Attacks on Lin's Mobile Dynamic Identity-based Authenticated Key Agreement Scheme using Chebyshev Chaotic Maps

SK Hafizul Islam [a]

Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333 031, India

Abstract

In 2014, Lin proposed an authentication system with dynamic identity of the user for low-power mobile devices using Chebyshev chaotic map. The scheme is proposed to provide mutual authentication and session key agreement between a remote server and its legitimate user. The scheme provides user anonymity and untracibility, and resilience from many cryptographic attacks. However, the author of this paper showed that Lin's scheme is no longer usable for practical applications as (i) it cannot verify the wrong identity and password at the user side in the login and password change phases, (ii) it cannot protect user impersonation attack, and (ii) it has the problem of session key forward secrecy.

Keywords: Chaotic maps; Password; Mobile device; Authentication; Hash function.

1. Introduction

The password-based remote user mutual authentication and secure session key establishment between a legitimate user and a remote server over any hostile network is an important paradigm in information security. By the remote user authentication, a user can communicate and exchange confidential information with the remote server. However, the malicious parties have always tries to break the secure communication to masquerade either the legitimate user or the remote server. Therefore, the security and privacy in user authentication paradigm become hot issues. As the session key agreement is an essential factor in any mutual authentication system, the resilience from the known cryptographic attacks such as impersonation attack, replay attack, denial of service attacks, password guessing attack, server spoofing attack, etc. needs to be archived along with other security objectives. In the literature, many such user authentication systems [1, 2, 3, 4] have been implemented using one-way hash function. In addition, user anonymity and untracibility are also two important factors for any mutual authentication systems. The user anonymity hides the original identity from the outsiders and the untracibility makes difficult to recognize that two or more login sessions are performed by the same user. Recently, many dynamic identity-based remote user mutual authentication schemes [5, 6, 7, 8, 9] are designed to achieve user anonymity and untracibility.

In recent years, Chebyshev chaotic map-based cryptographic schemes [10, 11, 13, 14, 16, 17, 18, 19, 20, 21, 22] are widely accepted due to the computation and security strengths. In 2014, Lin [23] proposed a mobile dynamic identity-based mutual authentication and key agreement scheme based on chaotic maps for low-power mobile device. The author claimed that in his scheme a mobile user can securely login to the remote server and establish a shared session key with the server, and the scheme can withstand many active attacks. However, in this paper some problems in Lin's scheme [23] have been analyzed. It has been analyzed that Lin's scheme is unfriendly as (i) it cannot verify the wrong identity and password at the user side in the login and password change phases, (ii) it cannot protect user impersonation attack, and (ii) it has the problem of session key forward secrecy.

The rest of the paper is organized as follows. In Section 2, chaotic map and some hard problems on it are briefly studied. The review of Lin's authentication and key agreement scheme is introduced in Section 3 and its design issues are rigorously analyzed in Section 4. The Section 5 draws some concluding remarks.

[a]Corresponding author: hafi786@gmail.com, hafizul.ism@gmail.com, Ph.: +91-8797369160

2. Chebyshev chaotic maps

Definition 1 (Chaotic map)**.** Let n be an integer x is a real number from the set $[-1, 1]$, the Chebyshev polynomial $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ is defined as [18, 19, 20, 21, 22],

$$T_n(x) \quad = \quad cos(n \cdot cos^{-1}(x))$$

The recurrence relation of Chebyshev polynomial is defined as [18, 19, 20, 21, 22]:

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

where, $n > 2$, $T_0(x) = 1$, $T_1(x) = x$. Some of other Chebyshev polynomials are $T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$, $T_5(x) = 16x^5 - 20x^3 + 5x$.
The Chebyshev polynomials has the following two interesting properties [18, 19, 20, 21, 22]:

Definition 2 (Semigroup property)**.** The semigroup property of the Chebyshev polynomial $T_n(x)$ is defined as follows [18, 19, 20, 21, 22]:

$$\begin{aligned} T_r(T_s(x)) &= cos(r\, cos^{-1}(cos(s\, cos^{-1}(x)))) \\ &= cos(rs\, cos^{-1}(x)) \\ &= T_{sr}(x) \end{aligned}$$

where r and s are positive integer and $x \in [-1, 1]$. Chebyshev polynomials also satisfy the commutative property under composition as follows:

$$T_r(T_s(x)) \quad = \quad T_s(T_r(x))$$

Definition 3 (Chaotic property)**.** The Chebyshev map $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ of degree $n > 1$ is a chaotic map with invariant density $f^*(x) = \frac{1}{\pi \sqrt{(1-x^2)}}$ for positive Lyapunov exponent $\lambda = (\ln n) > 0$ [18, 19, 20, 21, 22].

