International Journal of Internet of Things and Big Data
Vol.4, No.1 (2019), pp.17-22
http://dx.doi.org/10.21742/ijitbd.2019.4.1.03

The Internet-Connected Device Vulnerability Information Management System in IoT Environment

Taeeun Kim[1], Yong Hoon Jung[2] and Moon-Seog Jun[3]

[1,3]Dept. of Computer Science, Soong-Sil University, Korea
[2]BaaS LAB, Korea
[1]eunii31@gmail.com, [2]jung7773@naver.com, [3]jaehwan@kongju.ac.kr

Abstract

Recently, the performance of wireless communication and small devices has greatly improved. As these technologies and environments change, there is a growing number of services that utilize various types of IoT devices. Devices such as small sensors and CCTVs that were used offline are being connected to the Internet. However, a large number of IoT devices use an open-source with no security function. In addition, network equipment such as switches and gateways, which have been used for a long time, is also used with many vulnerabilities because users do not have regular updates. Such weak devices are connected to the Internet and operating, making them vulnerable to malicious attackers. In this paper, we propose a system for collecting Internet-connected device information and identifying and managing vulnerability information by utilizing Internet-Wide Scan technology.

Keywords: *Vulnerability information management, Security management, IoT security*

1. Introduction

A modern IT environment depends heavily on and is closely related with the Internet. Many people use diverse web services and mobile devices every day, and create and provide a wide variety of information. The performance (e.g. speed and reliability) of wireless communication (Wi-Fi, Bluetooth, Zigbee, etc.) has advanced, and the diffusion of the small-size devices connected to the Internet (CCTV, Smart-Home, etc.) has increased sharply. The number of services that use various types of IoT devices is also increasing in line with the ongoing technological and environmental changes. Business Insider reported in 2016 that the number of IoT devices in the market will reach 24 billion by 2020 [1].

Conversely to the sharp increase in the number of IoT devices and services, research on those devices and services remains in its initial stages, while cyber-attacks that exploit the vulnerability of Internet-connected devices are on the rise. According to the results of a device vulnerability inspection conducted by CISCO in 2016, network devices such as routers and switches have twenty-eight vulnerabilities on average. In addition, 23% of those devices were found to have a vulnerability that had been announced five years before, and 10% of them were found to have a vulnerability dating back more than a decade [2]. Generally speaking, such networks and IoT devices are not properly managed, i.e. they are not subjected to periodic firmware updates after the first installation by the user. Therefore, preventive measures - like

Article history:
Received (July 8, 2019), Review Result (August 13, 2019), Accepted (October 9, 2019)

Print ISSN: 2207-3507, eISSN: 2207-3515 IJITBD

quick scan - are needed for devices with an old vulnerability, because such devices can become major attack targets.

Vulnerable Internet-connected devices have the following characteristics in common. First, vulnerable devices have no security function and use vulnerable version OS, open source, and communication protocols for the sake of convenient development. Second, there is a management difficulty caused by the characteristics of device usage. According to report published by CISCO, devices such as CCTVs, IP routers and printers are not directly connected to devices, so users tend not to apply security updates periodically and left unattended. A device left in such a vulnerable state may well run normally, but it can be exploited maliciously by a hacker.

As described above, we are using many vulnerable devices that lack proper security in order to distribute convenient services quickly. Therefore, we need to develop a technology quite unlike the conventional method of managing a few devices such as PCs and servers. The "Internet Wide Scan" is a representative technology that locates many IP address-based devices and collects information from them. There is also a "security vulnerability analysis" technology that analyzes known vulnerabilities in collected device information by using known vulnerability information. Using those technologies, this paper emphasizes the importance of advance prevention based on the identification - rather than on the updating of vulnerable devices.

This paper proposes a system architecture that can prevent cyber-attacks by searching for vulnerabilities in an Internet-connected device, and then verifies its performance comparatively.

2. Related work

2.1. Internet-wide scan

The previous network scan technology collected device information by checking the operating system of a single device (single IP) and scanning open ports[3][4][5][6]. Then, the vulnerability of a particular device was searched to analyze its vulnerability, using an aggressive technique. For example, well-known IDs and passwords are used to check the vulnerability of the default password, and the device is attacked directly using the exploit code. This type of scan is called "Active Scan" and includes such tools as nmap, Nessus, and Defensics. However, these tools are unsuitable for checking many remote devices. The reason for this is that the device cannot run normally because aggressive behavior or traffic is created by the device itself, and it may not run again due to a shutdown. Therefore, the "Passive Scan" technology has been developed rapidly in order to collect information on many remote devices quickly [7][8][9][10][11][12][13][14][15][16].

