韓國컴퓨터情報學會 論文誌
第15卷 第1號, 2010. 1.

2010-15-1-3-4

Cryptanalysis and Enhancement of a Remote User Authentication Scheme Using Smart Cards

Youngsook Lee*, Dongho Won**

스마트카드를 이용한 사용자 인증 스킴의 안전성 분석 및 개선

이 영 숙*, 원 동 호**

Abstract

A remote user authentication scheme is a two-party protocol whereby an authentication server in a distributed system confirms the identity of a remote individual logging on to the server over an untrusted, open network. In 2005, Liao et al. proposed a remote user authentication scheme using a smart card, in which users can be authenticated anonymously. Recently, Yoon et al. have discovered some security flaws in Liao et al.'s authentication scheme and proposed an improved version of this scheme to fix the security flaws. In this article, we review the improved authentication scheme by Yoon et al. and provide a security analysis on the scheme. Our analysis shows that Yoon et al.'s scheme does not guarantee not only any kind of authentication, either server-to-user authentication or user-to-server authentication but also password security. The contribution of the current work is to demonstrate these by mounting two attacks, a server impersonation attack and a user impersonation attack, and an off-line dictionary attack on Yoon et al.'s scheme. In addition, we propose the enhanced authentication scheme that eliminates the security vulnerabilities of Yoon et al.'s scheme.

요 약

사용자 인증 스킴은 개방된 통신환경에서 원격지에 있는 사용자가 서버에 로긴할 때 정당한 사용자 인지를 확인하는 것이다. 2005년 Liao등은 스마트 카드를 이용해서 사용자의 익명성을 보장하는 사용자 인증 스킴을 제안하였다. 최근 Yoon등은 Liao가 제안한 사용자 인증 스킴의 안전성 분석을 수행한 후 그 스킴에 존재하는 결점을 보완하는 향상된 스킴을 제안하였다. 그러나 안타깝게도 그들이 제안한 스킴은 사용자가 서버를 인증하는 방식과 서버가 사용자를 인증 방식을 모두 수행할 수 없고 패스워드의 안전성에도 문제점이 존재한다. 이러한 문제점을 이 논문에서는 서버 가장 공격, 사용자 가장 공격, 오프라인 사전공격을 수행하여 지적하였다. 아울러 본 논문에서는 Yoon등이 제안한 논문의 취약점을 제거하여 보다 안전한 사용자 인증 스킴을 제안하였다.

▸ Keyword : Authentication scheme; User anonymity; Impersonation attack; Off-line dictionary attack

• 제1저자 : 이영숙 교신저자 : 원동호
• 투고일 : 2009. 11. 23, 심사일 : 2009. 12. 02, 게재확정일 : 2010. 01. 26.

* 호원대학교 사이버수사 경찰학부 전임강사 ** 성균관대학교 전기전자컴퓨터공학부 교수

※ 이 논문은 2010년 호원대학교 연구비 지원을 받은 것임.

Ⅰ. Introduction

The feasibility of password-based user authentication in remotely accessed computer systems was explored as early as the work of Lamport [1]. Due in large part to the practical significance of password-based authentication, this initial work has been followed by a great deal of studies and proposals, including solutions using multi-application smart cards [2,3,4,5,6,7]. In a typical password-based authentication scheme using smart cards, remote users are authenticated using their smart card as an identification token; the smart card takes as input a password from a user, recovers a unique identifier from the user-given password, creates a login message using the identifier, and then sends the login message to the server who then checks the validity of the login request before allowing access to any services or resources. This way, the administrative overhead of the server is greatly reduced and the remote user is allowed to remember only his password to log on. Besides just creating and sending login messages, smart cards support mutual authentication where a challenge-response interaction between the card and the server takes place to verify each other's identity. Mutual authentication is a critical requirement in most real-world applications where one's private information should not be released to anyone until mutual confidence is established [8,9].

The experience has shown that the design of secure authentication schemes is not an easy task to do, especially in the presence of an active adversary; there is a long history of schemes for this domain being proposed and subsequently broken by some attacks (e.g., [10,11,12,13,14,7,15,16]). Therefore, authentication schemes must be subjected to the strictest scrutiny possible before they can be deployed into an untrusted, open network, which might be controlled by an adversary.

