NFC 기술 동향과 보안 취약점 분석

신상호* · 윤은준** · 유기영***

1. 서 론

NFC(Near Field Communication) 기술은 기존의 13.56 MHz RFID(Radio Frequency Identification) 태그인식 기법을 스마트폰과 같은 이동식 단말기 내에 적용하여 개인 정보 서비스, 전자 금융 거래 서비스와 개인 대 개인(peer-to-peer)간의 양방향 데이터 전송 서비스 등이 사용자들에게 제공되고 있다.

최초의 NFC 기술은 2002년 일본의 Sony, 네덜란드의 NXP에 의해 개발되었고, 현재는 구글, 애플사 등의 스마트폰 플랫폼 사업자와 이동통신사업자, 단말기 제조사 등을 중심으로 모바일 서비스 시장을 선점하기 위해서 다양한 연구 및 개발이 진행되고 있다[1-3,13,14].

최근 스마트 폰 사용의 증대에 따라 이와 관련된 NFC 응용 기술들에 대한 관심이 높아지고 있다. 특히, 양방향 데이터 전송과 모바일 금융 거래 서비스가 차세대 스마트폰 및 모바일 기술로서 주목받고 있다.

본 논문에서는 NFC 기술 개요와 특징, 기술 동향, 제공되는 서비스 및 응용분야에 대해 소개하고, 각각의 제공되는 서비스에서의 보안 취약점을 분석하여 향 후 NFC 보안 기술의 개발 및 향상에서 논의 및 고려되어야 할 사항을 살펴보고자 한다.

※ 교신저자(Corresponding Author) : 유기영 주소 : 대구시 북구 산격 3동 1370번지 경북대학교 컴퓨터학부(702-701), 전화: 053)950-5553, E-mail : yook@knu.ac.kr
* 경북대학교 전자전기컴퓨터학부 박사과정
(E-mail: shshin80@infosec.knu.ac.kr)
** 경일대학교 사이버보안학과 교수
(E-mail : ejyoon@kiu.ac.kr)
*** 경북대학교 컴퓨터학부 교수
※ 본 논문은 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 육성지원 사업과 지식경제부 및 한국산업기술평가원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행하였음.(NIPA-2012-(C1090-1221-0002)) & [10041145, 자율군집을 지원하는 웰빙형 정보기기 내장 소프트웨어 플랫폼 개발]

2. NFC 기술 개요와 동향

2.1 NFC 기술 개요와 표준화

NFC 기술은 13.56 MHz 대역에서 운용 중인 비접촉식 근거리 인식 기술인 RFID 통신 프로토콜과 데이터 전송 포맷의 ISO/IEC 14443 표준에 기반한 것으로 스마트폰에 접목하여 단말기 간 혹은 단말기와 태그 간의 데이터통신 및 개인 정보 제공 서비스 등으로 응용할 수 있다.

2004년 Sony, NXP를 주축으로 결성된 NFC Forum[15]에서 ISO/IEC 18092 표준[17]으로 제정되었고, 13.56 MHz 대역에서 자기장 커플링 방식의 기기 간 통신 인터페이스 및 프로토콜을 정의했다는 점에서 기존의 비접촉식 스마트카드 기술과 다른 새로운 기술로 인식된다[1-3,13,14].

이후 1m 범위에서 무선인식이 가능한 ISO/IEC

15693 표준과 앞에서 언급한 ISO/IEC 18092 표준을 통틀어 NFC Interface and Protocol(NFCIP-2)로 정의하고 이를 ISO/IEC 21481로 통합하여 표준을 제정하였다. 이 외에도 NFC 보안 관련 표준으로 ISO/IEC 13157-1과 ISO/IEC 13157-2가 각각 존재한다.

표 1은 NFC 관련 표준 기술에 대해 비교한 것이다.

