Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8838363, 4 pages
https://doi.org/10.1155/2020/8838363

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 Liu**[4]

[1]*College of Cyber Science, Nankai University, Tianjin 300350, China*
[2]*School of EECS, Peking University, Beijing 100089, China*
[3]*School of CyberSpace security, Beijing University of Posts and Telecommunications, China*
[4]*China 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

Academic Editor: Qi Jiang

As an important application of the Internet of Things, smart home has greatly facilitated our life. Since the communication channels of smart home are insecure and the transmitted data are usually sensitive, a secure and anonymous user authentication scheme is required. Numerous attempts have been taken to design such authentication schemes. Recently, Shuai et al. (Computer & Security 86(2019):132146) designed an anonymous authentication scheme for smart home using elliptic curve cryptography. They claimed that the proposed scheme is secure against various attacks and provides ideal attributes. However, we show that their scheme cannot resist inside attack and offline dictionary attack and also fails to achieve forward secrecy. Furthermore, we give some suggestions to enhance the security of the scheme. These suggestions also apply to other user authentication schemes with similar flaws.

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 conversations 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 [3] (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_i 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. $U_i \Rightarrow \mathrm{RA} : \{\mathrm{ID}_i, \mathrm{HPW}_i\}$, where $\mathrm{HPW}_i = h(\mathrm{PW}_i \| a)$ and a is a random nonce.

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

RA first checks the availability of ID_i and computes $K_{\mathrm{GU}} = h\{\mathrm{ID}_i \| K\}$, $A_1 = K_{\mathrm{GU}} \oplus \mathrm{HPW}_i$. Finally, RA generates TEMP where TEMP is initialized to 0.

Step 3. U_i computes $A_2 = a \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i)$, $A_3 = h(\mathrm{ID}_i \| \mathrm{HPW}_i)$ and stores $\{A_1, A_2, A_3, \mathrm{TEMP}\}$ into the mobile device.

2.2. The Smart Device Registration Phase

Step 1. $\mathrm{SD}_k \Rightarrow \mathrm{RA} : \{\mathrm{SID}_k\}$.

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

Step 3. SD_k stores K_{GS}.

2.3. Login and Authentication Phase

Step 1. $U_i \rightarrow \mathrm{GWN} : \{\mathrm{DID}_i, A_4, M_1, V_1\}$.

U_i provides ID_i and PW_i, and then, the mobile device computes $a^* = A_2 \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i)$, $\mathrm{HPW}^* = h(\mathrm{PW}_i \| a^*)$. $A_3^* = h(\mathrm{ID}_i \| \mathrm{HPW}_i^*)$. If $A_3^* \neq A_3$, the mobile device rejects the request and sets TEMP to TEMP + 1. Once TEMP ≥ 3, the mobile device will be suspended till U_i reregisters. Otherwise, the mobile device computes $K_{\mathrm{GU}} = A_1 \oplus \mathrm{HPW}_i$, $A_4 = \omega \cdot P$,$A_5 = \omega \cdot X$, $\mathrm{DID}_i = \mathrm{ID}_i \oplus A_5$, $M_1 = (R_1 \| \mathrm{SID}_k) \oplus K_{\mathrm{GU}}$, and $V_1 = h(\mathrm{ID}_i \| R_1 \| K_{\mathrm{GU}} \| M_1)$, 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. $\mathrm{GWN} \rightarrow \mathrm{SD}_k : \{M_2, V_2\}$.

GWNcomputes $A_5{}^* = x \cdot A_4$,$\mathrm{ID}_i^* = \mathrm{DID}_i \oplus A_5^*$, $K_{\mathrm{GU}} = h\{\mathrm{ID}_i^* \| K\}$, $R_1^* \| \mathrm{SID}_k = M_1 \oplus K_{\mathrm{GU},} V_1^* = h(\mathrm{ID}_i \| R_1 \| K_{\mathrm{GU}} \| M_1)$. If $V_1^* \neq V_1$, GWN ends the session. Otherwise, GWN computes $K_{\mathrm{GS}} = h(\mathrm{SID}_k \| K)$, $M_2 = (\mathrm{ID}_i \| \mathrm{GID}_j \| R_1 \| R_2) \oplus K_{\mathrm{GS}}$, and $V_2 = h(\mathrm{ID}_i \| \mathrm{GID}_j \| K_{\mathrm{GS}} \| R_1 \| R_2)$, where R_2 is a random number.