To analyze the security of remote user authentication schemes using smart cards, we need to consider the capabilities of the adversary. First, we assume that the adversary has complete control of every aspect of all communications between the server and the remote user. That is, he/she may read, modify, insert, delete, replay and delay any messages in the communication channel. Second, he/she may try to steal a user's smart card and extract the information in the smart card by monitoring the power consumption of the smart card [17,18]. Third, he/she may try to find out a user's password. Clearly, if both (1) the user's smart card was stolen and (2) the user's password was exposed, then there is no way to prevent the adversary from impersonating the user. However, a remote user authentication scheme should be secure if only one of (1) and (2) is the case. So the best we can do is to guarantee the security of the scheme when either the user's smart card or its password is stolen, but not both. This security property is called two-factor security.

In 2004, Das et al. [19] proposed a remote user authentication scheme in which users may send a login request message without disclosing their identities. In addition to providing user anonymity, this scheme exhibits various other merits: (1) it does not require the server to maintain a password table for verifying the legitimacy of login users; (2) it allows users to choose and change their passwords according to their liking and hence gives more user convenience; and (3) it is extremely efficient in terms of the computational cost since the protocol participants perform only a few hash function operations.

However, Liao et al. [20] have pointed out that Das et al.'s scheme is vulnerable to a password guessing attack; an attacker can easily find out the password of some registered user simply by eavesdropping a login request message of the user. To fix this security vulnerability, Liao et al. have presented a modified version of Das et al.'s scheme, and have claimed, among others, that their modified version achieves mutual authentication between the server and remote users. But, Yoon et al. [21] have recently discovered that Liao et al.'s modification does not achieve any kind of authentication, either server-to-user authentication or user-to-server authentication, and then presented an improved version of Liao et al.'s scheme in order to fix the security problems. However, in this article, we uncover that Yoon et al.'s scheme provides neither mutual authentication between a remote individual and the server nor password security. We show these by mounting two impersonation attacks, a server impersonation attack and a user impersonation attack, and an off-line dictionary attack, respectively, on Yoon et al.'s scheme. What we do in this work is to report these security vulnerabilities of Yoon et al.'s scheme and to show how to eliminate them.

II. Liao et al.'s Authentication Scheme and Its Weakness

2.1 Review of Liao et al.'s Authentication Scheme

Liao et al. [20] have recently presented an improved version of Das et al.'s scheme [19]. Besides preventing the password guessing attack, Liao et al.'s scheme intends to provide mutual authentication between the remote server and the user. We begin by describing the top level structure of the scheme. The scheme consists of two phases: registration phase and authentication phase. The registration phase is performed only once per user when a new user registers itself with the remote server. The authentication phase is carried out whenever a user wants to gain access to the server.

Before the registration phase is performed for the first time, the server S decides on the following system parameters: a one-way hash function h and two cryptographic keys x and y. The key x is kept secret by the server, while y is shared securely among the server and all registered users.

2.1.1 Registration Phase

The registration of a new user U_i to the server S proceeds as follows:

Step 1. U_i chooses its password PW_i at will and submits a registration request, consisting of its identity ID_i and the hashed password $h(PW_i)$, to the remote server S via a secure channel.

Step 2. Upon receiving the request $\langle ID_i, h(PW_i)\rangle$, S computes $N_i = h(PW_i) \oplus h(ID_i \parallel x)$ and issues a smart card containing $\langle N_i, y, h(\bullet)\rangle$ to U_i.

2.1.2 Authentication Phase

This phase constitutes the core of the scheme and is performed whenever some user U_i wants to log on to the server S. U_i initiates this phase by inserting its smart card into a card reader and entering its password PW_i. Given the user input, the smart card and the server perform the following steps:

Step 1. The smart card obtains the current timestamp T_1 and computes $CID_i = h(PW_i) \oplus h(N_i \oplus y \oplus T_i)$, $A_i = h(CID_i \oplus h(PW_i))$, $C_i = h(T_1 \oplus N_i \oplus A_i \oplus y)$.

The smart card then sends the login request message $\langle CID_{i,}\ N_i,\ C_i,\ T_1\rangle$ to the server S.

Step 2. After receiving $\langle CID_i, N_i, C_i, T_1\rangle$, S first acquires the current timestamp T_2 and computes $Z_i = CID_i \oplus h(N_i \oplus y \oplus T_1)$ and $B_i = h(CID_i \oplus Z_i)$. Then S verifies that: (1) $T_2 - T_1 \le \triangle T$, where $\triangle T$ is the maximum allowed time interval for transmission delay and (2) C_i equals $h(T_1 \oplus N_i \oplus B_i \oplus y)$. If either of these conditions is untrue, S rejects the login request. Otherwise, S generates a new timestamp T_3, computes $D_i = h(T_3 \oplus N_i \oplus B_i \oplus y)$, and sends the response message $\langle T_3,\ D_i\rangle$ to the smart card.

