The Analysis and Research on the Internet of Things Security Issues

Xinyue XU

Electronics and Information Engineering School, Anhui University, Hefei, China
xuxinyuekelly@163.com

Keywords: The Internet of Things,Perceiving Layer,Network Layer,Application layer

Abstract: Nowadays, the Internet of Things technology has become a global hot topic. With the widespread applications of the Internet of Things, security issues attract people’s attention. Firstly, the article introduces the concept, three layers and functions of the Internet of Things. Secondly, the article analyze and study the Internet of Things security issues from the angle of perceiving layer, network layer, application layer, and illustrate some domestic existing solutions. Finally, summarizing and imagining the development of the Internet of Things in the future.

Introduction

The birth of the Internet of Things (IoT) is based on computer and Internet technology, including multiple technologies, such as computers, communications, networking, intelligent computing, and sensors. November 2005, the International Telecommunication Union (ITU) released a report, formally presented the Internet of Things (IoT), causing widespread concern around the world. Although the report did not make a clear definition of IoT, the report explains the concept from functional and technical two aspects. From functional aspect, ITU think that "all objects are available to exchange information through the Internet, to achieve omnipresent networking and omnipresent computing, and to make any object can interconnect anytime and anywhere.” From technical aspect, ITU think that "the IoT relates to Radio Frequency Identification technology (RFID), Sensor technology, Nanotechnology and Smart technology and so on." This show that IoT integrates a variety of sensing, communications and computing technology, not only making communication between human to human (H2H) more convenient, but also making communication between human to thing (H2T), thing to thing (T2T) become possible. At last, making human society, information space and the physical world integrated.

The layer of the Internet of Things

Based on the analysis of domestic and foreign authoritative experts of IoT, the IoT is divided into three levels: perceiving layer, network layer, application layer. Perceiving layer use Radio Frequency Identification technology (RFID), Sensor technology, Wireless networks and other networking technology to achieve the identification and collection of information. Sensor network will transmit information collected to the database through the network layer. This layer is considered to be the core of IoT. The network layer is responsible for access and transport functions, divided into access network and transmission network. Network layer needs to transmit information collected from perceiving layer to the database, by the Internet, Wireless Communications Network and so on. The network layer is established on the basis of the existing communication network and the Internet, consisted of the private network, Internet, wireless communication network, cloud computing platform, etc. Application layer is data processing platform, and human-computer interaction interface. The application layer manage, store and analyze large amounts of data transmitted from the network layer in information processing platform. Application layer implement the result from information processing platform, through middleware, virtualization, cloud computing services technology and other advanced technologies and service models, to provide users needed services.

The status of the Internet of Things technology security issues

The application of IoT technology makes the interaction between people and things more obvious, and brings people a lot of convenience. However, IoT is still in infancy stage in our country, there are many issues to be resolved. Many domestic IoT technologies are not perfect, so there are many core technology introduced from abroad. Those technologies are expensive, and there is a risk of leaking state secrets. Currently, the IoT technology did not have uniform industry standards in our country. The IoT product quality is uneven on the market, so the security can not be guaranteed. With the development of IoT technology and application, the management of IoT has become increasingly complex. The IoT contains the communication between human to human, human to thing and thing to thing, and provides a wide range of application, so the security issues become particularly important. Privacy, network security, data processing, communication and other equipment are the focus of monitoring in the process of information transmission. Any part of it damaged will leak a lot of information, and cause incalculable loss.

The analysis of the Perceiving Layer security issues. Security issue is particularly important in the perceiving layer in IoT because the leakage of personal information may happen through this layer. RFID technology allows reader with RFID tags to read each other’s information without contacting. This technology has brought great convenience for intelligent library, intelligent recognition, intelligent logistics and other applications, but there are also very serious security risks. Because usage amount of RFID tag is very large in practical applications, and the cost must be limited within a certain range, so the RFID tag itself does not have the ability to protect their own information, and can not distinguish between legal literacy and illegal signal. This defect is used to steal personal privacy information by lawbreaker. The reader technology of RFID technology is very simple, so it’s easy to be counterfeit. The tag and the reader can have non-contact wireless communication via electromagnetic waves, so the reader can read the tag information from a distance. Many criminals scan in the crowd by bogus reader, which caused a lot of personal information was stolen. Criminals can even make use of information obtained from the RFID tag to track others, which brought great personal safety hazards. During the war, if our location information is stolen by enemy army, it would cause irreparable serious consequences.

Perceiving layer identify and collect information of items by a large number of sensors, which transmit information via wireless communication, without human care, saving labor and costs. However, because most of these wireless devices are set in place of unmanned surveillance, where criminals can easily do bad things, so that a lot of sensor devices and RFID tags are destroyed and theft, and even change their software and hardware. After the attacker steal the radio tag, he will remove the chip package in the laboratory by physical means, and use microprobe to get sensitive signal to forge, copy, tamper RFID tag.

There are thousands of sensor nodes in perceiving layer of IoT. These sensor nodes are difficult to manage because of large quantity, and face serious security threat. These nodes are fragile and changeable. Once the attacker control one node, all information transmitted by this node will be stolen. If the node is tampered by attacker, then the transmission of information will be wrong, resulting in paralysis of the entire network.

