Bulletin of Networking, Computing, Systems, and Software – www.bncss.org, ISSN 2186-5140
Volume 8, Number 2, pages 104–107, July 2019

A Framework of Moving Target Defenses for the Internet of Things

Wai Kyi Kyi Oo
Graduate School of Information Science and Electrical Engineering
Kyushu University
Fukuoka, Japan
kyi.oo.wai.kyi.219@s.kyushu-u.ac.jp

Hiroshi Koide
Research Institute for Information Technology
Kyushu University
Fukuoka, Japan
koide@cc.kyushu-u.ac.jp

***Abstract*—As the amount of Internet of Things (IoT) connected devices is expected to be more than 75 billion worldwide by 2025, these IoT systems such as smart devices, smartphones, as well as computer systems, become vulnerable to possible security breaches in various forms of cyber-attacks including hacking, phishing, etc., and the impact of actual attacks also continues to be expanded. Hence, the security concerns of establishing a new defense framework are of paramount importance for the IoT. The idea of Moving Target Defense (MTD) is giving uncertainties and difficulties to adversaries by shuffling or randomizing variants or attributes that can be possibly exposed as vulnerabilities of a target system. In this research, we propose a framework for adopting MTD concept as a proactive defense approach to protect IoT systems with the aim of establishing the method of MTDs and developing the mechanisms of research for continuous IoT systems. We then discuss two feasible, existing MTD techniques: IP address shuffling and code diversification. Considering the security of the IoT, we believe this is an essential first step towards investigating whether the application of MTDs is effective for future use.**

***Index Terms*—IoT security, moving target defense, diversification**

I. Introduction

By 2025, researchers predict that 75 billion embedded devices will be connected through the Internet [1]. When different types of everyday embedded "things/objects" (e.g. smart devices, automobiles, healthcare, energy and more) are formed and interconnected to send and receive data from each other through the Internet, it becomes a huge network: that we call nowadays as the Internet of Things (IoT) [2]. It has been reported that the security of these things are weak, and most of them can be easily accessible and attacked from the network as well as vulnerable to exploits. Additionally, since IoT devices are constrained in computational power, memory, and processing; various security considerations should be addressed such as applicability, compatibility, lightweight, and more. The development of IoT security has been positively attained and researchers have proposed possible defense solutions to secure the IoT environment in each layer of communicating one device to another. Nevertheless, the research in IoT security is still in the early stage of development, hence, it is necessary to investigate feasible and practicable defense techniques for protecting not only the information but also the devices themselves from cyber-attacks.

Moving Target Defense (MTD) technology, in other words, diversification approach has recently drawn significant attention to security researchers because of its effectiveness. Generally, attackers can make reconnaissance to identify a target system or device for conducting an attack. To disrupt their efforts in terms of time, cost, and information, the idea behind MTD is to create, evaluate, and deploy mechanisms, and these techniques should be diversified, or constantly altered and adjusted over time to make it harder and costlier to launch an attack [3].

In this paper, we aim to implement two MTD techniques: IP address diversification and code diversification, on each layer of IoT systems. They have been successful in disrupting malicious attacks; the former is used to prevent from attacker's reconnaissance, the latter is aimed at mitigating malware from various injections.

The goals of this research are manifold.

- To establish a secure IoT framework by adopting a proactive defense technology
- To examine the effect of MTD techniques and how they can be combined for an IoT system
- To evaluate existing MTD methods which have not yet been evaluated

Our intent is that this framework will provide a useful starting point for combining several moving target defenses in different levels of the IoT. To the best of our knowledge, no academic research that studies the combination of several MTDs for different layers of IoT environments has not yet been proposed. Therefore, we expect our framework will benefit the research in the security community.

The remainder of this paper is structured as follows. Section II presents the background theory including an overview of security concerns for the IoT, and why we use MTD techniques in our research. Section III discusses some related works of IoT-based MTDs. Section IV includes an overview of our IoT framework including the description of two adapted MTD methods. Finally, Section V provides conclusion and recommendation for future work.

