Security Analysis of A Remote User Authentication Protocol by Liao and Wang

Dang Nguyen Duc*,[a], Kwangjo Kim[a]

[a] *Auto-ID Lab Korea, Department of Information and Communications Engineering, KAIST, 119 Munjiro, Yuseong-gu, Daejeon, 305-732, Republic of Korea*
Phone: +82-42-866-6236, Fax: +82-42-866-6273

Abstract

In Elsevier's journal of Computer Standards & Interfaces, 2007, Liao and Wang proposed an authentication protocol using smart card and claimed that their protocol provides security against replay attacks, active attacks and insider attacks. In addition, they argued that user anonymity is guaranteed. In this paper, we point out that Liao-Wang protocol is vulnerable to an insider attack by presenting a simple method for a malicious server to impersonate any user authenticating to the server. We also demonstrate that user anonymity can be violated as colluding servers can easily track activities of users.

Key words: Authentication, Smartcard, Anonymity, Insider Attack, Cryptanalysis

1. Introduction

Liao and Wang proposed an authentication protocol using smartcard [1] (hereafter, referred to as Liao-Wang protocol) which also serves as a session key establishment protocol. Liao-Wang protocol uses a secure cryptographic hash function as its building block which can be implemented easily on low-cost hardware including smartcard. The following security properties of Liao-Wang protocol were claimed:

- Mutual authentication between users and service providers is secure against replay attacks, service provider spoofing attacks and insider attacks.
- The privacy of a user is strictly protected.

*Corresponding author
Email addresses: nguyenduc@icu.ac.kr (Dang Nguyen Duc), kkj@cs.kaist.ac.kr (Kwangjo Kim)

This paper was submitted to Elsevier's journal of Computer Standards & Interfaces but rejected because the editors thought the paper was out of the scope of the journal.

- The session establishment protocol is secure against known-key attack. In addition, the security of past-session keys is guaranteed even if the master secret of the registration center is compromised. This property is called forward security.

In this paper, we analyze the security of Liao-Wang protocol and find that their protocol is not secure against insider attack as claimed by the authors. In addition, we point out that the privacy of a user can be violated if the user does not update his password after every session. We think that it is important to report security flaws of a cryptographic protocol that claims to be secure so that it will not misused. More importantly, our attack shows that one must design a cryptographic protocol carefully, especially when considering the balance between security and efficiency. In the case of Liao-Wang protocol, the authors avoided using more functional but computationally expensive cryptographic primitives like block ciphers and public key cryptography so that the protocol can be implemented on smartcard. However, as we will see later in our analysis, using hash function alone fails to deliver security properties promised by Liao-Wang protocol.

2. Liao-Wang Authentication Protocol

In this Section, we briefly review Liao-Wang protocol using the same notations used in [1].

Notation	Description
U_i	The i-th user
S_j	The j-th user
RC	The registration center
ID_i	Unique identification of U_i
PW_i	Unique password of U_i
SID_j	Unique identification of S_j
CID_i	Dynamic ID of U_i
$h(.)$	A one-way hash function
x	The master secret of RC
y	The secret shared between RC and each server
SK	The shared session key between an user and a server

Table 1: Notations

In Liao-Wang protocol, there are three types of entities: user, server and registration center. The registration center is a trusted party and in charge of issuing a smartcard for each user. The smartcard issuing process for the user U_i is proceeded as follows: after user U_i submitting his ID_i and PW_i, RC builds a smartcard with a 5-tuple $(V_i, B_i, H_i, h(.), y)$ where $V_i = h(ID_i||x) \oplus h(ID_i||PW_i)$, $B_i = h(PW_i) \oplus h(x)$ and $H_i = h(h(ID_i||x))$. The smartcard is then sent to the user via a secure channel.

When the user U_i wants to access services provided by the server S_j, he submits his identity, ID_i, password, PW_i and the identity of the server SID_j to his smartcard. The smartcard first verifies the user be checking if $H_i =$

$h(V_i \oplus h(ID_i||PW_i))$. If the verification succeeds, the smartcard initiates an authentication and key establishment session with the server which is illustrated in Fig. 1.

