https://doi.org/10.33778/kcsa.2020.20.4.209

Security Enhancement of Lightweight User Authentication Scheme Using Smartcard

Youngsook Lee*

ABSTRACT

The environment of the Internet provides an efficient communication of the things which are connected. While internet and online service provide us many valuable benefits, online services offered and accessed remotely through internet also exposes us to many different types of security threats. Most security threats were just related to information leakage and the loss of authentication on client-server environment. In 2016, Ahmed et al. proposed an efficient lightweight remote user authentication protocol. However, Kang et al. show that it's scheme still unstable and inefficient. It cannot resist offline identity guessing attack and cannot provide session key confirmation property. Moreover, there is some risk of biometric information's recognition error. In this paper, we propose an improved scheme to overcome these security weaknesses by storing secret data in device. In addition, our proposed scheme should provide not only security, but also efficiency since we only use hash function and XOR operation.

스마트카드를 이용한 안전한 경량급 사용자 인증 스킴의 설계

이 영 숙*

요 약

인터넷을 통한 통신환경은 연결 가능한 사물들 간에 효율적인 통신을 제공한다. 이런 환경에서의 정보통신은 우리에게 편리함을 제공하기는 하나 여러 형태의 보안위협이 도사리고 있는 실정이다. 인터넷을 이용하여 원격으로 접속하여 제공받는 서비스에 존재하는 보안위협 중 대부분은 전송되는 정보의 유출과 클라이언트 서버 간 인증에 대한 손실이다. 2016년 Ahmed 등이 스마트카드를 이용한 안전한 경량급 사용자 인증 스킴을 제안하였다. 그러나 Kang등이 제안한 논문에서 그들이 제안 프로토콜은 identity guessing attack에 취약하고 session key confirmation을 달성할 수 없다는 것을 주장하였다. 본 논문은 Ahmed 등이 제안한 논문의 취약점을 개선하여 더욱 안전하고 효율적인 경량급 사용자 인증 스킴을 제안하였다.

Key words : User Authentication Scheme, Smart Card, Session Key, Hash function, Idendity Guessing Attack

접수일(2020년 09월 01일), 수정일(1차: 2020년 10월 15일), (2차: 2020년 10월 22일), 게재확정일(2020년 10월 29일)

* 호원대학교 IT소프트웨어보안학과

1. 서 론

The environment of the internet concept is growing quite popular which is all about control and automation, reducing expenses, efficient communication of the things which are connected[1]. While internet and online service provide us many valuable benefits, online services offered and accessed remotely through internet also exposes us to many different types of security threats. Most security threats were just related to information leakage and the loss of authentication on client-server environment. In fact, the communication opens the door to attackers to intercept messages, insert forged data or impersonate users. Thus, robust security mechanisms must be deployed in order to prevent illegal access of unauthorized parties. However, the limited size of communication resources implies other constraints such as limited energy and computation capabilities. Therefore, authentication scheme designed for a secure and lightweight communication aim to save network communication resources and low computation cost[2].

In 2016, Ahmed et al proposed an efficient lightweight user authentication protocol using smart card[3]. In their article, they claim that the user can be authenticated using a biometric information and establishers the session key to be shared with between the remote server and the user. However, in [4], Kang et al. uncover Ahmed et al.'s scheme also showed weaknesses and scheme's progress was incomplete. They show that it's scheme still unstable and inefficient. It cannot resist offline identity guessing attack and cannot provide session key confirmation property. Moreover, there is some risk of biometric information's recognition error[5 ,6, 7].

Now, we proposed improved Ahmed et al..'s protocol for lightweight user authentication environment. This study proposes a security enhanced remote user authentication scheme and provides a security analysis and formal analysis. Finally, the efficiency analysis reveals that the proposed scheme can protect against several possible types of attacks with only a slightly high computational cost.