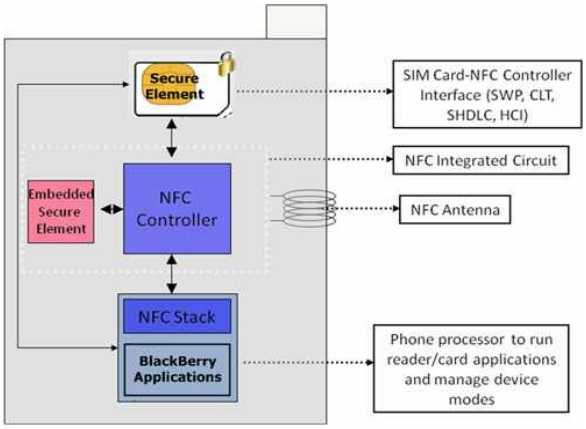


그림 1. 블랙베리폰의 NFC 아키텍쳐

2.2 NFC 시스템과 통신 방식

NFC 기술을 사용하기 위해서는 NFC 태그(tag) 또는 NFC 기능을 지원하는 금융 USIM(Universial Subscriber Identity Mudule) 칩이 필요하다. 이를 이용해 그림 1의 NFC 컨트롤러와 리더에 의해 NFC 내의 정보를 이용하여 각종 서비스를 제공하게 된다. 그림 1은 블랙베리사에서 설계하여 실제 사용하고 있는 블랙베리폰 내에서의 NFC 솔루션이다. NFC 리더와 제어 모듈, NFC 보안 모듈, NFC 지원 블랙 베리 애플리케이션 모듈로 구성되어 있다. 일반적인 모바일 NFC 시스템 아키텍쳐는 네트워크 사업자, 서비스 제공자, 단말기 제조사 모듈로 구성되어 NFC 관련 서비스를 제공한다.

일반적인 NFC 통신은 임의의 장치가 이니시에이터(initiator)로 작동하게 되면 다른 대상 장치는 타겟(target)이 되는 반 이중 방식으로 동작한

표 1. NFC 관련 표준 기술의 비교 [1-3]

구 분	ISO/IEC 14443	ISO/IEC 15693	ISO/IEC 18092(NFC)
주파수대역	13.56 MHz		
인식거리	10cm 이내	1m(실제 70cm)	10~20cm 이내
전송속도	106Kbps~212 Kbps	26Kbps	424Kbps~1Mbps
동작모드	수동	수동	능동/수동
상용화	-Type A, Type B: 금융권의 비접촉식 결제 솔루션의 표준 -Type C: NTT Docomo, 홍콩 Octopus, 싱가폴 Land Transit Aythority -스마트카드(교통/신용카드)	-티켓팅, 물품관리, 출입관리, 색인등 -스마트레이블(상품인식)	휴대폰 이외에 디지털 카메라, 컴퓨터, PMP, MP3 Player 등 다양한 멀티미디어 기기 및 모바일 기기를 지원
비고	1994년에 발의, 2001년에 최종 제정, 스마트카드 표준	보안 프로토콜을 요구하지 않음	-리더와 리더간의 통신 지원 -NFC 장치들의 변조방식과 코딩, 전송속도 RF 인터페이스의 프레임 포맷, 초기화시의 데이터 충돌 제어를 위한 초기화 방식 및 조건 등 명시

다. 이니시에이터 NFC 단말기는 주기적으로 RF를 송출해 RF 필드를 검색하고, RF 필드가 검색되면 초기 작업을 수행하여 타겟 단말기와 통신을 시작한다. 타겟 단말기는 이니시에이터 단말기로부터 받은 데이터에 대해 응답하고, 응답을 받은 이니시에이터 단말기는 다음 과정을 처리하여 타겟 단말기에게 데이터를 송신하는 과정을 반복한다. 그림 2는 이러한 과정을 도식화한 것이다 [1,4,13,14].

NFC 통신 모드는 크게 두 가지가 존재한다. 수동 모드와 능동 모드로 나뉘고, 수동 모드의 경우 이니시에이터 단말기에서 먼저 RF 필드를 제공하여 통신이 시작되는 것을 의미하고, 능동 모드의 경우 이니시에이터 단말기와 타겟 단말기 모두가 RF 필드를 동적으로 생성하여 통신하게 되는 것을 의미한다.

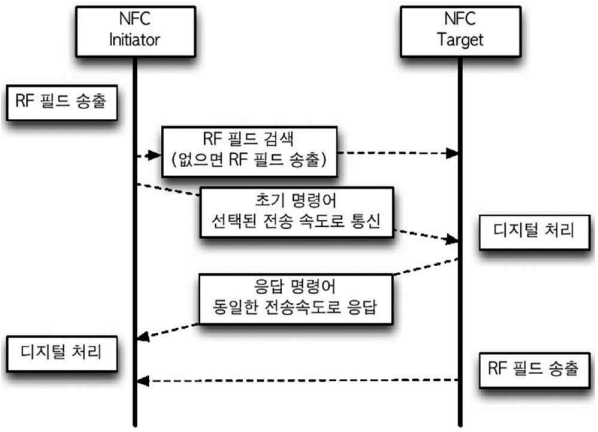


그림 2. NFC 통신 프로토콜 [1,2,17]

2.3 NFC 태그 종류와 운용 모드

NFC Forum[15]에서는 태그 제조사들 간의 호환성을 보장하기 위해 NFC에 사용되는 태그의 종류는 4가지로 분류하여 정의했다. 표 2는 4가지 타입의 NFC 태그와 이에 대한 주요 특징을 서술한 것이다.

