Security and Privacy on Internet of Things

Zejun Ren, Xiangang Liu, Runguo Ye
Information Security Research Center
China Electronics Standardization Institute
Beijing, China
{renzj, liuxg, yerg}@cesi.cn

Tao Zhang
College of Information Science and Engineering
Ocean University of China
Qingdao, Shandong Province, China
oucseczt@126.com

Abstract—**There are billions of Internet of things (IoT) devices connecting to the Internet and the number is increasing. As a still ongoing technology, IoT can be used in different fields, such as agriculture, healthcare, manufacturing, energy, retailing and logistics. IoT has been changing our world and the way we live and think. However, IoT has no uniform architecture and there are different kinds of attacks on the different layers of IoT, such as unauthorized access to tags, tag cloning, sybil attack, sinkhole attack, denial of service attack, malicious code injection, and man in middle attack. IoT devices are more vulnerable to attacks because it is simple and some security measures can not be implemented. We analyze the privacy and security challenges in the IoT and survey on the corresponding solutions to enhance the security of IoT architecture and protocol. We should focus more on the security and privacy on IoT and help to promote the development of IoT.**

Keywords-security; privacy; internet of things (IoT)

I. INTRODUCTION

As an emerging technology, Internet of Things (IoT) is defined as a network with everything that can connect to the Internet, such as light bulbs and temperature sensors. Gartner[1] says that there are more than 6 billion IoT devices connecting to the Internet and the number will be more than 26 billion. And the IoT industry will generate about 300 billion revenue by 2020. IoT technologies can be applied in different fields, such as agriculture, healthcare, manufacturing, energy, retailing and transportation. And IoT has been changing the world, the way we live and companies do business.

Everything is a double sword, so does the IoT. The introduction and development of IoT can bring us both good service and bad effects. In Oct 2016, Dyn, a Domain name system (DNS) service provider, encountered a severe DDoS (Distributed Denial of Service) attacks which disrupted uninterrupted service of many important websites such as Amazon, Twitter, Facebook. And the source of the attack is partly from the Mirai botnet with thousands of compromised IoT devices. More than 5000 IoT devices in a university campus ranging from light bulbs to vending machines are used to launch attacks on DNS queries[2]. Without proper protection, IoT devices are more likely and easily to be attacked and used for malicious purposes and we should take more consideration on IoT security and privacy protection.

II. IOT AND KEY TECHNOLOGIES OF IOT

A. Definition

ITU defines IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [3]. We can simply understand IoT as smart things such as sensors are connected to the Internet. As the technology evolves, Internet of everything will be an extension of IoT.

B. Architecture of IoT

There is no uniform IoT architecture and many architectures have been proposed in the past years, including generic architecture and ITU architecture. All these architectures of IoT are multi-layer architectures. The generic architecture of IoT are composed of four layers, including perception layer, network layer, middleware layer and application layer. ITU IoT architecture[4] is a five layer architecture, the sensing layer, access layer, network layer, middleware layer and application layer. The following is a brief introduction of the four layer generic IoT architecture.

Perception layer. The perception layer is the foundation of IoT architecture, and the main infrastructure includes sensors, tags, barcode and so on. The data transmitted on the network layer is collected from sensors of the perception layer.

Network layer. The network layer is responsible for transmitting data collected from the sensors of the perception layer, such as temperature data from temperature sensors.

Middleware layer. The middleware layer is service oriented which ensures same service type between the connected devices.

Application layer. Smart home, smart city, smart transportation and smart hospital are typical applications of IoT.

C. Key Technologies of IoT

The key technologies of IoT include Electronic Product Code (EPC), short range wireless technologies, and wireless sensor network. Some emerging technologies like cloud computing, IPv6, artificial intelligence also have great effect on the development of IoT.

1) E-code and Electronic product code

E-code. Barcode and QR code are the most widely used e-code in the IoT systems. E-code is a symbol attached to the object which can be identifiable and read by the scanner. E-code can be read by many kinds of devices, such as specific devices or smartphone with Internet access.

