Password Authenticated Key Exchange Protocol for Multi-Server Mobile Networks Based on Chebyshev Chaotic Map

Chien-Lung Hsu
Information Management
Chang-Gung University
Tao-Yuan, Taiwan (R.O.C.)
clhsu@mail.cgu.edu.tw

Tzu-Wei Lin
Information Management
Chang-Gung University
Tao-Yuan, Taiwan (R.O.C.)
elliot.lin49@gmail.com

Abstract—In a single-server mobile network, authorized users can dynamically login to the server for requiring internet services or resources. A password authenticated key exchange protocol can be used to authenticate user’s legitimacy and establish a secure communication between a user and a logon server by using his friendly memorized password. In generally, users can dynamically access internet resources and services from multiple servers via mobile networks. However, it is difficult for users and servers to easily and securely manage passwords and secret keys in multi-server mobile networks. This paper proposes a password authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map. Properties of the proposed protocol are given below. (i) The user can easily memorize a single password to login different servers without the assistance of a trusted registration authority. (ii) The user can share distinct secret information with different servers, and hence a malicious server cannot use it to masquerade as the user to login the other server(s). (iii) It is secure against some potential attacks. (iv) An authenticated key shared between the user and the server can be established for securing their communications. (v) It can provide key confirmation for the shared session key. (vi) It can provide higher security assurance in generating secret keys.

Keywords—multi-server; mobile network; cryptography; authenticate; password; Chebyshev chaotic map

I. INTRODUCTION

The Internet environment has become a single society in which all of the services required for daily living are implemented online nowadays [5]. The more mobile communication technology is being developed, the more people can take services they want through mobile devices whenever and wherever they are [8]. For such reasons, a user might register to several remote servers for requesting different services. In a mobile network, all messages are transmitted over the air and it might be suffered from some potential attacks, such as interception, masquerade, compromising attacks, etc. A password-based authenticated key exchange protocol can be used to provide the security assurance for mobile networks. It allows the user to login to server by using his memorized password and establish a secret key shared among them for securing subsequent communications. Multi-server mobile network has a fantastic property called mobility which means users can pass through multiple access points while maintaining progressional connections. This kind of network can provide users more diversified services. Namely, a user can login different servers through mobile network to obtain diversified services. If utilizing traditional password-based authenticated key exchange protocol to ensure security of multi-server wireless mobile network, we might face some problems: (1) A user has to manage more than one pairs of identifiers and passwords which might increase user’s load and risk of managing passwords. (2) In general cases, if user utilizes one single password to login different servers, we will need a registration center (RC) which must be trusted. In 2008, Tsai proposed a multi-server authentication protocol based on one-way hash function without verification table [10]. The user and server have both to authenticate with registration center before verifying each other. There are many protocols that utilize the similar methods for the past several years [2, 4, 6, 11, 12]. (3) A malicious server might masquerade as the user to login the other server(s). (4) The cost of logging in and establishing session key, such as computational complexity, storage, rounds, etc., is related to number of servers. In other words, the cost of our protocol is not related to how many servers there are.

For guaranteeing the security and confidentiality of subsequent transmission, a shared session key will be established after authenticated key exchange protocol. In 2012, Hsu et al. proposed a password-based authenticated key exchange protocol [3] with smart card, and the protocol has properties below: (1) It can be applied in the multi-servers architecture. (2) It can avoid attacks from malicious person in the registration center. (3) It can transfer information publically. (4) It can apply smart card. We will point out the vulnerabilities of Hsu et al.’s protocol [3] and demonstrate three kinds of attacks.

A chaotic system is characterized by sensitive dependence on initial conditions, pseudo-randomness and ergodicity. These features have excellent properties of diffusion and confusion which are important to cryptography, especially secret key cryptosystems [14]. In 2003, Kocarev et al. proposed a public key encryption protocol based on Chebyshev chaotic maps [7]. Because of the mathematical properties and characterizes of Chebyshev chaotic maps, it is more secure to utilize Chebyshev chaotic maps in public-key cryptosystems. Wang et al. have implemented it, and experimental results and performance analyses had been proved that it is secure and practical [13]. In 2005, Bergamo et al. [1] pointed out that Kocarev et al.’s protocol [7] is not secure because the adversary can recover the plaintext from
given ciphertext without any private key based on the periodicity of cosine function. In 2010, Wang et al. pointed out that some key agreement protocols based on chaos have several drawbacks as follows [13]: (1) Some protocols are vulnerable to Bergamo et al.’s proposed attack [1] because the periodicity of the cosine function makes public encryption. (2) Some protocols cannot resist man-in-the-middle attack or replay attack. (3) Some protocols did not provide mutual authentication of both communication sides. (4) Clock synchronization is difficult to achieve in some cases. (5) Because of sharing secret key between every two parties, it becomes difficult to distribute keys.

