안전한 NDEF 메시지 전송 기법에 관한 연구

박성욱, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail : swpark@sch.ac.kr, imylee@sch.ac.kr

A Study on Secure Transmission Scheme of NDEF Message

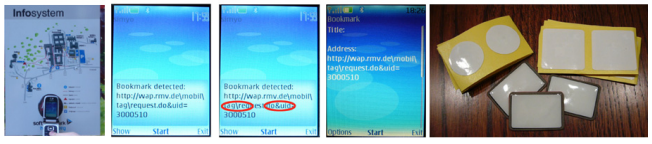
Sung-Wook Park, Im-Yeong Lee
Dept of Computer Software Engineering, Soonchunhyang University

요 약

최근 NFC가 탑재된 모바일 기기는 결제, 할인쿠폰, 사용자 인증 등 각종 기능을 제공하는 수단으로 활용되면서 NFC 모바일 서비스 시장이 급성장할 것으로 전망되고 있다. 하지만 현재 NFC 기반의 다양한 서비스들은 관련 보안 기술 및 연구가 부족한 실정이다. 그럼에도 불구하고 다양한 NFC 비즈니스 모델을 통한 이윤 창출에 바쁜 국내 업체들은 검증되지 않은 다양한 서비스들을 내놓으며 서비스 활성화에 열을 올리고 있다. 이에 따라 NFC 기반 서비스의 사용이 증가하는 만큼 다양한 보안상 위협요소에 대처하기 힘들 것으로 예상된다. 특히 NFC 간 통신을 위해 사용되는 NDEF 메시지는 이미 그 취약성이 드러나 최초 NDEF 메시지 전송 단계에서 데이터의 위·변조된 이루어지기 때문에 네트워크 통신 단계와 물리적 공간에 보안기술을 적용해 둔다 하더라고 원천적인 문제점의 해결책이 될 수 없다. 따라서 본 논문에서는 NDEF 메시지 상에서의 보안 위협에 대해 분석하고 표준 기술 구조를 고려하여 NDEF 레코드간의 조합을 통한 안전한 NDEF 메시지 전송 기법에 대해 제안한다.

1. 서론

NFC(Near Field Communication)는 13.56MHz대역의 Short range high frequency를 이용한 RFID(Radio Frequency Identification)의 하나로 스마트폰과의 융합을 통해 단말 간 read/write가 가능한 양방향 데이터통신을 제공한다. 또한 RFID와의 상호 호환성을 제공하며 암호화 표준(NFC-SEC)의 적용으로 데이터 통신간의 안전성을 제공하는 등의 장점들로 인해 새로운 응용비즈니스 모델 적용이 가능할 것으로 분석되고 있다. 그러나 이미 오래전부터 NFC 태그가 보안상 많은 취약점을 가지고 있다는 것이 밝혀진바 있다[1,2]. (그림 1)과 같이 메타정보를 사용자가 가시적으로 판단하여 결정을 내리는 부분에 대한 취약점이 존재하며 결제 수행 시 사용되는 태그의 신뢰성이 제공되지 않는다. 이에 따라 표준에서는 전자 서명을 NDEF 메시지와 조합하여 신뢰성을 제공하려 했지만 Record Composition 및 Record Hiding과 같은 공격에 의해 취약점이 드러났다. 이후 이러한 문제점을 해결하기 위해 NDEF 메시지의 서명 범위를 넓히는 등의 다양한 방법들이 제안되었지만 이전 버전 NDEF 메시지와의 하위 호환성에 대한 문제점으로 인해 아직까지 그 문제가 고려되고 있다[3]. 따라서 본 논문에서는 표준 스펙의 물리적인 변화 없이 NDEF 레코드 간의 메시지 조합을 통한 안전한 NDEF 메시지 전송 기법에 대해 제안하였다.



