Enhancement of "Secure user authentication scheme for wireless healthcare sensor networks"

Jung-San Lee [1*], Ya-Han Kang [2]

[1, 2] Department of Information Engineering and Computer Science,

Feng Chia University,

Taichung 407, Taiwan, ROC

[1] leejs@fcu.edu.tw

Abstract

Liu and Chung have proposed a secure user authentication mechanism for wireless healthcare sensor networks for granting legal participants access to the patient data, including blood pressure, heart rate, and body temperature in 2016[Computers and Electrical Engineering]. Nevertheless, we have found two obvious security problems in the login and access stages. Aside from pointing out the weakness, we have provided proper suggestions for repairing the problem.

Keywords: Wireless sensor network, healthcare, secure data transmission, replay attack

1. Introduction

Establishing a tele-care system is an emergent and important issue for our daily lives. In 2016, Liu and Chung have proposed a brand-new medical healthcare mechanism for achieving user authentication in a wireless sensor network. For simplicity, we have the abbreviation of this secure authentication method as SAW[4]. The main contribution of this work is to grant doctors or family members the access to the patient data, including blood pressure, heart rate, and body temperature. The system architecture of their mechanism is depicted in Figure 1. Each patient is equipped with sensors for data collection. TA (trust authority) is responsible for generating secret key and issuing smart card. Legal participants have to register at TA before access the healthcare information. After a successful login to the system, participants can learn data from sensors within a valid period.

* Corresponding author: Jung-San Lee, leejs@fcu.edu.tw

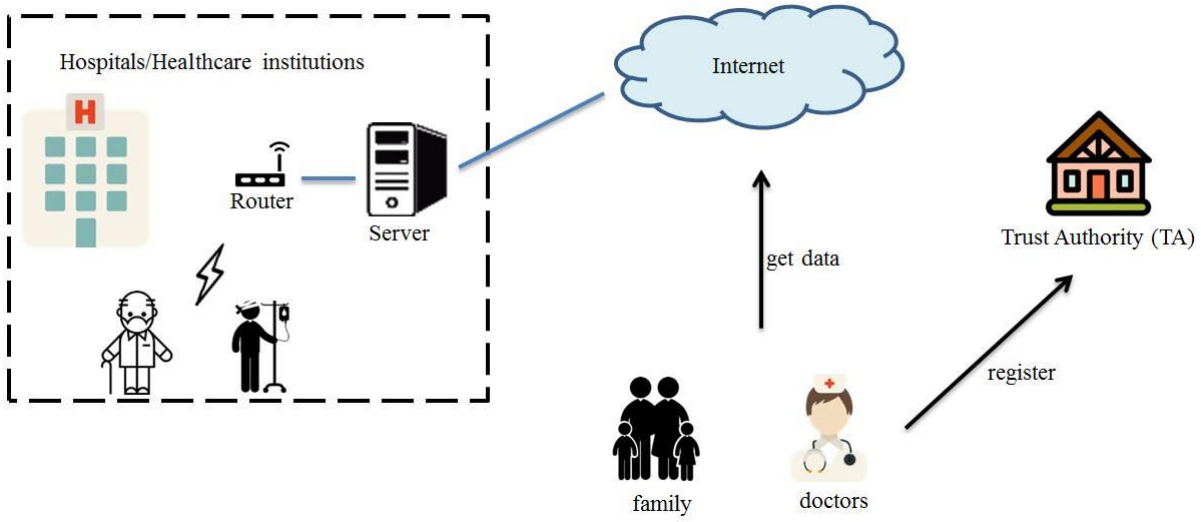

Figure 1: System architecture

Unfortunately, we have found that this method exist two security drawbacks. The first one is that it may suffer from the replay attack as the timestamp is out of protection. It is easy for attacker to replace a current timestamp and replay the login request. The second one is the risk from stolen smart card attack. As introduced in [1, 2, 3], we shall prove the security of the authentication scheme even under the assumption that the smart card has been stolen. If an attacker could steal the smart card and retrieve useful information for further impersonation, it is concluded that the method cannot resist the stolen smart card attack. Since the secret information kept in the smart card is without protection, SAW cannot resist this attack. Also, we have provided appropriate suggestions on SAW for preventing these two attacks.

The rest of this article is organized as follows. The review and security examination of SAW is introduced in Section 2, followed by the suggestions for repairing the drawbacks. Finally, we make conclusions in Section 3.

