Near Field Communication

Teodora Kostic

1. Introduction

Near Field Communication (NFC) is a short-range wireless connectivity technology that enables simple two-way interactions among electronic devices. It is a combination of RFID and contactless smart card technologies, with the purpose of creating device-independent communication and secure payment and data store functions for mobile and consumer electronics devices. As an open platform technology, NFC was standardized in ECMA 340 (Near field communication interface and protocol i.e. NFCIP-1) and was approved as an ISO/IEC standard at 2004 (ISO/IEC 18092). This standard alone does not specify encryption or security for the contactless communication at all. After short review of NFC standard we will discus possible security threats and solutions to protect against these threats.

2. NFC Standard

NFC relies on the proximity-card standard ISO/IEC 14443 allowing communication only over a distance up to 20cm. It works in the unlicensed and globally available ISM band of 13.56MHz. The communication always occurs between an NFC initiator and an NFC target and it starts by bringing them closely together. The initiator sends requests to the target, the target replies to these requests.

The NFCIP-1 standard defines two different communication modes: passive and active. In the passive mode, the NFC initiator supplies the RF field and starts the communication. It sends data to the NFC target at 106, 212 or 424 kbps. The NFC target does not have to generate a field, but sends data back to the initiator at the same speed using a load modulation scheme. In the active mode both devices are active and use their own RF field to enable communication. In this mode, both devices need to have a power supply. Mobile devices operating primarily in passive mode can achieve significant power savings, making longer precious battery life. It is not possible for initiator to be a passive device.

This standard specifies two different coding schemes to transfer data. If an active device transfers data at 106 kbps, a modified Miller coding with 100% modulation is used. If the bitrate is greater than 106 kbps the Manchester coding scheme is used with a modulation ratio of 10%. The data is sent using amplitude shift keying (ASK).

NFC devices can receive and send data at the same time. When at least two targets simultaneously transmit data the initiator can check the RF field and detect a collision. In order to avoid collision initiator for NFC communication will sense continuously for the presence of an external RF field. It will generate its own RF field if no external RF field is detected within defined timeframe [1].

Today NFC devices do not only implement NFCIP-1, but also NFCIP-2, which is defined in ISO 21481 and ECMA 352. New standard allows selecting one of three operating modes: NFC peer to peer mode (ISO 18092), card emulation mode (proximity inductive coupling card- PICC defined in ISO 14443), and reader/writer mode (Proximity Coupling Device-PCD).

3. Attacks

It should be emphasized that none of the above-mentioned NFC standards provide protection against possible attacks. Short descriptions of some relevant attacks are given below:

Data destruction: One possibility to disturb the signal is the usage of an RFID jammer. There is no way to prevent such an attack, but if the NFC devices check the RF field while they are sending, it is possible to detect collision. It is essentially a Denial of Service attack.

Data modification: Unauthorized modification of data, which results in valid messages, is much more difficult. In order to modify the transmitted data an adversary has to deal with the single bits of the RF signal. The feasibility of this attack depends on the strength of the amplitude modulation.

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.

Eavesdropping: Currently the NFCIP-1 link is a plain data link with no security underneath. This enables adversary to eavesdrop the communication and/or to modify the data over the RF link. In practice a malicious person would have to keep a longer distance in order not to get noticed. The question how close an adversary has to be located to recover a usable RF signal is difficult to answer. It depends on various factors listed in [2] : RF field 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.

Also, eavesdropping is extremely affected by the communication mode. A passive device, which does not generate its own RF field, is much harder to eavesdrop on than an active device. In [2] are given rough distances: up to 1m for passive mode and up to 10m for active mode.

Relay attack: Both standards ISO14443 and ISO18092 are open to relay attacks which can neither be recognized by the card nor by the reader. Relay attack is a type of attack related to man-in-the-middle attacks, in which the adversary makes independent connections with the card and the reader and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the adversary. The adversary must be able to intercept all messages going between the card and the reader and inject new ones, which is straightforward in many situations.

4. NFC- SEC

In order to propose protection against eavesdropping and data manipulation ECMA International released NFC security standard in December 2008. **ECMA-385** NFC-SEC: NFCIP-1 Security Services and Protocol is the common framework which defines services, the PDUs and the protocol. This standard is completed by **ECMA-386** NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES. This standard specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement and the Advanced Encryption Standard (AES) algorithm for data encryption.

