The Third International Conference on Availability, Reliability and Security

NFC Devices: Security and Privacy

Gerald Madlmayr, Josef Langer
University of Applied Sciences of Upper Austria, Hagenberg
{gmadlmay, jlanger}@fh-hagenberg.at

Christian Kantner
mobilkom austria AG
c.kantner@mobilkom.at

Josef Scharinger
Johannes Kepler University
josef.scharinger@jku.at

Abstract

The aim of this paper is to show security measures for NFC (Near Field Communication) use cases and devices. We give a brief overview over NFC technology and evaluate the implementation of NFC in devices. Out of this technology review we derive different use cases and applications based on NFC technology. Based on the use cases we show assets and interfaces of an NFC device that could be a possible target of an attacker. In the following we apply different attacks against the operation modes to show how applications and devices could be protected against such attacks. The information collected is consolidated in a set of threats giving guidelines on how to improve security and overcome privacy issues. This allows integrating NFC technology in a secure way for the end consumer.

1 Introduction

NFC (Near Field Communication) is a wireless proximity communication technology, allowing us to transfer data over a distance of up to 10 cm. The major advantage of NFC over other wireless communication technology is *simplicity*: transaction are initialized automatically, simply be touching a reader, another NFC device or an NFC compliant transponder. NFC technology gives additional functionality to a mobile device, like using it as a contactless credit card or as a contactless bus ticket. Bluetooth and WiFi connections can be established simply by touching a transponder. Estimations show that by 2012 there are about 180 million mobile devices (equivalent to 20 % penetration) equipped with this technology [1].

Combining a wireless communication technology with applications such as payment and ticketing in one device may raise potential privacy issues and security risks. Attacks against an NFC device can be performed anywhere and may not be noticed by the victim as the communication itself is contactless. Additionally, the benefit achieved from taking over an NFC device is high. Attackers would be able to abuse payment functionality or use the device for voice calls or data traffic [2]. Thus the integration of both – technology and applications – needs to go hand in hand to protect the device and the consumer.

The following section introduces NFC technology and its operation modes. Chapter 3 shows use cases for NFC and potential attack scenarios in RFID environments that can be used and adapted for NFC devices and applications. The threat model proposed in this chapter, is a cross combination of attack scenarios and use cases. Finally we provide a conclusion in the ending section.

2 Technological aspects of NFC

NFC is a bidirectional, proximity coupling technology based on to the smart card standard ISO14443. The physical and data link layer of NFC peer-to-peer mode is already standardized in ISO18092, whereas applications, device architecture and related topics are still discussed by the NFC-Forum[1].

An NFC device features the following operating modes [3]. (See table 1 for related use cases.)

Reader/Writer Mode (Proximity Coupling Device, PCD): Operating in this mode, the NFC device can read and alter data stored in NFC compliant passive (without battery) transponders. Such tags can

[1] `http://www.nfc-forum.org`

0-7695-3102-4/08 $25.00 © 2008 IEEE
DOI 10.1109/ARES.2008.105

be found on *SmartPoster* e. g., allowing the user to retrieve additional information by reading the tag with the NFC device.

Card Emulation (Proximity Inductive Coupling Card, PICC): An NFC device can also act as smart card (ISO14443) after being switched into card emulation mode. In this case an external reader cannot distinguish between a smart card and an NFC device. This mode is useful for payment and ticketing applications for example.

Peer-to-Peer (Near Field Communication, NFC): The NFC peer-to-peer mode (ISO18092) allows two NFC enabled devices to establish a bidirectional connection to exchange contacts, Bluetooth pairing information or any other kind of data. To establish a connection a client (NFC peer-to-peer initiator) is searching for host (NFC peer-to-peer target) to setup a connection.

The standards ISO14443 (for contactless smart cards) and ISO18092 (for NFC peer-to-peer mode) do not specify encryption or security for the contactless communication at all. Such a feature must be implemented by the developer on application level. At the moment the two major players in the smart card market, NXP Semiconductors with their product *Mifare* and Sony with *Felica*, have implemented a proprietary encryption for their products on top for securing the communication.

