Research Article

Security Analysis on “Anonymous Authentication Scheme for Smart Home Environment with Provable Security”

Meijia Xu,1 Qiying Dong,1 Mai Zhou,2 Chenyu Wang,3 and Yangyang Liu4

1College of Cyber Science, Nankai University, Tianjin 300350, China
2School of EECS, Peking University, Beijing 100089, China
3School of CyberSpace security, Beijing University of Posts and Telecommunications, China
4China Academy of Information and Communications Technology, China

Correspondence should be addressed to Chenyu Wang; wangchenyu@bupt.edu.cn

Received 11 August 2020; Revised 17 September 2020; Accepted 16 October 2020; Published 16 November 2020

1. Introduction

Smart home is a new paradigm of the Internet of Things, which can greatly facilitate our life; thus, it attracts much attention. In smart home environments, the smart devices can communicate and cooperate with each other to provide comprehensive services for users. However, the communications between the users and the smart devices are carried out in an insecure open channel. The adversary can eavesdrop the sensitive data transmitted over the insecure channel. Therefore, it is of importance to provide a security mechanism to secure the conversations. Multifactor user authentication [1, 2] is one of the important ways to identify the authenticity of a user. In a multifactor user authentication scheme for smart home environment, there are usually four participants: a set of users, the register center, the gateways, and the sensor nodes. The user owns her personal secrecy information, such as a password and a smart device. All participants are required to register in the register center. When a user wants to access real-time data stored on a sensor node, she can initiate an access request. Then, the gateway and the sensor node will verify the user. If the user is valid, a session key will be built to encrypt the subsequent conversations. In such schemes, the adversary is usually assumed to be able to (1) control the open channel, that is, she can intercept, modify, and eavesdrop the messages in the open channel; (2) list all the items in the space of passwords and identities; (3) compromise \( n - 1 \) factor(s) of a \( n \)-factor authentication scheme; (4) acquire the long-term secret key when accessing forward secrecy; (5) break some of sensor nodes; (6) obtain the previous session keys; and (7) register as a legitimate participant.

Recently, numerous user authentication schemes are proposed [4–7]. Most recently, Shuai et al. [8] designed a new anonymous authentication scheme for a smart home environment. They employ the elliptic curve cryptography to authenticate the users with resistance to offline dictionary attack and generate pseudoidentity DID, to provide user anonymity. However, some subtleties are overlooked, which results in vulnerability to various attacks. In this paper, we
demonstrate that their scheme cannot resist offline dictionary attack and inside attack and fails to achieve forward secrecy. Besides, we also discuss the causes and countermeasures of these security flaws. The countermeasures we proposed can also be applied to other authentication schemes with similar problems.

2. Review of Shuai et al.’s Scheme

In this section, we briefly review Shuai et al.’s scheme. The notations and abbreviations are shown in Table 1. Firstly, the registration authority RA chooses an elliptic curve $E$ and an additive group $G$ of $E$ with order $q$ and generator $P$. Next, RA generates a pair of private/public key $(x, X)$, where $x \in Z_q^*$ and $X = x \cdot P$, a long-term secret key $K$ and a hash function $h(\cdot): \{0, 1\}^* \rightarrow Z_q^*$. Note that $x$ and $K$ will be stored in GWN, and $(E(F_p), G, P, X, h(\cdot))$ will be published to all participants.

2.1. User Registration Phase

Step 1. $U_i \rightarrow RA : \{ID_i, HPW_i\}$, where $HPW_i = h(PW_i||a)$ and $a$ is a random nonce.

Step 2. $RA \rightarrow U_i : \{A_i, TEMP\}$.

RA first checks the availability of $ID_i$ and computes $K_{GU} = h(ID_i||K), A_i = K_{GU} \oplus HPW_i$. Finally, RA generates TEMP where TEMP is initialized to 0.

Step 3. $U_i$ computes $A_2 = a \oplus h(ID_i||PW_i), A_3 = h(ID_i||HPW_i)$ and stores $\{A_i, A_2, A_3, TEMP\}$ into the mobile device.

2.2. The Smart Device Registration Phase

Step 1. $SD_k \Rightarrow RA : \{SID_k\}$.