표 2. NFC 태그 타입별 구분 [1,2]

태그	Type 1	Type 2	Type 3	Type 4
인터페이스	ISO 14443A	ISO 14443A	ISO 18092	ISO 14443
속도	106 Kbps		212 Kbps	ISO 14443-4
프로토콜	자체 명령어		FeliCa	ISO 7816-4
메모리 공간	96 byte	48 byte	2 Kbyte	96 byte

NFC의 통신은 RFID에서의 단 방향 통신뿐만 아니라 능동형(active)기기 간의 양방향 통신을 지원해주기 때문에 운용 방법에 따라 그림 3과 같이 3가지 모드로 규정하고 있다.

Card Emulation 모드의 경우 교통카드 및 상품 결제를 위해 적용되는 것으로 비접촉 IC카드 방식의 수동형 태그 형식으로 작동하고, 기기 내에 저장하고 있는 정보를 외부의 능동형 단말기에 전달하는 역할을 수행할 수 있다.

Reader/Writer 모드는 외부 전자 태그 상에 존재하는 정보를 획득하여 이에 해당하는 정보를 제시한다. RFID 태그의 제품 정보, 가격 등의 정보를 읽고 쓰기 위해 고안된 것으로 스마트폰에 NFC가 탑재되면서 칩 기반 태그의 읽기 기능을 수행할 뿐만 아니라 인쇄된 코드도 스캔 후 NFC

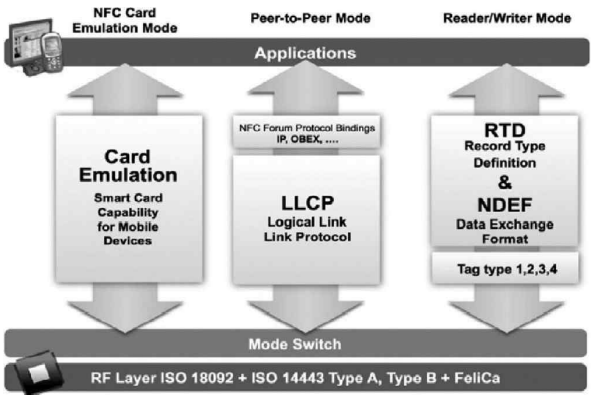


그림 3. 3가지 NFC 운용모드 [1,2,17]

포맷으로 변환하여 기록할 수 있다.

Peer-to-Peer 모드는 두 대의 NFC 기능이 탑재된 단말기가 능동 모드로 통신을 하는 방식으로 기기간의 멀티미디어 데이터와 기타 정보를 전송 및 기기간의 연결을 수행하는 기능을 수행한다. 그러나 능동모드로 데이터 전송을 수행해야하기 때문에 RF 필드의 생성과 같은 과정에서 전력 소모량이 큰 단점이 존재한다.

2.4 NFC 응용

2007년부터 사용된 스마트폰의 영향으로 NFC 기반의 응용기술 및 다양한 서비스가 개발되고 있다. NFC는 대표적으로 비접촉식 근거리 무선통신 기술을 포함하는 접근제어, 근태 관리, U-헬스케어, 정보 수집, 모바일 금융 거래 및 결제 등 다양한 분야에서 널리 사용이 가능하다. 다음은 주요 응용 분야에 대해 작성한 내용이다[6-8, 11,14,16].

2.4.1 NFC 지원 단말 간 데이터 교환

스마트폰 단말 간의 데이터 전송, PC와 스마트폰 단말 간의 파일 공유, 일반 가전제품과 스마트폰 간 정보 업데이트 등 NFC를 지원하는 모든 단말기 사이의 직접적인 데이터 통신을 간단한 '접촉(Touch-and-go)'을 통해 처리할 수 있다.

2.4.2 서비스 발견 및 연결

NFC 태그가 부착되어 있는 스마트 포스터를 이용하여 직접적인 정보 획득 및 관련 웹사이트로의 연결까지 제공함으로써 새로운 서비스 연결이 가능해졌고, Wi-Fi 간편 보안 설정과 Bluetooth 단말기 간의 간편 연결에도 사용되고 있다.

2.4.3 전자결제 및 티켓팅

NFC의 비접촉식 스마트카드 기술과 보안 기술로 인해 모바일 결제 방식을 제공할 수 있으며, 교통카드와 할인쿠폰 등의 다양한 결제수단으로 활용될 수 있다.

