Information Sciences 290 (2015) 63–71

Contents lists available at ScienceDirect

Information Sciences

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

Enhancing the security of password authenticated key agreement protocols based on chaotic maps

Tian-Fu Lee *

Department of Medical Informatics, Tzu Chi University, No. 701, Zhongyang Rd., Sec. 3, Hualien 97004, Taiwan, ROC

ARTICLE INFO

Article history:
Received 27 June 2013
Received in revised form 31 July 2014
Accepted 15 August 2014
Available online 24 August 2014

Keywords:
Password
Authentication
Key agreement protocol
Chaotic map
Network security

ABSTRACT

Password authenticated key agreement allows users to only keep a weak password and establish an authentication key shared with a server. However, the chaotic maps based authenticated key agreement protocol of Xiao et al. in which time-stamps are used to resist replaying attacks and the subsequent group key agreement protocol of Guo and Zhang in which chaotic hash is used as an alternative are insecure against off-line password guessing attacks and violate the session key security. Therefore, this work presents two secure password authenticated key agreement protocols based on chaotic maps. One is based on synchronized clocks, while the other uses nonces. Besides preventing the limitations of previous protocols and reducing the number of messages during communication, the proposed protocols do not require extra equipment for storing long-term secrets in the client.

1. Introduction

Password authenticated key agreement enables users to only keep a weak password and establish an authentication key shared with a server. Many chaotic maps-based password authenticated key agreements and related approaches have been developed recently, owing to that chaotic map operations provide the semi-group property and have a higher efficiency than modular exponential operations and scalar multiplications on an elliptic curve [1,11,13,20,25,31,32].

Xiao et al. [27] in 2007 developed a nonce-based authenticated key agreement protocol using chaotic maps. However, their protocol fails to withstand the relay attacks [10]. Two mechanisms can guarantee the freshness of messages and prevent replaying attacks in communicating protocols. One such mechanism is based on synchronized clocks (i.e. timestamp-based), while the other one uses random numbers or nonces (i.e. nonce-based). A timestamp-based communicating protocol involves constructing complex synchronized clocks in a network environment. However, the timestamp-based communicating protocol requires fewer communicating messages than a nonce-based communicating protocol does [4–6,12,14–17]. By using timestamps, Xiao et al. [28] in 2008 developed an enhanced chaotic maps-based key agreement protocol to eliminate the limitations of their previous protocol [27]. Gong et al. [7] in 2012 proposed a key agreement protocol based on extended chaotic maps with password sharing. Later, Wang and Luan [26] showed that the key agreement protocol of Gong et al. had some key management issues and potential security problems. To solve the limitations in the protocol of Gong et al., Wang and Luan also developed a secure and efficient timestamp-based key agreement protocol by using extended chaotic maps. In the protocol of Wang and Luan, the communicating participants consist of a trusted authentication server and two communicating

* Tel.: +886 3 856 5301x2403; fax: +886 3 857 9409.
E-mail addresses: jackytflee@mail.tcu.edu.tw, tflee@ismail.csie.ncku.edu.tw

http://dx.doi.org/10.1016/j.ins.2014.08.041
0020-0255/

users. Thus, the protocol of Wang and Luan is suitable for three-party communicating environment. Guo and Zhang [9] in 2012 demonstrated that a malicious server can predetermine a session key alone in the protocol of Xiao et al. Namely, their protocol fails to satisfy the requirements with the contributory nature of key agreement. Guo and Zhang also designed a group key agreement protocol using chaotic hash as an alternative. However, both the improved protocol of Xiao et al. [28] and that of Guo and Zhang [9] are insecure against off-line password guessing attacks. Moreover, attackers with a user's password can derive a common session key. However, to increase their security many related protocols [7,17,23,24,26,29,30] store a long-term secret key by using additional equipment (e.g., smart cards). However, this measure fails to allow users to only keep a weak password and establish an authentication key shared with a server.

While addressing the limitations of the protocols of Xiao et al. [28] and Guo and Zhang [9], this work presents efficient and secure authenticated key agreement protocols based on chaotic maps. One protocol is nonce-based, while the other one is timestamp-based. The proposed protocols avoid the limitations of previous ones. Additionally, the proposed protocols allow users to only keep their password without requiring additional equipment (e.g., smart cards or RFID tags) for storing a long-term secret key.

The remainder of this paper is organized as follows. Section 2 reviews the authenticated key agreement protocols of Xiao et al. and Guo and Zhang, as well as describes their limitations. Section 3 then introduces the proposed nonce-based and timestamp-based authenticated key agreement protocols using chaotic maps. Next, Section 4 analyzes the security of the proposed protocols and compares them with other related protocols. Conclusions are finally drawn in Section 5.

2. Related works

This section first lists the used definitions, defines Chebyshev chaotic maps, and then describes the concepts of the key agreement protocols proposed by Xiao et al. and proposed by Guo and Zhang and their weaknesses.

2.1. Chebyshev chaotic maps [1,11,31]

The Chebyshev polynomial $T_n(x)$ is a polynomial in x of degree n, defined by the following relation:

$$T_n(x) = \cos n\theta, \text{ where } x = \cos\theta.$$

The recurrence relation of $T_n(x)$ is defined as:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x),$$

for any $n \geqslant 2$, with $T_0(x) = 1$ and $T_1(x) = x$.

The Chebyshev polynomial satisfies the semi-group property and satisfies:

$$T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x)),$$

for $s, r \in Z^+$.

The Chebyshev polynomial also provides chaotic property: When $n > 1$, Chebyshev polynomial map T_n: $[-1,1] \to [-1,1]$ of degree n is a chaotic map with its invariant density

$$f^*(x) = 1\Big/\left(\pi\sqrt{1-x^2}\right),$$

for Lyaounov exponent $\ln n > 0$.

2.2. Quadratic residue assumption [3,18,19]

Assume that p and q are two large primes and $n = p \times q$. Let the symbol QR_n denotes the set of all quadratic residues in $[1, n-1]$. If $y = x^2 \bmod n$ has a solution, i.e. $\exists$ a square root for y, then y is named as a quadratic residue modulo n. Assume that $y \in QR_n$. To find x satisfying $y = x^2 \bmod n$ without the knowledge of p and q is computationally infeasible since no polynomial algorithm has been found to solve the factoring problem.

2.3. Improved key agreement protocol of Xiao et al.

This section briefly reviews the improved key agreement protocol of Xiao et al. [28]. Assume that a user A whose identification is ID_A and a server B share a hash value $h_{PW} = H(ID_A, PW)$ of A's random password PW, where $H(\cdot)$ denotes the chaotic hash function. The improved key agreement protocol of Xiao et al. consists of authentication phase and key agreement phase, which works as follows.

2.3.1. Authentication phase

(1) A chooses a random number $ra \in [-1,1]$, then he sends his/her user identity ID_A, and ra to B.
(2) B chooses a random number rb and sends it back to A.