International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:3, No:11, 2009

Security Weaknesses of Dynamic ID-based Remote User Authentication Protocol

Hyoungseob Lee, Donghyun Choi, Yunho Lee, Dongho Won, Seungjoo Kim

***Abstract*—** Recently, with the appearance of smart cards, many user authentication protocols using smart card have been proposed to mitigate the vulnerabilities in user authentication process. In 2004, Das *et al*. proposed a ID-based user authentication protocol that is secure against ID-theft and replay attack using smart card. In 2009, Wang *et al*. showed that Das *et al*.'s protocol is not secure to randomly chosen password attack and impersonation attack, and proposed an improved protocol. Their protocol provided mutual authentication and efficient password management. In this paper, we analyze the security weaknesses and point out the vulnerabilities of Wang *et al*.'s protocol.

***Keywords*—**Message Alteration Attack, Impersonation Attack

I. INTRODUCTION

With the increase of users using commercial services through networks, the user authentication protocol has been regarded as a most important security issue. However, many vulnerabilities have been exposed in the user authentication protocol due to the careless password management and the sophisticated attack techniques. Recently, with the appearance of smart card, these vulnerabilities were mitigated.

In 2004, Das *et al*. proposed ID-based authentication protocol to mitigate vulnerabilities of the password-based authentication protocol[3]. This authentication protocol has some advantage that it allows a user to change a password easily, and requires low computations cost by using the hash function, moreover, the server does not need to maintain the password verification table. In 2009, Wang *et al*. pointed out that Das *et al*.'s protocol allowed an attacker to complete the authentication without knowing the password and did not provide the mutual authentication between user and remote server[4]. To improve the previous protocol, Wang *et al*. proposed the secure protocol using dynamic ID and the mutual authentication between user and remote server. The Wang *et al*.'s protocol, however, is not secure against the message alteration attacks and impersonation attacks.

In this paper, we analyze the vulnerabilities of Wang *et al*.'s protocol. This paper is organized as follows. In section II, we briefly review previous protocols. In section III, we describe the vulnerabilities of Wang *et al*.' protocol. and finally the conclusion is presented in section IV.

H. Lee, D. Choi, Y. Lee, D. Won and S. Kim are with Information Security Group, Sungkyunkwan University, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea (e-mail : {hslee, dhchoi, leeyh, dhwon, skim} @security.re.kr)
Corresponding author: Seungjoo Kim

II. RELATED WORKS

A. Das et al.'s Protocol

In 2004, Das *et al* proposed ID-based remote user authentication protocol. This protocol is divided into the four phases of registration, log-in, verification, and password-changing. The notations used in this protocol are defined in Table I.

1. Registration Phase

User U_i transmits his or her password before communicating with remote server S , and the server issues a smart card to U_i .

1. U_i transmits password PW_i to S .
2. S computes $N_i = h(PW_i) \oplus h(x)$ using its secret - variable x .
3. S saves $[h(\bullet), \gamma, N_i]$ in smart card and issues the smart card with PW_i to U_i . γ is a secret value to be stored in smart card that is issued to each user.

2. Log-in Phase

User U_i inputs his or her password PW_i after inserting the smart card into terminal. The smart card performs the following steps.

1. Compute $CID_i = h(PW_i) \oplus h(N_i \oplus \gamma \oplus TS)$ using the information stored in smart card. TS is the time stamp of the present date and time.
2. Compute $B_i = h(CID_i \oplus h(PW_i))$ using the result from the step 1.
3. Computes $C_i = h(TS \oplus N_i \oplus B_i \oplus \gamma)$ using the result from the step 2.
4. Transmit the log-in requesting message $\langle CID_i, N_i, C_i, TS \rangle$ to S .

3. Verification Phase

After remote server S received the log-in requesting message $\langle CID_i, N_i, C_i, TS \rangle$ from U_i at time TS^*, he or she performs the following steps.

1. S checks the validity of the time interval by verifying

the time stamp. If $TS^* - TS \le \Delta TS$, the log-in requesting message of U_i is accepted, if NOT , the log-in request is rejected.

2. S computes $h'(PW_i) = CID_i \oplus h(N_i \oplus \gamma \oplus TS)$.
3. S computes $B'_i = h(CID_i \oplus h'(PW_i))$ using the result from the step 2.
4. S computes $C_i' = h(TS \oplus N_i \oplus B_i' \oplus \gamma)$ using the result from the step 3. If the computed C_i' and C_i are equal, the log-in request of U_i is accepted.

4. Password-changing Phase

If user U_i wants to change password, he or she inputs new password PW_N . smart card computes $N_i^* = N_i \oplus h(PW_i) \oplus h(PW_N)$ and replaces N_i to a new N_i^* .

