Cryptanalysis of A Mutual Authentication Scheme for Smart Healthcare Systems under Global Mobility Networks Notion

IOP Conf. Series: Materials Science and Engineering **569** (2019) 042038 doi:10.1088/1757-899X/569/4/042038

Cryptanalysis of A Mutual Authentication Scheme for Smart Healthcare Systems under Global Mobility Networks Notion

Shuying Yang[1*], Chengbo Xu[2]

[1]School of Data and Computer Science, Shandong Women's University, Jinan, Shandong, 250300, China

[2]School of Mathematical Sciences, University of Jinan, Jinan, Shandong, 250022, China

[*]Corresponding author's e-mail: cbqysy@163.com

Abstract. Authentication and key agreement scheme is an important mechanism for legal users to access the services of smart healthcare systems under global mobility networks notion. However, the design of authentication and key agreement schemes is still quite a challenging problem. In this paper, we analyse a novel mutual authentication scheme for smart healthcare systems under global mobility networks notion proposed by Wu et al. in 2018, and point out the scheme is vulnerable to malicious user impersonation attack, offline guessing attack and suffers from low efficiency.

1. Introduction

With the rapid development in telecommunication and information technology, smart health is expected to provide comprehensive and qualified healthcare service. However, since these systems involve various sensitive information, such as medical data and privacy records, it has become an indispensable task to safeguard the security and privacy of smart healthcare systems (Li et al., 2016). As yet, the design of user authentication and key agreement scheme for resource deficient mobile users has been substantially addressed by various researchers.

In 2004, Zhu and Ma [1] first proposed a two-factor user authentication with anonymity under wireless circumstance. However, Lee et al. [2] analysed Zhu and Ma's scheme [1] and pointed out that the scheme does not resist forgery attack and fail to achieve mutual authentication. In order to conquer these drawbacks, Lee et al. proposed an improved scheme [2]. In 2009, Chang et al. [3] found Lee et al.'s scheme [2] is also unable to provide the feature of anonymity and improved the scheme. Unfortunately, the improved scheme was found unable to resist user forgery attack and lack of forward security [4]. In 2011, Yoon et al. [5] proposed an anonymous authentication scheme for wireless communication using digital certificates. Later, the scheme was pointed out unable to provide fair key agreement and untraceability [6]. In 2013, Jiang et al.[7] designed a novel and anonymous user authentication scheme for global mobility networks. However, Wen et al. [8] pointed out the scheme is unable to resist stolen-verifier attack and replay attack. To remendy these drawbacks, Wen et al. proposed an improved scheme [8]. Later, Gope and Hwang [9] showed the improved scheme is still unsecure and vulnerable to offline guessing attack and forgery attack. In 2016, Gope and Hwang [10] analysed He et al.'s scheme [11] and found some weaknesses. Based on this, they proposed their own authentication scheme. Although the scheme is really efficient for GLOMONET environment, it is also unsecure due to vulnerability to denial-of-service (DoS) attack, lack of perfect forward secrecy of

session key etc.[12] Recently, Wu et al. [13] proposed a new mutual authentication scheme for smart healthcare systems under global mobility networks notion. In this paper, we analysed the scheme and found it is vulnerable to malicious user impersonation attack, offline guessing attack and suffers from low efficiency due to lack of wrong password detection mechanism.

The rest of this paper is organized as follows: in section 2, we briefly review Wu et al.'s scheme [13]. Section 3 points out the weaknesses of Jiang et al.'s scheme. Finally, we draw our conclusion in section 4.

The notations used throughout this paper are summarized in Table 1.

Table 1. Notations.

MU	Mobile User
FA	Foreign Agent
HA	Home Agent
ID_{MU}	MU's identity tag
PW_{MU}	MU's password
ID_{HA}	HA's identity tag
x	HA's secret key
ID_{FA}	FA's identity
SK_{MU}	The session key computed by MU
SK_{FA}	The session key computed by FA
K_{fh}	Secret key shared between FA and HA
l	Secure length for random numbers and hash results
$h(\cdot)$	One-way hash function
$\|$	Message concatenation operation
$\oplus$	X-or operation

2. Review of Wu et al.'s scheme

In this section, we briefly review the Wu et al.'s scheme [13]. Their scheme includes four phases: initialization phase, registration phase, mutual authentication and key agreement(MAKA) phase, password renewal phase, and involves three entities: mobile user (MU), home agent (HA) and foreign agent (FA).

