A Secure Authentication and Key Agreement Scheme in Smart Home

Dawei Song and Fengtong Wen
School of Mathematical Sciences, University of Jinan, Jinan, 250022, China.
Email: wftwq@163.com

Abstract. Secure communication between users and devices is an important aspect of IoT applications. Smart home is an emerging key element in IoT applications. Due to limited computing resources, it is difficult to deal with these communication problems. Therefore, a safe and efficient solution is needed to complete the communication between users and devices. Sometimes secure communication of information is required between devices and devices. In view of this point, this paper proposes a secure and efficient authentication and session key negotiation scheme between smart home devices.

1. Introduction
Generally, a smart home network is composed of many isomerism smart devices, such as an intelligent lighting system, an intelligent security system, a network home appliance, an audio and video device, a camera, etc. But most devices have limited computing power. In the smart home system, the following entities generally exist: (1) A trusted third party: it is usually a local server, while sometimes it is a cloud server, which responsible for registering new users and new smart devices, initializing the system, and pre-processing some parameters. (2) Smart home equipment: any home equipment that can be remotely controlled, the computing power of the equipment is limited. (3) End-user equipment for monitoring and controlling home devices such as mobile phones, tablets or smart watches via Wi-Fi or the Internet, and the computing power is not strong. (4) HG: the gateway is the management and control center of the smart home system, which act as an intermediary between devices, and help to authenticate and exchange information between devices through Wi-Fi or the Internet.

There are many challenges in the Internet of Things. Security and privacy are the most important points, performance, reliability and management are behind them [1]. In 2015, Suresh and Sruthi [2], clearly pointed out the advantages of smart home, but in the same year min and Varadh - arajan [3,4] pointed out the potential dangers of smart homes. There are about 390,000 new malware samples are registered every day. Malware attacks are getting more complicated. Most of the new malware that appears every day is a modified version, while using more complicated techniques, [3,4,5,6,7,8,9] are some of the proposed malware attacks.

On this basis, some identity authentication and secure communication schemes for smart home systems have been proposed [10,11,12] Gomez and Paradells [11] discussed different types of wireless home automation network architectures and technologies, including a series of security barriers. The program aims to establish a framework for smart home appliances. The authors focus on the availability of smart devices, control of electricity prices and operational safety. The framework can provide effective and reliable security protection, but does not consider device authentication, data confidentiality and integrity. This means that the framework may not be able to be used under the collaborative opponent model (e.g., the Dolev-Yao model),[13] also doing similar work. Kim [12] proposed a seamless integration of heterogeneous devices and access control in smart homes. The
authors observe that devices from different vendors in smart homes communicate with each other without de facto communication standards. Therefore, based on the Open Services Gateway initiative, they proposed a smart home architecture that built heterogeneous protocols in the Home Area Network (HAN), but this solution did not consider device authentication when deploying home networks [14].

proposed a scheme that requires each device to communicate with the manufacturer, but always accessing the manufacturer and sending authentication information to it is cumbersome and costly.

In 2016, Geetha et al.[15] proposed an identity authentication and key agreement protocol, which uses a lightweight computing tool to establish a secure session key. The author considers identity authentication and key agreement between the device and the gateway, as well as group authentication of multiple devices between different gateways. However, identity authentication and key agreement between smart devices are not considered, and the group authentication process is too complicated. Based on this, we propose a simple and secure mutual authentication and key agreement protocol between devices, which can also be applied to devices belonging to different gateways.

The remainder of this paper is organized as follows. Section 2 presents a brief review and cryptanalysis of Geetha et al.’s scheme. Then, we proceed with analyzing its weaknesses in Section 3. Subsequently, we present a new scheme in Section 4. And we prove that our scheme is more efficient and security in Section 5. Section 6 concludes the paper.

