A Record Composition/Decomposition Attack on the NDEF Signature Record Type Definition

Muhammad Qasim Saeed
ISG, Department of Mathematics
Royal Holloway University of London
Egham, UK
muhammad.saeed.2010@live.rhul.ac.uk

Colin D.Walter
ISG, Department of Mathematics
Royal Holloway University of London
Egham, UK
Colin.Walter@rhul.ac.uk

***Abstract*—The Signature Record Type Definition was released by the Near Field Communication (NFC) Forum to provide integrity and authenticity to the NFC Data Exchange Format (NDEF). It achieves this goal by adding a digital signature and corresponding certificates to the NDEF message. Although the Signature Record Type Definition (Signature RTD) specifies the use of strong cryptographic algorithms like RSA, DSA, ECDSA, a few vulnerabilities have been discovered in its implementation. A recently published Record Composition Attack by Roland *et al.* (2011) describes how data can be modified in an NDEF message by exploiting the Type Name Format (TNF) field even though the NDEF message is protected by a Signature Record. This paper takes a close look at this attack and points out that, apart from TNF value, a few other fields of the NDEF header must also be manipulated in order to implement this attack successfully. It is shown how to do this and some modifications to the signature scheme are proposed in order to counter such attacks. However, more significantly, we need to propose an update to the NDEF record specification in order to achieve the security required from a signature scheme.**

***Index Terms*—Near Field Communication; Security; Smart Poster; NFC Data Exchange Format (NDEF); Signature Record Type Definition.**

I. Introduction

This paper takes a close look at the Signature RTD, its vulnerabilities and countermeasures. The first part introduces the technical aspects of Near Field Communication (NFC), including the format for NFC messages and the originally proposed digital signature scheme [1]. After this, two attacks on the signature scheme by Roland *et al.* [2] are presented and some critical deficiencies are described. Our main novel contributions are firstly a revision of their Record Composition attack which does succeed, and, secondly, a revised signature scheme which is proposed to counter both this attack and their Record Decomposition attack. We conclude with our third and most important novel contribution, namely a necessary revision of the NDEF record specification. This is based on the conclusion that the NDEF record definition itself needs to be amended in order to guarantee the integrity and authenticity which a signature should provide against, in particular, the two attacks described. This is a significant result because of its implications for the existing NFC infrastructure.

II. Near Field Communication

Near Field Communication (NFC) is a short-range wireless technology compatible with contactless smart cards (ISO/IEC 14443) and radio-frequency identification (RFID) [3]. NFC communicates on the 13.56 MHz frequency band at a distance of less than 4 cm. It uses magnetic field induction for communication and powering the chip.

NFC technology has a number of applications such as ticketing and payment, retrieving information from information kiosks or setting up connections between devices (so called *device pairing*). A wide variety of applications is possible using the technology because of the different operation modes supporting both communication from device to device (peer-to-peer mode), communication between a device and a passive tag (read/write mode) and an emulation mode where a device can act like a contactless smart card [4].

III. The NFC Forum

The NFC Forum was established in 2004 to standardize the applications related to NFC [5]. The NFC Forum promotes sharing, pairing, and transactions between NFC devices or tags. In June 2006, the Forum formally outlined the architecture of NFC technology. One such use of NFC tags is in so-called Smart Posters. These contain information such as Title, SMS, and a URL or electronic business card. The user can access this information by simply touching the cell phone on such tags. Apart from displaying the information to the user, the smart poster can also trigger an action such as opening a specific website, calling the telephone number stored in the poster etc [6].

With the increasing number of available applications of NFC technology, threats of its abuse also emerged in parallel. In the case of abuses related to smart posters, an attacker may replace the URL address or the telephone number with malicious content. Consequently, it must be possible to guarantee the integrity and authenticity of NFC data.

The NFC Forum developed the Signature Record Type Definition (Signature RTD) in 2010 to fix such problems [1]. The main objective of the signature RTD is to digitally sign the data fields of an NDEF message thus providing integrity and authenticity.

