Cryptanalysis of a secure dynamic ID based remote user authentication scheme for multi-server environment

Te-Yu Chen
Department of Computer Science and Engineering
National Chung Hsing University
250 Kuo Kuang Road, Taichung 402, Taiwan
phd9211@cs.nchu.edu.tw

Cheng-Chi Lee
Department of Photonics and Communication Engineering
Asia University
500 Lioufeng Road, Wufeng Shiang, Taichung 413, Taiwan
cclee@asia.edu.tw

Min-Shiang Hwang*
Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road, Taichung 402, Taiwan
mshwang@nchu.edu.tw

Jinn-Ke Jan
Department of Computer Science and Engineering
National Chung Hsing University
250 Kuo Kuang Road, Taichung 402, Taiwan
jkjan@cs.nchu.edu.tw

*Corresponding author: Min-Shiang Hwang

Abstract—The conventional user authentication scheme is designed for a single-sever environment. In the case of multiple servers, a user must register with each server individually, and memorize different pairs of identities and passwords to login to each one. This approach is inconvenient and impractical for a multi-server environment. Therefore, various user authentication schemes for multi-server environments have been proposed. In these schemes, a user only needs to register with the registration center once, and then he/she will be allowed to login to any server in this system. Recently, Liao and Wang proposed a dynamic ID-based remote user authentication scheme for multi-server environments. However, some flaws have been identified in their scheme. This paper demonstrates that anyone with relevant server access not only can derive each session key agreed upon between any user and any server, but he/she also can masquerade as any user to login to whichever server in this system.

Keywords—cryptography; cryptanalysis; authentication; password; multi-server; session key; smart card;

I. INTRODUCTION

With the rapid development of network technologies, increasing numbers of services are provided through the Internet instead of the traditional manners. Owing to the openness of the Internet, method of guarding valuable resources from unauthorized access is an essential part of network security infrastructures. A user authentication scheme is a mechanism used by a server to authenticate the user before he/she is allowed to access the service. A considerable number of user authentication schemes have been proposed, as in [1], [3], [4], [6], [8], [13], [16], [17], [18], [19], [23]. However, these conventional schemes designed for a single-sever environment are not suitable for multi-server systems. If a conventional authentication scheme is applied to a multi-server system, a user must register with each server separately, and memorize all different pairs of identities and passwords which he/she uses to login to the corresponding servers. This approach becomes inconvenient and impractical. Therefore, as the amounts of multi-server systems in the distributed environment increase, more user authentication schemes for multi-server environments are proposed [2], [5], [7], [11], [12], [14], [15], [20], [21], [22].

In general, there are three kinds of participants in a user authentication scheme for a multi-server system: users, a group of servers, and the registration center. If a user wants to enroll in a multi-server system, he/she must register with the registration center instead of with each server individually. After the registration, the user is allowed to login to any server in this system.

As mentioned in [7], a user authentication scheme for a multi-server system should meet the following basic criteria: single registration, no verification table, freely chosen password, efficiency, mutual authentication, and session key agreement. In addition to these basic criteria given above, the following security criteria should be further examined [5], [7], [20]: session key security; known-key security; forward secrecy; and resistance to well-known attacks such as insider attack, impersonation attack, replay attack, password guessing attack, stolen-verifier attack, and server spoofing attack.

In 2001, Li et al. [11] proposed a remote password authentication scheme for the multi-server architecture utilizing neural networks. Introducing neural networks into the scheme was novel, but to train and maintain neural networks would take a great deal of time. Moreover, their scheme could not resist password guessing attacks and insider attacks [9]. Therefore, Lin [14] proposed a modified scheme to remedy these vulnerabilities. Nevertheless, neither
That is, an insider from any server who obtains the secret appropriate for specific applications such as e-commerce. Hence, the scheme is vulnerable to the insider attack and could not provide forward secrecy. Chang and Kuo [2] proposed another authenticated key agreement protocol based on the Chinese Remainder Theorem and a modulus table in 2005. Huang and Shiau [5] showed that both [7] and [2] lacked of explicit key authentication and were inefficient with respect to communication costs. Hence, they proposed an improved authenticated key agreement protocol based on the line of geometry. However, Huang and Shiau’s scheme still lacks of forward secrecy, and each server must maintain a user table.

Recently, Liao and Wang [12] proposed a dynamic ID based remote user authentication scheme for a multi-server environment. They utilized a dynamic ID instead of a static ID to achieve user anonymity. Hence, the scheme is appropriate for specific applications such as e-commerce. However, their scheme is not secure. This paper demonstrates that their scheme is vulnerable to the insider attacks. That is, an insider from any server who obtains the secret values $h(x)$ and $y$ not only can derive each session key agreed upon between any user and any server, but he/she also can masquerade as any user to login to any server in this system.

The remaining sections of this paper are organized as follows. Section 2 reviews Liao and Wang’s scheme. Then, cryptanalysis of Liao and Wang’s scheme is presented in Section 3. Finally, Section 4 concludes this paper.

