Global Journals LaTeX JournalKaleidoscopeTM

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Strengths and Weaknesses of Near Field Communication (NFC) Technology

Dr. Mohamed Mostafa Abd Allah[1]

[1] Royal Commission, Yanbu Industrial Collage,KSA

Received: 6 January 2011 Accepted: 3 February 2011 Published: 18 February 2011

Abstract

This paper gives a comprehensive analysis of security with respect to NFC. We propose a protocol that can be used between an RFID tag and a reader to exchange a secret without performing any expensive computation. The paper introduced an NFC specific key agreement mechanism, which provides cheap and fast secure key agreement. Key agreement techniques without authentication can be used to provide a standard secure channel. This resistance against Man-in-the-Middle attacks makes NFC an ideal method for secure pairing of devices. The paper lists some of threats, which are applicable to NFC, and describes solutions to protect against these threats.

Index terms— Near Field Communication, threats, key agreement.

1 Introduction

ear Field Communication (NFC) is a technology for high frequency wireless short-distance pointto-point communication. The operational range for NFC is within less than 20 cm which is good from a security perspective as it diminishes the threat of eavesdropping. Other reasons to use NFC are the low cost of the necessary components and that the connecting time is negligible. It is small circuit attached to a small antenna, capable of transmitting data to a distance of several meters to a reader device (reader) in response to a query. Most RFID tags are passive, meaning that they are battery-less, and obtain their power from the query signal. They are already attached to almost anything: clothing, foods, access cards and so on. It is impossible to give a complete picture of NFC applications as NFC is just an interface. Contactless Token covers most of applications, which use NFC to retrieve some data from a passive token. The passive token could be a contactless Smart Card, an RFID label, or a key fob. In Ticketing / Micro Payment application example, the NFC interface is used to transfer some valuable information. The ticket or the micro payment data is stored in a secure device. This could be a contactless Smart Card, but could as well be a mobile phone.

When the user wants to perform a payment or use the stored ticket, the user presents the device to a reader, which checks the received information and processes the payment or accepts/rejects the ticket. In this application example the user device must be able to perform a certain protocol with the reader. A simple read operation will not be sufficient in most cases. Also, the user device is likely to have a second interface which is used to load money or to buy tickets. This second interface can for example be linked to the mobile phone CPU. The ticket data could then be loaded into the mobile phone via the cellular network. Because NFC is a wireless communication interface it is obvious that threat is an important issue. When two devices communicate via NFC they use RF waves to talk to each other. An attacker can of course use an antenna to also receive the transmitted signals. Either by experimenting or by literature research the attacker can have the required knowledge on how to extract the transmitted data out of the received RF signal. Also the equipment required to receive the RF signal as well as the equipment to decode the RF signal must be assumed to be available to an attacker as there is no special equipment necessary. In this paper we use a systematic approach to analyze the various aspects of security whenever an NFC interface is used. We want to clear up many misconceptions about security and NFC in various applications. The paper lists the threats, which are applicable to NFC, and describes solutions to protect against these threats. The rest of this paper is organized as follows. A brief description about NFC operation modes are given in Section (2). A list of threats technique is discussed in Section (3). Real solution against these threats and establishes a secure channel is presented in Section (4). Finally, concluding remarks are made in Section (5).

2 NFC Operation Modes

NFC can operate in two modes. The modes are distinguished whether a device creates its own RF field or whether a device retrieves the power from the RF field generated by another device. If the device generates its own field and has a power supply, it is called an active device; otherwise it is called a passive device. When two devices communicate three different configurations are possible (Active-Active, Active-Passive, and Passive-Active). These configurations are important because the way data is transmitted depends on whether the transmitting device is in active or passive mode.

In active mode the data is sent using amplitude shift keying (ASK) [1], [2]. This means the base RF signal (13,56 MHz) is modulated with the data according to a coding scheme. If the baudrate is 106 kBaud, the coding scheme is the so-called modified Miller coding. If the baudrate is greater than 106 kBaud the Manchester coding scheme is applied. As shown in figure **??**, each single data bit in both coding schemes is sent in a fixed time slot. This time slot is divided into two halves, called half bits. In Miller coding a zero is encoded with a pause in the first half bit and no pause in the second half bit. A one is encoded with no pause in the first bit, but a pause in the second half bit. In the modified Miller coding some additional rules are applied on the coding of zeros. In the case of a one followed by a zero, two subsequent half bits would have a pause. Modified Miller coding avoids this by encoding a zero, which directly follows a one with two half bits with no pause.