2. The proposed a Lightweight User Authentication Scheme

This section presents our lightweight user authentication scheme for open networks, etc. The scheme participants include a remote user, and a server. For simplicity, we denote the remote user by U_i, and the server by S. Our scheme consists of three phases: registration phase, login phase, and authentication phase. The registration phase is performed only once per user when a new user registers itself. The authentication phase is carried out whenever a user wants to gain access to the remote server. The system parameters listed in Table 1 are assumed to have been established in advance before the scheme is used in practice.

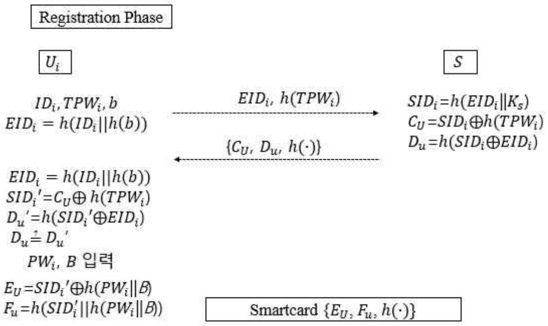
<Table 1> Notation

U_i	device of entity U_i
ID_i	identity of an entity U_i
SID_i	identity of a server S
B	the feature of the user U_i's biometric information(generated the biometric information B by using the fuzzy extractor)
K_s	the secret key of the server S
T_i	timestamp of current time i
ΔT	the maximum allowed time interval for transmission delay
$h()$	one-way hash function
$\|\|$	concatenation operation

$\oplus$	XOR operation

2.1 Registration Phase

This is the phase where a new registration of a user takes place. The reiteration phase is described in Figure1. Prior to the begging the registration phase, the biometric encryption will take place by using a fuzzy commitment scheme as in [5, 6]. The user U_i computes B by using a biometrics scanning device. The registration proceeds as follows:



(Figure 1) Registration Phase

Step 1. User U_i chooses its identity ID_i, temporary password TPW_i, and random number b. U_i computes $EID_i = h(ID_i \| h(b))$. Then sends the registration request message ⟨ EID_i, $h(TPW_i)$ ⟩ to remote server S via a secure channel.

Step 2. Upon receiving the request ⟨ EID_i, $h(TPW_i)$ ⟩, remote server S computes

$SID_i = h(EID_i \| K_s)$,

$C_u = SID_i \oplus h(TPW_i)$,

$D_u = h(SID_i \oplus EID_i)$.

Then, S issues a smart card and stored $\{C_u, D_u, h(\cdot)\}$ into a smart card and sends it to U_i via a secure channel.

Step 3. U_i inserts a smart card into a card reader and its identity ID_i, temporary password TPW_i, and chosen random nonce b once again. Smart card computes

$EID_i = h(ID_i \| h(b))$,

$SID_i' = C_u \oplus h(TPW_i)$,

$D_u' = h(SID_i' \oplus EID_i)$.

Smart card verifies than D_u equals D_u'. If this condition hold, smart card terminate the registration session.

Step 4. Now the user U_i chooses its own password PW_i and imprints biometric information B such as fingerprint, iris, etc. Smart card computes

$E_u = SID_i' \oplus h(PW_i \| B)$,

$F_u = h(SID_i' \| PW_i \| B))$.

Then, U_i stores the values $\{E_u, F_u, , h(\cdot)\}$ on its smart card.

2.2 Login Phase

This phase is carried out whenever the user wants to gain access to the server S. This scheme carry the login phase out as shown in Figure 2.

Step 1. U_i inserts its smart card into card reader, and inputs ID_i, PW_i, B.

Step 2. Smart card computes

$SID_i'' = E_u \oplus h(PW_i \| B)$,

$F_u' = h(SID_i'' \| h(PW_i \| B))$.

Smart card checks that whether F_u' equals F_u or not. If the value is not equal, U_i rejects the login request. Otherwise, the application is proceeded.

