Volume : 1 | Issue : 5 | May 2012 ISSN - 2250-1991

Research Paper Engineering

Security For Near Field Communication in Cell Phone

* Biren M Patel ** Vijay B Ghadhvi *** Mr Ashish Kumar

* M.Tech Student, Dept Computer Science, Arya Institute of Technology, Jaipur

** M.Tech Student, Dept Computer Science, Mewar University, Chittodgarh

** *Asst.Prof, Dept Computer Science Arya Institute of Technology, Jaipur

ABSTRACT

In this paper gives a comprehensive analysis of security with respect to NFC. It is not limited to a certain application of NFC, but it uses a systematic approach to analyze the various aspects of security whenever an NFC interface is used. The authors 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. All of this is given in the context of currently available NFC hardware, NFC Applications and possible future developments of NFC.

Keywords :

INTRODUCTION

NFC stands for Near Field Communication. The specification details of NFC can be found in ISO 18092. The main characteristic of NFC is that it is a wireless communication interface with a working distance limited to about 10 cm. The interface can operate in several 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 it is called an active device, otherwise it is called a passive device. Active devices usually have a power supply, passive devices usually don't (e.g. contact less Smart Card). When two devices communicate three different Configurations are possible.

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 this means the base RF signal (13.56 MHz) is modulated with the data according to a coding scheme. If the baud rate is 106 k Baud, the coding scheme is the so-called modified Miller coding. If the baud rate is greater than 106 k Baud the Manchester coding scheme is applied. In both coding schemes a single data bit is sent in a fixed time slot. This time Slot is divided into two halves, called half bits. 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 baud rate. Greater than 106 k Baud the base RF signals at 13.56 MHz is modulated.

II. Applications

It is impossible to give a complete picture of NFC applications as NFC is just an interface. The following sub sections introduce three example applications.

A. Contact less Token

This covers all applications, which use NFC to retrieve some data from a passive token. The passive token could be a contact less Smart Card, an RFID label, or a key fob. Also, the token could be physically included in a device without any electric connections to that device.

B. Ticketing / Micro Payment

In this example application, 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 contact less 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.

C. Device Pairing

In this application the two devices communicating would belong to the same group of devices. An example could be a laptop and a digital camera. The user wants to establish a Bluetooth connection between the two devices to exchange image data. The Bluetooth link is established by bringing the two devices close together and running a given protocol over NFC between the two devices. This makes it obvious for the user which two devices get actually linked and takes away the burden of navigating through menus and selecting the right devices from lists of possible communication partners.

III. Threats

A. Eavesdropping

Because NFC is a wireless communication interface it is obvious that eavesdropping 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. 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 answer. For example the distance depends on the following parameters, and there are many more.

- RF filed characteristic of the given sender device.
- Characteristic of the attacker's antenna.
- Quality of the attacker's receiver
- Quality of the attacker's RF signal decoder
- Setup of the location where the attack is performed
- Power sent out by the NFC device

B. Data Corruption

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. Data corruption can be achieved by transmitting valid frequencies of the data spectrum at a correct time. The correct time can be calculated if the attacker has a good understanding of the used modulation scheme and coding. This attack is not too complicated, but it does not allow the attacker to manipulate the actual data. It is basically a Denial of Service attack.

C. Data Modification

In data modification the attacker wants the receiving device to actually receive, 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% and 10% modulation. In 100% modulation the decoder basically 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 it is preceded by a one. 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).Units Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). An exception is when English units are used as identifiers in trade, such as "3$\frac{1}{2}$ in disk drive." Avoid combining SI and CGS units. If you must use mixed units, clearly state the units for each quantity in an equation.

IV. Data Insertion

This means that the attacker inserts messages into the data exchange between two devices. But this is only possible, in case the answering device needs a very long time to answer. The attacker could then send his data earlier than the valid receiver. The insertion will be successful, only, if the inserted data can be transmitted, before the original device starts with the answer. If both data streams overlap, the data will be corrupted.

V. Man-in-the-Middle-Attack

In the classical Man-in-the-Middle Attack, two parties which 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 1.

Figure 1 Man-in-the-Middle Setup

Alice and Bob must not be aware of the fact that they are not talking to each other, but that they are both sending and receiving data from Eve. Such a setup is the classical threat in unauthenticated key agreement protocols like Diffie-Hellmann protocol. Alice and Bob want to agree on a secret key, which they then use for a secure channel. However, as Eve is in the middle, it is possible for Eve to establish a key with Alice and another key with Bob. When Alice and Bob later use their key to secure data, Eve is able to eavesdrop on the communication and also to manipulate data being transferred.

How would that work when the link between Alice and Bob is an NFC link?

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 eaves drop 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 active-active 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-word scenario.

VI. 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-in-the-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.

REFERENCES

[1] "Information technology - Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)", ISO/IEC 18092, First Edition, 2004-04-01. | [2]Morris Dworkin, "Recommendation for Block Cipher Modes of Operation", NIST Special Publication 800-38A, 2001. | [3]W. Diffie and M.E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory 22 (1976), 644-654.