Practical Experiences with NFC Security on mobile Phones

Gauthier Van Damme    Karel Wouters

Katholieke Universiteit Leuven
ESAT/SCD/IBBT-COSIC

Workshop on RFID Security, 2009
Outline

1 Security of the NFC Standard
   • The NFC Standard
   • NFC Security

2 Our Secure NFC Application
   • NFC Based Offline Payment System
   • Security of the System

3 Real NFC Security in Practice
   • Implementation Challenges
   • Implementation Results
Outline

1 Security of the NFC Standard
   - The NFC Standard
   - NFC Security

2 Our Secure NFC Application
   - NFC Based Offline Payment System
   - Security of the System

3 Real NFC Security in Practice
   - Implementation Challenges
   - Implementation Results
Outline

1. Security of the NFC Standard
   - The NFC Standard
   - NFC Security

2. Our Secure NFC Application
   - NFC Based Offline Payment System
   - Security of the System

3. Real NFC Security in Practice
   - Implementation Challenges
   - Implementation Results
Outline

1 Security of the NFC Standard
   • The NFC Standard
     • NFC Security

2 Our Secure NFC Application
   • NFC Based Offline Payment System
     • Security of the System

3 Real NFC Security in Practice
   • Implementation Challenges
     • Implementation Results
The ISO 18092 NFC Standard

- Near Field Communication (NFC) is a short range wireless communication standard based on inductive coupling at 13.56 MHz.
- 10 cm communication range in two modes: passive or active.
- Devices can be in both reader or card emulation mode.

Three basic transfer rates chosen by initiator: 106, 212 or 424 kbit/s.
- Very similar to some existing RFID standards.
The ISO 21481 NFC Standard

- Based on the previous NFC standard and older RFID standards at 13.56 MHz.
  It defines a framework for the following standards:
  - The ISO 18092 standard for NFC
  - The ISO 14443 Type A/B standard for proximity cards (e.g. Mifare)
  - The ISO 15693 standard for vicinity cards (e.g. FeliCa)
- This makes the NFC standard compatible with existing and widely deployed RFID systems.
Outline

1. Security of the NFC Standard
   - The NFC Standard
   - NFC Security

2. Our Secure NFC Application
   - NFC Based Offline Payment System
   - Security of the System

3. Real NFC Security in Practice
   - Implementation Challenges
   - Implementation Results
Attacks on NFC communications

Haselsteiner and Breitfuss [RFIDSec 06] showed that even with the short transmission range, attacks on NFC remain possible:

- **Eavesdropping:**
  - Possible if the attacker is more or less close.
  - Harder for passive communications.
  - Up to 10 m for active and 1 m for passive devices.

- **Data Modification:**
  - Only to some extent for the 106 kbit/s transfer rate.
  - Possible for the other transfer rates.

- **Man-In-The-Middle attacks:**
  - Not possible at the communication layer due to collision detection.
  - As will be explained later: possible at higher application layer.
Attacks on NFC communications

Haselsteiner and Breitfüß [RFIDSec 06] showed that even with the short transmission range, attacks on NFC remain possible:

- **Eavesdropping:**
  - Possible if the attacker is more or less close.
  - Harder for passive communications.
  - Up to 10 m for active and 1 m for passive devices.

- **Data Modification:**
  - Only to some extent for the 106 kbit/s transfer rate.
  - Possible for the other transfer rates.

- **Man-In-The-Middle attacks:**
  - Not possible at the communication layer due to collision detection.
  - As will be explained later: possible at higher application layer.
Attacks on NFC communications

Haselsteiner and Breitfuß [RFIDSec 06] showed that even with the short transmission range, attacks on NFC remain possible:

- **Eavesdropping:**
  - Possible if the attacker is more or less close.
  - Harder for passive communications.
  - Up to 10 m for active and 1 m for passive devices.

- **Data Modification:**
  - Only to some extent for the 106 kbit/s transfer rate.
  - Possible for the other transfer rates.

- **Man-In-The-Middle attacks:**
  - Not possible at the communication layer due to collision detection.
  - As will be explained later: possible at higher application layer.
Attacks on NFC communications

Haselsteiner and Breitfuß [RFIDSec 06] showed that even with the short transmission range, attacks on NFC remain possible:

- **Eavesdropping:**
  - Possible if the attacker is more or less close.
  - Harder for passive communications.
  - Up to 10 m for active and 1 m for passive devices.

- **Data Modification:**
  - Only to some extent for the 106 kbit/s transfer rate.
  - Possible for the other transfer rates.

- **Man-In-The-Middle attacks:**
  - Not possible at the communication layer due to collision detection.
  - As will be explained later: possible at higher application layer.
Outline

1. Security of the NFC Standard
   - The NFC Standard
   - NFC Security

2. Our Secure NFC Application
   - NFC Based Offline Payment System
   - Security of the System

3. Real NFC Security in Practice
   - Implementation Challenges
   - Implementation Results
Current Payment Systems and Drawbacks

Current commercial offline payment systems (eWallets) use contact smart cards (e.g. The Proton System in Belgium).