2. Review and security analysis of SAW

2.1 Review of SAW

The authentication architecture of SAW consists of four phases, including setup phase, registration phase, login and verification phase, access control and encryption phase. Notations

used in SAW are defined in Table 1.

Table 1: Natation used in SAW

Notation	Definition
i	A user
TA	The trust authority
S	A sensor
G_1 / G_2	A cyclic multiplicative group G_1 and a cyclic additive group G_2
P	The generator of G_1
P_{pub}	The public parameter
ID_i / PW_i	Identification/Password of user i
U_{pub} /U_{priv}	The public/private key of the user
$h(.)$	One-way hash function
a /b/s	Random numbers
T_1 /T_2/T_3	Timestamp
m	The data

Setup phase

Step 1: TA chooses a bilinear map $\hat{e}$ and a point P of group G_1.

$$\hat{e}: G_1 \times G_1 \to G_2$$

Step 2: TA generates two one-way hash functions h_1, h_2.

$$h_1: \{0,1\}^* \to G_2$$
$$h_2: G_2 \to \{0,1\}^*$$

Step 3: TA chooses a random number s and computes $P_{pub} = s \times P$.

Registration phase

Once a user *i* wants to join the system, he has to move to the healthcare institution personally for registration.

Step 1: User i sends ID_i and PW_i to TA through a secure channel.

Step 2: TA generates a public key U_{pub} and computes the corresponding private key U_{priv} for *i*

$$U_{priv} = s \times U_{pub}$$

Step 3: TA issues the smart card $< h(.), U_{priv}, ID_i, PW_i, a >$ to user i.

Login and verification phase

After the registration, user *i* can request to login the system as follows. The flowchart of this phase is illustrated in Figure 2.

Step 1: User i inserts the smart card into a card reader and enters the ID_i and PW_i.

Step 2: Smart card checks the correctness of ID_i and PW_i entered by the user i.

Step 3: Smart card computes Sig as,

$$r = h(ID_i \| PW_i \| a),$$
$$Sig = r \times U_{priv}$$

Step 4: Smart card generates T_1 and transmits $\{Sig, r, T_1, ID_i\}$ to the TA.

Step 5: Upon receiving the login request, TA checks the user i's legality.

$$\hat{e}(P, Sig) = \hat{e}(P_{pub}, r \times U_{pub})$$

Step 6: TA checks the freshness of T_1. If it is valid, TA generates *b* and computes

$$E = h(b \oplus U_{pub})$$

Step 7: TA transmits E to user i and broadcasts $\{T_2, b, ID_i\}$ to all the sensors, where T_2 is the valid period for *i* to query data from sensors.