In this paper, we propose an authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map not only solving problems above but remaining some general properties, such as mutual authentication, session key establishment, no verification table, etc. We sketch the remaining organization of this paper below. In section II, we briefly review Hsu et al.’s protocol [3]; we demonstrate three kinds of attack in section III; we introduce our protocol in section IV; some security analyses are detailed in section V; finally, a conclusion is made in section VI.

II. REVIEW OF HSU ET AL.’S PROTOCOL

Hsu et al.’s protocol [3] is divided into four phases: the system initialization, the user registration, the authenticated key exchange and password changing phase. Some used notations are defined as Table 1.

<table>
<thead>
<tr>
<th>TABLE 1. NOTATIONS OF HSU ET AL.’S PROTOCOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notations</td>
</tr>
<tr>
<td>ID_{ui}</td>
</tr>
<tr>
<td>ID_{sj}</td>
</tr>
<tr>
<td>⊕</td>
</tr>
<tr>
<td>H(·)</td>
</tr>
<tr>
<td>PW_i</td>
</tr>
<tr>
<td>X_i</td>
</tr>
<tr>
<td>k</td>
</tr>
<tr>
<td>E_k(·)</td>
</tr>
<tr>
<td>D_k(·)</td>
</tr>
<tr>
<td>r</td>
</tr>
<tr>
<td>g, p, q</td>
</tr>
<tr>
<td>T</td>
</tr>
<tr>
<td>USB</td>
</tr>
</tbody>
</table>

In the system initialization phase, each user sets up his smart card by entering identifier and password into it. Let remote servers generate the following parameters according to the Digital Signature Algorithm (DSA) [9]: p and q are two large primes satisfying that q(p − 1); g is a generator of order q over GF(p). Figures 1, 2, and 3 illustrate these phases. Figure 1 illustrates the registration phase. Figure 2 illustrates the authenticated key exchange phase. User and server verify each other and establish session key in this phase. Figure 3 is password changing phase which can let user update the password of smart card.

III. THE PROPOSED ATTACKS ON HSU ET AL.’S PROTOCOL

Recall that the random number r of user and B server calculated are stored in portable USB device. If user loses the USB and the adversary gets it, the adversary might obtain B and r. If the password that the adversary guesses is match to user’s, the adversary can compute user’s A = H(PW_i) ⊕ H(r || ID_{sj}). Because B = u_i ⊕ A = H(ID_{ui} || X_i) ⊕ H(PW_i) ⊕ H(r || ID_{sj}), we can obtain u_i from u_i = B ⊕ A. The adversary can use u_i in the authenticated key exchange phase for online user impersonating, online server spoofing, and offline user impersonating attack. There are the details for the attacks below.
A. Online User Impersonating

If the adversary has the USB of legitimate user and obtains B and r, the adversary can guess a password $PW^*$, compute $u_i$ and the message with the same method, and send it to server. If the server verifies MAC successfully, server will use the adversary’s message to establish session key and send it to the adversary for authenticating without knowing the user has been impersonated. There is the detail below.

<table>
<thead>
<tr>
<th>Attacker $E_i$</th>
<th>Remote Server $S_j$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter $ID_{U_i}$, $PW_i^*$</td>
<td></td>
</tr>
<tr>
<td>2. $A^* = H(PW^*) \oplus H(r | ID_{S_j})$</td>
<td></td>
</tr>
<tr>
<td>3. $u_i^* = B \oplus A^*$</td>
<td></td>
</tr>
<tr>
<td>4. $V_A^i = g^{u_i^*} \mod p$</td>
<td></td>
</tr>
<tr>
<td>5. $e \in \mathbb{Z}_p^*$</td>
<td></td>
</tr>
<tr>
<td>6. $R_e = g^e \mod p$</td>
<td></td>
</tr>
<tr>
<td>7. $M_f = (R_e | ID_{U_i})$</td>
<td></td>
</tr>
<tr>
<td>8. $X_e = (R_e | H(M_f | T)) \oplus V_A^i$</td>
<td></td>
</tr>
</tbody>
</table>

9. $(ID_{U_i}, X_e)$

10. $u_i = H(ID_{U_i} \| X_e)$

11. $V_b = g^{u_i} \mod p$

12. $(R_A^* \| H(M_f \| T)) = X_e \oplus V_b$

13. $M_f^* = (R_A^* \| ID_{U_i})$ |

14. $MAC = (R_A^* \| H(M_f \| T^*))$

15. $MAC = (R_A^* \| H(M_f \| T) \oplus V_A^i)$

If MAC computed by server is match to the one of Step 13, it means that attacker guesses the password successfully, or the attacker has to go back to Step 10.

