ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

스마트 카드를 사용한 검증자 없는 사용자 인증 및 접근 제어 방법: Chen-Yeh 방법의 개선☆

A Verifier-free Scheme for User Authentication and Access Control Using Smart Cards: Improvement of Chen-Yeh's Method

김 용[1] 정 민 교[2*]
Yong Kim Min Gyo Chung

요 약

고도의 보안 시스템에서 사용자 인증과 접근제어는 두 가지 중요한 요소이다. 최근 Chen & Yeh는 이 두 가지 보안 요소를 원활하게 잘 통합한 방법을 제안하였다. 그러나 Chen-Yeh 방법은 원격 서버에 스마트 카드 ID 자료를 유지하기 때문에 SVA(stolen verifier attack: 도난 검증자 공격)에 취약하다는 단점을 가지고 있다. 따라서 본 논문에서는 Chen & Yeh 방법의 이런 단점을 개선하고, 장점은 그대로 유지하는 새로운 사용자 인증 및 접근제어 방법을 제안한다. 보안 분석 결과에 의하면, 기존 방법들에 비하여 제안 방법은 여러 가지 다양한 보안 침해 공격에 강인하면서, 사용자 인증 및 접근제어에 도움이 되는 많은 좋은 특징을 보유하고 있는 것으로 입증되었다.

주제어 : 사용자 인증, 접근제어, 스마트 카드, 도난 검증자 공격

ABSTRACT

User authentication and access control are two important components in high security applications. Recently, Chen and Yeh proposed a method to integrate both of them seamlessly. However, Chen-Yeh's scheme is vulnerable to a stolen verifier attack, since it maintains a smart card identifier table in a remote server. Therefore, this paper modifies Chen-Yeh's scheme and propose a new integrated authentication and access control scheme that is resilient to the stolen verifier attack while inheriting all the merits of Chen-Yeh's scheme. Security analysis shows that the proposed scheme withstands well-known security attacks and exhibits many good features.

☞ keyword : user authentication, access control, smart card, SVA(stolen verifier attack)

1. Introduction

Indeed, a high security networked system with a variety of resources requires some kind of authentication and access control mechanism. Authentication is used to verify if communicating entities are really trustworthy, whereas access control is used to determine what an entity can do on the resources in the system.

Lamport [1] introduced an authentication scheme using a password table in early 1980s. A wealth of user authentication methods has since been proposed in the literature to improve Lamport's scheme [2]-[10]. Meanwhile, a notion of access matrix, the earliest formal description of access control, was presented by Lampson [11]. Several forms of access control were developed afterward, e.g., discretionary access control, mandatory access control, and role-based access control [12].

In general, authentication is followed by access control. Thus, a lot of research efforts have been made to securely integrate authentication and access control [13]-[18]. Nevertheless, most of them are vulnerable to various security attacks. For example, Chien-Jan's method [14] is susceptible

1 Department of Library and Information Science, Chonbuk National University, Jeonju, Chonbuk, 561-756, Korea
2 Department of Computer Science, Seoul Women's University, Seoul, 139-774, Korea
* Corresponding author (mchung@swu.ac.kr)
[Received 21 May 2013, Reviewed 30 May 2013, Accepted 1 August 2013]
☆ 본 연구는 2013학년도 서울여자대학교 교내학술특별연구비의 지원을 받았음.

http://dx.doi.org/10.7472/jksii.2013.14.4.43

to reflection attacks (In the login request phase, an intruder intercepts the message sent by the user. The intruder forges it and sends it back to the user for the purpose of impersonating the legitimate server), parallel session attacks (In the verification phase, an intruder intercepts the message sent to the user. The intruder then starts a new session with the server by reusing the intercepted message. As a result, the intruder can masquerade as a legitimate user), and privilege elevation attacks. Further, it does not protect the privacy of access requests, since the access rights information in the request phase is sent to the server without any encryption. Recently, Chen and Yeh enhanced Chien-Jan's method by eliminating the aforementioned attacks [15]. However, Chen-Yeh's method is still vulnerable to a stolen verifier attack, because it holds a smart card identifier table in a remote server. Therefore, in this paper, we propose an improved integrated scheme that is resilient to the stolen verifier attack while keeping all the merits of Chen-Yeh's scheme.