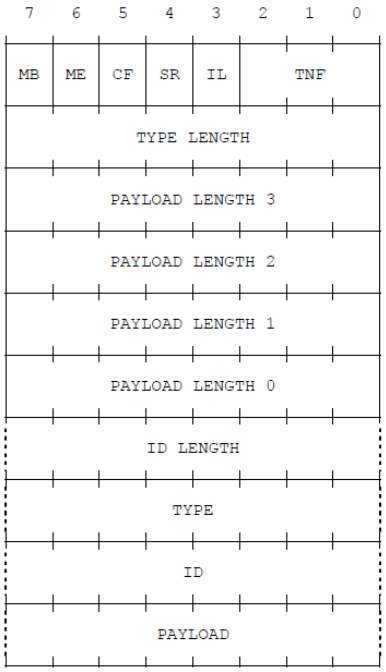

Fig. 1. NDEF Record Layout ([7], fig. 3)

A. NFC Data Exchange Format

The NFC Data Exchange Format (NDEF) specification defines a common format and rules to exchange information in the NFC environment. NDEF is a lightweight, binary message format that can be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct. Each payload is described by a type, its length, and an optional identifier. A record is the unit for carrying the payload within an NDEF message. An NDEF message contains one or more NDEF records [7]. The structure of an NDEF record is shown in Figure 1.

Message Begin *(MB)* and Message End *(ME)* mark the first and the last record of an NDEF message respectively. The Chunk Flag *(CF)* specifies that the payload of that record is continued in the next record. Short Record *(SR)* is a 1-bit flag which, if set, indicates that the size of the *Payload-Length* field is one byte. In this case, the payload size is restricted to between 0 and 255 bytes. Otherwise, the *Payload-Length* field consists of 4 bytes (as shown in Figure 1) and the Payload size ranges from 0 to $2^{32}-1$ bytes. The flag *IL* determines whether or not the optional *ID* field and corresponding *ID-Length* field are present.

The Type Name Format *(TNF)* is a 3-bit field indicating the structure of the *Type* field. Its value ranges between 0 and 7 as shown in Table I.

Type-Length and *ID-Length* are unsigned 8-bit integers that specify the length in octets of the *Type* field and *ID* field respectively. *Payload-Length* field is an unsigned integer that specifies the length in octets of the Payload field. The size of the *Payload-Length* field is 4 bytes when the *SR* flag is clear, and otherwise the size is 1 byte. The *Type* field describes the type of the payload. The *ID* field is an optional identifier in the form of a URI reference.

TABLE I
TYPE NAME FORMAT *(TNF)* DESCRIPTION (*cf* [7], TABLE 1)

TNF	Description
0	The record is empty and there is no payload or type associated with this record. The corresponding length fields are set to zero. This TNF value can be used whenever an empty record is needed.
1	indicates that the *Type* field contains a value that follows the RTD type name format defined in the NFC Forum RTD specification, such as Smart poster RTD, Signature RTD, URL RTD etc.
2	Type is a MIME media type identifier (RFC 2406).
3	Type is an absolute URI (RFC 3986).
4	Type is an NFC Forum external type.
5	Type is of unknown format. It is used when the type of the payload is unknown. When used, the *Type-Length* field must be zero and thus the *Type* field is omitted. In this case, the payload is stored but not processed.
6	The record continues the payload of the preceding chunked record. When used, the *Type-Length* field must be zero and thus the *Type* field is omitted.
7	Reserved for future use.

B. Record Chunks

A record chunk carries a chunk of a payload. It can be used to partition dynamically generated contents or very large entities into multiple subsequent record chunks within an NDEF message. Every chunk payload in encoded as an *initial* record chunk followed by zero or more *middle* record chunks and finally terminated by a *terminating* chunk record [7].

The initial record chunk has its *CF* flag set. The *Type* field and the *ID* field (if present) indicate the type and ID of the entire payload respectively. The *payload-length* field indicates the size of payload of the initial record only.

The *middle* and *terminating* record chunks do not have *Type* and *ID* fields as these are already indicated in the *initial* chunk. Their *TNF* field value is 6, indicating that the *Type* and *ID* are the same as for the *initial* record chunk. Their *Type-length* and *ID-length* fields are zero. The *CF* is set for middle chunks and is clear for the terminating chunk.

