Security of NFC-enabled mobile devices

Mark Vijfvinkel & Aram Verstegen
4077148 4092368

Abstract

Near Field Communication [ISO] is a short-range, low-power wireless communication system that uses the same principles as various *RFID* implementations. It's intended to be integrated into mobile devices, allowing for *contactless* payment applications. NFC is a relatively new technology which might have a big impact on the way we pay and gain access to buildings, computer systems or even public transport. Because of these applications and the number of people that will be using it, it is necessary to research how secure NFC really is. In this literature study we will look at the possibilities of NFC applications for mobile devices, document the architecture of NFC systems and identify some of the known and foreseen vulnerabilities.

1 Problem

These days most people have at least two things in their pocket, a mobile device (this can be a mobile phone, PDA or nowadays a combination of those two, called a *smartphone*) and a wallet. In the wallet there is a certain amount of money, either in the form of cash or a bankcard, or both. And with this everything is paid, from small *micropayments* (e.g. candy from a machine) to big purchases in a shop.

Recently a pilot has started [Pay] that integrates a person's payment card(s) into their mobile device using the NFC standard [ISO].

1.1 Research question

At the end of our research we will try to answer to following research question:

> What is the security architecture of NFC applications for mobile devices and what are some of the known and foreseen vulnerabilities?

1.1.1 Sub-questions

In order to answer the main research question, we'll answer the following sub-questions.

- What is the architecture of NFC-enabled mobile device? (e.g. hardware, software and communication)
- What are the possibilities of the NFC devices?
- What are some of the known vulnerabilities in NFC or NFC-like applications?
- How do these vulnerabilities work?
- Based on the architecture and known vulnerabilities, what could some foreseen vulnerabilities be?
- What might be possible countermeasures against these foreseen vulnerabilities?

1.1.2 Hypothesis

We are able to give the following hypothesis:

We think that most new vulnerabilities will be found in applications built on top of NFC systems, rather than in the NFC architecture itself. We envision vendors might try to apply existing business rules to this new system, even if their understanding of it is oversimplified.

2 Scope

We are aware that because of the time restrictions in place, we won't be able to cover the entire breadth and depth of NFC systems. In some implementations of an NFC system, a back-end is used to handle transactions. Because the back-end is likely to be different for each implementation, we will scope our research down to the technical details of a generalized NFC interaction. We will provide an up-to-date introduction to the possibilities of an NFC-enabled mobile device and the architecture it's built upon, focussing on the security model. Using this work as a guideline we will document known vulnerabilities in NFC applications, examining their technical details. We will mention known countermeasures for any vulnerabilities that we discuss. If time permits, we hope to illustrate these vulnerabilities by including a case study.

3 Motivation

With the current technology it is possible to make everyday jobs or actions easier and more comfortable. It is now possible to take your phone with you, instead of calling from a house, as was the case a few years ago. Instead of paying with coins and bills, we now pay using a bankcard. But in this century, the evolution of technology does not stop. So applications like paying with your phone come to mind. These days the development schedules are so tight, some details may be overlooked because companies may simply try to apply old methods to new technology. For systems requiring a high level of security, these kinds of oversights can be devastating.

In our opinion security issues should be addressed in any ICT project. Especially when the system will be exposed to the general public and a lot of people will depend on it for their day-to-day lives. When NFC-enabled devices take off and people start using NFC-based applications, it will be too late to makes significant changes that will improve security. Therefore we think it's very important to research and document the known security issues regarding NFC-enabled devices.

4 Strategy

In our study we want to investigate the architecture of NFC-enabled devices with a focus on the technical details of the security model. We first hope to reach a general, high-level understanding of the system's capabilities and uses, and write a solid introduction before delving into the more technical details. We will do this by summarizing existing work (such as [Pau07], [KKI09] and others) on the general workings of NFC systems.

After this high-level introduction which illustrates the context of our research we will limit our scope to the NFC devices themselves and will document the architecture of the security mechanisms in place. There is plenty of literature (such as [Mul09], [KW05] and others) to guide us in researching the security aspects of NFC systems. We hope to be able to point out some known or possible vulnerabilities in these. We would like to also include a case study of an NFC system implementation. This could be entirely theoretical but if time permits, would warrant some practical experimentation.

5 Time schedule

Week	Date	Activity	Deliverable
39		Researching NFC	
40	8-10	Researching NFC	Introduction chapter
41	15-10	Technical analysis, NFC communication	chapter NFC communication
42	22-10	Technical analysis, hardware architecture	chapter hardware architecture
43		Autumn break	
44	5-11	Technical analysis, generic software	chapter generic software
45		Case studies, analyse security	
46	19-11	Case studies, analyse security	chapter case studies
47		Preparing presentation and draft paper	
48		Preparing presentation and draft paper	
49	6-12		Draft paper and presentation sheets due
49	7-12		Final presentation
49	9-12	Supervisor review	
50	17-12	Feedback due	
51		Christmas break	
52		Christmas break	
1		Revise paper	
3	17-01	Revise paper	Revised final paper due

References

[ISO] ISO 10303-203:1994. *Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)*. ISO, Geneva, Switzerland.

[KKI09] Raine Kelkka, Tommi Kallonen, and Jouni Ikonen. Remote identification and information processing with a near field communication compatible mobile phone. In *CompSysTech '09: Proceedings of the International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing*, pages 1–6, New York, NY, USA, 2009. ACM.

[KW05] Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. pages 47–58, 2005.

[Mul09] C. Mulliner. Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. In *Proceedings of the 1st International Workshop on Sensor Security (IWSS) at ARES*, Fukuoka, Japan, March 2009.

[Pau07] Annika Paus. Near field communication in cell phones. A useful introduction to NFC technology, also touching on some of the security aspects, 2007.

[Pay] Payter. Proef rotterdam. `http://www.payter.nl/default.aspx?cp=content&contentcode=ProefRotterdam&language=nl`. webartikel over een proef met NFC telefoons in Rotterdam.