Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 687879, 8 pages
http://dx.doi.org/10.1155/2014/687879

Research Article

Security Analysis and Improvement of an Anonymous Authentication Scheme for Roaming Services

Youngsook Lee[1] and Juryon Paik[2]

[1] *Department of Cyber Investigation Police, Howon University, 64 3-gil, Gunsan, Jeollabuk-do 573-718, Republic of Korea*
[2] *Department of Computer Engineering, Sungkyunkwan University, 2066 Seoburo, Suwon, Gyeonggido 440-746, Republic of Korea*

Correspondence should be addressed to Juryon Paik; wise96@skku.edu

Received 7 August 2014; Accepted 25 August 2014; Published 11 September 2014

Academic Editor: Junghyun Nam

An anonymous authentication scheme for roaming services in global mobility networks allows a mobile user visiting a foreign network to achieve mutual authentication and session key establishment with the foreign-network operator in an anonymous manner. In this work, we revisit He et al.'s anonymous authentication scheme for roaming services and present previously unpublished security weaknesses in the scheme: (1) it fails to provide user anonymity against any third party as well as the foreign agent, (2) it cannot protect the passwords of mobile users due to its vulnerability to an offline dictionary attack, and (3) it does not achieve session-key security against a man-in-the-middle attack. We also show how the security weaknesses of He et al.'s scheme can be addressed without degrading the efficiency of the scheme.

1. Introduction

As wireless network and communication technologies advance, there has been a dramatic increase in the use of lightweight computing devices, such as sensors, smart phones, and tablet PCs, being used in our daily lives. To enjoy the convenience of mobility, a roaming service should be seamlessly provided with respect to availability and security, by means of using a visited foreign network. In general, three parties—a mobile user, a foreign agent, and the home agent—participate in a roaming process. A seamless roaming service requires significant security challenges to be addressed among the participants. Basically, authentication and key establishment between the mobile user and the foreign agent should be achieved via assistance of the home agent to prevent illegal usages of the network and to protect their subsequent communications. Achieving anonymity of the mobile user is also important in a roaming service to protect the privacy of the user. Anonymity has recently been identified as a major security property for many applications, including location-based services, anonymous web browsing, and e-voting. These security challenges and their cryptographic solutions, commonly called *anonymous authentication schemes*, constitute an active research area.

The first anonymous authentication scheme for roaming services was proposed by Zhu and Ma [1] in 2004. This initial proposal has been followed by a number of authentication schemes offering various levels of security and efficiency. Some schemes [2–4] have been proven secure using a computer security approach while others (e.g., [5–7]) justify their security on purely heuristic grounds without providing no formal analysis of security. However, despite all the work conducted over the last decade, it still remains a challenging task to come up with an authentication scheme that meets all the desired goals for roaming services [8]. Most of the existing schemes fail to achieve important security properties such as user anonymity [2, 6], session-key security [9], perfect forward secrecy [10], two-factor security [11], resistance against impersonation attacks [12], and resistance against offline dictionary attacks [13]. For this domain, all published schemes are far from ideal as evidenced by a continual history of schemes being proposed and years later found to be flawed.

Recently, Xie et al. [4] proposed a new authentication scheme for roaming services and claimed that their scheme not only provides efficiency and user friendliness but also is secure against various attacks. But He et al. [12] demonstrated that Xie et al.'s scheme is susceptible to impersonation attacks and therefore does not achieve mutual authentication between a mobile user and the foreign agent. In addition, He et al. proposed a new authentication scheme which improves Xie et al.'s scheme in terms of both security and efficiency. However, we found that He et al.'s improved scheme is not satisfactory enough but still suffers from major security weaknesses.

(i) He et al.'s scheme does not provide user anonymity not only against the foreign agent but also against any third party.

(ii) He et al.'s scheme may not protect the passwords of mobile users against an offline dictionary attack.

(iii) He et al.'s scheme is not secure against a man-in-the-middle attack and thus cannot guarantee the security of session keys.

Besides reporting these weaknesses in He et al.'s scheme, we also propose an improved authentication scheme which achieves, among others, user anonymity, session-key security, and resistance against offline dictionary attacks. The performance of our scheme is similar to that of He et al.'s scheme but is superior to that of Xie et al.'s scheme (see Section 4).

Throughout the paper, we make the following assumptions on the capabilities of the probabilistic polynomial-time adversary in order to properly capture security requirements of two-factor authentication schemes using smart cards in global mobility networks.

(i) The adversary has the complete control of all message exchanges between the three parties: a mobile user, the foreign agent, and the home agent. That is, the adversary can eavesdrop, insert, modify, intercept, and delete messages exchanged among the parties at will [14–16].