The rest of this paper is organized as follows. Section 2 gives an overview of Chen-Yeh's scheme and a discussion of its weaknesses. Section 3 describes the proposed scheme in detail. Section 4 provides the security analysis of the proposed scheme. Finally, Section 5 gives a short concluding remark.

2. Related Work

Take, for example, a system that provides a video streaming service on the Internet. Typically, the system will consist of a remote sever and a database of videos, and will maintain an *access control list*, which is a list of accessible videos with privileges (e.g., one-time viewing, two-time viewing, one-day viewing, etc.) for each user. Based on the access control list, the streaming server will allow only authenticated users to access the permitted videos in the manner specified in the access control list. Authentication and access control in such kind of systems are carried out independently. Recently, however, the demand for integrating the two separate processes has been on the increase for the purpose of protecting the systems as a whole [15].

In this section, a review is made on Chen-Yeh's scheme, which was proposed as a part of the above demand. It consists of three phases: *registration*, *login request* and *verification* phases. See the summary in Fig. 1. For convenience of description, the symbols and notations similar to the ones used by Chen and Yeh are employed here.

- S, x : a remote server and its secret key, respectively.
- n : number of resources on the server S.
- r_i : a bit string to represent access rights (privileges) for resource i, $1 \leq i \leq n$.
- U_u, ID_u, PW_u : a user, his identifier, and his password, respectively.
- N_c, N_s : two nonce values.
- T_1, T_2 : two current timestamps.
- $h(\cdot)$: a hash function.
- $\oplus$: bitwise XOR operation.
- $X \rightarrow Y$ $\{M\}$: X sends a message M to Y.

2.1 Registration Phase

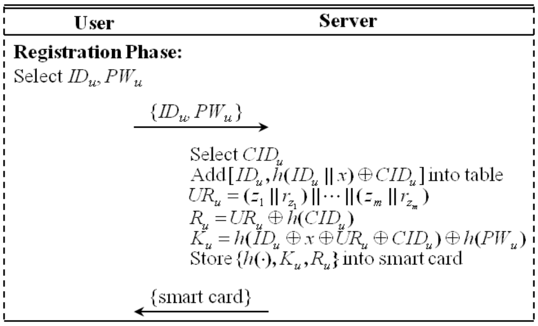
In this phase, the user U_u registers with the server S.

1. U_u submits his identity ID_u and password PW_u to S over a secure communication channel.
2. S creates a smart card identifier CID_u and stores a new entry $[ID_u,\ h(ID_u \| x) \oplus CID_u]$ into a card identifier table.
3. S grants U_u the access rights of m resources ($m \leq n$). Assuming that the indices of m resources are $\{z_1, z_2, \cdots, z_m\}$ and r_{z_i} represents the access rights of resource z_i, S generates an access control list for the user U_u, $UR_u = (z_1 \| r_{z_1}) \| (z_2 \| r_{z_2}) \| \cdots \| (z_m \| r_{z_m})$.
4. S computes $R_u = UR_u \oplus h(CID_u)$ and $K_u = h(ID_u \oplus x \oplus UR_u \oplus CID_u) \oplus h(PW_u)$, and stores $h(\cdot)$, R_u, and K_u into a smart card. Finally, S issues the smart card to U_u.

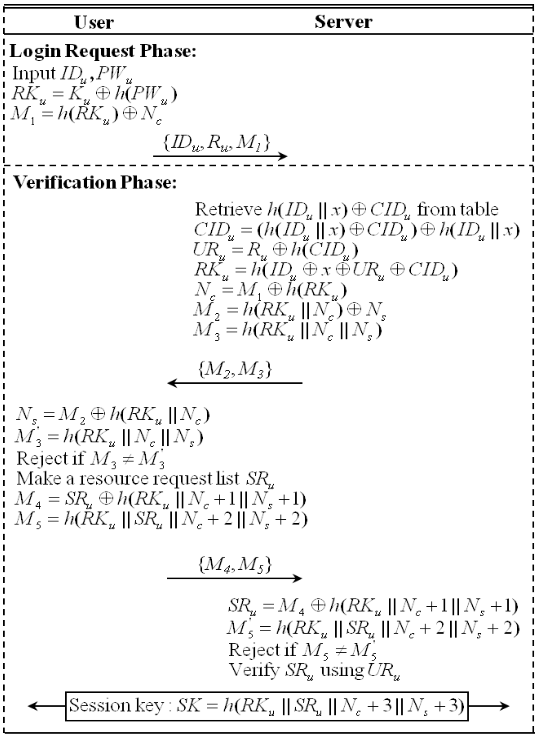
2.2 Login Request Phase

In this phase, the user U_u submits a login request to the server S whenever U_u wants to access some resources upon S.