Passive Scan technology does not use an aggressive method to collect device information. This tool obtains the necessary information from the response message after sending a normal communication message to the device concerned in order to collect information. In addition, the majority of Internet-connected devices are targets of collection. The banner information that can be obtained when connecting to the Telnet service, as well as the communication traffic header information can be collected quickly. Shodan, Censys, and Masscan are all tools that use this type of scan.

However, Shodan and Censys are search engines that match the keyword retrieved by the user in the banner. An accurate result cannot be obtained easily using the keyword (e.g. product type) entered by the analyst to check the device vulnerability information. For example, when a keyword like 'CCTV' is entered, Shodan and Censys may match the keyword in the CCTV

sales website, but the analyst consequently needs to summarize, check, and analyze the search result.

2.2. Technology for analyzing security vulnerability information

Currently, security vulnerability technology can be classified according to whether it applies a direct action to the analysis target (device), i.e. in the same way as the classification of network scan technology, or does not.

A technology that does not apply a direct action to the analysis target is referred to as a "technology for analyzing security vulnerability information". The related area includes a technology that creates a structured database in order to manage vulnerability information, and that analyzes congratulations with the analysis target using the accumulated vulnerability information. Many organizations manage security vulnerability information according to their own criteria. The CVE (Common Vulnerabilities and Exposures) managed by the NVD (National Vulnerability Database) are the representative criteria, while Bugtraq, VulDB, and device and software manufacturers also manage vulnerability information.

A "vulnerability information scan technology" finds and identifies a vulnerable device using the structured information as described above. A vulnerability information scan technology analyzes the correlation between vulnerability information and device information after collecting the information from a device for the purpose of analysis. There are diverse algorithms ranging from simple keyword matching to similarity analysis. To detect vulnerabilities like Heartbleed and Poodle, Shodan and Censys find the OpenSSL version information from the collected traffic and match it with the relevant vulnerability information for analysis [17][18].

3. Vulnerability information management system of the internet-connected device

This chapter proposes a system that can prevent cyber threats by searching for an Internet-connected device based on the IPv4 address and then identifying the security vulnerability information. The proposed system uses the passive scan technology (Internet Wide Scan) and the technology for analyzing security vulnerability information among the related technologies.

3.1. Composition of the proposed technology

A technology for collecting both device information and vulnerability information and for analyzing the vulnerability information contained in a device is needed to manage the vulnerability information of Internet-connected devices. Therefore, the proposed system comprises three functional modules, namely, the Internet-Connected Devices Scan Module, Vulnerability Information Management Module, Devices Vulnerability Analysis Module as shown in [Figure 1].

The Internet-Connected Devices Scan Module sends communication packets to scan a device in the IPv4 address range and collects response packets to collect the device information. The Vulnerability Information Management Module crawls websites that provide vulnerability information in order to analyze the vulnerability information of the device. The Devices Vulnerability Analysis Module analyzes the correlation between the device information and the vulnerability information collected by the previous two modules, and manages the result. Each module runs in a different server to maximize the system's performance.