(ii) The adversary is able to (1) extract the sensitive information on the smart card of a mobile user possibly via a power analysis attack [17, 18] or (2) learn the password of the mobile user through shoulder surfing or by employing a malicious card reader. However, it is not allowed that the adversary compromises both the information on the smart card and the password of the mobile user; it is clear that there is no way to prevent the adversary from impersonating the mobile user if both factors are compromised.

2. A Review of He et al.'s Scheme

He et al.'s authentication scheme [12] consists of three phases: the registration phase, the login and key agreement phase, and the password update phase. The system parameters listed in Table 1 are assumed to have been established in advance before the scheme is used in practice. Let $\|$ and $\oplus$ denote the string concatenation operation and the bitwise exclusive-OR (XOR) operation, respectively.

Table 1: System parameters.

ID_{HA}, ID_{FA}	The identities of HA and FA, respectively
p, q	Two large primes such that $p = rq + 1$ for some $r \in \mathbb{N}$
x	The master secret key of HA
k_{HF}	A (cryptographically strong) key shared between HA and FA
(E, D)	A pair of symmetric encryption and decryption algorithms
$H(\cdot)$	A cryptographic hash function

2.1. Registration Phase. For a mobile user MU, this phase is performed only once when MU registers itself with the home agent HA.

(1) MU chooses its identity ID_{MU} and password pw_{MU} freely and sends the identity ID_{MU} to HA via a secure channel.

(2) HA computes $SID_{MU} = E_x(ID_{MU}\|ID_{HA})$ and $DID_{MU} = H(ID_{MU})^x \bmod p$ and issues MU a smart card loaded with $\{SID_{MU}, DID_{MU}, ID_{HA}, p, q, (E, D), H\}$.

(3) MU replaces SID_{MU} and DID_{MU}, which are contained in the smart card, with $TID_{MU} = SID_{MU} \oplus H(0\|pw_{MU})$ and $EID_{MU} = DID_{MU} \oplus H(1\|pw_{MU})$, respectively.

2.2. Login and Key Agreement Phase. This phase is carried out whenever MU visits a foreign network and wants to gain access to the network. During the phase, mutual authentication and session-key establishment are conducted between MU and FA with the help of HA. Algorithm 1 depicts how the phase works, and its description follows.

Step 1. MU inserts its smart card into the card reader and inputs its identity ID_{MU} and password pw_{MU}. Next, MU retrieves the current timestamp T_1, chooses a random number $a \in \mathbb{Z}_q^*$, and computes

$$\begin{aligned} A &= H(ID_{MU})^a \bmod p, \\ K_{MH} &= (EID_{MU} \oplus H(1\|pw_{MU}))^a \bmod p \\ &= H(ID_{MU})^{ax} \bmod p, \\ k_{MH} &= H(K_{MH}\|T_1), \\ SID_{MU} &= TID_{MU} \oplus H(0\|pw_{MU}) \\ &= E_x(ID_{MU}\|ID_{HA}), \\ C_{MH} &= E_{k_{MH}}(SID_{MU}\|ID_{MU}\|ID_{FA}). \end{aligned} \tag{1}$$

Then, MU sends the message $M_1 = \langle ID_{HA}, T_1, A, C_{MH}\rangle$ to the foreign agent FA.

$\boxed{MU}$ $\boxed{FA}$ $\boxed{HA}$

inputs ID_{MU} and pw_{MU}
retrieves the timestamp T_1
$a \in_R \mathbb{Z}_q^*, A = H(ID_{MU})^a$
$K_{MH} = (EID_{MU} \oplus H(1\|pw_{MU}))^a$
$\quad = H(ID_{MU})^{ax}$
$k_{MH} = H(K_{MH}\|T_1)$
$SID_{MU} = TID_{MU} \oplus H(0\|pw_{MU})$
$C_{MH} = E_{k_{MH}}(SID_{MU}\|ID_{MU}\|ID_{FA})$

$$\xrightarrow{M_1=\langle ID_{HA},T_1,A,C_{MH}\rangle}$$

checks the freshness of T_1
retrieves the timestamp T_2
$C_{FH} = E_{k_{HF}}(ID_{FA}\|T_2\|M_1)$

$$\xrightarrow{M_2=\langle ID_{FA},T_2,C_{FH}\rangle}$$

checks the freshness of T_2
Does $D_{k_{HF}}(C_{FH})$ yield ID_{FA} and T_2?
$K_{MH} = A^x, k_{MH} = H(K_{MH}\|T_1)$
Does $D_{k_{MH}}(C_{MH})$ yield ID_{FA}?
Does $D_x(SID_{MU})$ yield ID_{MU}?
retrieves the timestamp T_3
$\sigma = H(M_1\|T_3\|K_{MH}\|ID_{MU}\|ID_{FA}\|ID_{HA})$
$C_{HF} = E_{k_{HF}}(ID_{MU}\|ID_{FA}\|T_3\|\sigma)$

