A Study on Asset Identification in Smart Buildings Automation Systems

Minsu Park
Dept. of AI-based Convergence
Dankook University
Yongin, Republic of Korea
mspark@dankook.ac.kr

Seong-je Cho
Dept. of Software Science
Dankook University
Yongin, Republic of Korea
sjcho@dankook.ac.kr

Hongeun Kim
Graduate School of International Affairs
& Information security
Dongguk University
Jung-gu, Republic of Korea
Hgkim4044@gmail.com

***Abstract* —** Smart building automation systems (BASs) are designed to improve the convenience of residents and achieve efficient energy management, resulting in an increase in their components. However, unlike conventional building systems, smart BASs are connected to the Internet, and cybersecurity threats targeting the smart BASs are on the rise. To address this issue, it is essential to identify the assets or devices that make up a smart BASs and mitigate the vulnerabilities in the assets. However, applying asset identification techniques used in traditional information technology (IT) systems to smart BASs is challenging because smart BASs consist of IT, operational technology (OT), and industrial IoT (IIoT) devices. In this paper, we conduct a basic experiment to analyze network traffic of some assets and try to identify each asset in a mini smart building system. We then present the challenges that need to be addressed for effective asset identification in smart BASs.

Keywords—Smart buildings; asset identification; network scanning; building automation system

I. INTRODUCTION

Smart buildings consist of various Internet of Things (IoT) sensors, actuators, controllers, and computers that are interconnected to perform critical functions in modern buildings [1, 2]. The Building Automation System (BAS) is the core of smart buildings and is used in conjunction with various IoT/IIoT devices to improve energy efficiency in the buildings [3, 4]. With the interconnectivity of various devices and components in smart buildings to the Internet, cybersecurity threats targeting BASs have increased [5, 6]. To mitigate such threats, it is essential to identify assets or devices within smart BASs and address their security vulnerabilities [7, 8].

Identifying assets or devices consisting of a smart BAS is crucial for establishing a secure smart BAS. However, the BAS is different from traditional information technology (IT) systems in its components and characteristics, making conventional asset identification challenging [9]. For example, the BAS can be composed of operational technology (OT) systems such as Programmable Logic Controllers (PLC), building-specific control units, and Direct Digital Control (DDC), and interacts with the physical world through IoT sensors and actuators [10]. Due to the characteristics of OT systems such as device heterogeneity, proprietary protocols, and device computational power [9], it can be unsuitable to apply the conventional asset identification used in traditional IT systems to OT systems.

In this paper, we first investigate the asset identification based on network scanning. We then construct a mini smart BAS and perform experiments analyzing the network traffic of the system's devices. Finally, we present limitations in applying the traditional asset identification to a smart BAS, and challenges to be addressed to overcome them.

II. BACKGROUND

In this section, we examine network scanning or device discovery methods commonly used in traditional IT systems. Network scanning can be categorized into two methods: Active Scanning and Passive Scanning [7].

Active scanning is a technique that involves sending direct queries to the devices connected to a target network and identifies the type and operating system (OS) of each device by analyzing the query results [7, 11]. This technique utilizes the fields in the Transmission Control Protocol (TCP) packet header as a feature set and compares them with an OS fingerprint database to predict the OS of each device. Nmap is a popular tool for active scanning. It transmits packets to up to 16 network ports and identifies the OS by analyzing the header information of the response packets. Active scanning is known to have higher accuracy in identifying the OS of devices than passive scanning, but it requires interaction with the target devices, which results in performance overhead [12].

Passive Scanning, on the other hand, is a technique that observes the traffic occurring in a network without generating direct queries to target devices. It tries to identify each device based on the observed traffic information [11, 12]. P0f is a representative tool for passive scanning. P0f predicts the OS of devices based on the TCP traffic generated by the system, especially SYN, SYN+ACK, and RST, RST+ACK. Passive scanning takes a longer time to discover devices than active scanning, and the prediction accuracy may be lower than active scanning [12].

III. EXPERIMENTS IN A MINI-SMART BUILDING SYSTEM

We collect and analyze network packets using Wireshark in a mini–smart BAS constructed by ourselves where port mirroring was set up on the network hub. The mini-smart BAS measures temperature, humidity, and other environmental

This research was partly supported by Basic Science Research Program the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (no. 2021R1A2C2012574) and partly supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20212020800120).

factors, and controls boilers and air conditioners. Tab 1. lists the information of devices used in the experiment.