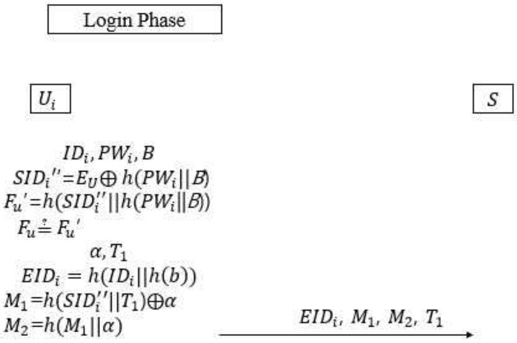
Step 3. Smart card continually picks up rhe current timestamp and generates the random nonce α. Then, computes

$EDI_i = h(ID_i \| h(b))$,

$M_1 = h(SID_i'' \| T_1) \oplus \alpha$,

$M_2 = h(M_1 \| \alpha)$.

Step 4. After that, U_i sends $<EID_i, M_1, M_2, T_1>$ to the server S via public channel.



(Figure 2) Login Phase

2.3 Authentication and key agreement Phase

2.3.1 Authentication Phase

With the four login request message $\langle EID_i, M_1, M_2, T_1 \rangle$, the scheme enters the authentication phase during which S performs the following steps:

Step 1. When the login request arrives $\langle EID_i, M_1, M_2, T_1 \rangle$, the server S retrieves the current timestamp T_2 and verifies the freshness of the U_i's timestamp T_1 using $(T_2 - T_1) \le \Delta T$. The server S aborts if the check T_1 fail. Otherwise, S picks up the current timestamp T_3 and computes

$\alpha' = M_1 \oplus h(SID_i' \| T_1)$,

$M_2' = h(M_1 \| \alpha')$.

The server S verifies that $M_2 = M_2'$. If the verification fails, S aborts the scheme. Otherwise, generates a random number β and retrieves the current timestamp T_3. The server S computes

$M_3 = h(SID_i' \| T_3) \oplus \beta$,

$M_4 = h(M_3 \| \beta)$,

$SK_s = h(\alpha \| \beta \| EID_i \| SID_i)$.

After that, the server S sends the message $\langle M_3, M_4, T_3, SK_s \rangle$ to the user U_i.

Step 2. After receiving $\langle M_3, M_4, T_3, SK_s \rangle$ from S, the user U_i obtains the current timestamp T_4 and computes

$\beta' = M_3 \oplus h(SID_i \| T_3)$,

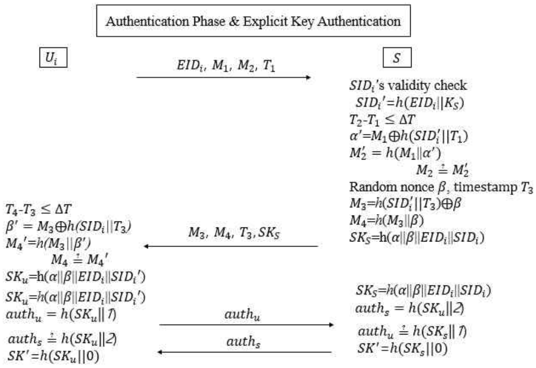
$M_4' = h(M_3 \| \beta')$,

$SK_u = h(\alpha \| \beta' \| EID_i \| SID_i')$.

The user U_i verifies that (1) $T_4 - T_3 \le \Delta T$ (2) M_4 equals M_4'. If both of these conditions are hold, U_i accepts as authentic the server. Otherwise, U_i stop the following procedure.

Step 3. U_i computes $auth_u = h(SK_u \| 1)$ and sends $auth_u$ to the server . Similarly, the server S computes $auth_s = h(SK_s \| 2)$ and sends $auth_s$ to the user.

Step 4. Upon receiving $auth_s$, the user U_i checks the equality $auth_s \stackrel{?}{=} h(SK_u \| 2)$. If they are equal, then U_i computes it final session key SK' as $SK' = h(SK_u \| 0)$. Otherwise U_i aborts the scheme. Likewise, the server S, after receiving $auth_u$, verifies that $auth_u$ equals $h(SK_s \| 1)$. If so, then the server S computes the final session key SK' as $SK' = h(SK_s \| 0)$. Otherwise, S aborts the scheme. This procedure of adding explicit authentication is outlined in Figure 3.



