ISSN: 2688-8645

Research on Internet of Things Security Management Platform

Weiming Li, Zongting Wu

Department of Electronic and Information Technology, Jiangmen Polytechnic, Jiangmen, PR China.

Abstract

Internet of Things (IoT) security management platform is mainly to scan and monitor the network layer, sensing layer hardware and application system of IoT, find potential security vulnerabilities and carry out targeted early warning and processing, so as to effectively improve the security of IoT system and reduce the possibility of IoT security incidents.

Keywords

Internet of Things, security, vulnerability scanning.

1. Introduction

The application fields of Internet of Things mainly include industrial IoT, Internet of vehicles, smart home, smart city, smart logistics, etc. While the Internet of Things brings convenience to production and life, the security situation of the Internet of Things is becoming more and more serious. First, there are so many connected devices that it is more and more difficult to prevent them; second, the Internet of Things and the Internet connect the virtual world and the real world together, and attacks in the network may become real injuries in the physical world. According to the prediction of international authoritative consulting institutions, by 2020, 25% of the network security events will be related to the Internet of Things, and the devices, cloud and applications of the Internet of Things may bring security problems, which also shows that the traditional network security method can not meet the threat of network attacks that the Internet of Things may encounter.

2. Major Internet of Things Security Issues

The structure and characteristics of the Internet of Things can reveal its related security issues. The security management platform of the Internet of Things also closely focuses on these security issues. The security issues of the Internet of Things are mainly as follows:

(1) The security of data acquisition and transmission in the sensing layer. Because the design function of sensor nodes is generally single and there are many kinds, it is impossible for them to have high-performance security protection capability.

(2) Traditional security problems in network layer. Although the current network security system is mature, there are still many vulnerabilities. For example, a large number of malicious nodes send data at the same time to cause DoS attacks, so we need to take protective measures in network security to ensure the information transmission security of the Internet of Things.

(3) Application layer security issues. Internet of Things in different application reas will have different complexity and diversity of security issues.

(4) The contradiction between safety and cost. If the cost of each sensor node is too low, there will be a large number of low-performance nodes, which will reduce the security of the sensor network. On the contrary, high-quality and high-performance nodes can improve the security, but the cost of network construction and maintenance will increase accordingly.

ISSN: 2688-8645

(5) Complexity issues. The type of Internet of Things application determines the number and complexity of its security issues, so we should consider the security issues of each layer comprehensively.

3. Platform Key Technology

The Internet of Things security management platform detects the characteristics of the Internet of Things devices through the distributed vulnerability scanning engine. Once the corresponding device type is detected, the built-in vulnerability module will be used for deep vulnerability scanning. The scanning node supports both Linux and Windows systems. The platform is based on the basic research and development of heterogeneous framework. All scanning tools are packaged in the form of plug-ins and loaded dynamically according to the scanning task. The working process is as follows: after acquiring the basic information such as the operating system and open port of the target IoT device, the scanning node uses the vulnerability plug-in to detect the vulnerability of the target system and deal with it. The functions and advantages of the platform are as follows:

(1) Combining big data and machine learning method to model the behavior of Internet of Things devices;

(2) It can repair the network security vulnerability, automatically generate the network topology map, integrate with the existing network infrastructure, realize visual control, and support ACL control of switches, routers and firewalls to complete security defense;

(3) Using the agent-free method, we identify and classify the IoT devices by active and passive discovery methods, and evaluate the security status at the same time;

(4) Realize the security situation visualization of the whole network terminal, real-time monitoring the security situation of the Internet of Things terminal, and use the security centralized management platform to dynamically issue security policies to achieve emergency response.

4. Platform Composition

The Internet of Things security management platform conducts identification and discovery, anomaly detection, access control and security protection for the terminal equipment of the Internet of Things, and centralized monitoring and management, event analysis, global perception and emergency response for the security protection gateway of the Internet of Things. The composition of the platform is as follows:

(1) Vulnerability scanning module of sensing layer of Internet of Things

The main devices in the sensing layer include RFID module, ZigBee module and other wireless sensor devices. Data is mainly transmitted through wireless network, so the signal is exposed in public space. The Internet of Things vulnerability scanning platform has a built-in sensing layer vulnerability scanning module, which mainly integrates various signal scanning tools, and analyzes whether there are monitoring, interception and interference vulnerabilities in the data package.

(2) Internet of Things network layer vulnerability scanning module

The security flaw in the Internet of Things network layer are mainly traditional network security problems. The security of Internet of Things communication network will threaten the confidentiality and integrity of data. Although the existing communication network has relatively complete and secure protection measures, there are still some common problems, including illegal network intrusion, information eavesdropping, integrity damage, DoS attack, virus intrusion, vulnerability attack, etc.

(3) Application layer vulnerability scanning module

ISSN: 2688-8645

Internet of Things has different security problems in different application fields. Although there is no unified standard for the application layer architecture of the Internet of Things, some enterprises have implemented the M2M mode of the Internet of Things, such as smart community, smart home, smart medical, etc. The security problems of application layer are complex, but some common security problems can still be summed up. According to different devices and applications, vulnerability scanning plug-ins are established, and finally the application layer vulnerability scanning module and vulnerability library are formed.

5. Conclusion

This research is a beneficial exploration for the way of Internet of Things security protection. Its application value is to minimize the harm of Internet of Things security and effectively improve the overall security of Internet of Things.

References

[1] E. Bertino and N. Islam, "Botnets and Internet of Things Security," in Computer, vol. 50, no. 2, pp. 76-79, Feb. 2017.

[2] C. Lee and A. Fumagalli, "Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 24-28.

[3] C. Bing, D. Yuebo, J. Bo, Z. Xiang and Z. Lijuan, "The RFID-based electronic identity security platform of the Internet of Things," 2011 International Conference on Mechatronic Science, Electric Engineering and Computer (MEC), Jilin, 2011, pp. 246-249.

[4] Y. Lee, Y. Park and D. Kim, "Security Threats Analysis and Considerations for Internet of Things," 2015 8th International Conference on Security Technology (SecTech), Jeju, 2015, pp. 28-30.

[5] S. Narang, T. Nalwa, T. Choudhury and N. Kashyap, "An efficient method for security measurement in internet of things," 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2018, pp. 319-323.

[6] X. Xingmei, Z. Jing and W. He, "Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of things," Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, Dalian, 2013, pp. 825-828.