Smart Card Based User Authentication Scheme Secure Against Password Guessing Attack

Young-Do Joo*

요 약

최근 Yoon 등은 스마트카드를 이용하여 원격지에 있는 사용자를 인증할 수 있는 개선된 스킴을 제안하였다. Yoon 등은 인증 서버의 비밀키 유출과 도용 시에도 보안성이 있으며, 사용자와 인증서버 간 상호인증이 가능한 효율적인 사용자 인증 방법을 소개하였다. 그러나 패스워드 기반 스마트카드를 이용한 사용자 인증 스킴에서 고려하는 보안 요구사항을 완전히 만족하지 못하고 있다. 본 논문에서는, 허가받지 않은 침입자가 사용자의 스마트카드를 훔치거나 일시적으로 접근할 수 있는 경우에 Yoon 등의 스킴이 오프라인 패스워드 추측공격에 취약하다는 것을 밝혀낸다. 따라서 제안하는 사용자 인증 스킴은 이와 같은 보안 문제를 해결하기 위해 Hash 함수와 랜덤 nonce를 기반으로 패스워드 추측공격을 포함한 다양한 공격에 견딜 수 있는 개선안을 제시한다. 보안성을 위한 비교분석을 통해 제안하는 인증 스킴은 무시할 정도의 exclusive-OR 연산의 수행이 조금 더 요구되지만, Yoon 등의 인증 스킴보다 안전하고 효율적인 스킴임을 알 수 있다.

ABSTRACT

Recently Yoon et al. proposed the remote user authentication scheme using smart cards. But their scheme has not satisfied security requirements which should be considered in the user authentication scheme using the password based smart card. In this paper, we prove that Yoon et al.'s scheme is vulnerable to a password guessing attack in case that the attacker steals the user's smart card and extracts the information from the smart card. Accordingly, this paper proposes the improved user authentication scheme based on the hash functin and random nonce that can withstand various possible attacks including a password guessing attack. The result of comparative analysis demonstrates that the proposed scheme is more secure and efficient than Yoon et al.'s scheme, with a trivial trade-off to require just a few more exclusive-OR operations.

Keywords : User Authentication, Smart Card, Password Guessing Attack, Scheme, Mutual Authentication

* Division of Computer and Media Information Engineering, Kangnam university, Professor
* Corresponding Author (ydjoo@kangnam.ac.kr)
접수일자 : 2011년 07월 15일, 수정일자 : 2011년 08월 04일, 심사완료일자 : 2011년 08월 26일

Ⅰ. Introduction

With the rapid growth of computer networks, the achievement of secrecy and authentication has become increasingly important. A remote user authentication scheme allows a server to check the authenticity of a remote user through insecure channels like Internet. A variety of schemes have been proposed so far[1-8][11-14] through various ways of improvements.

After Lamport[1] introduced a password-based remote user authentication scheme in 1981, several schemes[2,3] were proposed to improve the security and the efficiency. However, these schemes suffered the risk of stolen password table and the high cost of maintaining and protecting the password table within the authentication server. Accordingly, Hwang and Li[4] proposed a new user authentication scheme using smart cards to eliminate such risk and cost to have to keep the password table. Later, more effective smart card based remote user authentication schemes[5,6] were proposed to enhance the efficiency of Hwang and Li's scheme.

More recently, Yoon et al.[7] proposed more secure and efficient enhancement than those of any previously proposed schemes. They claimed that their scheme is secure even if the secret key of the server is leaked or is stolen, and enables users to update their passwords securely while providing mutual authentication to allow higher security.

However, Yoon et al.'s scheme is insecure when an attacker may steal a user's smart card and then extract the information from it. In other words, their scheme can not resist the password guessing attack using stolen smart card in which the unauthorized users can successfully masquerade as the legitimate user. As pointed out in references[9,10], all existing smart cards have security weakness in that the secret values stored in it could be leaked by monitoring the power consumption.

As a result, an attacker can make another card digitally identical to the original card by obtaining the secrete keys and launch the off-line password guessing attack to seek the user's password. Accordingly, this paper demonstrates the security leak of Yoon et al.'s scheme and presents an enhancement to resolve such vulnerability.

The remainder of this paper is organized as follows. Section II reviews Yoon et al.'s scheme followed by its weakness. In section III, the proposed scheme is introduced and the security and efficiency of the proposed scheme are discussed. Final conclusions are briefly given in section IV.

Ⅱ. Review of Yoon et al.'s Scheme

This section briefly reviews the smart card based remote authentication scheme proposed by Yoon et. al.[7]. Their scheme is composed of registration, login, authentication and password change phase. For readers' understanding, the abbreviations and notations used through this paper are defined in Table 1.