II. Background

A. Overview of Security Concerns

Today, there are a lot of IoT applications used in different areas ranging from smart home, building, and health care to the smart grid, autonomous driving, manufacturing; and they have sensors which are used to collect information, and actuators which are aimed for performing physical tasks or real-time functions [4]. Therefore, in the current information technology field, we can simply address the IoT from cyber-physical system perspective: the interconnection between virtual systems (i.e. cyber) of information processing and real systems (i.e. physical) of sensors or actuators. They are therefore the bridge that connects the IoT with higher-level services through numerous networking communications, such as wireless sensor and actuator networks, machine-to-machine, a new technology: software-defined network, and so on. (See Fig. 1)

Insecure IoT devices and services can present as potential entry points for various types of cyber-attacks. The security issues in the IoT systems are different from those in traditional systems in terms of technology used and deployment. The security techniques and methods which have been observed for IoT systems are mainly based on conventional networks. Applying security mechanisms in IoT environments might be more difficult and complex than traditional network environments, as IoT devices are constrained in memory, processing, storage, and so on. Because of these unique characteristics and they may have high vulnerabilities to attacks, for instance, attackers can make Denial of Service attack which can cause a service disruption.

We assume that the defense solutions to IoT security should be collaborative, in which different techniques are deployed to mitigate a particular attack. We are also interested to investigate whether the current effective defense methods applied in conventional/traditional systems can also have impacts for the IoT environments.

When considering the security for the IoT environments, there are a lot of challenging issues are remained to be examined, such as privacy, authentication, verification, access control, system configuration, information storage, and more.

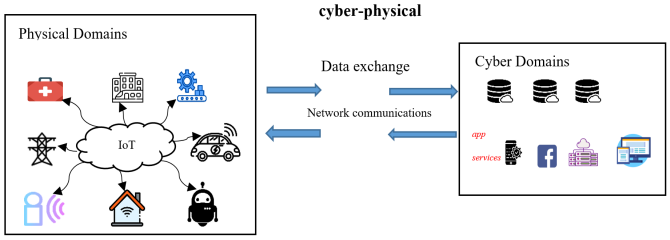

Fig. 1. Overview of interconnection between devices and services

B. The Inspiration of Moving Target Defense

The homogeneous and static nature of a system and its network configurations enable adversaries to carry out a large-scale attack easily with advantages in terms of time, information, and cost. As mentioned in the introduction, moving target defense is considered a promising technique which can reverse this situation. With MTD techniques, the properties or configurations of a system are dynamically changed in order to protect the software and devices from reconnaissance and malicious attacks, and it can greatly reduce an attacker's effort in making attacks successfully.

MTD techniques can be applied to different layers, such as application-layer, host-layer, and network-layer. Although an MTD technique cannot fully protect against all kinds of attacks, however, if we implement several MTDs on each layer, we can prevent most of attacks because each MTD defense is aimed to mitigate specific types of attacks.

Although MTD techniques are new in the security research field in traditional networks, a few techniques have already been available and applied in the real world. The address space layout randomization (ASLR) technique [5] is the most useful and successful MTD technique that has already been implemented in modern operating systems. ASLR is a dynamic runtime environment method and a memory-location technique that can thwart buffer overflows attack by randomizing the memory layout of an application program code. As a result of applying ASLR, the attacker cannot know the exact location of the diversified memory so that the attacker cannot use it.

Another notable and conventional technique for thwarting code-injection attacks is the instruction set randomization (ISR) technique [6], thus, we aim to deploy this in our research. The idea is to hide the behavior of instructions set of the target system by randomly altering the instructions used by the system. As a result, an injected code will not be correctly exploited because of the different behaviors.

As a security measure, many MTD techniques can be applied with other security measures like encryption, detection, and it can bring additional and effective security solutions for a system. Therefore, it has been gaining popularity among researchers to develop and assess for future use.

III. Related Work

Some researches focused on MTD techniques for the IoT have been recently proposed. In this paper [7], the author explored the existing method: network address shuffling [8], particularly they examined the impact of changing two versions of internet protocol addresses: IPv4 and IPv6. In their findings, the network-level MTD method might be feasible in IoT environments when using multiple IPv6 addresses, as it has the impact of performance overhead. In another related work of applying address change [9], they first proposed a design of implementing moving target defense IPv6 simulation-based to prevent IoT devices from reconnaissance. In this work, they mainly focused on the power consumption of a virtual machine by using Cooja, the network simulation tool for IPv6 network purpose use.

