Lee와 Chen의 일회용 비밀번호 인증기법 분석

유일선* · 김보남** · 김홍준***

Analysis of the Lee-Chen's One-Time Password Authentication Scheme

Ilsun You* · Bonam Kim** · HeungJun Kim***

요 약

Lee와 Chen은 2005년에 Yeh-Shen-Whang 인증기법을 stolen verifier 공격에 대응할 수 있도록 개선하였다. 이 기법은 서버와 각 사용자의 공유 비밀키를 서버의 비밀키로부터 파생하여 stolen verifier 공격을 무력화 하였다. 그러나 우리는 Lee와 Chen의 개선안이 서버의 비밀키에 대한 오프라인 사전공격에 취약하다는 것을 발견하였다. 본 논문에서는 이러한 취약점을 분석하고 가능한 공격을 보인 후, 하드웨어 보안 모듈을 사용하여 이 문제에 대한 해결방안을 제시하였다. 또한, Lee와 Chen의 문제점으로 알려진 서비스 거부 공격과 과거 세션키 유출 공격에 대한 취약점을 개선하였다. 결론적으로 제안 인증기법과 Lee와 Chen의 기법을 비교분석하여 제안 인증기법의 보안강도가 개선되었음을 보였다.

ABSTRACT

In 2005, Lee and Chen suggested an enhanced one-time password authentication scheme which can prevent the stolen verifier attack that the Yeh-Shen-Whang's scheme has. The Lee-Chen's scheme addresses the stolen verifier attack by deriving each user's pre-shared secret SEED from the server secret. However, we investigated the weakness of the Lee-Chen's scheme and found out that it was suffering from the off-line dictionary attack on the server secret. We demonstrated that the off-line dictionary attack on the server secret can be easily tackled with only the help of the Hardware Security Modules (HSM). Moreover, we improved the scheme not to be weak to the denial of service attack and allow compromise of the past session keys even though the current password is stolen. Through the comparison between the Lee-Chen's scheme and the proposed one, we showed that the proposed one is stronger than other.

키워드

S/Key, One-time password, Off-line dictionary attack

* 한국성서대학교 정보과학부
** 교신저자, 충북대학교 전기전자컴퓨터공학부
*** 진주산업대학교 컴퓨터공학부

접수일자 2008. 11. 05

Ⅰ. Introduction

The S/KEY one-time password authentication scheme has been designed to control the user access to remote hosts and to protect a system against the replay or eavesdropping attacks [1][2]. As with the S/Key scheme, the user's secret pass-phrase never has been sent across the network because it is only used to generate each one-time password. In addition, there is no need for the secret information to be stored on any system, including the protected server. However, as earlier studies show, the S/KEY scheme is vulnerable to the server spoofing, preplay, and off-line dictionary attacks [3][4].

In 2002, Yeh, Shen and Hwang [4]proposed a one-time password authentication scheme to improve the S/KEY scheme. In this scheme, each user utilizes a smart card to securely store its own login information and simplify the login process. Particularly, by adopting each user's *SEED* as a pre-shared secret, this scheme can solve the problems of the S/KEY scheme and also provides a session key that enables confidential communication over the network. However, such a pre-shared secret causes the scheme to be vulnerable to the stolen-verifier attack while being unable to achieve the strength of the S/KEY scheme that no secret information needs to be stored. Moreover, it is also susceptible to several attacks such as the denial of service and Denning-Sacco attacks [5]-[7].

Recently, Lee and Chen introduced an improvement on the Yeh-Shen-Whang's scheme to prevent its vulnerability from the stolen verifier attack [7]. Their scheme addresses the stolen verifier attack by deriving each user's *SEED* from the server secret. Thus, if the server secret is securely kept, this scheme can be immune to the stolen verifier attack while allowing the server not to store any secret information. However, because of focusing on only the stolen verifier attack, it is still vulnerable to the denial of service attack and also allows a compromise of past session keys [8]. More importantly, due to the dependency on the server secret, it suffers from the off-line dictionary attack. In this paper, we demonstrate that the Lee-Chen's scheme is susceptible to the off-line dictionary attack and present an approach based on the Hardware Security Modules (HSM) [9] to address the attacks. In addition, the scheme is enhanced not to be vulnerable to the denial of service attack and allow compromise of the past session keys even if a password is stolen.