IV. THE SIGNATURE RECORD TYPE DEFINITION

The Signature Record Type Definition specifies the format used when signing single or multiple NDEF records [1]. It defines a list of suitable algorithms and certificate types that can be used to create the signature. It provides users with the possibility of verifying the authenticity and integrity of the data within the NDEF message.

A. The Signature Record

The contents of the payload of a signature record consists of three parts: *Version*, *digital signature* and *certificate chain* as shown in Figure 2. The *Version* is a single byte field indicating the version of the specification to which a signature is compliant. Currently the only valid version is 1. The *signature* field contains either the actual signature or a URI

reference to a signature. The signature RTD supports RSA, DSA and ECDSA. The *certificate chain* contains the certificate format, the total number of certificates, the list of certificates and an optional URI reference.

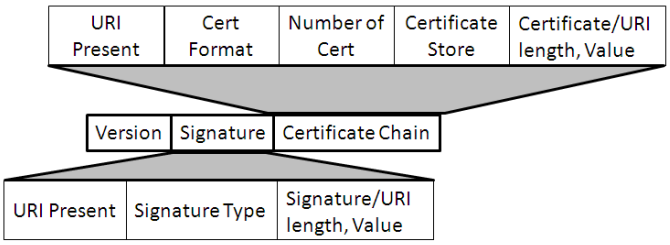

Fig. 2. Payload of an NDEF signature record, based on [2], fig. 2

B. Use of the Signature Record in an NDEF Message

The signature record applies to all preceding records, starting either from the first record of an NDEF message or from the first record following the preceding signature record as shown in Figure 3. The signature is applied to the Type, ID (if present) and payload of these records. The NDEF header and length fields are not signed as shown in Table II.

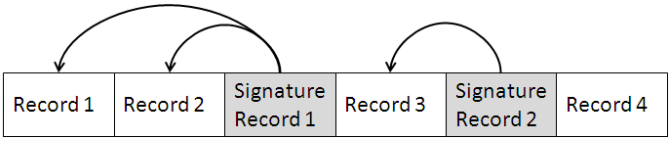

Fig. 3. An NDEF message consisting of multiple records. Signature Record 1 signs Records 1 and 2. It also marks the start of the signature of Record 3. Signature Record 2 signs Record 3 only whereas Record 4 has no signature [2], fig. 3.

TABLE II
SIGNING AN NDEF RECORD [1], §3.4

Field Name	Signed/Unsigned
Message Begin *(MB)*	Not signed
Message End *(ME)*	Not signed
Chunk Flag *(CF)*	Not signed
Short Record *(SR)* Flag	Not signed
ID-Length *(IL)* Present Flag	Not signed
Type Name Format *(TNF)*	Not signed
Type-Length	Not signed
Payload-Length	Not signed
ID-Length	Not signed
Type	Signed
ID	Signed
Payload	Signed

V. RELATED WORK

Haselsteiner [8] discovered that the transmission between the tag and the reader can be modified by an attacker. He pointed out that all the transmitted bits can be modified if Manchester coding with 10% ASK is used whereas, for Miller encoding with 100% ASK, this attack is feasible for certain bits but impossible for others. A strong synchronization is required between the attacker's device and legitimate devices to implement this attack, making it less than practicable. Madlmayr [4] indicates that the NDEF data is prone to various attacks if proper protection is not used. Roland [9] carried out an analysis regarding signing an NDEF message. He provides the justification for signing a few selected fields of an NDEF mesage. Roland in [2], exploits some vulnerabilities of the Signature RTD. Mulliner [3] exploits the size of the display screen to launch some attacks on the smart poster.

VI. THE RECORD COMPOSITION ATTACK

The Record Composition Attack is aimed at composing different records in such a way that the digital signature remains valid. There are two scenarios described by M. Roland to accomplish this attack [2] .