2.1 Architecture

Besides the NFC controller for the analog digital conversion of the signals transferred over the proximity connection, NFC devices include a secure smart card chip. This integrated circuit is also referred to as the secure element (SE) for the so called tag emulation operating mode. The secure element is connected to the NFC controller for proximity transactions (external mode for payment at point of sale e. g.). Also host-controller is able to exchange data with the secure element (internal mode for top up of money into the secure element over the air e. g.) as illustrated in Fig. 1. The physical link between the secure element and the NFC controller has not yet been defined. Currently the GSMA[2] is evaluating different options like S2C (Signal-in - Signal-out Connection) and SWP (Single Wire Protocol), whereas the SWP is the favorite option of the NFC working group of the GSMA [4]. Different implementations of secure elements are extensively discussed in [5].

[2] `http://www.gsmworld.com/`

NFC is closely related to RFID (Radio Frequency Identification). RFID is mainly used for remote tracking, tracing and identification of goods and persons without a line of sight. NFC on the other hand is used for more sophisticated and secure transactions like contactless access or payment. The benefit of the short operating distance is that transactions are usually only caused on purpose. Both technologies have several layers and protocol concepts in common and therefore are open for the same attacks.

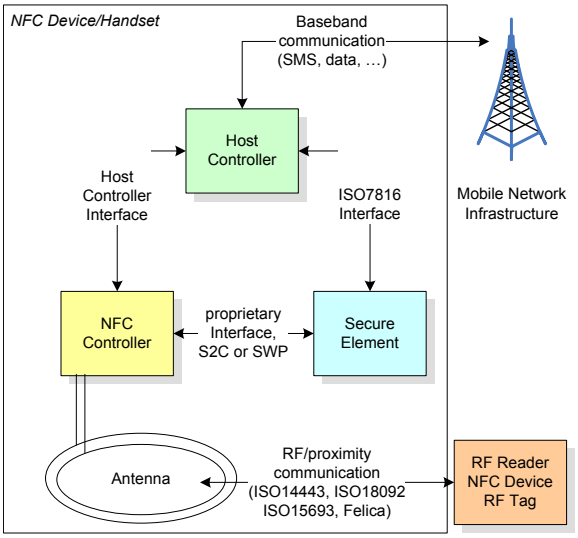

Figure 1. Architecture of NFC integrated in a mobile device.

3 Related work

Avoine shows in [6] a sound adversary model for attacking encrypted data transmissions and protocols over RF technology and thus provides a sound starting point for security in this regard.

RFID and smart card chips, like those acting as secure elements, have fixed IDs allowing a 3rd party to track people carrying such a transponder. The option of using a fixed or random UID can be specified during the personalization process if the smart card chip supports this option. Electronic passports for example have a random UID. Hayangjin and Jeeyeon line out this issue in [7].

Relay attacks are possible in RFID infrastructures as standards like ISO14443 do not deal with roundtrip times. Hancke et al. show this issue in detail in [8] and also propose a solution using an RFID distance bounding protocol in [9]. Unfortunately this is nei-

ther implemented in the smart card nor in the newer NFC standard. As long as such RFID transponders are readable by an external reader, relay attacks can be performed.

Cloning of tags – if possible – has the same impact as relay attacks with the big advantage to the attacker that the RFID tag can be reused without the victim. Heydt-Benjamin et al. show in [10] how to clone and abuse RFID credit cards of the first generation. Cards of this type could also be integrated into NFC devices offering a tag emulation mode.

In the following we deal with technology related attacks and do not consider attacks on protocols and above.

4 Threat Model

Due to contactless reading and identification of transponders without a line of sight, privacy as also security concerns go hand in hand with this technology. As the standardization of integrating NFC into mobile devices is still ongoing, there is a chance that security and privacy issues are well considered. Hence we analyze devices and technology as far as possible to provide a comprehensive report on those issues related with NFC.