Step 3. Upon receipt of the response $\langle T_3,\ D_i\rangle$, the smart card obtains a new timestamp T_4 and checks that: (1) $T_4 - T_3 \le \triangle T$ and (2) D_i is equal to $h(T_3 \oplus N_i \oplus A_i \oplus y)$. If both of these conditions hold, the smart card believes the responding party as the authentic server. Otherwise, the smart card aborts its login attempt.

2.2 Yoon et al.'s Attack on Liao et al.'s Scheme

Yoon et al. [21] showed that Liao et al.'s authentication scheme does not guarantee any kind of authentication, either server-to-user authentication or user-to-server authentication.

2.2.1 Impersonating S to U_i

First, Yoon et al. present a reflection attack where an attacker U_a impersonates the remote server S to a legitimate user U_i. The corresponding attack scenario is described as follows:

(1) As usual, the authentication phase begins when U_i's smart card computes CID_i, A_i and C_i, and sends the login request message $\langle CID_i, N_i, C_i, T_1\rangle$ to S.

(2) But, the attacker U_a intercepts this login request message and sets D_i equal to C_i. Then U_a, posing as S, immediately sends $\langle T_1, D_i\rangle$ in response to U_i's login

request.

(3) The timestamp T_1 that the smart card receives from U_a is in fact the timestamp sent out by the smart card itself. However, the smart card cannot detect this fact since the scheme does not require it to check whether or not the timestamp received from the server equals the one sent by itself; to follow the specification of the scheme is all that the smart card can and should do. Hence, the smart card proceeds as usual, checking that $T_4 - T_1 \leq \triangle T$ and D_i equals $h(T_1 \oplus N_i \oplus A_i \oplus y)$. Since both of these conditions hold, the smart card should believe U_a as the authentic server.

2.2.2 Impersonating U_i to S

Suppose now that an attacker U_a has stolen U_i's smart card or gained temporary access to it. Then U_a, who does not know U_i's password, is able to impersonate the legitimate user U_i to the server S. This is shown via a so-called stolen card attack on the scheme. The attack is described step by step as follows:

(1) U_a launches the attack by inserting U_i's smart card into a card reader and then entering an arbitrary password PW. Because this scheme provides no way to check whether the user-given password is correct or not, the smart card cannot detect any discrepancy and thus operates as usual. That is, given PW, the smart card generates a timestamp T_1, computes

$$CID_i = h(PW) \oplus h(N_i \oplus y \oplus T_1),$$

$$A_i = h(CID_i \oplus h(PW)),$$

$$C_i = h(T_i \oplus N_i \oplus A_i \oplus y),$$

and sends $\langle CID_i, N_i, C_i, T_1 \rangle$ to S.

(2) Upon receiving $\langle CID_i, N_i, C_i, T_1 \rangle$, S first acquires the current timestamp T_2, and computes

$h'(PW) = CID_i \oplus h(N_i \oplus y \oplus T_1)$ and

$B_i = h(CID_i \oplus h'(PW))$. Then S checks that: (1) $T_2 - T_1 \leq \triangle T$ and (2) C_i equals $h(T_1 \oplus N_i \oplus B_i \oplus y)$. Clearly, the first condition is true. The second condition also holds because $h(PW)$ equals $h'(PW)$ and so A_i equals B_i. Accordingly, S will welcome U_a's visit to the system and sends $\langle T_3, D_i \rangle$ to U_a.

III. Review of Yoon et al.'s Authentication Scheme

Yoon et al. [21] have also presented an improved version of Liao et al.'s scheme. The server in Yoon et al.'s scheme makes use of the same system parameters $\langle h, x, y \rangle$ as used in Liao et al.'s scheme. Yoon et al.'s scheme is outlined in Fig. 1, where dashed lines indicate a secure channel, and is described in more detail as follows:

3.1 Registration Phase

This is the phase where a new registration of a user takes place. The registration proceeds as follows:

Step 1. A user U_i, who wants to register with the server S, chooses its password PW_i and a random number R at will. Then U_i computes $Z_i = h(PW_i \| R)$ and submits a registration request, consisting of its identity ID_i and Z_i, to the remote server S via a secure channel.

