On Privacy Protection at Networking

Li Yang and ChangGen Zhu

Abstract: In recent years, the networking technology, as an important part of the new generation of information technology, has been developing rapidly. It is widely used in environmental monitoring and protection, personal health care, intelligent transportation, food safety traceability, logistics supplement chain management, and many other fields. Networking technology not only makes our lives more convenient, it but also faces many challenges. One of the most important challenges is its security. Since this technology is still in the early stage of development, the security system has not formed. In addition, this can be regarded as the extension and development of the Internet, with reference to some security technologies and strategies of Internet. However, this system contains a large number of different functions, computation and communication capabilities, and a large difference of all kinds of intelligent terminal and many specific application scenarios, which makes it unique, rather through the existing Internet security technology to solve the security problem. Since the networking is still in the process of evolution, there is not unified security architecture. Previous research on the security of networking is based on certain specific things technology and application scenarios (such as sensor networks, RFID systems, etc.), respectively, providing the corresponding solutions.

Keywords: information security; Internet of Things (IoT); privacy protection; information network

At present, a stage of high level of information technology has come. Information technology has changed people's production and living mode and brought digital, convenient and fast service to mankind. Especially, with the emergence of the Internet of Things (IoT) technology, new opportunities and challenges appear. In the integration of three networks, data exchange and processing speed, security and accuracy directly affect the quality of people's production and life. However, Internet of Things is a new type of information network, derived from the traditional Internet technology, and information security problems are inevitable, especially the Internet of Things is currently in the primary stage of development. What’s more, information
security and privacy mechanisms of technical standards are not mature, with its security issues to be resolved. This article introduces the technology and application of Internet of Things, and its RFID information security and privacy protection mechanism has been deeply discussed and studied, which can promote the development and application of the Internet of Things technology, with a positive significance.

1 Internet of Things (IoT) and information security
1.1 Internet of Things Technology and its Applications

Internet of Things technology has become the mainstream of the Internet and the new network technology, and will be the focus of future development of information technology. In the networking of Internet of Things, each network of objects has a specific identity, in order to achieve interactive communication. The number of objects of these things will be larger than the number of nodes in the Internet era. The networking of Internet of Things makes communication between people realized. At the same time, people can achieve many kinds of communication, such as objects - objects, people - objects, the communication between people. Internet of things has greatly expanded the dimensions and depth of information communication. The core technology of the Internet of things includes RFID technology, sensing technology, network communications, network integration, and other technologies. In the future, things exchange will be widely used in the in the kinds of information construction, and will greatly change the human production and living standards, such as intelligent power grid operation and management, intelligent traffic control desire management, intelligent medical systems, intelligent logistics management.

1.2 Internet of things information security

With the rapid development of information technology, the research concerning about this aspect is more and more, wider and wider. In the context of the Internet of Things, the definition of the network information safety is like this: under the given level of security, information systems against malicious behavior or unexpected events, these malicious actions (events) may make the information data storage, transmission and processing endangered. Therefore, in this context, the study of RFID information security and privacy protection mechanism is to protect the Internet of Things in the information system to provide services that are reliable, safe, confidential and controllable state.

2 Internet of Things RFID system security vulnerabilities

2.1 Vulnerability Analysis RFID System security

RFID System, the basis of the architecture of the Internet of things, is the core technology of the Internet of Things. The security of RFID system directly affects the application of the Internet of things technology in the industry. RFID system, as the core module of the Internet of things, shows more system security vulnerabilities. Its main performance is shown in the following: (1) RFID tag structure defects. Due to
the limited structure of RFID electronic tags, its economic cost is low, but it is difficult to ensure a certain degree of security protection. The price of currently and commonly used in RFID tag market is only 10 cents. Its internal structure includes only about 5000 logic gate structure, but only a small number of logic gates can support security features. In fact, to achieve complex encryption algorithms needs 4000 logic gates. Therefore, simple structure doomed RFID tags in the privacy information protection shows great defects. (2) Security flaw of the communication network channel. In the Internet of Things and its applications, wireless network communication channel is the main adoption to complete the transmission of information. However, wireless network channels often provide opportunities for illegal users or hackers. Some hackers may make use of these channels to intercept confidential information, even data tampering with data information. Hackers may also lead to extraneous emission caused by interference of signal channel congestion, thus disrupting normal operation of the information system. (3) Safety defect of RFID reader. In conjunction with the RFID label, readers also meet many security problems, because its structure is simple. It is easy to attempt hackers to forge readers for illegally obtaining the electronic tag information, tampering with, modifying, and destroying the data information of the network information system.

