Journal of Engineering and Applied Sciences 12 (22): 5979-5984, 2017
ISSN: 1816-949X

Security Analysis of Symmetric Key based Remote user Authentication Scheme with Forward Secrecy

Younsung Choi
Department of Cyber Security, Howon University, Impi-Myeon, Gunsan-si,
54058 Jeonrabuk-do, Korea

Abstract: Recently because of development of remote network technology, users are able to access the network freely without constraints of time and space. As users are getting more frequent to access the remote server in a computing environment, they are increasingly being exposed to various risk factors such as forward secrecy and server impersonation attack. Therefore, researches for remote user authentication scheme have been studying actively. This study overcomes the weaknesses of many authentication schemes proposed recently. This study suggests an improved authentication scheme that protects user's anonymity with preserving variable more safe and also provides forward secrecy.

Key words: Cryptanalysis, security analysis, smart card based password authethentication, preserving variable, forward secrecy, Korea

INTRODUCTION

With rapid advances in network technology, users can use internet service freely without boundary of time or place. Remote user authentication scheme controls access by unauthorized users to protect remote services or resources and is a very important process to validate the injured user. However, various authentication schemes in the remote environment are exposed the session key in key distribution process when the security key is exposed so, it is meant that the schemes cannot provide forward secrecy. And some authentication schemes have security weaknesses such as reply attack, impersonation attack, smart card attack, privileged insider attack, stolen verifier attack, man-in-the-middle attack and so on. User authentication scheme need to provide the confidentiality, integrity and availability and forward secrecy for safe authentication between remote server and remote users. The typical method of user authentication in a remote system environment is as follows (Choi *et al*., 2014ab; Jaspher *et al*., 2012 (Sensors); Chien *et al*., 2002; Ramasamy and Muniyandi, 2009).

Khan *et al*. (2011) claimed that Wang *et al*. (2009)'s proposed authentication scheme have security vulnerabilities such as anonymity and insider attack. So, Khan *et al*. (2011) proposed dynamic ID based remote user authentication scheme to resolve the problem by Wang *et al*. (2009)'s scheme (Khan *et al*., 2011). However, Chen *et al*. (2012) explained Khan *et al*. (2011)'s dynamic ID based authentication scheme have important problem with using variables that are vulnerable to internal attack and not registered and then proposed authentication scheme that improves use of variables and does not send user random value to public channels (Chen *et al*., 2012). Jiang *et al*. (2013), analyze Chen *et al*. (2012)'s scheme and found out their scheme is vulnerable on guess attack and tracking attack. Jiang *et al*. (2013) proposed security enhanced symmetric key based authentication scheme that provides user's anonymity and intractability. Kumari *et al*. (2013) point that Jiang *et al*. (2013)'s scheme has security vulnerability on user impersonation attack, guessing attack and denial of service attack. So, to overcome these problems, they proposed secure authentication scheme for telecare medical information system (Kumari *et al*., 2013). However, Kim and Lee (2014) claimed that Kumari *et al*. (2013)'s scheme cannot provide forward secrecy and user anonymity, so, an attacker can compute the session if the attacker know secret key, user's ID, random number. To solve the problem related user anonymity and forward secrecy, Lee *et al*. (2016) proposed a symmetric key-based remote user authentication scheme with forward secrecy and claimed that their scheme is secure against lack of forward secrecy, lost smart card attack, online password guessing attack, offline password guessing attack, user impersonation attack, denial of service, session key disclosure attack, stolen verifier attack, man-in-the-middle attack, privileged insider attack, provides user anonymity, user untraceability, replay attack and so on (Lee *et al*., 2016). This study analyzes the detailed process by Lee *et al*. (2016)'s authentication scheme. As a results, this study found out Lee *et al*. (2016)'s authentication scheme still has security vulnerability such off-line password attack, user anonymity, insider attack, user impersonation attack.