$$\xleftarrow{M_3=\langle ID_{FA},T_3,C_{HF}\rangle}$$

$ID_{MU}\|ID_{FA}\|T_3\|\sigma = D_{k_{HF}}(C_{HF})$
checks the freshness of T_3
$b \in \mathbb{Z}_q^*, B = H(ID_{MU})^b$
$K_{FM} = A^b, k_{FM} = H(K_{FM})$
$C_{FM} = E_{k_{FM}}(ID_{MU}\|ID_{FA}\|T_3\|\sigma\|B)$
$sk = H(K_{FM}+1)$

$$\xleftarrow{M_4=\langle ID_{FA},T_3,B,C_{FM}\rangle}$$

checks the freshness of T_3
$K_{FM} = B^a, k_{FM} = H(K_{FM})$
Does $D_{k_{FM}}(C_{FM})$ yield ID_{MU}, ID_{FA} and T_3?
$\sigma \overset{?}{=} H(M_1\|T_3\|K_{MH}\|ID_{MU}\|ID_{FA}\|ID_{HA})$
$sk = H(K_{FM}+1)$

Algorithm 1: Login and key agreement phase of He et al.'s scheme [12].

Step 2. Upon receiving M_1, FA checks the freshness of the timestamp T_1. If it is not fresh, FA aborts the session. Otherwise, FA retrieves the current timestamp T_2, computes

$$C_{FH} = E_{k_{HF}}(ID_{FA}\|T_2\|M_1) \tag{2}$$

and sends the message $M_2 = \langle ID_{FA}, T_2, C_{FH}\rangle$ to HA.

Step 3. HA checks if the timestamp T_2 is fresh. If not, HA aborts the session. Otherwise, HA decrypts C_{FH} with key k_{HF} and verifies that the decryption yields the same ID_{FA} and T_2 as contained in M_2. HA aborts if the verification fails. Otherwise, HA computes $K_{MH} = A^x \bmod p$ and $k_{MH} = H(K_{MH}\|T_1)$, decrypts C_{MH} with key k_{MH}, and checks if this decryption produces the same ID_{FA} as in M_2. HA aborts if the check fails. Otherwise, HA decrypts SID_{MU} with key x and checks if this decryption gives the same ID_{MU} as produced through the decryption of C_{MH}. If only the two IDs match, HA retrieves the current timestamp T_3, computes

$$\begin{gathered}\sigma = H(M_1\|T_3\|K_{MH}\|ID_{MU}\|ID_{FA}\|ID_{HA}),\\ C_{HF} = E_{k_{HF}}(ID_{MU}\|ID_{FA}\|T_3\|\sigma),\end{gathered} \tag{3}$$

and sends the message $M_3 = \langle ID_{FA}, T_3, C_{HF}\rangle$ to FA.

Step 4. FA decrypts C_{HF} with key k_{HF} and checks the freshness of the timestamp T_3. If only T_3 is fresh, FA chooses a random number $b \in \mathbb{Z}_q^*$ and computes

$$\begin{aligned}B &= H(ID_{MU})^b \bmod p,\\ K_{FM} &= A^b \bmod p\\ &= H(ID_{MU})^{ab} \bmod p,\end{aligned}$$

$$k_{FM} = H(K_{FM}),$$
$$C_{FM} = E_{k_{FM}}(ID_{MU} \| ID_{FA} \| T_3 \| \sigma \| B). \tag{4}$$

(Note, here, that the timestamp T_3 (received from HA) is used in generating the ciphertext C_{FM} since MU will need it to check the validity of σ.) Then, FA sends the message $M_4 = \langle ID_{FA}, T_3, B, C_{FM} \rangle$ to MU and computes the session key $sk = H(K_{FM} + 1)$.

Step 5. MU first checks the freshness of the timestamp T_3 and aborts the session if not fresh. Otherwise, MU computes $K_{FM} = B^a \bmod p$ and $k_{FM} = H(K_{FM})$, decrypts C_{FM} with key k_{FM}, and verifies that the decryption correctly returns ID_{MU}, ID_{FA}, and T_3. If the verification succeeds, MU checks if σ is equal to $H(M_1 \| T_3 \| K_{MH} \| ID_{MU} \| ID_{FA} \| ID_{HA})$ and if equal computes the session key $sk = H(K_{FM} + 1)$.

2.3. Password Update Phase. One of the general guidelines to get better password security is to ensure that passwords are changed at regular intervals. He et al.'s scheme allows mobile users to freely update their passwords.

(1) MU inserts his smart card into a card reader and enters both the current password pw_{MU} and the new password pw'_{MU}.

(2) The smart card computes $TID'_{MU} = TID_{MU} \oplus H(0\|pw_{MU}) \oplus H(0\|pw'_{MU})$ and $EID'_{MU} = EID_{MU} \oplus H(1\|pw_{MU}) \oplus H(1\|pw'_{MU})$ and replaces TID_{MU} and EID_{MU} with TID'_{MU} and EID'_{MU}, respectively.