1. U_u inserts the smart card into a smart card reader and inputs his identity ID_u and password PW_u.
2. The smart card extracts $RK_u = h(ID_u \oplus x \oplus UR_u \oplus CID_u)$ by calculating $K_u \oplus h(PW_u)$. It then generates a fresh random number N_c and computes $M_1 = h(RK_u) \oplus N_c$.
3. $U_u \rightarrow S$ $\{ID_u, R_u, M_1\}$.



(a) Registration phase.



(b) Login request phase and verification phase.

(Fig. 1) Chen-Yeh's integrated authentication and access control scheme.

2.3 Verification Phase

In this phase, the server S verifies the authenticity of U_u's request for both logging into the server and accessing resources on the server.

1. Upon receiving $\{ID_u, R_u, M_1\}$, S uses ID_u to retrieve $h(ID_u \| x) \oplus CID_u$ from the card identifier table and gets CID_u by computing $(h(ID_u \| x) \oplus CID_u) \oplus h(ID_u \| x)$.
2. S uses CID_u to extract UR_u from R_u by calculating $R_u \oplus h(CID_u)$.
3. Based on the obtained CID_u and UR_u, S computes $RK_u = h(ID_u \oplus x \oplus UR_u \oplus CID_u)$ and extracts N_c by calculating $M_1 \oplus h(RK_u)$.
4. S generates another random number N_s and computes M_2 and M_3, where $M_2 = h(RK_u \| N_c) \oplus N_s$ and $M_3 = h(RK_u \| N_c \| N_s)$.
5. $S \rightarrow U_u$ $\{M_2, M_3\}$.
6. Upon receiving $\{M_2, M_3\}$, the smart card extracts N_s by computing $M_2 \oplus h(RK_u \| N_c)$. Using the obtained N_s, the smart card computes $M_3' = h(RK_u \| N_c \| N_s)$ and checks whether $M_3 = M_3'$. If yes, U_u successfully authenticates S. Otherwise, U_u rejects S and terminates the connection.
7. Suppose that U_u attempts to access p resources ($p \leq m \leq n$) and that the indices and access rights of the p resources are recorded in SR_u. Now U_u computes M_4 and M_5, where $M_4 = h(RK_u \| N_c + 1 \| N_s + 1) \oplus SR_u$ and $M_5 = h(RK_u \| SR_u \| N_c + 2 \| N_s + 2)$.
8. $U_u \rightarrow S$ $\{M_4, M_5\}$.
9. Upon receiving $\{M_4, M_5\}$, S extracts SR_u by computing $h(RK_u \| N_c + 1 \| N_s + 1) \oplus M_4$. Using the obtained SR_u, S computes $M_5' = h(RK_u \| SR_u \| N_c + 2 \| N_s + 2)$, and checks whether $M_5 = M_5'$. If yes, S successfully authenticates U_u. Then S uses UR_u to verify SR_u.
10. After the successful authentication, both U_u and S have obtained N_c, N_s, RK_u, and SR_u. Now U_u and S independently generates a session key $SK = h(RK_u \| SR_u \| N_c + 3 \| N_s + 3)$. Subsequent communications of this session are encrypted using SK.

2.4 Security Analysis

Chen-Yeh's scheme maintains a smart card identifier table on a remote server. However, this smart card identifier table is always under the threat of a stolen verifier attack. The stolen verifier attack is a security attack by which an intruder steals or modifies a verification table stored in a server. In Chen-Yeh's scheme, if the smart card identifier table on the remote server is stolen and modified, a legitimate user cannot successfully log into the server, which results in a denial-of-service attack.