Now, we describe some computationally hard problems on Chebyshev polynomials [18, 19, 20, 21, 22].

Definition 4 (Chaotic maps-based discrete logarithm (CDL) problem)**.** For given a random tuple $\langle x, y \rangle$, it is infeasible to find the integer r by any polynomial time bounded algorithm, where $y = T_r(x)$.

Definition 5 (Chaotic maps-based Diffie-Hellman (CDH) problem)**.** For given a random tuple $\langle x, T_r(x), T_s(x) \rangle$, it is infeasible to find the $T_{rs}(x)$ by any polynomial time bounded algorithm.

3. Review of Lin's mobile dynamic identity-based authenticated key agreement scheme

This section describes chaotic map-based mobile dynamic identity authenticated key agreement scheme proposed recently by Lin [23]. This scheme has four phases of our scheme, called **Registration**, **Login**, **Verification** and **Password-change**. Assume that ID_a is the identity of the mobile user U_a and $h(\cdot)$ is a collision-resistant one-way hash function. The remote server B chooses a master secret s and a random variable x from $[-1, 1]$, and then computes $T_s(x)$. The server B keeps s kept secret and encapsulate $\langle x, T_s(x) \rangle$ in U_a's mobile device. The notations of Lin's scheme are illustrated in the Table 1.

Table 1: Descriptions of various notations used in Lin's scheme.

Notations	Description
U_a	The mobile user
ID_a	The identity of U_a
PW_a	The password of U_a
B	The remote server
s	The secret key of B
$T_l(x)$	The Chebyshev polynomial of degree l
x	The real number chosen from $[-1, 1]$
$h(\cdot)$	The secure and collision-resistance one-way hash function
$\oplus$	The bitwise XOR operator
$\|\|$	The concatenation operator
λ	The session key agreed between U_a and B

3.1. Registration phase

In this phase, U_a and B performs the following operations:

Step 1. U_a chooses his/her identity ID_a, password PW_a and a random integer t, and calculates $W_a = PW_a \oplus t$. Then U_a sends $\langle ID_a, W_a \rangle$ to B over a secure channel.

Step 2. On receiving $\langle ID_a, W_a \rangle$, B computes $H_a = h(s, ID_a)$, $n_a = h(W_a, ID_a) \oplus (H_a \| x \| T_s(x))$ and delivers n_a to U_a over a secure channel.

Step 3. On receiving n_a fom the remote server B, U_a computes $N_a = h(ID_a, PW_a) \oplus n_a \oplus h(W_a, ID_a)$ and stores it in his/her mobile device.

3.2. Login phase

U_a inserts his/her $\langle ID_a, PW_a \rangle$ into the mobile device, then the device chooses a random number k and computes $H_a \| x \| T_s(x) = N_a \oplus h(ID_a, PW_a)$, $Z = T_k(T_s(x))$, $CID_a = ID_a \oplus (H_a \| T_1 \| Z)$, $C = T_k(x)$, $R = H_a \oplus Z$ and $V_a = h(CID_a, C, H_a, R, T_1)$, here T_1 denotes the current timestamp. Now, the mobile device forwards the login message $\langle CID_a, C, V_a, R, T_1 \rangle$ to B over a public channel.

3.3. Verification phase

In this phase, B and U_a executes the following steps for mutual authentication and session key generation between them:

Step 1. On receiving $\langle CID_a, C, V_a, R, T_1 \rangle$, B validates the timestamp T_1.

Step 2. If the timestamp T_1 is valid, B computes $Z = T_s(C)$, $H_a = R \oplus Z$, $ID_a = CID_a \oplus (H_a \| T_1 \| Z)$, $V'_a = h(CID_a, C, H_a, R, T_1)$, and then verifies whether the equation $V'_a = V_a$ holds.

