WEI2202 Mid-Term Report

YUEN Yu Ching 1155143580

October 31, 2022

1 Testing Environment

For this project, we prepared the following hardware for testing:

- **Raspberry Pi Model 3B+**: The Raspberry Pi Model 3B+ ("Pi" below) is a small single-board computer. It comes with a BCM2837B0 quad-core CPU, which has a 32-bit ARMv8-A architecture. It is capable of Ethernet, WiFi, and Bluetooth networking. We have installed the Raspberry Pi OS on the system, as officially provided and supported by Raspberry Pi [1].
  Due to its real-world usage as part of IoT systems (as detailed in [2], [3], and [4]), we have adopted it to emulate an end node in a IoT network in this project.

Figure 1: Raspberry Pi Model 3B+

- **Mi Gaming Laptop 15.6**: The Mi Gaming Laptop ("Laptop" below) is a relatively high-end laptop. It features a Intel i5 8-core CPU, with NVIDIA GeForce GTX 1660 Ti Mobile; making it suitable for relatively heavy computing work.
  In this project, we will be using it to emulate a server/gateway serving as an intermediary between the end node and the end user. Due to its popularity in server contexts, Debian GNU/Linux has been installed on this machine.

Figure 2: Mi Gaming Laptop 15.6

In addition to the above equipment, we also prepared a small-size sample Internet-of-Things application for testing purposes. Due to the lack of environmental sensors available, we choose to use the CPU temperature of the Raspberry Pi to act as a pseudorandom statistic for testing purposes.

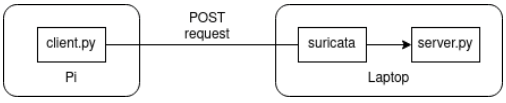

Figure 3: Structure of the system

The Pi acts as an end node, which will report its detected CPU temperature to the server every 5 seconds via a HTTP POST request. Meanwhile, the Laptop with a server running will receive the request; currently it is configured to print out the received content, with no further action.

2 Progress

We have installed Suricata from the Debian official repositories, and successfully ran it on the Laptop for a 10-minute period; during which Suricata executed as expected. The relevant logs can be found here: https://github.com/duncanyuen/WEI2202/tree/main/logs/log-202210312215

3 Next Steps

As outlined in the planning report, we are aiming to finish the IDS within the next month. Our future plans for this period are as follows:

1. Locally compile and run Suricata, with relevant optimizations
2. Compile situation-specific rules for Suricata
3. Develop an example IoT app over Bluetooth for testing purposes
4. (Next phase) Create playbook of attacks

References

[1] "Raspberry pi os - paspberry pi," Raspberry Pi, accessed 2022/10/30. [Online]. Available: https://www.raspberrypi.com/software/

[2] P. A, B. S, P. R, S. M, V. S, and N. M. M. Banu, "Internet of things based fall prediction and alerting device," in *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, 2022, pp. 01–05.

[3] N. R. Sogi, P. Chatterjee, U. Nethra, and V. Suma, "Smarisa: A raspberry pi based smart ring for women safety using iot," in *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2018, pp. 451–454.

[4] Y. Ma, F. Wang, and Z. Wang, "Intelligent laboratory management system based on internet of things," in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2017, pp. 464–467.