Suppose that an intruder steals the smart card identifier table and replaces the *i*-th entry [ID_i, $h(ID_i \| x) \oplus CID_i$] with [$ID_i$, X_i], where X_i is an arbitrary random number. Suppose now that the server *S* receives a login request from the user U_i. Then, in step 1 of the verification phase protocol, *S* will retrieve X_i from the card identifier table and will compute a wrong smart card identifier $CID_i^* = X_i \oplus h(ID_i \| x)$, instead of the correct one CID_i. Using the incorrect values $UR_i^* = R_i \oplus h(CID_i^*)$, $RK_i^* = h(ID_i \oplus x \oplus UR_i^* \oplus CID_i^*)$, and $N_c^* = M_1 \oplus h(RK_i^*)$, the server also calculates two erroneous messages $M_2^* = h(RK_i^* \| N_c^*) \oplus N_s$ and $M_3^* = h(RK_i^* \| N_c^* \| N_s)$, which are sent to U_i. In step 6, however, U_i rejects the authenticity of the server *S* and terminates the connection, because U_i finds that the received value M_3^* and the computed value M_3' are not equal. As a result, although the user U_i is a legitimate user, he cannot get connected to the server *S* due to the stolen verifier attack.

3. Proposed Scheme

Chen-Yeh's integrated scheme for authentication and access control was proposed to overcome the drawbacks of Chien-Jan's scheme. Nevertheless, it is still exposed to stolen verifier attacks.

Therefore, the proposed scheme is an extension of Chen-Yeh's scheme. It entails a new integrated scheme that withstands stolen verifier attacks while inheriting all the merits of Chen-Yeh's scheme (see Fig. 2). Some major modifications made to Chen-Yeh's scheme are as follows:

- To prevent stolen verifier attacks, the proposed scheme does not save the smart card identifier CID_u on the server any more, but encrypts it into the user's smart card (see $P_u = h(ID_u \oplus x) \oplus CID_u \oplus h(PW_u)$).
- The proposed scheme uses two timestamps instead of two nonce values. With the use of timestamps, the proposed scheme reduces the computational load of the smart card because it can complete the "login request-verification" phases with only two message exchanges, as opposed to three message exchanges in Chen-Yeh's scheme. This implies that the proposed scheme can greatly increase the efficiency of the authentication and access control process upon the low computational devices such as mobile phones or smart cards.

3.1 Registration Phase

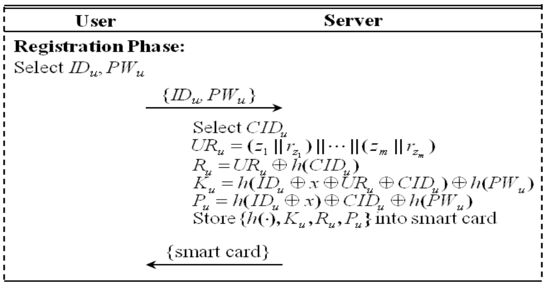
1. The user U_u submits his identity ID_u and password PW_u to the server *S* over a secure communication channel.
2. Upon receiving the message {ID_u, PW_u}, *S* generates a smart card identifier CID_u at random.
3. Now *S* decides which resources to grant and what access rights to be allowed for each resource. Assume that *m* (*m* ≤ *n*) resources are granted to U_u. Assuming further that the indices of *m* granted resources are {z_1, z_2, ⋯, z_m} and r_{z_i} represents the access rights of resource z_i, *S* generates an access control list for U_u, $UR_u = (z_1 \| r_{z_1}) \| (z_2 \| r_{z_2}) \| \cdots \| (z_m \| r_{z_m})$.
4. *S* computes three values R_u, K_u, and P_u, where $R_u = UR_u \oplus h(CID_u)$, $K_u = h(ID_u \oplus x \oplus UR_u \oplus CID_u) \oplus h(PW_u)$, and $P_u = h(ID_u \oplus x) \oplus CID_u \oplus h(PW_u)$. Finally, *S* stores $h(\cdot)$, R_u, K_u, and P_u into a smart card, and issues the smart card to U_u.