In the Manchester coding the situation is nearly the same, but instead of having a pause in the first or second half bit, the whole half bit is either a pause or modulated.

Besides the coding scheme also the strength of the modulation depends on the baudrate. For 106 kBaud 100% modulation is used. This means that in a pause the RF signal is actually zero. No RF signal is sent in a pause. For baudrates greater than 106 kBaud 10% modulation ratio is used. According to the definition of this modulation ratio [1], this means that in a pause the RF signal is not zero, but it is about 82% of the level of a non paused signal. This difference in the modulation strength is very important from a security point of view as we will describe later on in the security analysis.

In passive mode the data is sent using a weak load modulation. The data is always encoded using Manchester coding with a modulation of 10%. For 106 kBaud a subcarrier frequency is used for the modulation, for baudrates greater than 106 kBaud the base RF signal at 13.56 MHz is modulated.

Additionally to the active and passive mode, there are two different roles a device can play in NFC communication. NFC is based on a message and reply concept. This means one device A sends a message to another device B and device B sends back a reply. It is not possible for device B to send any data to device A without first receiving some message from device A, to which it could reply. The role of the device A which starts the data exchange is called initiator, the role of the other device is called target. Furthermore it should be mentioned that NFC communication is not limited to a pair of two devices. In fact one initiator device can talk to multiple target devices. In this case all target devices are enabled at the same time, but before sending a message, the initiator device must select a receiving device. The message must then be ignored by all non selected target devices. Only the selected target device is allowed to answer to the received data. Therefore, it is not possible to send data to more than one device at the same time (i.e. broadcasting messages are not possible). Typical communication procedure between the initiator and target can be highlighted as shown in figure **??**.

3 ? Handshake:

? The interrogator sends a command to start communication with transponder in the interrogator field and also to power it (passive transponders). ? Once the tag has received sufficient energy and command from the reader, it reply's with its ID for acknowledgment. ? The reader now knows which tag is in the field and sends a command to the identified tag for instructions either for processing (read or write) or Sleep. ? Data exchange:

? If the tag receives processing and reading commands, it transmits a specified block data and waits for the next command. ? If the tag receives processing and writing commands along with block data, it writes the block data into the specified memory block, and transmits the written block data for verification.

Although contactless token systems may emerge as one of the most pervasive computing technologies, there are still a vast number of problems that need to be solved before their massive deployment. One of the fundamental issues still to be addressed is privacy. Products labeled with tags reveal sensitive information when queried by readers, and they do it indiscriminately.

A problem closely related to privacy is tracking, or violations of location privacy. This is possible because the answers provided by tags are usually predictable: in fact, most of the times, tags provide always the same identifier, which will allow a third party to easily establish an association between a given tag and its holder or owner. Even in the case in which tags try not to reveal any kind of valuable information that could be used to identify themselves or their holder, there are many situations where, by using an assembly of tags (constellation), this tracking will still be possible. Although the two aforementioned problems are the most important security questions that arise from NFC technology, there are some others worth to mention:

4 1) Eavesdropping Threats

In this type of attacks, unintended recipients are able to intercept and read messages.

The NFC communication is usually done between two devices in close proximity. This means they are not more than 10 cm (typically less) away from each other. The main question is how close an attacker needs to be to be able to retrieve a usable RF signal. Unfortunately, there is no correct answer to this question. The reason for that is the huge number of parameters which determine the distance depends on the following parameters,

? RF filed characteristic of the given sender device (i.e. antenna geometry, shielding effect of the case, the PCB, the environment) ? Setup of the location where the attack is performed (e.g. barriers like walls or metal, noise floor level) Furthermore, eavesdropping is extremely affected by the communication mode. That's because, based on the active or passive mode, the transferred data is coded and modulated differently. If data is transferred with stronger modulation it can be attacked easier. Thus, a passive device, which does not generate its own RF field, is much harder to attack, than an active device.?

Therefore any exact number given would only be valid for a certain set of the above given parameters and cannot be used to derive general security guidelines.

