University of Applied Sciences

Digital Signature Records for the NFC Data Exchange Format

Michael Roland
Upper Austria University of Applied Sciences, Hagenberg, Austria

2nd International Workshop on Near Field Communication
20 April 2010, Monaco

This work is part of the project "4EMOBILITY" within the EU program "Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)" funded by the European regional development fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).

NFC Research Lab Hagenberg

- Part of the R&D department of the
  Upper Austria University of Applied Sciences
- Research on NFC since 06/2005
- Our focus:
  - Hardware & software systems for NFC
  - Interoperability and performance testing for NFC systems
  - NFC applications and infrastructure
  - Security and user experience with NFC
- 1st Austrian NFC trial
- NFC Congress in Hagenberg

Outline

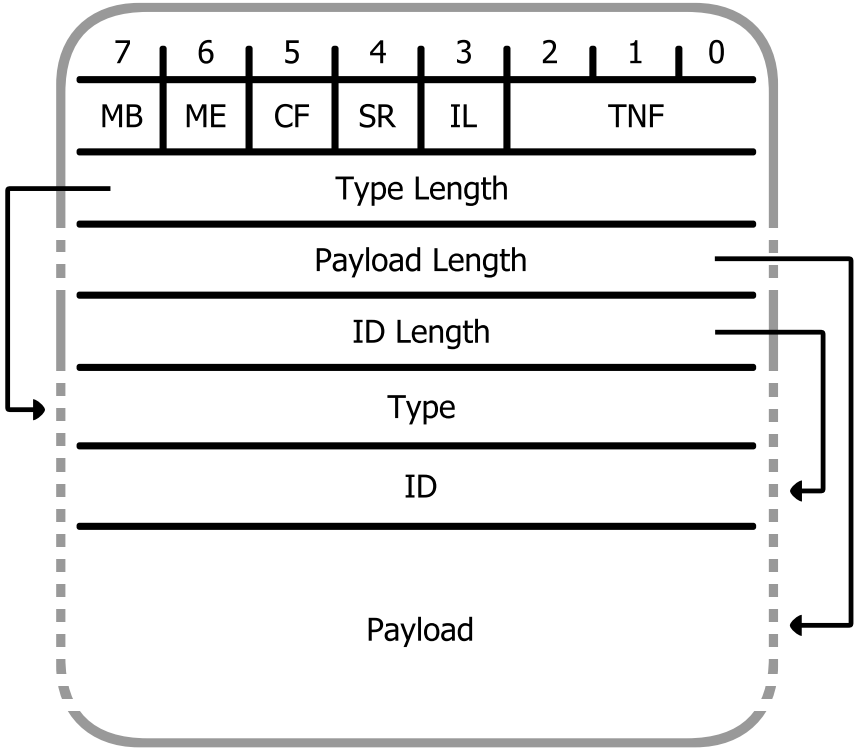
- Introduction and Motivation
  - What is the NFC Data Exchange Format?
  - What are potential attacks against NDEF applications?
  - How can digital signatures help?
- Signing NDEF Messages
  - How to add a signature to an NDEF message?
  - Are signatures backwards compatible?
  - Which parts of an NDEF record need to be signed?
- Conclusion

NFC Data Exchange Format (NDEF)

- Standardized data format for NFC applications
- Enables the “it’s all in a touch” principle:
  - Upon touching an NFC-enabled object with an NFC device NDEF messages are exchanged and an action is triggered.
- Applications are:
  - Business cards
  - Smart posters (i.e. posters with active content like a website‘s URL or instructions to send an SMS message)
  - Enabler for wireless technologies (i.e. Bluetooth or WiFi pairing)
  - …