Electronic Product Code (EPC). EPC[4] is a 64 bit or 98 bit code electronically recorded on an RFID tag, which is an improvement in the EPC barcode system. EPC can store information about the type of EPC, unique serial number of products, specifications, manufacturer information, etc.

2) Short range wireless technologies

The most widely used short range wireless technologies in the IoT are Radio Frequency Identification(RFID), Near Field Communication (NFC), WiFi, Bluetooth, Zigbee, IPv6 over LoWPAN (6LoWPAN) and Ultra WideBand.

NFC. NFC[4] is a set of short range wireless technology at 13.56 MHz, at a distance of 4 cm. NFC is the development of RFID and it is typically used for transactions, exchange digital content, connect electronic devices with a touch.

RFID. RFID[5] is the key technology for making the devices unique identifiable, which reduces size and cost and makes it integrated into any objects. The features of small size of RFID tags make it possible to apply into different areas, such as retail and logistic industry.

Bluetooth. Bluetooth is an open wireless technology for PAN(Personal Area Network) operating at 2.4GHz, and it is used for point to point communication. Bluetooth is mainly used for wearable electronic devices, smartwatches, phones, earphones, glasses and shoes.

WiFi. IEEE 802.11 is widely used as WiFi. WiFi is used to send, receive data, signal commands and much more. It works at frequency bands from 2.4 GHz to 60 GHz and the data rates ranges from 1Mb/s to 54 Mb/s. WiFi can be against landscape and environmental constraints, which is an advantage against wired infrastructure.

Zigbee. Zigbee is designed for small, low power radios based on IEEE 802.15.4-2003 WPAN standard, which is regarded as a low power version of WiFi. It operates on unlicensed bands including 2.4GHz, 900MHz and 868 MHz. Zigbee is the first choice by many IoT applications as communication protocol.

6LoWPAN. With the new features like larger address space, simplified header, flexible extension option, better support for security and mobility, Internet Protocol version 6 (IPv6) is designed as the next generation Internet Protocol to replace IPv4[6]. 6LoWPAN[7] is the combination of IPv6 and low power WPAN. For constraints like small code size, low power operation in the wireless network, 6LoWPAN is introduced in 2007 as a low energy IoT protocol and it plays a major role in IoT wireless communication.

Ultra-wideband. Ultra-wideband (UWB)[8] is a radio technology that can use a very low energy level for short-range, high-bandwidth communications over a large portion of the radio spectrum. UWB transmits data spread over a large bandwidth and does not interfere with conventional narrowband and carrier wave transmission in the same frequency band.

TABLE I. SHORT RANGE WIRELESS TECHNOLOGY

	NFC	**WiFi**	**Bluetooth**	**ZigBee**	**6LoWPAN**	**Ultra WideBand**
Standards	ISO / IEC 18000-3	IEEE 802.11	IEEE 802.15.1	IEEE802.15.4	RFC4919	-
Frequencies	13.56MHz	2.4GHz/5GHz	2.4—2.483GHz	2.4GHz	2.4GHz	3.1-10.6GHz
Range	10~20cm	100m	~10m	10～100m	-	~10m
Data rates	100-420kbps	54Mbps	2Mbps(max)	250kbps(2.4GHz), 40kbps(915 MHz), 20kbps(868 MHz)	-	100Mbps
Max node number	2 (point to point)	~	8	65000	2^{128}	-

3) Wireless sensor network(WSN)

WSN[9] is composed of WSN hardware, communication stack, and software. There are many nodes in the IoT and WSN is the most important part of IoT architecture.

4) Cloud computing

With billions of IoT devices connected to the Internet by 2020 and data generated from these IoT sensors will be huge. And where can we store these data and how to process these real time data like stream audio and video data? It is likely that only the cloud computing can provide increasing and flexible storage capacity and analyze these data timely and effectively. So cloud computing will play an important role in the future IoT architecture[10].