3.2 Login Request Phase

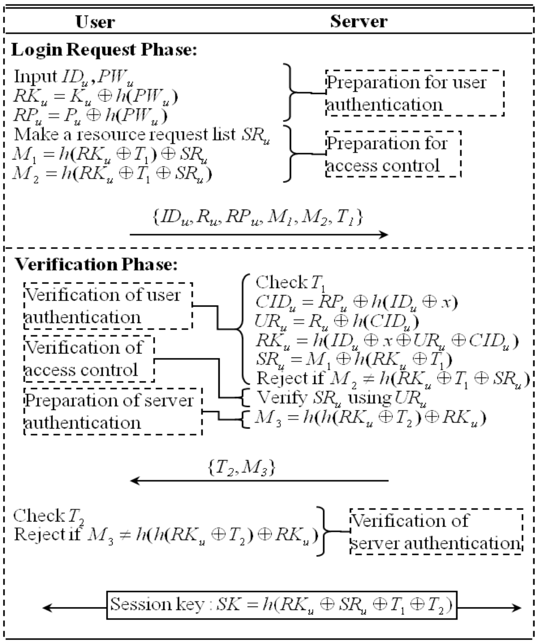
1. *Preparation for user authentication*: The user U_u inserts the smart card into a smart card reader and inputs his identity ID_u and password PW_u. The smart card extracts $RK_u = h(ID_u \oplus x \oplus UR_u \oplus CID_u)$ by calculating $K_u \oplus h(PW_u)$. Note that RK_u plays a role

of the smart card's secret key in the proposed scheme. Similarly, the smart card extracts RP_u = $h(ID_u \oplus x) \oplus CID_u$ by calculating $P_u \oplus h(PW_u)$.

2. *Preparation for access control*: Suppose that U_u attempts to access p resources ($p \le m \le n$) and their indices and access rights are recorded in SR_u = $(z_1' \| r_{z_1'}) \| (z_2' \| r_{z_2'}) \| \cdots \| (z_p' \| r_{z_p'})$. Using SR_u, the smart card computes M_1 = $h(RK_u \oplus T_1) \oplus SR_u$ and M_2 = $h(RK_u \oplus T_1 \oplus SR_u)$, where T_1 is the current timestamp.
3. $U_u \rightarrow S$ $\{ID_u,\ R_u,\ RP_u,\ M_1,\ M_2,\ T_1\}$.



(a) Registration phase.



(b) Login request phase and verification phase.

(Fig. 2) Proposed integrated scheme for authentication and access control.

3.3 Verification Phase

1. *Verification of user authentication*:
   (1) Upon receiving the message $\{ID_u,\ R_u,\ RP_u,\ M_1,\ M_2,\ T_1\}$, the server S examines the freshness of T_1 by checking whether $T' - T_1 \le \triangle T$, where T' is the time that S receives the message and $\triangle T$ is a valid time interval. If T_1 is not fresh, S terminates the current session.
   (2) S gets CID_u by computing $RP_u \oplus h(ID_u \oplus x)$, and also obtains UR_u by computing $R_u \oplus h(CID_u)$.
   (3) Using the two values CID_u and UR_u obtained in the previous step, S computes the smart card's secret key RK_u = $h(ID_u \oplus x \oplus UR_u \oplus CID_u)$ and then extracts SR_u by calculating $M_1 \oplus h(RK_u \oplus T_1)$.
   (4) Using the extracted SR_u, S computes M_2' = $h(RK_u \oplus T_1 \oplus SR_u)$ and checks whether M_2 = M_2'. If yes, S successfully authenticates U_u. Otherwise, S rejects U_u, terminating the current session.
2. *Verification of access control*: By comparing the currently requested resources SR_u with the granted resources UR_u, S verifies whether SR_u is valid. If not valid, S aborts the current session.
3. *Preparation for server authentication*: S computes M_3 = $h(h(RK_u \oplus T_2) \oplus RK_u)$, where T_2 is the new current timestamp.
4. $S \rightarrow U_u$ $\{T_2,\ M_3\}$.
5. *Verification of server authentication*: Upon receiving $\{T_2,\ M_3\}$, the smart card checks the freshness of T_2. If T_2 is not fresh, S terminates the current session. S computes M_3' = $h(h(RK_u \oplus T_2) \oplus RK_u)$ and checks whether M_3 = M_3'. If yes, U_u successfully authenticates S. Otherwise, U_u rejects S.
6. *Creation of session key*: The entire procedure for mutual authentication and access control between U_u and S has just been completed. Now that U_u and S come to know RK_u, SR_u, T_1, and T_2, both of them can use those values to create a session key SK = $h(RK_u \oplus SR_u \oplus T_1 \oplus T_2)$ independently. SK is used to encrypt the subsequent communications between U_u and S.