As the core part of IoT layer, perceiving layer played a crucial role. But security problems in perceiving layer is the most serious and most difficult to resolve. Currently, researchers have proposed some solution ways, like destroying tags and invalidating tags. When the transaction completed, the RFID tag will automatically void or sleep. However, these ways can only be used for single-use tags, not other items of long-term-use tags, caused great resources waste. We can also use encryption and identification technologies to solve security issues of perceiving layer. The RFID tag and the reader can discern each other, so that each part of the RFID tag only could be read by corresponding part of the reader. We can also use encryption technology to encrypt the contents of RFID tags, so the contents of RFID tags will not be read until corresponding reader send the password. But this technology greatly increases the cost of RFID tags, so it can not put a lot of use. To solve the perceiving layer security issues, we still need domestic researchers' efforts to find better solutions in the future.

The analysis of the Network Layer security issues. The network layer is also known as the transport layer, and is responsible to transmit information via 3G, GSM, Internet, etc. It is network core part of the IoT. The network layer of IoT is based on the Internet, so many attacks for the Internet can also destroy the IoT system, such as viruses, Trojans, worms, scripts, and so on.If the network core of the IoT has been attacked, the solution of IoT information security issues will be impossible. The IoT technology use wireless transmission. However, due to the openness of the wireless channel, the wireless signal transmitted between equipments is very easy to be eavesdropped, disturbed and shielded. The malicious program is very easy to invade in sensor networks and wireless network environment, causing damage.

In order to increase the range of applications of IoT, the network layer use heterogeneous network with a variety of access methods. Although the heterogeneous network increases the variety of accessed network, it also brings a lot of trouble for management. The presence of heterogeneous networks makes network security, network interoperability and network unity worse. The network becomes susceptible, and security becomes weak. Because there are large amount of transmission nodes and transmission data in network layer of IoT system, so the invasion of external programs and interference of transmission is very easy to cause network congestion and denial of service attack.

The network layer is most vulnerable parts of IoT, so security technology for the network layer is very important. Firstly, we need to analyze information transmitted, using data filtering technology to prevent virus or false information mixed into network layer. Secondly, the real-time monitoring and intrusion detection of network transmission process can prevent hacker attacks. We also need to protect key nodes in the network transmission, and establish end to end authentication mechanism to prevent the transmission process being disrupted by attacker. Network layer need to design a series of emergency measures to deal with failures and attacks of network transmission process, and to improve the safety and availability of the system.

The analysis of the Application Layer security issues. The application layer includes data processing center and the application implementation two major parts. There are a wide variety of data processing center in application layer, not only general information processor, but also cloud computing platform which could handle the massive data. Because the cloud computing platform handle large amount of information everyday, so once network interruption, large amounts of data will be lost. The cloud computing platforms include all information acquired from perceiving layer, so information security protection become extremely important. The cloud computing platform contains a lot of personal privacy information, and these privacy need to be recorded and contrasted, so this process is very easy to take mistakes and reveal information. Currently, the domestic IoT technology is always used for logistics management, remote monitoring, agriculture control, emergency rescue, telemedicine and so on. If the encryption mechanism for application information is not perfect, it will be used by criminals to steal trade secrets, patients' privacy information and so on.

If we want to improve the security issues of the application layer, it is necessary to strengthen the data protection for the information processing platform. In terms of technology, establishing and improving access control mechanism of the database, and strictly limiting personnel qualifications accessed database, and carrying on real-time monitoring to the database information. Enterprises should increase awareness of intellectual-property-rights protection, and use digital watermarking technology for patent information, and crack down on the behavior of stealing trade secrets. In addition, we also need to encrypt important information and increase encryption and decryption technology, such as key management, fingerprint identification mechanism, password authentication mechanism. In terms of non-technology, we should strengthen the management and training of personnel to prevent personnel's error leading to leakage of information.

Conclusion

With rapid development of the Internet of things, security issues can not be ignored. The article analyzes and researches on security issues of IoT, and presents a lot of potential risk of networking industry. Only by solving these problems and establishing perfect defense system can a smooth and healthy development of IoT be ensured. Currently, the IoT technology is still in the early stages of development in our country, and there are still a lot of technologies immature. But I believe that with the development of science and technology, the IoT industry is getting better and better in china.

References

[1] ChenHaiming, CuiLi, XieKaibin. A Comparative Study on Architecture and Implementation Methodologies of Internet of Things[J]. Chinese Journal of Computers, 2013(01):168-188

[2] PengYong, XieFeng, GuoXiaojing, SongDanjie, LiJian. Security Problems in the Internet of Things and Their Solutions[J]. Thematic security, 2011(10):4-6

[3] LiZhenshan. The Research of Internet of Things Security Issues[J]. Thematic security, 2010(12):1-3

[4] LiuBo, ChenHui, WangHaitao, FuYing. Security Analysis and Security Model Research on IOT[J]. Conputer and Digital Engineering, 2012(11):21-24