2.4.4 NFC를 이용한 개인 인증 및 정보 제공

NFC 내에 개인의 정보나 혹은 인증을 위한 데이터를 삽입하여 특정 기관의 출입이나 시스템의 사용을 위해 NFC를 이용한 인증 및 개인 정보 제공 서비스가 활발히 개발 중이다. 특히 모바일 금융 거래 시 사용자 자신임을 증명하거나 부인방지를 위한 NFC 기반의 여러 알고리듬들이 개발되는 추세이다. 그림은 현재 상용화되어 사용되는 NFC 기반의 응용기술들의 사례를 보여주고 있다.

3. NFC 기술에서 고려되어야 할 보안 사항

3.1 NFC 기술의 보안 표준

NFC 기술 관련 보안 표준은 앞에서 언급된 것처럼 ISO/IEC 13157-1(ECMA-385)과 ISO/IEC 13157-2(ECMA-386)가 각각 존재한다[18]. ISO/IEC 13157-1 표준에서는 보안 서비스와 보안 프로토콜에 대해 다루었다. 세부적인 내용은 공유된 비밀 서비스(Shared Secret Service: SSE), 보안 채널 서비스(Secure Channel Service: SCH), 안전한 (데이터) 교환 프로토콜(Secure Exchange Protocol: SEP)에 대해 정의하고, 이에 대한 상세한 설명을 다루고 있다. ISO/IEC 13157-2 표[18]에서는 ECDH(Elliptic Curve Diffie-Hellman)와 AES(Advanced Encryption Standard)를 사용한 (데이터) 암/복호 알고리듬에 대해 다루었다. 세부적인 내용은 ISO/IEC 13157-1의 서비스와 프로토콜에서 사용되는 데이터들의 암/복호 및 무결성(integrity)에 대한 내용을 다루고 있다. 표 3은 NFC 보안 표준 문서 내에서 지원되는 암호

표 3 NFC 보안 암호 알고리듬 목록 [1,2,18]

구 분	지원되는 암호 알고리듬
보안서비스	SSE, SCH
키 교환	ECMA-352
키 유도 함수	AES-XCBC-PRF-128
키 확인	AES-XCBC-MAC96
기밀성	AES-128-CTR, IV init : AES-XCBC-PRF-128
무결성	AES-XCBC-MAC-96

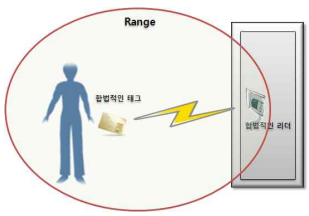
알고리듬의 목록이다.

3.2 NFC 보안 취약점

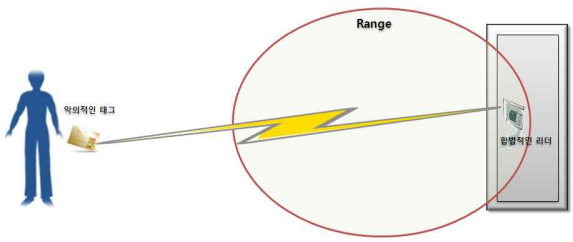
NFC에 기반한 여러 응용 기술들에서의 보안 취약점은 크게 하드웨어와 소프트웨어로 구분할 수 있다. 하드웨어의 경우 기존의 스마트폰을 기반으로 하는 물리적 공격과 RFID에서 발생할 수 있었던 보안 공격들이 존재한다. 스마트폰에서 발생할 수 있는 물리적 공격으로는 스마트폰의 통신 시 발생하는 전파의 도청 또는 간섭을 통한 통신 방해 공격이나 전류 증폭 또는 오류 신호를 보내어 스마트폰 내의 NFC 기능을 다운시키거나 특정 기능을 수행시키는 부채널 공격과 리버스 엔지니어링을 이용한 NFC 칩 또는 태그 내의 개인정보 유출이 대표적이다.

또한 RFID에서 발생할 수 있는 물리적 공격으로는 중간자 공격 또는 중계 공격이 대표적이라고 할 수 있다[19-26]. RFID 리더기는 일정한 인식 반경을 두고, 인식 반경 내에 존재하는 모든 RFID 태그들을 인식하게 된다. 이 때 Proxy RFID 리더기와 태그를 이용하여 인식 반경 내에 존재하지 않는 임의의 RFID 태그의 ID를 도청하여 인식 반경 내에 존재하는 것처럼 중계하거나 이를 이용하여 정보를 위조하는 등의 공격이 발생하게 된다. 중계 공격 시나리오에 대해 좀더 자세히 살펴보면 다음과 같다. 먼저 공격자는 넓은 공간에서 NFC 기반의 시도-응답(Challenge-Response) 인증 프로토콜이 진행되는 동안 리더와 태그사이에 교환되는 정보의 중계를 위해 두 개의 트랜스폰더를 사용한다. 실제 리더와 공격자의 프록시 리더 장치에 인접해 있는 프록시 태그 장치는 실제 태그와 근접해 있으며, 실제 태그 소유자는 이 사실을 알지 못하게 된다. 이후 공격자의 프록시 리더는 정당한 태그와 통신하여 인증 정보를 획득하고, 획득한 인증 정보를 담고 있는 프록시 태그는 정당한 리더와 통신하게 된다. 결과로 프록시 태그로부터 수신된 인증 데이터를 실제 리더가 잘못 인증을 하게 되어 리더는 실제적으로는 멀리 떨어져있는 합법적인 태그 대신 프록시 태그의 존재를 검증하게 된다.

