5F-05

An automated End-To-End Penetration testing for IoT

Alaa Allakany*, Geeta Yadav**, Vijay Kumar**, Kolin Paul***, and Koji Okamura****

* Cybersecurity Center, Kyushu University, Japan.

** School of Information Technology, IIT Delhi, India.

*** Department of Computer science & Engineering IIT Delhi, India.

**** Research Institute for Information Technology, Kyushu University, Japan.

***Abstract*— *In the Internet of Things (IoT) environment, objects are connected together on a network to share data, however, some of the IoT devices are developed and deployed with poor security consideration. As a result, these devices became a target of attacks. In this study, we will propose a framework for automated End-to-End penetration testing for IoT network. The existing penetration testing deployed based on the expert testers who have the knowledge to perform a manual test using many tolls, but this kind of manual Pen-test is highly cost and low efficiency. Furthermore, the existing automated penetration test doesn't consider End-to-End test for a system, it works by testing each part of a system separately that can lead to a gab that make the test not efficient. Due to such shortages, our framework will test the End-to-End network automatically (i.e., End devices, wireless communication between devices and the control unit, then communication to cloud server, and finally communication from the cloud to end user through mobile app or webpage). The proposed framework will automatically gather the information of the target IoT network and then perform various kinds of penetration testing through the network. Then it will summarize the results of Pen-test and gives the recommendations to secure a system.*

I. INTRODUCTION

Internet of things (IoT) is the system which devices can communicate with each other in order to provide a unique service for user's convenience and create a new way of data exchange. With growing IoT space, many of IoT device's provider developed a cheap devices without security consideration, these devices have many vulnerabilities that can be used by hackers to attack IoT space [1]. With increasing risk of vulnerabilities resulting from these poor security devices, penetration testing is required for testing your IoT system and provide instructions to enhance the security on the system.

Penetration testing is a process to identify security vulnerabilities by evaluating the system or network with various malicious techniques. The weak points of a system are exploited in this process through an authorized simulated attack. The purpose of this test is to secure important data from outsiders like hackers who can have unauthorized access to the system. Once the vulnerability is identified it is used to exploit the system in order to gain access to sensitive information. A penetration test tells whether the existing defensive measures employed on the system are strong enough to prevent any security breaches. Penetration test reports also suggest the countermeasures that can be taken to reduce the risk of the system being hacked. The purpose of penetration testing automation is to reduce the costs in terms of time and people (human resources) needed to perform the test[2,3].

II. RELATED WORK AND RESEARCH OBJECTIVE

PENTOS is one of the most related system to our system [4], it is a penetration testing tool for IoT devices. In this paper, the author presented a testing tool to automated penetration test for IoT devices, this tool provide a graphic interface for user to choice which part (item) of network to test. For instance, the user can select password attack, wireless attack or web hacking to a specific target in the network. However, we will prove in our paper that separating the automated penetration testing for a network items can cause a new gaps that cannot detected by such penetration testing tools.

Objectives of this study: is to automated and provide End-to-End penetration testing process in order to aid the organization to enhance the security of their system. The main points of the proposed system as follows: The system should cover all parts of a penetration testing process automatically. The system should consider that the testing of separated levels (items) of IoT network can lead to a gaps, thus, it should test all items on the network as connected network levels. The system should be able to incorporate new tools in an easy way. Finally, results found by the system will be presented in an easy-to-understand way.

To validate our proposed Penetration testing, we will perform experiments with different examples of IoT networks as case studies of this system. Figure 1, shows the definition of End-to-End in our system and shows some case studies that will tested based on our system, for instance, Philips hue and Alexa.

In the future, we will add other case studies to the proposed penetration testing framework. Moreover, it will be open source project so any other researchers can extend this project with many different IoT device systems.