Step 3. If $V'_a = V_a$ holds, B computes $\lambda = h(H_a, CID_a, V_a, T_1, T_2)$ and $V_s = h(\lambda, H_a, T_1, T_2)$, and sends the response message $\langle V_s, T_2 \rangle$ to U_a over a public channel.

Step 4. On receiving $\langle V_s, T_2 \rangle$, U_a validates the timestamp T_2. If T_2 is valid, U_a computes $\lambda = h(H_a, CID_a, V_a, T_1, T_2)$, $V'_s = h(\lambda, H_a, T_1, T_2)$ and then verifies whether the condition $V'_s = V_s$ holds. If $V'_s = V_s$ holds, U_a authenticates B and accepts λ as the correct session key shared with B.

3.4. Password change phase

In this phase, U_a enters his/her old and new passwords $\langle PW_a, PW'_a \rangle$ and the mobile device computes $N'_a = N_a \oplus h(ID_a, PW_a) \oplus h(ID_a, PW'_a)$, and updates N_a to N'_a.

4. Design issues of Lin's scheme [23]

In this section, we will prove that Lin's scheme for mobile users [23] is inefficient for practical use due to the following reasons:

4.1. Design flaw in login phase

The login and authentication phases of Lin's scheme [23] is impractical for practical use. In the login phase of Lin's scheme [23], the verification of wrong login identity and password at user side is not designed. The whole authentication system will suffers if the mobile user U_a mistakenly keys his/her identity and password. We assume that U_a mistakenly inputs the wrong identity and password $\langle ID_a^*, PW_a^*\rangle$ instead of $\langle ID_a, PW_a\rangle$.

Step 1. When U_a keys $\langle ID_a^*, PW_a^*\rangle$ into the mobile device, then the device computes $N_a \oplus h(ID_a^*, PW_a^*) = h(ID_a, PW_a) \oplus h(ID_a^*, PW_a^*) \oplus (H_a \| x \| T_s(x)) \neq H_a \| x \| T_s(x)$. We assume that $N_a \oplus h(ID_a^*, PW_a^*) = (H_a' \| x' \| T_s^{'}(x))$. Therefore, the mobile device chooses a random number k and then computes $Z' = T_k(T_s^{'}(x))$, $CID_a' = ID_a^* \oplus (H_a' \| T_1 \| Z')$, $C' = T_k(x)$, $R' = H_a' \oplus Z'$ and $V_a' = h(CID_a', C', H_a', R', T_1)$, T_1 is the current timestamp. The mobile device sends $\langle CID_a', C', V_a', R', T_1\rangle$ to B over a public channel.

Step 2. On receiving $\langle CID_a', C', V_a', R', T_1\rangle$, B finds that the timestamp T_1 is valid. Then B computes $Z'' = T_s(C')$, $H_a'' = R' \oplus Z''$, $ID_a'' = CID_a \oplus (H_a'' \| T_1 \| Z')$, $V_a'' = h(CID_a', C', H_a'', R', T_1)$. It can be noted that $Z'' = T_s(C') \neq Z'$, and thus, $H_a'' \neq H_a'$, $V_a'' \neq V_a'$. Accordingly, B aborts the session. However, U_a is a valid user for the remote server B. From this discussion, it it clear that the verification of the wrong password and identity detection at the user side is desirable, otherwise, it will put unnecessary computation and communication costs to the whole authentication system.

4.2. Design flaw in password change phase

The password change phase of Lin's scheme [23] also suffers from the same problem as discussed above. During password change operation, suppose that U_a mistakenly enters a new password PW_a' and the wrong old password PW_a^* instead of the original password PW_a. Then the mobile device computes $N_a' = N_a \oplus h(ID_a, PW_a^*) \oplus h(ID_a, PW_a') = h(ID_a, PW_a) \oplus (H_a \| x \| T_s(x)) \oplus h(ID_a, PW_a^*) \oplus h(ID_a, PW_a') \neq h(ID_a, PW_a') \oplus (H_a \| x \| T_s(x))$, and updates N_a to N_a'. It can be observed that, if in the next time U_a tries to login to the remote server B by the input $\langle ID_a, PW_a'\rangle$, then B always rejects U_a due to the reasons as discussed earlier (see section 4.1).