중계 공격은 일반적으로 그림 4, 5, 6과 같이 다시 경계 위조 공격(Distance Fraud Attack), 마피아 위조 공격(Mafia Fraud Attack)과 테러리스트 공격(Terrorist Attack)의 세 가지 형태의 중계 공격으로 나눌 수 있다[19-26]. 경계 위조 공격은 그림 4의 (a)와 같이 합법적인 태그를 소요한 사



(a) 정상적인 인증



(b) 경계 위조 공격 기반 인증

그림 4. 경계 위조 공격 시나리오

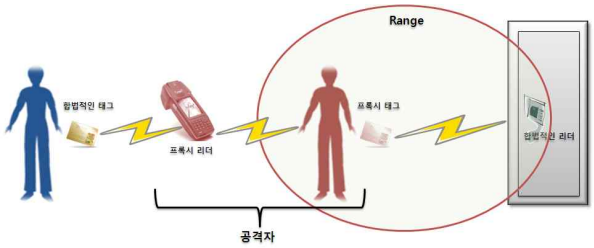


그림 5. 마피아 위조 공격시나리오

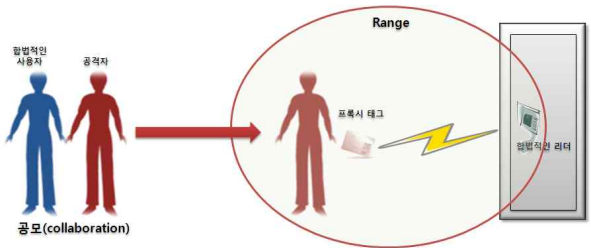


그림 6. 테러리스트 공격 시나리오

용자는 리더기 인식 반경(range)내에 존재하여 인증을 받아야 함에도 불구하고 그림 4.(b)와 같이 리더기가 인식 반경을 감지하지 못하는 취약점을 이용한 경계 위조 공격을 수행하여 리더기 인식 반경 밖에서 인증을 받는 공격이다.

마피아 위조 공격은 그림 5와 같이 합법적인 태그는 리더기의 인식 반경 밖에 존재하지만 공격자의 프록시 태그가 합법적인 태그로 위장하여 리더로부터 간단히 인증 받는 공격으로 리더와 태그 모두 공격자의 존재를 감지하지 못하게 되는 공격이다. 마피아 위조 공격은 리더와 태그에게 어떠한 예고도 없이 공격을 가할 수 있기 때문에 가장 심각한 공격으로서 중간자(Man-In-The-Middle) 공격과 같은 원리로 수행되는 공격이다. 마피아 위조 공격 시나리오에서는 리더와 태그 둘 다 정당하지만, 공격자는 정당한 리더의 경계 내에 존재하여 리더와 태그 사이에서 프록시 리더와 태그를 사용하여 중간자 공격을 수행한다. 프록시 태그는 정당한 리더와 통신하고, 프록시 리더는 정당한 태그와 통신한다. 프록시 태그와 리더는 서로 협력하며, 프록시 태그는 실제로 비밀정보에 대한 어떠한 것을 알 필요도 없이 정당한 태그의 비밀 정보에 관련된 진술서를 사용하여 리더와 인증하게 된다.

테러리스트 위조 공격은 마피아 위조 공격에서 확장된 공격으로 그림 6과 같이 합법적인 태그와 공격자의 프록시 태그가 공모(Collaboration)를 하여 리더기의 인식 반경 내에 존재하지 않으면서도 인증을 통해 반경 내에 존재하는 것처럼 속이는 공격이다. 테러리스트 위조 공격에서는 정당한 태그가 공격자의 프록시 태그와 협력하여 인증을 한다. 악의적인 태그는 근접해 있는 리더와 인증하기 위해 정당한 태그와 공모하고, 프록시 태그는 정당한 태그의 비밀키나 프라이버시를 알지 못하더라도 상관없다.