Their success is limited and their use is decreasing:

- Users can not check their balance anytime anywhere.
- Users can not transfer money to each other.
- Current online payment systems are almost as fast.
Current Payment Systems and Drawbacks

Current commercial offline payment systems (eWallets) use contact smart cards (e.g. The Proton System in Belgium).

Their success is limited and their use is decreasing:

- Users can not check their balance anytime anywhere.
- Users can not transfer money to each other.
- Current online payment systems are almost as fast.
Current Payment Systems and Drawbacks

Current commercial offline payment systems (eWallets) use contact smart cards (e.g. The Proton System in Belgium).

Their success is limited and their use is decreasing:

- Users can not check their balance anytime anywhere.
- Users can not transfer money to each other.
- Current online payment systems are almost as fast.
NFC enabled mobile phones have the interface to solve the previous issues and even improve usability:

- Users can check their balance anytime anywhere.
- Users can transfer money to each other.
- The contactless communication could improve speed.
- Users can top up their balance anytime anywhere.
- Transfer of money does not need a connection to an external server.
NFC enabled mobile phones have the interface to solve the previous issues and even improve usability:

- Users can check their balance anytime anywhere.
- Users can transfer money to each other.
- The contactless communication could improve speed.
- Users can top up their balance anytime anywhere.
- Transfer of money does not need a connection to an external server.
NFC enabled mobile phones have the interface to solve the previous issues and even improve usability:

- Users can check their balance anytime anywhere.
- Users can transfer money to each other.
- The contactless communication could improve speed.
- Users can top up their balance anytime anywhere.
- Transfer of money does not need a connection to an external server.
NFC Based Offline Payment Systems

NFC enabled mobile phones have the interface to solve the previous issues and even improve usability:

- Users can check their balance anytime anywhere.
- Users can transfer money to each other.
- The contactless communication could improve speed.
- Users can top up their balance anytime anywhere.
- Transfer of money does not need a connection to an external server.
NFC enabled mobile phones have the interface to solve the previous issues and even improve usability:

- Users can check their balance anytime anywhere.
- Users can transfer money to each other.
- The contactless communication could improve speed.
- Users can top up their balance anytime anywhere.
- Transfer of money does not need a connection to an external server.
NFC based offline payment systems

NFC enabled mobile phones have the interface to solve the previous issues and even improve usability:

- Users can check their balance anytime anywhere.
- Users can transfer money to each other.
- The contactless communication could improve speed.
- Users can top up their balance anytime anywhere.
- Transfer of money does not need a connection to an external server.
Security Issues of Offline NFC Payment

- Security challenges in wireless offline payment systems:
  - Money could be created or duplicated.
  - Money could be transferred to the wrong person.
  - Money could get lost in transaction.

- NFC does not guarantee enough security so cryptographic primitives are needed to prevent the above possibilities to happen.
The Developed NFC Payment System

- The system is based on the in Belgium very popular system of meal vouchers.

- Today paper vouchers are used.
  - Concept: put the vouchers on the mobile phone of the users:
    - They get the vouchers every month from their employee through SMS.
    - Each voucher has an amount and can be used during offline NFC payments.
    - Users can transfer vouchers to other users through NFC.
  - Highly secure protocols used to prevent previous issues.
  - Purpose: Check the feasibility of secure offline NFC payments using current technology.
The Developed NFC Payment System

- The system is based on the in Belgium very popular system of meal vouchers.

- Today paper vouchers are used.

- Concept: put the vouchers on the mobile phone of the users:
  - They get the vouchers every month from their employer through SMS.
  - Each voucher has an amount and can be used during offline NFC payments.
  - Users can transfer vouchers to other users through NFC.

- Highly secure protocols used to prevent previous issues.

- Purpose: Check the feasibility of secure offline NFC payments using current technology.
The Developed NFC Payment System

- The system is based on the in Belgium very popular system of meal vouchers.
- Today paper vouchers are used.
- Concept: put the vouchers on the mobile phone of the users:
  - They get the vouchers every month from their employee through SMS.
  - Each voucher has an amount and can be used during offline NFC payments.
  - Users can transfer vouchers to other users through NFC.
- Highly secure protocols used to prevent previous issues.
- Purpose: Check the feasibility of secure offline NFC payments using current technology.
The Developed NFC Payment System

- The system is based on the in Belgium very popular system of meal vouchers.

- Today paper vouchers are used.
- Concept: put the vouchers on the mobile phone of the users:
  - They get the vouchers every month from their employee through SMS.
  - Each voucher has an amount and can be used during offline NFC payments.
  - Users can transfer vouchers to other users through NFC.