Step 2. When the server S receives the request, it first computes $N_i = Z_i \oplus h(ID_i \| x)$ and $K_i = Z_i \oplus h(N_i \| y)$ and then issues a smart card containing $\langle N_i, y, K_i, h(\bullet) \rangle$ to the user U_i.

Step 3. Upon receiving the smart card, U_i enters the random number R into its smart card. Accordingly, R is additionally stored on the smart card.

3.2 Authentication Phase

When U_i wants to log in to the server, it inserts its smart card into a card reader and enters its password PW_i. With the user input, the scheme enters the authentication phase during which the server and the smart card perform the following steps:

Step 1. Using the user-given PW_i and the values K_i, R, N_i and y, the smart card computes

$Z_i = h(PW_i \| R)$, $V_i' = K_i \oplus Z_i$, and $V_i = h(N_i \| y)$. Then the smart card checks that V_i' is equal to V_i. If they are equal, the smart card proceeds to the next step. Otherwise, the smart card aborts the authentication phase.

Step 2. The smart card generates the current timestamp T_1 and computes

$$CID_i = Z_i \oplus h(N_i \parallel y \parallel T_i),$$
$$A_i = h(CID_i \parallel Z_i),$$
$$C_i = h(T_1 \parallel N_i \parallel A_i \parallel y).$$

Then the smart card sends the login request message $\langle CID_i, N_i, C_i, T_1 \rangle$ to the server S.

Step 3. When the login request arrives, S first acquires the current timestamp T_2 and computes

$$Z_i = CID_i \oplus h(N_i \parallel y \parallel T_1) \text{ and } B_i = h(CID_i \parallel Z_i).$$

Then S verifies that: (1) $T_2 - T_1 \le \triangle T$ where $\triangle T$ is the maximum allowed time interval for transmission delay and (2) C_i equals $h(T_1 \parallel N_i \parallel B_i \parallel y)$. If either of these conditions is untrue, S rejects the login request. Otherwise, S generates a new timestamp T_3, computes

$D_i = h(T_3 \parallel B_i \parallel y)$, and sends the response message $\langle T_3, D_i \rangle$ to the smart card.

Step 4. After receiving $\langle T_3, D_i \rangle$, the smart card obtains a new timestamp T_4 and checks that: (1) $T_4 - T_3 \le \triangle T$ and (2) D_i is equal to $h(T_3 \parallel A_i \parallel y)$. If both of these conditions hold, the smart card believes the responding party as the authentic server. Otherwise, the smart card aborts its login attempt

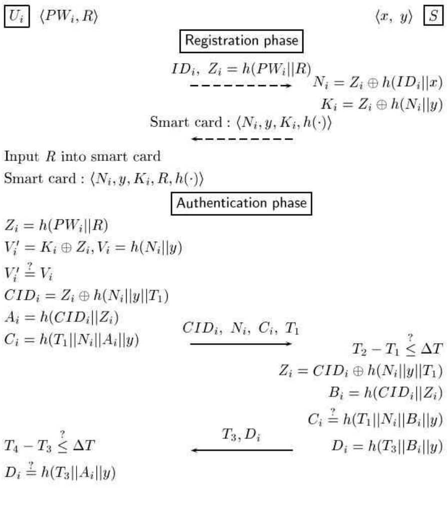
U_i $\langle PW_i, R \rangle$
$\langle x, y \rangle$ S
Registration phase
$ID_i,\ Z_i = h(PW_i\|R)$
$N_i = Z_i \oplus h(ID_i\|x)$
$K_i = Z_i \oplus h(N_i\|y)$
Smart card : $\langle N_i, y, K_i, h(\cdot) \rangle$
Input R into smart card
Smart card : $\langle N_i, y, K_i, R, h(\cdot) \rangle$
Authentication phase
$Z_i = h(PW_i\|R)$
$V_i' = K_i \oplus Z_i, V_i = h(N_i\|y)$
$V_i' \overset{?}{=} V_i$
$CID_i = Z_i \oplus h(N_i\|y\|T_1)$
$A_i = h(CID_i\|Z_i)$
$C_i = h(T_1\|N_i\|A_i\|y)$
$CID_i,\ N_i,\ C_i,\ T_1$
$T_2 - T_1 \overset{?}{\le} \Delta T$
$Z_i = CID_i \oplus h(N_i\|y\|T_1)$
$B_i = h(CID_i\|Z_i)$
$C_i \overset{?}{=} h(T_1\|N_i\|B_i\|y)$
T_3, D_i
$D_i = h(T_3\|B_i\|y)$
$T_4 - T_3 \overset{?}{\le} \Delta T$
$D_i \overset{?}{=} h(T_3\|A_i\|y)$

Fig. 1. Yoon et al.'s authentication scheme

IV. Cryptanalysis of Yoon et al.'s Scheme

In this section we point out that Yoon et al.'s scheme does not achieve its main security goal not only of authenticating between a remote individual and the server but also of password security.