4. Security Analysis

The proposed method is an integrated approach to manage both authentication and access control. Therefore, it is important to investigate how it reacts against access control-related security attacks as well as authentication-related attacks. Some important security attacks used for the evaluation of authentication and access control are briefly explained below. Furthermore, a number of good features of the proposed scheme as well as how the scheme resists various security attacks are explained below.

- A *replay attack* is a network attack in which a valid data transmission is captured from one session and is replayed or repeated later to attack another session.
- A *parallel session attack* occurs when an intruder uses messages from one session to form messages in another parallel session with fraudulent intentions.
- A *man-in-the-middle attack* is an attack in which an intruder intercepts messages between two communicating parties, forges them, and inserts them back to the networks without either party knowing that the communication session has been compromised.
- In a *stolen verifier attack*, an intruder steals or modifies a verification table stored in a server and uses it to masquerade as a legitimate user or mount a denial-of-service attack.
- An *impersonation attack* occurs as an intruder takes in the identity of the legitimate parties. The impersonation attack is called *masquerading server attack* or *masquerading user attack* if the party to be mimicked is a remote server or a user, respectively.
- A *privilege elevation attack* is a form of access control attacks in which an intruder attempts to gain access privileges that are not granted by a server.

4.1 Analysis from the Perspective of Authentication

- **Stolen verifier attack:** The proposed scheme is free from a stolen verifier attack since it does not store any kind of verification table on the server S.
- **Replay attack:** The proposed scheme resists a replay attack, because the validity of messages can be verified by checking the freshness of timestamps T_1 and T_2.
- **Parallel session attack:** An intruder may attempt a parallel session attack by replaying the response message of the current session as the request message at a later time. However, this attempt is not possible in the proposed scheme because the message structure of M_3 is different from that of M_1 or M_2.
- **Masquerading server attack:** If an intruder wants to masquerade as S, it must be able to forge the valid response message $\{T_2, M_3\}$. However, it is infeasible to compute $M_3 = h(h(RK_u \oplus T_2) \oplus RK_u)$ without the knowledge of RK_u.
- **Masquerading user attack:** If an intruder wants to masquerade as U_u, it must be able to forge the valid message $\{ID_u, R_u, RP_u, M_1, M_2, T_1\}$. However, it is impossible to compute $M_1 = h(RK_u \oplus T_1) \oplus SR_u$ and $M_2 = h(RK_u \oplus T_1 \oplus SR_u)$ without the knowledge of RK_u or SR_u.
- **Man-in-the-middle attack:** An intruder may attempt to alter the request message $\{ID_u, R_u, RP_u, M_1, M_2, T_1\}$ into $\{ID_u, R_u, RP_u, M_1^*, M_2^*, T_1^*\}$, where T_1^* is the current timestamp, and M_1^* and M_2^* are forged values. However, this insidious attempt will fail, because the intruder has no ways to know the smart card secret key RK_u and the resource request value SR_u, both of which are necessary to compute M_1^* and M_2^*. The intruder may also try to alter the server's response message $\{T_2, M_3\}$ into $\{T_2^*, M_3^*\}$. However, he cannot obtain the valid $M_3^* = h(h(RK_u \oplus T_2^*) \oplus RK_u)$, because it requires the knowledge of RK_u.
- **Server secret key guessing attack:** Probably, an attacker attempts to deduce the server secret key x from $K_u = h(ID_u \oplus x \oplus UR_u \oplus CID_u) \oplus h(PW_u)$ and $P_u = h(ID_u \oplus x) \oplus CID_u \oplus h(PW_u)$, both of which are stored in the smart card. However, this attempt will fail because it is computationally infeasible to invert the one-way hash function $h(\cdot)$.
- **Forward secrecy:** A *forward secure* scheme does not reveal any session keys even if the server secret key is revealed by accident. The proposed scheme supports

this useful property of forward secrecy, because the creation of a session key requires four values (i.e., RK_u, SR_u, T_1, and T_2). Besides, even the knowledge of the server secret key, x, does not directly lead to the disclosure of the session key $SK = h(RK_u \oplus SR_u \oplus T_1 \oplus T_2)$.