The rest of this paper is organized as follows. Section 2 reviews the Lee-Chen's scheme. In section 3, we show that the Lee-Chen's scheme is vulnerable to the off-line dictionary attack on the server secret. In section 4, we propose a HSM based method and show how these work for the off-line dictionary attack. Moreover, we add some enhancements to the Lee-Chen's scheme. In section 5, we conclude the paper.

Ⅱ. Review of the Lee-Chen's Scheme

2.1 Notification and preliminary

Before introducing the Lee-Chen's Scheme, we would like to present the following notation and definitions. These will be used in the following discussion for each stage.

- U denotes the user
- S denotes the server
- ID denotes the user identifier
- x denotes the server secret key
- K denotes the user secret key
- $H()$ denotes a collision-resistant hash function
- *SEED* denotes a pre-shared secret of the user and the server

  $SEED = H(ID \oplus x)$
- $\oplus$ denotes Exclusive-OR operation
- $|$ denotes a concatenate operation

It is assumed that the server initially issues a smart card to the user, which contains a pre-shared secret *SEED* (*=H(ID⊕x)*).

Also, the server securely keeps the secret x and performs all operations related to it within a temper-resistant hardware such as the Hardware Security Module (HSM) [9].

2.2 Registration Stage

(1) $U \rightarrow S : ID$

(2) $S \rightarrow U : N, H(SEED \oplus N) \oplus SK, H(SK)$

(3) $U \rightarrow S : P0 \oplus SK$

where $SK = D|TS$,

N is a permitted number of login times,

D is a random number,

TS is a timestamp,

$P_0 = H^N(K \oplus SEED)$

Before starting this stage, each user randomly generates a large number K and stores it in his or her smart card. To register a user, a server randomly generates D, computes $H(SK)$ and $H(SEED \oplus N)$, and performs an XOR operation on $H(SEED \oplus N)$ and SK. Then, it sends the $H(SEED \oplus N)$ SK and $H(SK)$ along with N, a permitted number of login times, to the user.

Upon receiving them, the user computes $H(SEED \oplus N)$ and applies an XOR operation to the result of the computed value and the received $H(SEED \oplus N) \oplus SK$ to extract SK.

If the hash value of the extracted SK is equal to $H(SK)$, the user computes and sends $P_0 \oplus SK$. As a result, the login information P_0 and N are stored at the server. In addition, the smart card stores P_0.

2.3 Login Stage

(1) $U \rightarrow S : ID$

(2) $S \rightarrow U : Ci, H(SEED \oplus Ci) \oplus SKi,$
$H(SKi) \oplus Pi\text{-}1$

(3) $U \rightarrow S : Pi \oplus SKi$

where $Ci = N\text{-}i$,

$SKi = Di|TSi$,

Di is the i th random number,

TSi is the i th timestamp,

$P_i = H^{Ci}(K \oplus SEED)$

After receiving the message of step (2), the user first computes $H(SEED \oplus Ci)$ and extracts SKi by performing an XOR operation on $H(SEED \oplus Ci) \oplus SKi$ and the computed value. Next, the user hashes SKi and extracts $H(SKi)$ from $H(SKi) \oplus P_{i-1}$. Then, the two values are compared to authenticate the server. If the server is valid, it computes and sends $P_i \oplus SKi$.

2.4 Authentication Stage

During this stage, the server extracts P_i from $P_i \oplus SKi$ and verifies if the hash value of Pi is equal to the stored P_{i-1}. If the verification is positive, the server can ensure that the user is valid. Finally, the server updates the last one-time password P_{i-1} with Pi and the count value with Ci. Also, SKi can be used to enable confidential communication between the server and the user.

Ⅲ. Off-line Dictionary Attack on the Lee-Chen's Scheme

In this section, we show that the Lee-Chen's scheme is vulnerable to the off-line dictionary attack. The off-line dictionary attack can be mounted by a legitimate user or a non- legitimate user as follows.

3.1 Attacks by Legitimate User

If an attacker is a legitimate user, he or she can easily mount the off-line dictionary attack on the server secret x through his or her own *SEED*. In this case, the attack proceeds as follows (Iterating upon all possible choices of secret x):

(1) Pick a candidate x'

(2) Compute $SEED' = H(ID \oplus x')$

(3) Compare $SEED'$ with his or her own $SEED$.

A match in the last step indicates the correct guess of the server secret x.