ECMA-385 standard defines two services: The Shared Secret Service (SSE) and the Secure Channel Service (SCH). The SSE establishes a shared secret between two peer NFC-SEC Users, which they can use at their discretion for proprietary encryption mechanisms. The SCH provides a secure channel - the only real solution to eavesdropping and data modification. It uses the shared secret established before for a standardized secure channel service to protect all communication in either direction across a channel.

The NFC security protocol, specified in ECMA-385, consists of two phases: key establishment phase (required for both SSE and SCH services) and secure data exchange phase - Encryption and MAC (required only by SCH). To enable secure communication between NFC devices public key cryptography is used to establish a shared secret between these devices. This shared secret is used to establish the SSE and the SCH. The security parameter of the mechanism is 192 bit.

Figure 1 depicts key agreement and key confirmation- two steps of key establishment phase. In key agreement protocol two peer NFC-SEC entities agree on a shared secret using key agreement mechanism 4 from ISO/IEC 11770-3 and the Elliptic Curves Diffie-Hellman primitives. The ECDH primitive outputs shared secret Z.

When a master key is derived using one of the key derivation function processes both NFC-SEC entities check that they indeed have the same key. Each entity generates a key confirmation tag and sends it to the peer entity (MacTagA and MacTagB). For SSE service shared secret takes the value of the master key. The specified key derivation function and key confirmation are based on AES.

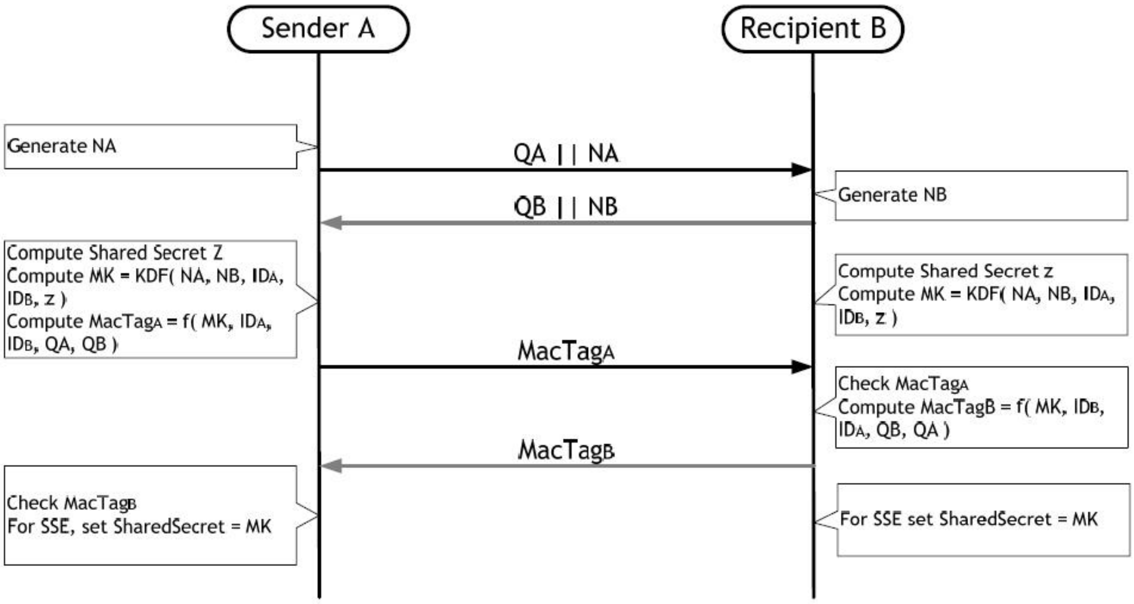
Sender A
Recipient B
Generate NA
QA | | NA
Generate NB
QB | | NB
Compute Shared Secret Z
Compute MK = KDF(NA, NB, IDA, IDB, z)
Compute MacTagA = f(MK, IDA, IDB, QA, QB)
Compute Shared Secret z
Compute MK = KDF(NA, NB, IDA, IDB, z)
MacTagA
Check MacTagA
Compute MacTagB = f(MK, IDB, IDA, QB, QA)
MacTagB
Check MacTagB
For SSE, set SharedSecret = MK
For SSE set SharedSecret = MK

Figure 1- Key agreement and confirmation overview [5]

After invocation of SCH data exchange between two entities, secure exchange protocol is used as defined in ECMA-385 as illustrated in Figure 2. Each entity generates the initial value of the CTR counter IV and initializes the Sequence Number variable SNV.