MATERIALS AND METHODS

Review of Lee *et al.* (2016)'s authentication scheme: To overcome weaknesses on various authentication scheme, Lee *et al.* (2016) propose secure user authentication scheme keeping the advantages by Kumari *et al.* (2013)'s authentication scheme which is secure against forward secrecy and smart card loss attack. Kumari *et al.* (2013)'s authentication scheme, session key is computed if an attacker knows the security key on the maintenance of forward security. So, when an attacker decrypted $AID = E_x(ID\|R)$, the attacker can obtain the user's ID and random number R. And then the attacker can compute previous session key using user's ID and J variable. Lee *et al.* (2016)'s proposed scheme an attacker cannot obtain the user's ID because the attacker do not know Y and b if the attacker obtains the security key using $AID = E_x(ID\oplus h(Y\|b)$. Moreover, J variable is computed by variable R, A and L. So, Lee *et al.* (2016)'s scheme is secure if an attacker obtain the information of smart card using the smart card attack.

Lee *et al.* (2016)'s proposed scheme consists of three phases: the registration phase; the login phase; the authentication phase; this study describes Lee *et al.* (2016)'s authentication scheme in detail. For convenience, the notations used throughout this study are summarized in Table 1.

Table 1: Notations

Notation	Description
U_i	A user i
S_i	A remote medical server
ID	The Identity of the user U_i
PW	The Password of the user U_i
RGR	A Registration record
N	The Number of times registers with server
r	A random nonce of U_i
T_x	A timestamp
x	The S_i's secret key
b	The S_i's random number
h(•)	A collision-free one-way hash function
Sk	The shared Session key
$\oplus$	The bitwise XOR operation
$\|$	The message concatenation operation
E_k(•)	A symmetric encryption using a key k
D_k(•)	A symmetric decryption using a key k

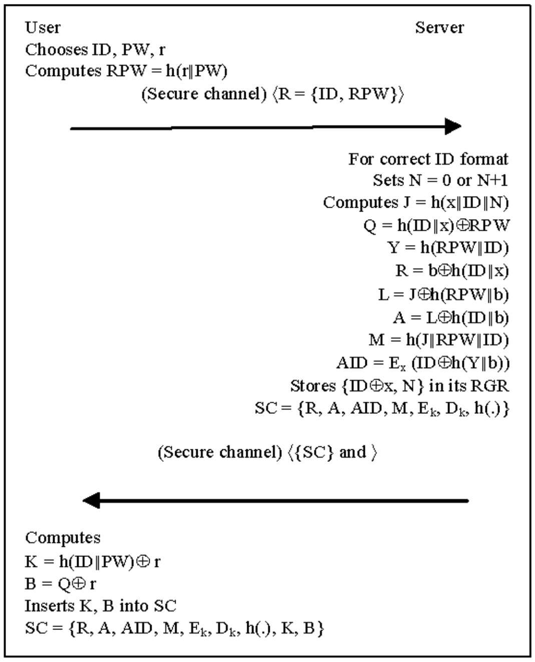

Fig. 1: Registration phase by Lee *et al.* (2016)'s scheme

Registration phase: Before starting Lee *et al.* (2016)'s authentication scheme, the server selects the master secret key x and b, a collision-free one-way hash function h(•). Then, the user U_i registers to the server S. The registration phase.

[R1]: The user U_i chooses his/her identity ID , password PW and a random number r.

[R2]: Then user computes $RPW = h(r\|PW)$ and submits ID, RPW to server using secure channel.

[R3]: The server checks the format of ID and assigns the number to Registered time such as N = 0 to new user and N = 1 to existing user.

[R4]: The server computes following parameters:

$$J = h(x\|ID\|N),\ Q = h(ID\|x)\oplus RPW$$
$$Y = h(RPW\|ID),\ R = b\oplus h(ID\|x)$$
$$A = L\oplus h(ID\|b),\ L = J\oplus h(RPW\|b)$$
$$M = h(J\|RPW\|ID),\ AID = E_x(ID\oplus h(Y\|b)$$

And the server stores $\{ID\oplus x, N\}$.

[R5]: The server store {R, A, AID, M, E_k, D_k, h(•)} to smart card and then send the smart card, variable Q to the server using secure channel (Fig. 1).

