Improved on an efficient user authentication scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment

Yalin Chen[1] and Jue-Sam Chou*[2] and Hung - Sheng Wu[3]

[1] Institute of information systems and applications, National Tsing Hua University

Yalin78900@gmail.com

[2] Department of Information Management, Nanhua University, Taiwan
*: corresponding author: jschou@mail.nhu.edu.tw
Tel: 886+ (0)5+272-1001 ext.56536

[3] Department of Information Management, Nanhua University, Taiwan

potui3805@gmail.com

Abstract

Recently, Farasha et al. proposed an efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. By using BAN-logic and AVISPA tools, they confirm the security properties of the proposed scheme. However, after analyzing, we determine that the scheme could not resist the smart card loss password guessing attack, which is one of the ten basic requirements in a secure identity authentication using smart card, assisted by Liao et al. Therefore, we modify the method to include the desired security functionality, which is significantly important in a user authentication system using smart card.

Keywords: user authentication, key agreement, cryptanalysis, smart card, password change

1. Introduction

There have been many cryptographic scientists working within the field of authentication using smart card system design [1-13]. A heterogeneous wireless sensor networks typically contain three roles: user, sensor node, and the gateway node (GWN); and three protocols: registration, login and authentication, and password change. In the protocol design principle, the user's identity should not be revealed to ensure his login privacy. In 2016, Farasha et al. [11] pointed out that have found that Turkanovic et al.'s scheme [6] has some security shortcomings and is susceptible to some cryptographic attacks. They overcome the security weaknesses of Turkanovic et

al.'s scheme, by proposing a new and improved user authentication and key agreement scheme (UAKAS). The proposed scheme enables the same functionality, but improves the security level and enables the heterogeneous wireless sensor networks (HWSN) to dynamically grow without influencing any party involved in the UAKAS. They claimed that the results of the security analysis by BAN-logic and AVISPA tools confirm the security properties of the proposed scheme. However, upon closer examination, we discovered that it does not support the security requirement of smart card loss password guessing attack. To enhance its security, we modified their scheme to include this feature. We will demonstrate the enhancement in this article.

2. Review of Farasha et al.'s scheme

Farasha et al.'s heterogeneous wireless sensor network is based on Turkanovic et al.'s scheme [6]. It consists of three roles: user, sensor node, and the gateway node (GWN); and some phases: pre-deployment, registration, login, authentication, password change and dynamic node addition phase. They claimed that their scheme not only tackles and eliminates all security shortcomings and vulnerabilities of Turkanovic et al.'s scheme, but also introduces some enhancement, which enables the WSN dynamical limitless growth, and makes the functionality and efficiency at the same level as the scheme of Turkanovic et al.s'. In this article, we only review the registration phase, and login and authentication phase to illustrate its weaknesses. As for the definitions of the used notations, please refer to the original article.

2.1 Registration Phase

This phase is divided into two parts, the user registration phase and sensor node registration phase. We describe both of them below.

(a). The user registration phase

The user U_i chooses its username ID_i, password PW_i, and selects a random nonce r_i. He then computes $MP_i = h(r_i \| PW_i)$ and sends $\{MP_i, ID_i\}$ to the GWN over a secure channel. After receiving the registration message from U_i, GWN computes the value $e_i = h(MP_i \| ID_i)$. Using U_i's secret data combined with its secret master key X_{GWN}, the GWN then computes $d_i = h(ID_i \| X_{GWN})$ and $g_i = h(X_{GWN}) \oplus h(MP_i \| d_i)$. After this, GWN then computes $f_i = d_i \oplus h(MP_i \| e_i)$. Finally, it stores $\{e_i, f_i, g_i\}$ to the smart card SC and presents it to the U_i. After receiving the SC, U_i inserts the previously selected r_i into it, and terminates the registration phase.