이를 위해 최근 RFID 인식 범위를 지정하여 이러한 공격을 막을 수 있는 RFID 경계결정 프로토콜의 연구 및 개발이 활발히 진행 중이다. 13.56 MHz 대역의 RFID 태그 인식 기술에 기반한 NFC 기술 역시 이러한 물리적 공격에 매우 취약하기 때문에 임의의 Proxy NFC 단말기와 태그를 소유한 악의적인 공격자에 의해 NFC 태그의 ID 및 개인 정보를 탈취 하여 모바일 금융 거래 혹은 개인 인증을 수행하는 보안 공격이 발생할 수 있다. 그러나 이와 관련된 보안 기술을 현재 존재하지 않으므로 앞으로 연구되어야 할 부분이다.

한편, 소프트웨어적 보안 공격으로는 기존에 알려진 스마트폰 보안 공격과 NFC 통신에서 발생할 수 있는 보안 공격들이 존재한다. 일반적으로 알려져 있는 스마트폰 보안 공격은 사용자들이 손쉽게 접할 수 있는 불법 루팅(최고관리자 권한 획득), 블랙마켓을 이용한 악성코드가 탑재된 앱의 다운로드에 의한 개인정보 유출, DDoS 공격 등이 존재한다. 이러한 보안 공격을 이용해 스마트폰 내에 존재하는 NFC 칩 또는 태그의 개인

정보 도용과 잘못된 정보로 변경하여 사용자로 하여금 인증 실패와 같은 보안 공격이 존재한다. NFC 통신 내에서도 단말기의 보안이 취약할 경우 보안 통신 프로토콜을 통해 안전하게 송수신된 데이터들이 도청, 중계 공격을 통해 위협 받을 수 있다.

응용 분야 측면에서도 여러 보안 취약점이 존재한다. 데이터 통신의 경우 상대방에 대한 인증을 수행하지 않거나 기법이 매우 단순한 경우가 대부분이기 때문에 경량의 안전한 보안 인증 기법이 도입되어야 할 것이다. 서비스 발견과 연결 측면에서도 역시 인증에 대해 매우 취약하다. NFC 칩 또는 태그를 이용한 WI-FI 접속과 연결의 경우 위조된 NFC 칩을 이용할 경우 사용자의 개인정보가 그대로 노출될 수 있기 때문에 NFC 칩에 대한 무결성 및 안전성을 제공하는 서비스 또는 알고리듬이 개발되어야 할 것이다. 모바일 금융거래의 경우 NFC 응용 기술 중 보안 공격으로부터 가장 노출이 많이 되어 있는 분야이다. 기존의 PC 또는 스마트폰에서 발생할 수 있는 다양한 보안 공격들을 약간의 변경을 통해 NFC 보안 공격에 적용할 수 있다. 이를 위해 보안 공격에 대비하여 표준을 제정하여 서비스에 대한 보안 정책, 보안 프로토콜, 암호 알고리듬을 제안하였다. 하지만 앞에서도 언급했듯이 인증에 대한 부분이 취약하기 때문에 앞으로 이러한 부분에 대한 연구와 개발이 활발히 수행되어야 할 것이다. NFC 칩 또는 태그를 이용한 개인정보의 사용에서도 기존의 표준에서 제안된 여러 기법을 이용해 비교적 안전하지만 스마트폰과 연계된 보안 기술의 부재로 인하여 스마트폰의 앱이나 O/S를 이용한 보안 공격에는 매우 취약한 상태이다. 이를 위해 앞으로는 스마트폰과 연계된 보안 기법들이 연구되어야 할 것이다[4-12].

4. NFC 기반 경계 결정 프로토콜 응용

연구자 Desmedt는 송수신 메시지의 왕복 시간 측정을 기반으로 경계 결정 개념을 최초로 소개하여 마피아 위조 공격에 대한 보안 대책으로 활용 가능함을 증명했다[19]. 그리고 1993년에 Brands와 Chaum은 Desmedt의 아이디어를 기반으로 경계 프로토콜을 처음으로 설계하여 시도-응답 기반 암호 프로토콜에서 n-라운드 동안의 단일 비트 왕복 시간(Time Round Trip of Single Bit Exchange)을 측정하는 경계 결정 프로토콜에 대해서 최초로 소개하였다[20]. Brands-Chaum의 경계 결정 프로토콜에서, 리더 역할을 하는 검증자(Verifier)가 1비트를 전송하는 시점에 타이머(Timer)가 시작되며, 태그 역할을 하는 증명자(Prover)가 검증자에게 응답 값으로 1비트를 전송하면 타이머는 중지한다. 이를 고속 비트 교환 단계(Rapid Bit Exchange Phase)라고 한다. 검증자는 비트 전달 시간을 측정하기 위해 왕복 시간 측정 기법인 RTT(Round Trip Time)를 사용하여 실제 검증자 인식 반경 내에 증명자가 존재하는 지를 검증하게 된다.