(그림 1) NDEF 메시지 변조 공격 사례

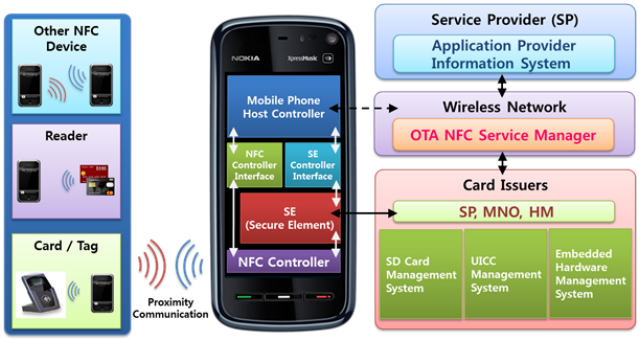
본 논문의 구성은 다음과 같다. 2장에서는 NDEF 메시지 변조가 NFC Mobile Architecture에 어떠한 영향을 미치는지 알아보고 NDEF 구조에 대해 분석한다. 3장에서는 NDEF 메시지에 무결성과 신뢰성을 제공하기 위한 Signature RTD의 보안상 취약성에 대해 분석하고, 4장에서는 보안 취약성을 해결하는 제안방식을 기술하며, 5장에서는 기존 기술과 제안방식을 비교 분석한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련연구

본 장에서는 NFC 모바일 아키텍처 상에서 발생할 수 있는 보안상의 위협을 분석하고 NDEF와 Signatre RTD, 그리고 “서명된 스마트 포스터” 구조에 대해 설명한다.

2.1 NFC Mobile Architecture

(그림 2)는 NFC 모바일을 이용한 서비스에서 활용되는 일반적인 아키텍처이다. 이 아키텍처는 대부분의 NFC 모바일 기반 비즈니스 모델에 적용이 가능하다. NFC 개체간의 Proximity Communication이 이루어질 때 NFC-SEC



(그림 2) NFC Mobile Architecture

에 의해 ECC기반의 키 교환 및 데이터 전송이 수행되며 (개체 인증이 이루어지지 않아 신뢰성을 제공할 수 없지만 본 논문의 범위에 해당하지 않으므로 더 이상 언급하지 않음), OTA 상에서 이루어지는 통신 역시 해당하는 프로세스에 따라 Secure Channel에서 안전한 데이터 교환이 이루어진다. 이후 각각의 무선통신(Proximity, OTA)에 의해 교환된 데이터는 NFC Controller와 Mobile Host Controller, SE Controller에 의해 SE(Secure Element)영역에 저장되어 안전하게 관리된다. 하지만 이러한 안전성은 기존에 정의된 NFC Controller의 안전성이 확보되었을 때의 상황이다. 이후 언급될 NDEF의 취약점이 보완되지 않는다면 SE영역과 NFC-SEC의 안전성을 확신할 수 없게 된다.

2.2 NDEF

NDEF(NFC Data Exchange Format)는 NFC 포럼에 의해 태그 또는 NFC 기반 디바이스 사이의 데이터 전송 시 상호 호환성 제공을 위해 정의된 메시지 구조이다[4,5]. NDEF 메시지는 하나 이상의 NDEF 레코드들을 가지며 임의의 타입의 페이로드를 전송하는데 목적이 있다.

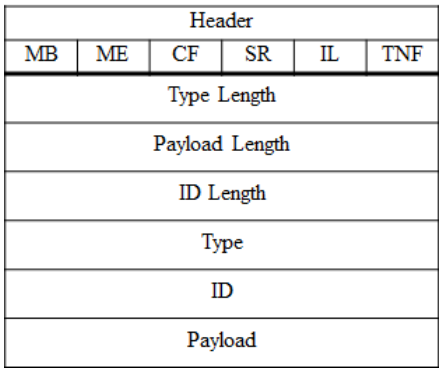
<표 1>은 NDEF 레코드의 일반적인 구성을 나타내며 <표 2>는 레코드 헤더에 들어간 정보를 나타낸다.

항목	설명
Header	레코드에 대한 기본적인 정보
Type Length	데이터 타입의 길이
Payload Length	페이로드의 길이
ID Length	ID의 길이
Type	레코드가 담고 있는 페이로드의 타입
ID	페이로드 ID
Payload	레코드가 담고 있는 페이로드

<표 1> NDEF 레코드의 구성

헤더 항목	설명
MB(Message Begin)	메시지의 시작을 나타냄
ME(Message End)	메시지의 끝을 나타냄
CF(Chunk Flag)	레코드 중간 여부를 구분
SR(Short Record)	설정유무에 따라 필드가 1옥텟 또는 4옥텟으로 결정
IL(ID Length)	레코드 ID 존재 유무
TNF(Type Name Format)	Type 필드 값의 구조 명시

