Eavesdropping Near Field Communication

Henning Siitonen Kortvedt and Stig F. Mjølsnes
Department of Telematics
NTNU

Abstract

Near Field Communication (NFC) specifies a standard for a short range wireless communication enabling data transfer by keeping two devices close together, about 10 cm maximum distance. Mobile phones with NFC integration can perform peer-to-peer communication or read information from RFID tags and cards. An NFC device in card emulation mode offers compatibility with other contactless smart card standards. This enables NFC devices to replace traditional contactless plastic cards used in public transport ticketing, access control, ATMs and other similar applications. This paper shows that it is possible to eavesdrop on NFC communication, and gives a thorough description of how this can be done using simple equipment and methods. The performed experiments show that the communication protocol does not offer any security in itself, and that data transmission can be picked up at least at a distance of approximately 20-30cm using an improvised passive antenna without any signal amplification or filtering circuitry. We assert that the use of an active radio receiver would increase the distance significantly. As NFC in active communication mode has a far greater eavesdropping range than the passive mode, the latter should be preferred in typical banking and payment applications.

1. Introduction

1.1. Near Field Communication Technology

The NFC technology is a spin-off from the established RFID technology, developed for mobile phone integration. The radio interface operates at 13.56 MHz with a communication range of up to approximately 10 cm, dependent on the physical implementation of the two communicating devices [2]. The design NFC antennas integrated in mobile phones is complex, so the communication range may vary quite a bit between different models.

ITU-T and ECMA have issued the NFC standard which defines three different modes of operation: peer-to-peer, active, and passive communication mode. Peer-to-peer mode enables communication between to NFC devices, for instance transferring pictures, business cards, music and video. Active and passive modes offer backward compatibility with contactless smart card standards based on RFID. In active communication mode, the NFC device generates an RF-field to read passive RFID tags, for instance containing advertisement, payment or configuration data. In passive (card emulation) mode, the NFC device acts as a contactless smartcard. This enables the mobile phone to perform existing contactless applications, such as public transport ticketing (MIFARE and FeliCa). [3, 6, 19, 17, 18]

Two recent announcements from Sony Ericsson [16] and Telenor together with "DnB NOR" (a Norwegian bank) [15], indicate that NFC might be heavily introduced to consumers during the next couple of years. According to Ericsson's vice president of systems architecture, all their phones will contain an RFID-chip within the summer of 2010. Credit card issuers, such as "DnB NOR", want to replace physical credit cards with software implemented virtual cards in mobile phones. The cooperation with Telenor and their new SIM-card (UICC) with NFC capabilities might launch a secure platform for cryptographic computation together with storage of keys and other sensitive data. If this work becomes a success, leather wallets stuffed with numerous

This paper was presented at the NISK 2009 conference.

plastic cards can be replaced by a mobile phone. The cards issuers may reduce costs related to production and distribution of physical cards. This solution does have an environmental aspect as well, as the billions of plastic cards in circulation will be significantly decreased.

1.2. The Security Problem of NFC

According the official NFC Forum pages, NFC shall be inherently secure because of the short communication range and the properties of the RF modulation [4]. On the other hand, radio transmission will always be possible to eavesdrop at some range, partly determined by the antenna signal gain. The signal has to be strong enough to induce sufficient voltage to power up the transponder in the passive mode device. The eavesdropping equipment may not have the same constraints. It may have a better antenna designed for best possible gain, and it does not need to be integrated in a mobile phone or tag. It may also have power supply, filters, signal amplifiers and other circuitry optimizing the receiving capabilities.

For example, it seems possible to make a device able to eavesdrop and store information transmitted between a contactless card and an automatic teller machine (ATM), similar to how magnetic strip card skimmers are working today [8, 9, 10, 11, 12, 13]. Although VISA and MasterCard may provide a well designed security solution protecting their application, NFC may still be a weakness. Attackers can use other NFC applications with low or no security as backdoors in order to launch attacks against the Visa or MasterCard applications. This motivates the need for some kind of NFC security protocol.