B. Wang et al.'s protocol

In 2009, Wang *et al*. pointed out the vulnerabilities of the Das *et al*.'s protocol and showed that their protocol allowed an attacker to complete the authentication without knowing the password and did not provide the mutual authentication between user and remote server. To solve these problems, Wang *et al*. proposed secure protocol using dynamic ID and mutual authentication. Their protocol is composed of the three phases of registration, log-in, and verification.

TABLE I
NOTATION

Item	Description
U_i	User
S	Remote Server
ID	User's ID
PW_i	User's Password
$h(\bullet)$	One-way hash Function
$\oplus$	Bitewise XOR Computation
γ	Secret Value of Server To Be Stored in Smart Card
x	Secret Variable of Server
TS	Time Stamp

1. Registration Phase

User U_i only transmits ID_i to remote server S .

1. U_i transmits ID_i to S
2. S computes $N_i = h(PW_i) \oplus h(x) \oplus ID_i$ after choosing its secret variable x and the U_i's password PW_i for itself.
3. S saves $[h(\bullet), \gamma, N_i]$ in smart card and issues the smart card with PW_i to U_i . γ is a secret value to be stored in smart card that is issued to each user.

2. Log-in Phase

User U_i inputs his or her ID_i and PW_i after inserting the smart card into terminal. The smart card performs the following steps.

1. Compute $CID_i = h(PW_i) \oplus h(N_i \oplus \gamma \oplus TS) \oplus ID_i$ using the information stored in smart card. TS is the time stamp of the present date and time.
2. Transmit the log-in requesting message $\langle ID_i, CID_i, N_i, TS \rangle$ to S .

3. Verification Phase

After remote server S received the log-in requesting message $\langle ID_i, CID_i, N_i, TS \rangle$ from U_i at time TS^*, he or she performs the following steps.

1. S checks the validity of the time interval by verifying the time stamp. If $TS^* - TS \le \Delta TS$, the log-in requesting message of U_i's is accepted, if NOT, the log-in request is rejected.
2. S computes $h'(PW_i) = CID_i \oplus h(N_i \oplus \gamma \oplus TS) \oplus ID_i$.
3. S computes $ID_i' = N_i \oplus h(x) \oplus h'(PW_i)$ using the result from the step 2. If the computed ID_i' and ID_i are equal, the log-in request of U_i is accepted.
4. S computes $a' = h(h'(PW_i) \oplus \gamma \oplus TS^*)$ using the result from the step 2. If the computed C_i' and C_i are equal, S transmit $\langle a', TS^* \rangle$ to U_i .
5. If the Verification message $\langle a', TS^* \rangle$ is arrived at time TS' , U_i checks the time stamp whether $TS' - TS^* \le \Delta TS$. If it holds, U_i computes $a = h(h(PW_i) \oplus \gamma \oplus TS^*)$ and compares a with a' .
6. If the two values are equal, U_i considers S to be a valid server.

In Wang *et al*.'s protocol, there is no need to alter the password since the user password is generated directly by the server S .

III. Security analysis of Wang *et al*.'s Protocol

In this section, we point out the vulnerabilities of Wang *et al*.'s protocol.

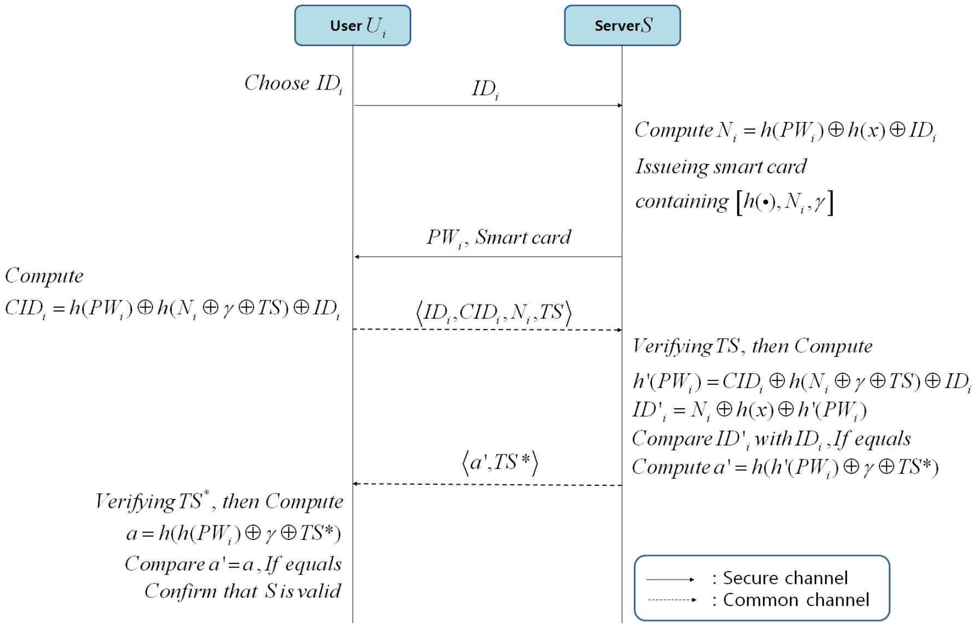

Fig. 1 Wang *et al.*'s protocol

A. Message Alteration Attack

In Wang *et al.*'s protocol, an attacker can be authenticated as a valid user without knowing the ID and password. If an attacker eavesdrops the log-in requesting message $\langle ID_i, CID_i, N_i, TS \rangle$ the valid user U_i transmitted to remote server S, the attacker A performs the following steps.

