Journal of Network and Computer Applications 87 (2017) 1–19

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems

Mohammad Masdari*, Safiyyeh Ahmadzadeh

Computer Engineering Department, Urmia Branch, Islamic Azad University, Urmia, Iran

ARTICLE INFO

Keywords:
TMIS
Authentication
Biometric
Password
Smart Card
Security
Attack

ABSTRACT

A Telecare Medical Information System (TMIS) enables doctors and physicians at a medical center to provide remote care via Internet to the registered patients at any place. Considering the privacy of the patients, medical data, secure and authenticated access to the medical data located at the medical severs are required. Recently, numerous states of the art authentication schemes are proposed in the literature to increase security of the Telecare Medical Information System (TMIS). This paper presents a comprehensive survey and taxonomy of these authentication schemes and classifies them based on the authentication methods applied in each scheme. In addition, a complete list of security attacks which can be conducted against the authentication schemes in the TMIS is provided, and the security capabilities of each scheme and their vulnerability to these attacks are discussed. Furthermore, the proposed authentication schemes are compared, and their advantages, properties and limitations are highlighted. Finally, the concluding remarks and open research issues in TMIS authentication schemes are provided.

1. Introduction

Major objective of The Telecare Medicine Information Systems (TMIS) is to provide the medical or health care facilities via Internet at the patient's home or any other position (Guo et al., 2012; Hamdi et al., 2014). These facilities are specifically very useful for those patients who are disabled or cannot attend hospital for various reasons (Mishra et al., 2014a; Okoh, 2015; Debiao et al., 2012). Thus, traditional time consuming modes of providing medical services are replaced by digitalized smart methods. Besides, the TMIS services can be presented in the form of cloud computing services and patients/users can access them using their smartphones (Masdari et al. 2016a, 2016b, 2016c; Masdari and Jalali, 2016). A Telecare Medical Information System (TMIS) contains medical servers that keep electronic medical record (EMRs) of registered users, and as indicated in Fig. 1, they provides access to the EMRs via the Internet to the users, physicians, health educators, hospitals, public health organizations and homecare service providers.

To prevent unauthorized and illegal access to the patients' private medical data in the medical servers, authenticated, protected and secure access to the medical data are needed (Sawand et al., 2015). For this purpose, the medical server should remotely authenticate users and provide the requested access to the corresponding medical records after successful authentication.

Authentication is the process of identifying the true identity of the communicating parties which in TMIS are conducted by using various cryptographic algorithms and biometric features.

After successful authentication, the participants may establish a session key or conduct a key agreement phase to agree about the cryptographic keys which will be used to protect the privacy and security of the subsequent data transfers (Gomes et al., 2007; Wu et al., 2012).

Numerous authentication schemes are designed for the TMIS which provide various authentication services for the users/patients, medical servers and other TMIS components. Depending on the security requirements, various forms of the authentication services can be provided in the TMIS services. For example, considering the number of the parties which should be authenticated in the authentication process, authentication schemes can be classified as follows:

- One-way authentication (one-to-one authentication)
- Mutual authentication
- Group authentication (many-to-many authentication)

In one-way authentication only one side (authenticator or verifier) is assured of the other side identity (prover) and in the mutual authentication, both side of the communications authenticate each other. Also, in group authentication all users belonging to the same

* Corresponding author.
E-mail addresses: M.Masdari@Iaurmia.ac.ir (M. Masdari), Safia.Ahmadzadeh@gmail.com (S. Ahmadzadeh).

http://dx.doi.org/10.1016/j.jnca.2017.03.003
Received 20 August 2016; Received in revised form 13 December 2016; Accepted 5 March 2017
Available online 07 March 2017

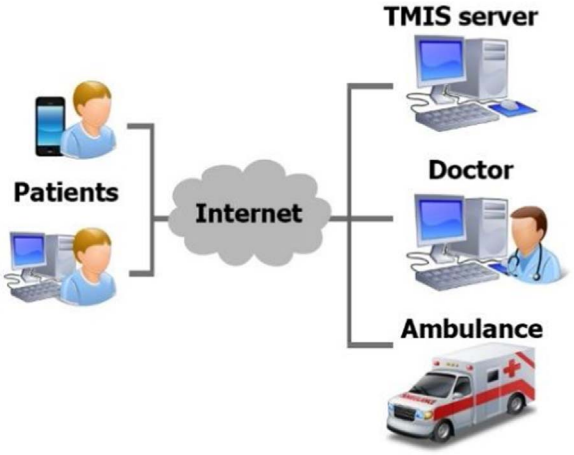

Fig. 1. Architecture of the E-healthcare systems.

group will be authenticated. In TMIS, medical server can authenticate the user/patient (one-way) or both the medical server and the user/patient can authenticate each other (mutual authentication).

Also, anonymous authentication is provided in the literature where the authenticator determines the authenticity of the other party without truly recognizing its identity.