1.3. Related Work and Contribution

Very recently, two ECMA standard drafts were published ECMA-385 and ECMA-386 that specify a security protocol to be used in the peer-to-peer mode of communication. Currently, the drafts are undergoing a 5 months ballot period at ISO/IEC as DISs (Draft for International Standard). [5, 22]

In [23], Kirschenbaum and Wool prove that the reading range of ISO-14443 tags can be increased 3-5 times relative to the original operating distance. They show that tags can be skimmed at a distance of about 25 cm by making a more effective reader. The skimmer reads the tag in the same way as a legitimate reader would do, but the tag owner will be unaware of the action taking place. This attack will be successful as long as tags cannot deny requests from false readers.

This paper shows that ongoing *NFC communication between an active and a passive device can be eavesdropped*, simply by modifying a standard tag antenna and using a digital storage oscilloscope.

Chapter 2 of this paper will describe the planning, carrying out and results of the eavesdropping experiment performed in the Master's Thesis. Chapter 3 will give a discussion concerning the experimental results and the security aspects related to NFC. The conclusion of the paper appears in Chapter 4.

2. Experiment

This chapter will present the essence of the experiment performed in the Master's thesis. Technical details and more thorough descriptions can be found in the thesis [1].

2.1. Theoretical Background

This experiment focuses on communication between an active and a passive device, as this seems to have the greatest commercial interest. An active device is constantly generating a magnetic field with specified strength limits. To transmit data this device uses ASK modulation (10% or 100%) generating short pauses in the signal. This is combined with pulse position modulation. The length of one bit duration (bd) is decided by the chosen bit rate. A ‘1’ is indicated by a pause starting in the middle of the bd. A ‘0’ has no pulse, but to ensure proper timing all consecutive ‘0’s after the first one have a pause in beginning of the bd.

The passive device has to use another scheme to send data back to the active device. By switching a load in the receiver, it can generate a load modulation scheme. Manchester Encoding with obverse amplitude is used to perform bit encoding. If the level goes high in the middle of a bd, it indicates a ‘1’. If the level goes low it indicates a’0’.

In order to avoid interference with other systems or ongoing communication, NFC has a strict connection initiation procedure with RF collision avoidance. If no collisions are detected, a single device detection (SDD) procedure follows in order to choose the device you want to communicate with. All the commands used in these procedures are described on bit level in the standard, so it can easily be compared with any eavesdropped results.

2.2. Setup

This chapter will present the equipment, methods and procedures used for the eavesdropping experiment. A selection of the graphical test result documentation will be presented to prove the findings. All the tests performed should be reproducible, but detailed knowledge of the communication protocol is required to be able to perform eavesdropping by the equipment and methods used here.

The purpose of the experiment was to prove that it is possible to pick up information sent between NFC devices by the use of simple equipment, in order to show that sophisticated security mechanisms are needed when developing NFC applications dealing with sensitive information. Figure 1 depicts the experimental setup of transmission eavesdropping between an NFC reader and an NFC tag by using an oscilloscope and an improvised antenna.

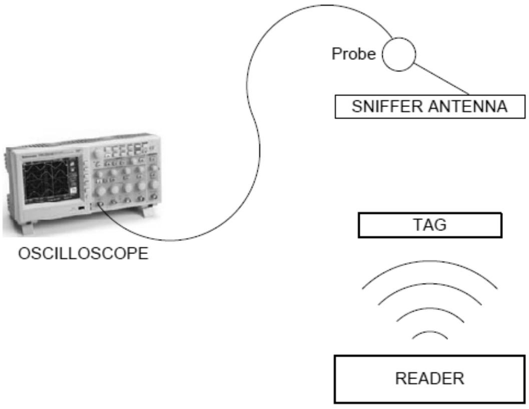


Figure 1: Test set-up illustration

2.3. Equipment

As shown in Figure 1, the basic test assembly consisted of a reader, a tag and a passive antenna connected to an oscilloscope. To perform accurate reading distance measurements, an adjustable rack transparent to RF-signals was built. The NFC reader used in this experiment was an ACR122U, a product of Advanced Card Solutions (ACS) in Hong Kong. This reader supports NFC, ISO/IEC-14443 Type A, ISO/IEC-14443 Type B, Mifare and FeliCa [14, 21]. The NFC-enabled cell phone used in the test is a NOKIA 6212 Classic. To analyze the RF-signals, a Tektronix TDS 2004B digital storage oscilloscope was used. The sniffing antennas used were made by modifying MIFARE Tags and MIFARE Classic cards, as shown in Figure 2 and Figure 3.