- Highly secure protocols used to prevent previous issues.
- Purpose: Check the feasibility of secure offline NFC payments using current technology.
Outline

1 Security of the NFC Standard
   - The NFC Standard
   - NFC Security

2 Our Secure NFC Application
   - NFC Based Offline Payment System
   - Security of the System

3 Real NFC Security in Practice
   - Implementation Challenges
   - Implementation Results
The Application Backbone

- To allow secure offline voucher transaction: PKI used.
- Use of a secure hardware module or Secure Element (SE) inside the phone:
  - Users have limited access to it.
    - Controlled by a Trusted Service Manager (TSM).
    - The application can be trusted by the users.
  - No meal vouchers leaves the SE unencrypted.
    - Malware on the untrusted mobile phone OS can not access meal vouchers.
    - In combination with the PKI: MITM attacks at higher layers impossible.
- Vouchers are numbered and signed by the issuer.
The Cryptographic Components

Cryptographic primitives used to obtain secure PKI based voucher transfer protocols:

- A public key encryption and signature scheme: 1024 bit RSA based.
- A hash function: SHA-1.
- A symmetric encryption function: 3DES.
- A Message Authentication function: 3DES based.
- Certificates for the PKI: X.509.
User To User Voucher Transfer

**Sender**
- Select Applet, PIN
- *Transfer X EUR*
- Set transfer PIN
- Verify Certificate Info, R1 = Enc_rsaop (K1), R2 = Session Id, Sig_send(C, Sess Id, Recip Id, K1), Certificate info
- check MAC, Mark vouchers V1...Vn as dirty, M1 = Enc, K1(V1...Vn)
- Verify MAC, Delete/trash V1...Vn

**Recipient**
- Select Applet
- Select transfer PIN
- Generate Random Challenge C
- Decrypt R1 -> K1
- Verify Signature, Certificate Info, K2 = SHA-1(K1), R3 = MAC_K2(Sess Id.C)
- Decrypt M1
- Store/verify V1...Vn, M2 = MAC_K2(V1...Vn)
- Select MIDlet (new Vouchers)
Outline

1 Security of the NFC Standard
   - The NFC Standard
   - NFC Security

2 Our Secure NFC Application
   - NFC Based Offline Payment System
   - Security of the System

3 Real NFC Security in Practice
   - Implementation Challenges
   - Implementation Results
Limitations of Java Card Development

- Java Card 2.2.1 running on the SE limits possibilities:
  - Not Object Oriented.
  - Limited number of cryptographic libraries.
  - Old and insecure primitives defined.
- No internal trusted clock.
- Connection to the SE through APDU calls is time consuming.
- Some problems solved in Java Card 3.0.
Outline

1 Security of the NFC Standard
   • The NFC Standard
   • NFC Security

2 Our Secure NFC Application
   • NFC Based Offline Payment System
   • Security of the System

3 Real NFC Security in Practice
   • Implementation Challenges
   • Implementation Results
Limitations of Java Card Hardware

- The SE has a co-processor for both 3DES and PKI operations.
- But translation from high level Java code to hardware causes big overhead.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Data Length</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Key Encryption</td>
<td>100 byte</td>
<td>98.8 ms</td>
</tr>
<tr>
<td>Private CRT Key Signature</td>
<td>100 byte</td>
<td>287.9 ms</td>
</tr>
<tr>
<td>Triple DES in CBC mode</td>
<td>100 byte</td>
<td>34.3 ms</td>
</tr>
<tr>
<td>SHA-1 Hashing</td>
<td>100 byte</td>
<td>29.5 ms</td>
</tr>
</tbody>
</table>

Table: Timing of different Java Card operations.

- Improve results by removing translation layers and use more efficient algorithms and hardware.
Limitations of the NFC Enabled Phones

- The Nokia NFC phones can not connect both to an external and an internal NFC device at the same time.
- The phone has to continuously poll: time consuming.

<table>
<thead>
<tr>
<th>Phone</th>
<th>External Phone Status</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nokia 6313</td>
<td>Off and zero distance</td>
<td>0.46 s</td>
</tr>
<tr>
<td>Nokia 6313</td>
<td>On and zero distance</td>
<td>0.68 s</td>
</tr>
<tr>
<td>Nokia 6313</td>
<td>On and 0.5 cm distance</td>
<td>0.8 - 1,0 s</td>
</tr>
<tr>
<td>Nokia 6212</td>
<td>On and zero distance</td>
<td>1.62 - 2.74 s</td>
</tr>
</tbody>
</table>

**Table**: Timings for opening connections.

- Improve results by allowing the internal NFC connection to remain open during external NFC connection.
Summary

- Implement a fully secure offline NFC based payment system.
- System is working but transactions are too slow for commercial implementations.
  Phone-to-phone transactions take approximately 6 seconds.
- Today’s technology not ready for advanced NFC-based eWallets.