Considering the privacy of the patient's medical data, supporting this type of authentication is very important. Moreover, based on the number of the factors applied in the authentication process, authentication schemes can be classified as:

- Single-Factor Authentication (SFA): Authentication is performed by using only one factor.
- Two-factor authentication (2FA): authentication is conducted by using two different factors. For example, a combination of biometric with a password can give stronger security for the authentication schemes than schemes which only apply passwords.
- Multi-factor authentication (MFA): authentication is performed based on multiple different factors. Considering numerous and diverse information and devices applied in the TMIS, effective multi-factor authentication schemes can be designed.

Considering the vulnerabilities of each authentication method, authentication schemes which utilize fewer factors become more vulnerable to more security attacks. For example, when an authentication system applies smart card and password, it will be vulnerable to the password guessing attacks once the smart card is stolen or lost. This problem can be mitigated by using another third factor in the authentications scheme. However, applying more authentication factors makes the authentication process more complicated.

Numerous authentication schemes are provided in the literature that apply a combination of authentication methods outlined before. For example, some mutual authentication schemes are designed which are anonymous and use single or multiple factors for authentication.

This paper provides a complete survey and taxonomy of the most recent authentication schemes proposed in the literature for the telecare medicine information systems (TMIS). It classifies the authentication schemes based on the techniques applied in each scheme to provide the intended authentication services. Furthermore, it describes the authentication capabilities of each proposed scheme and specifies the factors applied in each authentication scheme. Besides, the advantages, limitations and authentication overheads of each proposed scheme for the TIMS is highlighted. In addition, vulnerability of each authentication scheme to the various security attacks are illuminated, and their resistance against various attacks are specified. Finally, a complete comparison of the various security properties and features of authentication schemes are provided.

The rest of this article is organized as follows: Section 2 discuses vulnerabilities of the authentication scheme in TMIS, Section 3 studies classification of the proposed authentication schemes for TMIS, and Section 4 defines discussion. Finally, Section 5 presents the concluding remarks and open research issues.

2. Vulnerabilities of the authentication scheme in TMIS

Telecare Medicine Information Systems deal with the important and critical medical data of the patient's body, which must be secured against the adversary. However, like other network-based solutions, the TMIS systems and their various components such as WBANs (Zhang et al., 2016; Movassaghi et al., 2014; Otto et al., 2006; Dokovsky and Halteren, 2004; Rahim et al., 2012; Hughes et al., 2012; Fatehy and Kohno, 2013; Hur et al., 2013; Khan et al., 2014; Boulis et al., 2012; Ullah et al., 2012; Gao et al., 2014; Martelli et al., 2011; Kwak et al., 2010; Toorani, 2015; IEEE Standard, 2012; Somasundaram and Sivakumar, 2011; Tachtatzis et al., 2010; Ali and Khan, 2010) are vulnerable to several security attacks that can be conducted by internal or external attackers (Sampangi et al., 2012; Vallejos et al., 2012). This subsection describes some of the common security attacks conducted in the TMIS systems (Qadri et al., 2013):

- **Denial of service (DoS) attack:** Services are denied to the TMIS users/patients and the medical servers by the attackers (Shaqiri; Zia and Zomaya, 2006; Saleem et al., 2009).
- **Eavesdropping attack:** If an attacker can read the transmitted keys, an eavesdropping will happen (Jang et al., 2008).
- **Off-line password guessing attack:** In this attack, an attacker can employ some of the intercepted information, such as keys, or the self-generated parameters to guess the password of the patient (Munilla and Peinado, 2006). These attacks can never be 'prevented', but protocols can be made secure against such attacks.
- **On-line password guessing attack:** An adversary or attacker guesses every possible password of the patient, and tries to log into the medical server until he is successful.
- **Dictionary attack**
- **Privileged insider attack:** When the medical server needs to retain the patient's password for later authentication, the keys are probably being stolen by the adversary because the medical server can find out the patient's new password.
- **TMIS server impersonation attack:** An attacker masquerades as a legitimate user of the TMIS system (Wei-Chi and Chang, 2005; Gafurov et al., 2006). To succeed the user impersonation attack, an attacker has to generate a valid login message.
- **Patient impersonation attack:** In which a dishonest patient can easily impersonate another legal patient.
- **Man-in-middle attack:** An adversary intercepts the messages sent between the user and server and replaces them with his own messages.
- **Replay attack:** In a secure TMIS, replay attacks should be prevented by using timestamp and random numbers in the transmitted messages (Mana et al., 2009).
- **Selective forwarding attack:** An attacker may decrease to forward some keys.
- **Stolen-verifier attack:** In this attack, an adversary which is machinated inside member can modify the passwords or the patient verification tables stored in the medical server's database (Das et al., 2004).
- **Spoofing attack:** An attacker makes an interrupt by changing the routing information and keys in TMIS system (Sivaprasatham et al.).
- **Perfect forward secrecy:** This attack happens when an adversary is able to acquire the patient password or a secret key, and it will still be able to compute previous session keys (Krawczyk, 2011).
- **Parallel session attack:** In this attack, an adversary applies messages in another authentication process to replace the messages