HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Department: Information and communication technologies
Faculty: Information technology and communication systems
Orientation: Software engineering

Bachelor Thesis

RF fingerprinting on NFC devices

Not confidential

Student: Luc Wachter

Project proposed by: Joël Conus
Kudelski Group SA
22-24, Route de Genève
1033 Cheseaux-sur-Lausanne

Teacher in charge: Prof. Alberto Dassatti

Academic year: 2019-2020

Yverdon-les-Bains, 27th May 2020

HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Information and communication technologies
Information technology and communication systems
Software engineering
Student: Luc Wachter
Teacher in charge: Prof. Alberto Dassatti

Bachelor thesis 2019-2020

RF fingerprinting on NFC devices

Company name

Kudelski Group SA

Publishable summary

Dans ce travail... → Ceci est le résumé publiable...

Student:	Date and place:	Signature:
Luc Wachter	.....	.....
Teacher in charge:	Date and place:	Signature:
Prof. Alberto Dassatti	.....	.....
Company name and contact:	Date and place:	Signature:
Joël Conus Kudelski Group SA	.....	.....

Préambule

Ce travail de Bachelor (ci-après TB) est réalisé en fin de cursus d'études, en vue de l'obtention du titre de Bachelor of Science HES-SO en Ingénierie.

En tant que travail académique, son contenu, sans préjuger de sa valeur, n'engage ni la responsabilité de l'auteur, ni celles du jury du travail de Bachelor et de l'Ecole.

Toute utilisation, même partielle, de ce TB doit être faite dans le respect du droit d'auteur.

HEIG-VD

Vincent Peiris
Chef de département TIC

Yverdon-les-Bains, le 27th May 2020

Authentication

The undersigned, Luc Wachter, hereby certifies that he has carried out this work and has not used any other source than those expressly mentioned.

Le soussigné, Luc Wachter, atteste par la présente avoir réalisé ce travail et n'avoir utilisé aucune autre source que celles expressément mentionnées.

Yverdon-les-bains, le 27th May 2020

Luc Wachter

Scope statement

Scope statement for RF fingerprinting on NFC devices (Bachelor Thesis)

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

Duration: 450 hours (ends 31st July 2020)

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.

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.

The expected deliverables are the following:

- A tool able to identify NFC devices by analysing the RF spectrum of their signals, at least in an ideal environment and with a small number of devices
- A detailed account of the steps taken and the setup used (as part of the report)
- An analysis of the results (as part of the report)

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

Table of contents

Introduction

Description

RF fingerprinting is a technique that allows the identification of radio transmitters by extracting small imperfections in their spectrum. These imperfections are caused by tiny manufacturing differences in the devices' analog components. Using Software-Defined Radio (SDR) equipment, we can analyse this spectrum in order to extract the aforementioned differences and identify a device.

Such technique can be used on any type of radio transmission: Bluetooth, BLE, WiFi, LTE, etc. This project aims to use RF fingerprinting on NFC devices. Indeed, NFC is often used in access control and payment applications but many implementations are vulnerable to relay attacks. Spoofing the imperfections in an emitter's radio spectrum is close to impossible at the present time, since it is essentially a hardware signature. This is why a technique like the one described here would be a valuable additional security layer.

The goal of this project is to determine if RF fingerprinting of NFC devices could be used as an authentication technique, in order to prevent relay attacks.

Context

This project is conducted in the context of my bachelor thesis at HEIG-VD.

- Department: Information and communication technologies
- Faculty: Information technology and communication systems
- Orientation: Software engineering

State of the art

Conclusion

List of Figures

List of Tables