Integrity of all data transferred on the SCH is preserved through a MAC. The MAC used for data integrity is based on AES in XCBC-MAC-96 mode.

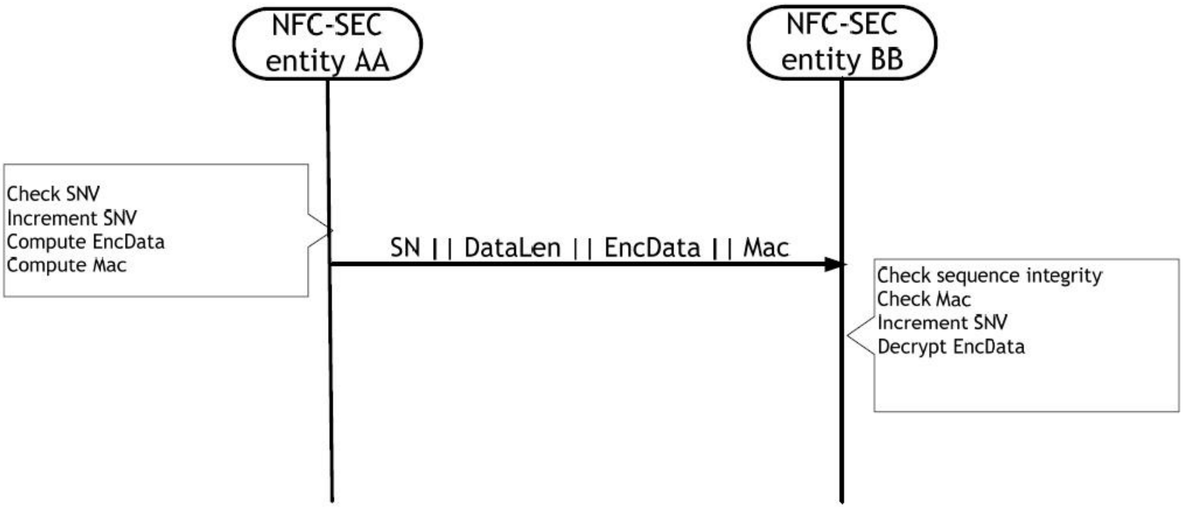

Figure 2 - SCH protocol overview [5]

5. Conclusion

NFC is an efficient short-range wireless communication technology. Combining such wireless communication technology with applications such as payment and ticketing in one device may raise potential privacy issues and security risks. NFC-SEC standard proposed by ECMA provides protection against eavesdropping and data modification attack but it stays vulnerable for Man-in-the-middle (MITM) attacks because no entity authentication can be provided since for the addressed use cases the peer NFC devices do not share any common secret. The practical risk of MITM attacks should be evaluated for individual implementation. The short operating distance and the specific RF characteristics of NFC [2] help keeping risk of MITM attacks low. Also, ECMA 385 and 386 address only peer to peer mode which is one of the 3 functioning modes of NFC. Currently, the NFC-SEC standard is submitted for ISO/IEC JTC1 Fast Track by ECMA International and is waiting for approval.

Reference

[1] Near Field Communication — Interface and Protocol (NFCIP-1), ISO/IEC 18092, First Edition, 2004-04-01.

[2] E. Haselsteiner and K. Breitfuss, *Security in near field communication*, Philips Semiconductors, Printed handout of Workshop on RFID Security RFIDSec 06, July 2006.

[3] G. Hancke, *Eavesdropping Attacks on High-Frequency RFID Tokens*. 4thWorkshop on RFID Security (RFIDsec'08), pp 100--113, July 2008.

[4] ECMA International: Standard ECMA-385, NFC-SEC: *NFCIP-1 Security Services and Protocol*, December 2008.

[5] ECMA International: Standard ECMA-386, NFC-SEC-01: *NFC-SEC Cryptography Standard using ECDH and AES*, December 2008.