3. Weaknesses in He et al.'s Scheme

In this section, we point out four weaknesses in He et al.'s scheme, starting with the most obvious one.

Weakness 1. He et al.'s scheme does not provide user anonymity against the foreign agent FA.

This weakness is straightforward to see as the identity of MU, ID_{MU}, is given to FA via the ciphertext C_{HF} (see Step 4 of the login and key agreement phase of the scheme).

Weakness 2. He et al.'s scheme may not protect the password of MU, pw_{MU}, against an offline dictionary attack.

Weakness 2 is due to the fact that EID_{MU} is computed using the bitwise XOR operation when the multiplicative subgroup of $\mathbb{Z}_p^*$ is not closed under the XOR operation. This design flaw allows an adversary to find out the password pw_{MU} by mounting an offline dictionary attack if the subgroup is much smaller than $\mathbb{Z}_p^*$. We observe, for He et al.'s scheme, that (1)p and q are defined as two primes such that $p = rq + 1$ for some $r \in \mathbb{N}$ and (2) the random exponents a and b are chosen from $\mathbb{Z}_q^*$. Based on these observations, it is reasonable to speculate that He et al.'s scheme was designed to work in a multiplicative subgroup of $\mathbb{Z}_p^*$ that has a prime order q, though not explicitly mentioned by the authors. For simplicity, let us denote the prime-order subgroup by $\mathbb{G}$. Since K_{MH} and DID_{MU} are computed as $K_{MH} = (DID_{MU})^a \bmod p$ and $DID_{MU} = H(ID_{MU})^x \bmod p$, it ought to be the case that $DID_{MU} \in \mathbb{G}$, which in turn implies that H is a hash function mapping arbitrary strings into elements of $\mathbb{G}$. Now, assume that an adversary $\mathscr{A}$ has gained temporary access to the smart card of MU and then obtained the value of EID_{MU} stored there (possibly by employing a power analysis attack [17]). Then, note that EID_{MU} can be used as a password verifier in an offline dictionary attack because EID_{MU} is computed as $EID_{MU} = DID_{MU} \oplus H(1\|pw_{MU})$ when $\mathbb{G}$ is not closed under the bitwise XOR operation. Let $\mathscr{PW}$ be the set of all possible passwords. The adversary $\mathscr{A}$ can mount an offline dictionary attack as follows.

Step 1. $\mathscr{A}$ makes a guess $pw'_{MU} \in \mathscr{PW}$ on the password pw_{MU} and computes

$$DID'_{MU} = EID_{MU} \oplus H\left(1\|pw'_{MU}\right). \tag{5}$$

Step 2. $\mathscr{A}$ then checks whether DID'_{MU} is an element of $\mathbb{G}$ or not. If $DID'_{MU} \notin \mathbb{G}$, $\mathscr{A}$ deletes pw'_{MU} from the dictionary $\mathscr{PW}$ (i.e., $\mathscr{PW} = \mathscr{PW} \setminus \{pw'_{MU}\}$). Note that $DID'_{MU} \notin \mathbb{G}$ implies $pw'_{MU} \neq pw_{MU}$.

Step 3. $\mathscr{A}$ repeats Steps 1 and 2 until the correct password is found (i.e., until $|\mathscr{PW}| = 1$).

If p is a safe prime (i.e., $p = 2q+1$), then this attack would fail, cutting only the size of $\mathscr{PW}$ about in half. However, if p is much greater than q (e.g., $\log_2 p = 512$ and $\log_2 q = 256$), the dictionary attack will succeed in determining the correct password with an overwhelming probability. Similar dictionary attacks have been also mounted against key exchange protocols; see, for example, [19]. Weakness 2 can be easily addressed by replacing the bitwise XOR operation with the multiplication operation.

Next, we identify two other major weaknesses in He et al.'s scheme.

Weakness 3. He et al.'s scheme may not guarantee user anonymity even against a third party who is not a legitimate protocol participant.

Weakness 4. He et al.'s scheme could wrongly lead MU and FA to establish a session key with a malicious party who is not even registered with HA.

We demonstrate Weaknesses 3 and 4 by mounting a type of man-in-the-middle attack against the scheme. The attack scenario is outlined in Figure 1 and is detailed as follows.

Step 1. As a preliminary step, the adversary $\mathscr{A}$ chooses a random number $a' \in \mathbb{Z}_q^*$ and computes $A' = H(ID)^{a'} \bmod p$, where ID denotes an arbitrary identity.