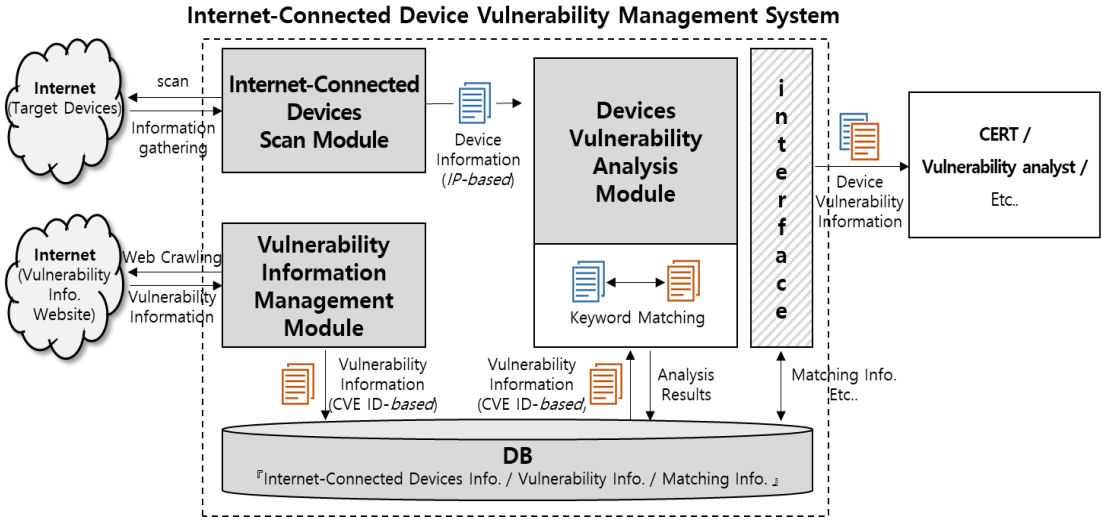

Figure 1. Diagram of vulnerability management system

3.2. Internet-connected devices scan module

A Two sub-modules were developed using the ZMap and ZGrab open sources to collect information on Internet-connected devices. In addition, the traffic management module was separately implemented to control the scan traffic generated by the two collection modules, and its performance was enhanced by applying DAG-CARD and PF-RING. The traffic management function generates and sends scan traffic to collect device information, and receives the response packet from the device.

3.3. Vulnerability information management module

A function that collects the open vulnerability information and structures the information for analysis is also needed, so that the vulnerability information of the Internet-connected device can be analyzed. The vulnerability information management module developed before downloads the CVE information from the NVD as a file, and classifies the information into CPE (Common Platform Enumeration), CWE (Common Weakness Enumeration), and CVSS (Common Vulnerability Scoring System) for structuralization. About 100,000 items of CVE vulnerability information have been collected up to now.

The vulnerability information is collected in the CVE/non-CVE type, and the new/modified information is updated every day. Bugtraq and VulDB have the assigned ID to each vulnerability and include the correlated CVE-ID. However, if a new vulnerability that is not registered in the CVE is found, it will be classified as “atypical vulnerability information” and processed to classify the vulnerability information type.

3.4. Devices vulnerability analysis module

The device information and the common keyword in the vulnerability information should be matched to check the existence of a vulnerability in the collected device information. The ‘Devices Vulnerability Analysis Module’ is composed of two sub-modules: the “device information analysis” module, which finds a keyword (e.g. manufacturer, product name) in the device information to identify the CPE information and the “vulnerability information analysis”

module, which then relates the CPE found by the device information analysis module to the vulnerability information.

a) The device information analysis module identifies the CPE information from the banner, packet payload (data), and Handshake traffic information collected by scanning the device. The CPE information to be identified is the name and version information of the standardized product as defined in the "CPE dictionary". Any similarity with the CPE dictionary information is analyzed to identify the CPE information from the device information, and the information is identified as CPE if the result of the similarity analysis is above 80%, so as to increase accuracy. A similarity analysis is conducted in the order of manufacturer and product version, if its accuracy in identifying the product name exceeds 80%.

b) The vulnerability information analysis module matches and analyzes the CPE information of the device identified by the previous device information analysis module and the CPE information included in the vulnerability information collected by the vulnerability information management module. If the CPE identified from the device information is included in the vulnerability information, it means that the matching vulnerability is present in the device.

A simple keyword matching algorithm rather than a complex algorithm is used for CPE information matching because the device information and vulnerability information are processed in advance. The device vulnerability information matched in this way is created and managed in the JSON format to share with the CERT and vulnerability analysts.

4. Conclusion

Recently, the number of Internet-connected devices has increased sharply due to the proliferation of IoT services. However, the security of IoT devices cannot be managed as easily as that of the existing PC and server use environment. A security program (such as a vaccine) cannot be installed in small devices, and network environment security (e.g. firewall) cannot be applied easily. In addition, IoT devices contain many vulnerabilities because they use vulnerable open source software and Cut-down OS. Small, vulnerable devices can be exploited for cyber-attacks, including large-scale DDoS attacks. Therefore, vulnerabilities should be managed on a regular basis to prevent such attacks.