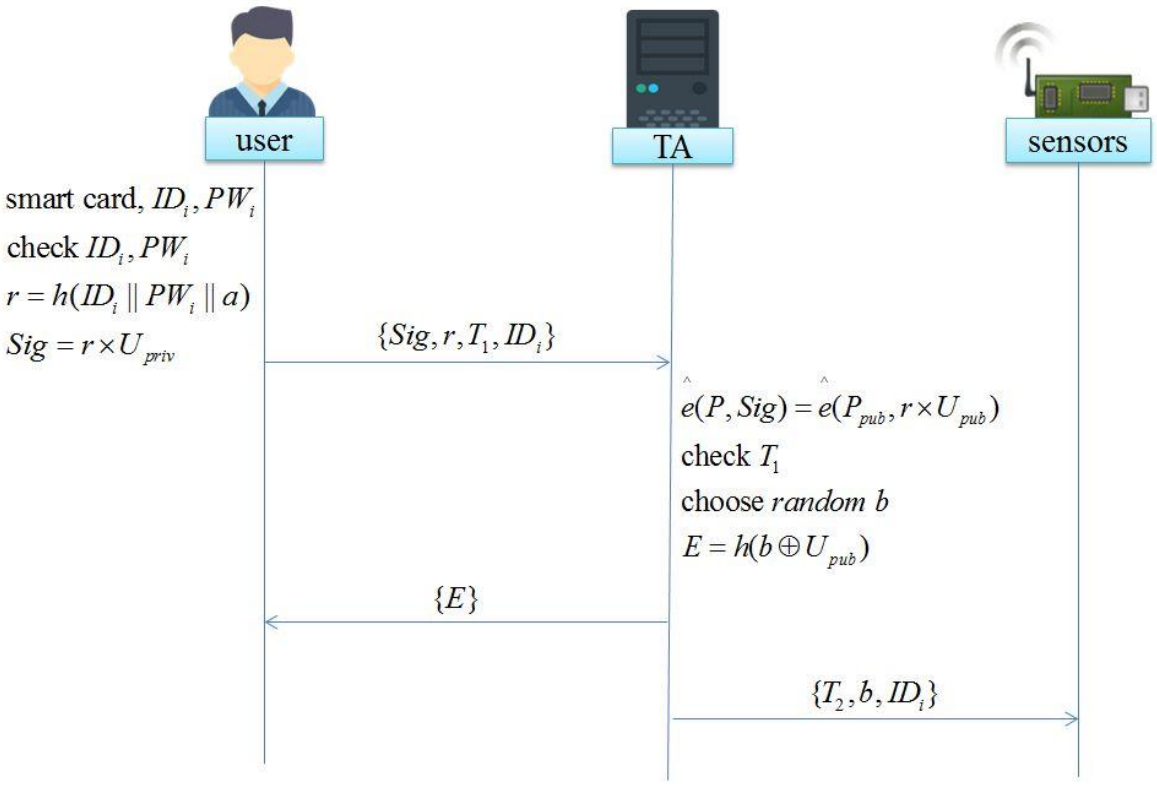

Figure 2: Login and verification phase

Access control and encryption phase

After finishing login and verification phase, the user *i* can request data from the sensor. The flowchart of this phase is shown in Figure 3.

Step 1: User i enters the ID_i and PW_i into smart card.

Step 2: Smart card checks the correctness of ID_i and PW_i entered by the user i. If they are valid, it computes $C = h(a \| ID_i) \oplus E$ and sends $\{C, ID_i, T_3\}$ to the sensor S, where T_3 is a timestamp.

Step 3: S checks the freshness of T_3 according to T_2. In case that it is valid, S computes and compares C' with the received *C*.

$$C' = h(a \| ID_i) \oplus h(b \oplus U_{pub})$$

Step 4: If they are the same, S prepares the data *m*, encapsulates it as M, and sends it to i.

$$M = m \oplus h_2(\hat{e}(U_{pub}, P_{pub}))$$

Step 5: User *i* applies U_{priv}, M and public information W to retrieve the data m as,

