# Survey of mobile network security in trending technologies, focusing on Bluetooth and NFC

Johannes Kurz
e0727957

Gerhard Schraml
e0728067

April 19, 2015

**Abstract**

Write a short abstract about the topics contained in the paper. This is usually the last step to do.

## 1 Introduction

What you should include in the introduction

- Describe the topic (Importance, Significance)
- Give a summary of the surveyed topic

| paper structure proposal | |
|---|---|
| 1 - 1½ page | title + abstract + introduction |
| 1 page | mobile networks security basics general |
| ½ page | nfc general description |
| ½ page | nfc threat introduction and listing |
| 3 - 5 pages | nfc threats in detail (1 page per threat?) + solution |
| 4 - 6 pages | bluetooth TODO shorty |
| ½ page | conclusion |
| 1 - 2 pages | references |
| 11½ - 17 pages | total |

# 2 Mobile Networks Security Basics General whatever

# 3 Security in Near Field Communication

## 3.1 Terms and general description

More and more people world wide start using *Near Field Communication* (NFC) for personal purposes. Goal of the technology is the convenient transfer of small amounts of data by just simply wiping compatible devices over each others. As the communication is contactless, bringing sender and receiver to close proximity suffices to establishing a connection. Usually the working distance for NFC connections does not exceed about 10 to 20 centimeters. The technology is based upon *Radio-Frequency Identification* (RFID) - it similarly uses electromagnetic radiation for transporting signals over small distances. Therefor a small magnetic field is established with the purpose of bridging the physical space between participating devices.

Basically two types of NFC devices exist. *Active devices* take care of the establishment of the necessary magnetic field. As this is an energy-consuming task, they are usually connected to a power supply. *Passive devices* normally don't possess a built-in power supply. They make use of small amounts of power they are able to harvest from the magnetic field issued by a connected active device. Hence, passive devices are idle when there is no connection present. Typical examples for such devices are so-called NFC tags, e.g. containing additional information about an exhibit in a museum where it is attached to. A user could then easily access this information by hovering its NFC-enabled electronic device, capable of reading the NFC tag, over it.

Mobile devices can choose out of three different communication modes. In *Peer-To-Peer* mode, two active NFC-enabled devices communicate on an equal basis. Usually the task of emitting the necessary magnetic field is carried out in an alternating way by both participants. In *Reader/Writer* mode an active device is reading data from respectively writing data to passive NFC tags. Finally, in *Card Emulation* mode a mobile device is acting as NFC tag allowing other (active) devices to read information from it. This mode is mostly used for electronic ticketing or contactless payment applications using mobile phones.

## 3.2 Selected security threats

bar bar foo foo einfhrender text ein paar zeilen was es nicht alles gibt bar bar foo foo bar bar foo foo bar bar foo foo bar bar foo foo

### 3.2.1 Smart Poster Spoofing

Typically, NFC communication between mobile devices and tags (or other devices) uses the *NFC Data Exchange Format (NDEF)*. It is defined by the NFC Forum[1], a standardization organisation in the area of NFC. The NDEF format consists of several record data types, headed by *Text*, *URI* and *Smart Poster* record types.[5]

Text records simply contain an arbitrary, human-readable text, optionally followed by a language identifier.

URI records include a URI of arbitrary protocol pointing to further information or an action to perform. Based on the protocol, e.g. HTTP, TEL, SMS, MAILTO, the receiving device determines the target application to deal with the given URI. Thus the NFC subsystem of a device can be seen as kind of a job dispatcher.

Smart Poster records usually consist of a text record, containing the title or short description of a hovered NFC tag, and a URI record pointing to some more detailed information on the item the tag is attached to. One proper use case is, as already mentioned above, to provide further information on museum exhibits by just hovering the attached NFC tag.

**Manipulating the content of a Smart Poster** In [5], a way of tricking users into acknowledging actions, they actually don't want to perform, is presented. One could physically replace smart tags with new ones containing malicious information. Due to limitations of a smart phone device, expected information is shown at the display of a victims device, while the underlying action e.g. links to an attackers site. In the test, a Nokia 6131 device was used, which would display only the text content of a Smart Poster if it exceeds the screen size. Thus, the transported URI is, at least at first sight, not presented to the user. Figure 1 shows an example of how such a spoofed message could be constructed. Another example is the abuse of the TEL protocol issuing a phone call. The attacker could display a trusted phone number while actually attaching a premium rate number leading to unwanted expenses for the victim.

[1] `www.nfc-forum.org`

```
Title: Bank of Germany
URL:   https://www.bankofgermany.de
```

(a) Original Smart Poster

```
Title: Bank of Germany\rhttps://www.
         bankofgermany.de\r\r\r\r\r.
URL:   http://www.attacker.com
```

(b) Malicious Smart Poster

Figure 1: Smart Poster Spoofing Example[5]

**Countermeasures against Smart Poster Spoofing** [7] presents S-SPAN, a system aiming at securing the use of Smart Poster reads from NFC tags. Basic approach is not to store the actual information in plain text on the NFC tag. The tag rather contains a non-guessable and non-human-readable identifier which is used to locate the Smart Poster contents in a online database. The user of the mobile device has to be logged into the online database when touching the NFC tag. Over secured connection, the database is queried for the identifier and replies with the actuals contents. The contents of the database are administered by the owner of the smart tag. Identifiers are never used twice to prevent accidental usage of old tags. Consequently, Smart Poster can expire at some time. The approach entails better security as actual URIs are always retrieved by a trusted entity. On the other hand, additional latency has to be accepted for querying the database.