16. $b \in \mathbb{Z}_p^*$

17. $V_b = g^b \mod p$

18. $K = (R_A)^* \mod p$

19. $\beta = H(K \| ID_{U_i} \| ID_{S_j})$

20. $\theta = E_{S_j}(V_X^*, \beta)$ |

21. $(\theta)$

Figure 4. Online user impersonating attack at authenticated key exchange phase of Hsu et al’s protocol [3]

B. Online Server Spoofing

If the adversary has the USB of legitimate user and obtains $B$ and $r$, the adversary can guess a password $PW^*$, compute $u_i$ and use $u_i$ to compute $X_e^*$. If $X_e^* = X_e$, the adversary impersonates user successfully.

<table>
<thead>
<tr>
<th>User $U_i$</th>
<th>Attacker $E_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter $ID_{U_i}$, $PW_i^*$</td>
<td></td>
</tr>
<tr>
<td>2. $A = H(PW^*) \oplus H(r | ID_{S_j})$</td>
<td></td>
</tr>
<tr>
<td>3. $u_i = B \oplus A$</td>
<td></td>
</tr>
<tr>
<td>4. $V_A = g^u \mod p$</td>
<td></td>
</tr>
</tbody>
</table>

5. $a \in \mathbb{Z}_p^*$

6. $R_a = g^a \mod p$

7. $M_f = (R_a \| ID_{U_i})$

8. $X_e^* = (R_a \| H(M_f \| T)) \oplus V_A$

9. $(ID_{U_i}, X_e^*)$

10. $A^* = H(PW^*) \oplus H(r \| ID_{S_j})$

11. $u_i = B \oplus A^*$

12. $V_b = g^{u_i} \mod p$

13. $(R_A^* \| H(M_f \| T)) = X_e^* \oplus V_A$

14. $M_f^* = (R_A^* \| ID_{U_i})$

15. $MAC = (R_A^* \| H(M_f \| T))$

16. $MAC = (R_A^* \| H(M_f \| T^*))$

17. $b \in \mathbb{Z}_p^*$

18. $V_b = g^b \mod p$

19. $K = (R_A)^* \mod p$

Figure 5. Online server spoofing attack at authenticated key exchange phase of Hsu et al’s protocol [3]

C. Offline User Impersonating

The adversary eavesdrops on the message $(ID_{U_i}, X_e)$ from user and gets $X_e$ for authentication. If the adversary has the USB of legitimate user and obtains $B$ and $r$, the adversary can guess a password $PW_i^*$, compute $u_i$, and use $u_i$ to compute $X_e^*$. If $X_e^* = X_e$, the adversary impersonates user successfully.
IV. PROPOSED PROTOCOL

We propose an authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map. We will introduce some mathematical theory and our protocol below.

A. Chebyshev chaotic map

This section describes the Chebyshev chaotic map, which has semi-group property [14].

Definition 1 (Chebyshev polynomials). Let \( n \) be an integer, and let \( x \) be a variable taking values over the interval \([-1, 1]\). Chebyshev polynomial maps \( T_{n} : R \rightarrow R \) of degree \( n \) is defined using the following recurrent relation:

\[
T_{n}(x) = 2xT_{n-1}(x) - T_{n-2}(x),
\]

where \( n \geq 2 \), \( T_0(x) = 1 \), and \( T_1(x) = x \).

The first few Chebyshev polynomials are:

\[
T_2(x) = 2x^2 - 1, \quad T_3(x) = 4x^3 - 3x, \quad T_4(x) = 8x^4 - 8x^3 + 1.
\]

The interval \([-1, 1]\) is invariant under the action of the map \( T_{n} \) : \( T_{n}([-1, 1]) \rightarrow [-1, 1] \). Therefore, the Chebyshev polynomial restricted to the interval \([-1, 1]\) is a well-known chaotic map for all \( n > 1 \). It has a unique absolutely continuous invariant measure with positive Lyapunov exponent \( \ln n \). For \( n = 2 \), the Chebyshev map reduces to the well-known logistic map.

