Anomaly Detection and Response Framework based on Network traffic and hardware Information of IoT Devices

Jaehyuk Lee(jaehyuk@kisa.or.kr), Sungtaek Oh, Mijoo Kim
Woong Go, Soon-tai Park
KISA(Korea Internet & Security Agency)

Abstract

Recently, a variety of products and services using IoT (IoT, Internet of Things) technology, in which sensors and communication functions are embedded in various objects, have been released following the development of IT technology. By connecting devices used in real life, the IoT industry is growing rapidly, and the entry into a hyper-connected society is accelerating. However, new security threats are occurring due to open platforms for IoT devices, limited resources, and interconnections between devices over the Internet. Since the security technology of an IoT environment with limited resources is developed focusing on device certification and encryption, there is not enough technology to cope with cyber infringement incidents (hacking). In this paper, we propose a methodology for a technology which can detect and respond to anomalies by collecting and analyzing the hardware and network information of low-weight IoT devices.

The IoT industry is growing rapidly, but attacks such as the Mirai malicious code are being attempted on IoT devices with weak security. These attacks currently cause massive socio-economic losses, with global economic losses from cybercrime reaching about USD 400 billion annually.
In this paper, we extract hardware information from IoT devices that have limited resources and examine a method to detect and respond to anomalies using the extracted hardware information.

we propose a methodology for security technology which can detect and respond to anomalies using hardware information and network information collected from low-weight IoT devices.

A. Information collection system
It is collected using port mirroring technology to replicate the network information. In addition, the items (CPU, memory, disk, network information) are collected from the client group and utilized in the analysis using the basic commands and hardware information collection tools provided by the IoT devices. If the basic commands provided by IoT devices are used, they can be used in low-weight IoT equipment because monitoring functions can be performed without installing any additional equipment.

B. Anomaly Detection and Response
An anomaly detection system based on hardware information and network information selects and extracts items that are highly associated with anomalies through basic commands and port mirroring of IoT devices. low-weight anomaly detection is performed through correlation analysis based on the selectively extracted data. It is collected using port mirroring technology to replicate the network information. The collected hardware and network information are divided into before and after the infection of malicious code to perform a correlation analysis between each characteristic, and the items showing the highest relevance and the highly weighted characteristics were selected to detect. Finally, the Security management unit sends control commands (Power On/Off, etc.) to the IoT device to respond to the detected anomaly, Hardware information was extracted using basic commands provided in a IoT environment, and correlation analysis were performed using network information. we plan to implement an anomaly detection framework for IoT devices that are actually used based on collected and analyzed hardware and network information.

ACKNOWLEDGEMENTS
This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2018-0-00232, Cloud-based IoT Threat Autonomic Analysis and Response Technology)

Keywords: *IoT, security, anomaly detection, computer security, network*

References

[1] IoT Analytics,“State of the IoT & Short term outlook 2018”, 2018.
[2] KOTRA,“Global Market Report 16-045”, 2016.
[3] Symantec Corporation, “2018 Internet Security Threat Report”, ISTR Volume 23, March. 2018.
[4] Babar, Sachin, et al., “Proposed security model and threat taxonomy for the Internet of Things(IoT)”, In International Conference on Network Security and Applications, pp. 420-429, Jul. 2010.
[5] Zhou, Liang and Han-Chieh Chao, Multimedia traffic security architecture for the internet of things, IEEE Network 25.3, 2011.

Biography

Jaehyuk Lee is graduated from Korea University with a master's degree.
and Currently working at KISA(Korea Internet & Security Agency)

project
17`. 4 ~ 18`. 2 Development of Profiling-based Techniques for Detecting and Preventing Mobile Billing Fraud Attacks(3 years, 5.75 billion dollar)
18`. 4 ~ 21`. 12 Cloud-based IoT Threat Autonomic Analysis and Response Technology(3 years, 8.51 billion dollar)