For building our threat model we rely on the threat model process described in [11]. At first we start off with describing the possible use cases of NFC and derive assumptions. Out of this we show the communication interfaces of the NFC technology integrated in the device and how these interfaces are protected. Out of this bulk of information we compose a list of threats showing the main areas to turn to, regarding security and privacy.

4.1 Use cases

Our analyses depend on a device integrating the NFC controller and the secure element as described in section 2.2. In the following we line out the operation modes and use cases to be considered:

Use of the unique ID: Each contactless smart card chip has a unique ID (ISO14443 A: UID, ISO14443 B: PUPI, Felica: IDm) which is 4, 7 or 10 Bytes long. This ID is needed for anti-collision during the process of contactless reading of transponders. As this ID is unique it could be used for identification. The ID can be already acquired during the selection process of the transponder and therefore is done in a quick way. Reading this ID does neither use encryption nor requires authentication of the reading device.

External mode of secure element: Smart card chips in NFC devices are needed for emulating a tag. In external mode, these secure elements can be accessed by an external reader. An external reader cannot distinguish between a smart card and an NFC device with a secure element in external mode. Running a credit card applet in the secure element turns the NFC handset in a mobile payment device.

Handset reads external tag: The content of an external RFID smart card chip is read by an NFC device. Currently the NFC Forum is standardizing the data format (NDEF; NFC Data Exchange Format) specifying the data types and data structure on the tag. Such tags can store information for opening a URI in a web browser or pairing information for a WiFi or Bluetooth connection. More generally speaking, by touching a tag containing an appropriate NDEF, the mobile device is about to launch an application to process the NDEF data.

Data exchange using NFC: Based on the NFC peer-to-peer mode (ISO18092) two NFC devices can exchange data using the NDEF. This data format is suitable for exchanging electronic business cards or pairing information, for example. The transaction protocol below does not include encryption or authentication. Therefore the application needs to implement means of security to ensure authenticity, integrity, and confidentiality. This use case itself is similar reading an external tag, but with the difference that the tag read, is exchanged by an NFC device in target mode.

Internal mode of secure element: A slightly different operating mode is reading and altering of information in the secure element through the host controller. In this case the information (data or applications) in the secure element can be altered by applications running on the host controller of the handset. This feature in combination with an online connection (GRPS e.g.) allows the remote management of data and information stored in the secure element. Therefore it is also called OTA (over the air) management. For NFC applications like ticketing this feature must be considered in detail, as it is the major advantage to using ordinary smart cards. The online connection could be used to store remotely tickets/money in the secure element.

4.2 Assumptions

For the following threat model and analysis we made some assumptions:

Communication Flow	*Operation Mode*	*Communication Interface*	*Use case*
(1) Use of unique ID Handset providing data Reader collecting data	– Tag Emulation Read/Write	ISO14443	Access Loyalty
(2) External mode of secure element Handset providing data Reader collecting data	– Tag Emulation Read/Write	ISO14443	Access Loyalty Payment
(3) Handset reads external tag Tag holding data Handset reading tag/target	– tag (emulation) Read/Write	ISO14443	BT/WiFi-Config VCard transfer SmartPoster
(4) Data exchange using NFC NFC target providing data Handset collecting data	– Peer (Target) Peer (Init)	ISO18092	BT/WiFi-Config VCard transfer data exchange
(5) Internal mode of secure element Secure elements in the handset Host Controller Application	– Internal mode Comm. channel to SE	ISO7816	OTA provisioning Ticket upload Money top up

Table 1. NFC Device Operating Modes

- The mobile device is a handset with a host controller allowing the use of GSM/UMTS.
- The NFC controller can feature three operating modes for RF/NFC applications.
- The secure elements can be accessed by the host controller or through an NFC connection (but not at the same time) whereas the communication flow is controlled by the NFC controller.
- Secure elements are tamper-proof and therefore only can be attacked through its defined interfaces by sending APDUs (as defined in ISO7816-4).
- To access data and/or applications stored in tags or secure elements an access key is needed.