2. Overview of Geetha Et Al.’s Scheme

In this section, we review Geetha et al.’s scheme (2016). Their scheme is made up of three phases: System setup phase, Authentication and key establishment phase, Add new equipment phase. The notations mentioned in Geetha et al.’s scheme are showed in Table 1.

| Notation | Meaning |
|----------|---------|
| SP       | Security service provider |
| id_A     | smart device A’s identity |
| K_A      | smart device A’s unique key |
| Kid_A    | smart device A’s Key identifier |
| Token_A  | smart device A’s authentication token |
| Sid_A    | smart device A’s serial number |
| Gid      | Home Gateway identity |
| T_x      | Current time |
| T        | Effective time interval |
| ||       | String concatenation operation |
| h(·)     | An hash function |
| MAC[·]   | An message authentication code |
| HMAC[·]  | Another message authentication code |
| E_{K_A}(·) | Use A’s key encrypt |

2.1. System Setup Phase

First and the most important, each device should be registered to the SP offline and get some security parameters. For each smart device A, the SP assigns \( id_A, Token_A, K_A, Kid_A \) to A, then stores them with Gid in A, and calculates \( Q_A = h(Token_A \| Gid \| Sid_A) \). Then SP stores \( id_A, Q_A, K_A, Kid_A \) to the Home Gateway(HG) where A is located. Finally, SP maintains a database for recording devices that have already been set up. For security reasons, we can assume that all stored keys have a lifetime, depending on the SP settings.

2.2. Authentication and Key Establishment Phase

In order to maintain initial trust between smart devices, this phase provides authentication and key establishment mechanisms. This stage is divided into four steps.
• Step 1: HG generates a nonce $r$, and calculates $C = MAC[Q_A, Gid \parallel id_A \parallel T_2 \parallel r]$ , then sends a request message $\{Gid, C, T_1, r\}$ to $A$.

• Step 2: Once $A$ receives the request message, $A$ checks whether $T_2 - T_1 < 0$. If it is correct, $A$ continues to calculate $Q_A = h(Tok_{en} \parallel Gid \parallel Sid_A)$ and $C = MAC[Q_A, Gid \parallel id_A \parallel T_1 \parallel r]$. Then $A$ verifies $C = C^*$, if they are not equal, generates an error message and terminates the system. Otherwise $A$ generates a random secret $s$ and calculates $N_A = E_{K_A}[id_A, s, r, T_2]$ and $tag = HMAC[Q_A, id_A \parallel Gid \parallel s \parallel r \parallel T_2]$. Finally $A$ sends a respond $\{K_{id_A}, N_A, tag, T_2\}$ to HG.

• Step 3: HG first checks $T_3 - T_2 < 0$. If it is established, $HG$ retrieves the $K_A$ corresponding to $K_{id_A}$ from its own database, and decrypts $N_A$ to get $id_A^*' = id_A, s^* = s, r^* = r$. If they are not equal, $HG$ generates an error message and terminates the system. Otherwise $HG$ calculates $tag^* = HMAC[Q_A, id_A \parallel Gid \parallel s \parallel r \parallel T_2]$ then verifies whether $tag^* = tag$. If the verification passes, the session key $sk = h(id_A \parallel Gid \parallel s \parallel T_2)$ is generated by $HG$ at the same time $HG$ calculates $N_{HG} = E_{K_{HG}}[sk, s, T_3]$ and finally sends the message $\{N_{HG}, T_3\}$ to $A$.

• Step 4: Once $A$ receives the HG’s message, $A$ checks $T_4 - T_3 < 0$. If it is established, then uses $K_{id_A}$ to decrypt the $N_{HG}$ to obtain $\{sk^*, s^*, T_3\}$, verifies whether $T_3 = T_3, s^* = s$. If they are equal, the session key is securely established between the gateway and the device.

2.3. Add New Equipment Phase
New smart devices can be arbitrarily added to the smart home network. If a new device wants to join a gateway, it only needs SP to perform the system setup phase operation, then the gateway and device perform the above interaction.

3. Limitation of Geetha Et Al.’s Scheme
Based on the above comments, we can find the solution of Geetha et al. Only mutual authentication and session key establishment between the device and the gateway are introduced. However, in a smart home system, there is more than one way of interacting with information, which also happens between devices. So we built a simple and secure authentication and key agreement protocol between devices.