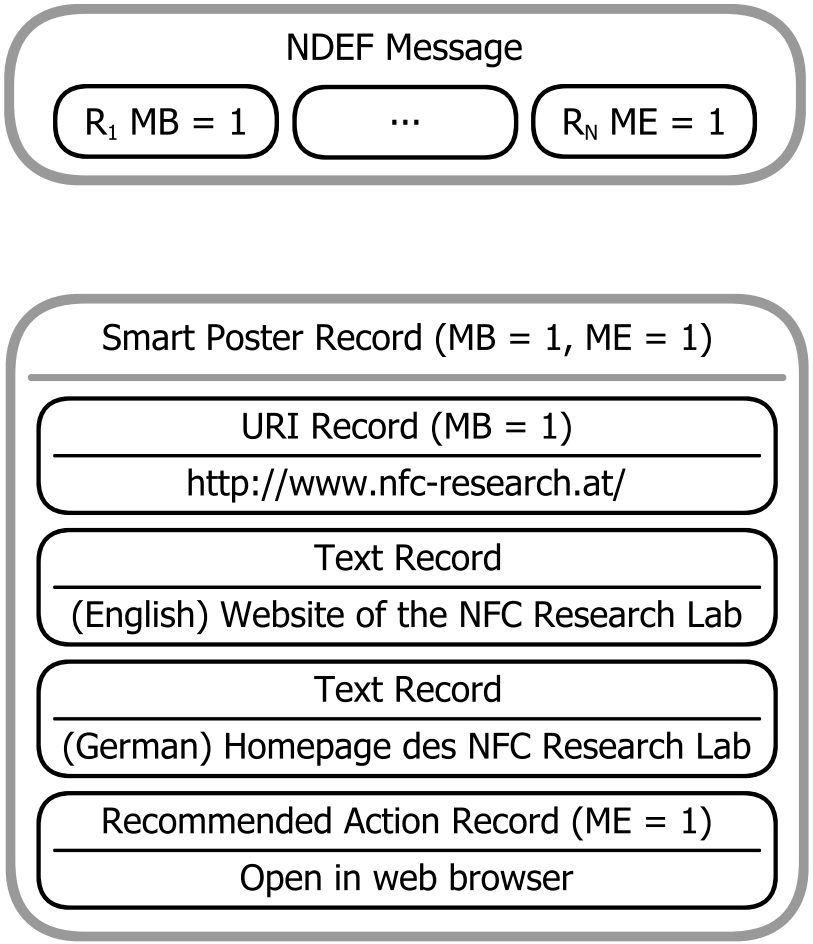
NDEF Record

- Header
  - Flags
    - Message Begin (MB)
    - Message End (ME)
    - Chunk Flag (CF)
    - Short Record (SR)
    - ID Length present (IL)
  - Type Name Format (TNF)
  - Length fields
  - Type
  - ID
- Payload



NDEF Message

- Sequence of one or more NDEF records
- First record has MB set
- Last record has ME set
- Records can contain NDEF messages as payload
  - Smart Poster Record



Vulnerabilities of NDEF applications

- Manipulation/replacement of NFC tags and their content
- The average user cannot distinguish forged from genuine tags!
- Flaws in current NDEF implementations:
  - E.g. it is possible to hide a smart poster‘s URI on the Nokia 6131 NFC
- Typical attack scenarios:
  - Replace a smart poster‘s URL (e.g. redirect to phishing site)
  - Replace a phone number (e.g. redirect to premium rate service)

Digital Signatures

- What is a signature?
  1. A hash value is generated from the data.
     - Assures integrity of the signed data
  2. The hash value is encrypted with the signers secret key.
     - Assures authenticity of the signed data
- Properties of a digital signature:
  (based on a trustworthy certification infrastructure)
  - Authentic: The signer‘s identity can be verified.
  - Unforgeable: Only the owner of the signing key can produce a certain signature.
  - Non-reusable: The signature is only valid for the signed data.

Digital Signatures

- Potentials:
  - Origin of data can be verified
  - Trustworthiness of data can be estimated based on its origin
- Dangers:
  - False sense of protection (due to bad implementations)
  - Not all types of attack can be avoided
    - E.g. valid signed tags could be misplaced within the system
    - Denial of service attacks

Signing NDEF messages

- NFC Forum‘s approach:
  - use a dedicated record type (“Signature Record Type”)
- Signature record is appended to a sequence of records
- Signature record signs every record between the previous signature record and itself (or the beginning of the NDEF message and itself)
- One NDEF message may contain more than one signature

Backwards compatibility

- 2 types of compatibility:
  - Compatibility to devices that do not support signature records
  - Compatibility to tag infrastructures that do not use signatures
- Signature Record Type is compatible to existing devices, as unknown record types will be ignored.
- Existing tag infrastructures that do not use signatures:
  - Disallowing NDEF records without signature would render current tag infrastructures unusable
  - BUT: NDEF records without signature must be treated with a different level of trust than signed records

Signing NDEF records

- Including certain fields of an NDEF record into the signature has advantages and disadvantages
- Advantages and disadvantages were evaluated

Message Begin (MB), Message End (ME)

- MB and ME mark the first and the last record in an NDEF message
- When the signature record is appended to the signed records, none of the signed records must have the ME flag enabled.
  - ME must not be included into the signature!
- When MB is signed, a signed sequence of records cannot be moved away from or to the beginning of a message.
  - Including MB is not useful!