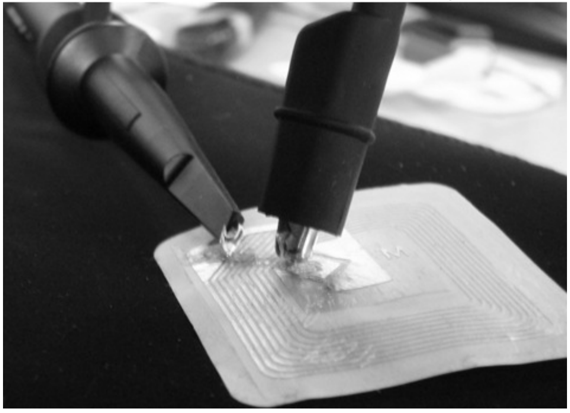


Figure 2: Sniffer antenna made of a Mifare UltraLight Label

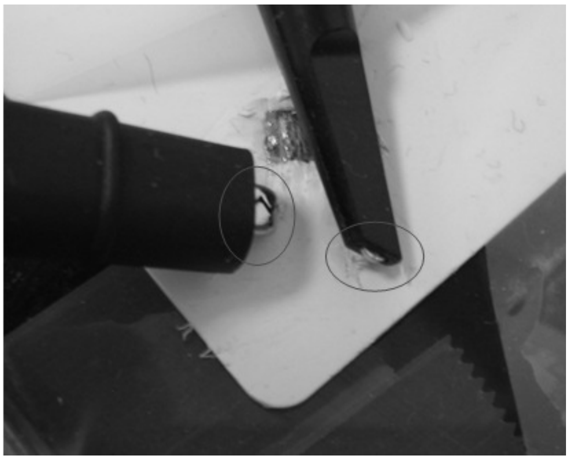


Figure 3: Sniffer antenna made of a Mifare Classic Card

Tests showed that the Mifare Classic Card had the best reading range, but as the Mifare UltraLight Labels were easier to modify they were used in all the initial testing. The Mifare Classic Card was only used in the final eavesdropping range measurements.

A test program managed the accurate measurements of the transmitted signal, making sure that the scope triggered on the same sequence every time [20]. The RF-interface had to be switched off while preparing the oscilloscope for triggering. Whenever ready the RF-interface should be switched on when the reader sends out an ALL_REQ to initiate communication with nearby devices. The tag will then respond with a SENS_RES. These commands are followed by SEL_REQ and SEL_RES to complete the “Single Device Detection”-procedure (SDD). This sequence showed to be stable and repetitive and was implemented in a Java-program based on modification of example code provided with the reader’s SDK.

2.4. Procedures

This section gives a short summary of how the experiments were performed.

2.4.1. General

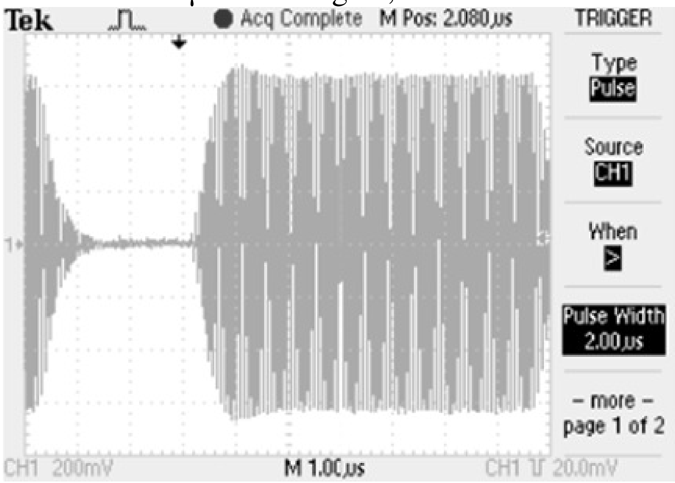
Throughout the tests performed in this experiment, a step-by-step procedure has been followed. [7] As the oscilloscope has limited display window, only a few bits of information can be visually interpreted at one time. The work is tedious, but easy to get into. However, it's important to know what you look for, i.e. what type of modulation you expect to see and where in the signal's time domain the modulation should appear. Another challenge is to configure the oscilloscope to display the signal in the way you want, and to make it trigger on the desired events.