4.3. User impersonation attack

In this section, we will show that a user U_a of the scheme [23] can impersonate another valid user U_j of the remote server B in the following ways:

Step 1. U_a extracts the registration information $N_a = h(ID_a, PW_a) \oplus (H_a \| x \| T_s(x))$ from his/her mobile device using the methods proposed in [24, 25, 26].

Step 2. U_a then computes $(H_a \| x \| T_s(x)) = N_a \oplus h(ID_a, PW_a)$ using his/her $\langle ID_a, PW_a\rangle$.

Step 3. U_a chooses the login identity ID_j of a valid user U_j of B. U_a selects two random integers k and H_j and then computes $Z_j = T_k(T_s(x))$, $CID_j = ID_j \oplus (H_j \| T_1 \| Z_j)$, $C_j = T_k(x)$, $R_j = H_j \oplus Z_j$ and $V_j = h(CID_j, C_j, H_j, R_j, T_1)$. The mobile device then delivers the login message $\langle CID_j, C_j, V_j, R_j, T_1\rangle$ to B over a public channel.

Step 4. On receiving the login message $\langle CID_j, C_j, V_j, R_j, T_1\rangle$, B finds that T_1 is correct. B then computes $Z_j = T_s(C_j)$, $H_j = R_j \oplus Z_j$, $ID_j = CID_j \oplus (H_j \| T_1 \| Z_j)$, $V_j' = h(CID_j, C_j, H_j, R_j, T_1) = V_j$, and thus B accepts the login message $\langle CID_j, C_j, V_j, R_j, T_1\rangle$. As a result, U_a successfully impersonate the user U_j by login to the remote server B.

4.4. *Lack of session key forward secrecy*

In any key agreement protocol, the session key forward secrecy is an important security attributes that includes that none of the past or future session keys can be compromised even if the long-term private keys are disclosed. The forward secrecy problem in Lin's scheme [23] can be describes with the following operations:

Step 1. Assume that the private key s of the remote server B is disclosed to an adversary $\mathcal{A}$.

Step 2. The adversary $\mathcal{A}$ obtains the login message $\langle CID_a, C, V_a, R, T_1 \rangle$ and the response message $\langle V_s, T_2 \rangle$ in a session transmitted over a public channel. Here $H_a = h(s, ID_a)$, $Z = T_k(T_s(x))$, $CID_a = ID_a \oplus (H_a \| T_1 \| Z)$, $C = T_k(x)$, $R = H_a \oplus Z$ and $V_a = h(CID_a, C, H_a, R, T_1)$ and $V_s = h(\lambda, H_a, T_1, T_2)$.

Step 3. The adversary $\mathcal{A}$ computes $Z = T_s(C)$, $H_a = R \oplus Z$ and $ID_a = CID_a \oplus (H_a \| T_1 \| Z)$. With these information, $\mathcal{A}$ computes the session key as $\lambda = h(H_a, CID_a, V_a, T_1, T_2)$. Therefore, Lin's scheme is insecure against session key forward secrecy property.

5. Conclusion

With the security advantages and computation efficiencies of Chebyshev chaotic map over other cryptosystems, Lin [23] proposed a new dynamic identity-based authenticated key agreement protocol for mobile users. Although, the scheme is shown to be secure and efficient for practical use in resource-constrained environments, however, this paper cryptanalyzes and proves that Lin's scheme is impractical for practical use since (i) its login and password change phase cannot detect the wrong identity and password at user side, (ii) it is vulnerable to the user impersonation attack, and (iii) it cannot avoid the problem of session key forward secrecy. Therefore, the Lin's scheme is inefficient and unfriendly for practical applications.

References

[1] Chen, C., He, D., Chan, S., Bu, J., Gao, Y., Fan, R. (2011). Lightweight and provably secure user authentication with anonymity for the global mobility network. International Journal of Communication Systems, 24(3), 347-362.

[2] He, D., Chen, J., Zhang, R. (2011). A more secure authentication scheme for telecare medicine information systems. Journal of Medical Systems, 36(3), 1989-1995.

[3] Khan, M. K., Kim, S. K., Alghathbar, K. (2011). Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, 34(3), 305-309.