II. REVIEW OF LIAO AND WANG’S SCHEME

The dynamic ID based remote user authentication scheme for multi-server environments proposed by Liao and Wang is reviewed in this section. There are three types of participants in the user authentication scheme for multi-server environments: the users, the servers, and the registration center. Liao and Wang’s scheme is composed of four phases: the registration phase, the login phase, the mutual verification and session key agreement phase, and the password change phase. The details of the four phases in their scheme are illustrated as follows:

[Registration phase]

This phase is initiated by a user whenever he/she wants to enroll in the multi-server system. The user $U_i$ submits his/her identity $ID_i$ and password $PW_i$ to the registration center $RC$. Then the registration center $RC$ performs the following steps:

1. The registration center $RC$ uses its master secret key $x$ to compute $T_i = h(ID_i||x)$, $V_i = T_i \oplus h(ID_i||PW_i)$, $B_i = h(PW_i) \oplus h(x)$, and $H_i = h(T_i)$.

2. The registration center $RC$ loads $(V_i, B_i, H_i, h(), y)$ into a smart card and issues the smart card to the user $U_i$ through a secure channel. In addition, the registration center $RC$ securely distributes the secret keys, $h(x)$ and $y$, among the servers in this system.

[Login phase]

This phase is invoked while a user $U_i$ wants to access the resources provided by a server $S_j$. The user $U_i$ inserts his/her smart card into the terminal, and he/she enters his/her identity $ID_i$, password $PW_i$, and the server identity $SID_j$ in order to login to the server. Then, the smart card performs the following steps:

1. The smart card computes $T_i = V_i \oplus h(ID_i||PW_i)$, $H_i = h(T_i)$, and then checks $H_i$ by comparing the computed value with the value stored on the smart card. If they are not equivalent, the smart card terminates this session; otherwise, the smart card performs the following steps.

2. The smart card randomly selects a nonce $N_i$ and computes $CID_i = h(PW_i) \oplus h(T_i||y||N_i)$, $P_{ij} = T_i \oplus h(y||N_i||SID_j)$, and $Q_i = h(B_i||y||N_i)$.

3. Finally, the smart card sends the login request message $\{CID_i, P_{ij}, Q_i, N_i\}$ to the server $S_j$.

[Mutual verification and session key agreement phase]

The server $S_j$ and the user $U_i$ authenticate each other and agree on a session key $SK$ in this phase. While receiving the login request message from the user $U_i$, the server $S_j$ performs the following steps:

1. The server computes $T_i = P_{ij} \oplus h(y||N_i||SID_j)$, $h(PW_i) = CID_i \oplus h(T_i||y||N_i)$, and $B_i = h(PW_i) \oplus h(x)$.

2. The server $S_j$ verifies whether $h(B_i||y||N_i) = Q_i$ holds. If it fails, the server $S_j$ rejects the login request and terminates this session; otherwise, the server $S_j$ proceeds with the following steps.

3. The server $S_j$ randomly selects a nonce $N_j$ and computes $M_{ij1} = h(B_i||y||N_i||SID_j)$, and then sends back the acknowledgement message $\{M_{ij1}, N_j\}$ to the user $U_i$.

While receiving the acknowledgement message $\{M_{ij1}, N_j\}$, the user $U_i$ performs the following steps:

4. The user $U_i$ verifies whether $h(B_i||y||N_i||SID_j) = M_{ij1}$ holds. If it fails, the user $U_i$ interrupts this session and aborts the following procedures.

5. The user $U_i$ computes $M_{ij2} = h(B_i||y||N_j||SID_j)$, and sends $\{M_{ij2}\}$ back to the server $S_j$.

6. While receiving the message $\{M_{ij2}\}$, the server $S_j$ verifies whether $h(B_i||y||N_j||SID_j) = M_{ij2}$ holds. If it holds, the user $U_i$ and the server $S_j$ complete the mutual authentication.

Once the user $U_i$ and the server $S_j$ have mutually authenticated, they both compute $SK = h(B_i||y||N_i||N_j||SID_j)$.
as their session key individually.

[Password change phase]

When the user $U_i$ wants to update his/her password from $PW_i$ to $PW_i'$, he/she inserts his/her smart card into a terminal and inputs his/her identity and old password $PW_i$. The smart card first verifies the legality of the cardholder by performing step 1 of the login phase. Once the identity of the cardholder has been proven, the smart card allows the cardholder to input a new password $PW_i'$. The smart card updates $V_i$ and $B_i$ with $V_i' = T_i \oplus h(ID_i||PW_i) \oplus h(ID_i||PW_i')$ and $B_i' = B_i \oplus h(PW_i) \oplus h(PW_i')$ respectively.

III. CRYPTANALYSIS OF LIAO AND WANG’S SCHEME

In a multi-server system, there are numerous servers distributed over the system. If a user authentication scheme for the multi-server system is unable to resist malicious insiders, any malicious insider from a given server may be harmful to the whole system. This will make the system high-risk. Therefore, an insider attack is a serious threat to a user authentication scheme for a multi-server system.