<표 2> NDEF 레코드 헤더 정보



(그림 3) NDEF 레코드 형식

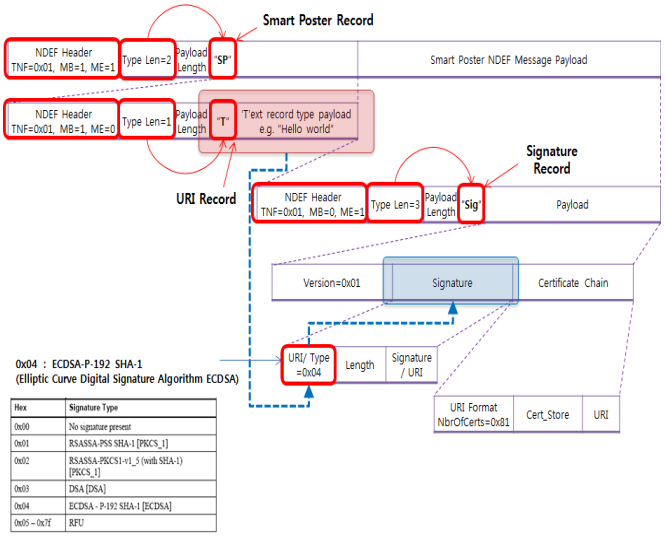
2.3 Signature Record Type Definition

Signature RTD(Record Type Definition)은 NFC 포럼에 의해 처음 발표되었다. Signature RTD는 NDEF(NFC Data Exchange Format) 메시지에 디지털 서명과 인증서를 추가하여 NDEF의 무결성과 신뢰성을 제공한다[6].

Signature Record의 페이로드 내용은 Version, Signature, Certificate Chain 세 부분으로 구성된다. Version Field는 서명이 준수하는 사양의 버전을 나타내는 단일 바이트 필드로써 현재 유효한 버전은 한 가지만이 존재한다. Signature Field는 실제 서명 또는 서명에 대한 URI(Uniform Resource Identifier) 참조 중 하나를 포함한다. Certificate Chain Field는 인증서 포맷, 인증서의 총 개수, 인증서의 목록과 URL 참조(선택적)를 포함하고 있다.

2.4 Simple Signed Smart Poster

하나의 스마트 포스터 레코드에는 Text 레코드와 이를 서명한 Signature 레코드가 존재한다. (그림 4)은 NFC 태그로부터 단순히 특정 텍스트 기반의 메시지와 메시지의 대한 서명 정보만을 불러오는 예제이다. Text 레코드는 Signature Type에 따라 SHA-1, DSA, ECDSA 등과 같은 표준 기술을 선택하여 서명하는 것이 가능하다.



(그림 4) Simple Signed Smart Poster

3. Signature RTD의 보안상 취약점

3.1 Record Composition Attack

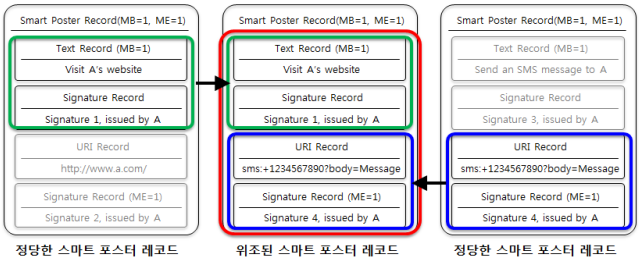
NDEF 표준 문서에 따르면 Signature RTD는 단지 NDEF 레코드의 Type, ID, Payload 필드만이 서명되는 것을 정의하고 있다. 다시 말해서 이것은 나머지 필드들(Length Field, Header Field, Byte Field)이 서명에 의해 보호되지 않음을 뜻한다. 따라서 (그림 5)과 같이 정당한 두 개의 스마트 포스터 A와 B로부터 A의 Text 레코드와 이에 해당하는 서명 레코드 그리고 B의 URI 레코드와 이에 해당하는 서명 레코드를 추출하여 또 하나의 위조된 스마트 포스터를 만드는 것이 가능하다[7,8].