3.2 Attacks by Non-Legitimate User

Even though an attacker is a non-legitimate user, he or she can launch the off-line dictionary attack during the registration stage or the login stage.

Registration stage: It is assumed that an attacker can eavesdrop and record messages. In this stage, to register a user, a server makes a message for step (2), which is then sent to that user. If an attacker captures the message during step (2), he or she can launch the off-line dictionary attack as follows (Iterating upon all possible choices of secret x):

(1) Pick a candidate x'

(2) Compute $SEED' = H(ID \oplus x')$

(3) Compute $A = H(SEED' \oplus N)$

(4) Compute $B = H(A \oplus (H(SEED \oplus N) \oplus SK))$

(5) Compare B with $H(SK)$

A match in the last step indicates the correct guess of the server secret x.

Login stage: It is assumed that an attacker records all messages exchanged between the server and the user during this stage. The attacker can mount the following off-line dictionary attack (Iterating upon all possible choices of secret x):

(1) Pick a candidate x'

(2) Compute $SEED' = H(ID \oplus x')$

(3) Compute $A(i) = H(SEED' \oplus CNi)$ and

$A(j) = H(SEED' \oplus CNj)$,

where $j=i+1$, $0 < i < N$

(4) Compute $B(i) = A(i) \oplus (H(SEED \oplus CNi) \oplus SKi)$ and

$B(j) = A(j) \oplus (H(SEED \oplus CNj) \oplus SKj)$

(5) Compare $H((Pj \oplus SKj) \oplus B(j))$ with

$(Pi \oplus SKi) \oplus B(i)$

A match in the last step indicates the correct guess of the server secret x.

3.3 Successive Attacks

After the exposure of the server secret x, an attacker can easily compute any user's pre-shared secret. Then, the computed $SEED$ is usefully applied to the successive attacks such as the off-line dictionary attack on the user secret K, the server spoofing attack, the preplay attack, and the compromise of past session keys.

Off-line dictionary attack on the user's secret: Given the server secret x, an attacker can easily compute a user's $SEED$ and then extract the user's (i-1)th password Pi-1 from the message of step (2) during the login stage. With $SEED$ and P_{i-1}, he or she can mount the off-line dictionary attack on the user secret K.

Server spoofing attack: Given the server secret x, an attacker can easily compute a user's $SEED$ and then impersonate the server by forging the message of step (2) during the registration stage. In the login stage, the attacker can be authenticated as the server via SEED and P_{i-1}.

Preplay attack: Given the server secret x, an attacker can easily impersonate the server and predict the next challenge to deceive the user into giving the fresh one-time password during the login stage. With the presented password, the attacker can masquerade the user.

Compromise of pass session keys: Given the server secret x, an attacker can easily compute a user's $SEED$ and

then extract the ith password Pi from the messages of step (2)-(3) during the login stage. With the password, the attacker is able to get the earlier session keys *(SK1, SK2, . , SKi)* as follows:

(1) $Pi = H(Pi)$
(2) $i = i-1$, *if* $(i < 1)$ *exit*
(3) $SKi = Pi \oplus SKi$
(step (3) message of the login stage)
(4) *goto (1)*

Ⅳ. Improvement

In this section, we improve the Lee-Chen's scheme to defend against the off-line attacks described above as well as the attacks demonstrated in [8].

4.1 HSM-based multiple server secrets

In the Lee-Chen's scheme, when the server secret *x* is revealed due to the off-line dictionary attack, it allows the successive attacks to be launched as mentioned in the previous section. In this case, to repair the authentication scheme, the server should update its secret x and all users should reinitialize their login information including the pre-shared secret and smart card. Unfortunately, this scheme does not provide a proper way to securely distribute the pre-shared secrets to the users. And to make a bad situation worse, the off-line dictionary attack is a kind of a passive attack, which is invisible and non-detectable. Therefore, this attack is the most critical security threat to the Lee-Chen's scheme and should be prevented.

As an alternative to address the attacks, the adoption of the Hardware Security Modules (HSM) [9] can be considered. In this approach, multiple server secrets are used to compute each user's seed instead of using only one server secret. The server secrets can be safely stored and effectively managed within a highly secure, tamper-resistant hardware environment provided by the HSM. Moreover, the HSM can be activated only after its own strong authentication is successfully confirmed. It enables this approach to defend against the stolen verifier attack despite of the compromise with the server.

