Master's Thesis

Hands-on IoT Security Training Using IoT Testbeds

1710428 ZHAO, Min

Supervisor	Research Associate Professor Razvan BEURAN
Main Examiner	Research Associate Professor Razvan BEURAN
Examiners	Professor Yasuo TAN
	Associate Professor Yuto LIM
	Research Associate Professor Ken-ichi CHINEN

Graduate School of Advanced Science and Technology
Japan Advanced Institute of Science and Technology
(Information Science)

August 2019

Abstract

Nowadays, the IoT (Internet of Things) is not a virtual concept anymore, it is becoming a quite usual thing which can be seen everywhere in our lives and slowly filtering into people's minds.

From smart home to smart cars, smart industries, smart cities, etc., this new situation is quickly arising that sensors are connected to the Internet, collect data actively or receive the instructions passively, and transmit data, instructions to the cloud for processing, and then provide plentiful of services for people or companies. Although the concept that "machines will assist human in daily life" had already been described in 1932, in 2020, people will be surrounded by 50 billion Internet connected devices based on predictions of Cisco.

However, while people enjoy these conveniences via technology, an inevitable problem is the security of IoT. With the rapid development of IoT, cyber-attacks occur worldwide day by day. A notorious conducted DDoS attack case happened in 2016, named Dyn cyberattack, which was using a large number of IoT devices, such as printers, IP cameras that had been infected with the Mirai malware. As a matter of fact, Gartner also predicts that from 2018 to 2021, the worldwide spending on IoT security will increase from $1.5 billion to $3.1 billion. Thus, the focus on IoT security issues is becoming more and more critical.

Comparing with theoretical lectures, we believe that, under a complex and volatile security environment, it is necessary to do specific hands-on training, which can give trainees not only the necessary background information, but also indispensable, precious practice experience, in order to handle the rapidly and continuously changing security issues in an efficient way. Besides, we found that preparing a training environment is necessary for some training tutorials, but it is also like a stumbling block for beginners. Thus, it is useful to provide an online, "access-and-use" style, user-friendly training environment. Moreover, for the instructors, this training environment needs to be managed lightly and efficiently.

This problem does not exist for trainees like students only. As a matter of fact, in practice, only a small percentage of professionals are exposed to the production environments directly, and they do not make decisions. People who actually make security, technical or strategic decisions have little idea about the front-line environment. In this situation, during the promotion of emerging technology, should we just wait at ease, embrace it without borders, or use it for our benefit in a targeted way? The answer is obviously the last

one. But how to use technology in a targeted way? One of the solutions is to test and implement it in a virtual training environment first. Thus, questions like how to identify the standards of best practices and how to adjust measures to specific conditions will smoothly be solved.

This thesis presents IoTrain-Lab (IoT Training Platform using FIT/IoT-LAB Testbed), which is an open-source, easy to maintain, migrate and expand platform that also supports for multiple users' training for those who would like to know about IoT or IoT security. Furthermore, it contains both fundamental training and security training for meeting different demands.

There is no doubt that, for practical and flexibility reasons for designing, implementing, and testing experiments, simulators, emulators, and testbeds are beneficial tools. However, we have to consider the gap between simulation and reality. As we know, the simulator can change parameters as instructor wants, the ideally simulated environment may lead to single result set compared to real deployments. A satisfactory solution for these issues is using physical testbed. We did a survey and compared the differences between various IoT testbeds, and an open-source, open-access, multi-user testbed comprised of several wireless nodes and mobile robots, named FIT/IoT-LAB, became main candidate.

FIT/IoT-LAB is part of OneLab (Internet-overlaid, Broadband access, wireless & loT), and it has six sites across France. Each site has different devices, but all of these sites are related, and users can use the same web portal to access the devices. Moreover, FIT/IoT-LAB provides three kinds of hardware, which represent low complexity devices, middle devices, and rich devices. Except for these static nodes, another type is mobile nodes, robots which can be used at all sites. These up-to-date, programmable devices are free to use for research.

From the instructor point of view, considering the time cost issues, IoTrain-Lab was designed and implemented on Docker, an emerging virtualization approach solution. The instructor can implement IoTrain-Lab through the Docker files and Docker-compose files, which is efficient, and easier for maintenance and expansion. Comparing with the traditional virtualization way of virtual machines, Docker has several advantages, such as a more efficient use of system resources, faster start-up time, easier migration, easier maintenance and expansion, etc. When an instructor creates tutorials based on different demands, they can release it to Moodle web page, at the same time, trainees can use their own browser to access the Moodle web page and get the training tutorials. We also provide a Linux training environment which is connected with a clientless remote desktop gateway and it is also an online and "access-and-use" environment.

There are three clear classifications for fundamental training from top to

down, Application, Network Protocols, and Devices. This part is mainly for trainees who do not have much experience in the IoT area. It introduces the experiments from basic to complex, from a single node to several nodes, from perception, communication to application. For example, in the Devices part, we divided it into two subparts, consumption and radio in order to match the different training targets. For the consumption, we gave an experiment about battery consumption monitoring, and the trainees can do the hands-on practice based on this tutorial and FIT/IoT LAB Testbed, so that trainees can get results and analyze the results based on the testbed.

For trainees who already have an understanding of IoT, or would like to extend their knowledge to IoT security area, a similar structure with fundamental training includes IoT Service Ecosystem, Communication Network Ecosystem and Endpoint Ecosystem from top to down. This structure is based on the GSMA IoT security model, which promotes the best practice for secure design, development, and deployment of IoT services. These interrelated training contents ensure trainees have as many choices as they need.

In this thesis, first, we describe the research background, motivation and a short definition of the Internet of Things and current situation for IoT security. Then we introduce what an IoT testbed is, what is the difference between FIT/IoT-LAB and other testbeds, the architecture of IoTrain-Lab, furthermore, the necessary external tools like Docker and Apache Guacamole. Next, we address the training content and we offer precise training content details for both fundamental training and security training based on individual structures, however, due to various conditions, only the details and implementation of Flooding attack is provided and explained in this paper, and other parts are still on-going. At chapter five, two evaluation methods will be given, feature evaluation and user evaluation via SUS (System Usability Scale) which is a reliable tool for measuring usability. Last, conclusion and future work will be presented.

Keywords: IoT security training, IoT Testbed.