[R6]: The user receives the smart card and variable Q, and then computes $K = h(ID\|PW)\oplus r$, $B = Q\oplus r$ and the user stores K, B to the smart card.

User registration phase: This phase is invoked whenever, the user U_i wants to login to the server S. The

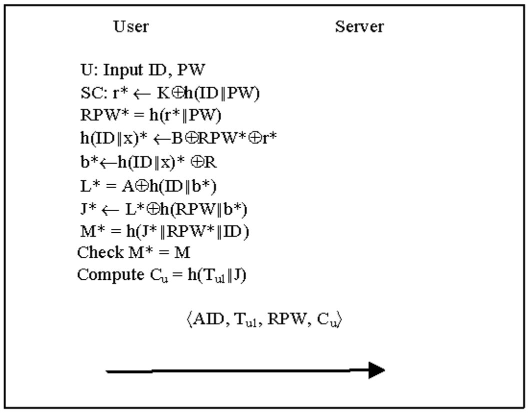
User
Server
U: Input ID, PW
SC: $r^* \leftarrow K \oplus h(ID \| PW)$
$RPW^* = h(r^* \| PW)$
$h(ID \| x)^* \leftarrow B \oplus RPW^* \oplus r^*$
$b^* \leftarrow h(ID \| x)^* \oplus R$
$L^* = A \oplus h(ID \| b^*)$
$J^* \leftarrow L^* \oplus h(RPW \| b^*)$
$M^* = h(J^* \| RPW^* \| ID)$
Check $M^* = M$
Compute $C_u = h(T_{u1} \| J)$
$\langle AID, T_{u1}, RPW, C_u \rangle$

Fig. 2: The login phase by Lee *et al.* (2016)'s scheme

login phase is shown in Fig. 2. The steps of the login phase are shown as follows; the steps of this phase are conducted as follows.

[L1]: The user inserts the smart card SC and inputs user's ID and password PW.

[L2]: SC computes the r^* and RPW^* using ID and PW:

$$r^* \leftarrow K \oplus h\,(ID \,\|\, PW),\ RPW^* = h\,(r^* \,\|\, PW)$$

[L3]: The SC computes the following parameters using RPW:

$$h\,(ID \,\|\, x)^* \leftarrow B \oplus RPW^* \oplus r^*$$
$$b^* \leftarrow h\,(ID \,\|\, x)^* \oplus R\,,\ L^* \leftarrow A \oplus h\,(ID \,\|\, b^*)$$
$$J^* \leftarrow L^* \oplus h\,(RPW^* \,\|\, b^*)\,,\ M^* = h\,(J^* \,\|\, RPW^* \,\|\, ID)$$

[L 4]: SC checks the sameness the M^* and M. If the they are same, the SC computes:

$$C_u = h\,(T_{u1} \,\|\, J)$$

If they are not same, the user closes session.

[L 5]: The user send login messages $\{AID, T_{u1}, RPW, C_u\}$ to server using public channel.

Authentication phase: After completing this login phase, the user U_i and the server S can authenticate each other and establish a shared session key. The authentication phase is shown in Fig. 3.

[A 1]: The sever receives the login messages and then, generates T_{ms1} and checks $(T_{ms1}–T_{u1}) > \Delta T$. If the condition of messages and time stamp is not suitable, the server closes the session.