3.2 Record Hiding & Composition Attack

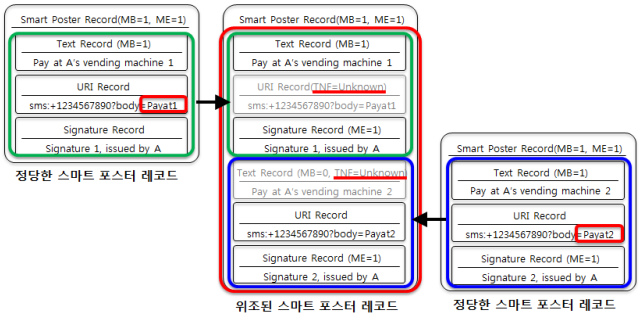
Record Hiding 공격은 NDEF Layout 내에 TNF 필드를 0x05(Unknown)으로 설정함으로써 발생될 수 있다. Unknown TNF에 대해 NFC 포럼에서 발표한 NDEF Technical Specification에서는 "NDEF 레코드 수신 시 NDEF 파서가 저장 메커니즘을 제공하지만 페이로드는 프로세싱하지 않는 것을 권장한다"고 정의하고 있다[4]. 따라서 NDEF 레코드를 수신하는 모바일은 이러한 레코드를 프로세싱하지 않게 되고 이를 통해 공격자는 서명된 NDEF 메시지로부터 선택적으로 레코드를 감출 수 있다. 이러한 Record Hiding 공격과 Composition 공격을 연계하여 공격자는 서명된 두 개의 스마트 포스터를 이용하여 다음과 같은 공격이 가능하다[7,8].

1. 정당한 스마트 포스터 A의 레코드를 TNF 필드의 Unknown 설정을 통해 URI 레코드(결제 또는 URL연결 정보) 부분을 감춘다.
2. 정당한 스마트 포스터 B의 레코드를 숨 필드의 Unknown 설정을 통해 사용자가 가시적으로 감지할 수 있는 Text 레코드 부분을 감춘다.
3. 정당한 스마트 포스터 A와 B의 데이터를 합쳐 또 하나의 새로운 스마트 포스터 C를 생성한다.
4. 사용자가 가시적으로 판단할 수 있는 정보는 스마트 포스터 A의 Text 레코드 정보이며 실제 연결되는 URI 레코드 정보는 스마트 포스터 B의 URI 레코드이다.

스마트 포스터 이용 시 위와 같은 공격을 통해 사용자에게 가시적으로 보여지는 부분은 "무료 결제 정보" 또는



(그림 5) Record Composition Attack



(그림 6) Record Hiding & Composition Attack

"정당한 웹사이트 정보"이지만 실제 연결되는 정보는 "유료 결제 정보" 또는 공격자의 웹사이트"이다.

4. 제안방식

이 장에서는 3장의 보안위협을 해결하는 연관 레코드 조합 서명 기법을 제안한다. 본 제안방식에서는 서명 생성 단계와 서명 검증단계로 구성되며 각 단계의 수행절차는 다음과 같다.

4.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템계수를 사용하여 프로토콜을 설계한다.

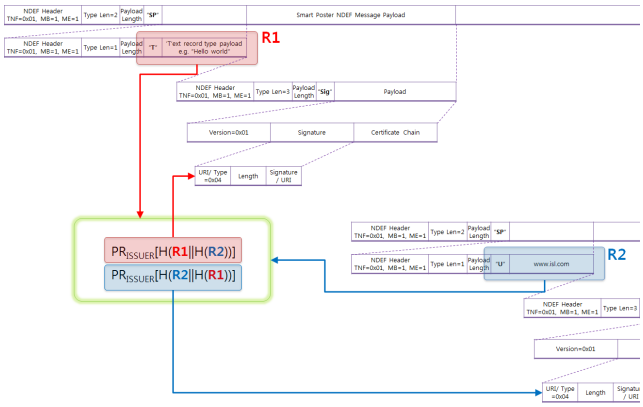
- $*$: 각각의 개체 (C : *Client*, I : *Issuer*)
- *Client* : 스마트 포스터를 이용하는 모바일 사용자
- *Issuer* : 스마트 포스터
- $R1$: 사용자에게 가시적으로 표시되는 레코드
- $R2$: 결제 또는 URL연결을 수행하는 레코드
- PR_* : Signature RTD에 정의된 서명 개인키
- PU_* : Signature RTD에 정의된 서명 공개키
- $H()$: 암호학적 해시 함수

4.2 연관 레코드 조합 서명 생성

Step 1: 스마트 포스터의 생성에 필요한 데이터 레코드 $R1$과 $R2$에 대해 아래와 같은 형태의 서명을 수행한다.