4.3 Components and Trust Levels

The three major components and the trust levels are the following:

Host controller: By compromising the host controller or applications in the host controller, processes initialized by the NFC controller can be blocked, modified or eavesdropped. Secondly data received during the OTA management of the secure element can be blocked, modified or eavesdropped. Malware can make use of other data stored on the host controller (address data e.g.) or abuse functionality of the handset (air time, sending short messages e. g.).

Applications on the host controller may run even without the knowledge of the user. Applications can be given more trust by signing them with a code signing certificate to put them into a different security domain on the handset. In any case, this component is considered as untrusted.

NFC controller: Modifying the NFC controller can end up in disabling the NFC functionality of the device. Additionally all data transferred over the RF can be block, modified or eavesdropped including the unique IDs of the smart card chips. Additionally the communication flow between the secure elements and external readers or the host controller can be (re)routed.

Secure Element: The secure element is the only secure place in an NFC device. Although, applications using weak encryption or being implemented insecurely can be attacked through the RF interface as well as the host controller. Additionally an attacker could add a modified secure element to the device and make use of security leaks (as the communication between the secure elements and the NFC controller is not yet fixed, this case is not considered at the moment).

4.4 Assets to be protected

The major assets to be protected are the following:

- The User's privacy being represented by the data stored on the host controller (address book, short messages e. g.) as well as information in the secure element (prepaid money, tickets e. g.).

- Operability of the device (voice and data connectivity as well as NFC functionality).
- Functionality of the host controller (for voice and data traffic) as well as functionality of applications in the secure element (for payment, access e. g.).
- Information transferred over the RF link.

4.5 Threats

Out of the components discussed so far we are able to derive several cases that are vulnerable to attacks. Avoine proposes four different threat categories for RFID-Systems in [12], which are the following: DoS (Denial of Service), impersonation, information leakage and malicious traceability. We now map these categories to an NFC device:

Denial of Service: Just touching an NFC device – even with an empty tag – causes a reaction of the device. Even if it is only an error message, this is a simply way to occupy the device. Thus there should be some kind of mechanism controlled by the user to turn on and of the NFC reader/write functionality.

Relay data transferred over the RF: As discussed in chapter 2 both standards ISO14443 and ISO18092 are open to relay attacks which can neither be recognized by the card nor by the reader. An additional issue in this context is the so-called battery-off mode. In this case the smart card functionality could even be relayed if the battery was removed from the device. From the current point of view a button on the device to turn on tag emulation would be a sufficient implementation. It is an easy and suitable solution for both the handset manufacturers and consumers which provides a sound security, regarding replaying, skimming and also tracking and tracing. Additionally we would like to point out that, if a user removes the battery of his device it must not be able to be used for any communication. But a functionality without the device being powered on should be considered. This *NFC transaction flight mode* would be useful in case the device runs out of battery but the user still wants to use it for access or payment.

Skimming of applications in the secure element: Both memory cards (NXP's Mifare Application Directory e.g.) and processor cards (JCOP e.g.) provide an index of applications stored in the secure element. Unfortunately this feature allows 3rd party players also to see which other applications there are on the secure elements. This is not an issue directly related to the NFC technology but more to the smart card industry. However, as NFC will probable make smart cards redundant as they are likely to be integrated into future NFC handsets, this is a privacy issue that should be turned to.

Managing in-device security: Applications running on the host controller need to authenticate against the secure element before a communication can be established. Such applications are needed for OTA transactions or to act as an interface to applets in the secure element. We propose to implement a certificate based authentication between the application running on the host and the applets in the secure element.

Transactions over NFC peer link: Currently the NFCIP-1 link is a plain data link with no security underneath. This enables attackers to eave drop the communication and/or alter the data over the RF link. Hence we recommend the introduction of a security layer using a certificate based authentication or Diffie-Hellman Key exchange.

Issues due to the fixed unique ID: As the unique ID is specified in the standard for anti-collision, a simple hardware like OpenPICC [13] simulates an arbitrary ID to spoof someone's identity. Hence applications based on unique IDs are not only a privacy issue to the holder but also a security risk for the application making use of it. The ID can also be acquired by eaves dropping the communication between the reader and the smart card chip as it is not encrypted. This privacy issue could be bypassed by having a random number for anti-collision as already used for NFC targets and in e-passports [14]. Therefore it cannot be used for tracking or identification. But still by tracing users, the attacker could find out if the victim is carrying an RFID transponder like a smart card or an NFC device.

