Analyses of Secure Authentication Scheme for Smart Home System based on Internet on Things

Jung Tae Kim

Mokwon University
Dept. of Electronic Engineering, Mokwon University
Doanbook-ro 88, Seo-gu, Daejeon, South Korea

(82)42-829-7657 and jtkim3050@mokwon.ac.kr

Abstract

Recently, advanced technologies in the semiconductor process have a great developed with nano technology. It enabled cost effective solutions to directly integrate wireless network connectivity with embedded processors and sensors. From the improved technology, IoT lead to great interest in the the field of inforamtion and communication technology, It is defined as integrated, fused and networked interconnection with objects. Security challenges in IoT include privacy, authentication and secure end-to-end connection. In addition, with the presence of multiple smart home standards currently used in market, any security scheme needs to consider inter-compatibility among the multiple standards. We analyzed and surveyed critical issues for technologies and securities of IoT, and discussed the applications and challenges of smart home network and related to IoT systems. Finally, to provide secure authentication procedure, we proposed the security protocol in IoT service in this paper.

Key words: IoT, Internet of things, Smart Home Network, Authentication, Security

Introduction

The term of IoT was first introduced by Kevin Aston. It was introduced by concept of the internet of things (IoT) at MIT's AutoID lab in 1999. The internet of things is understood to be a global network infrastructure. It is composed of linking physical and virtual objects through internet network. The information is interconnected by sensing technique and operability between device and device. These kinds of infrastructures include existing, internet attached and network developments. It provides specific object-identification, sensor recognition and connection capability with independent cooperative services and applications. The characteristics of sensing in IoT can be classified by a high degree of independent data capture, event transfer, network connectivity and interoperability. Previous works are discussed from the point of view regarding to secure transmission problems in the wireless sensor network [1]. The Internet of Things is composed with RFID, WSN, sensors, Internet and other network. Information security issues in IoT become more complicated and essential. Traditional and existing security in single network environment can't support enhanced secure data exchange in IoT. In general, we consider that privacy and data protection and information security are complementary requirements for IoT services. In particular, information security is regarded as providing confidentiality, integrity and availability. IoT is now considered as the ready technology for the consumer electronics 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 the two key factors influencing their decision. To implement enhanced secure communication between IoT devices, we have to solve the problems such as access control and interface how to connect running on mobile devices such as the ubiquitous smart phone.

Architecture of smart home network

We analyzed component of security architecture with relationship ISO7 layer, sensor protocol stack and security requirements as shown in figure 1.

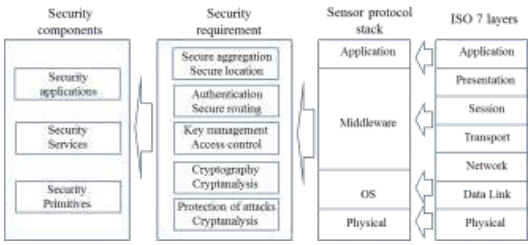

Fig. 1 Basic component of Security Architecture

Position figures and tables are at the second page, if possible.

Example of IoT based smart home network is described in figure 2. There are many consideration matters in inner home networks. The critical point is vulnerability and attack. We cannot implement existing and conventional cryptography techniques. The resources are restricted with limited small memory and low power computing capability. This occurs imperative and critical security issues [2].

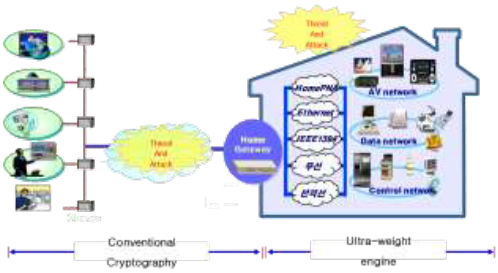

Fig. 2 Example of IoT based Network Topology.

We have to improve secure relation between device and device with its network areas, respectively.

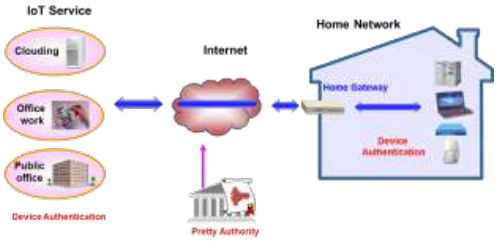

Fig. 3 Example of Secure Authentication Procedure Model on Smart Home Network

The security of necessity in authentication level can be classified authentication and authorization part. The representative characteristics are shown in figure 1.

Security mechanism	Authentication method	Security mechanism
Authentication	User's authentication	- PKI, OTP, certification of official recognition - Home gateway authentication - Fingerprint, vein
	Service authentication	Authentication between home service provider and home service
	Device authentication	- Authentication by certification - Home gateway is operated as authentication server
Authorization Access control	User's access control	- Access control by policy of security level - Access control profile by security level
	Device to device authentication	Necessity of access control between heterogeneous device
	Perception of situation Access control	- Restriction of user's service - Access control by location based service

Fig. 4 Characteristics of authentication method

Computing service under ubiquitous surrounding should be considered with vulnerability and services viewpoints. The major factors are follows [3].
- Confidentiality
- Authentication and access control
- Integrity and Non-repudiation
- Availability and survivability
- Privacy and authority control
- Freshness

Also threat factors can be considered as follows.
- Sensor node attack
- Eavesdropping
- Sensing data privacy
- Denial of service

We give a brief of characteristics of smart home network and described as follows.
- Home-network may not be an isolated sub-network
- WiFi & PLC signals may propagate to the next door
- Different network/addressing scheme
- IP address vs Group/node ID
- Some devices have low computational power and memory
- No public key cryptography

To enhance high level of security, we have to consider intrusion protection and detection in sensor network. Especially, home gateway should be required advanced security framework, authorized control, privacy and resilience of survival.
Heterogeneous connection between devices under IoT cannot provide with conventional cryptography techniques. We cannot utilize existing PKI and lightweight schemes. Many researchers should focus on following techniques in the future relating to smart home network security.
- Integration of security on middleware
- Develop new security function beyond security function of Middleware
- Analyze safety about middleware security function
- Lightweight algorithm
- Provide user's convenience

Conclusions

We analyzed security requirement regarding to secure authentication scheme between device and device. Heterogeneous connection and interconnected devices under IoT surroundings cannot provide with conventional cryptography and security engine. Therefore we have to choose another idea and scheme with light-weight algorithm.

Acknowledgments

This research was supported by Basic Science Research Program through the National Re-search Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Number: 2015R1D1A09061435)

References

[1] Se-Hwan Kwon and Dea-Woo Park, Hacking and Security of Encrypted Access Points in Wireless Network, Journal of Information and Communication Convergence Engineering (JICCE), Vol.10, No.2, pp.156-161, 2012
[2] Hui Suo, Jiafu Wan, Caifeng Zou and Jianqi Liu, Security in the Internet of Things: A Review, 2012 International Conference on Computer Science and Electrics Engineering, pp.648-651, 2012I. S. Jacobs and C. P. Bean, *Magnetism*, 3, G. T. Rado and H. Suhl, Eds., New York: Academic Press, 1963, pp. 271-350.
[3] Jung Tae Kim, Analyses of Vulnerability for Healthcare System on Internet of Things, The 3rd Asia Workshop on IT Convergence of KIICE2017, pp.87-88. 2017

 ISBN 978-1-5090-4897-7