4. Our Proposed Scheme
Our scheme has been improved on the Geetha et al.’s scheme. It can also be divided into three parts: System setup phase, Authentication and key establishment phase, Add new equipment phase.

4.1. System Setup Phase
First, each device should be registered to the SP offline and gets a series of security parameters. For each smart device $A$, the SP assigns $id_A, Token_A, K_{id_A}$ to $A$, and stores them with $Gid, K_{HG}$ in $A$, simultaneously calculates $Q_A = h(Tok_{en} \parallel Gid \parallel Sid_A)$ then stores $id_A, Q_A, K_{id_A}$ to $HG$’s unique key $K_{HG}$ to the Home Gateway where $A$ is located. It is worth mentioning that these operations are all done through a secure channel. Finally SP maintains a database for recording devices that have already been set up. For security reasons, we can assume that all stored keys have a lifetime, depending on the SP settings.

4.2. Authentication and Key Agreement
When smart device $A$ wants to communicate with device $B$ in the same gateway, it can perform the following interaction with $B$. There are four steps in authentication and key agreement phase.

• Step 1: $A$ generates a nonce $a$ and calculates $Q_{AB} = h(K_{HG} \parallel id_A \parallel id_B)$ and $C = MAC[Q_{AB}, Gid \parallel id_A \parallel T_2 \parallel a]$ then sends a request message $\{id_A, C, T_1, a, id_B\}$ to $B$.

• Step 2: Once $B$ receives the request message, $B$ checks $T_2 - T_1 < 0$, if it is correct, continues to calculate $Q_{AB} = h(K_{HG} \parallel id_A \parallel id_B)$ and $C^* = MAC[Q_{AB}, Gid \parallel id_A \parallel T_2 \parallel a]$ , then verifies whether $C = C^*$, if they are not equal, $B$ generates an error message and terminates the
system. Otherwise \( B \) generates a random secret \( b \) and calculates \( N_B = E_{K_{HG}}[id_B, b, a, T_2] \) and \( tag = HMAC[Q_{AB}, id_B \parallel b \parallel a \parallel T_2] \), finally sends a response message \( \{N_B, tag, T_2\} \) to \( A \).

- **Step 3:** \( A \) first checks \( T_3 - T_2 \leq T \), if it is established, decrypts \( N_B \) to get \( \{id'_B, b, a', T'_2\} \) used \( K_{HG} \), then verifies whether \( T'_2 = T_2, id'_B = id_B, a' = a \). If they are not equal, \( A \) generates an error message and terminates the system. Otherwise \( A \) calculates \( tag' = HMAC[Q_{AB}, id_A \parallel id'_B \parallel b' \parallel a' \parallel T'_2] \) then verifies whether \( tag' = tag^* \). If the verification passes, the session key \( sk = h(id_A \parallel id_B \parallel b \parallel T_3 \parallel T_2 \parallel Q_{AB}) \) is generated. Finally \( A \) calculates \( N_{AB} = E_{K_{HG}}[sk, b, T_3] \), and sends the message \( \{N_{AB}, T_3\} \) to \( B \).

- **Step 4:** Once \( B \) receives the \( A \)'s message, \( B \) checks whether \( T_4 - T_3 \leq T \), if it is established, \( B \) decrypts the \( N_{AB} \) to obtain \( sk^*, b^*, T_3^* \) used \( K_{HG} \), then verifies whether \( T_3^* = T_3, b^* = b \). If they are equal, \( B \) believes that \( sk^* \) is the session key between \( A \) and \( B \).

### 4.3. Add New Equipment Phase

This phase is similar to the scheme of Geetha et al. New smart devices can be arbitrarily added to the smart home network. If a new device wants to join a gateway, it only needs \( SP \) to perform the system setup phase operation, then the gateway and device perform the above interaction.