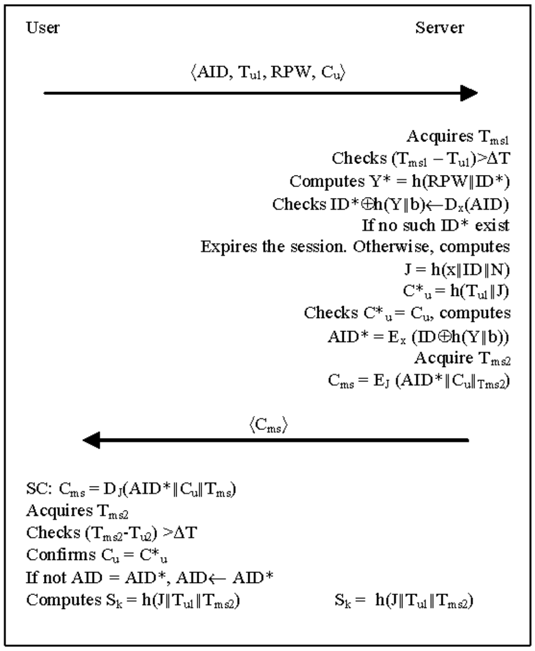
User
Server
$\langle AID, T_{u1}, RPW, C_u \rangle$
Acquires T_{ms1}
Checks $(T_{ms1} - T_{u1}) > \Delta T$
Computes $Y^* = h(RPW \| ID^*)$
Checks $ID^* \oplus h(Y \| b) \leftarrow D_x(AID)$
If no such ID^* exist
Expires the session. Otherwise, computes
$J = h(x \| ID \| N)$
$C^*_u = h(T_{u1} \| J)$
Checks $C^*_u = C_u$, computes
$AID^* = E_x\ (ID \oplus h(Y \| b))$
Acquire T_{ms2}
$C_{ms} = E_J\ (AID^* \| C_u \| _{Tms2})$
$\langle C_{ms} \rangle$
SC: $C_{ms} = D_J(AID^* \| C_u \| T_{ms})$
Acquires T_{ms2}
Checks $(T_{ms2}\text{-}T_{u2}) > \Delta T$
Confirms $C_u = C^*_u$
If not $AID = AID^*$, $AID \leftarrow AID^*$
Computes $S_k = h(J \| T_{u1} \| T_{ms2})$
$S_k = h(J \| T_{u1} \| T_{ms2})$

Fig. 3: Authentication phase by Lee *et al.* (2016)'s scheme

[A 2]: The server computes the Y^* and checks as follows:

$$Y^* = h\,(RPW \,\|\, ID^*),\ ID^* \oplus h\,(Y^* \,\|\, b)\ ? = D_x\,(AID)$$

If ID is not in RGR, the session is closed, otherwise the server computes J and C^*_u:

$$J = h\,(x \,\|\, ID \,\|\, N),\ C^*_u = h\,(T_{u1} \,\|\, J)$$

[A 3]: The server checks the sameness of C^*_u and C_u . If they are same, the server computes $AID^* = E_x\ (ID \oplus h\ (Y \,\|\, b))$ and generates T_{ms2}.

[A 4]: The server computes $C_{ms} = E_J\,(AID^* \,\|\, C_u \,\|\, T_{ms2})$ using T_{ms2} and send C_{ms} to the user using public channel.

[A 5]: The user receives C_{ms} from the server and then computes $C_{ms} = D_J\ (AID^* \,\|\, C_u \,\|\, T_{ms2})$ and generates timestamp T_{u2}.

[A 6]: The user checks $(T_{ms2}–T_{u2}) > \Delta T$ using computed T_{u2}. If the condition is accepted, The user checks the sameness between C^*_u and C_u. If the C^*_u and C_u are not same, the user closes the session.

[A 7]: If the C^*_u and C_u are same, the user checks the sameness between AID^* and AID. AID^* and AID are not same, the user replaces the AID by $AID \leftarrow AID^*$.

[A 8]: The user and server compute the session key $S_k = h\ (J\ ||\ T_{u1}\ ||\ T_{ms2})$ and finish the login and authentication phases.

RESULTS AND DISCUSSION

Security analysis of Lee *et al.* (2016)'s scheme: This study analyzes Lee *et al.* (2016)'s authentication scheme and find out various security vulnerabilities including off-line password (and identity) guessing attack, user impersonation attack, weak anonymity and insider attack.