In the first scenario, two different smart posters are selected in which every record has its own signature. A malicious smart poster record can be created by selecting only a few of the records along with their signatures from first poster and other records along with their signatures from the second poster. Similarly, many records along with their respective signatures can be combined together in a single NDEF message. The combined NDEF message will consist of a sequence of records that may be totally meaningless, but still have valid signatures.

In the second scenario, the Record Composition Attack is accomplished by combining and hiding selected records from different NDEF messages. An adversary takes two smart posters records signed by the same parties or two different parties A and B. Each smart poster consists of records of various types like *Text, URI* etc. followed by the signature. The attacker takes all records from both posters and combines them to form a new smart poster record. The new poster will have two valid signature records corresponding to data from each parent tag. The attacker then effectively removes the unwanted records from the message but keeps the signatures valid. As all the records are digitally signed, the actual removal of any record invalidates the signature. Instead the chosen records are retained but hidden from the user as follows.

To hide records, the *TNF* field is exploited. The TNF value is changed from 1 to 5, i.e. from the NFC Forum *well-know*n Type to an *Unknown* Type. The *TNF* value can be changed as this value is not signed. The NDEF parser receiving an NDEF record with a *TNF* value of *Unknown* will store the payload of that record without processing it. In this case the payload will not appear to the user. So, rather than removing a record, it has been hidden simply by changing the *TNF* value.

VII. THE NEW AMENDED ATTACK

In fact, Roland's attack [2] described thus far does not necessarily work because there are few other changes that may have to be carried out in order to keep the signature valid. These necessary modifications were overlooked in [2].

For *TNF=5*, the *Type-Length* field must be zero and there is no *Type* Field (see Table I). This is not the case when the TNF value is 1. As the *Type-Length* field is not signed it

can indeed be changed to zero, but the *Type* and *ID* fields are digitally signed and omitting or altering these fields to maintain a meaningful payload may invalidate the signature. Specifically, the signature on $Type||ID||Payload$ has become a signature on $ID'||Payload'$, which is the same string but now interpreted with a different, possibly invalid ID' and a new, probably meaningless, message $Payload'$. Quite apart from the semantic issues, the signature verification now fails unless *Type-Length* = 0 because it is now performed on a string of only (*ID-Length*)+(*Payload-Length*) bytes, which is *Type-Length* bytes shorter than the string from which the presented signature was calculated.

Therefore, apart from only changing the *TNF* value, some manipulation in the NDEF header is also required to keep the signature valid. This manipulation can be achieved by considering separately the two cases determined by the value of the *IL* flag. These are presented next.

A. When the ID Field is present

Presence of the *ID* field is indicated by the *IL* flag. If set, the *ID-Length* field is present in the header along with the *ID* field. Otherwise, both, the *ID-Length* and the *ID* fields are omitted. The following procedure is to be followed in order to hide records with *ID* flag set but keeping its signature valid.

- Step I: Change the *IL* Flag to zero. This step is done so that the new tag record should not have an *ID* field. Since the *IL* flag is not signed, it can be easily changed.
- Step II: Change the *TNF* value from 1 to 5, so the record type in the new tag is now *Unknown*.
- Step III: Change the *Type-Length* field to 0. This field is also not signed and can be changed.
- Step IV: Increment the *Payload-Length* field by the values of the *Type-Length* and *ID-Length* fields in the original tag. For example, if the value of *Type-Length* field is 2 and of *ID-length* is 2, then the *Payload-Length* field is incremented by 4. As the *Payload-Length* field is also not signed, it can be modified in this way.
- Step V: Remove the data of *ID-Length* as IL flag is zero.
- Step VI: Concatenate the *Type*, *ID* and *payload* fields to form the payload of the new record.

The new record formed in this way will not appear to the user, however the signature will remain valid. This procedure is illustrated in Figure 4.

B. When the ID Field is not present

When *ID* is not present, the *IL* flag is zero and the *ID-Length* field is omitted. The following procedure is to be followed in order to hide the record but keep the signature valid (*see* Figure 5, *cf* [9] §V(L)).