(Figure 3) Authentication Phase

3. Security Analysis in the

Proposed Scheme.

This section describes the security analysis to confirm the our propose scheme. We need to provide the following definitions to then compare the proposed scheme to othere authentication schemes, including that 2016 proposed by Ahmed et al's scheme.

Definition 1. A strong secret key $(\alpha,\ \beta)$ has a high value of entropy SK that cannot be find out in polynomial time.

Definition 2. A secure one-way hash function $y = f(x)$ is the following. Given x to compute y is easy but y to compute x is very hard.

Definition 3. A fuzzy extractor prevents biometric errors.

3.1 Biometric recognition error

The proposed our scheme prevents a biometric recognition error by using fuzzy extraction. Ahmed et al.'s scheme use a hash function to check for conformity in the biometric information. Even if they use a threshold τ, because the hash function makes slight differences in the input data that produces very large differences in the output data. It is possible for biometric recognition errors to occurs. However, our proposed scheme described using fuzzy recognition errors. Generated the biometric information B by using the fuzzy extractor is a uniform and random string. Even if, the user inputs slightly differences biometrics, so the our proposed scheme is secure against a biometric recognition error [6, 7, 11].

3.2 Key authentication

3.2.1 Implicit key authentication

The fundamental security goal for a key exchange scheme to achieve is implicit key authentication. Loosely stated, a key exchange scheme is said to achieve implicit key authentication if each party trying to establish a session key is assured that no other party aside from the intended parties can learn any information about the session key. Our scheme guarantees the implicit key authentication. Namely, without knowing PW_i, no one computes the session key. In the scheme, the session key SK is computed as $SK_s = h(\alpha \| \beta \| EID_i \| SID_i)$. Since h is a one-way hash function, SK cannot be obtained without knowing the common secrete value α, β. We claim that only U_i and S can compute this common secrete value.

3.2.1 Explicit key authentication

Another stronger kind of security goal for a key exchange scheme to achieve is explicit authentication, the property obtained when both implicit authentication and key confirmation hold. It is straightforward to see that our scheme does not achieve explicit authentication. However, it is easy to transform any key exchange scheme P with implicit authentication into a scheme P' providing explicit authentication by using standard techniques [9,10].

The transformation works as follows. Suppose that in scheme P, two agents U_i and S ended up with computing their session key SK_u and SK_s, respectively. In scheme X', user U_i sends one additional flow $auth_u = h(SK_u \| 1)$ to the server S and similarly, server S sends $auth_s = h(SK_s \| 2)$ to user U_i. Upon receiving $auth_s$, user U_i checks the equality $auth_s \stackrel{?}{=} h(SK_u \| 2)$. If they are equal, then U_i computes its final session key SK' as $SK' = h(SK_s \| 0)$. Otherwise, U_i aborts the scheme. Likewise, the remote server S, after receiving $auth_u$, verifies that

$auth_u$ equals $h(SK_s\|1)$. If so, then the server S computes the final session key SK' as $SK' = h(SK_s\|0)$. Otherwise, S aborts the scheme.

3.3 Offline identity guessing attack

The vulnerability of Ahmed et al.'s scheme to the identity guessing attack is due to the following fact: to find out the identity of the user, they suffic e to obtain the information stored in its smart card and read the exchanged message between the serve r and the remote user. More concretely, the proble m with Ahmed et al.'s scheme is that whoever o btains these values of b stored in U_i's smart card, the part of the user U_i's login message EID_i can b reak the user U_i's identity ID_i. But, our proposed s cheme effectively defeats these kind of attacks men tioned above Even if the attacker obtains the infor mation (i.e., E_u, F_u) stored in the smart card and t he exchanged message between the server and the user, he/she can no longer find out the identity of t he user U_i. In the proposed scheme, the only infor mation related to identity is $EID_i(=h(ID_i\|h(b)))$, b ut because b is the secret information that the user only knows, this value does not help the attacker to verify directly the correctness of guessed identity. Thus, off-line identity guessing attacks would be u nsuccessful against the proposed scheme. Hence, ou r proposed scheme guarantees user anonymity [8,9].