Off-line password (and identity) guessing attack: Various studies explain that all information stored on user's smart cards could be extracted by physically monitoring its power consumption such as simple power analysis and differential power analysis. Therefore, when a user loses user's smart card an attacker can get all information in the smart card. Lee *et al.* (2016)'s authentication scheme, the smart card stores important information about user's authentication. The smart card for the user U_i stores $\{R, A, AID, M, E_k, D_k, h(\bullet), K, B\}$. Using smartcard stored information and RPW, attacker can guess the user's ID and password PW_i as Fig. 4.

First, the attacker can obtain RPW in public channel and then the attacker take user's smart card to reveal the user's identity and password. By simple power analysis and differential power analysis on smart card, the attacker can get all of information on user's smart card. So, the attacker can obtain $\{R, A, AID, M, E_k, D_k, h(\bullet), K, B\}$ then the attack knows the following equation:

$$r = K\oplus h\ (ID\ ||\ PW\ ),\ h\ (ID\ ||\ x) = B\oplus RPW\oplus r$$
$$b = h\ (ID\ ||\ x)\oplus R,\ L = A\oplus h\ (ID\ ||\ b)$$
$$J = L\oplus h\ (RPW\ ||\ b),\ M = h\ (J\ ||\ RPW\ ||\ ID)$$

Using equation J, attacker recomputed the equation M:

$$\neg M = h\ (L\oplus h\ (RPW\ ||\ b)\ ||\ RPW\ ||\ ID)$$

Using equation L, the attacker recomputed:

$$\neg M = h\ (A\oplus h\ (ID||\ b)\oplus h\ (RPW\ ||\ b)||\ RPW\ ||\ ID)$$

And using formula b, h (ID || x) and r, the attacker recomputed as follows:

$$\neg M = h(A\oplus h\ (ID||h(ID||x)\ \oplus R)\oplus h(RPW||h(ID||x)\ \oplus R)\ ||\ RPW\ |\ |ID)$$

$$\neg M = h\ (A\oplus h\ (ID||\ B\oplus RPW\oplus r\oplus R)\oplus h\ (RPW\ ||\ B\ \oplus RPW\oplus r\oplus R\ ||\ RPW\ ||\ ID)$$

An attacker obtains RPW in public channel
An attacker takes the user U_i's smart card
An attacker obtains all information of smart card using physical monitoring
→ So, attacker can gets R, A, AID, M, E_k, D_k, h(*) K, B
Attacker computer the parameters

- $r = k\oplus h\ (ID\|\ PW)$ • $h\ (ID\|\ x) = B\oplus PRW\oplus r)$
- $b = h\ (ID\|x)\oplus R$ • $L = A\oplus h\ (ID\|b)$
- $J = L\oplus h\ (RPW\|b)$ • $M = h\ (J\|PW\|ID)$

→ $M = h\ (L\oplus h\ (RPW\|b)\ \|RPW\|ID)$; using J
→ $M = h\ (A\oplus h\ (ID\|b)\oplus h\ (RPW\|b)\ \|\ RPW\|ID)$; using L
→ $M = h\ (A\oplus h\ (ID\|h)\ (ID\|x)\oplus R)\oplus h(RPW\|h)\ ID\|x)\oplus R)\|PW\|ID)$; using b
→ $M = h(A\oplus h\ (ID\|B\oplus RPW\oplus\ r\oplus R)\oplus h(RPW\|B\oplus RPW\oplus\ r\oplus)\ R)\|RPW\|ID)$; using h (ID‖x)
→ $M = h(A\oplus h\ (ID\|B\oplus RPW\oplus k\oplus h\ (ID\|PW)\oplus R)\oplus h(RPW\|B\oplus RPW\oplus k\oplus\|h\ (ID\|PW)\oplus R)\|RPW\|ID)$; using r

Attacker know all formula's parameter except for ID, PW
→ D_{id} and D_{pw} are very limited in practice such as $|D_{id}| \leq |D_{pw}| \leq 10^6$
→ So, attacker can executes off-line password attacker and obtain ID and PW

Fig. 4: Off-line password (and identity) guessing attack

$$\neg M = h(A\oplus h(ID||B\oplus RPW\oplus K\oplus h(ID||PW)\oplus R)\oplus h(RPW||B\oplus RPW\oplus K\oplus h(ID||PW)\ \oplus R\ )\ ||\ RPW\ ||\ ID)$$