$$Issuer: PR_{Issuer}[H(R1 \| H(R2))]$$

$$Issuer: PR_{Issuer}[H(R2 \| H(R1))]$$



(그림 7) 제안된 서명 생성 방식

Step 2: 생성된 서명을 각 레코드와 연관된 서명 레코드에 삽입한 후 *Client*가 요청 시 해당 정보를 전송한다.

$$Issuer: PR_{issuer}[H(R1\|H(R2))] \rightarrow Signature\ Field$$
$$Issuer: PR_{issuer}[H(R2\|H(R1))] \rightarrow Signature\ Field$$

4.3 연관 레코드 조합 서명 검증

Step 1: *Client*는 수신된 메시지로부터 *Issuer*의 공개키 PU_{Issuer}를 이용하여 각각의 데이터 레코드의 해당하는 서명 레코드를 복호한다.

$$Client: PU_{Issuer}[PR_{Issuer}[H(R1\|H(R2))]]$$
$$Client: PU_{Issuer}[PR_{Issuer}[H(R1\|H(R2))]]$$

Step 2: *Client*는 각 데이터 레코드 $R1$과 $R2$의 해쉬 값 $H(R1')$과 $H(R2')$를 생성하여 아래와 같이 무결성 검사를 수행한다.

$$Client: H(R1\|H(R2)) = H(R1'\|H(R2'))$$
$$Client: H(R2\|H(R1)) = H(R2'\|H(R1'))$$

위 과정을 통해서 각 데이터 레코드에 대한 무결성과 연관된 데이터 레코드 간의 무결성을 동시 검증하는 것이 가능하다.

5. 제안방식분석

본 제안방식은 3장에서 도출된 보안 위협에 대해 다음과 같이 만족한다.

· Record Composition 공격 : 두 개의 연관레코드에 따른 서명 검증이 이루어지므로 안전성을 제공한다.
· Record Hiding 공격 : Record 값이 숨겨질 경우 초기에 생성한 해쉬 값과 일치하지 않으므로 두 개의 연관 레코드 해시 값 검증을 통해 안전성을 제공할 수 있다.
· Record Hiding & Composition 공격 : 두 방식을 연계한 공격이라도 제안된 방식은 필드를 구별하지 않고 페이로드 전체의 값을 검증하는 방식이므로 안전하다.

구분		기존방식	제안방식
메시지 변조	Record Composition	X	O
	Record Hiding	X	O
	Record Hiding & Composition	X	O

<표 3> NDEF 레코드의 구성

6. 결론

본 제안은 기존 NDEF 메시지 취약점에 대한 문제점을 해결하며 위조된 NFC 태그로부터 사용자를 보호한다. 또한 물리적인 변화 없이 기존 기종의 하위 호환성을 유지하며 제안 방식을 적용하는 것이 가능하다. 가령, 사용자가 NFC 서비스 이용 시 응용 소프트웨어를 통해서 제안된 기법이 적용되었는지의 여부를 판별하여 적용되어 있지 않는 태그에 대해 업데이트를 실시할 경우 별도의 추가 비용 없이 유지보수가 가능하다. 하지만 본 제안은 앞서 언급한 위협에 대해 취약점을 해결하는 것만 고려되었을 뿐 효율성 측면이 충분히 고려되지 못했으므로 추가적인 연구가 필요할 것으로 사료되며, 향후 구현을 통한 검증이 이루어져야할 것으로 판단된다.

참고문헌

[1] Collin Mulliner, "Attacking NFC Mobile Phones", EUSecWest 2008, 2008
[2] Collin Mulliner, "Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones", 2009 International Conference on Availability, Reliability and Security, 2009
[3] 한국인터넷진흥원, "NFC 개인정보보호 대책", 2011.1
[4] NFC Forum, "NFC Data Exchange Format(NDEF) Technical Specification", 2006.7
[5] Michael Roland, Josef Langer, "Digital Signature Records for NFC Data Exchange Format", Second International Workshop on Near Field Communication, 2010.10
[6] NFC Forum, "Signature Record Type Definition Technical Specification", 2010.11
[7] Michael Roland, Josef Langer, Josef Scharinger, "Security Vulnerabilities of the NDEF Signature Record Type", 2011 Third International Workshop on Near Field Communication, 2011.0
[8] Michael Roland, "Security & Privacy Issues of the Signature RTD", NFC Forum Member Meeting, 2012.02