4.1 Attacks against Mutual Authentication

Unfortunately, Yoon et al.'s remote user authentication scheme supports neither server-to-user authentication nor user-to-server authentication. In this subsection, we show this by presenting two impersonation attacks, a server impersonation attack and a user impersonation attack. The server impersonation attack and the user impersonation attack are given to violate respectively server-to-user and user-to-server authentications of Yoon et al.'s scheme.

4.1.1 Impersonating S to U_i

First, we present a server impersonation attack where an attacker U_a, who is a legitimate user registered with the server, can easily impersonate the remote server S to any other registered user U_i. Before describing the attack, we note that the secret values stored in a smart card could be extracted by monitoring its power consumption [17,6]. We now proceed to describe the server impersonation attack.

(1) As a preliminary step, the attacker U_a extracts the server's secret key y stored in its smart card.

(2) Now when U_i initiates the authentication phase with the login request message $\langle CID_i, N_i, C_i, T_1 \rangle$, the attacker U_a posing as S intercepts this login request and sends immediately back to U_i a forged response message as follows: U_a first generates the current timestamp T_3, computes

$Z_i = CID_i \oplus h(N_i \parallel y \parallel T_1), B_i = h(CID_i \parallel Z_i)$ and $D_i = h(T_3 \parallel B_i \parallel y)$, and then sends $\langle T_3, D_i \rangle$ in response to U_i's login request.

(3) The forged response $\langle T_3, D_i \rangle$ will pass the verification test by U_i since the timestamp T_3 is valid and

D_i is equal to $h(T_3 \| A_i \| y)$. Hence, U_i believes U_a as the authentic server.

4.1.2 Impersonating U_i to S

Now suppose that an attacker U_a is a deregistered user and thus, has an expired smart card. Then we present a user impersonation attack where an attacker, who is no longer a legitimate user, is able to forge a valid login request message without registering again. The attack scenario is described as follows:

(1) The attacker U_a begins by extracting the server's secret key y stored in the expired smart card. Next, U_a chooses two random numbers Z_i' and N_i', obtains the current timestamp T_1, and computes

$$CID_i' = Z_i' \oplus h(N_i' \| y \| T_1),$$
$$A_i' = h(CID_i' \| Z_i'),$$
$$C_i' = h(T_1 \| N_i' \| A_i' \| y).$$

Then U_a posing as some registered user U_i sends $\langle CID'_i, N'_i, C'_i, T_1 \rangle$ as a login request message to the server S.

(2) After receiving $\langle CID_i', N_i', C_i', T_1' \rangle$, the server S proceeds to verify the authenticity of the login request. That is, S acquires the current timestamp T_2, computes $Z_i' = CID_i' \oplus h(N_i' \| y \| T_1), B_i' = h(CID_i' \| Z_i')$, and checks that: (1) $T_2 - T_1 \le \triangle T$ and (2) C_i' equals $h(T_1 \| N_i' \| B_i' \| y)$. Since both of the two conditions hold, S will welcome U_a's visit to the system and sends the response message $\langle T_3, D_i \rangle$ to U_a.

4.2 Attack against Password Security

Yoon et al.'s [21] remote user authentication scheme does not guarantee its fundamental goal of password security. We demonstrate this by showing that Yoon et al.'s authentication scheme is vulnerable to an off-line dictionary attack in which an attacker U_a can easily find out the password of a user U_i. Assume that the attacker has stolen the U_i's smart card or gained access to it and extracted the secret values stored in it by monitoring its power consumption [17,6]. Now the attacker U_a who has obtained the values N_i K_i, and R stored in the U_i's smart card can find out PW_i by employing the dictionary attack, in which each guess PW'_i for PW_i can be verified by computing $Z_i' = K_i \oplus h(N_i \| R)$ and by checking the equality $Z_i' \overset{?}{=} h(PW_i' \| R)$.

