POSTER: Experimentation platform for repeatable security analysis in IoT heterogeneous environments

Florent Galtier
Paul L. R. Olivier
LAAS-CNRS
Toulouse, France
firstname.lastname@laas.fr

Guillaume Auriol
Vincent Nicomette
LAAS-CNRS, INSA-Toulouse
Toulouse, France
firstname.lastname@laas.fr

Romain Cayre
EURECOM
Biot, France
firstname.lastname@eurecom.fr

ABSTRACT

This poster introduces a platform addressing challenges in creating a representative environment for IoT wireless protocols. It aims to facilitate experiment repeatability by generating realistic traffic, executing attacks, and monitoring wireless communications. It offers a controlled environment for producing datasets suited for the assessment of intrusion detection systems.

CCS CONCEPTS

• **Networks** → **Wireless local area networks**; • **Security and privacy** → **Mobile and wireless security**.

KEYWORDS

IoT, platform, security, wireless protocols, datasets

ACM Reference Format:
Florent Galtier, Paul L. R. Olivier, Guillaume Auriol, Vincent Nicomette, and Romain Cayre. 2024. POSTER: Experimentation platform for repeatable security analysis in IoT heterogeneous environments. In *WiSec '24: 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks, May 27–May 30, 2024, Seoul, Korea.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/xxxxxxx.xxxxxxx

1 INTRODUCTION

With the rise of the Internet of Things, a large set of wireless protocols has emerged, each optimized to address its particular requirements and limitations. Their simultaneous deployment in the same frequency bands has led to increased their complexity in order to avoid interference. In addition, the dynamic nature of IoT ecosystem forced these protocols to always undergo changes in their specifications, while keeping a degree of compatibility to adapt to competition and new use cases. In particular, new attacks and defense mechanisms require to keep the protocol up to date.

While a lot of papers have been published to highlight new attack vectors [5], reproducing these results is generally difficult. This situation significantly complicates the collection of traffic traces for defensive research. Attacks must be reproduced to be thoroughly studied from various perspectives to build comprehensive datasets. These can then be used to design and evaluate intrusion detection and prevention systems.

Wireless IoT protocols introduce new challenges when it comes to experiments repeatability. The nature of protocols themselves introduces technical challenges that could lead to unstable attacks. For instance, the channel hopping mechanism in Bluetooth Low Energy (BLE) requires the attacker to synchronize with its victims before launching its attacks [2]. Moreover, the existence of attacks exploiting the lowest communication layers underlines the need to collect not only the packets but also radio signals. It is typically the case when targeting the Link Layer and Physical Layer in BLE [1] , or when impacting compatibility between wireless technologies.

More importantly, an IoT environment is generally composed of multiple networks based on heterogeneous protocols interconnected by gateways. Building a realistic IoT environment involves encompassing all these elements into a cohesive system. While it is already difficult to produce representative attack datasets for standard protocols on wired networks, IoT protocols face the additional above-mentioned challenges. De Keersmaeker et al. also highlight the lack of exploitable IoT public datasets in their survey [4].

In this poster, we present the development of a platform targeting challenges of experiment repeatability with IoT wireless protocols. This platform aims to generate legitimate and malicious traffic in a realistic IoT environment to support research into intrusion detection in wireless protocols. It provides a set of preconfigured tools allowing to capture and inject traffic from different devices deployed in the environment. The platform is currently under active development. Its final aim is to enable researchers to configure their own experimental setup and launch it automatically.

2 MAIN FEATURES

Legitimate traffic generation. Our approach focuses on deploying off-the-shelf devices composed of commercial products and programmable devices. Commercial devices, such as lightbulbs and smartwatches, generate realistic traffic linked to a specific application. Programmable devices can generate and replay pre-defined traffic. They are configured by the user to choose the traffic suited for their experiment.

Malicious traffic generation. Passive and active attacks can be performed from different nodes, targeting the deployed protocols. Examples of attacks available to platform users include spoofing, Man-in-the-Middle, hijacking, jamming and sniffing. In addition, it is possible to collect generated logs from each attack module.

Multi level monitoring. Monitoring wireless communications efficiently is a key feature of the platform. The platform currently

WiSec '24, May 27–May 30, 2024, Seoul, Korea

ACM ISBN 978-1-4503-XXXX-X/21/06…$15.00
https://doi.org/10.1145/xxxxxxx.xxxxxxx

includes Software Defined Radios (SDR) (e.g., USRP), which collect the whole traffic at the physical layer. Later, the platform will be enriched with more specialized sniffers such as Ubertooth and RZUSBStick. Those directly demodulate the signal, exposing the binary packets. It is also possible to instrument some devices to collect their received and transmitted traffic. This way, we capture traffic on different layers (radio signal, packets) and from different locations (external probe, on-device).

Repeatable and controlled environment. A major challenge in repeating wireless security experiments is the large variety of environments, along with the time and financial cost required to reproduce experimental setups.The platform provides a set of devices and protocols diverse enough to be representative of a realistic environment. The state of all devices can be controlled individually.

3 PLATFORM DESCRIPTION

The architecture of the platform has been designed to simplify the execution of the various experiments and the collect of the corresponding datasets. The platform contains a set of Raspberry Pi controlled with Mirage [3], a Python framework for IoT auditing. It features several well-known short-range wireless protocols, such as Bluetooth Low Energy (BLE), ZigBee, 6LoWPAN and Wifi. For each supported protocol, it embeds analysis and attack modules, as well as means to communicate as a standard device. Of course, some other tools may also be used to carry out specific attacks if necessary. We are also currently working on integrating longer-range protocols such as LoRaWAN. The platform also contains various wireless devices supporting those protocols, that can be controlled or attacked remotely from Raspberry Pi running Mirage, as well as SDR devices. By precisely controlling the environment and the attacks that are performed, this platform generates meaningful data for assessing intrusion detection mechanisms.

