An Enhanced and Provably Secure Chaotic Map-Based Authenticated Key Agreement in Multi-Server Architecture

Azeem Irshad1 · Shehzad Ashraf Chaudhry1 · Qi Xie2 · Xiong Li3 · Mohammad Sabzinejad Farash4 · Saru Kumari5 · Fan Wu6

Received: 12 January 2017 / Accepted: 20 July 2017 / Published online: 11 August 2017
© King Fahd University of Petroleum & Minerals 2017

Abstract In the multi-server authentication (MSA) paradigm, a subscriber might avail multiple services of different service providers, after registering from registration authority. In this approach, the user has to remember only a single password for all service providers, and servers are relieved of individualized registrations. Many MSA-related schemes have been presented so far, however with several drawbacks. In this connection, recently Li et al. in Wirel. Pers. Commun., (2016). doi: 10.1007/s11277-016-3293-x presented a chaotic map-based multi-server authentication scheme. However, we observed that Li et al. suffer from malicious server insider attack, stolen smart card attack, and session-specific temporary information attack. This research work is based on improving security of Li et al.’s protocol in minimum possible computation cost. We also evaluate the security for the contributed work which is provable under formal security analysis employing random oracle model and BAN Logic.

Keywords Multi-server authentication · Chebyshev chaotic map · Cryptography · Authentication · Attacks

1 Introduction

The extensive growth of computer networks in every domain has raised the concerns about information security manifolds. As for security, the authentication protocols have developed from conventional single-factor to multi-factor techniques, from hash-based operations to complex cryptographic operations-based schemes that have greatly enhanced the security of a user. In this context, the chaos cryptography being one of the efficient cryptographic tools has been adopted due to its computational efficiency and miscellaneous features [1]. In this work, the chaos cryptography is adopted to address the ongoing problems in securing the multi-server authentication protocols.

The first simple authentication scheme was presented by Lamport [2]. Then, these schemes evolve from password-based schemes to smart card [3,4] and biometric-based schemes [5,6]. At the same time, the traditional single-server authentication techniques [7,8] are unable to meet the current challenges of a sophisticated user, which gives rise to another multi-server-based paradigm. The MSA paradigm obviates.
the need for a user to maintain multiple passwords for different services; rather a single registered password may suffice the authentication requirements of several service providers. The first ever scheme for MSA problem was put forward by Li et al., in 2001 based on neural networks. However, the scheme [9] was found inefficient for overheads due to the training of a neural network. In 2003, Lin et al. [10] presented an ElGamal digital signature-based scheme for MSA environment. However, the large number of system parameters as used in the scheme brought inefficiency at the server’s end.

Next, to remedy the flaws, Juang [11] introduced a low-cost hash and symmetric operations-based scheme for MSA. However, the Juang scheme was found under attacks by Chang and Lee [12] with the introduction of an improved scheme. The scheme [12] was again found vulnerable to impersonation attacks [13]. Thereafter, Tsaur et al. designed two MSA-based schemes [13,14] depending on Lagrange polynomial interpolation and digital signature standard. Afterwards, Tsai and Lo [15] presented another MSA protocol relying on symmetric cryptography. Few attacks were discovered on Tsai and Lo by [16,17]. These prior schemes were also lacking anonymity and relying on static identity, which was focused in forthcoming schemes by introducing a dynamic identity. First time in 2009, Liao and Wang [18] presented a dynamic identity-based MSA scheme, which helped the subscribers to remain indistinguishable among different sessions. The scheme [18] was found vulnerable for different attacks by Hsiang and Shih [19]. Hsiang and Shih also introduced an improved protocol [19], which was further found defective by Sood et al. [20] and Lee et al. [21] with the introduction of improved techniques. However, both [20,21] were again found prone to attacks [22,23].

We notice a growing focus towards an efficient chaos-based Chebyshev cryptography for designing protocols in a few years. A few chaotic map-based schemes have been presented for MSA protocols lately [24–33]. In this connection, in 2012, Tsaur et al. [24] presented an efficient MSA-based scheme relying on self-certified timestamp. However, it was found to be having insider attack and known-plaintext attacks by Lee et al. [33]. Later on, Li et al. [34] pointed few attacks in [33], i.e. unauthorized login, faulty password modification, and spoofing attacks, and also presented an improved model. However, recently we have identified that the Li et al. scheme does not provide resistance to stolen smart card attack, malicious server attacks (biometric guessing and user impersonation attacks) and also session-specific temporary information attack. We have proposed a secure and enhanced protocol within the same cost [34] as proved in the forthcoming sections. In this study, we critically examine the Li et al.’s protocol and also ascertain its performance against contributed scheme using formal security analysis and BAN logic.

For scheme’s layout, Sect. 2 illustrates the preliminaries, defining Chebyshev chaotic map and biohashing. Section 3 presents the working of Li et al. protocol. Section 4 illustrates cryptanalysis for Li et al. Section 5 demonstrates the proposed scheme. Section 6 presents the security and performance analysis, while Sect. 7 concludes the manuscript.

2 Preliminaries

This section briefly presents the Chebyshev chaotic map and the biometric biohashing function as follows.

2.1 Chebyshev Chaotic Maps

Some features of Chebyshev-based polynomial and chaotic maps [35–40] can be illustrated as follows:

1. We take $\Xi$ as a prime integer and variable $t$ having interval $[-1, 1]$. Besides, the Chebyshev polynomial could be stated as $T_\Xi(t)$: $[-1, 1] \rightarrow [-1, 1]$ as $T_\Xi(t) = \cos(\Xi \arccos(t))$. A recurring relation is mostly utilized for describing Chebyshev chaotic polynomial $T_\Xi: \mathbb{R} \rightarrow \mathbb{R}$ having degree $\Xi$, as given below.

$$T_\Xi(t) = 2t \cdot T_{\Xi-1}(t) - T_{\Xi-2}(t).$$

Given $\Xi \geq 2$, $T_0(t) = 1$, and $T_1(t) = t$

We list a few Chebyshev polynomials as:

$$T_2(t) = 2t^2 - 1$$

$$T_3(t) = 4t^3 - 3 \cdot t$$

$$T_4(t) = 8t^4 - 8 \cdot t^2 + 1$$

2. The chebyshev polynomial bears the understated features:

The chaotic feature: For $\Xi \geq 1$, the Chebyshev chaotic map $T_\Xi(t)$: $[-1, 1] \rightarrow [-1, 1]$ with degree $\Xi$ depicts a chebyshev-map for invariant density $\mu_\Xi(t) = 1/(\pi \sqrt{1-t^2})$ related to all positive Lyapunov-exponent $\ln \Xi$.

The semigroup property [28]: This property of chaotic polynomial could be identified on interval, i.e. $[-\infty, +\infty]$ as given in the following:

$$T_\Xi(t) = (2t \cdot T_{\Xi-1}(t) - T_{\Xi-2}(t)) \mod p$$

Such as $\Xi \geq 2$, $t \in [-\infty, +\infty]$, and $p$ characterize a high entropy prime number. Moreover,

$$T_a(T_b(t)) \equiv T_{ab}(t) \equiv T_b(T_a(t)) \mod p$$