2.4.2. *Test plan*

A number of tests with increasing complexity were planned. In order to start the testing, a proper antenna had to be designed. The first test goal was to be able to find the modulated signal and decide whether specific bit durations indicates a "0" or a "1". The next step was to recognize complete commands, and check whether they matched with the communication sequences described in the standards. If single commands are able to be captured, the next challenge would be to capture a whole communication sequence. If all the previous tests were successful, the final goal would be to perform maximum reading range tests. As these tests were performed with completely passive equipment, they will only give an indication of the eavesdropping possibility. One can expect that the ranges can be increased significantly by introducing a radio receiver with signal amplifiers.

2.4.3. *Amplitude-shift keying reading*

The ASK signal was the easiest to find and convert to byte code. This is the communication from the reader to the tag, and is thus the first signal that will appear in the time domain. A bit duration (bd) is 9,44µs, and a pulse with duration of around 2-3µs may occur within the bd. Figure 3 shows how one single bd looks on the oscilloscope. The screen covers 10µs of the signal, i.e. a little bit more than one bd.


Tek ● Acq Complete M Pos: 2.080µs

TRIGGER

Type: Pulse

Source: CH1

When: >

Pulse Width: 2.00µs

– more – page 1 of 2

CH1 200mV M 1.00µs CH1 ⨍ 20.0mV

Figure 4: A 100% ASK pulse that occurs in the beginning of one bit duration.

The pulse's position is deciding what value a bit duration has. By showing a number of bit durations, you can start interpreting the actual data given that you know the position of the "start of communication" pulse.

2.4.4. *Load modulation reading*

The load modulated signal was more difficult to display, because of the much smaller amplitude difference in the carrier signal. It is however possible to minimize the effect of this by just looking at one side lobe of the signal. By adjusting the vertical position of the oscilloscope so that the average peak value appears around the middle of the screen and adjusting the vertical resolution to the finest level (20mV on the scope used), you are creating the best conditions for reading out '0's and '1's.

2.4.5. Eavesdropping range set-up

The goal of this test was to draw a rough radiation diagram showing how the possible eavesdropping distance is changing according to the antennas position relative to the reader. This was done by placing the antenna in 17 different positions and adjusting the distance so that the load modulated signal is visually readable.

2.4.6. Oscilloscope configuration

A digital storage oscilloscope with pulse triggering opportunities is needed to perform the tests as described. For each test with specific distances between the reader, tag and test antenna, the average signal level has to be measured. This is done by setting the scope to trigger on an event that is always happening. In this case you can enable positive edge triggering with low amplitude trigger level. To catch the first ASK pulse, set the oscilloscope to trig on pulses with negative polarity, trig level about ¼ of the signals peak-to-peak value and define the pulse width to be larger than 2µs. With “Single-Sequence-Triggering”, this set-up will always trig on the first ASK pulse. The load modulated signal has no properties of which the oscilloscope can trigger. To overcome this, the storage capabilities of the oscilloscope have to be exploited. By capturing and storing a part of the ongoing communication, you can analyze the signal afterwards. The two first frames, ALL_REQ and SENS_RES, are easy to find. The start of ALL_REQ is off course the pulse that the oscilloscope triggers on. A SENS_RES will always follow 162,8µs after the first pause in the “Short frame” sent from the reader. After SENS_RES, only minimum delay period between each transmission sequence is defined. The only way to find them with the oscilloscope is to adjust the horizontal position some bits at a time until you find another modulated sequence [2]. Further details on triggering can be found reading Ref. [1]

2.5. Test Results

Only a selection of the retrieved graphical result documentation is presented in this paper. For further details, please read Ref. [1].