그림 7은 Brands와 Chaum이 제안한 저속→고속→저속의 단계로 구성된 경계 결정 프로토콜 검증 수행과정을 보여준다. Brands-Chaum의 경

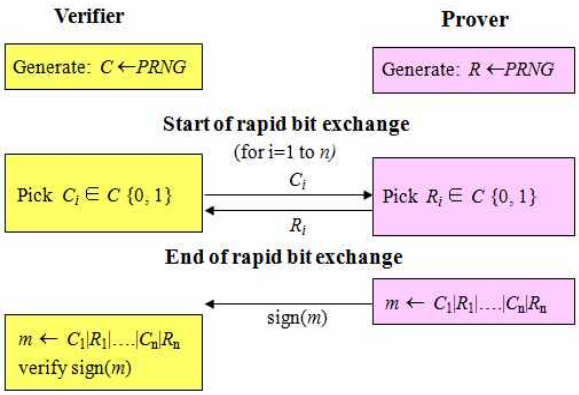


그림 7. Brands-Chaum의 경계 결정 프로토콜

계 결정 프로토콜에서는 검증자(verifier)와 증명자(prover)는 먼저 난수 비트 스트링인 $C = C_1 C_2 \cdots C_n$와 $R = R_1 R_2 \cdots R_n$을 각각 생성한다. 그러고 나서 검증자는 하나의 요청 비트인 C_i $(i = 1, \ldots, n)$를 한 번에 1비트씩 전송하고, 증명자는 R_i를 가지고 즉시 응답한다. 검증자는 각 비트 C_i의 전송과 그에 대응하는 응답 비트 R_i의 수신 사이의 시간을 왕복 중계 시간으로 기록한다. 모든 n비트가 교환된 후에 증명자는 두 개의 비트 스트링인 C와 R을 위해 메시지 인증 코드 또는 디지털 서명을 전송하여 검증함으로써 프로토콜을 종료한다.

5. 결 론

본 논문에서는 NFC 기술에 대한 개요에 대해 설명하고, NFC 기술에서 발생할 수 있는 보안 취약점에 대해 분석하였다. NFC는 스마트폰과 연계된 차세대 기술로서 모바일 금융 거래, 양방향 데이터 전송, 개인정보를 이용한 접근제어 등의 많은 IT분야에 응용 및 적용할 수 있다.

그러나 NFC와 관련된 보안 기술은 현재 미비한 실정이다. 데이터 통신 시 사용하는 보안 프로토콜과 암/복호, 무결성과 같은 알고리듬은 표준으로 제정이 되었지만 스마트폰 내에서 발생할 수 있는 여러 보안 공격과 인증과 관련 공격 문제에 대해서는 현재 모바일 금융 거래 및 특정 시스템의 접근제어와 같은 서비스가 활발히 진행 중이므로 앞으로 지속적인 연구가 수행되어야 할 것이다. 또한 NFC 기술에 대한 보안 연구뿐만이 아니라 NFC 사용자 측면에서 발생할 수 있는 개인 프라이버시 혹은 새로운 형태의 보안 공격에 대해서도 적극적인 연구를 통해 안전하고, 효율적인 스마트라이프(smart-life)를 영위할 수 있도록 노력해야 할 것이다.

참 고 문 헌

[1] 조미영, 김기천, “NFC 시장 현황 및 활성화 방안 연구,” 한국통신학회지(정보와통신), 제 29권 제 6호, pp. 58-66, May, 2012.

[2] 김형준, 권태경, “NFC 기술 동향과 보안 이슈,” 한국통신학회지(정보와통신), 제29권 제8호, pp. 57-64, July, 2012.

[3] 김선배, 김형국, 윤희용, “NFC에서의 보안 취약점 분석,” 한국인터넷정보학회 추계학술발표대회 논문집 제 12권 제 2호, pp. 185-186, Nov., 2011.

[4] 임선희, 전재우, 정임진, 이옥연, “NFC 보안 기술 분석 및 UICC 적용 효과 연구,” 한국통신학회논문지, 제36권 제1호, pp. 29-36, Jan., 2011.

[5] 이재식, 김형주, 유한나, 박태성, 전문석, “NFC 환경에서 개인정보보호를 위한 취약점 분석 및 대책 수립 방법론,” 한국정보보호학회논문지, 제22권 제2호, pp. 357-365, April, 2012.

[6] 박충범, 이재호, 이형석, 마진석, “스마트폰 환경에서 NFC를 이용한 Wi-Fi 접속 기법,” 한국정보과학회 학술발표논문집 제 39권 제 1D호, pp. 47-48, June, 2012.