The following describes the approach in detail:

It is assumed that n is the number of users, *user(j)* is the jth user, m is the number of server secrets ($n \geq m$), and *x(i)* is the ith server secret. In addition, *assign(i)* is the number of users who are assigned to *x(i)*.

At the beginning, the server is initialized as follows:

(1) *index = 0*
(2) ***for*** *j = 1* ***to*** *j < n+1*
(3) ***begin***
(4) *index = (index + 1) mod (m+1)*
(5) ***if*** *index == 0* ***then***
(6) *index = 1*
(7) *SEED = H(user(j)'s ID* $\oplus$ *x(index))*
(8) *index* and *SEED* are assigned to *user(j)*
(9) *assign(index) = assign(index)+1*
(10) ***end***

In line (8), each SEED is put into *user(j)*'s smart card while index is stored with *user(j)*'s login information in the server. When authenticating a user, the server finds the server secret assigned to the user through the server secret index and then computes *SEED*.

The following algorithm is for the case that a new user is registered to the authentication scheme.

(1) *index = -1*
(2) *temp = n+1*
(3) ***for*** *i = 1* ***to*** *i < m+1*
(4) ***if*** *assign(i) < temp* ***then***
(5) ***begin***
(6) *temp = assign(i)*
(7) *index = i*
(8) ***end***

(9) $SEED = H(ID \oplus x(index))$

(10) *index* and *SEED* are assigned to the new user

(11) $assign(index) = assign(index)+1$

As mentioned above, the server stores the index i of the selected secret with the user's login information to its database, while not sending it to the user. Therefore, even though the server is compromised, the stolen-verifier attack is not possible since only the users' indexes are exposed. In addition, the Lee-Chen's scheme can be immune to the off-line dictionary attack due to the multiple server secrets.

The security strength of this method is in proportion to the number m of the sever secrets. That is, it is desirable to let each server secret assigned to only one user $(m \geq n)$ if the capacity of the HSM is acceptable.

4.2 Additional enhancements

In this section, we enhance the drawbacks of the Lee-Chen's scheme as follows: First, in order to solve the vulnerability to DoS attacks, we add $H(P0||SK)$ to the step (3) message of the registration stage. That makes it possible for the server to ensure that P0 is not altered and thus prevent desyncronization between the client and itself. Second, in the step (3) of the login stage, $Pi \oplus SKi$ is changed into $Pi \oplus H(SKi)$. In this way, the enhanced scheme does not allow an attacker to obtain SKi or the past session keys even if it has a knowledge of Pi.

4.3 Comparison

This section compares the Lee-Chen's scheme with the proposed one. Table 1 summarizes the comparison.

Off-line attacks: Because the proposed scheme's cost for initializing the clients' secret is $O(n)$, the scheme has the same efficiency as the Lee-Chen's scheme. Also, if one server secret is revealed, the proposed scheme's cost for recovering is cheaper than that of the Lee-Chen's one. That is, in the Lee-Chen's scheme, because the clients' secrets are derived from only one server one, if the server secret is revealed, all clients' ones should be changed. On the other hand, in the proposed one, because there are multiple server secrets, even if the one is revealed, the secrets of just $\lceil \frac{n}{m} \rceil$ clients should be recovered. In order to guess all client secrets in the Lee-Chen's scheme, an attacker needs to focus on the one server secret. Thus, the cost for this attack is $O(|x\,RIGHT|)$. In the proposed scheme, the cost for guessing all client secrets is $O(m \times |x\,RIGHT|)$ because there are m server secrets. As a result, in terms of defending against off-line dictionary attacks, the proposed scheme is better than the Lee-Chen's scheme.

Table 1. Comparison of two schemes
표 1. 두 기법의 비교

(1) Off-line attack
(2) Stolen-Verifier Attack
(3) Denial of Service Attack
(4) Compromise of past session keys
(a) Cost for initializing the client secrets
(b) Cost for recovering the client secrets
(c) Cost for guessing all client secrets

Schemes		Lee-Chen	Proposed scheme
(1)	(a)	$O(n)$	$O(n)$
	(b)	$O(n)$	$O(\lceil \frac{n}{m} \rceil)$
	(c)	$O(\|x\,RIGHT\|)$	$O(m \times \|x\,RIGHT\|)$
(2)		O	O
(3)		X	O
(4)		X	O

* |x| means the size of the secret x

Other attacks: As shown in table 1, both the schemes are not vulnerable to the stolen verifier attack. Note that the server secrets are safely stored into and used for computation within the HSM devices in the proposed scheme. In this way, the proposed scheme can prevent the

attack. In addition, unlike the Lee-Chen's scheme, the proposed scheme is not weak to the DoS attack while not allowing compromise of past session keys even if the current password is stolen.