5) Other technologies

Artificial intelligence. Artificial intelligence can help to tailor embedded IoT devices to be more intelligent, such as adapt to changes in response to the owner, be context aware, even can recognize the situation. AI can also help decrease the number of redundant sensors and assign the storage more reasonable.

III. PRIVACY AND SECURITY CHALLENGES IN THE IOT

IoT is an extension of Internet and Internet is not secure enough. With new features introduced, there will be more security and privacy challenges in the application of IoT. There should be more consideration on IoT security, because IoT security can cause a disaster to us, such as DDoS attacks from Mirai botnet. IoT devices with access to the Internet are more vulnerable to attacks, because IoT devices have less protection

than PCs and smartphones. To reduce cost, manufacturers focus only a little on IoT device security and IoT devices have only simple functions and traditional security solutions are not applicable, such as firewall.

A. Perception Layer

Physical security. The IoT devices such as sensors are always placed in one place for a long time, which may be attacked physically. What's worse, some security plans can't be implemented. IoT devices, like smart TVs, video game devices, and smart wearable devices, are collecting data about us and data may be shared or accessed by unauthorized parties.

There are some potential threats in the perception layer, such as unauthorized access to tags, tag cloning, eavesdropping, spoofing, RF jamming. The RFID system is simple and there is no authentication mechanism in the RFID system, so the data on the tags is easily to be changed. Tag cloning is possible because the reader can't distinguish between the original and cloned tags.

B. Network Layer

Attacks on the network layer include sybil attack, sinkhole attack, sleep deprivation attack, denial of service (DoS) attack, malicious code injection, and man in middle attack[11]. Attacks on the WSN can be insider attacks and outsider attacks. The insider attacks can be compromised nodes that are controlled by malicious attacks.

Middle-ware layer. The layer is composed of data storage technologies and data may be accessed by unauthorized parties and malicious insiders. DoS attacks on the middle-ware layer may result in unavailability of services.

C. Application Layer

CoAP[12](Constrained Application Protocol) is an application layer protocol and is a customized and compressed version of HTTP protocol which is estimated to be the future of application protocols. The security of CoAP depends on the Data Transport Layer Security (DTLS) and sometimes IPSec. However, the cost of computation and handshake in the message are heavy and may cause message fragmentation. DTLS is lacking in some areas and it is a potential threat for the CoAP.

D. 6LoWPAN Security

6LoWPAN is based on IPv6 and 802.15.4 and IPv6 is not secure as we thought. Neighbor discovery protocol is a basic protocol of IPv6 protocol stacks and is vulnerable to various attacks such as DoS, DDoS, replay and redirect attacks[6]. 6LoWPAN is vulnerable to hidden and exposed wormhole attacks[11].

E. Cloud Security

With the combination of IoT and cloud, the security for the cloud should be considered. The cloud computing faces some technologies risks and legal risks, such as storage of resource, isolation failure, malicious insiders, loss of keys and data protection[13]. With node compromise attacks, malicious attackers can extract secret keys from the compromised IoT devices and the keys can be used to attack other devices in the same local WSN.

F. Privacy

IoT devices are closely related to our daily life and these devices can generate large amount of valuable information which may be collected by manufacturers, vendors or other interested parties. These data have our private information, such as location information, health conditions information from smart bracelet. Some claims that IoT brings more privacy concerns than foreseeing benefits[10].

Unauthorized access to data[14]. RFID tags and EPC contain the identification data, which may disclose confidential information about the user. These tags may be read by a miscreant reader, modified or damaged, such as RFID virus.

Some IoT devices may have private information about public and people[15], such as cameras on the public places. With more IoT devices connecting to the Internet, more privacy about us will be exposed to the public and malicious attackers. IoT devices like sensors are collecting data at very high frequency, then store data on the cloud or other places. When data was stored on the cloud, the owner will lose control of the data, too. These data include the identity data, location data and other privacy information. The location privacy may disclose our living habit. And our private information need more protection.