The platform is accessed and managed by three machines: 1) A web server, that users access to configure and launch experiments, as well as receive the results ; 2) An orchestrator, that receives commands from the web server and configures the platform accordingly ; and 3) A central monitor linked to a SDR device, allowing to test centralized Intrusion Detection Systems.

Experiments are set up from a web interface where one can specify which commands they want to run, where and when. This generates a JSON file that will then be sent to the orchestrator, and integrated with the output data. The user can also directly provide a JSON file to launch an experiment. For each experiment, the orchestrator first generates a schedule for all devices inside the platform, according to the requested configuration. It contains the different commands that should be run, when, and the execution time, at the end of which the command is killed if it didn't finish. Then, it manages powering on or off the devices needed for the experiment, and sends to each device that should run commands the corresponding individual schedule. Finally, it sends to the central monitor information on the experiment duration and frequency band, to configure correctly the radio receiver.

On reception of this configuration, the central monitor schedules a radio capture at the requested time and frequencies. In the current state of the platform, the monitor analyses the signal to detect the presence of emissions, and returns this information along with the raw signal. In time, users will be able to integrate their own analysis code, for example an Intrusion Detection System that could return its alerts in the experiments logs.

Each experiment generates an archive containing: 1) The raw signal captured during the experiment (in complex format), 2) PCAP files corresponding to the communications identified at the SDR device, 3) Logs from the Mirage commands that were executed during the experiment. The raw signal captures are performed using several USRP B200. This allows recovering a wide band capture from separate synchronized captures from the USRP.

The whole architecture of the platform is described in Figure 1. In its current state, the platform contains: 20 controllable Raspberry Pi 3, plus a last one managing a local Wifi network; 1 controllable Raspberry Pi 4; 2 BLE outlets; 1 BLE lightbulb; 3 BLE smart watches; 1 BLE thermometer; 3 Philips Hue lightbulbs plus an associated gateway; 1 6LoWPAN thermometer linked to a 6LoWPAN water heater (heating control system); 1 WiFi outlet and 1 Google Doorbell.

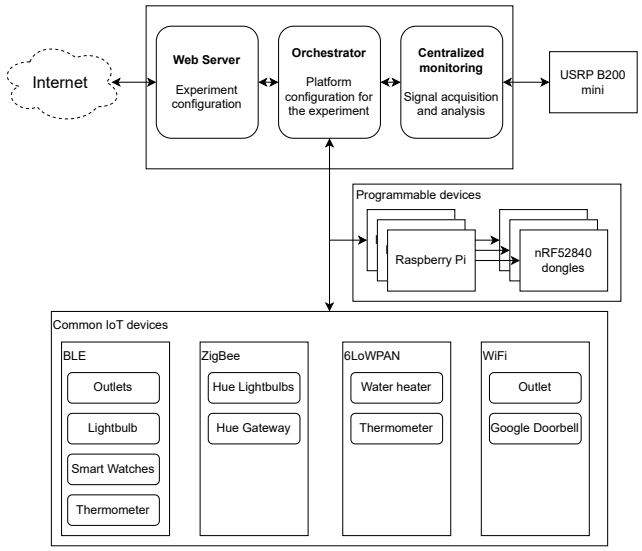

Figure 1: General architecture

4 CONCLUSION

We are currently working on experiment automation and the instrumentation of the commercial devices, to control them more finely. We plan to isolate the platform in a Faraday cage, allow the generation of arbitrary signal from the USRP, and use it to provide several large datasets to the community, including labelled legitimate and malicious activity.

REFERENCES

[1] S. Bräuer, A. Zubow, S. Zehl, M. Roshandel, and S. Mashhadi-Sohi. 2016. On practical selective jamming of Bluetooth Low Energy advertising. In *2016 IEEE Conference on Standards for Communications and Networking (CSCN)*. 1–6. https://doi.org/10.1109/CSCN.2016.7785169

[2] Damien Cauquil. 2018. You'd better secure your BLE devices or we'll kick your butts !. In *DEF CON*, Vol. 26. Available at https://media.defcon.org/DEFCON26/DEFCON26presentations/DEFCON-26-Damien-Cauquil-Secure-Your-BLE-Devices-Updated.pdf.

[3] Romain Cayre, Vincent Nicomette, Guillaume Auriol, Eric Alata, Mohamed Kaâniche, and Geraldine Marconato. 2019. Mirage: towards a Metasploit-like framework for IoT. In *2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE)*. Berlin, Germany. https://laas.hal.science/hal-02346074

[4] François De Keersmaeker, Yinan Cao, Gorby Kabasele Ndonda, and Ramin Sadre. 2023. A Survey of Public IoT Datasets for Network Security Research. *IEEE Communications Surveys Tutorials* 25, 3 (2023), 1808–1840. https://doi.org/10.1109/COMST.2023.3288942

[5] Jianliang Wu, Ruoyu Wu, Dongyan Xu, Dave Tian, and Antonio Bianchi. 2023. SoK: The Long Journey of Exploiting and Defending the Legacy of King Harald Bluetooth. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 23–23.