4. Conclusion

Now, we proposed improved Ahmed et al..'s li ghtweight user authentication. Some modifications are accomplished to improve their scheme. In othe r words, no combination of transmission message s reveal user's identity and secret session key. Th e improved scheme not only provides user anony mity against passive adversaries and malicious us ers, but also is resistant to known session key att acks. It is still efficient and suitable for invironme nt by using only low-cost functions such as one way hash functions and exclusive-OR operations. Therefore, the proposed scheme is more secure an d still efficient lightweight user authentication.

Reference

[1] Omar Cheikhrouhou, Anis Koubaa, Manel Boujelben, and Mohamed Abid, "A Lightweight User Authentication Scheme for Wireless Sensor Networks", Ad Hoc Networks, Vol. 9, No. 5, pp. 727-735, 2011.

[2] Hwang, Min-Shiang, and Li-Hua Li, "A new remote user authentication scheme using smart cards." IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28-30, 2000.

[3] Al_Sahlani, Ahmed YF, and Songfeng Lu, "Lightweight Communication Overhead Authentication Scheme Using Smart Card." Indonesian Journal of Electrical Engineering and Computer Science Vol. 1, No. 3, pp. 597-606, 2016.

[4] D. Kang, J. Jung, H. Yang, Y. Choi, and D Won, "Cryptanalysis of Lightweight User Authentication Scheme Using Smartcard", AHFE 2017, Los Angeles, USA, pp. 78-84, 2017.

[5] Y. Lee, "Security Analysis of a Biometric-Based User Authentication Scheme", The Korea-Society of Digital Industry& Information Management, Vol. 10, No.1, pp. 81-87, 2014.

[6] Y. Choi, Y. Lee, D. Won, "Security Improvement on Biometric Based Authentication Scheme for Wireless Sensor Networks Using Fuzzy Extraction", International Journal of Distributed Sensor Networks Volume 2016, Article ID 8572410, 16 pages http://dx.doi.org/10.1155/2016/8572410, 2016.

[7] Y. Lee, "Security Analysis to an Biometric Authentication Protocol for wireless Sensor Networks", The Korea-Society of Digital Industry& Information

Management, Vol. 11, No. 1, pp. 59-67, 2015.

[8] Lee, Hanwook, et al., "Forward Anonymity-Preserving Secure Remote Authentication Scheme." KSII Transactions on Internet & Information Systems, Vol. 10, No. 3, 2016.

[9] Chien, Hung-Yu, and Che-Hao Chen, "A remote authentication scheme preserving user anonymity", Advanced Information Networking and Applications, AINA 2005 19th International Conference on. Vol. 2. IEEE, 2005.

[10] Y. Lee, J. Nam, J Kwak, and D Won, "Password-Only Authenticated Key Exchange Between Two Agents in the Four-Party Setting", KES-AMSTA, LNAI 4496, pp. 616 - 625, 2007.

[11] Y. Lee, "Security Enhancement to an Biometric Authentication Protocol for WSN Environment", Journal of Information and Security, Vol. 10, No. 1, pp. 83−88, 2016.

〔저자소개〕

이 영 숙 (Youngsook Lee)

2009년 ~ 현재 호원대학교 IT소프트웨어보안학과 교수
2008년 8월 성균관대학교 컴퓨터공학과 공학박사
2005년 2월 성균관대학교 정보보호학과 공학석사
1987년 2월 성균관대학교 정보공학과 공학사

email : ysooklee@howon.ac.kr