V. Enhancement Security of Yoon et al.'s Scheme

One intuitive way of preventing the attacks above is to modify the Yoon et al.'s scheme [21] so that we propose the improved authentication scheme which eliminates the security vulnerabilities in the scheme. The following system parameters used in the scheme is decided on by the server S: a one-way hash function h, a cryptographic key x, a large prime number p, and a timestamp T_i generated by the server upon registering U_i. The key x is kept secret by the server. In describing the protocol, we will omit 'mod p' from expressions for notational simplicity. The proposed scheme proceeds as illustrated by Fig. 2, where dashed lines indicate a secure channel.

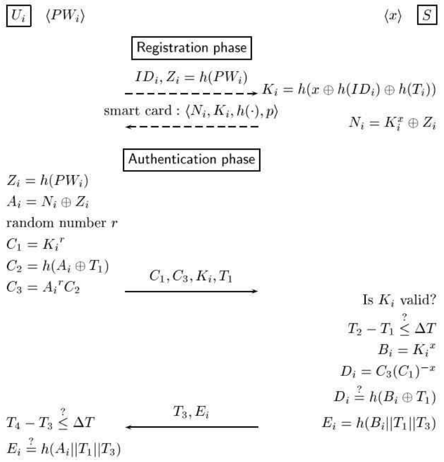
U_i $\langle PW_i \rangle$
$\langle x \rangle$ S
Registration phase
$ID_i, Z_i = h(PW_i)$
$K_i = h(x \oplus h(ID_i) \oplus h(T_i))$
smart card : $\langle N_i, K_i, h(\cdot), p \rangle$
$N_i = K_i^x \oplus Z_i$
Authentication phase
$Z_i = h(PW_i)$
$A_i = N_i \oplus Z_i$
random number r
$C_1 = K_i{}^r$
$C_2 = h(A_i \oplus T_1)$
$C_3 = A_i{}^r C_2$
C_1, C_3, K_i, T_1
Is K_i valid?
$T_2 - T_1 \overset{?}{\le} \Delta T$
$B_i = K_i{}^x$
$D_i = C_3(C_1)^{-x}$
$D_i \overset{?}{=} h(B_i \oplus T_1)$
T_3, E_i
$E_i = h(B_i || T_1 || T_3)$
$T_4 - T_3 \overset{?}{\le} \Delta T$
$E_i \overset{?}{=} h(A_i || T_1 || T_3)$

Fig. 2. Our proposed remote user authentication scheme

5.1 Description of the Proposed Scheme

5.1.1 Registration Phase

The registration of a new user U_i to the remote server proceeds as follows:

Step 1. A new user U_i, who wants to register with the server S, chooses its password PW_i, compute $Z_i = h(PW_i)$, and submits a registration request, consisting of its identity ID_i and Z_i, to the remote server S via a secure channel.

Step 2. Upon receiving the request, S first generates a timestamp T_i, computes $K_i = h(x \oplus h(ID_i) \oplus h(T_i))$ and $N_i = K_i^x \oplus Z_i$ and issues a smart card containing $\langle N_i, K_i, h(\bullet), p \rangle$ to the user U_i.

5.1.2 Authentication Phase

When U_i wants to log in to the server, it inserts its smart card into a card reader and enters its identity ID_i and password PW_i. With the user input, the scheme enters the authentication phase during which the server and the smart card perform the following steps:

Step 1. Given PW_i, the smart card chooses a random number r and computes

$$Z_i = h(PW_i),$$
$$A_i = N_i \oplus Z_i,$$
$$C_1 = K_i^T,$$
$$C_2 = h(A_i \oplus T_1),$$
$$C_3 = A_i^r C_2.$$

The smart card then sends the login request message $\langle C_1, C_3, K_i, T_1 \rangle$to the server S.

Step 2. After receiving $\langle C_1, C_3, K_i, T_1 \rangle$, S first acquires the current timestamp T_2 and computes $B_i = K_i^x$ and $D_i = C_3(C_1)^{-x}$. Then S verifies that:

(1) K_i is valid, (2) $T_2 - T_1 \leq \triangle T$, where $\triangle T$ is the maximum allowed time interval for transmission delay, and (3) D_i equals $h(B_i \oplus T_1)$. If one of these conditions is untrue, S rejects the login request. Otherwise, S obtains a timestamp T_3 compute $E_i = h(B_i \parallel T_1 \parallel T_3)$, and sends the response message $\langle T_3, E_i \rangle$ to U_i.