In M formula, the attacker know all parameter except for ID, PW, Let $|D_{id}|$ and $|D_{pw}|$ denote the number of identities in D_{id} and the number of passwords in D_{pw}, respectively. The running time of the aforementioned attack procedure is $O|D_{id}|*|D_{pw}|*T_H)$, where $T_H$is the running time for hash because both password and identity are human-memorable short strings but not high-entropy keys that is to say, they are often chosen from two corresponding dictionaries of small size. As $|D_{id}|$ and $|D_{pw}|$ are very limited in practice, $|\ D_{id}| \leq |\ D_{wp}| \leq 10^6$, the aforementioned attack can be completed in polynomial time. So, the attacker can compute user's ID and PW using off-line password (and identity) attack using information in user's smart card and RPW in public channel (Ma *et al*., 2014).

User impersonation attack: User impersonation attack is an attack in which an attacker successfully assumes the identity of one of the legitimate parties in a system or in a communications. Lee *et al.* (2016)'s scheme when an attacker stole the user's smart card, the attacker can login and authenticate to server and compute the session key S_k between the user and server, so, the attacker can successfully impersonate legitimate user, Lee *et al.* (2016)'s authentication scheme. If the attacker can authenticate with the server using user's smart card, it is serious problem (Rhee *et al*., 2009).

An attacker obtains AID T_{u1}, RPW in public channel
An attacker takes the user U_i's smart card
An attacker obtains all information of smart card using physical monitoring
→ So, attacker can gets R, A, AID, M, E_k, D_k, h (.), K, B
An attacker computer the parameters

- $r = K \oplus h\ (ID \| PW)$ • $h\ (ID \| x) = B \oplus PRW \oplus r)$
- $b = h\ (ID \| x) \oplus R$ • $L = A \oplus h\ (ID \| b)$
- $J = L \oplus h\ (RPW \| b)$

→ $J = A \oplus h\ (ID \| b) \oplus h\ (RPW \| b)$; using L
→ $J = A \oplus h\ (ID \| h\ (ID \| x) \oplus R) \oplus h\ RPW \| h\ (ID \| x) \oplus R$; using b
→ $J = A \oplus h\ (ID \| B \oplus RPW \oplus r \oplus R) \oplus h(RPW \| B \oplus RPW \oplus r \oplus R)$; using $h(ID \| x)$
→ $J = A \oplus h\ (ID \| B \oplus RPW \oplus K \oplus h\ (ID \| PW) \oplus R) \oplus h(RPW \| B \oplus RPW \oplus K \oplus h)\ (ID \| PW) \oplus R)$; using r

Attacker know all formula's parameter inciuding ID, PW from the attack 3.1
→ So, attack can compute J and decrypt C_{ms}, obtain T_{ms2}
→ So, attacker can impersonate the legal user and compute session key S_k easily

Fig. 5: User impersonation attack

Figure 5 describes the user impersonation attack on Lee *et al*. (2016)'s authentication scheme. An attacker obtains AID, T_{u1}, RPW in public channel and if the attacker takes the user U_i's smart card, he can obtains all information of smart card using physical monitoring like DPA, SPA. So, the attacker has R, A, AID, M, E_k, D_k, h(•), K, B, RPW and knows the formulas of parameters such as r, h (ID || x), b, L including J = L⊕h (RPW || b). So, the attacker recomputed equation J using L, b, h (ID || x), r as follows:

$$\rightarrow [\text{Using L}]:\ J = A \oplus h\ (ID \,||\, b) \oplus h\ (RPW \,||\, b)$$

$$\rightarrow [\text{Using b}]:\ J = A \oplus h\ (ID \,||\, h\ (ID \,||\, x) \oplus R) \oplus h\ (RPW \,||\, h\ (ID \,||\, x) \oplus R)$$

$$\rightarrow [\text{Using h (ID || x)}]:\ J = A \oplus h(ID \,||\, B \oplus RPW \oplus r \oplus R) \oplus h\ (RPW \,||\, B \oplus RPW \oplus r \oplus R)$$

$$\rightarrow [\text{Using r}]:\ J = A \oplus h(ID \,||\, B \oplus RPW \oplus K \oplus h(ID \,||\, PW) \oplus R) \oplus h(RPW \,||\, B \oplus RPW \oplus K \oplus h\ (ID \,||\, PW) \oplus R)$$