표 1. 약어 및 표기
Table 1. Abbreviations and Notations

U_i	user i
ID_i	identifier of the user i
PW_i	password of the user i
S	authentication server
x	secret key of authentication server, S
h()	secure one-way hash function
⊕	exclusive-OR operation

1. Yoon et al.'s Scheme

▪ **Registration Phase**

This phase is invoked when a user Ui wants

to register authentication server, S. It comprises the following steps.

(1) Ui submits his identifier IDi and password PWi to S through a secure channel.

(2) Upon receiving the registration request, S computes Vi=h(IDi,Ttsa,x) and Ai=Vi⊕PWi, where x is a secret key maintained by S and Ttsa is time stamp provided by TSA(Time Stamp Authority).

(3) S issues the smart card written by personalized information, {IDi,Vi,Ai,h()}.

▪ **Login Phase**

This phase is invoked when Ui logins to S. To access S, Ui inserts his smart card into the card reader and keys in IDi and PWi*. The smart card performs the following operations.

(1) Computes Bi=Ai⊕PWi* and verifies the equality of Bi and Vi. If they are identical, then computes C1=h(Bi,T), where T is the current date and time of the input device.

(2) Sends a login request, {IDi,C1,T} to S.

▪ **Authentication Phase**

Upon receiving the login request message, {IDi,C1,T}, the server and user's smart card perform the following steps for mutual authentication between the user, Ui and the server, S.

(1) S checks the format of IDi. If the format is invalid, the login request is rejected.

(2) S verifies the freshness of T. If (T'−T) ≥ △T, where T' is the server's current time and △T is the expected valid time interval for a transmission delay, S rejects the login request.

(3) S computes Bi*=h(IDi,Ttsa,x) and C1*=h(Bi*,T) and then compares C1 and C1*. If they are equal, then S accepts the login request and proceeds to the next steps, otherwise it rejects the login request.

(4) S computes C2=h(Bi*,C1*,T") after obtaining the current time T", and then sends back the message, {C2,T"} to Ui.

(5) Upon receiving the message, {C2,T"}, Ui's smart card verifies the validity of the time interval between T" and its current time, T"', then computes C2*=h(Bi,C1,T"). If C2 and C2*are equal, Ui accepts the authenticity of S, otherwise Ui interrupts the connection.

▪ **Password Change Phase**

This phase is invoked when Ui wants to change his password from PWi to PWi'. The smart card performs the following operations.

(1) Computes Bi=Ai⊕PWi*<=h(IDi,Ttsa,x)> and compares Bi and Vi. If they are equal, the smart card let Ui select a new password PWi', otherwise it rejects the password change request.

(2) Computes Ai'=Bi⊕PWi' and stores Ai' into the smart card in place of Ai.

2. Security Flaw of Yoon et al.'s Scheme

This section demonstrates that Yoon et al.'s scheme is vulnerable to the password guessing attack if an attacker, Ua steals Ui's smart card and extracts the values in it by some means[9,10] without being noticed. If Ua acquires Vi, Ai and h(), then he can guess Ui's password by the following attacking procedures.

Step 1: The legal user, Ui generates login request message, {IDi,C1,T} and sends it to the authentication server, S.

Step 2: At that time, the attacker, Ua intercepts the login request message and obtains C1 and T.

Step 3: Ua starts off−line password guessing attack by utilizing the information acquired. The scenario of Ua to catch the password of Ui is as follows.

(1) Guesses PWi" as the user's password.

(2) Computes C1"=h(Bi,T)=h(A⊕PWi",T).

(3) Verifies the correctness of PWi" by

checking C1"=C1.

(4) Repeats procedures above (1) through (3) until PWi" satisfies the condition of (3).

Finally, the attacker, Ua can find the correct password. In addition, the attacker can simply calculate the correct password out of PWi=Ai⊕Vi by using the values, Ai and Vi. Accordingly, Yoon et al.'s remote user authentication scheme has security flaw to allow for the password guessing attack in which the unauthorized attacker can successfully masquerade as the legitimate user.

Ⅲ. Improvement of Yoon et al.'s Scheme

In this section, an enhancement of Yoon et al.'s scheme is proposed that can withstand the security flaw described in the previous section. The security of the proposed scheme is based on a one-way hash function and random nonce, and consists of registration, login, authentication and password change phase.

1. Proposed Scheme

▪ Registration Phase

Fig. 1 illustrates the registration phase in the proposed scheme. When a user, Ui wants to register authentication server, S, the following steps are executed.

(1) Ui selects his identifier IDi and password PWi and submits (IDi,PWi) to S through a secure channel.

(2) Upon receiving the registration request, S computes the equations (1) and (2).

$$V=h(IDi,Ttsa,x) \quad (1)$$

$$Ai=V\oplus PWi \quad (2)$$

where x is a secret key maintained by S and Ttsa is time stamp provided by TSA(Time Stamp Authority).

(3) S personalizes the smart card with the secure information, {IDi,Ai,h()}.

