NFC
Near Field Communication

– Easy to use wireless communication interface for the last few centimeters
– Easy to use target selection, by simply holding two devices close to each other

NFC is as easy as ...
... a touch
Near Field Communication

- Wireless short range communication technology
  - NFC is designed for short distance wireless communication
  - Allows intuitive initialization of wireless networks
  - NFC is complementary to Bluetooth and 802.11 with their long distance capabilities
  - NFC also works in dirty environment
  - NFC does not require line of sight
  - Easy and simple connection method
  - Provides communication method to non-self powered devices
NFC - Technical Basics

- Wireless Short Range Communication Technology
  - Based on RFID technology at 13.56 MHz
  - Operating distance typical up to 10 cm
  - Compatible with today’s field proven contactless RFID technology
  - Low bandwidth: data rate today up to 424 kilobits/s
NFC – Technical Basics (Cont.)

• It’s a contactless card and a contactless reader in one chip

• Applications aimed for are
  – Ticketing
  – Payment
  – Device Pairing

Short Range
13,56MHz
RF Link
Near Field Communication
Applications

- Smart Key
  - for mobile local payment

- Peer to Peer communication, Virtual Connector
  - either directly or by establishing wireless links

- Low cost solution to distribute info / services
  - e.g. by passive loops embedded in paper media

NFC enables a unique blend of valued applications
Differences from other wireless technologies

- **Bluetooth**: Although both Bluetooth and NFC can be used to transfer data, Bluetooth has been designed to transfer data over much greater distances. NFC is designed to be close proximity only.

- **Wi-Fi / IEEE 802.11**: Wi-Fi is designed for local area networks, and is not a short range peer to peer technology.

- **RFID**: Although RFID is very similar to NFC in many respects, RFID is a much broader technology. NFC is a specific case which is defined by standards enabling it to be interoperable.
Two Operation modes

• There are dedicated roles
  – **Initiator** and **Target**
  – Any data transfer is a message and reply pair.

• There are dedicated modes of operation
  – **Active** and **Passive**
  – Active means the device generates an RF field
  – Passive means the device uses the RF field generated by the other device
Three communication modes

• **Read / Write:**
  – allows applications to transfer data in an NFC Forum-defined message format
  – not secure
  – supported the Contactless Communication API

• **NFC card emulation:**
  – enables the NFC device to behave as a standard Smartcard
  – data transfer is secure
  – supported by the Contactless Communication API.

• **Peer to peer:**
  – device to device link-level communication
  – not supported by the Contactless Communication API.
## More details

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Active</th>
<th>Passive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Possible</td>
<td>Not Possible</td>
</tr>
<tr>
<td>Target</td>
<td>Possible</td>
<td>Possible</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Baud</th>
<th>Active</th>
<th>Passive</th>
</tr>
</thead>
<tbody>
<tr>
<td>106 kBaud</td>
<td>Modified Miller, 100% ASK</td>
<td>Manchester, 10% ASK</td>
</tr>
<tr>
<td>212 kBaud</td>
<td>Manchester, 10% ASK</td>
<td>Manchester, 10% ASK</td>
</tr>
<tr>
<td>424 kBaud</td>
<td>Manchester, 10% ASK</td>
<td>Manchester, 10% ASK</td>
</tr>
</tbody>
</table>
Manchester coding

Low -> high: 0
High -> low: 1

Coded “0”

Coded “1”

Manchester Coding, 10% ASK
Modified Miller coding

Key:
- 0 after 0
- 0 after 1
- 1 after 0 or 1
NFC Security

• Eavesdropping
  – No protection
    • Use a Secure Channel

• Data Modification
  – No protection
    • Use Secure Channel

• Replay attacks
  – No protection

• Man in the Middle Attack
Man in the Middle Attack

Man-in-the-Middle

Alice

Eve

Bob
Man in the Middle Attack

- Alice
- Bob
- Eve

Message

Man-in-the-Middle
Man in the Middle Attack

Alice → Bob

Message

Eavesdropping

Eve

Man-in-the-Middle
Man in the Middle Attack

[Diagram showing the interaction between Alice, Bob, and Eve with arrows indicating message flow and eavesdropping.

- Alice
- Bob
- Eve

Message flow:
- Alice → Bob
- Alice → Eve (Man-in-the-Middle)

Annotations:
- Disturb
- Eavesdropping

Legend:
- Man-in-the-Middle

Contents:
- NFC Intro
- Eavesdropping
- Data Modification
- Secure Channel
- Conclusion
Man in the Middle Attack

Alice detects the disturbance and stops the protocol

- Check for active disturbances!
Man in the Middle Attack

Man-in-the-Middle

Alice

Bob

Eve

Message
Eve cannot send to Bob, while RF field of Alice is on!
- Use Active – Passive connection!
- Use 106 kBaud!
NFC Security

• Eavesdropping
  – No protection
  • Use a Secure Channel

• Data Modification
  – No protection
  • Use Secure Channel

• Replay attacks
  – No protection

• Man in the Middle Attack
  – Protection