Step 3. Upon receipt of the response $\langle T_3, E_i \rangle$, user U_i checks that: (1) $T_4 - T_3 \leq \triangle T$, where $\triangle T$ is the maximum allowed time interval for transmission delay and (2) E_i is equal to $h(A_i \parallel T_1 \parallel T_3)$. If both of these conditions hold, the smart card believes the responding party as the authentic server. Otherwise, the smart card aborts its login attempt.

Table 1. Comparison of formula methods

	Liao	Yoon	Our
Information stored in the smart card	$\langle N_i, y, h(\bullet) \rangle$	$\langle N_i, y, K_i, h(\bullet) \rangle$	$\langle N_i, K_i, h(\bullet), p \rangle$
N_i	$N_i = h(PW_i) \oplus h(ID_i \parallel x)$	$N_i = Z_i \oplus h(ID_i \parallel x)$	$N_i = K_i^x \oplus Z_i$
K_i		$K_i = Z_i \oplus h(N_i \parallel y)$	$K_i = h(x \oplus h(ID_i) \oplus h(T_i))$
Z_i		$Z_i = h(PW_i \parallel R)$	$Z_i = h(PW_i)$

5.2 Security Analysis

The security vulnerabilities of Yoon et al.'s scheme are attributed to the following fact:

- To forge a valid response message $\langle D_i, T_3 \rangle$ or a valid login request message $\langle CID_i, N_i, C_i, T_1 \rangle$, or to find out the password PW_i of U_i, it suffices to obtain the information stored in a smart card; N_i, K_i, y, and R.

Having identified the source of the problem, it is apparent how to repair the Yoon et al.'s scheme. So we proposed the revised one over their scheme. These modifications effectively defeats these kind of attacks discussed previous section.

Firstly, even if the attacker obtains all the information $(i.e., N_i, \text{ and } K_i)$ stored in the smart card, he/she can no longer forge a valid response message $\langle E_i, T_3 \rangle$ or a valid login request message $\langle C_1, C_3, K_i, T_1 \rangle$. Forging a response message is impossible because computing $E_i = h(B_i \parallel T_1 \parallel T_3)$ requires the knowledge of $B_i = K_i^x$ which in turn needs the knowledge of the server's secret value x. Forging a login request message is also infeasible. This is because no one can compute $C_3 = A_i^r h(A_i \oplus T_1)$ without knowing $A_i (= N_i \oplus Z_i)$, or equivalently knowing $B_i (= K_i^x)$. Clearly, computing $A_i (= B_i)$ requires either N_i and PW_i or K_i and x. But since the attacker knows neither PW_i nor x, he/she cannot compute A_i. One may think that a deregistered user U_i can still send a valid login request by extracting N_i in the expired smart card and then by deriving A_i as$A_i = N_i \oplus h(PW_i)$. But this kinds of attack is prevented in our revised scheme, because the server checks the validity of K_i by maintaining a list of all expired K_i's. Therefore, the attacks against authenticating between the remote user and the server will no longer be applied against our revised scheme.

Secondly, in the proposed scheme, even if the attacker learns both of the values N_i and K_i stored in the smart card, he/she can no longer find out the password of the user U_i. Because, now, the only information related to passwords is $N_i(=K_i^x \oplus h(PW_i))$. This value does not help the attacker to verify directly the correctness of guessed passwords since x is the secret information that the server only knows. Hence, the off-line dictionary attack is also defeated in our countermeasure.

Table 2 Comparison of security properties

	Liao	Yoon	Our
Impersonating S to U_i	Yes	Yes	No
Impersonating U_i to S	Yes	Yes	No
Mutual authentication	not - satisfy	not - satisfy	satisfy
Password security	not - satisfy	not - satisfy	satisfy

VI. Conclusion

We have analyzed the security of the smart card based user authentication scheme proposed by Yoon et al. [21]. Our security analysis uncovered that Yoon et al.'s scheme does not achieve its main security goal of not only mutual authentication between a remote individual and the server but also password security. The failure of Yoon et al.'s scheme to achieve authentication has been made clear through two attacks, a server impersonation attack and a user impersonation attack, on the scheme. The server impersonation attack and the user impersonation attack have been considered to infringe respectively server-to-user and user-to-server authentications of the scheme. In addition, the flaw of password security has been shown via the off-line dictionary attack. Besides reporting these security vulnerabilities, we proposed the improved secure user authentication scheme which eliminates them.

Reference

[1] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[2] C.-C. Chang, T.-C. Wu, "Remote password authentication with smart cards," IEE Proceedings E - Computers and Digital Techniques, Vol. 138, No. 3, pp. 165-168, 1991.