▪ Login Phase

Fig. 2 illustrates the login and authentication phases in the proposed scheme. To access S, Ui inserts his smart card into the card reader and keys in IDi and PWi. The smart card performs the following operations.

(1) Computes the next equations.

$$Bi=Ai\oplus PWi \quad (3)$$

$$Ci=Bi\oplus Ni \quad (4)$$

$$Vi=h(IDi,Ci,Ni) \quad (5)$$

where Ni is a random nonce generated by smart card.

(2) Sends a login request, {IDi,Ci,Vi} to S.

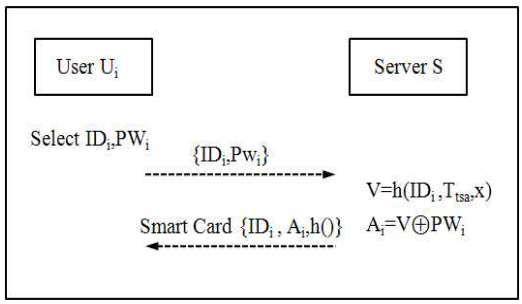

그림 1. 제안하는 스킴의 등록단계
Fig 1. Registration Phase of Proposed Scheme

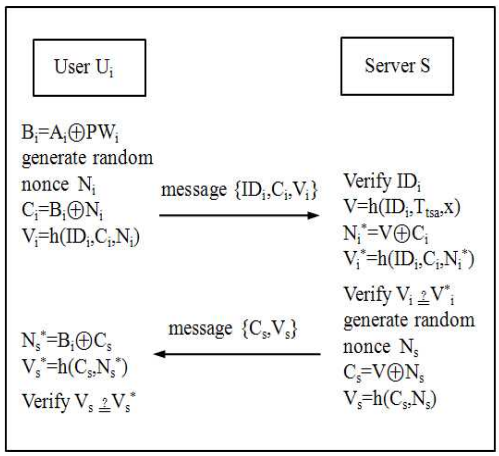

그림 2. 제안하는 스킴의 로그인 단계와 인증 단계
Fig 2. Login and Authentication Phases of Proposed Scheme

▪ **Authentication Phase**

Upon receiving the login request message, {IDi,Ci,Vi}, the server and user's smart card perform the following steps for mutual authentication.

(1) S verifies the format of IDi. If the format is invalid, the login request is rejected.

(2) S computes the following equations.

$$V=h(IDi,Ttsa,x) \quad (6)$$

$$Ni*=V\oplus Ci \quad (7)$$

$$Vi*=h(IDi,Ci,Ni*) \quad (8)$$

If Vi=Vi*, S accepts the login request by authenticating Ui.

(3) S generates random nonce, Ns and computes the next equations.

$$Cs=V\oplus N \quad (9)$$

$$Vs=h(Cs,Ns) \quad (10)$$

S sends back the message, {Cs,Vs}.

(4) Upon receiving the message, {Cs,Vs}, the smart card computes the following equations.

$$Ns*=Bi\oplus Cs \quad (11)$$

$$Vs*=h(Cs,Ns*) \quad (12)$$

If Vs and Vs* are equal, Ui accepts the authenticity of S, otherwise Ui interrupts the connection.

▪ **Password Change Phase**

When Ui wants to change his password from PWi to PWi_new, the smart card performs the following operations.

(1) Computes Bi=Ai⊕PWi and compares Bi and Vi. If they are equal, the smart card let Ui select a new password PWi_new.

(2) Computes Ai_new=Bi⊕PWi_new and stores Ai_new into the smart card in place of Ai.

2. Security Analysis

The proposed scheme presents an improvement to Yoon et al.'s scheme in order to eliminate the security leak mentioned previously. This section investigates the security robustness of the proposed scheme to endure the well-known hacking activities such as password guessing attacks, relay attacks and forgery attacks.

For password attacks, an attacker intercepts messages {IDi,Ci,Vi} and {Cs,Vs} over a public network and Ai, h() from the user's smart card. However, the attacker can not derive the password PWi' from Ci=Bi⊕Ni=Ai⊕PWi⊕Ni and Cs=V⊕Ns=h(IDi,Ttsa,x)⊕Ns as introduced in the proposed scheme. This is infeasible, because the random nonce values Ni, and Ns as well as hash function h() have to be obtained.

For forgery attack, an attacker, Ua tries to impersonate the legitimate user, Ui by modifying the login request {IDi,Ci,Vi} into {IDi,Ca,Va} and sending it to the server. However, such a forgery can not pass the authentication phase because the attacker has no way of obtaining the value V=h(IDi,Ttsa,x) to compute the valid parameter Vi*. Similarly, the attacker is also unable to masquerade the server to the user.