Step 2. $RA \Rightarrow SD_k : K_{GS}$. RA checks the validity of $SID_k$ and computes $K_{GS} = h(SID_k||K)$.

Step 3. $SD_k$ stores $K_{GS}$.

2.3. Login and Authentication Phase

Step 1. $U_i \rightarrow GWN : \{ID_i, A_1, M_1, V_1\}$.

$U_i$ provides ID$_i$ and PW$_i$, and then, the mobile device computes $a^* = A_i \oplus h(ID_i||PW_i), HPW^* = h(PW_i||a^*), A_3^* = h(ID_i||HPW^*)$. If $A_3^* \neq A_3$, the mobile device rejects the request and sets TEMP to TEMP + 1. Once TEMP $\geq 3$, the mobile device will be suspended till $U_i$ reregisters. Otherwise, the mobile device computes $K_{GU} = A_4 \oplus HPW_i, A_4 = \omega \cdot P, A_5 = \omega \cdot X, DID = ID_i \oplus A_5, M_1 = (R_1||SID_k) \oplus K_{GU},$ and $V_1 = h(ID_i||R_1||K_{GU}||M_1)$, where $R_1$ and $\omega \in Z_n^*$ are two random numbers, and SID$_k$ is the identity of the target SD$_k$.

Step 2. $GWN \rightarrow SD_k : \{M_2, V_2\}$.

Table 1: Notations and abbreviations.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U_i$</td>
<td>$i^{th}$ user</td>
</tr>
<tr>
<td>GWN</td>
<td>The gateway node</td>
</tr>
<tr>
<td>SD$_k$</td>
<td>$j^{th}$ smart device</td>
</tr>
<tr>
<td>ID$_i$</td>
<td>Identity of $U_i$</td>
</tr>
<tr>
<td>PW$_i$</td>
<td>Password of $U_i$</td>
</tr>
<tr>
<td>GID$_i$</td>
<td>Identity of GWN</td>
</tr>
<tr>
<td>SID$_k$</td>
<td>Identity of SD$_k$</td>
</tr>
<tr>
<td>RA</td>
<td>Registration authority</td>
</tr>
<tr>
<td>$K$</td>
<td>The secret key of GWN</td>
</tr>
<tr>
<td>$\oplus$</td>
<td>Bitwise XOR operation</td>
</tr>
<tr>
<td>$|$</td>
<td>Concatenation operation</td>
</tr>
<tr>
<td>$h(\cdot)$</td>
<td>One-way hash function</td>
</tr>
<tr>
<td>$\Rightarrow$</td>
<td>A secure channel</td>
</tr>
</tbody>
</table>

GWN computes $A_2^* = x \cdot A_4, ID_i^* = DID \oplus A_5^*, K_{GU} = h\{ID_i^*||K\}, R_1^* = SID_k = M_1 \oplus K_{GU}, V_1^* = h(ID_i||R_1^*||K_{GU}||M_1)$. If $V_1^* \neq V_1$, GWN ends the session. Otherwise, GWN computes $K_{GS} = h(SID_k||K), M_2 = (ID_i||GID_j||R_1||R_2) \oplus K_{GS}$, and $V_2 = h(ID_i||GID_j||K_{GS}||R_1||R_2)$, where $R_2$ is a random number.

Step 3. $SD_k \rightarrow GWN : \{M_3, V_3\}$.

SD$_k$ computes $(ID_i||GID_j||R_1||R_2) = M_2 \oplus K_{GS}, V_3^* = h(ID_i||GID_j||K_{GS}||R_1||R_2)$. If $V_2^* \neq V_2$, SD$_k$ ends the session. Otherwise, SD$_k$ computes $SK = h(ID_i||GID_j||SID_k||R_1||R_2)$, $M_3 = R_3 \oplus K_{GS}$, and $V_3 = h(R_3||K_{GS}||SK)$, where $R_3$ is a random number.

Step 4. $GWN \rightarrow U_i : \{M_4, V_4\}$.

GWN computes $R_3 = M_3 \oplus K_{GS}, SK = h(ID_i||GID_j||SID_k||R_1||R_2||R_3)$, and $V_3^* = h(R_3||K_{GS}||SK)$. If $V_3^* \neq V_3$, GWN ends the session. Otherwise, GWN computes $M_4 = (GID_j||R_2||R_3) \oplus K_{GS}$ and $V_4 = h(K_{GU}||SK||R_2||R_3)$.