In summary, we can conclude that the proposed scheme provides stronger security than the Lee-Chen's scheme. Note that such improvements need additional two hash operations besides the HSM device and its management module. Because only the server needs the HSM device and its management module, the cost for the improvement is reasonable. Also, in terms of the computation overhead, because just two hash operations are required, the proposed scheme can sustain the efficiency of the Lee- Chen's one.

V. Conclusion

In this paper, we have demonstrated that the Lee-Chen's scheme is susceptible to the off-line dictionary attack on the server secret. If the server secret is revealed by this attack, the scheme cannot be easily recovered while suffering from the successive attacks. Therefore, we suggest the HSM based approach, and explain how this method is operating well to the off-line dictionary attack. Moreover, we improved the scheme not to be vulnerable to the denial of service attack and allow compromise of the past session keys if a password is stolen. Through the comparison and analysis, it can concluded that the proposed scheme provides stronger security than the Lee-Chen's one with such enhancements. Also, the proposed scheme does not result in considerable computational overheads and thus keeps the efficiency of the Lee-Chen's one.

References

[1] N. Haller, "The S/KEY One-time Password," IETF RFC 1760 (1995)

[2] N. Haller, C. Metz, P. Nesser and M. Straw, "A One-time Password System," IETF RFC 2289 (1998)

[3] C. J. Mitchell and L. Chen, "Comments on the S/KEY User Authentication Scheme," ACM Operating Systems Review, Vol. 30, No. 4 (1996) 12-16

[4] T. C. Yeh, H. Y. Shen and J. J. Hwang, "A Secure One-Time Password Authentication Scheme Using Smart Cards," IEICE Transaction on Communication, Vol. E85-B, No. 11 (2002) 2515-2518

[5] I. You and K. Cho, "Comments on YEH-SHEN-HWANG's One-Time Password Authentication Scheme," IEICE Transaction on Communication, vol. E88-B, no. 2 pp.751-753, Feb. 2005

[6] W.C. Ku, C.M. Chen and H.L. Lee, "Cryptoanalysis of a Variant of Peyravian-Zunic's Password Authentication Scheme," IEICE Trans. Commun., vol.E86-B, no.5, pp.1682-1684, May. 2003

[7] N. Y. Lee and J. C. Chen,"Improvement of One-Time Password Authentication Scheme Using Smart Cards," IEICE Transaction on Communication, Vol. E88-B, No. 9 (2005) 3765-3767

[8] I. You and E. Jung,"A Light Weight Authentication Protocol for Digital Home Networks,"ICCSA 2006, Springer-Verlag LNCS 3938 (2006) 416-423

[9] nCipher corporation Ltd., "Hardware Key Protection," http://www.ncipher.com

저자소개

유 일 선 (Ilsun You)

1995년 단국대학교 전산통계학과 졸업 (학사)
1997년 단국대학교 전산통계학과 졸업 (석사)
2002년 단국대학교 전산통계학과 졸업 (박사)
2005년~현재 한국성서대학교 정보과학부 조교수
※관심분야 : MIPv6, 인터넷 보안, 접근통제

김보남(Bonam Kim,)

1991년 단국대학교 전산통계학과 졸업(학사)
2003년 Auburn Univ. 컴퓨터공학과 (석사) (석사)
2006년 Auburn Univ. 컴퓨터공학과 (석사) (박사)
2007년~현재 충북대학교 전기전자 컴퓨터공학부 연구원
※관심분야 : 무선네트워크(ad hoc, sensor, and mesh 네트워크), 네트워크 보안등

김흥준(HeungJun Kim)

1989년 단국대학교 전자계산학과 졸업(학사)
1993년 단국대학교 대학원 전산통계학과 (석사)
1999년 단국대학교 대학원 전산통계학과 (박사)
1999년~현재 진주산업대학교 컴퓨터공학부 부교수
※관심분야 : 컴퓨터구성, 모바일 네트워킹, P2P