NFC 보안 구조 및 취약성 분석*

전호성, 이옥연
국민대학교 수학과
e-mail:hsjeon@kookmin.ac.kr, oyyi@kookmin.ac.kr

NFC security architecture and vulnerability analysis

HoSung Jeon, Okyeon Yi
Department of Mathematics, Kookmin University

요 약

NFC(Near Field Communication) 기술은 근거리 무선통신 기술로서 다양한 모드에서의 서비스를 지원한다. 결제, 할인쿠폰 등 각종 기능을 제공하는 수단으로서 통신과 금융이 융합된 모바일 NFC 서비스의 시장이 급성장 할 것으로 전망되고 있다. 그 결과로 NFC Forum, ECMA International 등 관련 단체에서는 모바일 NFC 서비스를 이루는 각 구성요소의 역할, 기능, 보안 요구사항 등을 제시하며 보안의 중요성을 강조하였다. 본 논문에서는 NFC기술과 보안요소(Security Element)에 대해 소개를 하고, 보안 위협과 그에 대한 대응방안에 대해 소개한다.

1. 서론

최근 무선 네트워크 기술들의 비약적인 발전으로 통신, 금융 등 다양한 응용 서비스들에 활발하게 적용되고 있다. 각 무선 네트워크 기술들의 특징에 따라 UMTS, WiBro 같은 광대역 이동통신 망 서비스, 로컬영역에서의 무선 네트워크 서비스인 무선랜 서비스뿐만 아니라 근거리 통신인 UWB (Ultra-wideband), Bluetooth, ZigBee 기술에 적합한 응용 서비스들이 모색되고 있다. 이러한 무선 네트워크 기술 가운데 근거리 무선통신기술인 NFC(Near Field Communication)가 주목 받고 있다. 최근 스마트 장치는 결제, 할인쿠폰 등 각종 기능을 제공하는 수단으로 진화하면서 통신과 금융이 융합된 모바일 NFC 서비스의 시장이 급성장할 것으로 전망되고 있는데 지불, 마케팅, 고객관리, 티켓팅과 같은 다양한 응용서비스에 적용 가능한 잠재력을 가지고 있다. 특히 모바일 NFC 결제 서비스 시장의 활성화가 예상됨에 따라 모바일 NFC 결제 서비스는 국내·외로 널리 주목받고 있다. NFC 기술은 모바일장치, 특히 스마트폰과의 융합을 통해 단말 간 데이터 통신을 제공할 수 있을 뿐만 아니라 기존의 비접촉식 스마트카드 기술 및 무선인식기술(RFID)과의 상호호환성을 제공한다. 하지만 이를 주도할 수 있는 보안 관련 기술력이 아직 미미한 상태이다. NFC결제 서비스의 활성화에 의해 고객정보 이외의 금융 정보까지 확대되어 관리될 가능성이 내재됨에 따라 보안에 대한 관심도는 더욱 고조되고 있다. 이에 NFC 결제 서비스의 보안 위협을 사전에 분석하여 안전한 서비스를 위한 대응책을 형성해야 한다.

* 본 연구는 국토해양부 첨단도시개발사업의 연구비지원(07첨단도시 A01)에 의해 수행되었습니다.
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No.2011-0029927).

2. NFC

수년 전부터 차세대 모바일지급결제서비스의 핵심 기술로서 주목받아 왔던 NFC는 13.56MHz 주파수 대역에서 10cm 내외의 근거리에 있는 두 매체가 비접촉으로 상호통신할 수 있는 근거리무선통신 규격이다. NFC는 13.56MHz 대역 비접촉식 근거리 무선통신기술을 의미하는 용어로 NFC 기술은 ECMA, ISO, ETSI에서 표준을 진행하고 있다. 특히, ECMA-340(NFCIP-1)과 ECMA-352(NFCIP-2) 표준을 중심으로 NFC 기술에 대해 정의하고 있다. 사실 NFC는 국내에서 이미 활성화되어 있는 ISO14443 기반의 스마트카드 비접촉무선결제와 비교할 때 서비스 프로세스 측면에서 차이점이 거의 없다고 볼 수 있다. 다만, 수동형(passive) 모드로 작동되는 ISO 14443 규격과는 달리 능동형(active) 모드로도 작동할 수 있어 태그로서의 역할 뿐 아니라 태그를 읽는 리더(reader), 태그를 입력하는 라이터(writer) 기능으로 활용될 수 있으며, P2P 또한 가능하다는 점에서 서비스 활용 폭이 상당히 넓은 ISO 14443의 확장된 기술 규격이라 하겠다.

