against various types of security attacks. In this study, we show that their proposed system is susceptible to insider, replay, and password-guessing attacks. We propose a more secure authentication system that can withstand discrete attacks, and measure the total execution time to determine what realistic implementation is needed to carry out an entire scheme.

1. Introduction

With the rapid evolution of the internet and considerable growth in network applications, remote user authentication has become a necessary function for accessing many resources. However, the internet is an insecure communication network; however, it is used for the process of user verification. Password authentication is one of the simplest and common techniques currently in use. Traditionally, password authentication schemes require that a user supply an identity and password to a server in order to log into a computer system. A basic authentication system maintains a server-side password table, and the server provides access to resources if valid credentials are entered. A user accessing software or running a hardware from an off-site location is known as a remote user. The process of authentication is divided into two phases: *Verification* and *Identification*. In the Verification phase, the system validates each user by cross-checking supplied information against a system database containing some set of credentials. In the Identification phase, the system validates the user by cross-examining the stored information against a scheme database [22].

Smart cards offer many benefits including low cost, efficiency, portability, and encrypted data storage capacity. Hence, they have been widely adopted by many e-commerce applications such as remote login systems, automated teller machines (ATMs), personal digital assistants (PDAs), database management systems, and network security protocols. Presently, many

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Z. Arnavut.

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

https://doi.org/10.1016/j.compeleceng.2017.12.045
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

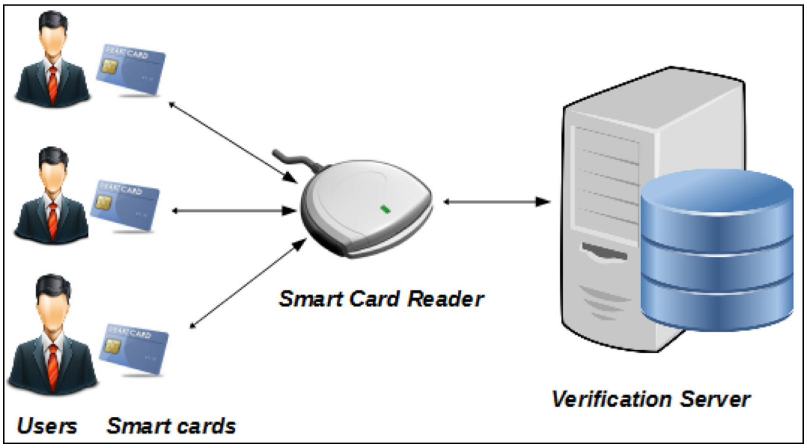

Fig. 1. General architecture of remote user authentication.

authentication systems verify users using smart cards. Traditional authentication mechanisms suffer from data leakage, theft, and/or corruption. A server administrator may reveal passwords if user data is stored in plain text on a server, allowing an adversary to impersonate a legitimate applicant by stealing user credentials from the password table. Encryption and passwords stored as hashes can mitigate these two problems [16].

Thus, remote user authentication is a procedure in which a server confirms the legitimacy of a user remotely requesting access over a free communication medium. There are many remote user authentication models, which can be employed depending on their respective merits. A familiar aspect among most schemes is that a user's identity is unchanged during transaction sessions, which can leak a users information and induce a risk of identity theft during message dissemination. To overcome this risk, many researchers have proposed dynamic identity-based user authentication systems. Fig. 1 presents a simple framework of a remote user authentication system that includes users using smart cards, a server, and a smart card reader to get system access.

Our contribution: In this paper, we performed cryptanalysis of the scheme presented in Nikooghadam et al. [21], finding it to be susceptible to insider, replay, and password-guessing attacks. Additionally, we recommend an advanced model for overcoming its drawbacks.

Paper organization: The rest of this article is organized as follows. In Section 2, we survey different authentication models. In Section 3, we review required background needed for describing the scheme. In Section 4, we briefly review the scheme from Nikooghadam et al. After that, we describe its security flaws in Section 5, and then present an advanced authentication framework in Section 6. In Section 7, we explain the security analysis of our proposed scheme, and in Section 8 we compare a performance analysis of the suggested model to other verification systems. We summarize our conclusions in Section 9.

2. Literature review

In 1981, Lamport [1] laid out an authentication model using a one-way hash function. In this protocol, the server stored a hashed value of a users password in order to confirm the identity of the user upon login. Lennon et al. [2] showed that this scheme [1] was vulnerable to a stolen verifier attack. Worse, any malicious person can obtain the confidential verification data by getting into to the servers database. With the hashed value of a user's password in hand, an attacker could guess the password offline, and then fool the server through impersonation. Hwang and Li [3] proposed a two-factor authentication scheme, in which a user provides his or her smart card and text-based password. For a malicious user to penetrate the system, the adversary would need a smart card along with the password to break the system. However, Chan and Cheng [4] showed that this protocol [3] was also vulnerable to impersonation. Further work (e.g., [7]) has discussed how to retrieve stored data from smart cards.

Sun [5] also describes a two-factor authentication scheme based on hash functions. Later, Chien et al. [6] suggested that the scheme in [5] was vulnerable to multiple attacks and lacked provisions for changing passwords. After that, Chien et al. proposed an improved authentication scheme. Ku and Chen [8] discovered that parallel-session and insider attacks were possible with the scheme [6] and offered a revised authentication scheme to overcome its drawbacks. This scheme was challenged by Yoon et al. [9], who described that the scheme from [8] was susceptible to denial-of-service (DOS) and parallel-session attacks. They also suggested an authentication scheme and claimed it to be secure against various attacks. Wang et al. [10] identified that the ([8] and [9]) schemes were vulnerable to attacks such as forgery, password guessing, and DOS, and suggested a novel scheme to remedy the pitfalls of these two schemes. In turn, Wang et al. [12] challenged the scheme from [9], proving that it was prone to impersonation, offline password guessing, and DOS attacks. They also went on to propose a scheme of their own. Das et al. [11] recommended a dynamic identity-based authentication model, which was quickly challenged ([12]) as being susceptible to a remote server attack.