TABLE I. Device information used in the experiment.

System	Device type	Model (or OS[PC])	Vendor
OT	TCP/IP Modbus Gateway	MS-SM162	Realsys
	Distribution Board	GEMS3512	Leehansolutec
	HVAC Controller	LG-ACP 5	LG Electronics
IT	Management PC	Windows 10	-
	Client PC	Windows 10	-
	DB Server	Ubuntu MySQL Server 10.5.8	-

Realsys MS-SM162 converts Modbus/RTU communication to Modbus/TCP for transmitting data over Ethernet. Power distribution systems distribute incoming electricity back to each electrical load. Leehansolutec GEMS3512, an on-board power distribution system, is used for efficient power distribution, while LG Electronics LG-ACP 5 controls the air cooling and heating in the room. The management and client PCs run on the Windows 10 OS, while the DB Server uses Ubuntu MySQL Server 10.5.8 to receive and store data from the OT devices.

Fig 1. shows the number of packets per second for each device listed in Table 1. Network packets were collected for approximately 45 minutes, with the packet collection continuing up to 2600 seconds. The horizontal axis represents time in seconds, while the vertical axis represents packets per second (packet/sec), with a maximum value of 1000.

(a) The traffic on the MS-SM162 generates a very regular signal, with the protocol interacting with the Management PC using Modbus/TCP. The maximum number of packets per second is approximately 240, occurring equally for a certain period (about 300 seconds). (b) GEMS3512 does not have a regular time to hold 240 maximum packets per second, but some parts of the time hold for about 300 seconds. (c) The graph for LG-ACP 5 shows a periodic appearance of up to 150 packets per second for approximately 1500 seconds, with the number of packets generated being relatively small compared to other devices (MS-SM162 and GEMS3512). However, due to the short packet collection time, we could not verify whether the number of packets was periodically generated. (d) The graph shows the results of checking the traffic generated by the Management PC, Client PC, and DB Server. The number of packets per second was not constant compared to other devices, with a significant difference between the maximum and minimum packets.

The experiment results show that OT devices generate periodic communication traffic and the number of their packets per second is relatively constant. In contrast, IT devices generate relatively high traffic and the number of their packets per second is variable. The smart building automation communication is similar to industrial communication protocol [21]. Communication traffic of industrial control system (ICS) is known to be stable and periodic unlike general Internet traffic [1]. Thus, OT devices exhibit the periodic traffic pattern. Although the packet collection time was short, our experiment