(b). The sensor node registration phase

A specific sensor node Sj has to register with a message $\{SID_j, MP_j, MN_j, T1\}$ to the GWN over the insecure channel. This is done by Sj first randomly selecting a nonce rj and computing the values $MP_j = h(X_{GWN-Sj} \| r_j \| SID_j \| T_1)$ and $MN_j = r_j \oplus X_{GWN-Sj}$. After receiving the registration message from the S_j, GWN checks whether $|T_1 - T_c| < \triangle T$ holds, if the verification holds, the GWN then computes random nonce $r_j = MN_j \oplus X_{GWN-Sj}$. Then, GWN can compute $MP_j' = h(X_{GWN-S\,j} \| r_j \| SID_j \| T_1)$ and check if it is equal to the received MP_j . If it holds, GWN computes the values $x_j = h(SID_j \| X_{GWN})$, $e_j = x_j \oplus X_{GWN-Sj}$, $d_j = h(X_{GWN} \| 1) \oplus h(X_{GWN-S\,j} \| T_2)$ and $f_j = h(x_j \| d_j \| X_{GWN-S\,j} \| T_2)$. The GWN then sends S_j the following message $\{e_j, f_j, d_j, T_2\}$. S_j checks whether $|T_2 - T_c| < \triangle T$. If the verification holds, GWN computes value $x_j = e_j \oplus X_{GWN-S\,j}$ and $f_j' = h(x_j \| d_j \| X_{GWN-S\,j} \| T_2)$. He then compares the values of both f_j' and the received f_j. If they are equal, GWN computes $h(X_{GWN} \| 1) = d_j \oplus h(X_{GWN-S\,j} \| T_2)$ and stores both the $h(X_{GWN} \| 1)$ and x_j to its memory. Finally, S_j deletes X_{GWN-Sj} and sends a confirmation message to the GWN, whereby it also deletes X_{GWN-Sj} and SID_j from its memory.

.

2.2 Login and authentication phase

This phase is to enable a user to negotiate a session key with a specific sensor node without contacting the GWN. The session key will be used for secure communication between the user and the sensor node.

(a). Login phase

U_i inserts his SC into a card reader and inputs its username ID_i and password PW_i. The SC then verifies the owner of the SC with the secret data stored in it. First, the SC computes $MP_i = h(r_i \| PW_i)$ using PW_i and the stored r_i. SC then computes the value $e_i' = h(MP_i \| ID_i)$ and compares it with the stored one to see if e_i' equals e_i. If it holds, SC acknowledges the legitimacy of the U_i.

(b). Authentication phase

SC first computes $d_i = f_i \oplus h(MP_i \| e_i)$ using the stored values f_i and e_i, and MP_i. Second, the SC computes $h(X_{GWN}) = g_i \oplus h(MP_i \| d_i)$ using the stored g_i and the computed d_i and MP_i. The SC then computes the value $M_1 = ID_i \oplus h(h(X_{GWN}) \| T_1)$, where T_1 is the current timestamp. Second, the SC randomly chooses a secret nonce K_i to compute $M_2 = K_i \oplus h(d_i \| T_1)$. Finally, the SC computes $M_3 = h(M_1 \| M_2 \| K_i \| T_1)$ and sends the authentication message $\{M_1, M_2, M_3, T_1\}$ to the sensor node S_j via an insecure channel. After receiving the message from the U_i, S_j first checks to see whether $(|T1 - Tc| < \triangle T)$ holds. If it holds, S_j computes $ESID_j = SID_i \oplus h(h(X_{GWN}$

$\| 1) \| T_2$) and then randomly chooses a nonce K_j to compute the value $M_4 = h(x_j \| T_1 \| T_2) \oplus K_j$, where x_j is the stored value, T_1 is U_i's initial timestamp and T_2 S_j's current timestamp. S_j then uses value M_4, its identity SID_j, K_j, and the timestamps to compute $M_5 = h(SID_j \| M_4 \| T_1 \| T_2 \| K_j)$. S_j then sends message $\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}$ to the GWN.

