Contents lists available at ScienceDirect

Future Generation Computer Systems

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

A secure chaotic map-based remote authentication scheme for telecare medicine information systems

Xiong Li [a],*, Fan Wu [b], Muhammad Khurram Khan [c], Lili Xu [d], Jian Shen [e], Minho Jo [f]

[a] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
[b] Department of Computer Science and Engineering, Xiamen Institute of Technology, Xiamen 361021, China
[c] Center of Excellence in Information Assurance, King Saud University, Riyadh 11653, Saudi Arabia
[d] School of Information Science and Technology, Xiamen University, Xiamen 361005, China
[e] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China
[f] Department of Computer and Information Science, Korea University, Sejong City, South Korea

HIGHLIGHTS

- A secure remote authentication scheme for TMIS using the chaotic maps is proposed.
- Formal proof shows that attacker has a negligible probability to crack the scheme.
- Formal verification by using Proverif shows that our scheme can resist the attackers.
- Comparison results show that our scheme is secure and efficient for TMIS application.

ARTICLE INFO

Article history:
Received 16 April 2017
Received in revised form 19 July 2017
Accepted 15 August 2017
Available online xxxx

Keywords:
TMIS
Chaotic maps
Authentication
User anonymity
Bergamo et al.'s attack

ABSTRACT

As a kind of e-health notion, telemedicine employs telecommunication and information technologies to provide remote clinical health care. Telecare medicine information system (TMIS) is a widely used application nowadays. Through the services provided by such e-health systems, doctors can obtain the variation of patients' conditions and make treatments quickly and accordingly. Recently, researchers have employed the Chebyshev chaotic maps in the authentication process of TMISs. Unfortunately, many kinds of security weaknesses such as off-line guessing attack, destitution of user anonymity and session key agreement happen in relative work. To overcome the disadvantages, we propose a secure remote authentication scheme employing the chaotic maps. We use the formal proof under random oracle model, and the famous verification tool Proverif to prove the security of the proposed scheme. Besides, informal analysis including ten security properties and performance comparison are shown to supplement the security properties. From the formal proof, we can see that the attacker has a negligible probability to crack the scheme over the active guessing attack. The formal verification demonstrates that our scheme can resist the attackers simulated by the tool Proverif. Moreover, we compare our scheme with several recent schemes, and the comparison results show that our scheme reaches the level of security requirements and also has suitable cost in performance. Thus, it is more applicable to telecare medicine environments.

1. Introduction

With the development of cloud computing, the concept of cloud assisted E-health develops fast nowadays. [1–6] proposed different security solutions from different aspects for could computing, and they are useful for building secure E-health system. As a sort of cognition of cloud assisted E-health, telemedicine attracts people's attention. Telecare Medical Information System (TMIS) [7,8] is one of the most popular applications of remote E-health service. It employs the traditional medical care services such as clinical diagnosis and health records storage. Both doctors and patients can enjoy the convenience of TMISs. The messages among the doctors, the patients and the servers are transmitted via the public networks. Any modification of those data may bring patients hazard. Also, patients' information should be secret. The leakage of such data threats the patients' privacy and makes them inconvenience. So how to make the transmission secure in TMISs is a hot issue.

To protect the important information flowing in the public channel [9], the method authentication and key agreement

* Corresponding author.
E-mail address: lixiongzhq@163.com (X. Li).

http://dx.doi.org/10.1016/j.future.2017.08.029
0167-739X/© 2017 Elsevier B.V. All rights reserved.

becomes a necessary part in the communication process, like [10–22]. Besides the password, a storage device, such as a smart card, or a mobile device, containing user's special secret data, owned by the user is employed in the remote authentication systems. This device is issued by a trusted server. The user who wants to join the system must submit his own information, such as the identity and some preprocessed strings which are related to registration to the server. The reason why network-based applications face above hazards is that many malicious adversaries exist in the network. For example, they may eavesdrop, intercept or even forge messages to disrupt the normal communications. Then dangers such as the user impersonation attack, the server spoofing attack and the off-line guessing attack occur. In order to overcome the weaknesses, many such schemes have been proposed [16,23–28].