IV. SOLUTIONS

Kumar[16] proposes two Secure Split Test (SST) techniques to mitigate IC counterfeiting, SST with functional testing capability (SSTF) scheme and a Physical Unclonable Function based SSTF (PUF-SSTF). SSTF is designed to mitigate the counterfeits from untrusted foundries. And PUF-SSTF is to address the identity management issue in IoT's and counterfeiting of ICs. The results of experiments show that the two methods can create a comprehensive secure supply chain solution.

Yashiro[17] proposes a new IoT architecture based on Uid-CoAP architecture which integrates existing embedded system with the IoT network. The architecture is applicable to both simple IoT sensor nodes and complex embedded systems.

Legal course of action. European commission passed a legislation in a lawful, ethical way respecting the right to privacy and ensuring protection of personal information, just because it is aware of the security and privacy issues on the RFID and IoT[18]. With the legislation, companies including the cloud service providers should take more on the protection of users' private information and privacy.

Babar[19] proposes an integrated and interrelated prospective on security, trust, privacy and chooses a cube structure as a modeling mechanism for security, trust and privacy on the IoT. The cube structure depicts the convergence of security, trust and privacy. The privacy is composed of respondent privacy, owner privacy, ethical and laws. The security is composed of authorization, identification and

authentication, confidentiality, integrity, non-repudiation and availability. Beliefs, credentials, delegation, recommendation and reputation together form the trust foundation of IoT.

Hardware based protection. A compromised IoT device can be utilized to attack other devices in an unsuspecting victim's network[20]. So it is necessary to enhance the security of IoT devices and cryptography is a good suggestion. However, cryptography adds too much computational overhead and is not practical in simple IoT devices. With the development of memory and CPU, higher memory and CPU will be cheaper and there will be a balance among security, cost and performance.

RFID system is a vital part of IoT system and Li Ye[21] proposes a new mutual authentication protocol based on hash function. The protocol is divided into five phases, initial setup, challenge, T-R response, R-D response, D-R reply and R-T reply. Using hash function, the ID of the tags can be substituted by the randomly chosen nickname which can protect the privacy of the device owners. The protocol is secure against various types of attacks and there is a beneficial compromise during security and efficiency.

Cryptography in WSNs. Cryptography can also be used in WSNs and it can help enhance the security of network. Selecting an appropriate cryptograhic methid is critical because the chosen method should meet the constraints of IoT devices and WSNs. Wang[22] compares the operation time of different kinds of encryption algorithms, including public key cryptography and symmetric key cryptography, average energy cost of digital signature and key exchange computations of public key cryptography. His conclusion is that symmetric key cryptography is faster and consumes less energy than public key cryptography and symmetric key cryptography is preferred in a WSN.

V. CONCLUSIONS

There are billions of IoT devices connecting to the Internet and many of these devices bring potential risks on our privacy. Because these devices generate large amount of valuable information about us, such as location information, motion information and health information. IoT devices and data from them are not under proper protection for cost and other reasons. IoT is an extension of Internet, which brings new security and privacy challenges. As a developing technology, IoT has no uniform reference models and appropriate standards. And some existing security solutions are not applicable to the IoT. The proposed IoT architectures are under various attacks on different layers, such as man in middle attacks, spoofing, unauthorized access to private data. There should be universal standards in architecture, protocol, security and privacy requirements. New security protocols should be proposed to resist network layer attacks,. Cryptography algorithms and key management schemes for IoT devices and WSNs can be helpful to promote the development and adoption of IoT. Only in this way, can IoT develop better and can we achieve more benefits from the technology.

REFERENCES

[1] http://www.gartner.com/newsroom/id/2684616.

[2] http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf

[3] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items

[4] Madakam, S., Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3, 164-173. http://dx.doi.org/10.4236/jcc.2015.35021

[5] U. Farooq M, Waseem M, Mazhar S, et al. A Review on Internet of Things (IoT)[J]. International Journal of Computer Applications, 2015, 113(1):1-7.