After receiving the message from S_j, GWN first checks for a replay attack. If it does not happen, the GWN first computes S_j's identity $SID_j = ESID_i \oplus h(h(X_{GWN} \| 1) \| T_2)$ using $ESID_i$ and T_2 both received in the message, alongside with its own secret master key X_{GWN}. After that, GWN computes the values $x_j = h(SID_j \| X_{GWN})$ and $K_j = M_4 \oplus h(x_j \| T_1 \| T_2)$ using the received values M_4, T_1 and T_2, and verifies the legitimacy of the S_j by computing $M_5 = h(SID_j \| M_4 \| T_1 \| T_2 \| K_j)$. He then compares whether the equation equals the received one $M_5 =? M_5$. If S_j is authentic, GWN computes $ID_i = M_1 \oplus h(h(X_{GWN}) \| T_1)$ and $d_i = h(ID_i \| X_{GWN})$. After this, GWN computes $K_i = M_2 \oplus h(d_i \| T_1)$ and checks whether the received M_3 is equal to $h(M_1 \| M_2 \| K_i \| T_1)$. The GWN then compares the computed version with one $M_3 =? M_3$. If the equation holds, GWN acknowledges the legitimacy of U_i. The GWN then prepares four auxiliary values M_6, M_7, M_8 and M_9 by computing $M_6 = K_j \oplus h(d_i \| T_3)$, $M_7 = K_i \oplus h(x_j \| T_3)$, $M_8 = h(M_6 \| d_i \| T_3)$, and $M_9 = h(M_7 \| x_j \| T_3)$, respectively. And finally sends it to the S_j. If S_j receives the confirmation message from GWN, it confirms that U_i is legitimate. S_j then checks for any replay attack. If it does not happen, S_j then checks the legitimacy of the received message by calculating $M_9 = h(M_7 \| x_j \| T_3)$ and then compares it with the received one. If the verification holds, the S_j computes $K_i = M_7 \oplus h(x_j \| T_3)$ and constructs the session key $SK = h(K_i \oplus K_j)$. Finally, the S_j computes $M_{10} = h(SK \| M_6 \| M_8 \| T_3 \| T_4)$ and sends $\{M_6, M_8, M_{10}, T_3, T_4\}$ to U_i. U_i also checks for any replay attacks and verifies the legitimacy of the received message to avoid any GWN or S_j impersonation attacks. If a replay attack is ruled out, the U_i computes the value $M_8 = h(M_6 \| d_i \| T_3)$ and compares it to the received one. If they are equal, it represents that U_i successfully verifies GWN. After successfully authenticating GWN, U_i calculates $K_j = M_6 \oplus h(d_i \| T_3)$ and $SK = h(K_i \oplus K_j)$. And finally verifies the legitimacy of the SK by comparing whether the received M_{10} is equal to $h(SK \| M_6 \| M_8 \| T_3 \| T_4)$. If the verification holds, the U_i authenticated the S_j.

3. Weakness of this scheme

Due to the parameters f_i, e_i, g_i ,r_i stored in the smart card and the user himself can compute the value MP_i, an insider attacker can compute his own $d_i = f_i \oplus h(MP_i \| e_i)$ and $h(X_{GWN}) = g_i \oplus h(MP_i \| d_i)$. That is, each user can know the value $h(X_{GWN})$. Under this situation, we can see that their scheme suffers from (1). The smart

card loss password guessing attack, and (2). Anonymity breach.

(1). The smart card loss password guessing attack

If a user loses his smart card obtained by an insider attacker, the insider can launch a smart card loss password guessing attack as follows.

The insider first calculates $A=g_i' \oplus h(X_{GWN})$ and guesses the lost card owner's password pw_i'. He then computes $MP_i'=h(ri' \| PW_i')$, $di'= fi' \oplus h(MPi' \| ei')$, and $h(MP_i' \| di')$, where ri', g_i', fi', ei' are the parameters stored in the lost smart card. That is, if the attacker guesses the right password pw_i', he will obtain the user's di', then the computed value $h(MP_i' \| di')$ will definitely equals to A. Therefore, the attack succeeds.

(2). Anonymity breach

Due to the two equations, $M_1 = ID_i \oplus h(h(X_{GWN}) \| T_1)$ and $ESID_j = SID_i \oplus h(h(X_{GWN} \| 1) \| T_2)$, and both of the transmitted messages transferred in the login and authentication phase, $\{M_1, M_2, M_3, T_1\}$ from U_i to S_j and $\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}$ from S_j to GWN, where T_1, T_2 are the current timestamps, an insider user can compute $ID_i= M_1 \oplus h(h(X_{GWN}) \| T_1)$ from the calculated $h(X_{GWN})$ and an insider sensor node can compute $SID_i = ESID_j \oplus h(h(X_{GWN} \| 1) \| T_2)$ from the stored $h(X_{GWN} \| 1)$, respectively. Thus, their scheme does not possess the anonymous property.