1. A alters the log-in requesting message $\langle ID_i, CID_i, N_i, TS \rangle$ into $\langle ID_j, CID_i, N_i, TS \rangle$ by choosing the random ID_j.
2. A transmits altered log-in requesting message $\langle ID_j, CID_i, N_i, TS \rangle$ to S.
3. S computes
$$h''(PW_i) = CID_i \oplus h(N_i \oplus \gamma \oplus TS) \oplus ID_j$$
$$= h(PW_i) \oplus h(N_i \oplus \gamma \oplus TS) \oplus ID_i \oplus h(N_i \oplus \gamma \oplus TS) \oplus ID_j$$
$$= h(PW_i) \oplus ID_i \oplus ID_j$$
4. S computes
$$ID_i'' = N_i \oplus h(x) \oplus h''(PW_i).$$
$$= h(PW_i) \oplus h(x) \oplus ID_i \oplus h(x) \oplus h(PW_i) \oplus ID_i \oplus ID_j$$
$$= ID_j$$
As the computed ID_i'' and the ID_j contained in the altered message are equal, S accepts the log-in request.
5. S transmits $\langle a', TS^* \rangle$ to the attacker after computing $a' = h(h''(PW_i) \oplus \gamma \oplus TS^*)$.

Even though attacker A transmits the log-in requesting message to the server only with the altered ID, he or she is able to complete the authentication process successfully. That is, Wang *et al.*'s protocol is equivalent to the protocol in which the user ID and PW are not needed.

B. Impersonation Attack

Although the smart card is equipped with tamper resistance, many researches have shown that the secret values stored in smart card can be extracted by executing the differential power attacks and fault attacks[7][8]. Malicious attacker U_m participating in protocol as a valid user can execute the impersonation attack because U_m can extract the secret value of γ server stored in his or her smart card by executing the differential power attacks and fault attacks. U_m can compute the secret value $h(PW_i)$ of valid user U_i by executing the impersonation attack. If U_m eavesdrops the log-in requesting message $\langle ID_i, CID_i, N_i, TS \rangle$ the user transmitted, the U_m performs the following steps.

1. U_m computes $h(N_i \oplus \gamma \oplus TS)$ using the secret value γ of server.
2. U_m computes $h'(PW_i) = CID_i \oplus h(N_i \oplus \gamma \oplus TS) \oplus ID_i$ from log-in requesting message $\langle ID_i, CID_i, N_i, TS \rangle$.
3. U_m computes $a'' = h(h'(PW_i) \oplus \gamma \oplus TS^*)$ using the result from the step 2 and transmits the $\langle a'', TS^* \rangle$ to U_i.

4. U_i compares a'' within the verification message $\langle a'', TS^* \rangle$ received from U_m with computed $a = h(h(PW_i) \oplus \gamma \oplus TS^*)$.

As the attacker U_m forges the valid verification message $\langle a', TS^* \rangle$ using the secret value γ of server, the user U_i recognizes the attacker U_m as a valid server.

IV. CONCLUSION

In this paper, we have analyzed the security of Wang *et al.*'s protocol. Although Wang *et al.*'s protocol provided mutual authentication and overcame the fatal drawback of Das *et al.*'s protocol, we have shown that Wang *et al.*'s protocol is insecure against the message alteration attack and impersonation attack.

ACKNOWLEDGMENT

* This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract UD070054AD.
* This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2009-(C1090-0902-0016))

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol 24, pp 770-772, 1981
[2] M.S. Hwang, L.H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics 46 , pp28–.30, 2000
[3] ML Das, A Saxena, VP Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Transactions on Consumer Electronics 2004, volume 50, Issue 2, pp. 629-631, 2004.
[4] Y Wang, J Liu, F Xiao, J Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," Computer Communications 32, Volume 32, Issue 4, 2009, pp 583-585
[5] H.M. Sun,"An efficient remote user authentication scheme using smartcards," IEEE Transactions on Consumer Electronics 46, pp 958–961. 2000
[6] YP Liao, SS Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, Volume 31, Issue 1, pp 24-29, 2009
[7] HC Hsiang, WK Shih, "improvement of the secure dynamic id based remote user authentication scheme for multi-server environment,"Computer Standards & Interfaces 31, Issue 6, 2008, pp 1118-1123, 2008
[8] T.S. Messergers, E.A. Dabbish, R.H. Sloan, "Examining smart card security under the threat of power analysis attacks," IEEE Trans. Comput. 51, pp 541–.552. 2002