Avoiding eavesdropping can be done by establishing a secure channel as outlined in section 4.1. This requires the establishment of a session secret key, which is not always an easy task considering the very limited devices' capacities.

5 2) Data Modification Threats

As shown in figure 3, instead of just listening, an attacker can also try to modify the data which is transmitted via the NFC interface. In the simplest case the attacker just wants to disturb the communication such that the receiver is not able to understand the data sent by the other device.

In data modification, the attacker wants the receiving device to actually receive some valid, but manipulated data. This is very different from just data corruption.

The feasibility of this attack highly depends on the applied strength of the amplitude modulation. This is because the decoding of the signal is different for 100% in modified Miller coding modulation and 10% in Manchester coding modulation.

In 100% modulation the decoder checks the two half bits for RF signal on (no pause) or RF signal off (pause). In order to make the decoder understand a one as a zero or vice versa, the attacker must do two things. First, a pause in the modulation must be filled up with the carrier frequency. This is feasible. But, secondly, the attacker must generate a pause of the RF signal, which is received by the legitimate receiver. This means the attacker must send out some RF signal such that this signal perfectly overlaps with the original signal at the receiver's antenna to give a zero signal at the receiver. This is practically impossible. However, due to the modified Miller coding in the case of two subsequent ones, the attacker can change the second one into a zero, by filling the pause, which encodes the second one. The decoder would then see no pause in the second bit and would decode this as a correct zero, because a one precedes it. In 100% modulation an attacker can therefore never change a bit of value 0 to a bit of value 1, but an attacker can change a bit of value 1 to a bit of value 0, in case this bit is preceded by a bit of value 1 (i.e. with a probability of 0.5). In 10% modulation the decoder measures both signal levels (82% and Full) and compares them. In case they are in the correct range the signal is valid and gets decoded. An attacker could try to add a signal to the 82% signal, such that the 82% signal appears as the Full signal and the actual Full signal becomes the 82% signal. This way the decode would decode a valid bit of the opposite value of the bit sent by the correct sender. Whether the attack is feasible depends a lot on the dynamic input range of the receiver. It is very likely that the much higher signal level of the modified signal would exceed the possible input range, but for certain situations this cannot be ruled out completely. The conclusion is that for the modified Miller encoding with 100% ASK this attack is feasible for certain bits and impossible for other bits, but for Manchester coding with 10% ASK this attack is feasible on all bits.

Protection against data modification can be achieved in various ways. By using 106k Baud in active mode it gets impossible for an attacker to modify all the data transmitted via the RF link as described above. This means that for both directions active mode would be needed to protect against data modification. While this is possible, this has the major drawback, that this mode is most vulnerable to eavesdropping. In addition, the protection against modification is not perfect, as even at 106k Baud some bits can be modified. The two other protection options might therefore be preferred. NFC devices can check the RF field while sending. This means the sending device could continuously check for such an attack and could stop the data transmission when an attack is detected. The third and probably best solution would be a secure channel as described in section 4.1.

6 3) Man-in-the-Middle Threats

In Man-in-the-Middle Attack, two parties want to talk to each other, called Alice and Bob, are tricked into a three party conversation by an attacker Eve. This is shown in Figure 3. Assuming that Alice uses active mode and Bob would be in passive mode, we have the following situation. Alice generates the RF field and sends data to Bob. In case Eve is close enough, she can eavesdrop the data sent by Alice. Additionally she must actively disturb the transmission of Alice to make sure that Bob doesn't receive the data. This is possible for Eve, but this can also be detected by Alice. In case Alice detects the disturbance, Alice can stop the key agreement protocol. Let's assume Alice does not check for active disturbance and so the protocol can continue. In the next step Eve needs to send data to Bob. That's already a problem, because the RF field generated by Alice is still there, so Eve has to generate a second RF field. This however, causes two RF fields to be active at the same time. It is practically impossible to perfectly align these two RF fields. Thus, it is practically impossible for Bob to understand data sent by Eve. Because of this and the possibility of Alice to detect the attack much earlier we conclude that in this setup a Man-in-the-Middle attacks is practically impossible.