2.1. Initialization phase

In this phase, FA chooses and sends ID_{FA} and a random number r_1 to HA through a secure channel. Then HA computes $K_{fh} = h(ID_{FA} \| r_1 \| x)$ and sends K_{fh} to FA also by a secure channel. FA stores $\{K_{fh}, r_1\}$. Besides, FA and HA shares these elliptic curve parameters: a finite field F_p where p is a large prime, an elliptic curve group G where P is a generator.

2.2. Registration phase

In this phase, the secure channel is also used, and there are three steps as follows:

Step 1: MU selects ID_{MU}, PW_{MU} and a random number r_0, calculates $HPW_{MU} = h(PW_{MU} \| r_0)$ and $PID_{MU} = h(ID_{MU} \| r_0)$, and sends $\{ID_{MU}, PID_{MU}, HPW_{MU}\}$ to HA.

Step 2: HA checks the validity of ID_{MU}. If so, ID_{MU} is stored in database. Then HA computes $D_1 = h(PID_{MU} \| x) \oplus HPW_{MU}$ and $D_2 = h(ID_{HA} \| ID_{MU} \| x) \oplus h(ID_{MU} \| HPW_{MU})$. Finally it stores $(D_1, D_2, PID_{MU}, ID_{HA}, h(\cdot))$ in a smart card and issues it to MU.

Step 3: MU computes $D_3 = r_0 \oplus h(ID_{MU} \| PW_{MU})$ and stores it into the smart card.

2.3. MAKA phase

Step 1: MU enters the smart card to the terminal and inputs (ID_{MU}, PW_{MU}). The card calculates $r_0 = D_3 \oplus h(ID_{MU} \| PW_{MU})$ and $HPW_{MU} = h(PW_{MU} \| r_0)$. Then it generates two random numbers $\mu \in Z_n^*$ and r_{MU}, and calculates $B_1 = D_1 \oplus HPW_{MU}$, $B_2 = D_2 \oplus h(ID_{MU} \| HPW_{MU})$, $C_1 = B_1 \oplus r_{MU}$, $Q_1 = \mu P$, $C_2 = ID_{MU} \oplus h(PID_{MU} \| r_{MU} \| Q_1)$, $PID_{MU}^{new} = h(ID_{MU} \| r_{MU})$ and $C_3 = h(ID_{MU} \| B_1 \| PID_{MU} \| Q_1 \| ID_{HA})$. Then the message $M_1 = \{PID_{MU}, C_1, C_2, C_3, ID_{HA}, Q_1\}$ is sent to FA.

Step 2: FA generates two nonces r_{FA} and $v \in Z_n^*$, calculates $Q_2 = vP$, $C_4 = h(K_{fh} \| Q_2) \oplus r_{FA}$, $C_5 = h(C_4 \| r_{FA} \| Q_2 \| ID_{FA} \| ID_{HA})$, and sends $M_2 = \{PID_{MU}, C_1, C_2, C_3, C_4, C_5, Q_1, Q_2, ID_{FA}, Q_1\}$ to HA.

Step 3: HA calculates $B_3 = h(PID_{MU} \| x)$, $r_{MU} = C_1 \oplus B_3$ and $ID_{MU} = C_2 \oplus h(PID_{MU} \| r_{MU} \| Q_1)$. Then it checks ID_{MU}. After that, HA computes $PID_{MU}^{new} = h(ID_{MU} \| r_{MU})$ and checks $C_3 = h(ID_{MU} \| B_3 \| PID_{MU}^{new} \| Q_1 \| ID_{HA})$. If the verification does not pass for three times in a short time span, U_i will be frozen. Otherwise, HA calculates $K_{fh} = h(ID_{FA} \| r_1 \| x)$ and $r_{FA} = C_4 \oplus h(K_{fh} \| Q_2)$ and checks $C_5 = h(C_4 \| r_{FA} \| Q_2 \| ID_{FA} \| ID_{HA})$. If wrong case happens, the session will be aborted. Otherwise, HA calculates $B_4 = h(PID_{MU}^{new} \| x)$, $K_{fh}^{new} = h(ID_{FA} \| r_{FA} \| x)$, $B_5 = h(ID_{HA} \| ID_{MU} \| x)$, $C_6 = h(B_3 \| B_5 \| r_{MU} \| Q_1 \| Q_2) \oplus B_4$, $C_7 = h(B_3 \| B_4 \| C_6)$, $C_8 = h(K_{fh} \| r_{FA} \| Q_2) \oplus K_{fh}^{new}$ and $C_9 = h(K_{fh} \| r_{FA} \| Q_2 \| K_{fh}^{new})$. Finally, HA sends $M_3 = \{C_6, C_7, C_8, C_9\}$ to FA.