[7] 구철회, 이원규, 박청호, 김영곤, “무인화 마켁을 구현하기 위한 모바일 NFC 결제 시스템,” 한국정보과학회 학술발표논문집 제38권 제2D호, pp. 81-84, June, 2012.

[8] 박재영, 김용강, 이정현, 최광훈, “NFC 모바일 폰을 활용한 도서관 시스템,” 한국정보과학회 학술발표논문집, 제38권, 제2D호, pp. 43-45, Nov., 2011.

[9] Roland, M. Langer, J., “Digital Signature Records for the NFC Data Exchange Format,” Proceedings og 2010 Second International Workshop on Near Field Communication (NFC), pp. 71-76, April 2010.

[10] Reveilhac, M., Pasquet, M., “Promising Secure Element Alternatives for NFC Technology,” Proceedings og First International Workshop on Near Field Communication 2009(NFC09), pp. 75-80, Feb. 2009.

[11] Mulliner, C., "Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones," Proceedings of International Conference on Availability, Reliability and Security 2009 (ARES '09), pp. 695-700, March 2009.

[12] Hsu-Chen Cheng, Wen-Wei Liao, Tian-Yow Chi and Siao-Yun Wei, "A secure and practical key management mechanism for NFC read-write mode," Proceedings of 2011 13th International Conference on Advanced Communication Technology (ICACT), pp. 1095-1011, Feb. 2011.

[13] Michahelles Florian, Thiesse Frederic, Schmidt Albrecht and Williams John R., "Pervasive RFID and Near Field Communication Technology," Pervasive Computing, IEEE, Vol.6, No.3, pp. 94-96, Sept. 2007.

[14] Want R, "Near field communication," Pervasive Computing, IEEE, Vol.10, No.3, pp. 4-7, Sept. 2011.

[15] NFC Forum, http://www.nfc-forum.org/

[16] Google Wallet, http://www.google.com/wallet

[17] ISO/IEC 18092:2004 Information technology-Near Field Communication-Interface and Protocol (NFCIP-1)

[18] ISO/IEC 13157:2010 Information technology-Telecommunications and information exchange between systems - NFC security (NFC-SEC)

[19] Y. Desmedt. Position Statement in RFID S&P Panel: From Relative Security to Perceived Secure. In Financial Cryptography, vol. LNCS 4886, pp. 53-56, 2007.

[20] S. Brands and D. Chaum. Distance-Bounding Protocols. EU-ROCRYPT'93, Vol. LNCS 765, pp. 344-359, 1993.

[21] G. Avoine, C. Floerkemeier, and B. Martin. RFID Distance Bounding Multistate Enhancement. Indocrypt 2009, vol. LNCS 5922, pp. 290-307, 2009.

[22] G. Avoine and A. Tchamkerten. An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-acceptance Rate and Memory Requirement. ISC'09, volume 5735 of LNCS, pp. 250-261, 2009.

[23] G. Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005.

[24] G. Hancke. Practical Attacks on Proximity Identification Systems. IEEE Symposium S&P 2006, pp. 328-333, 2006.

[25] G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. SecureComm 2005, 2005.

[26] G. Hancke, K. Mayes, and K. Markantonakis. Condence in Smart Token Proximity: Relay Attacks Revisited. In Elsevier Computers & Security, June 2009.

신 상 호

• 2006년 금오공과대학교 응용수학/컴퓨터공학 학사
• 2008년 경북대학교 전자전기컴퓨터학부 석사
• 2009년~현재 경북대학교 전자전기컴퓨터학부 박사과정
• 관심분야 : 암호학, 양자암호, 고속암호시스템, 클라우드 컴퓨팅보안, 스테가노그래피

윤 은 준

• 1995년 경일대학교 학사
• 2003년 경일대학교 컴퓨터공학과 석사
• 2007년 경북대학교 컴퓨터공학과 박사
• 2007년~2008년 수성대학교 컴퓨터정보계열 전임강사
• 2009년~2011 경북대학교 대학원 전자전기컴퓨터학부 계약교수
• 2011년~현재 경일대학교 사이버보안학과 교수
• 관심분야 : 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

유 기 영

• 1976년 경북대학교 수학교육과 학사
• 1978년 한국 과학 기술원 전산학과 석사
• 1992년 미국 뉴욕 Rensselaer Polytechnic Institute 전산학과 박사
• 1978년~현재 경북대학교 컴퓨터학부 교수
• 1997년~1998년 한국정보과학회 영남지부장
• 1999년~현재 한국정보과학회 영남지부장
• 1999년~현재 한국 정보과학회 이사
• 2006년~현재 제12대 한국 정보보호학회 부회장
• 관심분야: 암호학, 정보보호, 유비쿼터스보안, 네크워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