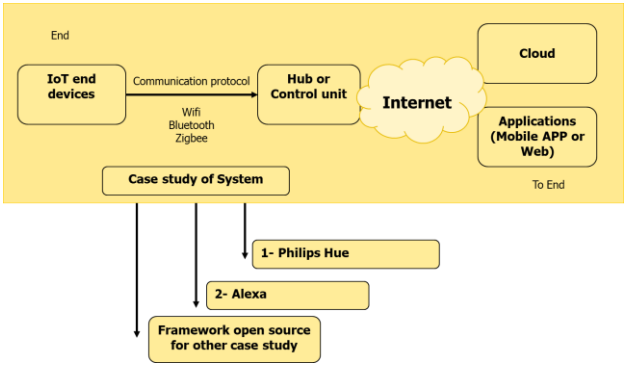

Figure 1: Overview of End-to-End

III. DESIGN

Since the organization need to perform the pentation testing regular in following situations: new infrastructure is added, software is installed, system updates are applied, security patches are applied and user policies are modified. These items have to be tested in each time the organization perform any change to the system. It can be tested manually by expert tester or automatically by automated system. We showed in introduction that automated system have many advantages comparing with manual test. However, the existing automated system provide a separate testing for each level of the system individually [4]. The existing automated system didn't consider that these separated items are connected on one system and testing each level (items) of the system separately can cause some gabs (vulnerabilities) that cannot discover by such automated pentation testing. For that our method will cover End-to-End Penetration testing for IoT system.

We will show later on our full paper a mathematical model that prove that testing each level (item) of the system separately can cause some vulnerabilities that cannot detected by existing automated system. Figure 2 summarize the main steps of any pentation testing that also will be similar to our proposed pen-test, but the framework that we going to proposed it can test the End to End IoT system one time. The following sub-section show the steps of the proposed framework.

A. *Planning*

This is the first stage in penetration testing. This stage usually involves the standard planning steps of setting goals. It work by gathering all information about the target system and mapping the network.

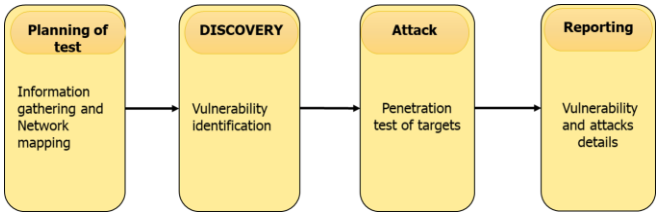

Figure 2: Steps of penetration testing

B. *Discovery*

The penetration testing start with this step. The main task of this step is to finds the vulnerabilities on the target system by port and network scanning. Also, there are some other activity in this step such as packet capturing, banner grabbing. Then, the system apply the vulnerability analysis to be used as input data to the next step of the penetration testing.

C. *Attack*

In this step of testing the system performing the attacks on the IoT network. The attacks are performed on the vulnerabilities that have been discovered through the previous step (discovery phase). On this step of testing the proposed system will test every discovered vulnerability and a loop of attack will be continued until all the objectives of the attack phase are completed.

D. *Reporting*

Finally, all result of the previous two step of this test will be compiled and presented as a report to users, this report include the details of the vulnerabilities and the attacks performed on the target system.

IV. CONCLUSION

We will proposed the End-to-End Penetrating testing that provides the user with the ability to have a test from inside or outside the system automatically. Once the user connect to the system the proposed framework will scan the system for any vulnerabilities and then attack script is triggered and maliciously crafted packets are sent to the specified system. Once the attack is completed a report is generated. This End-to-End pen-test enables the user to identify and analyze the security threats.

ACKNOWLEDGMENT

This research was supported by Strategic International Research Cooperative Program, Japan Science and Technology Agency (JST) , SICORP and JSPS KAKENHI Grant Number JP16K00480.

REFERENCES

[1] Eduard Kovacs. "Brian Kreb's Blog Hit by 665 Gbps DDoS Attack". 21 September 2016 [Online]. Available: http://www.securityweek.com/brian-krebs-blog-hit-665-gbps-ddosattack.

[2] M. Denis, C. Zena and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, 2016. pp. 1-6. doi: 10.1109/LISAT.2016.7494156.

[3] L. Epling, B. Hinkel, and Y. Hu, "Penetration Testing in a Box", 2015 Information Security Curriculum Development Conference (InfoSec '15), ACM, New York, USA, Article 6.

[4] V. Visoottiviseth, P. Akarasiriwong, and S. Chaiyasart, Siravit Chotivatunyu, "PENTOS: Penetration Testing Tool for Internet of Thing Devices". Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017.