The only other possible setup is that Alice uses active mode and Bob uses active mode, too. In this case Alice sends some data to Bob. Eve can list and Eve again must disturb the transmission of Alice to make sure that Bob does not receive the data. At this point Alice could already detect the disturbance done by Eve and stop the protocol. Again, let us assume that Alice does not do this check and the protocol continues. In the next step Eve would need to send data to Bob. At first sight this looks better now, because of the activeactive communication Alice has turned off the RF field. Now Eve turns on the RF field and can send the data. The problem here now is that also Alice is listening as she is expecting an answer from Bob. Instead she will receive the data sent by Eve and can again detect a problem in the protocol and stop the protocol. It is impossible in this setup for Eve to send data either to Alice or Bob and making sure that this data is not received by Bob or Alice, respectively.

We claim that due to the above given reasons it is practically infeasible to mount a Man-in-the-Middle attack in a real-world scenario. It is practically impossible to do a Man-in-the-Middle-Attack on an NFC link. Therefore, setup a secure channel with an active-passive communication mode as outlined in section 4.1 can be used to improve privacy and prevent tracking against Man-in-the-Middle-Attacks Additionally, the active party should listen to the RF filed while sending data to be able to detect any disturbances caused by a potential attacker.

IV.

7 Solutions and Recommendations

In this section we present the best solutions proposed so far to solve the security problems and threats associated with the use of NFC systems. Our objective is not to give a detailed explanation of each solution, but to provide the fundamental principles and a critical review of every proposal.

8 Figure4 NFC specific Key Agreement

Most of classical solution approach protecting the privacy of NFC communication is done by isolating them from any kind of electromagnetic waves. This can be made using what is known as a Faraday Cage (FC), a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies). There are currently a number of companies that sell this type of solution [13]. Other solution is active jamming approach that disturbing the radio channel, RF signals. This disturbance may be done with a device that actively broadcasts radio signals, so as to completely disrupt the radio channel, thus preventing the normal operation of RFID readers. 1) Secure Channel for NFC Establishing a secure channel between two NFC devices is clearly the best approach to protect against eavesdropping, data modification attack, and enhance the inherent protection of NFC against Man-in-the-Middle-Attacks. A standard key agreement protocol like Diffie-Hellmann based on RSA [4] or Elliptic Curves could be applied to establish a shared secret between two devices. The shared secret can then be used to derive a symmetric key like 3DES or AES, which is then used for the secure channel providing confidentiality, integrity, and authenticity of the transmitted data. Various modes of operation for 3DES and AES could be used for such a secure channel and can be found in literature [3].

9 2) Proposed NFC Key Agreement

The proposed NFC specific key agreement does not require any asymmetric cryptography and therefore reduces the computational requirements significantly. The scheme works with 100% ASK only where, both devices say Device A and Device B, send random data at the same time. In a setup phase the two devices synchronize on the exact timing of the bits and also on the amplitudes and phases of the RF signal. This is possible as devices can send and receive at the same time. After that synchronization, A and B are able to send at exactly the same time with exactly the same Figure5-Total signal seen on RF Field amplitudes and phases. While sending random bits of 0 or 1, each device also listens to the RF field. When both devices send a zero, the sum signal is zero and an attacker, who is listening, would know that both devices sent a zero. This does not help. The same thing happens when both, A and B, send a one. The sum is the double RF signal and an attacker knows that both devices sent a one. It gets interesting once A sends a zero and B sends a one or vice versa. In this case both devices know what the other device has sent, because the devices know what they themselves have sent. However, an attacker only sees the sum RF signal and he cannot figure out which device sent the zero and which device sent the one. This idea is illustrated in Figure **??**.