[3] refers to the latency problem of S-SPAN and presents a "Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters". The proposed middleware is run between the NFC controller and the application layer of the device and takes care of all Smart Poster tag reads. In contrast to S-SPAN, data (Text and URI) is directly stored on the tag. The middleware, depicted in figure 2, performs a series of checks against the delivered URI. First, a *white list* is queried against the URI. If the given URI can be found, the Smart Poster is directly forwarded to the application layer. If not, a *black list* approach is performed. If the URI is blacklisted, the middleware prompts the user to decide on whether to continue reading the Smart Poster. If the URI is not blacklisted, a final validation attempt is made by querying *Crowd-sourced Internet Website Reputation Ratings*. When the query results in a predefined minimum reputation score, the Smart Poster again is forwarded. Performance observations show, that white- and blacklist hits cause very low latency, while reputation querying takes a maximum of 1 second in the given test environment.

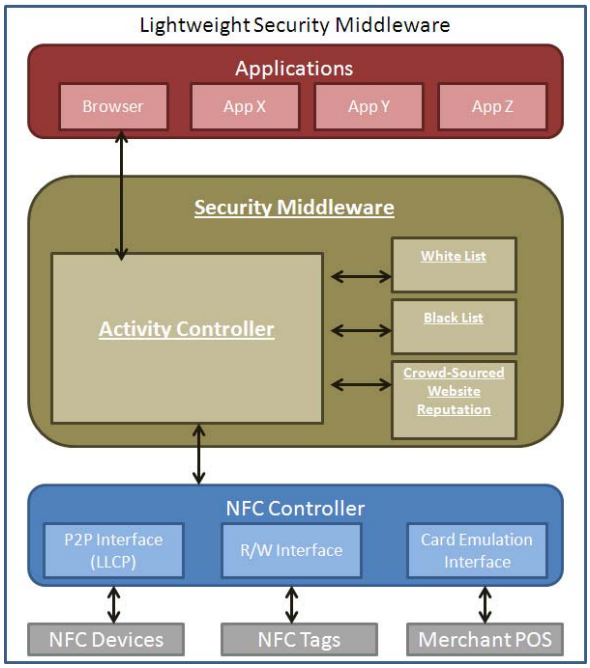


Figure 2: NFC application architecture from [3]

### 3.2.2 Eavesdropping

threat description and possible solution (*nShield*) [8]
bar bar foo foo

### 3.2.3 Relay attacks

TODO man-in-the-middle? more general than relay attacks?
Problem description, practical implementations and countermeasures [4] [1] [6]
bar bar foo foo

### 3.2.4 Signal jamming

*EnGarde* - rule based signal jamming as a protection mechanism [2]
TODO denial of service? = basically just jamming the signal
bar bar foo foo

# 4 Security in Bluetooth communications

# 5 Conclusion

Put your conclusion about the topic here

# References


[1] Lishoy Francis, Gerhard P. Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. In Siddika Berna Ors Yalcin, editor, *Radio Frequency Identification: Security and Privacy Issues - 6th International Workshop, RFIDSec 2010, Istanbul, Turkey, June 8-9, 2010, Revised Selected Papers*, volume 6370 of *Lecture Notes in Computer Science*, pages 35–49. Springer, 2010.

[2] Jeremy Gummeson, Bodhi Priyantha, Deepak Ganesan, Derek Thrasher, and Pengyu Zhang. Engarde: protecting the mobile phone from malicious NFC interactions. In Hao-Hua Chu, Polly Huang, Romit Roy Choudhury, and Feng Zhao, editors, *The 11th Annual International Conference on Mobile Systems, Applications, and Services, MobiSys'13, Taipei, Taiwan, June 25-28, 2013*, pages 445–458. ACM, 2013.

[3] Sufian Hameed, Bilal Hameed, Syed Atyab Hussain, and Waqas Khalid. Lightweight security middleware to detect malicious content in NFC tags or smart posters. In *13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014, Beijing, China, September 24-26, 2014*, pages 900–905. IEEE, 2014.

[4] Gerhard P. Hancke, Keith Mayes, and Konstantinos Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615–627, 2009.

[5] Collin Mulliner. Vulnerability analysis and attacks on nfc-enabled mobile phones. In *Proceedings of the The Forth International Conference on Availability, Reliability and Security, ARES 2009, March 16-19, 2009, Fukuoka, Japan*, pages 695–700. IEEE Computer Society, 2009.

[6] Michael Roland, Josef Langer, and Josef Scharinger. Relay attacks on secure element-enabled mobile devices - virtual pickpocketing revisited. In Dimitris Gritzalis, Steven Furnell, and Marianthi Theoharidou, editors, *Information Security and Privacy Research - 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete,*

*Greece, June 4-6, 2012. Proceedings*, volume 376 of *IFIP Advances in Information and Communication Technology*, pages 1–12. Springer, 2012.

[7] Jason Wu, Lin Qi, Ram Shankar Siva Kumar, Nishant Kumar, and Patrick Tague. S-SPAN: secure smart posters in android using NFC. In *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, USA, June 25-28, 2012*, pages 1–3. IEEE Computer Society, 2012.

[8] Ruogu Zhou and Guoliang Xing. nshield: a noninvasive NFC security system for mobiledevices. In Andrew T. Campbell, David Kotz, Landon P. Cox, and Zhuoqing Morley Mao, editors, *The 12th Annual International Conference on Mobile Systems, Applications, and Services, MobiSys'14, Bretton Woods, NH, USA, June 16-19, 2014*, pages 95–108. ACM, 2014.