WEI2202 Planning Report

YUEN Yu Ching 1155143580

September 29, 2022

1 Project Goal

In this project, we will study some emergering security and privacy threats on the IoT platform. Specifically, we will be studying Low-Power Wide-Area Networks (LPWANs), and the feasibility of intrusion detection in them.

2 Significance of the project

Currently, there is a high presence of IoT in various fields, ranging from healthcare, urban planning, to smart watches. [1] states that there are 12.2 billion connected IoT decvices globally, with a forecasted growth to 27 billion devices by 2025. This demonstrates a high presence of IoT in a high fraction in the global population's lives, with the pervasiveness projected to further increase in the coming years.
Hence, the security of IoT networks are certainly of high importance, as the attacks can leverage against both the vitality of the services provided by the IoT networks, as well as the raw computational/networking power provided by the device inside the network. Examples include the Mirai botnet, in which a large amount of IoT devices are infected and used to launch a Distributed Denial of Service attack to victim servers, and the BrickerBot, which "bricks" victim devices and renders them permanently useless [2].
In [3], multiple usages of LPWANs are proposed, including Smart Agriculture, Healthcare, and Smart Homes. Should the devices in these scenarios be infected, the monetary cost of replacing the devices notwithstanding, it may also lead to loss of privacy in case the data from healthcare/smart homes are intercepted, or crop damages to agriculture scenarios.

3 Problem statement

The problem statement for this project is as follows:
Ideal:

- Ideally, all IoT networks would provide secure and private services to its users.

Reality:

- Many IoT networks are neither secure nor private, and are vulnerable to naive attacks.

Consequences:

- Loss of privacy from intercepted data/unrestricted access to insecure devices.
- Monetary/property loss from incorrect operations (e.g. DDoS, bricked devices)

Proposal:

- Investigate and try to implement an intrusion detection system as a preliminary approach to detecting and preventing attacks againt IoT networks.

4 Proposed solutions

To achieve this, we will be splitting the project into four phases:

4.1 Developing the IDS using Suricata

Suricata is an open-source intrusion detection system (IDS). We will be using it to develop an IoT-specific IDS.
Deliverables: An executable IDS based on Suricata.

4.2 Create playbook of various attacks

In this phase, we will go over existing documentation and papers to come up with a list of potential attacks that can be executed (e.g. SSH brute force, etc.) with Kali Linux.
Deliverables: A playbook of attacks against IoT networks.

4.3 Evaluate which type of attack can be blocked by Suricata

We will try to launch the attacks theorized in the previous phase, and during the process attempt to monitor, detect, and block the attacks.
Deliverables: Report regarding the detection/blocking of different types of attacks.

4.4 Deploy to PC and Raspberry Pi

After developing and testing, we will be deploying the finished IDS into a PC and Raspberry Pi as a proof-of-concept.
Deliverables: Proof-of-concept IoT network with an IDS.

5 Proposed timelines

We propose a timeline as follows:

Phase	Time
IDS Development	Oct-Nov 2022
Playbook Creation	Dec 2022-Jan 2023
Attack Evaluation	Jan-Mar 2023
Deployment	Mar-Apr 2023

Under this timeline, we will be spending approximately 1.5-2 months per phase. The first term will mainly be spent on the development of the intrusion detection system, and the other phases will be executed throughout the winter break and the second term.

References

[1] M. Hasan, "State of iot 2022: Number of connected iot devices growing 1814.4 billion globally," IoT Analytics, May 18 2022, accessed 2022/09/06. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[3] S. K. R, G. P. M, B. K. R, A. J, and A. D, "Lpwan for iot," in *2022 International Conference on Advanced Computing Technologies and Applications (ICACTA)*, 2022, pp. 1–4.