Advanced Science and Technology Letters
Vol.64 (Security 2014), pp.51-54
http://dx.doi.org/10.14257/astl.2014.64.13

Security and Privacy Issues of Element Technologies on Internet of Things

Jung Tae Kim

[1] Dept. of Electronic Engineering, Mokwon University,
800, Doan-dong, Seo-gu, Daejeon, South Korea
jtkim3050@mokwon.ac.kr

Abstract. The meaning of Internet of Things (IoT) refers to unique identified objects which can interact with other object through wireless and wired communication. The concept of Internet of Things (IoT) has been proposed and studied as a mean to provide communication in different types of physical objects that support our daily activities. The Internet of Things (IoT) is the development production of the computer science and communication technology. As IoT is broadly used in many fields, the security of IoT is becoming especially important and critical issues. The IoT is required for a new paradigm of security, which should consider the security problem.

Keywords: RFID, Healthcare system, Security protocol, Privacy, IoT

1 Introduction

Current Internet is a collection of uniform and individual devices, IoT (Internet of Things) can be merged with much higher level of heterogeneous connection, as objects of totally different functionality, technology and application fields under same communication environment. Internet of Things means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocol. It is possible to identify distinct macro-trends that will shape the future of IT, together with the explosion of ubiquitous devices that constitute the future of IoT [1, 2]. In terms of the security, the IoT will be faced with more severe challenges. There are the following reasons: 1) the IoT extends the internet through the traditional internet, mobile network and sensor network and so on, 2) every 'thing' will be connected to this 'internet', 3) these 'things' will communicate with each other. Therefore, the new security and privacy problems will arise [3]. Explosion of the amount of data collected and exchanged can be deluged. Due to limited resources, energy required to operate intelligent devices should be minimized. The sensor devices will become increasingly smaller. To operate the devices with autonomic management, the devices and systems should have self-management, self-healing, and self-configuration capabilities. Especially, the network would be based on IPv6 as an integration layer.

ISSN: 2287-1233 ASTL

2 Challenges of Internet of Things

First, the key elements of Internet of Things are as follows and should be take into account with requirement of necessity [4, 5].

a) Energy: issues related with energy such as energy harvesting and low-power chipsets are critical and major concerns to the development of IoT.
b) Intelligence: devices should have capabilities such as context-awareness and co-operated communication to reach neighbor sensor devices.
c) Communication: new, smart multi-frequency band antennas, integrated on-chip and made of new materials are the communication means that will enable the devices to communicate.
d) Integration: integration of smart devices into the products themselves will reduce a significant cost saving and increase reduced dimension.
e) Interoperability: protocols for interoperability have to be standardized.
f) Standards: open standards will be the key enablers for the success of the IoT. Energy-efficient communication standards are needed. Also security and privacy use compatible or identical protocols.

3 Characteristics security issues of Internet of Things

Cryptosystem is basis of information security. In the traditional network, there are two uppermost forms of cryptographic applications such as point to point encryption and end to end encryption. As far as we know, their system can be merged with the IoT framework [6, 7]. Generally, the node of sensor layer is low speed CPU such as single chip system. Encrypt and decrypt programs cannot use large storage and high-power. So Encryption mechanism in IoT should be lightweight. Compared with traditional network, sensor nodes in IoT deployed in an unattended environment, there are some new characteristics in sensor network. First, wireless link signal is very weak. Second, node is exposed. Third, network topology is dynamic [8]. Emergence of IoT will generate only when strong security solutions are in place. The standards must define different security features to provide confidentiality, integrity, or availability of services. The issues related to identity objects must be dealt with in politics and legislations. Enablers of Internet of Things have following characteristics [9].

a) Manufacturing, logistics and retail sectors: product authentication and anti-counterfeiting, next-generation industrial automation and supply chain management, inventory management, track & trace, remote maintenance, service and support.
b) Energy and utilities sectors smart electricity and water transmission grids, real-time monitoring of sewage systems, efficient energy and water consumption at homes enabled by connected devices to the grid.
c) Intelligent transportation systems support for vehicular ecosystems, use of in-vehicle sensor networks, telematics, GPS and wireless networks for developing smart vehicles, vehicle-to-vehicle and vehicle to roadside communication for

collaborative road safety and efficiency, vehicle tracking, traffic data collection for traffic management etc.

d) Environment monitoring systems wireless sensor nodes to monitor weather, environment, civil structures, soil conditions etc.
e) Home management and monitoring use of sensor nodes, smart applications, wireless networks, home gateways for applications such as home security, elderly care, smart energy control etc.