This section shows that if there is a malicious insider, Liao and Wang’s scheme is vulnerable to impersonation attack and the agreed session key between the user and the server is not secure. Anyone who obtains the secret keys, $h(x)$ and $y$, not only can derive all session keys between the user and the server, but he/she also can masquerade as any user to login to any server successfully.

A. Impersonation attack

An attacker who knows the secret keys, $h(x)$ and $y$, can eavesdrop on the login request messages, $\{CID_i, P_{ij}, Q_i, N_i\}$, transmitted from the user $U_i$ to the server $S_j$. This attacker is then able to counterfeit messages to masquerade as the user $U_i$ to login to any server in the system. The following steps can be performed by the attacker to masquerade as the user $U_i$ to login to a server $S_k$.

StepI. The attacker performs the following computation to obtain the information of $U_i$ using the eavesdropped login request message, $\{CID_i, P_{ij}, Q_i, N_i\}$, and the secret keys, $h(x)$ and $y$.

$$T_i = P_{ij} \oplus h(y||N_i||SID_j)$$
$$h(PW_i) = CID_i \oplus h(T_i||y||N_i)$$
$$B_i = h(PW_i) \oplus h(x)$$

StepII. With the secret keys, $h(x)$ and $y$, as well as the values $T_i$, $h(PW_i)$, and $B_i$ computed in the above step, the attacker chooses a random number $N_i'$ and computes $CID_i'$, $P_{ik}$, and $Q_i'$ as follows.

$$CID_i' = h(PW_i) \oplus h(T_i||y||N_i')$$
$$P_{ik} = T_i \oplus h(y||N_i'||SID_k)$$
$$Q_i' = h(B_i||y||N_i')$$

Subsequently, the attacker sends the login request message $\{CID_i', P_{ik}, Q_i', N_i'\}$ to the server $S_k$. Obviously, the login request message can pass through the verification of steps 1, 2, and 3 in mutual verification phase performed by the server $S_k$. After the verification, the server $S_k$ will send the acknowledgement message $\{M_{ik_2}, N_k\}$ to the attacker.

StepIII. Upon receiving the acknowledgement message $\{M_{ik_2}, N_k\}$, the attacker computes $M_{ik_2}$ as the following.

$$M_{ik_2} = h(B_i||y||N_k||SID_k)$$

Afterwards, the attacker responds with the message $\{M_{ik_2}\}$ to the server $S_k$. Evidently, the message $\{M_{ik_2}\}$ is qualified to the verification of step 6 in mutual verification phase performed by the server $S_k$.

Interacting with the server $S_k$ by performing the steps illustrated above, the attacker will fool the server $S_k$ into believing that the attacker is a legitimate user. Moreover, the attacker and the server $S_k$ will agree on the same session key $SK = h(B_i||y||N_i'||N_k||SID_k)$. Hence the attacker gains his/her purpose in masquerading as a legitimate user.

B. Disclosure of session key

In Liao and Wang’s scheme, an attacker who obtains the secret keys, $h(x)$ and $y$, can derive all the session keys between any user and any server. The following steps shows how the attacker who knows the secret keys, $h(x)$ and $y$, derives the session key between a user $U_i$ and a server $S_k$.

StepI. The attacker eavesdrops the login request message $\{CID_i, P_{ik}, Q_i, N_i\}$ and the acknowledgement message $\{M_{ik_1}, N_k\}$ which are transmitted between the user $U_i$ and the server $S_k$.

StepII. With the eavesdropped login request message, $\{CID_i, P_{ik}, Q_i, N_i\}$, as well as the secret keys, $h(x)$ and $y$, the attacker can get $B_i$ by performing the following computations.

$$T_i = P_{ij} \oplus h(y||N_i||SID_k)$$
$$h(PW_i) = CID_i \oplus h(T_i||y||N_i)$$
$$B_i = h(PW_i) \oplus h(x)$$

StepIII. With the intercepted nonces, $N_i$, $N_k$, as well as the secret key $y$ and the data $B_i$ computed in Step II, the attacker can compute the session key $SK$ agreed between the user $U_i$ and the server $S_k$ as below.

$$SK = h(B_i||y||N_i||N_k||SID_k)$$

Therefore, the mechanism of the session key agreement in Liao and Wang’s scheme does not meet the security requirement.

IV. CONCLUSIONS

Liao and Wang proposed a dynamic ID based remote user authentication scheme for multi-server environments. However, their scheme is not secure. This paper shows that the scheme is vulnerable to the insider attacks. In a
multi-server system, there are numerous servers distributed over the system. If a user authentication scheme for the multi-server system is unable to resist an insider attack, any malicious insider who infiltrates the servers may be harmful to the whole system. Therefore, insider attacks on the user authentication scheme for multi-server systems deserve serious consideration.

REFERENCES