This experiment succeeded in finding both the ASK-signal and the load modulated signal, and we were able to interpret bits visually. While capturing completed commands and comparing the results with actual commands described in the standard, perfect matches for all sequences were found. Examples of commands captured with the oscilloscope are presented in Figure 5.

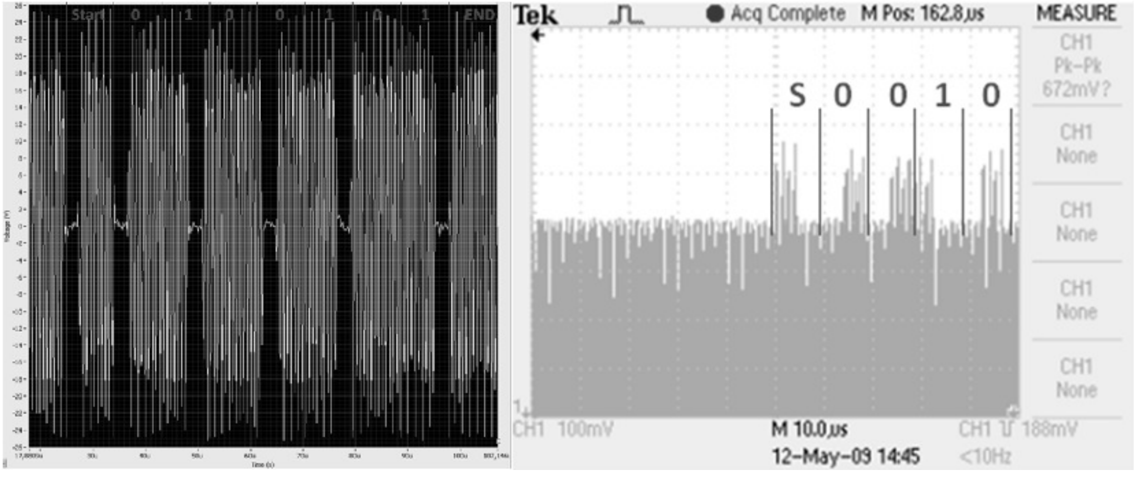


Figure 5: Screenshot of ASK command to the left and load modulated command to the right.

The first ALL_REQ command can be recognized with one screenshot on the oscilloscope, and all the data bits are sent without interruption between the start and end delimiters. For the rest of the commands, each byte of data is followed by a parity bit. Table 1 shows how to translate between the captured bits and actual data.

Bd	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Byte	1									2								
Bit	0	1	2	3	4	5	6	7	P	0	1	2	3	4	5	6	7	P
Value	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Table 1: Interpretation of all bits in a SENS_RES command sent from target to reader.

The bit pattern is transmitted least significant bit first within each byte and then least significant Byte first, so the bit order has to be rearranged to get the real command value, as indicated in Table 2. Bit 0-7 of byte 2 in Table 1 becomes bit 8-15 in Table 2.

b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

Table 2: Data bits of an interpreted SENS_RES command.

The goal of the command recognition test was to be able to capture a complete communication sequence. Comparing the test results with the standard showed that a complete communication initiation sequence was captured, including command values and the unique ID of the tag. The sequence consists of four commands and the byte values related to the specific tag used are presented in Table 3. The CRC byte was computed by entering the bit string into a self developed checksum program. This value did also match with the interpreted bytes.

ALL_REQ	1010010				
SENS_RES	0000 0000 00 0 00100				
SEL_REQ	93	70	0C CF BD 40	3E	2A CC
	SEL_CMD	SEL_PAR	NFCID	BCC	CRC
SEL_RES	08	B6	DD		
	SEL_RES	CRC			

Table 3: Results of capturing a whole communication sequence from initiator to target.

As the command sequenced recognition proved to be possible, the final task was to perform measurements of the maximum eavesdropping ranges. The first test was done with two different antennas leveled right above the reader.

Antenna	Eavesdropping distance
Mifare UltraLight Label	17,4 cm
Mifare Classic Card	29,2 cm

Table 4: Eavesdropping ranges for the available antennas.