Step 4: FA calculates $K_{fh}^{new} = C_8 \oplus h(K_{fh} \| r_{FA} \| Q_2)$ and checks $C_9 = h(K_{fh} \| r_{FA} \| Q_2 \| K_{fh}^{new})$. If so, it computes $SK_{FA} = h(Q_1 \| Q_2 \| vQ_1)$ and $C_{10} = h(SK_{FA} \| C_6 \| C_7)$. Then it sends $M_4 = \{C_6, C_7, C_{10}, Q_2\}$ to MU and updates (K_{fh}, r_1) with (K_{fh2}, r_{FA}).

Step 5: When receiving M_4, the smart card continues to compute $B_6 = C_6 \oplus h(B_1 \| B_2 \| r_{MU} \| Q_1 \| Q_2)$ and checks $C_7 = h(B_1 \| B_6 \| C_6)$. If so, the smart card computes $SK_{MU} = h(Q_1 \| Q_2 \| \mu Q_2)$, and checks $C_{10} = h(SK_{MU} \| C_6 \| C_7)$. If it is correct, the smart card calculates $D_1^{new} = B_6 \oplus HPW_{MU}$ and $D_3^{new} = r_{MU} \oplus h(ID_{MU} \| PW_{MU})$. Finally, the card replaces (PID_{MU}, D_1, D_3) with $(PID_{MU}^{new}, D_1^{new}, D_3^{new})$.

3. Weaknesses of Wu et al.'s scheme

In this section, we will show that Wu et al.'s scheme [13] is vulnerable to malicious user impersonation attack and node capture attack and suffer from forward security problem, low efficiency problem. To illustrate logically, we firstly give the following three assumptions about attacker's capability.

Assumption 1. Attacker fully controls the public communication channels between the user and the server. Hence, the attacker can intercept, eavesdrop, insert and replay all the authentic messages from or into related channels freely.

Assumption 2. Now, there are several effective methods by which an attacker can extract the values stored in smart cards, such as Kocher et al. [14] and Messerges et al. [15]. Therefore, we assume the attacker is allowed to either compromise user's smart card or to compromise user's password, but not both.

Assumption 3. The attacker is able to offline guess the user's password PW since the password is generally selected freely by user himself/herself and hence with low entropy. However, the attacker cannot guess the password and the user's fingerprint information simultaneously in real polynomial time.

3.1. Malicious user impersonation attack

Malicious user impersonation attack means that a malicious registered user can impersonate as other registered users to login the system, and access the sensed data under the name of other legitimate users. In this subsection, only assumption 1 is assumed. Suppose that an attacker A has eavesdropped message $M_1 = \{PID_{MU}, C_1, C_2, C_3, ID_{HA}, Q_1\}$, the attacker can launch an attack as follows:

Step 1: The attacker A registers with the information PID_{MU}. Specificially, A selects ID_A, HPW_A and sends message $\{\mathrm{ID}_A, \mathrm{PID}_{MU}, \mathrm{HPW}_A\}$ to HA.

Step 2: When HA receiving the message, it will checks the format of ID_A, and computes $D_1 = h(PID_{MU} \| x) \oplus HPW_A$ and $D_2 = h(ID_{HA} \| ID_A \| x) \oplus h(ID_A \| HPW_{MU})$. Then it stores $(D_1, D_2, PID_{MU}, ID_{HA}, h(\cdot))$ in a smart card and issues it to attacker A.

Step 3: The attacker A extracts information D_1 from his/her smart card. Then A computes $B_1 = D_1 \oplus HPW_{MU}^* = h(PID_{MU} \| x)$.

Step 4: The attacker calculates $r_{MU} = C_1 \oplus B_1$ where C_1 is from the eavesdropped message M_1.