Step 2. When MU sends the first message $M_1 = \langle ID_{HA}, T_1, A, C_{MH} \rangle$ to FA, $\mathscr{A}$ eavesdrops on this message to obtain A

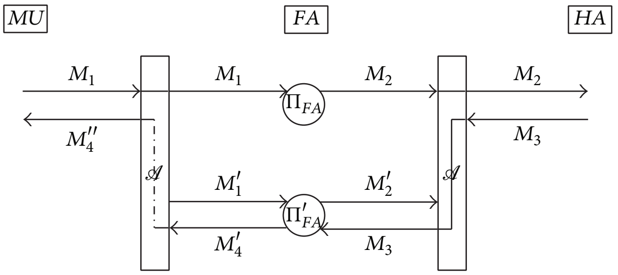

Figure 1: A man-in-the-middle attack on He et al.'s scheme.

and C_{MH}. Immediately after the eavesdropping, $\mathscr{A}$ retrieves the current timestamp T'_1 and sends a fake message $M'_1 = \langle ID_{HA}, T'_1, A', C_{MH}\rangle$ to FA as if it is another roaming request from a mobile user.

Step 3. Since both T_1 and T'_1 are fresh, FA will compute $C_{FH} = E_{k_{HF}}(ID_{FA} \| T_2 \| M_1)$ and $C'_{FH} = E_{k_{HF}}(ID_{FA} \| T'_2 \| M'_1)$ and send two messages $M_2 = \langle ID_{FA}, T_2, C_{FH}\rangle$ and $M'_2 = \langle ID_{FA}, T'_2, C'_{FH}\rangle$ to HA. Let Π_{FA} and Π'_{FA} be the instances of FA who sends the messages M_2 and M'_2, respectively.

Step 4. $\mathscr{A}$ intercepts the message M'_2 while letting M_2 reach its destination, HA. Since M_2 is a valid message, HA will compute

$$\begin{aligned} \sigma &= H\left(M_1 \| T_3 \| K_{MH} \| ID_{MU} \| ID_{FA} \| ID_{HA}\right), \\ C_{HF} &= E_{k_{HF}}\left(ID_{MU} \| ID_{FA} \| T_3 \| \sigma\right), \end{aligned} \tag{6}$$

and send the message $M_3 = \langle ID_{FA}, T_3, C_{HF}\rangle$ to FA.

Step 5. $\mathscr{A}$ redirects the message M_3 so that it is delivered to Π'_{FA} instead of Π_{FA}. As a result, Π_{FA} will not receive any response message and thus will abort after a certain amount of time.

Step 6. After decrypting C_{HF} and since T_3 is fresh, Π'_{FA} will proceed as per the protocol specification. That is, Π'_{FA} will choose a random number $b' \in \mathbb{Z}^*_q$, compute

$$\begin{aligned} B' &= H(ID_{MU})^{b'} \bmod p, \\ K'_{FM} &= A'^{b'} \bmod p \\ &= H(ID)^{a'b'} \bmod p, \\ k'_{FM} &= H\left(K'_{FM}\right), \\ C'_{FM} &= E_{k'_{FM}}\left(ID_{MU} \| ID_{FA} \| T_3 \| \sigma \| B'\right), \end{aligned} \tag{7}$$

send the message $M'_4 = \langle ID_{FA}, T_3, B', C'_{FM}\rangle$ to MU, and then compute its session key as

$$sk_{FA} = H\left(K'_{FM} + 1\right). \tag{8}$$

Step 7. $\mathscr{A}$ intercepts the message M'_4, computes $K'_{FM} = B'^{a'} \bmod p$ and $k'_{FM} = H(K'_{FM})$, and decrypts C'_{FM} with key k'_{FM} to obtain ID_{MU}, ID_{FA}, and σ. Then, $\mathscr{A}$ chooses a random number $b'' \in \mathbb{Z}^*_q$, computes

$$\begin{aligned} B'' &= H(ID_{MU})^{b''} \bmod p, \\ K''_{FM} &= A^{b''} \bmod p \\ &= H(ID_{MU})^{ab''} \bmod p, \\ k''_{FM} &= H\left(K''_{FM}\right), \\ C''_{FM} &= E_{k''_{FM}}\left(ID_{MU} \| ID_{FA} \| T_3 \| \sigma \| B''\right), \end{aligned} \tag{9}$$

and sends the message $M''_4 = \langle ID_{FA}, T_3, B'', C''_{FM}\rangle$ to MU as if it is from FA.

Step 8. Upon receiving M''_4, MU will proceed to compute its session key

$$sk_{MU} = H\left(K''_{FM} + 1\right), \tag{10}$$

where K''_{FM} is computed as $K''_{FM} = B''^{a} \bmod p$, because (1) T_3 is fresh, (2) decryption of C''_{FM} with key k''_{FM} correctly yields ID_{MU}, ID_{FA}, and T_3, and (3) σ is equal to $H(M_1 \| T_3 \| K_{MH} \| ID_{MU} \| ID_{FA} \| ID_{HA})$.