Phishing: Additionally to the technical issues there will also attackers try to mislead users by social engineering. The inhibition threshold of touching a tag or a reader with the mobile phone is probably much lower than making an intended connection with a wire. Thus phishing attacks could easily be performed by modifying or replacing tags. This is a simple and inexpensive way to mislead the user. Using signatures on tags and transporters would be suitable way to overcome this issue.

5 Conclusion

As a summary we propose the following measure to deal with NFC security and privacy issues:

- Introduce a button to turn on NFC functionality consciously by the user.
- Introduce a management instance for the secure elements in the device. Only the random NFC ID should be used for anti-collision (no use of ID based systems).
- Allow the NFC controller/management instance to use security features of a secure element for securing NFC peer-to-peer connections.
- Integrate an authentication of signed applications against the secure element/management instance of the secure elements.
- Using signed tags to prevent phishing attacks

From the current point of view there are some issues regarding security and privacy that could be solved by technical means. But it has to be kept in mind, that the standardization is still ongoing. As NFC devices and services do not only rely on a handset but also on lots of different parties, security and privacy issues should be already considered on the bottom level of technology if possible.

Acknowledgment

This work is part of the NFC Research Project funded by FFG (Austrian Research Funding Agency), Project #811408.

References

[1] J. Collins, "ABI Research Insight: No OTA, No NFC," http://www.abiresearch.com/, 10 2007.

[2] Z. Kfir and A. Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard," *SecureComm*, vol. 1, pp. 47–58, 2005.

[3] G. Madlmayr, O. Dillinger, J. Langer, C. Schaffer, C. Kantner, and J. Scharinger, "The benefit of using sim application toolkit in the context of near field communication applications for mobile applications," in *ICMB 2007*, vol. 06, 07 2007, p. 7.

[4] *mobile NFC technical guidelines*, 1st ed., GSMA London Office, 1st Floor, Mid City Place, 71 High Holborn, London WC1V 6EA, United Kingdom, 04 2007, 1st Revision.

[5] C. Bishwajit and R. Juha, *Mobile Device Security Element*, Mobey Forum, Satamaradankatu 3 B, 3rd floor 00020 Nordea, Helsinki/Finland, 02 2005.

[6] G. Avoine, "Rfid: Adversary model and attacks on existing protocols," EPFL, Station 14 - Building INF CH-1015 Lausanne, Switzerland, Tech. Rep. LASEC-REPORT-2005-001, September 2005.

[7] S. Weis, "Security and Privacy in Radio-Frequency Identification Devices," Master's thesis, Massachusetts Institute of Technology, 2003.

[8] G. Hancke, "A Practical Relay Attack on ISO 14443 Proximity Cards," *Symposium on Security and Privacy*, vol. 02, p. 328333, 2006, university of Cambridge, Computer Laboratory JJ Thomson Avenue, Cambridge CB3 0FD, UK ghancke@ieee.org.

[9] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," *SecureComm*, vol. 1, pp. 67–73, 2005.

[10] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. O'Hare, "Vulnerabilities in first-generation RFID-enabled credit cards," *FC07*, vol. 11, pp. 1–22, 2007.

[11] P. Torr, "Demystifying the Threat-Modeling Process," *IEEE Security and Privacy*, vol. 03, no. 5, pp. 66–70, 2005.

[12] C. Castelluccia and G. Avoine, *Smart Card Research and Advanced Applications*. Springer Berlin / Heidelberg, 2006, ch. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags, pp. 289–299.

[13] H. Welte, "OpenPCD," urlhttp://www.openpcd.org/, 08 2007.

[14] I. Naumann, "Advanced Security Mechanisms for Machine Readable Travel Documents Extended Access Control (EAC)," Federal Office for Information Security, Tech. Rep., 2006.