Step 5: The attacker A restores the identity of user $ID_{MU} = C_2 \oplus h(PID_{MU} \| r_{MU} \| Q_1)$.

Step 6: Since ID_{MU} and r_{MU} are both known, the attacker A can calculates $PID_{MU}^{new} = h(ID_{MU} \| r_{MU})$.

Step 7: A generates a new μ^*, and computes $Q_1^* = \mu^* P$.

Step 8: A computes $C_2^* = ID_{MU} \oplus h(PID_{MU} \| r_{MU} \| Q_1^*)$.

Step 9: A *computes* $C_3^* = h(ID_{MU} \| B_1 \| PID_{MU}^{new} \| Q_1^* \| ID_{HA})$.

Step 10: The attacker A forges a valid login message $M_1^* = \{PID_{MU}, C_1, C_2^*, C_3^*, ID_{HA}, Q_1^*\}$.

Step 11: After receiving M_1^*, FA generates nonces r_1, r_{FA}, $v \in Z_n^*$, calculates $Q_2^* = vP$, $C_4 = h(K_{fh} \| Q_2^*) \oplus r_{FA}$ and $C_5 = h(C_4 \| r_{FA} \| Q_2^* \| ID_{FA} \| ID_{HA})$, then sends to HA the message $M_2^* = \{PID_{MU}, C_1, C_2^*, C_3^*, C_4, C_5, Q_1^*, Q_2^*, ID_{FA}, r_1\}$.

Step 12: Since the items in message M_2^* are consistent as to Wu et al.'s scheme, HA naturally accepts the message without realizing existence of the attacker A. Furthermore, HA will calculate those related values and construct the message $M_3^* = \{C_6^*, C_7^*, C_8^*, C_9^*\}$ which is transmitted to FA.

Step 13: When receiving $M_3^* = \{C_6^*, C_7^*, C_8^*, C_9^*\}$, FA firstly computes $K_{fh}^{new} = C_8^* \oplus h(K_{fh} \| r_{FA} \| Q_2^*)$, verifies $C_9^* = h(K_{fh} \| r_{FA} \| Q_2^* \| K_{fh}^{new})$ which is potentially valid, and then calculates $SK_{FA} = h(Q_1^* \| Q_2^* \| vQ_1^*)$ and $C_{10}^* = h(SK_{FA} \| C_6^* \| C_7^*)$. Finally, FA updates K_{fh} to K_{fh}^{new} and sends message $M_4^* = (C_6^*, C_7^*, C_{10}^*, Q_2^*)$ to the attacker A.

Step 14: Upon obtaining the message $M_4^* = (C_6^*, C_7^*, C_{10}^*, Q_2^*)$, the attacker A computes the agreed session key $SK_{MU}^* = h(Q_1^* \| Q_2^* \| \mu^* Q_2^*)$. Then A can impersonate the user MU to do what he/she wants to do.

3.2. Offline guessing attack 1

Suppose the user MU's smart card is lost or stolen, an attacker obtains it. According to assumption 2, he/she has the capability to extract the information $\{D_1, D_2, D_3, PID_{MU}, ID_{HA}\}$ stored in smart card. Once knowing these values, the attacker can launch an offline guessing password attack as follows:

Step 1: The attacker A guesses a password PW_{MU}^* and a identity tag ID_{MU}^*.

Step 2: Attacker A computes $r_0^* = D_3 \oplus h(ID_{MU}^* \| PW^*)$ where D_3 is a value extracted from smart card.

Step 3: Attacker A checks whether the equality $PID_{MU} = h(ID_{MU}^* \| r_0^*)$ is correct or not. If it is correct, the attacker succeeds in conducting this attack, and PW_{MU}^* and ID_{MU}^* are the correct password and identity tag respectively. Otherwise, attacker A has to go to step 1 and guess new password and identity tag, then conduct step 2.

3.3. Offline Guessing attack 2

Another approach to guessing password and identity tag will use the values $\{C_1, C_2, C_3\}$, which are from a veritable login request message $M_1 = \{PID_{MU}, C_1, C_2, C_3, ID_{HA}, Q_1\}$. The steps are as follows:

Step 1: The attacker A guesses a password PW_{MU}^{*} and a identity tag ID_{MU}^{*}.