[4] Tang, H. B., Liu, X. S. (2012). Cryptanalysis of a dynamic ID-based remote user authentication with key agreement scheme. International Journal of Communication Systems, 25(12), 1639-1644.

[5] Tsai, J. L., Wu, T. C., Tsai, K. Y. (2010). New dynamic ID authentication scheme using smart cards. International Journal of Communication Systems, 23(12), 1449-1462.

[6] Wang, R. C., Juang, W. S., Lei, C. L. (2011). Robust authentication and key agreement scheme preserving the privacy of secret key. Computer Communications, 34(3), 274-280.

[7] Wang, Y. Y., Liu, J. Y., Xiao, F. X., Dan, J. (2009). A more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, 32(4), 583-585.

[8] Wang, Y. Y., Liu, J. Y., Xiao, F. X., Dan, J. (2009). A more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, 32(4), 583-585.

[9] Wen, F., Li, X. (2011). An improved dynamic ID-based remote user authentication with key agreement scheme. Computers and Electrical Engineering, 38(2), 381-387.

[10] Wu, S., Zhu, T., Pu, Q. (2011). Robust smart-cards-based user authentication scheme with user anonymity. Security and Communication Networks, 5(2), 236-248.

[11] Gong, P., Li, P., Shi,W. B. (2012). A secure chaotic maps-based key agreement protocol without using smart cards. Nonlinear Dynamics, 70(4), 2401-2406.

[12] He, D., Chen,Y., Chen, J. H. (2012).Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. Nonlinear Dynamics, 69(3), 1149-1157.

[13] Han, S. (2008). Security of a key agreement protocol based on chaotic maps. Chaos, Solitons & Fractals, 38(3), 764-768.

[14] Lee, C. C., Chen, C. L.,Wu, C.Y., Huang, S.Y. (2012).An extended chaotic maps-based key agreement protocol with user anonymity. Nonlinear Dynamics, 69(1-2), 79-87.

[15] Lee, C. C., Hsu, C.W. (2012). A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. Nonlinear Dynamics, 71(1-2), 201-211.

[16] Xiao, D., Liao, X., Deng, S. (2007).Anovel key agreement protocol based on chaotic maps. Information Sciences, 177(4), 1136-1142.

[17] Xue, K., Hong, P. (2012). Security improvement on an anonymous key agreement protocol based on chaotic maps. Communications in Nonlinear Science and Numerical Simulation, 17(7), 2969-2977.

[18] Xie, Q., Tu, X. (2013). Chaotic maps-based three-party password-authenticated key agreement scheme. Nonlinear Dynamics, 74, 1021-1027.

[19] Farash, M. S., Attari, M. A. (2014). An efficient and provably secure three-partypassword-based authenticated key exchange protocol based on Chebyshev chaotic maps. Nonlinear Dynamics. DOI 10.1007/s11071-014-1304-6.

[20] Xue, K., Hong, P. (2012). Security improvement on an anonymous key agreement protocol based on chaotic maps. Communications in Nonlinear Science and Numerical Simulation, 17, 2969-2977.

[21] Guo, Cheng, Chang, C-C. (2013). Chaotic maps-based password-authenticated key agreement using smart cards. Communications in Nonlinear Science and Numerical Simulation, 18, 1433-1440.

[22] Farash, M. S., Attari, M. A. (2014). Cryptanalysis and improvement of a chaotic map-based key agreement protocol using Chebyshev sequence membership testing. Nonlinear Dynamics. DOI 10.1007/s11071-013-1204-1

[23] Lin, H-Y. (2014). Chaotic Map Based Mobile Dynamic ID Authenticated Key Agreement Scheme. Wireless Personal Communications. DOI: 10.1007/s11277-014-1829-5

[24] Messerges, T. S., Dabbish, E. A., Sloan, R. H. (2012). Examining smart card security under the threat of power analysis attacks. IEEE Transactions on Computers, 51(5), 541-552.

[25] Joye, M., and Olivier, F. (2005). Side-channel analysis, Encyclopedia of Cryptography and Security. Kluwer Academic Publishers, pp. 571-576.

[26] Kocher, P., Jaffe, J., Jun, B. (1999). Differential power analysis. In: Proceedings of Advances in Cryptology (Crypto'99), LNCS, pp. 388-397).