In figure **??**, the top figure shows the signals produced by A and by B. A sends the four bits: 0, 0, 1, and 1. B sends the four bits: 0, 1, 0, and 1. The lower graph shows the sum signal as seen by an attacker. It shows that for the bit combinations (A sends 0, B sends 1) and (A sends 1, B sends 0) the result for the attacker is absolutely the same and the attacker cannot distinguish these two cases. The two devices now discard all bits, where both devices sent the same value and collect all bits, where the two devices sent different values. They can either collect the bits sent by A or by B. This must be agreed on start-up, but it doesn't matter. This way A and B can agree on an arbitrary long shared secret. A new bit is generated with a probability of 50%. Thus, the generation of a 128 bit shared secret would need approximately 256 bits to be transferred. At a baud rate of 106 k Baud this takes about 2.4 ms, and is therefore fast enough for all applications. The security of this protocol in practice depends on the quality of the synchronization which is achieved between the two devices. Obviously, if an eavesdropper can distinguish data sent by A from data sent by B, the protocol is broken. The data must match in amplitude and in phase. Once the differences between A and B are significantly below the noise level received by the eavesdropper the protocol is secure. The level of security therefore also depends on the signal quality at the receiver. The signal quality however again depends on many parameters (e.g. distance) of the eavesdropper. In practice the two devices A and B must aim at perfect synchronization. This can only be achieved if at least one of A or B is an active device to perform this synchronization.

V.

10 Conclusion

We presented typical use cases for NFC interfaces. A list of threats has been derived and addressed. NFC by itself cannot provide protection against eavesdropping or data modifications. The only solution to achieve this is the establishment of a secure channel over NFC. This can be done very easily, because the NFC link is not susceptible to the Man-inthe-Middle attack. Therefore, well known and easy to apply key agreement techniques without authentication can be used to provide a standard secure channel. This resistance against Man-in-the-Middle attacks makes NFC an ideal method for secure pairing of devices. Additionally, we introduced an NFC specific key agreement mechanism, which provides cheap and fast secure key agreement. [1] [2] [3] [4]