There are a few kinds of research focus on applying software-level MTD methods for the resource-constrained devices. In this paper [10], the authors proposed an MTD

framework based on two coding techniques: context-aware coding by partitioning code with specific context and code diversification using ASLR. However, they did not analyze the possibility of their approach, and they will implement the approach on the drone controller.

Similarly, in these works [11] and [12], authors propose the code diversification approach for operating system (OS) interfaces of IoT environments. The authors of the former research implemented their code diversification approach on two operating systems: Thingsee OS, the real-time operating system, and Raspbian OS. In the latter research, although they proposed two novel approaches: program obfuscation and diversification, they did not implement them in a real environment, and also did not mention what functions or software would be utilized in their approach.

According to these diversification-based related works, IP address or network address translation technique and code or operating system diversification techniques are worthwhile to be applied for protecting IoT systems and their applications from security attacks at network layer and application layer.

IV. Overview of Framework

Firstly, we construct an MTD-IoT framework: a cyber-physical system, shown in Fig. 2, consisting of a real and virtual IoT systems. A real system has many sensors, and some sensors will be configured with detection system; for instance, a firewall setting or a web application configured with an attack detection system for possible attacks. A virtual system will receive the information from the real system when the attack happens, then it will send back the feedback to the real system. By doing this, we can estimate the future status of the virtual system by sending feedback information to the real system.

Two MTD techniques will also be deployed on each system. Additionally, we plan to implement an attack detection system for web applications which is currently being operated for several months on AWS and Azure Cloud to detect multiple real attacks.

Considering an effective defense IoT framework, we intend to adapt existing works of two different MTD techniques, which have already been proposed in [6] and [8] for a traditional system, as a potential way to mitigate the risk of certain malicious attacks.

Since the functions of sensors and devices are equipped with the operating systems and software in the IoT, same as any other software system in a traditional system, they also have flaws and vulnerabilities that make them prone to several attacks. An attacker can exploit vulnerabilities on the system by identifying the entry to the system. In this research, we do not attempt to remove these vulnerabilities, but we intend to prevent or make it harder for the attacker to find discover and utilize them by diversifying the interface of operating systems and APIs, as well as randomly rotating IP addresses of each device.

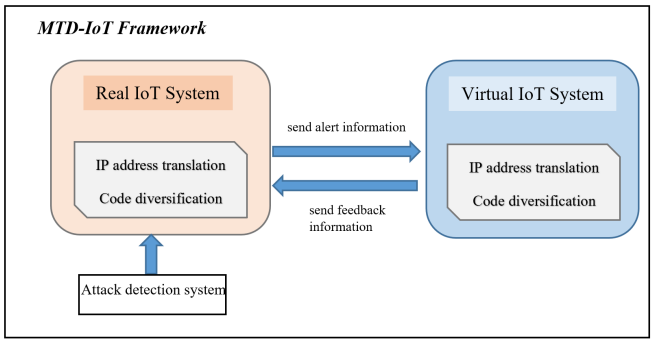

Fig. 2. Overview of a proposed MTD-based IoT framework

A. IP Address Diversification

The IP address diversification is adopted to prevent targeted attacks on IoT systems at the network layer by dynamically rotating IP addresses in order to prevent an attacker from conducting reconnaissance. As a result, attackers cannot identify what node is being served the information and service, as well as they will need more time before launching actual attacks. The randomization algorithm will be utilized for periodically changing IP addresses at a certain time.

B. Code Diversification

Software or code diversification technique has been effective in disrupting a lot of attacks including memory corruption attack, OS command injection, and buffer overflows attacks. By applying this technique in a victim system, the likelihood of attack possibility can be reduced because attackers have to figure out the exact internal functions of the system.

When we request services from a computer's OS through applications, these applications use library functions to access the critical resources of a device through system calls. If we alter the symbol names in these libraries, attackers cannot use the libraries as well as its entry points to attack the system.