As indicated in Table 4, the Mifare Classic card antenna had nearly twice the range of the Mifare UltraLight Label antenna. This antenna was then put in 8 different test positions to measure the ranges in different angles relative to the reader, as shown in Figure 6.

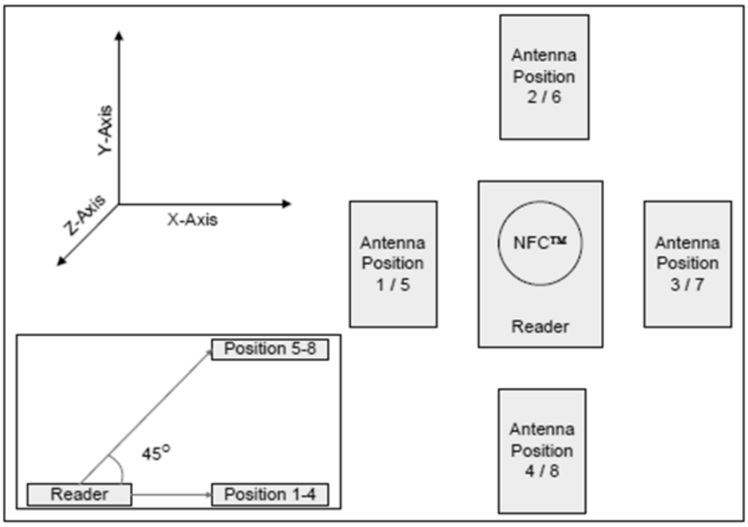


Figure 6: Antenna positions in maximum eavesdropping range test.

The 8 tests were first performed with the antenna leveled, and then perpendicular to the vector from the centre of the reader to the centre of the antenna. The results are presented in Table 5.

		Antenna position							
	Antenna angle	1	2	3	4	5	6	7	8
Range in cm	Leveled	22,3	20,6	21,7	23,2	19,1	16,7	19,6	20,3
	Perpendicular	19,1	20,1	19,6	22,9	23,5	24,4	23,2	25,2

Table 5: Maximum eavesdropping range test results.

3. Discussion

This chapter will present a discussion of the test results and the practical feasibility of NFC eavesdropping.

3.1. Summary of Experimental Results

The test results prove the hypothesis made early in the thesis, namely that it is easy to eavesdrop NFC-communication. This means that any transmitted bit sequence can be picked up by an antenna placed within the possible reading range. We have shown here that the reading procedure can be done visually using passive equipment only. Furthermore, developing radio receivers performing the same task in a much more effective way should be easy. It should be possible to capture a whole communication sequence in one piece, and the eavesdropping ranges are expected to increase significantly by the use of active circuitry.

Although there were some problems capturing the communication sent from the NOKIA 6212 Classic, this was related to limitations of the oscilloscope triggering only. A radio receiver made for this type of communication would not have this problem because it doesn't need all RF-fields to be switched off before making ready for signal reception.

It is important to notice that the tests performed here have a certain margin of error, as all tests are based on human opinion of what is possible to read visually. Although this might give an uncertainty on 1-2 cm on each measured value, it does however not influence the fact that the channel can be eavesdropped in ranges up to 30 cm with passive equipment. The environmental variables have not been considered. All tests have been performed in a lab room holding a lot of different electronic equipment, such as wireless access points, desktops, laptops and mobile phones. This means that the radio environment may be quite complex. To get optimal conditions, these tests could have been performed inside a protected environment, such as a Faraday cage. Alternatively, the background noise could have been measured to get an idea of the interference from the surroundings. Because of frequent changes in the total amount of equipment in use in the room, such a measurement would probably not be accurate for any longer period. For the concept of this task it was far more important to prove the possibility than making 100% accurate measurements.

3.2. The Practical Feasibility of NFC Eavesdropping

To succeed in using eavesdropping on NFC communication in large scale you need some radio receiver equipment with data storage capabilities and a high gain antenna. Devices that are able to sniff on several types of RFID standards are commercially available already. As NFC is a derivate of RFID, there should be no reason to believe that this device is not modifiable to work with NFC communication as well. With good knowledge of radio communication in general, detailed studies of NFC and access to advanced soldering equipment, more sophisticated equipment with greater reading ranges and significantly decreased size can be manufactured.