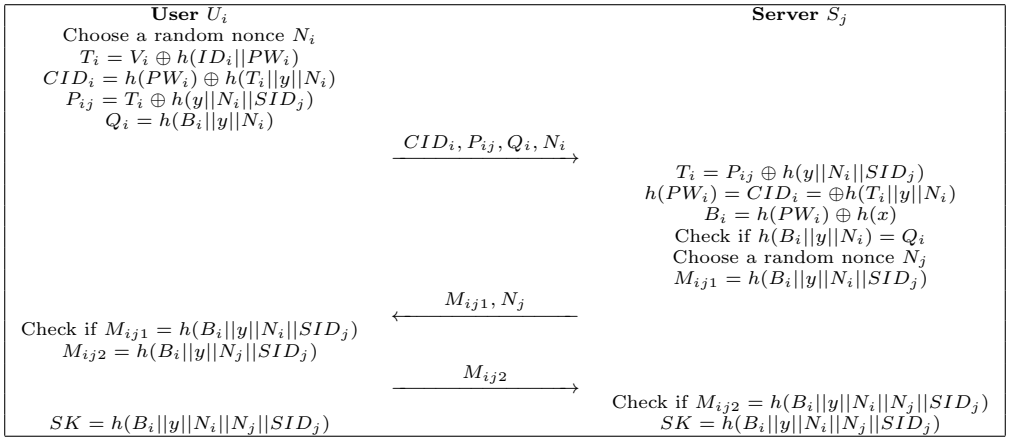

Figure 1: Liao-Wang Remote User Authentication Protocol

3. Security Analysis of Liao-Wang protocol

Remark. Note that, Liao and Wang did not specify clearly how a server obtains $h(x)$. As the secret x is required to issue a smartcard, x must not be available to any entity rather than the registration center. Therefore, a server cannot know the secret x which seems to contradict to what is described in [1]. We think that $h(x)$ should be available to a server as a secret information in Liao-Wang protocol. Indeed, Liao and Wang argued that their proposed protocol is secure against insider attacks because when a server is compromised, only $h(x)$ is revealed. However, we will show that by knowing the value of $h(x)$ only, not x itself, it is sufficient for a server to impersonate any user connecting to the server.

3.1. An insider attack on Liao-Wang protocol

We present here an insider attack allowing any malicious server to create a customized smartcard to impersonate any user connecting to it. We observed that all the information required to compute a valid login request message of the user U_i, *i.e.,* $(CID_i, P_{ij}, Q_i, N_i)$, are available to the server S_j. Those information include T_i, $h(PW_i)$, y, B_i and N_i. Consequently, the server S_j can create a cloned smartcard containing the following 5-tuple: $(T_i, B_i, h(PW_i), h(.), y)$ which is sufficient to successfully complete an authentication session to any server on behalf of the user U_i.

As specified in Liao-Wang protocol, a user has to be authenticated by his smartcard first. However, the cloned smartcard can be manufactured to accept

any ID and password or skip this verification process entirely. An attacker can impersonate the user U_i when authenticating to a server S_k by using a cloned smartcard as follows:

- The cloned smartcard skips user-to-smartcard authentication phase and computes the login request message $CID_i = h(PW_i) \oplus h(T_i||y||N_i)$, $P_{ik} = T_i \oplus h(y||N_i||SID_k$ and $Q_i = h(B_i||y||N_i)$ where N_i is generated at random. The login request message $(CID_i, P_{ik}, Q_i, N_i)$ will be correctly verified by the server S_k because it is computed exactly like the legitimate smartcard would do.

- When the server S_k replies with (M_{ik1}, N_k), the cloned smartcard can compute the key confirmation message $M_{ik2} = h(B_i||y||N_k||SID_k)$. Then, it can derive the shared session key $SK = h(B_i||y||N_i||N_k||SID_k)$.

The important flaw in the design of Liao-Wang protocol is that after the smartcard successfully verifies the user given the user's ID and password, the smartcard does not explicitly make use of the user's password, but the hashed password. Unfortunately, the hashed password can be computed by the server. This leads to separation between user-to-smartcard and smartcard-to-server authentication. Another issue with Liao-Wang protocol is that it does not follow the conventional structure of an authentication protocol in which the server should first send a random challenge and then the user responses with its login message derived from the server's challenge and the user's password. That so called challenge-response approach is widely used in cryptographic literature. Sadly, the authors of [1] failed to take into account those vast previous works.

3.2. Tracking a user in Liao-Wang protocol

Even though in Liao-Wang protocol, the identities of its users are not revealed to any server, users are still subject to different aspects of privacy invasion called tracking. As a server can compute $h(PW_i)$ for the user U_i and $h(PW_i)$ is likely unique among all users, the server can use this value to track the user U_i activities inside the server. When multiple malicious servers collude, they can even build preferences, track movements of users, *etc.* To prevent this attack, a user is required to update his password after every authentication session. But this is very inconvenient and unlikely to happen in practice.

4. Concluding Remark

In this paper, we have shown that Liao-Wang authentication protocol with smartcard does not achieve the security properties claimed by the authors. In particular, we pointed out that the protocol is not secure against insider attacks. In addition, the protocol does not provide strong user privacy protection. Our attack shows that a cryptographic protocol must be designed carefully such that security is not sacrificed for the sake of efficiency.

References

[1] Y.-P. Liao, S.-S. Wang, *A Secure dynamic ID based remote user authentication scheme for multi-server environment*, Computer Standards and Interfaces (2007), doi:10.1016/j.csi.2007.10.007.