[3] W.-H. Yang, S.-P. Shieh, "Password authentication schemes with smart card," Computers & Security, Vol. 18, No. 8, pp. 727-733, 1999.

[4] M.-S. Hwang, L.-H. Li, "A new remote user authentication scheme using smart cards," IEEE Transaction on Consumer Electronics, Vol. 46, No. 1, pp. 28-30, 2000.

[5] H.-M. Sun, "An efficient remote user authentication scheme using smart cards," IEEE Transaction on Consumer Electronics, Vol. 46, No. 4, pp. 958-961, 2000.

[6] H.-Y. Chien, J.-K. Jan, Y.-M. Tseng, "An efficient and practical solution to remote authentication: smart card," Computers & Security, Vol. 21, No. 4, pp. 372-375, 2002.

[7] E.-J. Yoon, E.-K. Ryu, K.-Y. "Yoo, An improvement of Hwang-Lee-Tang's simple remote user authentication scheme," Computers & Security, Vol. 24, No. 1, pp. 50-56, 2005.

[8] Anti-Phishing Working Group *(http://www.antiphishing.org).*

[9] 최병훈, 김상근, 배제민. “다중체계 인증을 이용한 중요 시스템 보안 접근에 관한 연구,” 한국컴퓨터정보학회논문지, 제 14권, 제 7호, 2009년 7월.

[10] W. Diffie, P. C. van Oorschot, M. J. Wiener, "Authentication and authenticated key exchange," Designs, Codes and Cryptography, Vol. 2, No. 2, pp. 107-125, 1992.

[11] R. Bird, I. Gopal, A. Herzberg, P. A. Janson, S. Kutten, R. Molva, M. Yung, "Systematic design of a family of attack-resistant authentication protocols," IEEE Journal on Selected Areas in Communications, Vol. 11, No. 5, pp. 679-693, 1993.

[12] U. Carlsen, "Cryptographic protocol flaws: know your enemy," Proceedings of the 7th IEEE Computer Security Foundations Workshop, pp. 192-200, 1994.

[13] G. Lowe, "An attack on the Needham-Schroeder public-key authentication protocol," Information Processing Letters, Vol. 56, No. 3, pp. 131-133, 1995.

[14] C.-L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," Computer Standards and Interfaces, Vol. 26, No. 3, pp. 167-169, 2004.

[15] E.-J. Yoon, W.-H. Kim, K.-Y. Yoo, "Security enhancement for password authentication schemes with smart cards," Proceedings of the 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus 2005), Lecture Notes in Computer Science, Vol. 3592, pp. 90-99, 2005.

[16] W.-C. Ku, S.-T. Chang, M.-H. Chiang, "Weaknesses of a remote user authentication scheme using smart cards for multi-server architecture," IEICE Transactions on Communications, Vol. E88-B, No. 8, pp. 3451-3454, 2005.

[17] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis," Advances in Cryptology{CRYPTO99}, pp. 388-397, 1999.

[18] T.-S. Messerges, E.-A. Dabbish, R.-H. Sloan, "Examining smart card security under the threat of power analysis attacks," IEEE Transaction on Computers, Vol. 51, No. 5, pp. 541-552, 2002.

[19] M.L. Das, A. Saxena, V.P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Transaction on Consumer Electronics, Vol. 50, No. 2, pp. 629-631, 2004.

[20] I.-E. Liao, C.-C. Lee, M.-S. "Hwang, Security enhancement for a dynamic ID-based remote user authentication scheme," Proceedings of the IEEE International Conference on Next Generation Web Services Practices (NWeSp'05), pp. 437-440, 2005.

[21] E.-J. Yoon, K.-Y. Yoo, "Improving the Dynamic ID-Based Remote Mutual Authentication Scheme," Proceedings of 2006 OTM Confederated International workshops (OTM 2006), Lecture Notes in Computer Science, Vol. 4277, pp. 499-507, 2006.

저자소개

이 영 숙

1987 : 성균관대학교 공학사.
2005 : 성균관대학교 공학석사
2008 : 성균관대학교 컴퓨터공학과 공학박사
2009 - 현재 : 호원대학교 사이버수사 경찰학부 전임강사
관심분야: 정보보안. 암호프로토콜

원 동 호

1976년~1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~2003년 :
성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년 :
국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
2002년~2008년 : 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT감사 자문위원
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장
관심분야 : 암호이론, 정보이론, 정보보호