2.1 NFC 운영모드

NFC 기술은 다양한 근거리 무선 통신들의 다양한 성질들을 결합하여 다음과 같이 세 가지 모드로 작동 가능하

다. 이 모드들은 각각 RFID와 같이 데이터를 읽고 수정할 수 있는 모드, 블루투스 등과 연결하여 데이터 통신 서비스 가능 모드, 카드에 탑재되어 비접촉식 카드의 성질을 지원하면서 스마트카드의 안전성을 기반으로 하는 안전한 서비스들이 지원 가능하다. RF를 이용한다는 점에서 NFC는 RFID의 한 범주가 될 수 있으며, 가장 큰 차이점은 P2P 모드의 통신이 가능하다는 점이다.

2.1.1 Reader/Writer 모드

NFC 디바이스는 NFC 트랜스폰더에 저장된 데이터를 일고 수정할 수 있다. 사용자는 NFC 디바이스가 NFC 태그를 읽어 추가정보를 조회할 수 있는 기술이다. 정보가 저장되어 있는 태그에서 NFC 디바이스를 터치하면 그 정보를 읽고 정보의 접근을 지원한다.

2.1.2 Card Emulation 모드

NFC 디바이스가 스마트카드(ISO 14443)처럼 작동하는 모드이기 때문에 외부 NFC 리더기는 스마트카드와 NFC 디바이스를 구분할 수 없다. 하지만 외부의 리더와 데이터를 교환할 수 있다. 이 모드에서는 비접촉식 지불, 티켓팅 서비스가 가능하다.

2.1.3 P2P 모드

P2P 모드는 두 개의 NFC 디바이간의 링크 수준의 통신을 지원한다. 블루투스 페어링 절차를 NFC 통신으로 대체하여 연결하는 모드이다. 연결을 위해 NFC 디바이스는 NFC 타겟을 검색하고 NDEF(NFC Data Exchange Format) 메시지 형식을 통해 데이터를 전송한다.

2.2 NFC 응용 서비스

NFC 기술은 대표적인 비접촉식 근거리 무선기술을 모두 포괄함으로써 출입통제, 가전, 체크인 시스템, 헬스케어, 정보수집, 쿠폰, 결제, 교통 등 실생활과 연계된 다양한 분야에 활용될 수 있다. 이에 대한 방법으로 모든 타입의 사용자 장치에 대해서 터치형식으로 직관적 연결이 가능하도록 했다. 직관적 연결은 사용자가 두 개의 NFC 장치들을 가까이 접촉함으로써 각 환경에서 필요한 정보를 전송하고 환경 설정 과정 동안 사용자 개입없이 상호작용이 가능하다. 이러한 편리성으로 인해 NFC 기술은 단순 콘텐츠 캡처, 태그를 가진 포스터로부터의 URL 주소 획득 및 연결 등과 같은 응용 서비스들이 고려되고 있다. 특히, 가상쿠폰 서비스, 포스터 광고 및 티켓 구매 서비스, 자판기 서비스와 같은 소액 결제 서비스에서부터 의료서비스까지 NFC 기술은 단순 태그 인식 서비스를 지원하는 RFID 기술보다는 보다 복잡하고 상호 데이터통신을 요구하는 응용 서비스들에 적용가능하다.

2.2.1 장치간 데이터 교환

스마트폰 간 데이터 전송, PC와 스마트폰 간 파일공유, 일반 가전제품과 스마트폰 간 정보 업데이트 등 NFC를 지원하는 모든 장치 사이의 직접적인 데이터 통신을 간단하게 한 번의 터치를 통해 처리할 수 있다. NFC는 와이파이나 블루투스 등 기존의 근거리 무선통신과는 달리 '터치'라는 직관적인 사용자 이용방식을 통해 구현되므로 매우 간편하게 데이터 통신을 연결할 수 있다.

2.2.2 서비스 발견 및 연결

RFID 태그가 부착되어 있는 스마트 포스터에 NFC 스마트폰을 터치하여 직접적인 정보획득을 할 뿐만 아니라 관련 웹사이트로의 연결까지 제공함으로써 새로운 서비스 연결이 가능해 진다. 또한 와이파이 간편 보안설정과 블루투스 장치가 간편 연결에도 NFC가 이미 사용되고 있다.