4.2 Analysis from the Perspective of Access Control

- **Privilege elevation attack:** All the privileges (or access rights) of granted resources are recorded into the symbol UR_u, which is used in computing the smart card secret key RK_u. Assume that an intruder attempts to launch a privilege elevation attack with a forged UR_u*. He should then be able to provide $M_1 = h(RK_u^* \oplus T_1) \oplus SR_u$, where $RK_u^* = h(ID_u \oplus x \oplus UR_u^* \oplus CID_u)$. However, it is impossible for him to derive the correct RK_u^* without the knowledge of other three values ID_u, x, and CID_u. Therefore, the privilege elevation attack will definitely fail.
- **Privacy of access requests:** In the proposed scheme, there are two values UR_u and SR_u to denote the access rights of resources. To protect the privacy of the access requests during the message transmission, the proposed scheme carries those values over the networks in encrypted forms. That is, UR_u is encrypted into R_u by $h(CID_u)$, and SR_u is encoded into M_1 or M_2 by using RK_u and T_1. Therefore, it is difficult to guess UR_u or SR_u without the knowledge of CID_u, RK_u, and T_1, which means that the proposed scheme preserves the privacy of access requests.

4.3 Comparison of Methods

Lee's scheme [13] is vulnerable to privilege elevation attack and does not support mutual authentication. Chien-Jan's scheme [14] is also vulnerable to reflection attacks, parallel session attacks, and privilege elevation attacks. Further it does not protect the privacy of access requests. Chen-Yeh's scheme [15] is an improved version of Chien-Jan's scheme, but is still exposed to stolen verifier attacks because it maintains a smart card identifier table in a remote server.

The proposed method does not keep any kind of verification table on a server, thereby removing the possibility of stolen verifier attacks. In addition, the proposed scheme considerably reduces the computational load of the smart card because it completes the "login request-verification" phases with only two message exchanges, as opposed to three message exchanges in Chen-Yeh's scheme. The comparison between existing methods and the proposed method is well summarized in Table 1.

(Table 1) Comparison of various methods. X: Cannot resist a given attack, O: Can resist a given attack, P: Provided, N/P: Not Provided, *m*: Number of resources granted to a user, *e*: Time for an exponential operation, *h*; Time for a hashing operation, *E*: Time for an encryption operation with a symmetric key, and *i*: *i*-th time authentication ($1 \le i \le N$, where *N* is the permitted number of login times). Note that the hashing time, *h*, is much smaller than *e* or *E*.

Security Attacks		L[13]	CJ[14]	CY[15]	CZ[17]	JCC[18]	Ours
Authentication	Stolen verifier attack	X	X	X	X	O	O
	Mutual Authentication	N/P	P	P	P	P	P
	Session key agreement	N/P	N/P	P	P	P	P
Access control	Privilege elevation attack	X	X	O	X	X	O
	Privacy protection of access requests	N/P	N/P	P	P	P	P
Computational cost	Login request phase	$(2m+1)e+h$	$(m+3)h$	$2h$	$3e+h$	$(i+4)h+2E$	$3h$
	Verification phase	$(2m+2)e+h$	h	$12h$	$(m+6)h$	$3h+3E$	$9h$

Currently, the proposed scheme does not have a password change phase that allows users to update their passwords. As a follow-up study, therefore, we will modify the proposed scheme to support the password change functionality.

5. Conclusion

In this paper, we extend Chen-Yeh's scheme and propose a new integrated authentication and access control scheme that is resilient to stolen verifier attacks while inheriting all the merits of Chen-Yeh's scheme. The proposed scheme resists many possible malicious attacks including replay attacks, parallel session attacks, masquerading server attacks, masquerading user attacks, man-in-the-middle attacks, server secret key guessing attacks, and privilege elevation attacks.

The proposed scheme also exhibits some good useful features such as session key forward secrecy and privacy protection of access requests. Moreover, the proposed scheme completes the "login request-verification" phases with only two message exchanges, greatly increasing the efficiency of the authentication and access control process upon the low computational devices such as mobile phones or smart cards.

