Securing IoT for Smart Home System

Freddy K Santoso, and Nicholas C H Vun
School of Computer Engineering,
Nanyang Technological University, Singapore.
fred0005@e.ntu.edu.sg, aschvun@ntu.edu.sg

***Abstract*—This paper presents an approach to incorporate strong security in deploying Internet of Things (IoT) for smart home system, together with due consideration given to user convenience in operating the system. The IoT smart home system runs on conventional wifi network implemented based on the AllJoyn framework, using an asymmetric Elliptic Curve Cryptography to perform the authentications during system operation. A wifi gateway is used as the center node of the system to perform the system initial configuration. It is then responsible for authenticating the communication between the IoT devices as well as providing a mean for the user to setup, access and control the system through an Android based mobile device running appropriate application program.**

***Keywords*—IoT; smart home; authentication;**

I. Introduction

Recent advancements in the semiconductor technology have enabled cost effective solutions to directly integrate wireless network connectivity in embedded processors and sensors, which in turn lead to great interest in the Internet of Things (IoT), defined as the networked interconnection of everyday objects. IoT is now considered as the ready technology for the consumer electronics market, and smart home has been touted as one of the market segment with very high potential for IoT deployment, such as to enable home automation and energy management. However, the rate of IoT adoption among home users depends on their willingness to purchase these devices, and convenience and security are identified to be the two key factors influencing their decision[1]. As such, this paper describes the design and implementation of a Wi-Fi based IoT smart home system that uses a gateway to enable secure communication between IoT devices, and to also allow user to configure, access and control the system through user friendly interface running on mobile devices such as the ubiquitous smart phone.

II. System Design Considerations

While many existing home automation system uses ZigBee or Bluetooth for the wireless connection, wifi is also a viable alternative[2][3] due to the introduction of IPv6 that enables the connection of almost unlimited number of embedded devices, and its ubiquitous presence in many CE devices.

Security challenges in IoT include privacy, authentication and secure end-to-end connection[4]. In addition, with the presence of multiple smart home standards currently used in the market, any security scheme needs to consider inter-compatibility among the multiple standards.

Figure 1 shows the setup of the proposed system, consists of a home gateway and several IoT devices connected via a wifi network. The user can access and control the system using a mobile device by accessing the home gateway. The gateway is responsible for authenticating and monitoring the communication between devices in the system. The gateway can also provide translation between different IoT standards at the lower layer while maintaining a common security scheme at the higher layer. Each IoT device can only communicate with the gateway. Based on user preferences, the information from one device can also trigger the gateway to send a message to another device in order to response with appropriate action..

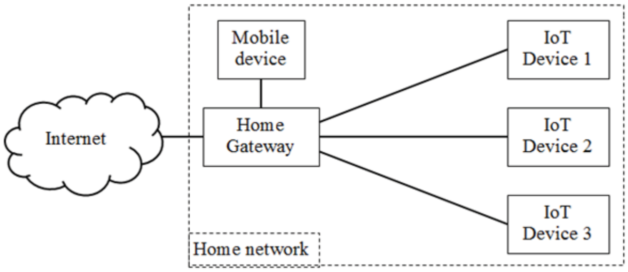

Fig. 1. System Setup.

III. Authentication Process

Authentication is a major challenge in IoT but most CE devices lack a user interface for entering authentication information. As such there is a need for a convenient and robust authentication procedure for the smart home system. One such approach is the use of public key mutual authentication protocol [5], with pre-shared keys between a gateway and a new device, based on the procedure shown in Figure 2.

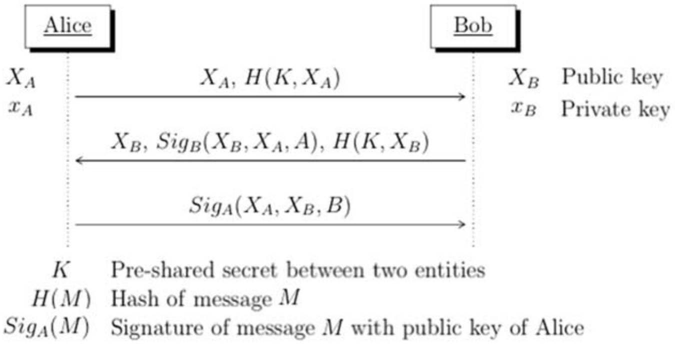
Alice
Bob
X_A
x_A
X_B Public key
x_B Private key
X_A, $H(K, X_A)$
X_B, $Sig_B(X_B, X_A, A)$, $H(K, X_B)$
$Sig_A(X_A, X_B, B)$
K Pre-shared secret between two entities
$H(M)$ Hash of message M
$Sig_A(M)$ Signature of message M with public key of Alice

Fig. 2. Authentication Procedure [5].