2.2.3 전자결제 및 티켓팅

NFC는 비접촉식 스마트카드 기술과 보안기술을 접목해 안전한 모바일 결제방식을 제공할 수 있으며, 교통카드와 할인쿠폰 등의 다양한 결제수단으로 활용할 수 있다. PC에서 NFC를 제공하는 경우 e-commerce의 인증방식 및 결제수단으로 NFC를 사용하면 매우 편리하다.

3. NFC 보안위협

NFC 기술적 취약점은 물리적 취약점과 NFC 응용계층에서의 논리적 취약점 등으로 구별된다. [표 1]은 NFC의 기술적 취약점을 정리한 것이다.

3.1 물리적 공격

3.1.1 도청

NFC는 다른 무선 통신과 마찬가지로 무선 통신의 특성상 도청 공격이 가능하다. 두 NFC 장치가 RF 신호를 사용해 데이터를 주고받을 때 공격자는 안테나를 사용하여 RF 신호를 도청할 수 있다. RF 신호의 강도와 퀄리티

[표 1] NFC 기술적 취약점

분류	취약점	대책
물리적	도청 (Eavesdrop)	보안채널 이용
	데이터 변조 (Data Corruption)	보안채널 이용 RF 필드 체크
	데이터 수정 (Data Modification)	보안채널 이용 RF 필드 체크
	데이터 삽입 (Data Insertion)	보안채널 이용 RF 필드 체크
논리적	중간자 공격 (MITM Attack)	사전비밀 공유 RF 필드 체크
	중계 공격 (Relay Attack)	타이밍 체크 위치 체크
	스마트 포스터 URI 스푸핑 (Smart Poster URI Spoofing)	URI 검증 URI 문법 체크

(Quality)에 따라 도청 가능한 거리가 변하지만 일반적으로 능동(Active) 모드일 경우에는 10m, 수동(Passive) 모드일 경우에는 1m이다.

3.1.2 데이터 변조

데이터 변조 공격은 NFC 장치 간 통신시 통신방해, RF 신호 송출, 데이터 전송 등의 방법을 사용하여 데이터의 변질 또는 변형을 일으키는 공격으로 서비스 거부 공격(DOS)과 비슷하다.

3.1.3 데이터 수정

데이터 수정 공격은 NFC 장치 간 통신시 주파수를 수정하여 데이터를 고치는 방법으로 데이터를 변형하는 공격이다. 데이터의 유효성 체크를 하지 않는 서비스의 경우 의미 없는 데이터가 전송되어 일종의 서비스 거부 공격이 될 수도 있다. 또한 보안 채널을 이용하지 않은 경우 데이터의 수정으로 인하여 잘못된 데이터가 전송되어 서비스가 공격자의 의도로 변형되어 제공될 수 있다.

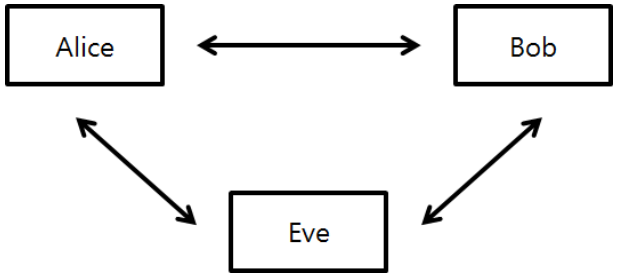
3.1.4 데이터 삽입

데이터 삽입 공격은 두 NFC 장치 간 데이터 전송시 공격자의 메시지를 전송하여 삽입시키는 공격 방법이다. 본 공격은 어느 한 NFC 장치에서 응답 데이터를 전송하는데 오랜 시간이 걸릴 때 유효한 공격이다.

3.2 논리적 공격

3.2.1 중간자 공격

전형적인 중간자 공격(Man-in-the-Middle-Attack)은 [그림 1]과 같이 Alice와 Bob간의 통신시 공격자인 Eve가 각각의 사용자인 Alice와 Bob인 것처럼 가장하여 중간에서 데이터를 취득하는 것이다. NFC는 10cm 이내의 거리에 있는 두 장치 사이에서 동작하기 때문에 중간자 공격에 안전하며, RF 필드의 체크를 통한 중간자의 개입을 확인하여 중간자 공격의 성공률은 극히 낮다. 하지만 10cm라는 거리상의 문제는 도청 공격과 마찬가지로 데이터 송



[그림 1] 중간자 공격

신자와 수신자 그리고 공격자의 안테나 기하학적 구조, 안테나 성능 및 환경에 의해 언제든지 그 상황이 변경 될 수 있다.