### 5. Analysis of Our Scheme and Conclusion

In our scheme, firstly, only the device in the gateway will have \( K_{HG} \), and it is well hidden. Therefore, \( Q_{AB} \) cannot be calculated by the attacker, and then \( C \) cannot be calculated, thus the attacker cannot pretend to be \( A \) to deceive \( B \). Then \( b \) is also hidden, so the attacker can't pretend to be \( B \) to deceive, and the session key cannot be calculated by the attacker. At the same time we have been using timestamps, which can avoid replay attacks.

Compared with the scheme of Geetha et al., our scheme does not pass through the gateway when the device information interacts, which saves some resources. It can also be used for information interaction between user terminals and home devices, which is essential in smart home environments. When the user registers with the \( SP \), the user can set his own account, that is, the identity \( id_u \), and then obtain a series of security parameters assigned by the \( SP \). Then, through the above interaction, the user complete the communication with the smart home device. This solution also applies to the interaction between devices and gateways. Because the gateway also has its own identity \( Gid \), we only need to change the \( id_g \) in the scheme to \( Gid \), and then perform similar operations to achieve secure communication between \( A \) and the gateway.

Finally, we think that devices between different gateways may also interact with information, such as between neighbors, between relatives, between companies and houses. We will continue to explore these aspects.

### 6. Acknowledgements

This study was supported by the National Science Foundation of Shandong Province (No. ZR2018LF006).

### 7. References

[1] Al-Fuqaha A, Guizani M and Mohammadi M 2015 Internet of Things: A survey on Enabling Technologies, Protocols, and Applications *IEEE Communications Surveys and Tutorials* **17**(4) 2347-76

[2] Suresh S and Sruthi P V 2016 A review on smart home technology *Online International Conference on Green Engineering and Technologies IEEE* pp 1-3

[3] Min B and Varadarajan V 2014 Design and Analysis of a New Feature-Distributed Malware *IEEE International Conference on Trust, Security and Privacy in Computing and Communications IEEE Computer Society* pp 457-464
[4] Min B and Varadharajan V 2016 Design and Evaluation of Feature Distributed Malware Attacks against the Internet of Things (IoT) International Conference on Engineering of Complex Computer Systems IEEE pp 80-89

[5] Coppolino L, Dalessandro V and Dantonio S 2016 My Smart Home is Under Attack IEEE International Conference on Computational Science and Engineering IEEE pp 145-151

[6] Pan J and Fung C C An offensive containment strategy based on Malware’s attack patterns International Conference on Machine Learning and Cybernetics. IEEE pp 1631-1636

[7] Mylonas A, Dritsas S and Tsoumas B 2014 Smartphone security evaluation The malware attack case Proceedings of the International Conference on Security and Cryptography IEEE pp 25-36

[8] Barabosch T and Gerhards-Padilla E 2014 Host-based code injection attacks: A popular technique used by malware International Conference on Malicious and Unwanted Software the Americas IEEE pp 8-17

[9] Sood A K and Zeadally S 2010 Drive-By Download Attacks: A Comparative Study ItProfessional 18(5) 18-25

[10] Ashibani Y and Mahmoud Q H 2017 An efficient and secure scheme for smart home communication using identity-based signcryption IEEE International performance computing and Communications Conference IEEE Computer Society pp 1-7

[11] Gomez C and Paradells J 2010 Wireless Home Automation Networks: A Survey of Architectures and Technologies Communications Magazine IEEE 9(17), 48(6) 92-101

[12] Ji E K, Barth T and Boulous G 2017 Seamless integration of heterogeneous devices and access control in smart homes and its evaluation International Conference on Intelligent Environments IEEE pp 206-213

[13] Chen Y and Luo B 2012 S2A:secure smart household appliances ACM Conference on Data and Application Security and Privacy ACM 217-228

[14] Han K, Kim J and Shon T 2013 A novel secure key pairing protocol for RF4CE ubiquitous smart home systems Personal and Ubiquitous Computing 17(5) 945-949

[15] Geetha A V and Rajesh Kumar PM 2016 Threshold Cryptography-based Group AuthenticationScheme for the Smart Home Environments (LBS College of Engineering, Kasaragod vol 5) Special Issue 1 Feburary