Step 9. $\mathscr{A}$ computes the two session keys, sk_{FA} and sk_{MU}, in the straightforward way.

Through the attack, user anonymity is completely compromised as the identity of MU, ID_{MU}, is disclosed to the adversary $\mathscr{A}$ in Step 7. From the viewpoint of session-key secrecy, the effect of our attack is the same as that of a man-in-the-middle attack. At the end of the attack, MU and FA believe that they have established a secure session with each other sharing a secret key, while in fact they have shared their keys with the adversary $\mathscr{A}$. As a result, $\mathscr{A}$ can not only access and relay any confidential messages between MU and FA but also send arbitrary messages for its own benefit impersonating one of them to the other. Man-in-the-middle attacks similar to the attack above have been also presented against various key exchange protocols; see, for example, [20, 21].

4. Our Improved Scheme

We now show how to address all the weaknesses identified in He et al.'s scheme without degrading the efficiency of the scheme. Let $\mathbb{G}$ be a cyclic group of prime order q. A standard way of generating $\mathbb{G}$ is to choose two large primes p, q such that $p = rq + 1$ for some small $r \in \mathbb{N}$ (e.g., $r = 2$) and let $\mathbb{G}$ be the subgroup of order q in $\mathbb{Z}^*_p$. Hereafter, we will omit "mod p" from expressions for notational simplicity. Assume that the master secret key of HA, x, is an element of $\mathbb{Z}^*_q$ (i.e., $x \in \mathbb{Z}^*_q$) and the secret key shared between FA and HA, k_{HF}, has length of ℓ bits. Then we define four cryptographic hash functions:

(i) $F : \{0,1\}^* \rightarrow \{0,1\}^{\ell}$,

(ii) $G : \{0,1\}^* \rightarrow \mathbb{G}$,

(iii) $H : \{0,1\}^* \rightarrow \{0,1\}^{\kappa}$, where κ represents the bit-length of session keys,

(iv) $I : \{0,1\}^* \rightarrow \{0,1\}^{\varepsilon}$, where ε represents the bit-length of SID_{MU} (for the definition of SID_{MU}, see the description of He et al.'s scheme given in Section 2).

We begin by presenting how to address Weaknesses 3 and 4 (described in the previous section). The vulnerability of He et al.'s scheme to the man-in-the-middle attack is because there is no way for an instance of FA to check whether the received ciphertext C_{HF} was sent in response to its own request or another instance's request. This design flaw allows the adversary to exploit HA's response sent for one session as the response for another session. To prevent the attack, we suggest to modify the computation of the ciphertext C_{HF} from $C_{HF} = E_{k_{HF}}(ID_{MU} \| ID_{FA} \| T_3 \| \sigma)$ to

$$C_{HF} = E_{k_{HF}}\left(ID_{MU} \| ID_{FA} \| T_2 \| T_3 \| \sigma\right). \qquad (11)$$

The timestamp T_2 is now included as part of the plaintext to be encrypted to C_{HF}. The inclusion of T_2 tightly links FA's request and HA's response and thus effectively prevents the man-in-the-middle attack.

However, with the above modification alone, He et al.'s scheme cannot fully achieve user anonymity in the sense that the identity of MU is still disclosed to FA. Therefore, we suggest to further modify the computation of C_{HF} as follows:

$$C_{HF} = E_{k_{HF}}\left(G\left(ID_{MU}\right) \| ID_{FA} \| T_2 \| T_3 \| \sigma\right). \qquad (12)$$

The ciphertext C_{HF} is now generated using $G(ID_{MU})$ instead of ID_{MU}. This modification certainly prevents FA from immediately learning ID_{MU} via decryption of C_{HF}.

We next present a possible way of eliminating the vulnerability of He et al.'s scheme to offline dictionary attacks. Recall that this vulnerability is due to the fact that EID_{MU} is computed using the bitwise XOR operation when the multiplicative subgroup of $\mathbb{Z}_p^*$ is not closed under the XOR operation. Given the flaw in the design, the solution is clear; use the multiplication operation instead of the XOR operation when computing EID_{MU}. Hence, we change the computation of EID_{MU} from $EID_{MU} = DID_{MU} \oplus H(1 \| pw_{MU})$ to

$$EID_{MU} = DID_{MU} \cdot G(1 \| pw_{MU})^{-1}. \qquad (13)$$

Accordingly, the computation of K_{MH} should be also changed to

$$\begin{aligned} K_{MH} &= \left(EID_{MU} \cdot G\left(1 \| pw_{MU}\right)\right)^{a} \\ &= G(ID_{MU})^{ax}. \end{aligned} \qquad (14)$$

Finally, we suggest the following additional changes to resolve some notational ambiguities and to correct the misuse of the hash function H:

$$\begin{gathered} SID_{MU} = E_{F(x)}\left(ID_{MU} \| ID_{HA}\right), \qquad DID_{MU} = G(ID_{MU})^{x}, \\ TID_{MU} = SID_{MU} \oplus I\left(0 \| pw_{MU}\right) \\ A = G(ID_{MU})^{a}, \\ k_{MH} = F\left(K_{MH} \| T_1\right), \\ SID_{MU} = TID_{MU} \oplus I\left(0 \| pw_{MU}\right), \\ B = G(ID_{MU})^{b}, \qquad k_{FM} = F\left(K_{FM}\right). \end{gathered} \qquad (15)$$

As a result of the above modifications, the password update phase is modified as follows.