2.2 The main method of attacking the RFID system

RFID tag is an important part of the network information system, with its storage in the commercial value of large amounts of information, but for the illegal users and hackers, with great temptation. Once the origin of information is disclosed or modified, disasters come about. Common methods of attacking RFID systems include:

(1) Data stealing and tracking. If the RFID system and data information of RFID is not encrypted protected, illegal users are likely to use listening, reading and writing device to obtain the label information data and system of commercial information. This kind of attack does not need direct access to the label, but will be able to obtain business information system.

(2) Attack in the course of communication. With data tracking, hackers can attack and intercept the interaction data between tags and systems. Illegal users in the tag and system access reading and writing devices, and steal the identity authentication information, the data information for tampering, destroying and then passing the reader data. The whole process is reasonable.

(3) Clone and deception attack. This type of attack is through legitimating label identity after stealing the label identity authentication information, and then obtaining the data short message within the time (one or more) of reading and writing, or sending a large quantity of data information, making reading and writing system unable to handle and causing the system to crash. In addition, cloning attacks can also make it realized that intercepted data information will be written to the multiple illegal labels.

(4) Denial of service attack. This attack method is similar to the denial of service of Internet. The area between the label and the system communication is
placed at the same frequency of interference signal source. Effects due to the label and reading-writing normal communication between the devices result in system failures, or destroying the commodity retail, the destruction of the transaction process. Or in the short time, a lot of junk data is sent, leading to the system congestion, system paralyzed and unable to provide normal services.

(5) Inactivated tag attack. Usually, it often happens in the mall retail transactions in the process, after the completion of the commodity transaction. It needs to be inactivated tags, so that you can prevent duplication charges. An illegal user may make a device that is to be inactivated by the transaction before the transaction is made.

3 Internet of things information security and privacy protection strategy

Prior to the promotion and application of Internet of Things technology, it should be the first to solve the problem of information security and protection. Privacy information includes basic personal information, identity information, property information, location information, personal beliefs, individual characteristics, etc.. To respect and protect the privacy of individuals is the consensus of the whole society, and it is also a common need. In the field of information security of Internet of Things, research and application of privacy information protection mechanism is of great significance. Specifically, you can start from the following aspects:

(1) Protection of laws and regulations: with legal policy to protect use of personal privacy information of the Internet of Things

(2) Privacy information using the principle: Users should be in a voluntary principle, as well as the need to be with the Internet of Things operators, network operators and other suppliers to reach an agreement to use personal privacy information.

(3) Anonymous identity applications: it is wise to use indirect and anonymous information to replace real name system information, preventing personal privacy information leakage and illegal users for illegal activities or behavior.

(4) Data encryption and decryption: Important data information, such as commodity trading information, personal location information can be protected by using complex encryption and decryption algorithm, by confusing or replacing the privacy of information to prevent unauthorized users from stealing.

4 Conclusion

Internet of Things technology has become a new generation of information technology with the Internet, mobile network. Broad application prospects, development and application of Internet of Things has important significance in the promoting of social economy. Research on RFID system security vulnerabilities and the development of information security protection mechanism can help to improve the robustness and security of the Internet of Things information system.
**Fund:** Jiangxi provincial project of Humanities and social science, 2015, “Environment protection of privacy at Networking” (project number: JC169).

**References**


[4] Ge Weiping; Wang Wei; Shi Bole; Zhou Haofeng; based on privacy preserving classification mining [J]; computer research and development; 2006 01.


[7] Liu Heng; Wang Tiejun; Zhou Mingtian; she Kun; in pervasive computing environment based on the role of privacy protection system design [J]; microelectronics and computer; 2010 12.