[6] Tao Zhang and Zhilong Wang, "Research on IPv6 Neighbor Discovery Protocol (NDP) security," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 2016, pp. 2032-2035. doi: 10.1109/CompComm.2016.7925057

[7] https://tools.ietf.org/html/rfc4919

[8] https://en.wikipedia.org/wiki/Ultra-wideband

[9] ayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, Volume 29, Issue 7, September 2013, Pages 1645-1660, ISSN 0167-739X, https://doi.org/10.1016/j.future.2013.01.010.

[10] In Lee, Kyoochun Lee, The Internet of Things (IoT): Applications, investments, and challenges for enterprises, Business Horizons, Volume 58, Issue 4, July–August 2015, Pages 431-440, ISSN 0007-6813, https://doi.org/10.1016/j.bushor.2015.03.008.

[11] Hon Sun Chiu and King-Shan Lui, "DelPHI: wormhole detection mechanism for ad hoc wireless networks," 2006 1st International Symposium on Wireless Pervasive Computing, 2006, pp. 6 pp.-.doi: 10.1109/ISWPC.2006.1613586

[12] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, 2016, pp. 1-7. doi: 10.1109/ICBDSC.2016.7460363

[13] Zhilong Wang, Tao Zhang, Yu Yang, and Haipeng Qu. 2016. Comparison of Security Frameworks for Governmental Clouds between United States and European Union. In Proceedings of the 6th International Conference on Communication and Network Security (ICCNS '16). ACM, New York, NY, USA, 30-34. DOI: https://doi.org/10.1145/3017971.3017985

[14] U. Farooq M, Waseem M, Mazhar S, et al. A Review on Internet of Things (IoT)[J]. International Journal of Computer Applications, 2015, 113(1):1-7.

[15] P. Suresh, J. V. Daniel, V. Parthasarathy and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," 2014 International Conference on Science Engineering and Management Research (ICSEMR), Chennai, 2014, pp. 1-8. doi: 10.1109/ICSEMR.2014.7043637

[16] K. Sudeendra Kumar, G. Hanumanta Rao, Sauvagya Sahoo, K.K. Mahapatra, Secure split test techniques to prevent IC piracy for IoT devices, Integration, the VLSI Journal, Available online 29 September 2016, ISSN 0167-9260, https://doi.org/10.1016/j.vlsi.2016.09.004.

[17] T. Yashiro, S. Kobayashi, N. Koshizuka and K. Sakamura, "An Internet of Things (IoT) architecture for embedded appliances," 2013 IEEE Region 10 Humanitarian Technology Conference, Sendai, 2013, pp. 314-319. doi: 10.1109/R10-HTC.2013.6669062

[18] Rolf H. Weber, Internet of Things – New security and privacy challenges, Computer Law & Security Review, Volume 26, Issue 1, 2010, Pages 23-30, ISSN 0267-3649, http://dx.doi.org/10.1016/j.clsr.2009.11.008.

[19] Babar S., Mahalle P., Stango A., Prasad N., Prasad R. (2010) Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In: Meghanathan N., Boumerdassi S., Chaki N., Nagamalai D. (eds) Recent Trends in Network Security and Applications. CNSA 2010. Communications in Computer and Information Science, vol 89. Springer, Berlin, Heidelberg

[20] O. Arias, J. Wurm, K. Hoang and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices," in IEEE Transactions on Multi-Scale Computing Systems, vol. 1, no. 2, pp. 99-109, April-June 1 2015. doi: 10.1109/TMSCS.2015.2498605

[21] Ye Li and Fumio Teraoka. 2012. Privacy protection for low-cost RFID tags in IoT systems. In Proceedings of the 7th International Conference on Future Internet Technologies (CFI '12). ACM, New York, NY, USA, 60-65. DOI=http://dx.doi.org/10.1145/2377310.2377335

[22] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," in IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006. doi: 10.1109/COMST.2006.315852