Definition 2 Let \( n \) be an integer, and let \( x \) be a variable taking values over the interval \([-1, 1]\). The polynomial \( T_{n}(x) : [-1, 1] \rightarrow [-1, 1] \) is defined as:

\[
T_{n}(x) = \cos(n \cos^{-1}(x)).
\]

Definition 3 (Semi-group property). One of the most important properties of Chebyshev polynomials is the so called semi-group property which establishes that:

\[
T_{r}(T_{s}(x)) = T_{rs}(x).
\]

An immediate consequence of this property is that Chebyshev polynomials commute under composition

\[
T_{n}(x) = 2xT_{n-1}(x) - T_{n-2}(x) \pmod{N},
\]

with \( n \geq 2 \), \( x \in (-\infty, +\infty) \), and \( N \) is a large prime number. Obviously,

\[
T_{rs}(x) = T_{r}(T_{s}(x)) = T_{s}(T_{r}(x)),
\]

so the semi-group property still holds and the enhanced Chebyshev polynomials also commute under composition.

B. Proposed protocol

Our protocol is divided into four phases: the system initialization, the user registration, the authenticated key exchange and password changing phase. Some used notations are defined as Table 2.

<table>
<thead>
<tr>
<th>TABLE II. NOTATIONS OF OUR PROTOCOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notations</td>
</tr>
<tr>
<td>( ID )</td>
</tr>
<tr>
<td>( SID )</td>
</tr>
<tr>
<td>( \oplus )</td>
</tr>
<tr>
<td>( HF(\cdot) )</td>
</tr>
<tr>
<td>( PW )</td>
</tr>
<tr>
<td>( x_{j} )</td>
</tr>
<tr>
<td>( k )</td>
</tr>
<tr>
<td>( E_{k}(\cdot) )</td>
</tr>
<tr>
<td>( D_{k}(\cdot) )</td>
</tr>
<tr>
<td>( r_{i} )</td>
</tr>
<tr>
<td>( b_{0}(\cdot) )</td>
</tr>
<tr>
<td>( USB )</td>
</tr>
<tr>
<td>( s )</td>
</tr>
<tr>
<td>( r_{i} )</td>
</tr>
</tbody>
</table>

In the system initialization phase, each user sets up his smart card by entering identifier and password into it. Figures 7, 8, and 9 illustrate these phases. Figure 7 illustrates the registration phase. Figure 8 illustrates the authenticated key exchange phase. User and server verify each other and establish session key in this phase. Figure 9 is password changing phase which can let user update the password of smart card offline.
In Hsu et al.’s protocol [3], user’s random number $\mathit{yi}$ and $s$ into message authentication code, they can confirm that the message is resent or not by checking information on the message authentication code. As a result, the proposed protocol can resist man-in-the-middle attack.

E. Resistant to replay attack

In the proposed protocol, we use random numbers $\mathit{yi}$ and $s$ to resist replay attack. Because two parties of the communication can put session key $\mathit{k}_i = \mathit{T}_y(x_i)$ and random numbers $\mathit{yi}$ and $s$ into message authentication code, they can confirm that the message is resent or not by checking information on the message authentication code. As a result, the proposed protocol can resist replay attack.

F. User anonymity

User’s identity is protected by encrypting it as $\mathit{Ci} = \mathit{E}_{\mathit{Ki}}(\mathit{ID}_i, \mathit{bi}, x_i)$ before sending it. $\mathit{ID}_i$ is encrypted in $\mathit{Ci}$ with $\mathit{K}_i$, and server has to obtain $\mathit{K}_i$ first by computing $\mathit{K}_i = T_i \oplus$
The adversary cannot get $ID_i$ even he gets $R_i$ and $C_i$, because only server knows the secret $x_{S_j}$. The adversary cannot obtain $K_i$ without knowing $x_{S_j}$ and decrypt $C_i$, so he cannot get $ID_i$, either. As a result, the proposed protocol can satisfy user anonymity on communication.

VI. CONCLUSIONS

We proposed an authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map, and the proposed protocol can resist some probable attacks and drawbacks at previous research, and it can also provide user anonymity. We proposed security analysis of Hsu et al.’s [3] protocol and describe the attack scenario first. Then, we proposed the enhanced protocol and analyzed security. Moreover, the proposed protocol is based on Chebyshev chaotic map, so it is more practical and efficient. Properties of the proposed protocol are given below. (i) The user can easily memorize a single password to login different servers without the assistance of a trusted registration authority. (ii) The user can share distinct secret information with different servers, and hence a malicious server cannot use it to masquerade as the user to login the other server(s). (iii) It is secure against some potential attacks. (iv) An authenticated key shared between the user and the server can be established for securing their communications. (v) It can provide key confirmation for the shared session key. (vi) It can provide higher security assurance in generating secret keys.

VII. ACKNOWLEDGMENT

We would like to thank anonymous referees for their valuable suggestions. This work was supported in part by National Science Council under the grants NSC 100-2628-H-182-001-MY3.

REFERENCES


