Commun Nonlinear Sci Numer Simulat 20 (2015) 482–488

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Improved chaotic maps-based password-authenticated key agreement using smart cards

Han-Yu Lin *

Department of Computer Science and Engineering, National Taiwan Ocean University, Keelung 202, Taiwan, Republic of China

ARTICLE INFO

Article history:
Received 7 June 2013
Received in revised form 20 May 2014
Accepted 26 May 2014
Available online 19 June 2014

Keywords:
Authentication
Key agreement
Chaotic map
Smart card
Cryptanalysis

ABSTRACT

Elaborating on the security of password-based authenticated key agreement, in this paper, the author cryptanalyzes a chaotic maps-based password-authenticated key agreement proposed by Guo and Chang recently. Specifically, their protocol could not achieve strong user anonymity due to a fixed parameter and a malicious adversary is able to derive the shared session key by manipulating the property of Chebyshev chaotic maps. Additionally, the author also presents an improved scheme to eliminate the above weaknesses and still maintain the efficiency.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

Key agreement protocols also known as key exchange ones aim at establishing a common session key between two communicating parties. The key challenge of designing such a protocol is how to securely and efficiently derive a session key that is only known to the communicated parties. Based on the famous discrete logarithm problem (DLP), in 1976, Diffie and Hellman [6] introduced the first key agreement protocol. In their scheme, each party could contribute partial value to the final session key. However, later analyses showed that a malicious adversary could easily plot the so-called man-in-the-middle attack to fool both sides in their scheme. So far, many related protocols have been proposed. According to their essential structures, we classify these schemes into the following types:

(1) *Pure password-based protocols:*

In 1981, Lamport [14] proposed a password-based authentication scheme in which a user is authenticated by his predefined password stored in the server. That is, the server has to maintain a password table for verification. Although a secure hash function was employed to protect users' passwords from being learned by any outsider directly, some security vulnerabilities were still found out in their scheme. Since then, lots of studies based on passwords [9,17,19,20] have been proposed to either strengthen the security level or improve the efficiency of existing schemes.

* Address: Department of Computer Science and Engineering, National Taiwan Ocean University, 2, Beining Road, Keelung, 202, Taiwan, Republic of China. Tel.: +886 2 2462 2192x6656; fax: +886 2 2462 3249.
E-mail address: lin.hanyu@msa.hinet.net

http://dx.doi.org/10.1016/j.cnsns.2014.05.027
1007-5704/© 2014 Elsevier B.V. All rights reserved.

(2) *Dynamic protocols:*

In 2004, Das et al. [5] raised the importance of keeping user's identity secret during communication as any adversary might easily reveal the identity of communicating user by eavesdropping the transmitted messages. Owing to this concern, they introduced the notion of dynamic authentication (also called anonymous authentication) in which a user will first transform his static ID into a dynamic one and then use the dynamic ID to request access of the server. Since the dynamic ID will change with different sessions and it is difficult to derive the static ID from its dynamic one based on some trapdoor one-way function, any adversary is impossible to obtain the real user identity. However, some later researches [15,24,28] pointed out potential security flaws of Das et al.'s scheme and gave the corresponding amendments, too. Inspired by Wang et al.'s scheme [24], in 2010, Khan et al. [11] came up with a new dynamic ID authentication protocol with better efficiency.

(3) *Dynamic protocols with smart cards:*

In 2010, Tsai et al. [22] utilized a smart card to assist with the user login process and demonstrated that the user identity of previous works [24,28] could be exposed. In 2011, Wen and Li [25] introduced a dynamic key agreement scheme further supporting revocation and secret renewal for both users and servers. Yet, in 2012, Tang and Liu [21] claimed that the Wen-Li scheme cannot be deployed in practical applications due to several security drawbacks. In addition to the above schemes, more related studies based on dynamic ID could also be found out in [1,4,8,10,13,16–18,23,26,29].

(4) *Chaotic map-based protocols with smart cards:*

By the semi-group property of Chebyshev chaotic map [2,12], Xiao et al. [27] presented the first chaos-based authenticated key agreement protocol. Such a scheme is unnecessary to choose large primes or perform complicated modular exponentiation computation and hence receives much attention for recent years. In 2013, Guo and Chang [7] proposed a chaotic maps-based password-authenticated key agreement using smart cards. They claimed that their scheme possesses necessary characteristics and achieves essential security requirements.

In this paper, the author pays his attention to the security of one recently proposed chaotic map-based protocol with smart cards, i.e., the Guo–Chang scheme. The first contribution of this paper is to cryptanalyze the Guo–Chang scheme. More precisely, the author will point out two drawbacks of their schemes. One is that their protocol cannot provide full protection for user's identity. The other is that a malicious adversary is capable of deriving the mutually shared session key by intercepting the transmitted messages between the user and the server. The second contribution of this paper is to further address an improved variant amending above security weaknesses without increasing the computational complexity.

The rest of this paper is organized as follows. Section 2 states some preliminaries. The formal model of authenticated key agreement protocol is described in Section 3. Section 4 will briefly review the Guo–Chang scheme. Cryptanalyses and improvement will be detailed in Section 5. Finally, a conclusion with the significance of this paper is presented in Section 6.

2. Preliminaries

We first state the properties of Chebyshev chaotic map and related computational problems which will be employed in the proposed scheme.

Let a be a random number and $x \in_R [-1, 1]$. The Chebyshev polynomial of degree a is denoted as $T_a(x) = \cos(a \cdot \arccos(x))$. The recurrent formulas of the Chebyshev polynomial is shown below:

$$\begin{aligned} &T_0(x) = 1, \\ &T_1(x) = x, \\ &T_2(x) = 2x^2 - 1, \\ &T_{a+1}(x) = 2xT_a(x) - T_{a-1}(x), \quad \text{for } a \in N. \end{aligned}$$

Chebyshev polynomial exhibits two important properties described as follows:

- Semi-group property

$$\begin{aligned} T_a(T_b(x)) &= \cos(a \cdot \arccos(\cos(b \cdot \arccos(x)))) \\ &= \cos(ab \cdot \arccos(x)) \\ &= T_{ba}(x) \\ &= T_b(T_a(x)). \end{aligned}$$

- Chaotic property
  When $a > 1$, Chebyshev polynomial map $T_a : [-1, 1] \to [-1, 1]$ of degree a is a chaotic map with its invariant density $f^*(x) = 1/(\pi\sqrt{1 - x^2})$ for Lyapunov exponent $\lambda = \ln a > 0$.

Download English Version:

https://daneshyari.com/en/article/755720

Download Persian Version:

https://daneshyari.com/article/755720

Daneshyari.com