And the attacker can illegally extract the secret values and computes ID and PW using off-line password guessing attack. Therefore the attacker can compute J and decrypt C_{ms} and obtain T_{ms2}. So, the attacker can computes compute session key $S_k = h\ (J \,||\, T_{u1} \,||\, T_{ms2})$. The attacker can login and authentication with server using user's smart card and computed ID, PW and can make the session key S_k between user and server. Therefore, the attacker can impersonate the legal user.

Weak anonymity: Lee *et al.* (2016)'s authentication scheme, they use anonymous identity AID to provide the anonymity but an attacker can know some information using AID. The user by Lee *et al.* (2016)'s authentication scheme sends AID to server for authentication over public communication so the attacker can obtain all of AID coming to the server because user's AID is always constant. In equation AID = Ex (ID⊕h (Y || b)), all of parameter (ID, Y, b) are constant so, AID is constant though parameters (ID, Y, b) are encrypted. By analyzing the messages for server of public communication an attacker can guess the number of registered user to sever. Moreover, the attacker can acquire information on which user communicates with server (Rhee *et al.*, 2005). Therefore, Lee *et al.* (2016)'s authentication scheme does not provide complete anonymity so, it is necessary for user to apply dynamic protection technique. Then, when user sends AID to server, the attack cannot extract the information from AID which is varied according to time.

Insider attack: Lee *et al.* (2016)'s authentication scheme, the server has all of information which is needed to authenticate between server and user. It is meant that an insider of server can impersonate to all of registered user if the insider steals the information stored the server (Stolfo *et al.*, 2008). To impersonate the registered user an attacker need to make {AID, T_{u1}, RPW, C_u} and to compute the session key S_k from C_{ms}. It is because that the server including RGR has all information such as user's ID and secret key. To solve this problem, the server reduce to store the information for login and authentication (especially, user's ID).

No perfect forward secrecy: Perfect forward secrecy is a property of secure communication protocols in which compromise of long-term keys does not compromise past session keys. It is meant the when one of the long-term keys is compromised in the future, if session key derived from a set of long-term keys will not be compromised, then it is meant that perfect forward secrecy is provided. However, Lee *et al.* (2016)'s scheme does not achieve perfect forward secrecy (Choi *et al.*, 2014). Lee *et al.* (2016)'s scheme, the attacker can compute the all session key between the user and server if the attacker knows the one of long-term keys in future. Figure 6 describes why Lee *et al.* (2016)'s scheme cannot provide perfect forward secrecy.

An attacker obtains T_{Pui} and C_{Pms} in previous communication between user and server. Then, the attacker knows one of long-term secret J. So, the attacker can decrypt the C_{pms} as follows:

$$D_J\ (C_{pms}) \rightarrow (AID_p \,||\, C_{pu} \,||\, T_{pms2})$$

- Attacker got T_{pu1} and C_{pms} in previous public communication
- Attacker know one of user's long-term secret: J
- Attacker has J, T_{pu1} and C_{pms}
  - → $D_J(C_{pms}) \rightarrow (AID_p \| C_{pu} \| T_{pms2})$
  - → Attacker has J, T_{pu}, T_{pms2}
  - → Previous $S_{pk} = h(J \| T_{pu1} \| T_{pms2})$
- Attacker has can compute all of previous session key S_{pk}

Fig. 6: No. perfect forward secrecy

Then, the attacker get J, T_{pu}, T_{pms2} which is the parameters that is needed for previous S_{pk}:

$$\text{Previous session key } S_{pk} = h\,(J \,\|\, T_{pu1} \,\|\, T_{pms2})$$

$$\text{Present session key } S_k = h\,(J \,\|\, T_{u1} \,\|\, T_{ms2})$$

The attacker can compute all of previous session key S_{pk} using J, T_{pu1} and T_{pms2}. And the attacker can make the present session key S_k = h (J || T_{u1} || T_{ms2}) also. Therefore, this scheme does not achieve perfect forward secrecy.