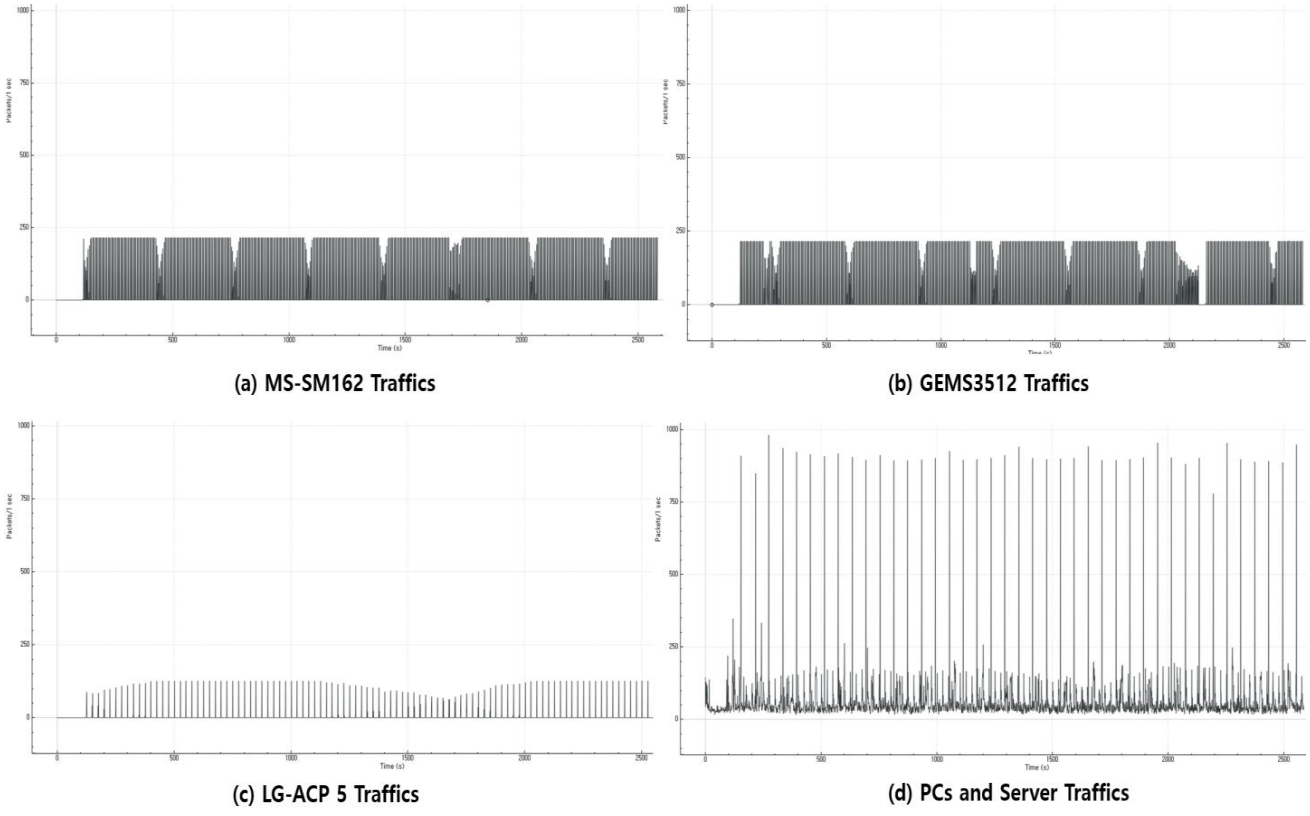

Figure 1. Compare packets per second by equipment.

results showed the difference between IT and OT devices.

IV. Discussion

Smart BAS consists of OT and IoT/IIoT devices. By analyzing some previous studies including the experiments of Section III, we have found that there are some issues to discover each device or identify each asset on OT or IoT/IIoT networks. Some issues to be addressed for identifying OT or IIoT devices are as follows:

Table II. Comparison of issues

Category	References	Challenge
Active Scanning	[13][14][15]	Availability of OT systems
	[16]	Accuracy in an environment with a firewall
Passive Scanning	[17][18][20]	Time for collecting data
	[17][19][20]	Scalability

Availability of OT systems Active scanning can affect availability of the OT devices depending on the process cycle time. To address this problem, it is necessary to examine the threshold at which devices can process network requests. It is needed to determine whether an impact occurs when devices with different resources have the same process cycle time.

Accuracy in an environment with a firewall Active scanning has poor accuracy in environments where firewalls exist. To figure out the cause of the problem, it is necessary to compare the accuracy of traditional asset identification techniques in a smart BAS with and without firewalls.

Time for collecting data Passive scanning needs longer time than active scanning (at least 3 to 26 weeks). Therefore, it is necessary to identify effective features that can quickly identify devices or develop active scanning with high availability.

Scalability Several researchers conducted passive scanning on 4 to 33 devices. This number of devices is insufficient to apply to a general smart BAS. General approach can handle more than 20 types of OT and IoT/IIoT devices and distinguish each device using an effective device fingerprint.

V. Conclusion

In this paper, we analyzed network traffics to identify each asset consisting of a mini smart BAS. We also examined challenges to be addressed for efficient asset identification (device discovery) in a smart BAS. Components of industrial control systems (ICS) which are very similar to BAS exhibit stable behavior in terms of traffic and communication patterns [9]. Unlike IT devices, the number of packets generated by OT devices was small and exhibited periodic characteristics However, our study had limitations in find out a device fingerprint that could identify individual OT devices. In the future, we plan to identify individual devices by collecting and analyzing the network traffic of various devices over a long period of time. We then will scan the identified devices for detecting security vulnerabilities.