참 고 문 헌(Reference)

[1] L. Lamport, Password authentication with insecure communication, CACM 24 (1981), 770-772.

[2] X. Tian, R. Zhu, D. Wong, Improved efficient remote user authentication schemes, International Journal of Network Security 4 (2) (2007), 149-154.

[3] R. R. Ahirwal, Y. K. Jain, An efficient smart card based remote user authentication scheme using hash function, Proceedings of 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (2012), 1-4.

[4] M. Kumar, An enhanced remote user authentication scheme with smart card, International Journal of Network Security 10 (3) (2010), 175-184.

[5] D. Wang, C. Ma, P, Wu, Secure password-based remote user authentication scheme with non-tamper resistant smart cards, Lecture Notes in Computer Science 7371 (2012), 114-121.

[6] C. L. Hsu, Security of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards and Interfaces 26 (3) (2004), 167-169.

[7] S. W. Lee, H. S. Kim, K. Y. Yoo, Improvement of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards and Interfaces 27 (2005), 181-183.

[8] K. C. Leung, L. M. Cheng, A. S. Fong, C. K. Chan, Cryptanalysis of a modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 49 (4) (2003), 1243-1245.

[9] J. J. Shen, C. W. Lin, M. S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 49 (2) (2003), 414-416.

[10] B. Wang, Z.-Q. Li, A forward-secure user authentication scheme with smart cards, International Journal of Network Security 3 (2) (2006), 116-119.

[11] B. W. Lampson, Protection, ACM Operating Systems Review 8 (1) (1974), 18-24.

[12] R. Sandhu, P. Samarati, Access control: principles and practice, IEEE Communications 32 (2) (1994), 40-48.

[13] N. Y. Lee, Integrating access control with user authentication using smart cards, IEEE Transactions on Consumer Electronics, 46 (4) (2000), 943-948.

[14] H. Y. Chien, J. K. Jan, An integrated user authentication and access control scheme without public key cryptography, Proceedings of IEEE 37th Annual International Carnahan Conference on Security Technology (2003), 137-143.

[15] Y. Chen, L. Yeh, An efficient authentication and access control scheme using smart cards, Proceedings of 11th International Conference on Parallel and Distributed Systems (2005), 78-82.

[16] J. K. Jan, Y. M. Tseng, Two integrated schemes of user authentication and access control in a distributed computer network, IEE Proceedings of Computers and Digital Techniques 145 (6) (1998), 419-424.

[17] X. Chengqiang, Z. Zhenli, An integrated one-time-password and access control authentication scheme, IEEE Proceedings of 3rd International Conference on

Computer Science and Information Technology (2010), 252-254.
[18] J. Jeong, M. Chung, H. Choo, Integrated OTP-based user authentication and access control scheme in home networks, Lecture Notes in Computer Science 4773 (2007), 123-133.

◐ 저 자 소 개 ◑

김 용
1986년 전북대학교 문헌정보학과 졸업 (문학사)
1995년 Univ. of North Texas 정보과학과 졸업 (정보학석사)
1996년~2008년 KT 서비스개발연구소 (책임연구원)
2002년 충남대학교 컴퓨터과학과 졸업 (이학석사)
2006년 연세대학교 문헌정보학과 정보학 전공 졸업 (문학박사)
2008년~현재 전북대학교 문헌정보학과 교수
관심분야 : 디지털도서관, 시맨틱 웹, 웹 마이닝, 스마트 카드, 정보 보호
E-mail : yk9118@jbnu.ac.kr

정 민 교
1985년 서울대학교 컴퓨터공학과 졸업 (공학사)
1987년 KAIST 컴퓨터학과 졸업 (공학석사)
1996년 University of Iowa 컴퓨터학과 졸업 (공학박사)
1987년~2000년 KT 멀티미디어 연구소 (전임 연구원/선임 연구원)
2001년~2002년 Vivcom Inc. (Founder & Engineering Director)
2003년~현재 서울여자대학교 정보미디어대학 교수
관심분야 : 컴퓨터 비전, 패턴인식, 기계학습, 영상처리, 정보보호, 생체인식
E-mail : mchung@swu..ac.kr