Internship Description

RF fingerprinting on NFC devices (Bachelor Thesis)

Position purpose: Develop a tool to identify NFC devices by analysing the RF spectrum of their transmitted signals

Duration: 450 hours

Detailed description

RF fingerprinting is a technique that allows the identification of radio transmitters (such as IoT devices) by analysing the spectrum of their transmissions. This analysis can typically be performed using machine learning algorithms. Prior research on this topic exists but has been tested as sub-optimal (i.e. overfitting).

NFC technology is often used in access control and payment applications but many implementations are vulnerable to relay attacks with research and tools that facilitate such attacks being publicly available.

The goal of this project is to determine if RF fingerprinting could be used as an authentication technique against relay attacks.

The main steps of this project are the following:

- Build a simple lab setup with Software-Defined Radio (SDR) equipment to acquire signals between an NFC device and its reader
- Acquire RF spectrum data of various NFC devices
- Analyse the signals
- Classify the signals of the devices by using supervised machine learning classification techniques in order to differentiate trusted devices from attacker / relay devices
- Determine if this identification technique could be used as an authentication feature against relay attacks

As the receiving equipment (SDR) has an influence on the recorded signals, for this project we consider a single receiver to record the RF samples. Similarly, the lab setup should be built to provide an ideal low-noise & low-interference environment to simplify the analysis phase.

Collaboration with other researchers in this field is wished (EPFL, ElectroSense).

Profile

- School knowledge and experience in Machine Learning
- Interest in the Software-Defined Radio technology and signals processing
- Fluent French or English mandatory