References

[1] A. H. Buckman, M. Mayfield, and S. B. M. Beck, "What is a smart building?" *Smart and Sustainable Built Environment*, vol. 3, no. 2, pp. 92-109, 2014.

[2] P. Ciholas, A. Lennie, P. Sadigova, and J. M. Such, "The security of smart buildings: a systematic literature review," *arXiv preprint* arXiv:1901.05837, 2019.

[3] Equipment-as-a-Service(Eaas), Deloitte AI Institute. [online] https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/energy-resources/deloitte-uk-energy-as-a-service-report-2019.pdf. 2019.

[4] Can you trust your smart building? [online] https://www.outsecure.com/wp-content/uploads/2019/08/IoTSF-Smart-Buildings-White-Paper-PDF-1.pdf. 2019.

[5] Y. Shah and S. Sengupta, "A survey on Classification of Cyber-attacks on IoT and IIoT devices," *11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2020.

[6] M. Chipley and T. Conway, "Next-Generation Cybersecurity for Buildings," SANS Institute. [online] https://www.fortinet.com/content/dam/fortinet/assets/reports/ko_kr/r-next-generation-cybersecurity-for-smart-buildings-kr.pdf, 2021.

[7] E. Bou-Harb, M. Debbabi, and C. Assi, "Cyber scanning: a comprehensive survey," *IEEE communications surveys & tutorials*, vol. 16, no. 3, pp. 1496-1519, 2013

[8] D. Duggan, M. Berg, J. Dillinger, and J. Stamp, "Penetration testing of industrial control systems," *Sandia national laboratories*, 2005.

[9] M. Caselli, D. Hadžiosmanović, E. Zambon, and F. Kargl, "On the feasibility of device fingerprinting in industrial control systems," *Critical Information Infrastructures Security: 8th International Workshop (CRITIS),* 2013.

[10] W. Kastner, G. Neugschwandtner. S. Soucek, and H. M. Newman, "Communication systems for building automation and control," *Proceedings of the IEEE,* vol. 93, no. 6, pp. 1178-1203, 2005.

[11] G. Olivero, "Asset Discovery Tools Supporting Cybersecurity Inventory," *POLITECNICO DI TORINO,* Master Degree Thesis, 2022.

[12] C. Mavrakis, "Passive asset discovery and operating system fingerprinting in industrial control system networks," Eindhoven University of Technology, Master Degree Thesis, 2015

[13] O. Pospisil, P. Blazek, R. Fujdiak, and J. Misurec, "Active Scanning in the Industrial Control Systems," *International Symposium on Computer Science and Intelligent Controls (ISCSIC),* 2021.

[14] T. Hanka, M. Niedermaier, F. Fischer, S. Kießling, P. Knauer, and D. Merli, "Impact of Active Scanning Tools for Device Discovery in Industrial Networks," *Security, Privacy and Anonymity in Computation, Communication, and Storage: SpaCCS 2020 International Workshops*, 2020.

[15] K. Coffey, R. Smith, L. Maglaras, and H. Janicke, "Vulnerability analysis of network scanning on SCADA systems," *Security and Communication Networks,* 2018.

[16] S. Im, S. H. Shin, K. Y. Ryu, and B. Roh, "Performance evaluation of network scanning tools with operation of firewall," *Eighth International Conference on Ubiquitous and Future Networks (ICUFN),* 2016.

[17] M. R. Shahid, G. Blanc, Z. Zhang, and H. Debar, "IoT devices recognition through network traffic analysis," *2018 IEEE international conference on big data (big data),* 2018.

[18] A. Sivanathan, H. H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Classifying IoT devices in smart environments using network traffic characteristics," *IEEE Transactions on Mobile Computing,* vol. 18, no. 8, pp. 1745-1759, 2018.

[19] D. Formby, P. Srinivasan, A. Leonard, J Rogers, and R. Beyah, "Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems," *NDSS,* 2016.

[20] L. Bai, L. Yao, S. S. Kanhere, X. Wang, and Z. Yang, "Automatic device classification from network traffic streams of internet of things," *IEEE 43rd conference on local computer networks (LCN),* 2018.

[21] G. Stamatescu, I. Stamatescu, N. Arghira, and I. Făgărăşan, "Cybersecurity perspectives for smart building automation systems," *12th IEEE International Conf. on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1-5, 2020.