The size and range of the equipment in use are important factors when evaluating the practical feasibility. If the range is short, the interception equipment has to be sufficiently small to mount close to the communicating devices, still without being easily detected. It is possible to place skimmers on ATMs copying magnet strips. A similar approach could also be possible with a NFC skimmer device. If it is possible to pick up the communication at greater ranges, one can put the equipment on people (e.g. instruments of street musicians) or other devices that can be placed in the street without being noticed. Then the constraints size and power supply of the equipment could be relaxed, thus likely increasing the reading range.

3.3. Security Aspects

As it is proven that it is possible and indeed practical to eavesdrop on communicating NFC devices, there should be no doubt that NFC communication needs to be combined with some kind of security protocol. An NFC device is expected to operate in various environments, some requiring a high level of security and some that does not really need any security in itself.

Some of the promoted applications are related to different types of public advertisement. In this area, the cost of the NFC tag is of great importance. It may however be a problem that this type of applications can be exploited in order to access the NFC device indirectly, say by open back doors, into other applications stored in the phone. As long as tag communication does not have authentication nor data integrity, the risk of transfer of malicious content to devices remains. This can be used for DOS attacks or more sophisticated attacks trying to retrieve private information.

Another proclaimed NFC use is for the replacement of identification cards and credit cards. Here the security requirements are stricter, but the need to keep the costs at a minimum still is important. This application is in need of authentication, integrity, confidentiality and replay protection.

The fact that ECMA has developed a security protocol to be used with NFC enforces the need for discussions concerning the security of NFC, although the web page of NFC Forum still states that NFC is “inherently secure” because of the short transmission range. ECMA has however only dealt with “active communication mode” in their security protocol. In [1], the security concerning “passive communication mode” is in focus. We present an outline of a layered security model with a minimum requirement of authentication before start of communication. The minimum requirement has to be achievable without generating great cost increases for tags with very limited computational capabilities. Developers can then add higher level of security according to the defined needs for each application. If this can be applied as a common standardized and trusted framework, the threshold for converting applications into NFC might decrease.

This matter is briefly discussed in [1] and further analysis should be made in order to develop an optimal security protocol dealing with the fact that an NFC phone will be used in a large number of varying scenarios.

4. Conclusions and Further Work

The experiments performed by this NTNU master thesis work show how it is practical to capture and demodulate data sent in both directions between two NFC devices communicating in passive communication mode. The background knowledge needed to succeed is open and available. This shows beyond any doubt that cryptographic protocols are needed to protect sensitive data sent between two NFC devices.

The signal that is load modulated on the RF carrier can be analyzed and demodulated visually at ranges up to 29 centimeters using completely passive equipment. The eavesdropping range is dependent on the implementation of the reader device, the tag device and the eavesdropping device. If a tag has a long reading range, it has an effective antenna which generates more power when transmitting the load modulated signal. In other words, devices with reading ranges in the area of 10 cm will be easier to eavesdrop than devices with ranges in the area of 2-3 cm.

The sniffer antenna can be made more sophisticated than the ones used in this experiment by active circuitry in order to increase the signal reading range. We conjecture that it should be possible to pick up the signal at meter distance in the passive communication mode, and at longer distance for the active communication mode.

Further work based on the results reported here may take several different directions. One possibility is to continue the analysis of the radio interface and assess the pickup range of peer-to-peer and active modes. Another direction is to construct a set of mechanisms and protocols that secure all three types of NFC communication. A goal could be to make security implementation easy for the application developers. An API and a programming language library could also be developed. It might also be possible to analyze this solution in comparison with a PKI approach, to find the most effective solution.

References

[1] Henning S. Kortvedt. Securing Near Field Communication. Master Thesis June 2009. Department of Telematics, Norwegian University of Science and Technology. 115 pages.

[2] ISO/IEC, *“Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)”*, 1.Edition. ISO/IEC 18092; 2004-04-01.

[3] ISO/IEC, *“Identification cards – Contactless integrated circuit(s) cards – Proximity cards- Part 1: Physical characteristics”*, 2.Edition. ISO/IEC 1443-1; 2008-06-15.