4. Modification

From the weaknesses found in Section 3, we note that the key point is the insider can obtain the GWN's secret $h(X_{GWN})$. To further disguise it, we modify the messages in the registration phase and the login and authentication phase as follows.

(1). For user i

Modify user i's stored value $g_i = h(h(X_{GWN}) \oplus h(e_i \oplus ID_i \oplus d_i)) \oplus h(MP_i \| d_i)$. Hence, $h(h(X_{GWN}) \oplus h(e_i \oplus ID_i \oplus d_i)) = g_i \oplus h(MP_i \| d_i)$ in the login and authentication phase of the user side. Let $= h(e_i \oplus ID_i \oplus d_i)$. Then, the user computes $M1 = ID_i \oplus h((g_i \oplus h(MP_i \| d_i)) \| T_1) = ID_i \oplus h(h(h(X_{GWN}) \oplus M_{12}) \| T1)$ and transfers the authentication message $\{M_1, M_2, M_3, M_{12}, T_1\}$ to the sensor node S_j.

(2). For the sensor node Sj

In the registration phase, S_j stores $x_j=h(SID_j \oplus X_{GWN} \oplus y_j)$, $y_j=h(X_{GWN} \oplus r_g)$, and r_g. After receiving the message from user i, he computes $ESID_j = SID_i \oplus h(h(X_{GWN} \| 1) \| T_2) \oplus y_i$ and sends message $\{M_1, M_2, M_3, M_{12}, T_1, T_2, ESID_j, M_4, M_5, r_g\}$ to the GWN for the authentication.

After the above modification we can see that even if an insider obtains a lost card and

knows the parameter e_i, he cannot compute the values of $h(X_{GWN})$ and $h(e_i \oplus ID_i \oplus d_i)$ due to the one-way hash and the unknown values of ID_i and d_i. And also, he may corrupt S_j, however, without the knowledge of gateway node's secret $X_{GWN,}$ he cannot calculate SID_i.

5. Conclusion

In this paper, we showed that Farasha et al.'s scheme is flawed, because it suffers from (1). The smart card loss password guessing attack, and (2). Anonymity breach. We, therefore, modify the scheme to avoid these weaknesses. From the analysis shown in Section 4, we see that we have corrected the security issues.

References

[1] Chun-Ta Li, Min-Shiang Hwang , "An efficient biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications, Volume 33, Issue 1, January 2010, Pages 1–5

[2] Wen-Chung Kuo, Hong-Ji Wei, Jiin-Chiou Cheng, "An efficient and secure anonymous mobility network authentication scheme", journal of information security and applications 19 (2014) 18-24

[3] Jue-Sam Chou, Yalin Chen, "An Efficient Two-Pass Anonymous Identity Authentication Protocol Using a Smart Card", Vol 63, No. 8;Aug 2013

[4] Ding Wang, Ping Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks", Ad Hoc Networks 20 (2014) 1–15

[5] "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity", Ding Wang, Nan Wang b, Ping Wang, Sihan Qing, Information Sciences 321 (2015) 162–178

[6] Muhamed Turkanovic´, Boštjan Brumen, Marko Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion", Ad Hoc Networks 20 (2014) 96–112

[7] Kaiping Xue, Peilin Hong, Changsha Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture", Journal of Computer and System Sciences 80 (2014) 195–206

[8] Ding Wang, Ping Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions" Computer Networks 73 (2014) 41–57

[9] Chun-Ta Li, Cheng-Chi Lee , “A novel user authentication and privacy preserving scheme with smart cards for wireless communications”, Mathematical and Computer Modelling 55 (2012) 35–44

[10] Ding Wang, Ping Wang,“Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks”, Ad Hoc Networks 20 (2014) 1–15

[11] Mohammad Sabzinejad Farasha, Muhamed Turkanovic, Saru Kumaric,Marko Hölblb,“An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment” Ad Hoc Networks 36 (2016) 152–176

[12] Celia Li, Uyen Trang Nguyen, Hoang Lan Nguyen, Nurul Huda, “Efficient authentication for fast handover in wireless mesh networks”, computers & securit y 37(2013) I 24 -I 42

[13] I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang, “A password authentication scheme over insecure networks”, Journal of Computer and System Sciences, Vol. 72, No. 4, pp. 727-740, 2006.