A Denial of Service Attack for IoT System

Ming Cheng, Yichao Xu, Kai Zheng, Xin Huang
Department of Computer Science and Software Engineering,
Xi'an Jiaotong-Liverpool University, China,
Ming.Cheng15@student.xjtlu.edu.cn, Yichao.Xu15@student.xjtlu.edu.cn, Kai.Zheng14@student.xjtlu.edu.cn,
Xin.Huang@xjtlu.edu.cn

***Abstract*—Denial of Services (DoS) attack, as the most widely used attack method, attacks victim host by invading a number of other hosts in the Internet of Things (IoT) system. In this paper, ICMP, UDP and NTP attack methods were used to imitate DoS attack. The data produced in this process were analyzed and the result shows ICMP DoS attack with hping3 had the best performance.**

Keywords—DoS attack, Internet of Things, Raspberry Pi.

I. INTRODUCTION

As IoT system becomes popular and has a little protective measure, DoS attack becomes the most widely used attack method recently. ICMP NTP and UDP are three different types of protocol, which can be used in it. ICMP attack attacks devices by sending a number of ICMP Echo Reply data packages in high speed. NTP replies flood attack by the vulnerability of NTP servers in the network. It uses short instructions to return huge instructions based on UDP transmission. Since the beginning of DoS attack, UDP attack method has been used. It sends a great deal of UDP small packages to attack DNS server.

Some related work about IoT platform and DoS attack is introduced in [1-2]. Some previous works about DoS are listed in [3-5]. In this paper, DoS attack will be simulated, data will be analyzed and experiment result will be compared. The contribution of this paper is shown as below:

- The data produced in this experiment will be analyzed, such as package loss rate and message transfer time.
- Comparison between the data will be given to evaluate the performance of different attack methods.

II. IMPLEMENTATION

A. Preparation

IoT remote reprogramming system represented the communication between a sensor and Raspberry Pi in our experiment. The components were sensor, Raspberry Pi, router, PC and attacker. A continued connection between PC and Raspberry Pi were set up in Linux. These programs could also test message transfer time and loss percent. The connecting condition between PC and Raspberry Pi with no attack was tested and the test result had been analyzed.

B. Attack

Three different DoS attack methods were simulated separately. ICMP attack method was executed by inputting the command "hping3 –i u40 –d 4 –p 6632 --rand-source 192.168.1.101 -1" in terminal of Kali. NTP attack was executed in Scapy by entering the command "send (IP (dst = '192.168.1.101') / UDP (dport = 6632) / NTP () / ("Data"), inter = 0.0004, loop=1)". UDP DoS attack was done by using LOIC in Win 10.

C. Comparison of 3 DoS Attack Methods

The package loss rate and message transfer time varying with package size in a fixed transmit frequency were first compared separately. Then, package size was set to a proper value to compare the package loss rate and message transfer time varying with transmitting frequency.

It could be concluded from the data that ICMP attack method had both the longest message transfer time and highest package loss rate among three different DoS attack methods. UDP and NTP attack methods had short message transfer time and low package loss rate overall.

III. CONCLUSION

In this paper, 3 different methods for DoS attack based on IoT system has been introduced and compared. In conclusion, ICMP DoS attack with hping3 had the best performance. UDP DoS attack using LOIC had better performance than NTP DoS attack using Scapy. Furthermore, the larger packages size and higher transmit frequency, longer message transfer time and higher package loss rate, better performance.

REFERENCES

[1] N. Xue, X. Huang and J. Zhang. "S2Net: A Security Framework for Software Defined Intelligent Building Networks". The IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Tianjin, China, 2016.

[2] X. Huang, P. Craig, H. Lin and Z. Yan. "SecIoT: a security framework for the Internet of Things". Security and Communication Networks, 2015.

[3] Gao, Yuan, H. Wang, and X. Huang. "Applying Docker Swarm Cluster into Software Defined Internet of Things." *International Conference on Information Technology in Medicine and Education* IEEE, 2017:445-449.

[4] Wang, Haoxuan, et al. "Bluetooth Based Software Defined Function in Internet of Things." *The, Conference on Emerging Topics in Interactive Systems* 2016.

[5] Czyz, Jakub, et al. "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks." *internet measurement conference* (2014): 435-448.