This paper proposes a system structure for managing the vulnerabilities of Internet-connected devices, and the developed system was tested comparatively in various environments. The existing Internet Wide Scan technology is being developed with the focus on a method of collecting a large amount of device information quickly. Experts in vulnerability analysis detect a device's vulnerability using the information provided by Shodan and other service providers that use scan technology. The proposed system is designed to prevent cyber-attacks in advance by automating the process of manual vulnerability analysis using the Internet scan. In the future, the scan performance and vulnerability analysis function of the developed system will be improved and used to respond to cyber-security threats.

References

[1] Business Insider Intelligence, "There will be 24 billion IoT devices installed on Earth by 2020," The Internet of Everything report, http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5, **(2016)**

[2] Cisco, "Cisco 2016 midyear cybersecyrity report of cisco," http://www.cisco.com/c/dam/m/en_ca/never-better/assets/files/midyearsecurity-report-2016.pdf, **(2016)**

[3] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," Proceedings of the IEEE Communications Surveys & Tutorials **(2016)**, vol.18, no.1, pp.94-104

[4] Y-C. Chen, Y. Liao, M. Baldi, S-J. Lee, and L. Qiu, "OS fingerprinting and thethering detection in mobile networks," Proceedings of the 2014 Conference on Internet Measurement Conference, pp.173-179, **(2014)**

[5] Z. Shamsi, A. Nandwani, D. Leonard, and D. Loguinov, "Hershel: Single-packet OS fingerprinting," Proceedings of the IEEE/ACM Transactions on Networking, vol.24, pp.2196-2209, **(2016)** DOI: 10.1145/2591971.2591972

[6] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares," Proceedings of the 23rd USENIX conference on Security Symposium, pp.95-110, **(2014)**

[7] G. Bartlett, J., Heidemann, and C. Papadopoulos, "Understanding passive and active service discovery," Proceedings of the 7th ACM SIGCOMM conference on Internet measurement (IMC), pp.57-70, **(2007)**

[8] M. Li, H. Chen, X. Huang, and L. Cui, "EasiCrawl: A sleep-aware schedule method for crawling IoT sensors," Proceedings of the IEEE International Conference on Parallel and Distributed Systems, pp.148-155, **(2015)**

[9] K. Yinghui and S. Danfeng, "Research on collecting real-time information on dynamic web pages of Internet of Things," Proceedings of the International Conference on Computational and Information Sciences, pp.563-566, **(2013)** DOI: 10.1109/ICCIS.2013.156

[10] D. Leonard and D. Loguinov, "Demystifying service discovery: Implementing an internet-wide scanner," Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, pp.109-122, **(2010)** DOI: 10.1145/1879141.1879156

[11] S. Khattak, D. Fifield, S. Afroz, M. Javed, S. Sundaresan, V. Paxson, S.J. Murdoch, and D. McCoy, "Do you see what I see? Differential treatment of anonymous users," Proceedings of the 23rd Network and Distributed System Security Symposium **(2016)**

[12] G.C.M. Moura, C. Ganan, Q. Lone, P. Poursaied, H. Asghari, and M. van Eeten, "How dynamic is the ISPs address space? Towards internet-wide DHCP churn estimation," Proceedings of the IFIP Networking Conference **(2015)**

[13] R. Trapkickin, "Who is scanning the internet?" Proceedings of the Seminars Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM) **(2015)**

[14] D. Myers, E. Foo, and K. Radke, "Internet-wide scanning taxonomy and framework," Proceedings of the 13th Australasian Information Security Conference **(2015)**

[15] Anton V. Arzhakov and Irina F. Babalova, "Analysis of current internet wide scan effectiveness," Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering **(2017)** DOI: 10.1109/EIConRus.2017.7910503

[16] Carna Botnet, "Internet census 2012, Port scanning /0 using insecure embedded devices," http://census2012.sourceforge.net/paper.html, **(2012)**

[17] B. Genge, C. Enachescu, "ShoVAT: Shodan-based vulnerability assesment tool for Internet-facing services," Proceedings of the Security & Communication Networks, vol.9, no.15, pp.2696-2714, **(2015)** DOI: 10.1002/sec.1262

[18] Z. Durumeric, J. Kasten, D. Adrian, J.A. Halderman, M.Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, and V. Paxson, "The matter of heartbleed," Proceedings of the Conference on Internet Measurement Conference, pp.475-488, November, **(2014)** DOI: 10.1145/2663716.2663755