(1) MU inserts his smart card into a card reader and enters the identity ID_{MU}, the current password pw_{MU}, and the new password pw'_{MU}.

(2) The smart card computes $TID'_{MU} = TID_{MU} \oplus I(0 \| pw_{MU}) \oplus I(0 \| pw'_{MU})$ and $EID'_{MU} = EID_{MU} \cdot G(1 \| pw_{MU}) \cdot G(1 \| pw'_{MU})^{-1}$ and replaces TID_{MU} and EID_{MU} with TID'_{MU} and EID'_{MU}, respectively.

Combining the above modifications together yields an improved authentication scheme described in Algorithm 2. Our scheme improves He et al.'s scheme in various aspects: (1) it enjoys the anonymity of the mobile user MU against any parties other than the home agent HA, including the foreign agent FA; (2) it withstands offline dictionary attacks even when the information in the smart card is disclosed; (3) it protects the security of session keys against man-in-the-middle attacks. Clearly, the performance of our scheme is similar to that of He et al.'s scheme. Hence, we can say that our improvement enhances the security of He et al.'s scheme while maintaining the efficiency of the scheme.

5. Concluding Remarks

This work demonstrated that He et al.'s authentication scheme for roaming services fails to achieve major security properties—user anonymity, password security, and session-key security—in the presence of a malicious adversary. We have shown that failure to achieving user anonymity and session-key security is due to the vulnerability to a man-in-the-middle attack while failure to achieving password security is due to the vulnerability to an offline dictionary attack. Note that the latter vulnerability implies that He et al.'s scheme does not achieve two-factor security. We hope that similar security flaws as identified in this work can be prevented in the future design of anonymous authentication schemes.

This work also showed how the security of He et al.'s authentication scheme can be improved without efficiency degradation. Our improved scheme not only protects user

```
MU                                                   FA                                                   HA
inputs $ID_{MU}$ and $pw_{MU}$
retrieves the timestamp $T_1$
$a \in_R \mathbb{Z}_q^*, A = G(ID_{MU})^a$
$K_{MH} = (EID_{MU} \cdot G(1\|pw_{MU}))^a$
      $= G(ID_{MU})^{ax}$
$k_{MH} = F(K_{MH}\|T_1)$
$SID_{MU} = TID_{MU} \oplus I(0\|pw_{MU})$
$C_{MH} = E_{k_{MH}}(SID_{MU}\|ID_{MU}\|ID_{FA})$
        $\xrightarrow{M_1=\langle ID_{HA},T_1,A,C_{MH}\rangle}$
                                    checks the freshness of $T_1$
                                    retrieves the timestamp $T_2$
                                    $C_{FH} = E_{k_{HF}}(ID_{FA}\|T_2\|M_1)$
                                            $\xrightarrow{M_2=\langle ID_{FA},T_2,C_{FH}\rangle}$
                                                        checks the freshness of $T_2$
                                                        Does $D_{k_{HF}}(C_{FH})$ yield $ID_{FA}$ and $T_2$?
                                                        $K_{MH} = A^x, k_{MH} = F(K_{MH}\|T_1)$
                                                        Does $D_{k_{MH}}(C_{MH})$ yield $ID_{FA}$?
                                                        Does $D_x(SID_{MU})$ yield $ID_{MU}$?
                                                        retrieves the timestamp $T_3$
                                                        $\sigma = H(M_1\|T_3\|K_{MH}\|ID_{MU}\|ID_{FA}\|ID_{HA})$
                                                        $C_{HF} = E_{k_{HF}}(G(ID_{MU})\|ID_{FA}\|T_2\|T_3\|\sigma)$
                                            $\xleftarrow{M_3=\langle ID_{FA},T_3,C_{HF}\rangle}$
                                    checks the freshness of $T_3$
                                    Does $D_{k_{MH}}(C_{HF})$ yield $T_2$ & $T_3$?
                                    $b \in \mathbb{Z}_q^*, B = G(ID_{MU})^b$
                                    $K_{FM} = A^b, k_{FM} = F(K_{FM})$
                                    $C_{FM} = E_{k_{FM}}(ID_{MU}\|ID_{FA}\|T_3\|\sigma\|B)$
                                    $sk = H(K_{FM} + 1)$
        $\xleftarrow{M_4=\langle ID_{FA},T_3,B,C_{FM}\rangle}$
checks the freshness of $T_3$
$K_{FM} = B^a, k_{FM} = F(K_{FM})$
Does $D_{k_{FM}}(C_{FM})$ yield $ID_{MU}$, $ID_{FA}$ and $T_3$?
$\sigma \overset{?}{=} H(M_1\|T_3\|K_{MH}\|ID_{MU}\|ID_{FA}\|ID_{HA})$
$sk = H(K_{FM} + 1)$
```