4 Enhancing of security and privacy

IoT should be needed a variety of different layers of the architecture and considered from different aspects of information security [10]. The representative consideration included security structure, key management, security law and Regulations. Security of information transmission in the Internet of Things is mainly related with the security of network hierarchy [11, 12]. The major role of network hierarchy is to transmit and communicate information, including the access layer and the core layer. The security of network hierarchy in the Internet of Things can mainly be divided into two categories: The first factor is the intrinsic potential safety hazard of the Internet of Things, while the second factor derives from security vulnerabilities and protocol defects in the technologies for constructing and realizing the hierarchical functions. The major issues of network hierarchy are security issues in operational flow model, air interface and network architecture [13]. In terms of privacy of communication and user data, a number of technologies have been developed to achieve information privacy goals. The representative privacy enhancing technologies (PET) are as follows.

a) Integrating policy-based release of data
b) Virtual Private Networks (VPNs): impractical beyond the borders of the extranets.
c) Transport Layer Security (TLS): as each ONS delegation step requires a new TLS connection, the search performance will be affected by introduction of additional layers.
d) DNS Security Extensions (DNSSEC):
e) Onion Routing
f) Private Information Retrieval (PIR)

5 Conclusions

The use of a mobile device such as NFC, RFID tag and small sensor nodes in hospital environment offers an opportunity to deliver better services for patients and staffs. Furthermore, medical errors will be reduced because u-health system helps to verify the medical procedure. As mentioned above, the security challenges for the IoT are severe. It is necessary to establish optimized security structure. The key management in the real large-scale sensor network is always a challenge, and the policies and regulations related to the IoT will also be a challenge matters.

Acknowledgments. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2011-0026950)

References

1. Young-Jae Park, et al, “On the Accuracy of RFID Tag Estimation Functions”, Journal of Information and Communication Convergence Engineering, March, pp.33-39 (2012)
2. Yang Xiao, et al, Security and Privacy in RFID and Applications in Telemedicine”, IEEE Communications Magazine, April, pp.64-72 (2006)
3. Hui Suoa, Jiafu Wan, Caifeng Zoua and Jianqi Liua, "Security in the Internet of Things: A Review", 2012 International Conference on Computer Science and Electronics Engineering, pp.648-651 (2012)
4. Shinyoung Lim, et al, “Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring”, 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing”, pp.327-332 (2010)
5. Wen Yao, Chao-Hsien Chu and Zang Li, “The Use of RFID in Healthcare: Benefits and Barriers”, IEEE International Conference on RFID Technology and Applications, pp.128-134, June (2010)
6. Jeonggil Ko, et al, “Wireless Sensor Networks for Healthcare”, Proceedings of the IEEE, v.98, n.11, pp. 1947-1960 (2010)
7. Lenka Lhotska, et al, “Security Recommendations for Implementation in Distributed Healthcare Systems”, ICCST2008, pp.76-83 (2008)
8. Quangang Wen, Xinzheng Dong and Ronggao Zhang, "Application of Dynamic Variable Cipher Security Certificate in Internet of Thing", Proceedings of IEEE CCIS2012, pp.1062-1066 (2012)
9. Azzedine Boukerche and Yonglin Ren, “A Secure Mobile Healthcare System Using Trust-based Multicast Scheme”, IEEE Journal on Selected Areas in Communications, v.27, n.4, pp.387-397, May (2009)
10. Hui Suoa, Jiafu Wana,Caifeng Zoua and Jianqi Liua, "Security in the Internet of Things: A Review", 2012 International Conference on Computer Science and Electronics Engineering, pp.648-651 (2012)
11. Wiem Tounsi, et al, “Securing the Communications of Home Health Care System based on RFID Sensor Networks”, 8th Annual Communication Network and Services Research Conference, pp.284-291 (2010)
12. Yanjun Zuo, “Survivable RFID Systems: Issues, Challenges, and Techniques”, IEEE Transactions on Systems, Man, and Cybernetics- part C: Applications and Reviews, v.40, n.4, pp.406-418. July (2010)
13. Lan Li, "Study on Security Architecture in the Internet of Things", 2012 1ntemational Conference on Measurement, Information and Control (MIC), pp.374-377 (2012)