1.1. Related works

Chebyshev chaotic map theory is now widely used in cryptography, such as S-boxes and hash functions. Recently, it is brought into the Client–Server architecture authentication protocols by researchers and naturally adopted by TMISs. In 2010, Guo and Zhang [29] pointed out that Xiao et al.'s scheme [30] vulnerable to the server spoofing attack. In 2012, Xue et al. [31] proposed an improved authentication scheme with chaotic maps. But Tan [32] pointed out that Xue et al.'s scheme was under the man-in-the-middle attack, also without strong anonymity. In 2013, Guo et al. [12] proposed a chaotic maps-based authentication scheme using smart cards. Unfortunately, Hao et al. [33] showed that Guo et al.'s scheme cannot guarantee the untraceability of the user. Also, there are two secret keys stored in the server as the burden. They presented a novel scheme for TMISs to avoid the weaknesses. But Jiang et al. [34] and Lee [35] showed the weaknesses in Hao et al.'s scheme, such as under the smart card loss attack and the attack proposed by Bergamo et al. [36]. They designed new schemes for TMISs, respectively. But Mishra et al. [15] showed that Jiang et al.'s scheme was under the de-synchronization attack, here we should point out that some papers [15,37] employ the name Denial of Service(DoS) attack refer to the de-synchronization attack, which may make rearers confused. The reason of such attack is that the latest updated information on different participants for the authentication process of next session are not the same, and we use the name de-synchronization attack to demonstrate the occurrence which blocks the normal authentication process. Also, Li et al. [37] showed that the schemes in [34,35] were insecure, and both the schemes in [34,35] have some weaknesses such as services misuse in the authentication process. For example, in both schemes, all users' real identities are useless in the authentication process. In 2014, Lin [14] presented a dynamic identity authentication scheme with chaotic maps. But in 2015, Wang et al. [16] found that Lin's scheme was insecure because it lacked user anonymity and was vulnerable to the user impersonation attack. They presented a new scheme with chaotic maps and mobile devices for the TMISs. But Wang et al.'s scheme is vulnerable to the attack which was described by Bergamo et al. [36], the off-line guessing attack, the user impersonation attack and the de-synchronization attack. Moreover, Wang et al.'s scheme cannot provide user anonymity and key agreement. Also in 2015, Lee [38] considered that the scheme in [29] could not resist the off-line guessing attack. In 2016, Islam et al. [24] pointed out that weaknesses such as user impersonation attack and lack of forward security existed in Lin's scheme [14]. But in fact it cannot keep user anonymity. Also in 2016, Liu and Xue [39] pointed out that the scheme in [38] was too complex with a traditional asymmetric encryption skeleton. However, the scheme in [39] has weaknesses including no friendly password for user and lack of user anonymity. In order to tackle the mentioned vulnerabilities, we propose a new remote authentication scheme with chaotic maps for TMISs. Formal proof is used to illustrate the security against attacks. We also do security verification by utilizing the popular tool Proverif and concrete analysis which prove that the proposed scheme is applicable and secure.

Table 1
Notations.

Symbol	Meaning
U_i, ID_i, PW_i	The *i*th user with his identity and password
S, s	The remote server with its secret key
$\mathcal{A}$	The attacker
$h(\cdot)$	The hash function
u, v	Random integers
sk_s, sk_u	The session keys calculated by S and U_i
$\oplus$	The XOR operation

1.2. Contributions & organization

The contributions of this paper are as follows:

1. We propose a novel remote authentication scheme for TMISs relied on chaotic maps and smart cards.
2. A formal proof of the proposed scheme is given to demonstrate the security of the attacker.
3. Via the code of Proverif, we show that the proposed scheme is robust and can resist various attacks simulated in the Proverif environment.
4. Compared to some recent chaotic maps-based authentication schemes for TMISs, our scheme performs well and is applicable for TMISs.

The rest of the article is organized as follows: some basic knowledge for the whole paper is illustrated in Section 2. We show our scheme in Section 3. In Sections 4 and 5, we use the formal proof and formal verification to prove the security of our scheme, respectively. Sections 6 and 7 demonstrate the security analysis of our scheme and the performance comparison among some recent schemes, respectively. Finally, the conclusion appears in Section 8.

2. Preliminaries

2.1. Notations

We list the notations used throughout the paper in Table 1.

2.2. Basic knowledge of Chebyshev chaotic maps

Here we list some preliminary knowledge about Chebyshev chaotic maps. The detailed expressions and explanations can be found in [40,41].

Definition 1. The original definition of Chebyshev polynomial:
n is a positive integer and x is a real number in $[-1, 1]$. The Chebyshev polynomial is $T_n(x) = cos(n(arccos(x)))$ with a degree n. Or we can see that:

$$T_n(x) = \begin{cases} 1 & n = 0 \\ x & n = 1 \\ 2xT_{n-1}(x) - T_{n-2}(x) & n \geq 2. \end{cases} \quad (1)$$

Definition 2. The enhancement of Chebyshev polynomial in cryptosystem:
$x \in (-\infty, +\infty)$ is an integer variable, and p is a large prime. The Chebyshev polynomial $T_n(x)$ is presented as follows:

$$T_n(x) = \begin{cases} 1 & n = 0 \\ x \bmod p & n = 1 \\ 2xT_{n-1}(x) - T_{n-2}(x) \bmod p & n \geq 2. \end{cases} \quad (2)$$

Please cite this article in press as: X. Li, et al., A secure chaotic map-based remote authentication scheme for telecare medicine information systems, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.08.029.