Algorithm 2: The login and key agreement phase of our improved scheme.

anonymity against any third parties other than the home agent but also is secure against offline dictionary attacks as well as man-in-the-middle attacks. We leave it as a future work to design an anonymous authentication scheme for roaming services that achieves provable security in a well-defined communication model while providing the same (or even better) level of efficiency as the schemes studied in this paper.

Conflict of Interests

The authors declare no conflict of interests.

Acknowledgment

This work was supported by Howon University in 2014.

References

[1] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 230–234, 2004.

[2] C. Chang, C. Lee, and Y. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," *Computer Communications*, vol. 32, no. 4, pp. 611–618, 2009.

[3] D. He, S. Chan, C. Chen, and J. Bu, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 61, no. 2, pp. 465–476, 2011.

[4] Q. Xie, B. Hu, X. Tan, M. Bao, and X. Yu, "Robust anonymous two-factor authentication scheme for roaming service in global mobility network," *Wireless Personal Communications*, vol. 74, no. 2, pp. 601–614, 2014.

[5] C. Lee, M. Hwang, and I. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, 2006.

[6] C. Wu, W. Lee, and W. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Communications Letters*, vol. 12, no. 10, pp. 722–723, 2008.

[7] K. Son, D. Han, and D. Won, "A privacy-protecting authentication scheme for roaming services with smart cards," *IEICE Transactions on Communications*, vol. 95, no. 5, pp. 1819–1821, 2012.

[8] R. Madhusudhan and R. Mittal, "Dynamic id-based remote user password authentication schemes using smart cards: a review," *Journal of Network and Computer Applications*, vol. 35, no. 4, pp. 1235–1248, 2012.

[9] T. Youn, Y. Park, and M. Li, "Weaknesses in an anon ymous authentication scheme for roaming service in global mobility networks," *IEEE Communications Letters*, vol. 13, no. 7, pp. 1118–1123, 2009.

[10] T. S. Messerges, E. A. Dabbish, and R. Sloan, "Examining smartcard security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[11] Q. Jiang, J. Ma, G. Li, and L. Yang, "An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 68, no. 4, pp. 1477–1491, 2013.

[12] D. He, N. Kumar, M. K. Khan, and J. Lee, "Anonymous two-factor authentication for consumer roaming service in global mobility networks," *IEEE Transactions on Consumer Electronics*, vol. 59, no. 4, pp. 811–817, 2013.

[13] W. Jeon, J. Kim, J. Nam, Y. Lee, and D. Won, "An enhanced secure authentication scheme with anonymity for wireless environments," *IEICE Transactions on Communications*, vol. 95, no. 7, pp. 2505–2508, 2012.

[14] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Advances in Cryptology—CRYPTO'93*, vol. 773 of *Lecture Notes in Computer Science*, pp. 232–249, Springer, Berlin, Germany, 1994.

[15] J. Nam, K. K. R. Choo, J. Kim, H. Kang, J. Paik, and D. Won, "Password-only authenticated three-party key exchange with provable security in the standard model," *The Scientific World Journal*, vol. 2014, Article ID 825072, 11 pages, 2014.

[16] J. Nam, K.-K. R. Choo, J. Kim et al., "Password-only authenticated three-party key exchange with provable security in the standard model," *The Scientific World Journal*, vol. 2014, Article ID 802359, 11 pages, 2014.

[17] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO' 99*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 388–397, Springer, 1999.

[18] H. Mun, K. Han, Y. Lee, C. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 214–222, 2012.

[19] J. Nam, K. K. R. Choo, M. Kim, J. Paik, and D. Won, "Dictionary attacks against password-based authenticated three-party key exchange protocols," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 12, pp. 3244–3260, 2013.

[20] J. Nam, J. Paik, and D. Won, "A security weakness in Abdalla et al.'s generic construction of a group key exchange protocol," *Information Sciences*, vol. 181, no. 1, pp. 234–238, 2011.

[21] J. Nam, K. K. R. Choo, M. Park, J. Paik, and D. Won, "On the security of a simple three-party key exchange protocol without server's public keys," *The Scientific World Journal*, vol. 2014, Article ID 479534, 7 pages, 2014.