Type, ID, Payload

- Payload contains the record‘s data
  - Must be included into the signature
- Type defines how the Payload field must be interpreted
  - Must be included into the signature
- ID contains a reference that allows linking from other records
  - Must be included into the signature
    - Otherwise links could be redirected to manipulated targets

Short Record Flag (SR)

- Controls the size of the Payload Length field:
  - SR = 0: Payload Length has 4 bytes
  - SR = 1: Payload Length has 1 byte
- When SR and Payload Length are not signed:
  - Repacking between short record format and standard record format possible
- When Length fields are signed but SR is not:
  - Bytes can be shifted from or to the Payload Length field, resulting in a (limited) manipulation of the length fields
  - Not signing SR has no advantage as repacking is not possible anyways

ID Length Present Flag (IL)

- Controls the presence of the ID Length (and the ID field):
  - IL = 0: no ID Length field available (no ID field)
  - IL = 1: ID Length field available (specifies the ID field's length)
- When IL and Length fields are not signed:
  - Attacker could add/remove an ID field
  - ID field could be used to hide a suffix of the Type field or a prefix of the Payload field
  - An existing ID field could be integrated into the Type or the Payload field
- When Length fields are signed but IL is not:
  - Attack is difficult as sizes cannot be arbitrarily chosen

Type Length, Payload Length, ID Length

- Length fields specify the length (in bytes) of corresponding the fields
- When Length fields are not signed:
  - Signed bytes can be moved between the field boundaries
    - E.g. ID field could be integrated into Payload or appended to Type field
  - Signed parts of subsequent records could be integrated into the preceeding record‘s Payload field
- When Length fields are signed:
  - Attacker can only change field sizes by modification of SR and IL (only very limited changes possible)

Chunk Flag (CF)

- Allows splitting the payload across multiple chained records
  - CF = 0: last record of a record chain
  - CF = 1: payload is continued in next record
- First record of a record chain contains the Type and ID fields, following records have Type Name Format (TNF) set to “continued payload” and have no Type and ID field
- When only Type, ID and Payload are signed:
  - Splitting and merging chunks is possible without invalidating the signature
- When CF is not signed:
  - Parts of a chunked NDEF record can be chopped off by clearing one CF flag
  - The chopped chunks are still part of the NDEF message, but the NDEF parser will drop them as invalid records
  - If TNF is not signed it could be set from “continued payload” to “unknown”, which makes the parser ignore the records without raising any error

Type Name Format (TNF)

- TNF specifies the interpretation of the Type field
  - Value can be:
    - Empty
    - NFC Forum well-known type
    - MIME media type
    - NFC Forum external type
    - Unknown
    - Continued from previous record
    - Reserved
- When TNF is changed, the meaning of the Type field changes (e.g. from well-known to external type)
  - Can be used to hide records from the receiving application

Contactless Communication API (JSR 257)

- Java API for encoding/decoding NDEF messages
- Has certain level of abstraction:
  - Record chunks are combined into one full record
- Consequence:
  - Header fields of all continued chunks are hidden from the user
  - These header fields cannot be used with signature implementations on top of JSR 257
  - On top of JSR 257 only Type, ID, Payload, Type Length and ID Length can be protected

Conclusion

- Some fields of an NDEF record must be signed:
  - Type, ID, Payload
- Some fields of an NDEF record should not be signed:
  - Message Begin (MB), Message End (ME)
- Signing the other fields has advantages and disadvantages

Conclusion

- Advantages:
  - Signatures can be used on top of current JSR 257 implementations
  - Records can be repacked (short records, chunked records)
- Disadvantages:
  - Vulnerable to attacks
    - Record hiding
    - Breaking ID field references

Field name	Signature useful	Possible on top of JSR 257
Message Begin	−−	−−
Message End	−−	−−
Chunk Flag	+	−−
Short Record Flag	+	−−
ID Length Present Flag	+	−−
Type Name Format	+	−−
Type Length	+	++
Payload Length	+	−−
ID Length	+	++
Type	++	++
ID	++	++
Payload	++	++

Thank You!

Michael Roland
Research Associate, NFC Research Lab Hagenberg
Upper Austria University of Applied Sciences, Hagenberg, Austria

michael.roland (at) fh-hagenberg.at

This work is part of the project "4EMOBILITY" within the EU program "Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)" funded by the European regional development fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).