Bachelor Thesis

RF fingerprinting on NFC devices

Student:	Luc Wachter
Project proposed by:	Joël Conus Kudelski Group SA 22-24, Route de Genève 1033 Cheseaux-sur-Lausanne
Teacher in charge:	Alberto Dassatti
Academic year:	2019-2020

Yverdon-les-Bains, 29th March 2020

1 Specification

Table of contents

2 Summary

3 Introduction

3.1 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.

3.2 Context

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

- Department: Information and communication technologies
- Sector: IT and communication systems
- Faculty: Software engineering

4 State of the art

5 Conclusion

List of Figures

List of Tables