$$m = M \oplus h_2(\hat{e}(U_{priv}, W))$$

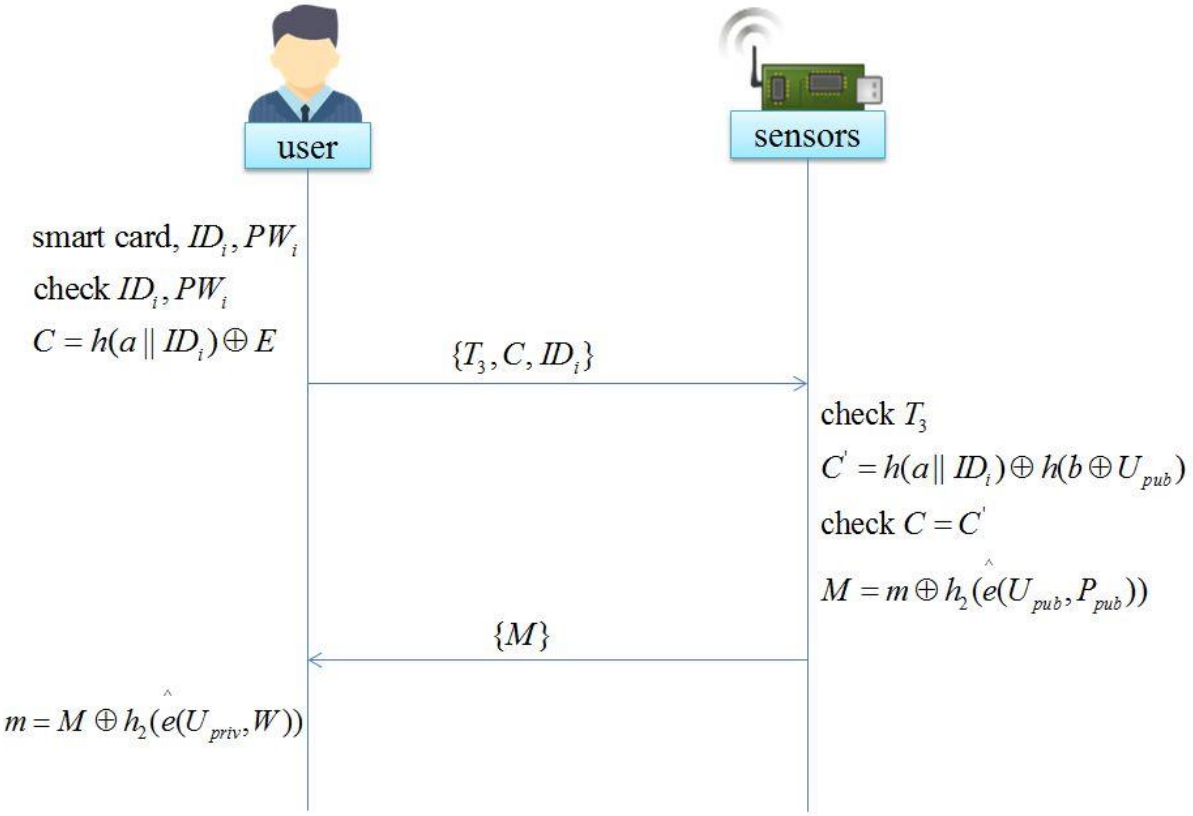

Figure 3: Access control and encryption phase

2.2 Security analysis of SAW

Here we mount two common attacks on SAW and propose corresponding suggestions to repair the weaknesses.

Replay attack:

In the login and verification phase, an attacker Eve could easily intercept the message $\{Sig, r, T_1, ID_i\}$ from the communication. Eve then generates a current timestamp T_e and replaces T_1 with T_e. After that, she can send $\{Sig, r, T_e, ID_i\}$ to TA for verification. According to the procedure mentioned above, this replayed request must be able to pass the validity checking $\hat{e}(P, Sig) = \hat{e}(P_{pub}, r \times U_{pub})$ as $Sig, r,$ and ID_i are the real ones generated by user i. Hereafter, TA checks the freshness of T_e. No doubt that T_e is fresh as it is a current one. Thus, Eve could successfully mount the replay attack on SAW.

Suggestion:

Actually, the sticking point is that the timestamp is not included in the verification token,

such as *r*. So, we suggest that $r = h(ID_i \| PW_i \| a)$ should be changed to $r = h(ID_i \| PW_i \| a \| T_1)$. Since no one could compromise the security of one-way hash function to replace the timestamp, the replay attack can be prevented in SAW.

Stolen smart card attack:

In case that an attacker Eve could steal the smart card and retrieve useful information for further impersonation, it is concluded that the method cannot resist the stolen smart card attack. As described in the registration phase of SAW, the smart card contains $< h(.), U_{priv}, ID_i, PW_i, a >$. It is obviously that Eve could extract secret information, including U_{priv}, from the smart card to impersonate user *i* to login the system once she could steal the smart card.

Suggestion:

The original verification procedure is to check if the input identity and password are the same as those recorded in the smart card. In particular, U_{priv} is without protection. Thus, we suggest that the secret information kept in the smart card should be $< h(.), U_{priv} \oplus h(PW_i), ID_i, a >$. Only the legal user with correct password can retrieve U_{priv} for further authentication.

3. Conclusions

In this article, we have examined the security of SAW which is designed for granting legal medical access to patient information. It has been demonstrated that SAW is incapable of resisting the replay and stolen smart card attacks. Also, we have proposed suggestions for repairing SAW so that it could get rid of those two weaknesses.

References

[1] C. Benzaid, K. Lounis, A. Al-Nemrat, N. Badache, and M. Alazab, "Fast authentication in wireless sensor networks," *Future Generation Computer Systems*, Vol. 55, pp. 362-375, February 2016.

[2] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, Vol.

36, pp. 152-176, January 2016.

[3] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Generation Computer Systems*, In Press, available online 6 May 2016.

[4] C. H. Liu and Y. F. Chung, "Secure user authentication scheme for wireless healthcare Sensor networks," *Computers and Electrical Engineering*, doi:10.1016/j.compeleceng.2016.01.002, 2016.