Step 2: Attacker A computes $r_0^{*} = D_3 \oplus h(ID_{MU}^{*} \| PW^{*})$ where D_3 is a value extracted from smart card.

Step 3: Attacker A calculates $HPW_{MU}^{*} = h(PW_{MU}^{*} \| r_0^{*})$.

Step 4: Attacker A calculates $B_1^{*} = D_1 \oplus HPW_{MU}^{*}$, where D_1 is a value extracted from smart card.

Step 5: Attacker A computes $r_{MU}^{*} = C_1 \oplus B_1^{*}$, where C_1 is a value extracted from the eavesdropped message M_1.

Step 6: Attacker A checks whether the equality $C_2 = ID_{MU}^{*} \oplus h(PID_{MU} \| r_{MU}^{*} \| Q_1)$ is correct or not. If it is correct, the attacker succeeds in conducting this attack, and PW_{MU}^{*} and ID_{MU}^{*} are the correct password and identity tag respectively. Otherwise, attacker A has to go to step 1 and guess new password and identity tag, then conduct step 2-6.

3.4. Low efficiency in wrong password detection

In Wu et el.'s scheme, no login detection mechanism. If a legal user MU inputs a wrong password by mistake, this wrong password will not be detected until the remote home agent HA verifies whether C_3 and $h(ID_{MU} \| B_3 \| PID_{MU}^{new} \| Q_1 \| ID_{HA})$ are equal in step 3 of the login and authentication phase. Therefore, Wu et al.'s scheme is low efficient to detect the user's wrong password.

4. Conclusions

In this paper, we analysed a mutual authentication scheme for smart healthcare systems under global mobility networks notion proposed by Wu et al. in 2018, and point out the scheme vulnerable to malicious user impersonation attack, offline guessing attack and suffers from low efficiency due to lack of wrong password detection mechanism.

Acknowledgments

This work was partially supported by the Youth Fund of Shandong Women's University (Granted No. 2014ZDX15) and the Doctoral Fund of University of Jinan (Granted No. XBS1455).

References

[1] Zhu J., Ma J. (2004) A new authentication scheme with anonymity for wireless environments. IEEE Trans. Consum. Electron, 50: 231-235.
[2] Lee C. C., Hwang M. S., Liao I. E. (2006) Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Trans. Ind. Electron, 53: 1683-1687.
[3] Chang C. C., Lee C. Y., Chiu Y. C. (2009) Enhanced authentication scheme with anonymity for roaming service in global mobility networks. Comput. Commun., 32: 611-618.
[4] Youn T. Y., Park Y. H., Lim J. (2009) Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks. IEEE Commun. Lett., 13: 471-473.
[5] Yoon E. J., Yoo K. Y., Ha K. S. (2011) A user friendly authentication scheme with anonymity for wireless communications. Comput. Electr. Eng., 37: 356-364.
[6] Niu J., Li X. (2014) A novel user authentication scheme with anonymity for wireless communications. Secur. Commun. Netw., 7: 1467-1476.
[7] Jiang Q., Ma J., Li G., Yang L. (2013) An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. Wirel. Pers. Commun., 68: 1477-1491.
[8] Wen F., Susilo W., Yang G. (2013) A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. Wirel. Pers. Commun., 73: 993-1004.
[9] Gope P., Hwang T. (2015) Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks. Wirel. Pers. Commun., 82: 2231-2245.

[10] Gope P., Hwang T. (2016) An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. Journal of Netw. Comput. Appl., 62: 1-8.
[11] He D., Zhang Y., Chen J. (2014) Cryptanalysis and improvement of an anonymous authentication protocol for wireless access networks. Wirel. Pers. Commun., 74: 229-243.
[12] Li X., Niu J. W., et al. (2018) A robust biometrics based three-factor authentication scheme for global mobility networks in smart city. Future Generation Computer Systems, 83, 607-618.
[13] Wu F., Li X., et al. (2018) A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion. Computers and Electrical Engineering, 68: 107-118.
[14] Kocher P., Jaffe J., Jun B. (1999) Differential power analysis. Advances in cryptology-CRYPT'99, pp. 388-397.
[15] Messerges T. S., Dabbish E. A., Sloan R. H. (2002) Examining smart-card security under the threat of power analysis attacks. IEEE Trans. Comput., 51: 541-552.