3.2.2 중계 공격

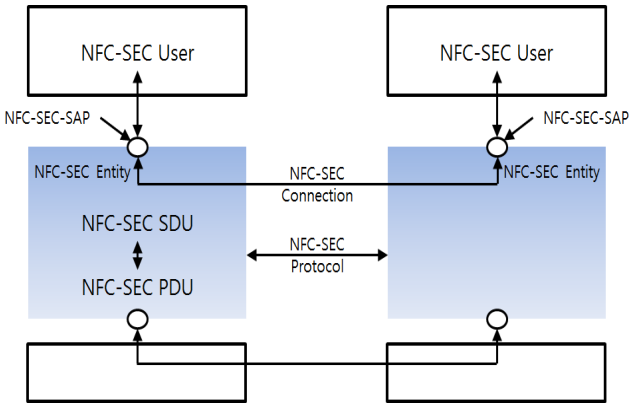
RF 신호를 사용하는 NFC는 기존의 RFID 시스템의 공격 방법 중 하나로 사용되고 있는 중간자 공격과 유사한 개념의 중계 공격이 가능하다. 중계 공격은 공격자가 단순히 데이터 전송에 사용되는 데이터를 중계만 해주기 때문에 보안채널 형성 등을 통한 데이터의 기밀성, 무결성을 유지하여도 그 속성들과 무관하게 공격이 가능하다.

3.2.3 스마트 포스터 URI 스푸핑

NFC 단말기는 스마트 포스터에 부착된 NFC 태그로부터 스마트 포스터의 URI 정보를 읽어 간편한 영화예매 등의 서비스 이용이 가능하다. 이때, 영화정보는 URI형태로 전송이 된다. 이러한 스푸핑 공격은 NFC 태그를 통해 읽어온 정보뿐만 아니라 SMS 등과 같은 형태로 정보를 전달 받았을 때도 동일하게 공격이 가능하다.

4. NFC 보안기술

NFC Forum, ECMA International 등에서 데이터 교환 형식, 보안 프로토콜 등에 대해 NFC 관련 보안 표준을 정의하고 있다. NFC 기술표준은 ECMA-340(NFCIP-1)과 ECMA-352(NFCIP-2)에 기술되어 있는데 NFCIP-1은 NFC 통신에 사용되는 인터페이스와 프로토콜이 설계되어 있으며 NFCIP-2는 기존 인터페이스에 표준들 사이에서 게이트웨이 기능 및 관련된 테스트 방법이 기술되어 있다. 보안과 관련된 주요 표준으로 ECMA에서는 ECMA-385를 발표했으며 내용을 보면 NFCIP-1의 데이터 교환을 위한 보안서비스 및 보안 프로토콜을 제시하였다. ECMA-385(NFC-SEC)는 NFCIP-1에 의해 NFC 장치 간의 통신이 연결된 후 보안 서비스를 수행하게 되는데 구조는 [그림 2]와 같다. 사용자는 NFC-SEC-SAP(Service Access Points)을 통해 NFC-SEC 서비스에 접근하게 된



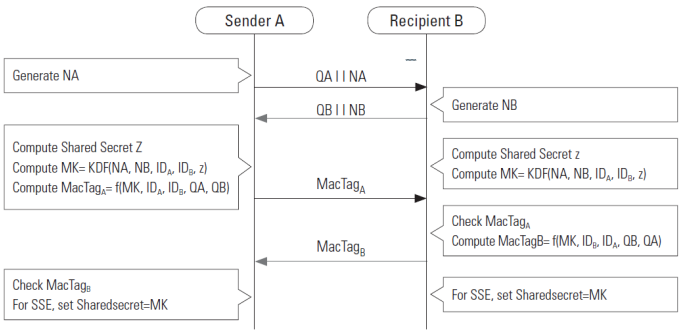
[그림 2] NFC-SEC 보안 계층 구조

다. NFC-SEC 서비스는 NFC-SEC 프로토콜로 NFC-SEC-PDU(Protocol Data Unit)를 교환한다. NFC-SEC 프로토콜 구성을 위해 제공하는 보안 서비스는 다음과 같다.