- Step I: Change *TNF* value from 1 to 5.
- Step II: Change the *Type-Length* field to 0. This field is not signed.
- Step III: Increment the *Payload-Length* field by the value of the *Type-Length* field.
- Step IV: Concatenate the *Type* and *payload* fields to form the payload of the new record.

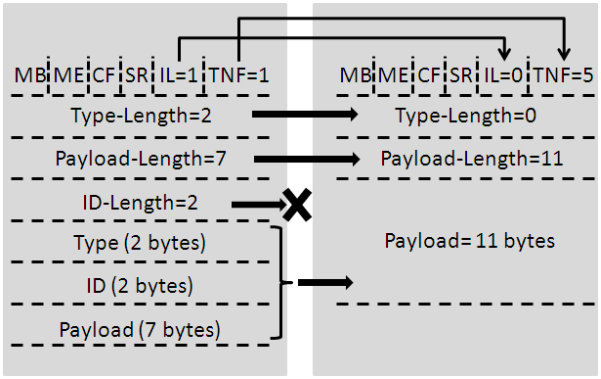

Fig. 4. Changes in the NDEF header when the *ID* field is present. The values are only for demonstration purposes.

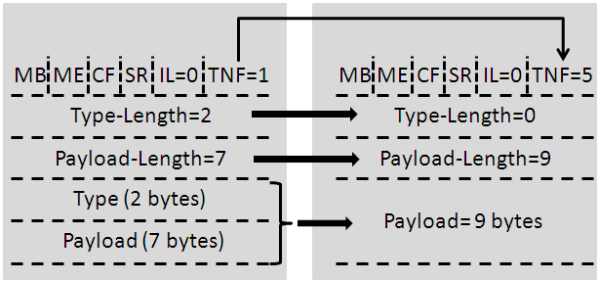

Fig. 5. Changes in the NDEF header when the *ID* field is not present. The values are only for demonstration purposes.

VIII. The Record Decomposition Attack

In this attack described by Roland *et al.* in [2], part of the payload is chopped off by changing the *Payload-Length* field. The trimmed part can then be hidden in a new record of *Unknown* type. An example of such attack is the text of a smart poster stating: *"Do not board the train until you have a valid ticket"*. This text is digitally signed and the signature is stored in Signature RTD. An attacker may split this message into two separate records. The first record stating *"Do not board the train"* will be visible to the user, whereas the second record stating *"until you have a valid ticket"* will not appear to the user as it is of unknown type. However, the digital signature will remain valid and the user will consider it as a valid message. This attack works in its original form without further modification of length fields such as those described in the previous section.

IX. Countermeasures

Roland proposed that the receiver should only trust the relationship of records if they are signed and if they share a common signature record [2]. But, as shown in the example of the Record Decomposition Attack in §VIII, the records share a common signature but only a part of the message is displayed to the user. This partially displayed message with a valid signature cannot be trusted. Hence, records sharing a common signature also cannot be trusted.

The easiest way to avoid these attacks is to sign all the header fields so that they may not be altered, but practically

this is not possible. The *MB* flag is not signed so that a group of signed NDEF records may be moved to any position within an NDEF message [9]. It is unnecessary to sign the *ME* flag: as for any signed record, the ME flag is always clear because the signed record will always be followed by the signature record.

The main reason to sign only the *Type*, *ID* and *Payload* is the desire to be able to partition an NDEF record into multiple record chunks or *vice versa* but keep the signature valid as shown in Figure 6. The inclusion of any other field, such as length fields, *TNF* or *CF* in the signature will make this process invalid.

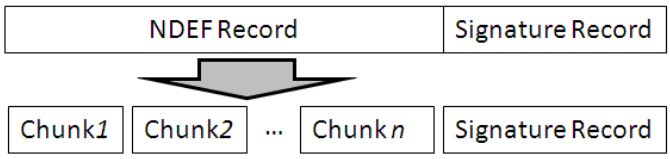

Fig. 6. An NDEF record appended with its digital signature is partitioned into multiple chunk records. The signature is valid for both cases.