Step 5. $U_i$ computes $(GID_j||R_2||R_3) = M_4 \oplus K_{GS}, SK = h(ID_i||GID_j||SID_k||R_1||R_2||R_3)$, and $V^* = h(K_{GU}||SK||R_2||R_3)$. If $V^* = V_4$, the authentication is finished successfully.

3. Cryptanalysis of Shuai et al.’s Scheme

In this section, we demonstrate that Shuai et al.’s scheme suffers from various attacks when assuming the adversary armed with real-world capabilities [9–11] as below:

1. Exhaust all the items in the Descartes space of passwords and identities
2. Get ID$_i$ when assess the security of the scheme
(3) Intercept, eavesdrop, or resend the messages in the open channel
(4) Get the data stored in the smart device
(5) Get previous session keys
(6) Get the secret key $K$ when accessing forward secrecy
(7) The adversary can be the administrator of the registration authority

3.1. Offline Dictionary Attack. When the adversary gets the data $\{(A_1, A_2, A_3)\}$ stored in the victim $U_i$’s mobile device, she can guess $U_i$’s password and identity correctly as the following steps:

The attack steps are as follows:

**Step 1.** Guess $PW_i$ to be $PW_i^*; ID_i$ to be $ID_i^*$.

**Step 2.** Compute $a^* = A_2 \oplus h(ID_i^* || PW_i^*)$.

**Step 3.** Compute $HPW_i^* = h(PW_i^* || a^*)$.

**Step 4.** Compute $A_3^* = h(ID_i^* || HPW_i^*)$.

**Step 5.** Verify the correctness of $PW_i$ and $ID_i$ by checking if $A_3^* = A_3$.

**Step 6.** Repeat Steps 1–5 until the equation holds.

The time complexity is $O(|PW_i^*| + |ID_i| + 3T_H)$, where $T_H$ is the time of the hash function.

Assuming the adversary gets the victim’s identity $ID_i$, the adversary, with the data stored in the smart device and transmitted in the open channel, can guess $U_i$’s password successfully as below:

The attack steps are as follows:

**Step 1.** Guess $PW_i$ to be $PW_i^*; ID_i$ to be $ID_i^*$.

**Step 2.** Compute $a^* = A_2 \oplus h(ID_i^* || PW_i^*)$.

**Step 3.** Compute $HPW_i^* = h(PW_i^* || a^*)$.

**Step 4.** Compute $K_{GU}^* = A_1 \oplus HPW_i^*$.

**Step 5.** Compute $R_1^* || SID_k = M_1 \oplus K_{GU}^*$.

**Step 6.** Compute $V_1^* = h(ID_i^* || R_1^* || K_{GU}^* || M_1)$.

**Step 7.** Verify the correctness of $PW_i$ and $ID_i$ by checking if $V_1^* = V_1$.

**Step 8.** Repeat Steps 1–6 until the correct value of $PW_i$ is found.

The time complexity is $O(|PW_i^*| + |ID_i| + 3T_H)$.

Possible Countermeasures: In offline dictionary attack, the inherent causes are as follows: (1) the adversary can find a verifier to check the correctness of the guessed password and (2) to the adversary, the verifier only contains one unknown parameter (i.e., the victim’s password), that is, all the parameters which consist of the verifier can be derived from the victim’s password. According to Wang and Xu [12], the offline dictionary attack can be divided into two types in terms of where the verifier is from. In the former attack, the verifier $A_3$ is extracted from the smart device. To deal with this attack, Wang and Wang [13] proposed a way of integrating the fuzzy-verifier technique and honeypots. That is, let $A_3 = h(ID || HPW_i)$ mod $n_0$, where $n_0$ is an integer and $2^4 \leq n_0 \leq 2^8$.

As such, there are about $|PW_i^*| + |ID_i| + 3T_H \approx 2^{32}$ candidate pairs of identity and password which satisfy the equation of Step 5, when $I_0 = 2^4$. To test the specific pair of identity and password, the adversary needs to initiate the access request online, and this (the failure attempt) can be detected and stopped by the parameter $TEMP$.