With this consideration, we intend to apply MTD system call number diversification method and ELF magic number diversification that are among the applications of the instruction set architecture randomization technique.

The idea of the former is that the system calls numbers and its entry point in the kernel are diversified as well as the applications that invoke those system calls. Therefore, a malware that does not have the knowledge about new system call interfaces cannot interact with the environment and becomes ineffective. Similarly, we will also implement the diversification of executable and linkable file (ELF) magic number bytes as the way we consider for the former approach.

V. Conclusion and Future Work

Due to the ever-growing network of physical objects through the Internet, the risk of exposure to advanced and persistent attacks becomes increasingly higher. Although the considerations of defense technologies have been studied for almost a decade, there are still many challenging tasks: implementing

existing methods in IoT devices and services as well as examining whether or not these methods can effectively prevent particular attacks. Addressing these challenges and ensuring security is a fundamental priority.

In this paper, we suggest a framework for developing a secure IoT by applying two diversification techniques. A more extensive study of a practical experiment will remain as future work. By considering the actual implementation and analysis, we plan to use these technologies: machine-to-machine communication for networking, several Linux-based IoT operating systems on Raspberry Pi as hardware testbeds. For the operating system, we plan to test Gentoo and other IoT-based operating systems by manually installing kernel with code diversification technique as mentioned above. Then, we will further validate the possibilities of diversification mechanisms and their effectiveness. As our primary goal is to establish a secure IoT framework, we hope that this proposal is a useful starting point to develop defense techniques for future use.

REFERENCES

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] Dabbagh, M., & Rayes, A. (2019). Internet of things security and privacy. In Internet of Things From Hype to Reality (pp. 211-238). Springer, Cham.

[3] Jajodia, S., Ghosh, A. K., Swarup, V., Wang, C., & Wang, X. S. (Eds.). (2011). Moving target defense: creating asymmetric uncertainty for cyber threats (Vol. 54). Springer Science & Business Media.

[4] Lee, E. A. (2008, May). Cyber physical systems: Design challenges. In 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC) (pp. 363-369). IEEE.

[5] Shacham, H., Page, M., Pfaff, B., Goh, E. J., Modadugu, N., & Boneh, D. (2004, October). On the effectiveness of address-space randomization. In Proceedings of the 11th ACM conference on Computer and communications security (pp. 298-307). ACM.

[6] Kc, G. S., Keromytis, A. D., & Prevelakis, V. (2003, October). Countering code-injection attacks with instruction-set randomization. In Proceedings of the 10th ACM conference on Computer and communications security (pp. 272-280). ACM.

[7] Judmayer A., Merzdovnik G., Ullrich J., Voyiatzis A.G., Weippl E. (2018) A Performance Assessment of Network Address Shuffling in IoT Systems. In: Moreno-Díaz R., Pichler F., Quesada-Arencibia A. (eds) Computer Aided Systems Theory – EUROCAST 2017. EUROCAST 2017. Lecture Notes in Computer Science, vol 10671. Springer, Cham

[8] Cai, G., Wang, B., Wang, X., Yuan, Y., & Li, S. (2016, January). An introduction to network address shuffling. In 2016 18th International Conference on Advanced Communication Technology (ICACT) (pp. 185-190). IEEE.

[9] Zeitz, K., Cantrell, M., Marchany, R., & Tront, J. (2018). Changing the game: A micro moving target IPv6 defense for the internet of things. IEEE Wireless Communications Letters, 7(4), 578-581.

[10] Mahmood, K., & Shila, D. M. (2016, December). Moving target defense for Internet of Things using context aware code partitioning and code diversification. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (pp. 329-330). IEEE.

[11] Mäki, P., Rauti, S., Hosseinzadeh, S., Koivunen, L., & Leppänen, V. (2016, December). Interface diversification in IoT operating systems. In Proceedings of the 9th International Conference on Utility and Cloud Computing (pp. 304-309). ACM.

[12] Hosseinzadeh, S., Hyrynsalmi, S., & Leppänen, V. (2016). Obfuscation and diversification for securing the Internet of Things (IoT). In Internet of Things (pp. 259-274). Morgan Kaufmann.