978-1-4673-7365-4/15/$31.00 ©2015 IEEE

The protocol uses Elliptic Curve Cryptography due to its high security level per key size while the use of pre-shared secret keys (*K*) removes the need to establish additional public key infrastructure for the system. After the authentication process is done, both parties can then use Elliptic Curve Diffie-Hellman (ECDH) operation to create a shared key for the subsequent symmetric encryption. Mobile devices can be used to facilitate the authentication process for devices with restricted user interface [6].

IV. System Operation and Implementation

The system initially only consists of the gateway in the home network; IoT devices have yet to be connected, while the user operates a wifi enabled mobile device (e.g. Smart phone) which can communicate with the gateway. Two rounds of authentication are needed. The first round is to authenticate the mobile device with the IoT device in order for the mobile device to share the home network credentials with the device. The second round is to authenticate the IoT device with the home gateway to establish connection for subsequent communication. All authentication rounds follow the protocol as indicated in Figure 2.

For the first authentication round, the user first obtains and loads the identity and the pre-shared secret key of the IoT device to the mobile device. Device identity can be any unique information of the device, e.g. device ID. The user then turns on the IoT device, which automatically starts in wifi access point (AP) mode, which allows it to be connected to the mobile device to start the authentication process. After both devices are mutually authenticated, the mobile device sends the home network credentials and the gateway location to the IoT device. The IoT device then connects to the home gateway to be ready for the second round of authentication.

To prepare for the second round of authentication, the user has to load the identity and the pre-shared secret key of the IoT device to the home gateway (using the mobile device). When an IoT device first contacts the gateway, the gateway only starts the authentication process if it has the identity and the pre-shared secret key of the device. Once this authentication process is completed, a shared key is created for both parties, which is to be used in their subsequent communication.

Communication between devices is performed based on the User Datagram Protocol (UDP). Before data is sent, the message is encrypted through symmetric cryptography (e.g. Advanced Encryption Standard (AES)) using the shared key created by the ECDH process. As each device only needs to store one shared key to communicate with the gateway, it reduces the storage burden on the IoT device.

During operation, each device in the system can advertise a list of events and actions to the gateway after the device setup. Events refer to the information obtained from the device (e.g. the device is on) while actions refer to the methods provided by the device (e.g. turn on/off the device). The user can access the gateway via the mobile device to get the list of events from all devices and setup different response actions for different devices. It is also possible to set an automatic rule in the gateway to select a certain sequence of actions when triggered by event(s) generated by a device.

A prototype system consists of a simple wifi enabled IoT device, an IoT gateway and an Android smartphone is setup to demonstrate the practical feasibility of the proposed idea. The IoT device consists of wifi enabled STM32F4 ARM Cortex-M4F microprocessor. The Raspberry Pi Linux computer board with wifi transceiver is used to implement the home gateway. An app is developed and is installed on an (Galaxy Note GT-N7000) Android smartphone, which allows the user to add new devices to the system by entering the device ID and pre-shared key.

AllJoyn framework [7] is used as a base for the implementation. It is an open source IoT framework developed by Linux Foundation and AllSeen Alliance, with support for multiple devices and different operating systems, as well as useful libraries for various operations e.g. adding new IoT device, cryptographic operations (ECC, AES), etc.

V. Summary

Security and convenience are two major requirements for successful deployment of IoT in a smart home environment. This paper proposes and implements a smart home system based on wifi network. Using the AllJoyn framework as the base, the proposed system uses a gateway to provide a better authentication process and a convenient interface for the user via an Android device.

However, the current method of entering device ID, pre-shared secret key and AP name by hand during the addition of a new device is inconvenient to the user, even though this process is only to be performed once for each device. A possible improvement to perform this procedure is to embed the relevant information of each device in a QR code on the device, which can then be scanned and read by the Android application initiated by the user.

References

[1] Y., Dong, X., & Sun, W. Chang, "Influence of characteristics of the Internet of Things on consumer purchase intention," *Social Behavior and Personality: an international journal*, vol. 42, no. 2, pp. 321-330, 2014.

[2] X. Zhao, "The strategy of smart home control system design based on wireless network," in *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, vol. 4, 2010, pp. V4-37.

[3] R., Pecorella, T., Viti, R., & Carlini, C. Fantacci, "Short paper: Overcoming IoT fragmentation through standard gateway architecture.," *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 181-182, 2014.

[4] M., & Koien, G. M. Abomhara, "Security and privacy in the Internet of Things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, 2014, pp. 1-8.

[5] M. Noack, “Optimization of Two-Way Authentication Protocol in Internet of Things”, M.S. thesis, Dept. Informatics, University of Zurich, Zürich, Switzerland, 2014.

[6] J. Suomalainen, "Smartphone assisted security pairings for the Internet of Things," in *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014 4th International Conference*, May 2014, pp. 1-5.

[7] AllJoyn Framework. [Online]. Available: https://allseenalliance.org/.

978-1-4673-7365-4/15/$31.00 ©2015 IEEE