In this improved scheme, the user's smart card updates a random nonce at each login. Accordingly, the replay of an old login message {IDi,Ci,Vi} in the login phase does not work due to the new random nonce, Ni generated at each session. The replay of the server's response message, {Cs,Vs} also fails in the authentication phase owing to the random nonce, Ns.

Table 2 shows the comparison of security properties of Yoon et al.'s scheme and the proposed scheme. In addition, the computation costs at all the phases of both schemes are summarized.

As you notice from Table 2, the proposed scheme is more secure with respect to security properties. In contrast to Yoon et al.'s scheme, the proposed scheme requires a few more exclusive-OR operations whose time is trivial to be ignored. Therefore, the security efficiency of the proposed scheme is relatively higher.

표 2. 안전성 비교 분석
Table 2. Comparative Security Analysis

Security Properties	Yoon et al.'s Scheme	Proposed Scheme
Password Guessing Attack	Yes	No
Forgery Attack	Yes	No
Replay Attack	No	No
Computation Cost	Yoon et al.'s Scheme	Proposed Scheme
Registration Phase	1T(h)+1T(⊕)	1T(h)+1T(⊕)
Login Phase	1T(h)+1T(⊕)	1T(h)+2T(⊕)
Authentication Phase	4T(h)	4T(h)+3T(⊕)
Password Change Phase	2T(⊕)	2T(⊕)

*T(h):hash 연산시간, T(⊕):exclusive-OR 연산시간

IV. Conclusions

In the current paper, an enhancement to Yoon et al.'s scheme was proposed. The proposed scheme demonstrated that Yoon et al.'s scheme is vulnerable to off-line password guessing attack if the smart card is stolen and the secret information is leaked. Consequently, this paper presented an improved user authentication based on hash functions and random nonce values, in order to resolve such security problem.

According to comparative analysis of security, the proposed scheme is more secure and efficient with the trivial trade-off to entail just a few more exclusive-OR operations while keeping the same merits of as Yoon et al.'s scheme to provide resonable secureness.

Acknowledgement

This work was supported by Kangnam University Research Grant in 2011.

References

[1] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[2] R. E. Lennon, S. M. Matyas and C. H. Mayer, "Cryptographic Authentication of Time-invariant Quantities," IEEE Trans. Commun., COM-29, Vol. 6, pp. 773-777, 1981.

[3] S. M. Yen and K. H. Liao, "Shared Authentication Token Secure against Replay and Weak Key Attack," Information Proceeding Letters, pp. 78-80, 1997.

[4] M. S. Hwang and L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards," IEEE Trans. Consum. Electron, Vol. 46, No. 1, 2000.

[5] H. M. Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards," IEEE Trans. Consum. Electron, Vol. 46, No. 4, 2000.

[6] M. S. Hwang, C. C. Lee and Y. L. Tang, "A Simple Remote User Authentication," Math. Comput. Model, Vol. 36, pp. 103-107, 2002.

[7] E. J. Yoon, E. K. Ryu and K. Y. Yoo, "An Improvement of Hwang-Lee-Tang's Simple Remote User Authentication," Computer & Security, Vol. 24, pp. 50-56, 2005.

[8] J. Xu, W. T. Zhu and D. G. Feng, "An Improved Smart Card Based Password Authentication Scheme with Provable Security," Computers Standards & Interfaces, Vol. 31, pp. 723-728, 2009.

[9] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," Proceedings of Advances in Cryptology (CRYPTO 99), pp. 388 - 397,

1999.

[10] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks," IEEE Transactions on Computers, Vol. 51, No. 5, pp. 541 - 552, 2002.

[11] C. W. Lin, C. S. Tsai and M. S. Hwang, "A New Strong-Password Authentication Scheme Using One-Way Hash Functions," Journal of Computer and Systems Sciences International, Vol. 45, No. 4, pp. 623-626, 2006.

[12] X. Duan, J.W. Liu and Q. Zhang, "Security Improvements on Chien et al.'s Remote User Authentication Scheme Using Smart Cards," IEEE International Conference on Computational Intelligence and Security (CIS 2006), Vol. 2, pp. 1133-1135, 2006.

[13] Y. S. Lee and D. H. Won, "Security Analysis and Improvement on Remote User Authentication Scheme," Journal of Korea Society of Computer and Information, Vol. 15, No. 1, pp. 139-147, Jan. 2010.

[14] Y. H. An and J. M. Suh, "Security Improvement on Remote User Authentication Scheme Using Smart Cards," Journal of Korea Society of Computer and Information, Vol. 15, No. 3, pp. 91-97, March 2010.

저자약력

주 영 도(Young-Do Joo) **정회원**

1983 한양대학교 전자통신공학과 학사
1988 남플로리다 주립대학 컴퓨터공학과 석사
1995 플로리다 주립대학 전산학과 박사
현재 강남대학교 컴퓨터 미디어공학부 교수

<관심분야> 정보보호, 정보검색, 지능형시스템