To the second attack, a public key is necessary [14]. In Shuai et al.’s scheme, we need to set the verifier $V_i = h(ID || R_i || |K_{GU}|| |M_i| || A_3|| D_{ID})$ and $D_{ID} = ID \oplus h(A)$. As such, there are essentially two unknown parameters to the adversary, i.e., the password and $A_3$, and the space of $A_3$ is too large for the adversary to conduct the offline dictionary attack.

3.2. Forward Secrecy. Forward secrecy requires that the exposure of the secrecy key $K$ will not affect the security of previous conversations. However, we find this scheme cannot provide forward secrecy. If the adversary gets $K$ and eavesdrops the parameters $\{M_3, M_5\}$, she can get the session key $SK$ as the following steps:

The attack steps are as follows:

**Step 1.** Compute $K_{GU}^* = h(SID_k || K)$.

**Step 2.** Compute $(ID_i^* || GID_i^* || R_1^* || R_3^*) = M_4 \oplus K_{GU}^*$.

**Step 3.** Compute $R_3^* = M_3 \oplus K_{GU}^*$.

**Step 4.** Compute $SK = h(ID_i^* || GID_i^* || R_1^* || R_3^* || R_5^*)$.

The time complexity is $O(|PW_i^*| + |ID_i| + 2T_H)$.

Possible Countermeasures: According to Ma et al. [14], the public key technique and two modular exponentiation or point multiplication operations on the smart device are required. Following this principle, we can let $SK = h(ID || |GID_i|| |A_4|| |A_6|| A_7)$, where $A_5 = R_3 \cdot P$, $A_7 = \omega \cdot A_6 = R_1 \cdot A_4 \cdot A_6$ is computed by $SD_k$ and should be transmitted to $U_i$ in the open channel. $A_4$ also needs to be sent to $SD_k$. $R_3$ cannot be transmitted to any participants. As such, the adversary has no way to compute $A_7$ (it is a computational difficult problem which cannot be solved within polynomial time), and the forward secrecy is achieved.

3.3. Inside Attack. Suppose the adversary is also the administrator of RA, then she can exploit the register message and the data stored in mobile devices to guess the victim’s password as follows:
The attack steps are as follows:

Step 1. Guess PW\(_i\) to be PW\(_i^\ast\), ID\(_i\) to be ID\(_i^\ast\).

Step 2. Compute a\(^\ast\) = A\(_2\) \oplus h(ID\(_i^\ast\)||PW\(_i^\ast\)).

Step 3. Compute HPW\(_i^\ast\) = h(PW\(_i^\ast\)||a\).

Step 4. Verify the correctness of PW\(_i\) and ID\(_i\) by checking if HPW\(_i^\ast\) == HPW\(_i\).

Step 5. Repeat Steps 1–4 until the correct value of PW\(_i\) and ID\(_i\) is found.

The time complexity is \(O(|D_{PW}|^*|D_{al}|^*2T_R)\).

Possible Countermeasures: Inside attack is practical although it has high requirements on the adversary’s capability. In this scheme, the verifier HPW\(_i\) contains PW\(_i\) and a, and a can be computed using the parameters in the mobile device. Therefore, a way to deal with this attack is to update a after the registration. After receiving the response from RA, the user side should select a new random nonce a’, update HPW\(_i\) as h(PW\(_i^\ast\)||a’), and then set A\(_2\) = a’ \oplus h(ID\(_i^\ast\)||PW\(_i^\ast\)) and A\(_3\) = h(ID\(_i^\ast\)||HPW\(_i^\ast\)).

4. Conclusion

In this paper, we have analyzed an anonymous authentication scheme for a smart home environment proposed by Shuai et al. [8]. We demonstrated that their scheme suffers from various attacks although it is proved to be secure under the random oracle model. We showed that this scheme cannot resist offline dictionary attack and inside attack and also fails to provide forward secrecy. After pointing out these security flaws, we proposed possible countermeasures to deal with them. These suggestions can also be applied to most similar schemes. Thus, our work is helpful to the design of a secure and efficient user authentication scheme for the smart home environment.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References


Wireless Communications and Mobile Computing