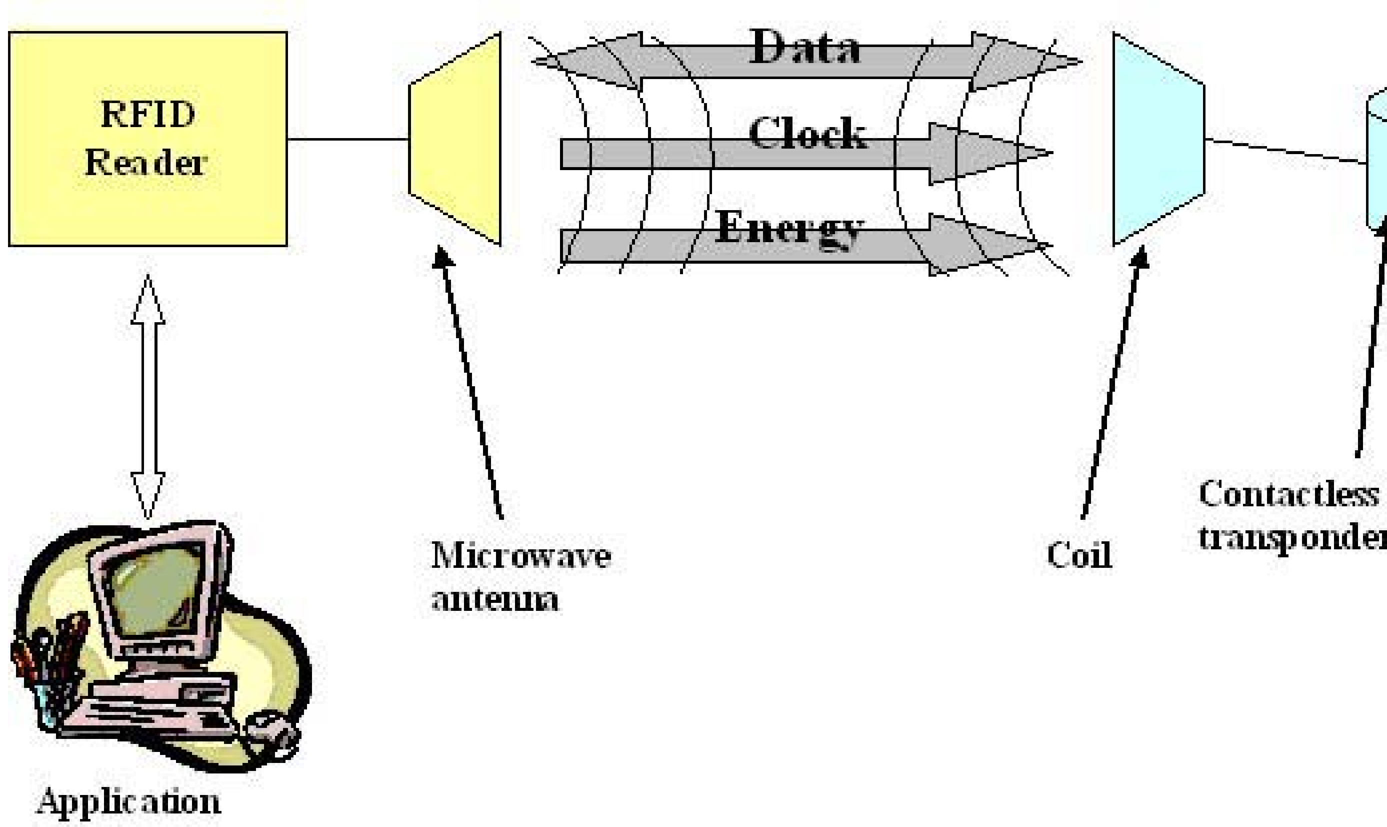
Figure 1: Figure1-

[1] March 2011©2011 Global Journals Inc. (US)

[2] March 2011III.NFC Applications Threats©2011 Global Journals Inc. (US)

[3] March 2011©2011 Global Journals Inc. (US)

[4] March 2011



3

Figure 2: Figure 3

[LNCS, IFCA] , FC'03. *LNCS, IFCA* Springer-Verlag. 2742 p. .

[Jung et al. ()] '8-bit microcontroller system with area efficient AES coprocessor for transponder applications'. M Jung , H Fiedler , R Lerch . *Ecrypt Workshop on RFID and Lightweight Crypto* 2005.

[Dimitriou ()] 'A lightweight RFID protocol to protect against traceability and cloning attacks'. T Dimitriou . *Proc. of SECURECOMM'05*, (of SECURECOMM'05) 2005.

[Juels and Weis ()] 'Authenticating pervasive devices with human protocols'. S Juels , Weis . *CRYPTO'05, IACR*, 2005. Springer-Verlag. 3126 p. .

[Lee et al. ()] 'efficient authentication for low-cost RFID systems'. S M Lee , Y J Hwang , D H Lee , J I L Lim . *Proc. of ICCSA'05*, (of ICCSA'05) 2005. Verlag. 3480 p. .

[Choi et al. ()] 'Efficient RFID authentication protocol for ubiquitous computing environment'. E Y Choi , S M Lee , D H Lee . *Proc. of SECUBIQ'05*, LNCS (of SECUBIQ'05) 2005.

[Henrici and Mäuller ()] 'Hash-based enhancement of location privacy for radiofrequency identi¯cation devices using varying identifiers'. D Henrici , P Mäuller . *PERSEC'04*, 2004. IEEE Computer Society. p. .

[Kinoshita et al. ()] 'Low-cost RFID privacy protection scheme'. S Kinoshita , F Hoshino , T Komuro , A Fujimura , M Ohkubo . *In IPS Journal* 2004. 45 p. .

[Juels ()] 'Minimalist cryptography for lowcost RFID tags'. A Juels . *SCN'04*, 2004. Springer-Verlag. 3352 p. .

[Castelluccia and Avoine ()] 'Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags'. C Castelluccia , G Avoine . *Proceedings of CARDIS*, (CARDIS) 2006. 3928 p. .

[Juels and Pappu ()] *Privacy protection in RFID-enabled banknotes*, R Juels , Pappu . 2003. (Squealing euros)

[Juels and Brainard ()] 'Soft blocking: Flexible blocker tags on the cheap'. J Juels , Brainard . *WPES'04, ACM*, 2004. ACM Press. p. .

[Feldhofer et al. ()] 'Strong authentication for RFID systems using the AES algorithm'. M Feldhofer , S Dominikus , J Wolkerstorfer . *Proc. of CHES'04*, (of CHES'04) 2004. 3156.

[Juels et al. ()] 'The blocker tag: Selective blocking of RFID tags for consumer privacy'. R Juels , M Rivest , Szydlo . *ACM CCS'03 ACM*, 2003. ACM Press. p. .

[Golle et al. ()] 'Universal re-encryption for mixnets'. P Golle , M Jakobsson , A Juels , P Syverson . *CT-RSA'04*, 2004. Springer-Verlag. 2964 p. .