① SSE(Share Secret Service) : NFC 장치 간 암호 채널 형성을 위해 비밀키 생성 및 키 확인(Key Confirmation) 과정 제공

② SCH(Secure Channel Service) : SSE 서비스를 통해 생성된 키를 이용하여 링크키를 생성하고 NFC 장치 간 통신 데이터의 기밀성과 무결성을 제공

또한 ECMA는 NFC-SEC의 보안 구조 하에 보안 메커니즘인 ECMA-386(NFC-SEC-01)을 제시하였다. 우선 NFC 장치는 ECDH(Elliptic Curve Diffie-Hellman) 공개키와 개인키를 소유한다는 가정 하에 SSE와 SCH를 시행한다. [그림 3]은 SSE를 위해 키(MK) 공유 과정을 나타내며 다음은 각 과정에 대한 설명이다.



[그림 3] 키 일치 및 확인

① ECDH 키 교환 과정으로 비밀 값 Z를 공유하고 이후 키 확인과정(MacTagA, MacTagB) 수행
② SSE 과정에서 키 공유와 확인과정이 성공적으로 수행되면 SCH 과정 진행
③ NFC 기기는 데이터의 기밀성과 무결성 제공을 위해 암호 키와 무결성 키를 비밀 값 Z와 랜덤 값 등으로부터 유도하여 공유
④ 생성된 암호키와 무결성 키를 이용하여 NFC장치 간 데이터를 AES - CTR모드로 암·복호화 및 AES-CBC 모드로 무결성 확인

ECMA에서는 NFC 기기에서 보안 서비스를 제공하기 위한 암호학적 함수들을 [표 2]과 같이 정의하였다.

[표 2] NFC-SEC 암호함수

과정	암호학적 함수
보안 서비스	SSE, SCH
키 공유	ECDH P-192
키 유도 함수	AES-XCBC-PRF-128
키 확인	AES-XCBC-MAC-96
기밀성	AES 128-CTR IV init:AES-XCBC-PRF-128
무결성	AES-XCBC-MAC-96
재생 공격 방지	SN(Sequence Number)

이는 NFC 보안 표준문서(ECMA-386)에 명시된 기본 보안 기술로써 위에 언급한 취약성을 모두 안전하게 막을 수 없다. 또한 외부 장비와 데이터 교환 시 데이터에 대한 무결성, 기밀성, 부인방지 기능이 완벽히 제공되어야 하며 무선 통신의 안전성 확보와 부채널 공격에 안전할 수 있도록 보안성을 강화해야 한다.

4. 결론

본 논문에서 NFC의 보안요소와 취약점분석에 대해서 살펴보았다. 국외뿐 아니라 국내에서도 NFC의 사용이 시작되고 기하급수적으로 늘어날 것으로 여겨짐에 따라 그에 따른 보안상의 문제 또한 많이 발생할 것이다. NFC는 중간자공격의 위협이 적지만 그 자체로는 도청이나 데이터손상에 대해 대처할 수는 없기 때문에 보안채널(Secure Channel)을 이용하여 통신하면 위의 문제에 대해서도 높은 보안수준을 유지할 수 있을 것이다. 이에 따라 보안대책을 사전에 미리 준비해서 사용자들이 정보 및 금전상의 피해 없이 NFC를 자유롭게 사용할 수 있는 환경을 만들어야 할 것이다. 또한 위에 소개한 보안상의 문제점뿐만 아니라 새로운 공격방법 등에 대한 취약점에 대한 맞춤형 대책을 세워야 한다.

참고문헌

[1] 임선희, 전재우, 정임진, 이옥연, “NFC 보안 기술 분석 및 UICC 적용 효과 연구”, 한국통신학회논문지, 11-01, 2010.
[2] 이수미, 임형진, 장재환, 성재모 “모바일 NFC 기반 보안 동향”, TTA Journal, 07/08 2011.
[3] ECMA International: “ECMA-340 Near Field Communication Interface and Protocol (NFCIP-1),” Dec, 2004.
[4] ECMA International: “ECMA-385 NFC-SEC NFCIP-1 Security Services and Protocol,” 2008.
[5] ECMA International: “ECMA-386_NFC-SEC-01 NFC-SEC Cryptography Standard using ECDH and AES,” Dec, 2008.