ISO/IEC, *“Identification cards – Contactless integrated circuit(s) cards – Proximity cards- Part 2: Radio Frequency power and signal interface”,* 1.Edition. ISO/IEC 1443-2; 2001-07-01.

[4] NFC Forum, *“NFC Forum Home Page “*. http://www.nfc-forum.org/home; 2009.

[5] ECMA, *“NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES”*. ECMA-386; 2008-12.

[6] ISO/IEC, *“Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-2)”*, 1.Edition. ISO/IEC 21481; 2004-04-01

[7] ECMA, *”NFCIP-1 - RF Interface Test Methods”*, 1.Edition. ECMA-356; 2004-6.

[8] Gerhard Hancke, *“A Practical Relay Attack on ISO 14443 Proximity Cards”*. Paper from MSc project report submitted to University of Cambridge, Computer Laboratory; 2005-02. http://www.rfidblog.org.uk/hancke-rfidrelay.pdf

[9] Gerhard Hancke, *“Eavesdropping Attacks on High-Frequency RFID Tokens”*. Proceedings of the 4th Workshop on RFID Security (RFID’sec08), pp 100-113; 2008-07. http://www.rfidblog.org.uk/Hancke-RFIDsec08-Eavesdropping.pdf

[10] Gerhard Hancke, *“Practical Attacks on Proximity Identification Systems (Short Paper)”*. Proceedings of IEEE Symposium on Security and Privacy 2006, pp. 328–333, Oakland, USA; 2006-05. http://www.rfidblog.org.uk/Hancke-IEEESP-RFIDPracAttacks.pdf

[11] Roel Verdult and Gerhard de Koning Gans, *“PROXMARK.org – A Radio Frequency Identification tool”*. http://www.proxmark.org/proxmark; 2009-05.

[12] Edouard Lafargue, *“The "official" Proxmark 3 user's and developer's manual”*. https://www.lafargue.name/rubrique63.html; 2009-05.

[13] proxmark3.com, *“proxmark^3 distribution information”*. http://proxmark3.com/; 2009-05.

[14] Smartcard Focus, *“ACR 122U Starter kit product information”*. http://www.smartcardfocus.com/shop/ilp/id~344/p/index.shtml; 2009-05.

[15] Digi.no, “SIM-kort vil erstatte bankkort”. http://www.digi.no/823818/sim-kort-vil-erstatte-bankkort; 2009-09. (Norwegian website)

[16] Silicon.com, ”RFID in all new mobiles by next summer”. http://networks.silicon.com/mobile/0,39024665,39444914,00.htm; 2009-06.

[17] NXP Semiconductors, *“MIFARE Product Information”*. http://www.mifare.net/; 2009-05.

[18] SONY Global, *“FeliCa Product Information”*. http://www.sony.net/Products/felica/index.html; 2009-05

[19] NFC Forum, *“Type 1 Tag Operation Specification”*. NFCForum-TS-Type-1-Tag_1.0; 2007-07-09.

NFC Forum, *“Type 2 Tag Operation Specification”*. NFCForum-TS-Type-2-Tag_1.0; 2007-07-09.

NFC Forum, “*Type 3 Tag Operation Specification”*. NFCForum-TS-Type-3-Tag_1.0; 2007-08-16.

NFC Forum, “*Type 4 Tag Operation Specification”*. NFCForum-TS-Type-4-Tag_1.0; 2007-03-13.

[20] ACS, *“ACR122U NFC Reader API”*, Version 1.2. http://www.acs.com.hk/drivers-manual.php?driver=ACR122; 2008-08.

[21] ACS, *“ACR122U NFC Reader SDK User Manual”*, Version 1.2. ACR122U Starter Kit CD-ROM; 2008-08.

[22] ECMA, *“NFC-SEC: NFCIP-1 Security Services and Protocol”*. ECMA-385; 2008-12.

[23] Ilan Kirschenbaum and Avishai Wool, *“How to Build a Low-Cost, Extended-Range RFID Skimmer”*. Proceedings of the 15th conference on USENIX Security Symposium - Volume 15; 2006-05-08. http://eprint.iacr.org/2006/054.pdf