Step 3. $\mathrm{SD}_k \rightarrow \mathrm{GWN} : \{M_3, V_3\}$.

SD_k computes $(\mathrm{ID}_i \| \mathrm{GID}_j \| R_1 \| R_2) = M_2 \oplus K_{\mathrm{GS}}$, $V_2^* = h(\mathrm{ID}_i \| \mathrm{GID}_j \| K_{\mathrm{GS}} \| R_1 \| R_2)$. If $V_2^* \neq V_2$, SD_k ends the session. Otherwise, SD_k computes $\mathrm{SK} = h(\mathrm{ID}_i \| \mathrm{GID}_j \| \mathrm{SID}_k \| R_1 \| R_2 \| R_3)$, $M_3 = R_3 \oplus K_{\mathrm{GS}}$, and $V_3 = h(R_3 \| K_{\mathrm{GS}} \| \mathrm{SK})$, where R_3 is a random number.

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

GWN computes $R_3 = M_3 \oplus K_{\mathrm{GS}}$, $\mathrm{SK} = h(\mathrm{ID}_i \| \mathrm{GID}_j \| \mathrm{SID}_k \| R_1 \| R_2 \| R_3)$, and $V_3^* = h(R_3 \| K_{GS} \| SK)$. If $V_3^* \neq V_3$, GWN ends the session. Otherwise, GWN computes $M_4 = (\mathrm{GID}_j \| R_2 \| R_3) \oplus K_{\mathrm{GS}}$ and $V_4 = h(K_{\mathrm{GU}} \| \mathrm{SK} \| R_2 \| R_3)$.

Step 5. U_i computes $(\mathrm{GID}_j \| R_2 \| R_3) = M_4 \oplus K_{\mathrm{GU}}$, $\mathrm{SK} = h(\mathrm{ID}_i \| \mathrm{GID}_j \| \mathrm{SID}_k \| R_1 \| R_2 \| R_3)$, and $V_4^* = h(K_{\mathrm{GU}} \| \mathrm{SK} \| R_2 \| R_3)$. If $V_4^* == V_4$, the authentication is finished sucessfully.

Table 1: Notations and abbreviations.

Symbol	Description
U_i	i^{th} user
GWN	The gateway node
SD_k	j^{th} smart device
ID_i	Identity of U_i
PW_i	Password of U_i
GID_j	Identity of GWN
SID_k	Identity of SD_k
RA	Registration authority
K	The secret key of GWN
$\oplus$	Bitwise XOR operation
$\|$	Concatenation operation
$h(\cdot)$	One-way hash function
$\rightarrow$	A common channel
$\Rightarrow$	A secure channel

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 $\mathrm{PW}_i{}^*$,ID_i to be $\mathrm{ID}_i{}^*$.

Step 2. Compute $a^* = A_2 \oplus h(\mathrm{ID}_i^* \| \mathrm{PW}_i{}^*)$.

Step 3. Compute $\mathrm{HPW}_i^* = h(\mathrm{PW}_i^* \| a^*)$.

Step 4. Compute $A_3^* = h(\mathrm{ID}_i^* \| \mathrm{HPW}_i^*)$.

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 $O(|D_{\mathrm{PW}}|^* |D_{id}|^* 3T_H)$, 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 $\mathrm{PW}_i{}^*$, ID_i to be $\mathrm{ID}_i{}^*$.

Step 2. Compute $a^* = A_2 \oplus h(\mathrm{ID}_i^* \| \mathrm{PW}_i{}^*)$.

Step 3. Compute $\mathrm{HPW}_i^* = h(\mathrm{PW}_i^* \| a^*)$.

Step 4. Compute $K_{\mathrm{GU}}^* = A_1 \oplus \mathrm{HPW}_i^*$.

