PROJECT PROPOSAL – SPRING 2023

PROJECT 100 HOURS = 5 ECTS

POST MASTER 18 & 24 MONTHS
ITS
SIC

Master 24 months in TU Opening
Data Science
Digital Security
IOT
Mobile Communication

PROJECT 200 HOURS = 10 ECTS

Master Double Diploma 18 months
Data Science
Digital Security
IOT
Mobile Communication

Cursus 6-12 months

Supervisor(s): Aurélien Francillon/ Romain Cayre

Number of students/group max.: 2

PROJECT TITLE: Security analysis of Bluetooth Low Energy Over-The-Air firmware updates

PROJECT DESCRIPTION:

- For 100 HOURS project

nRF51 and nRF52 chips from Nordic SemiConductor are widespread in Bluetooth Low Energy (BLE) enabled IoT devices, such as smartwatches or smartlocks. Nordic SemiConductor provides a proprietary Device Firmware Update process, allowing to update the firmware running on a device over a BLE connection, from a smartphone or a computer. It is implemented as a Bluetooth Low Energy GATT Service and a set of associated characteristics.

This project aims to reverse engineer this OTA firmware update process, document its internals and identify potential vulnerabilities. The main goal is to evaluate the attack surface exposed by this critical service and estimate if an attacker can compromise the target device by injecting a malicious firmware update.

- For 200 HOURS project (additional tasks)

- Implementing wireless attacks using a research framework to inject malicious firmware updates.
- Building a fingerprinting tool, allowing to identify the presence of this service in surrounding BLE devices.
- Developing a Play Store crawler to evaluate the deployment of this OTA update process in companion Android applications, by detecting the presence of associated libraries.