CONCLUSION

Lee *et al*. (2016) proposed a smart card based password authentication to overcome the weaknesses of many authentication schemes proposed recently but their scheme has security problem. So, this study analyzes Lee *et al*. (2016)'s scheme and points out that authentication scheme has security vulnerability such as off-line password (and identity) guessing attack, user impersonation attack, weak anonymity, insider attack, no perfect forward secrecy.

ACKNOWLEDGEMENT

This research was supported by financial support of Howon University in 2017.

REFERENCES

Chen, H.M., J.W. Lo and C.K. Yeh, 2012. An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems. J. Med. Syst., 36: 3907-3915.

Chien, H.Y., J.K. Jan and Y.M. Tseng, 2002. An efficient and practical solution to remote authentication: Smart card. Comput. Secur., 21: 372-375.

Choi, Y., D. Lee, J. Kim, J. Jung, and J. Nam *et al*., 2014b. Security enhanced user authentication p rotocol for wireless sensor networks using elliptic curves cryptography. Sens., 14: 10081-10106.

Choi, Y., J. Nam, D. Lee, J. Kim and J. Jung *et al*., 2014a. Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics. Sci World J., 2014: 1-15.

Jaspher, G., W. Katherine, E. Kirubakaran and P. Prakash, 2012. Smart card based remote user authentication schemes survey. Proceedings of the 2012 3rd International Conference on Computing Communication and Networking Technologies (ICCCNT), July 26-28, 2012, IEEE, Coimbatore, India, pp: 1-5.

Jiang, Q., J. Ma, Z. Ma and G. Li, 2013. A privacy enhanced authentication scheme for telecare medical information systems. J. Med. Syst., 37: 1-18.

Khan, M.K., S.K. Kim and K. Alghathbar, 2011. Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme. Comput. Commun., 34: 305-309.

Kim, K.W. and J.D. Lee, 2014. On the security of two remote user authentication schemes for telecare medical information systems. J. Med. Syst., 38: 1-11.

Kumari, S., M.K. Khan and R. Kumar, 2013. Cryptanalysis and improvement of a privacy enhanced scheme for telecare medical information systems. J. Med. Syst., 37: 1-11.

Lee, S., K. Park, Y. Park and Y. Park, 2016. Symmetric key-based remote user authentication scheme with forward secrecy. J. Korea Multimedia Soc., 19: 585-594.

Ma, C.G., D. Wang and S.D. Zhao, 2014. Security flaws in two improved remote user authentication schemes using smart cards. Intl. J. Commun. Syst., 27: 2215-2227.

Ramasamy, R. and A.P. Muniyandi, 2009. New remote mutual authentication scheme using smart cards. Trans. Data Privacy, 2: 141-152.

Rhee, H.S., J.O. Kwon and D.H. Lee, 2009. A remote user authentication scheme without using smart cards. Comput. Stand. Interfaces, 31: 6-13.

Rhee, K., J. Kwak, S. Kim and D. Won, 2005. Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment. In: Security in Pervasive Computing, Hutter, D. and U. Markus (Eds.). Springer, Berlin, Germany, ISBN:978-3-540-25521-5, pp: 70-84.

Stolfo, S.J., S.M. Bellovin, S. Hershkop, A.D. Keromytis and S. Sinclair *et al*., 2008. Insider Attack and Cyber Security: Beyond the Hacker. Vol. 39, Springer, Berlin, Germany, ISBN:13-978-0-387-77321-6, Pages: 223.

Wang, Y.Y., J.Y. Liu, F.X. Xiao and J. Dan, 2009. A more efficient and secure dynamic ID based remote user authentication scheme. Comput. Commun., 32: 583-585.