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

Step 6. Compute $V_1^* = h(\mathrm{ID}_i \| R_1^* \| K_{\mathrm{GU}}^* \| M_1)$.

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 $O(|D_{\mathrm{pw}}|^* |D_{\mathrm{id}}|^* 3T_H)$.

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 honeywords. That is, let $A_3 = h(\mathrm{ID}_i \| \mathrm{HPW}_i) \mod n_0$, where n_0 is an integer and $2^4 \le n_0 \le 2^8$.

As such, there are about $|D_{\mathrm{id}}{}^* D_{\mathrm{pw}}|/l_0 \approx 2^{32}$ candidate pairs of identity and password which satisfy the equation of Step 5, when $l_0 = 2^8$. 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 $V_i = h(\mathrm{ID}_i \| R_1 \| K_{\mathrm{GU}} \| M_1 \| A_5)$ and $\mathrm{DID}_i = \mathrm{ID}_i \oplus h(A)$. As such, there are essentially two unknown parameters to the adversary, i.e., the password and A_5, and the space of A_5 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 $\{M_2, M_3\}$, she can get the session key SK as the following steps:

The attack steps are as follows:

Step 1. Compute $K_{\mathrm{GS}}^* = h(\mathrm{SID}_k \| K)$.

Step 2. Compute $(\mathrm{ID}_i^* \| \mathrm{GID}_j^* \| R_1^* \| R_2^*) = M_2 \oplus K_{\mathrm{GS}}^*$.

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

Step 4. Compute $\mathrm{SK} = h(\mathrm{ID}_i^* \| \mathrm{GID}_i^* \| R_1^* \| R_2^* \| R_3^*)$.

The time complexity is $O(|D_{\mathrm{pw}}|^* |D_{\mathrm{id}}|^* 2T_H)$.

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 $\mathrm{SK} = h(\mathrm{ID}_i \| \mathrm{GID}_j \| A_4 \| A_6 \| A_7)$, where $A_6 = R_3 \cdot P$, $A_7 = \omega \cdot A_6 = R_3 \cdot A_4 \cdot A_6$ 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 $\mathrm{PW}_i{}^*$, ID_i to be ID_i^*.

Step 2. Compute $a^* = A_2 \oplus h(\mathrm{ID}_i^* \| \mathrm{PW}_i^*)$.

Step 3. Compute $\mathrm{HPW}_i^* = h(\mathrm{PW}_i \| a)$.

Step 4. Verify the correctness of PW_i and ID_i by checking if $\mathrm{HPW}_i^* == \mathrm{HPW}_i$.

Step 5. Repeat Steps 1–4 until the correct value of PW_i and ID_i is found.

The time complexity is $O(|D_{\mathrm{pw}}|^* |D_{\mathrm{id}}|^* 2T_H)$.

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 $h(\mathrm{PW}_i \| a')$, and then set $A_2 = a' \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i)$ and $A_3 = h(\mathrm{ID}_i \| \mathrm{HPW}_i)$.

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

[1] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K. K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.

[2] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: preserving security and privacy in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 8, pp. 1390–1397, 2010.

[3] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.

[4] F. Wang, G. Xu, G. Xu, Y. Wang, and J. Peng, "A robust IoT-based three-factor authentication scheme for cloud computing resistant to session key exposure," *Wireless Communications and Mobile Computing*, vol. 2020, 15 pages, 2020.

[5] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[6] F. Wang, G. Xu, and G. Lize, "A secure and efficient ECC-based anonymous authentication protocol," *Security and Communication Networks*, vol. 2019, 13 pages, 2019.

[7] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[8] M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Computers & Security*, vol. 86, no. 2019, pp. 132–146, 2019.

[9] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 76, pp. 37–48, 2016.

[10] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.

[11] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.

[12] C. Wang and G. Xu, "Cryptanalysis of three password-based remote user authentication schemes with non-tamper-resistant smart card," *Security and Communication Networks*, vol. 2017, 14 pages, 2017.

[13] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.

[14] C. Ma, D. Wang, and S. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," *International Journal of Communication Systems*, vol. 27, pp. 2215–2227, 2012.