We propose that the specification given for the chunk records by NFC Forum (Section 2.3.3 of [7]) be revised. There is some redundant data in the *middle* and *terminating* chunk records. The *middle* and *terminating* record chunks have *TNF*=6, indicating that the *Type* and *ID* of these records are unchanged. Therefore, the *Type-Length* and *ID-length* fields are set to zero and the *Type* and *ID* fields are omitted, as explained in §III-B.

Since the *Type-Length* field and *ID-length* field are redundant in the *middle* and *terminating* record chunks, TNF=6 indicates that these two fields can actually be *omitted* from the *middle* and *terminating* chunks. The new proposed construction of a record chunk is presented in Table III.

TABLE III
PROPOSED CONSTRUCTION OF CHUNK RECORDS WITH *IL* FLAG SET. *MB*, *ME* AND *SR* FLAGS ARE NOT SHOWN AS THEY ARE USED AS REQUIRED.

Field Name	Initial Chunk	Middle Chunks	Terminating Chunk
CF	1	1	0
TNF	Any	6	6
Type-Length	Present	–	–
Payload-Length	Present	Present	Present
ID-Length	Present	–	–
Type	Present	–	–
ID	Present	–	–
Payload	Present	Present	Present

After the modifications in the record chunk structure, we propose that the signature should be computed over the *Type-Length*, *ID-Length*, *Type*, *ID* and *payload* fields.

X. Analysis of the Attack on the Modified NDEF Record Structure

The revision to the NDEF specification of the record chunks results in a reduction of two bytes for each chunk. Apart from the slightly reduced overhead for space and signature computation, the amended Record Composition and Record Decomposition Attacks cannot be implemented on the proposed scheme as the *Type-Length* and the *ID-Length* fields are now digitally signed.

The proposed signature scheme can be successfully used with record chunks. As the *middle* and the *terminating* chunks do not have *Type-Length* and the *ID-Length* fields the signature is valid for both the parent record and the chunks records, as in Fig. 6. Therefore, a record may be partitioned into multiple chunks or *vise versa* without affecting the validity of the signature. Furthermore, although the CF flag is unsigned, altering it maliciously causes extra header fields to be included or excluded in the signature, thereby invalidating the signature.

XI. Conclusion

The Record Composition/Decomposition Attacks exploit unsigned fields in the NDEF header. Previously proposed attacks were not fully implementable without further modifications to these header fields. We refined those attacks and explained precisely what additional changes need to be made to exploit the unsigned fields. Such attacks can be countered if the length fields of the NDEF header are also signed. However, the process of record chunking requires the length fields to remain unsigned. We propose a solution that requires few, very mild modifications to the NDEF technical specification related to record chunks. These modifications not only reduce the computational and space overhead of the record chunks, but also make it possible to sign the length fields of the NDEF header. For the revised definition, we propose a related modification to the Signature RTD in which the *Type-Length* and *ID-Length* fields are included. This makes it more difficult to exploit the NDEF header in signature attacks, thus successfully countering Record Composition/Decomposition Attacks.

References

[1] NFC Forum, "Signature Record Type Definition: Technical Specification," http://www.nfc-forum.org/specs/spec_list/.
[2] M. Roland, J. Langer, and J. Scharinger, "Security Vulnerabilities of the NDEF Signature Record Type," *Near Field Communication, International Workshop on*, pp. 65–70, 2011.
[3] C. Mulliner, "Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones," in *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, March 2009, pp. 695–700.
[4] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC Devices: Security and Privacy," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, March 2008, pp. 642–647.
[5] NFC Forum, "NFC Forum Home Page," http://www.nfc-forum.org/home/.
[6] ——, "Smart Poster Record Type Definition: Technical Specification," http://www.nfc-forum.org/specs/spec_list/.
[7] ——, "NFC Data Exchange Format (NDEF): Technical Specification," http://www.nfc-forum.org/specs/spec_list/.
[8] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC): Strengths and Weaknesses," *Workshop on RFID Security, RFIDSec 06*, 2006.
[9] M. Roland and J. Langer, "Digital Signature Records for the NFC Data Exchange Format," *Near Field Communication, International Workshop on*, pp. 71–76, 2010.