情 報 保 護 學 會 誌
第23卷 第2號, 2013. 4

NFC 기반 모바일 서비스 보안 위협 및 대책

백 종 현*, 염 흥 열**

요 약

스마트폰, 태블릿 PC 등 2010년부터 폭발적으로 보급 확산된 스마트 디바이스의 영향으로 모바일 결제 분야에 가장 핫이슈로 떠오른 기술이 바로 NFC (Near Field communication) 기술이다. 사실, NFC 기술은 2004년부터 표준이 개발되었지만 이를 적용할 디바이스 및 서비스의 부재로 활용이 되고 있지 않다가 2011년 구글이 구글 월렛 서비스를 시작하면서 본격적으로 NFC 기반 서비스가 적용되기 시작하였다. 국내에서도 2011년 11월 명동 NFC 존 시범 사업을 통해 모바일 결제, 스마트 포스터, 스마트 주문 등 다양한 NFC 기반 서비스를 추진하였다. 이렇듯 국내외에서 다양한 NFC 기반 서비스 발굴 및 활성화에 노력을 기울이고 있기는 하지만, 보안을 고려하지 않은 서비스 제공 시 이에 대한 사고 피해는 상상을 초월할 수 있다. 특히, NFC 기반 서비스의 대부분이 사용자의 금전적 결제를 요구하는 서비스라는 점이 이를 입증해준다. NFC 기술 자체에는 보안 기능이 일부 포함되어져 있기는 하지만 NFC 기반 서비스별 보안 취약점이 존재할 수 있다. 이에 따라, 본 논문에서는 NFC 기반 서비스별 보안 위협·취약점 분석 및 해당 위협 및 취약점에 대한 기술적·제도적 보안 대책 등을 제시한다.

Ⅰ. 서 론

2010년부터 고성능 스마트폰, 태블릿 PC 등 스마트 디바이스의 보급이 확산되면서 본격적으로 국민생활에 밀접한 다양한 어플리케이션 및 서비스 개발이 급격하게 증가하고 있다. 이러한 스마트 디바이스의 확산과 무선 네트워크의 발전은 우리의 일상생활을 윤택하고 편리하게 변화시켜 나가고 있으며 앞으로도 다양한 분야로 지속적으로 확산되어 갈 것으로 예상된다. 이러한 혁신적인 변화에 반드시 필요한 기술 중에 하나가 바로 NFC (Near Field communication) 기술이다. NFC 기술은 근거리 무선 통신기술중에 하나로 10cm 이내의 거리에서 기기간 무선통신을 통해 다양한 서비스를 제공할 수 있는 기술이다[1][2]. 최초 NFC 기술표준이 제정된 시기는 2004년으로 최신의 기술은 아니지만 그동안 이를 활용한 디바이스가 부재하여 활용이 미미하다가 최근 스마트폰의 확산으로 본격적으로 NFC 기술이 주목을 받게 되었다. 국내에서는 작년 11월 방통위, KISA가 주관하고 이통사, 카드사, VAN사 등이 연합하여 명동 NFC 존 시범사업을 추진하였으며, 올해 5월부터는 여수엑스포에 NFC 서비스를 운영하고 있다. 국외에서도 Google사에서 Google wallet 서비스를 2011년 9월 상용화하여 현재 모바일 결제 및 쿠폰 서비스를 중심으로 사업을 추진하고 있다. 이러한 NFC 기반 모바일 결제 서비스를 통해 더 이상 지갑에 여러 장의 신용카드, 회원카드, 쿠폰 등을 별도로 보관하지 않고 스마트폰 하나만으로 간편한 소비생활을 할 수 있게 되었다. 또한 영국, 프랑스, 독일, 일본 등 여러 국가에서도 NFC서비스에 많은 관심을 가지고 다양한 서비스를 제공하고 있다. 하지만 이러한 편리성과 확장성의 장점을 가지고 있는 반면 보안을 고려하지 않을 경우 그만큼 피해도 크게 발생할 수 있기 때문에 NFC 기반 응용서비스를 제공하기 이전에 관련 보안 대책 수립이 반드시 선행되어야 한다.

본 논문에서는 NFC 기술 및 표준 분석, NFC 기반 응용서비스 현황 분석, NFC 기반 서비스 보안 위협·취약점 분석 및 이에 대한 보안대책에 대해 제시한다.

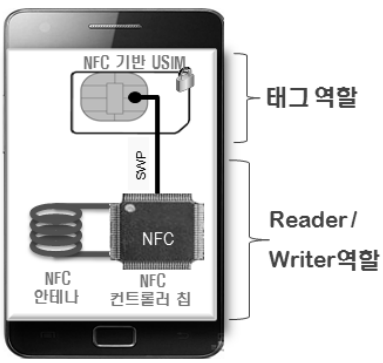
본 연구는 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. 2010-0025393)의 일환입니다.

* 한국인터넷진흥원 (jonghyunbaek0@gmail.com)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

Ⅱ. NFC 기술 및 표준 현황

2.1 NFC 기술 현황

NFC란 전자태그(RFID)의 일종으로 13.56MHz 주파수 대역을 사용하여 비접촉식으로 10cm 이내의 단거리에서 기기간 데이터를 전송하는 기술이다. NFC 기술은 기존의 비접촉식 스마트카드 기술(ISO/IEC 14443 Proximity-card 표준)을 기반으로 개발되었으나 단순 스마트카드 기능 뿐 아니라 양방향 통신을 통해 전자태그의 정보를 읽어오거나 반대로 정보를 입력할 수 있는 Read/Write 기능과 단말간 통신을 위한 P2P 기능까지 제공할 수 있다[3][4]. 이러한 NFC 주요기능을 제공하기 위해서는 기본적으로 NFC 칩, 안테나, SE(Secure Element, USIM 또는 SD 등 외장메모리에 위치) 등이 필요하며, 국내에서 개발되는 모바일 디바이스에는 SE가 USIM내에 포함되어 있다[5].



〔그림 1〕 NFC 기능 제공을 위한 디바이스 구성 요소

이러한 NFC의 다양한 기술을 통해 기존의 모바일 결제 뿐 아니라 교통카드, 공항 자동체크인, 스마트 주문, 스마트 포스터, 버스 도착 알림, 자동 도어락 등 일상생활에 편리함을 줄 수 있는 다양한 서비스 제공이 가능하다. 또한, NFC 기술 특성상 실제 5cm 이내로 디바이스를 접근시켜야 서비스 이용이 가능하기 때문에, 물리적으로 일정 수준의 보안이 보장된다고 할 수 있다. 또한, NFC 기술 자체적으로 암호화 기능을 포함하고 있기 때문에 기존 모바일 서비스에 비해 안전한 모바일 통신이 가능하다. NFC 디바이스간 안전한 데이터 통신을 위해 우선적으로 비밀키 생성 및 키교환(SSE : Shared Secret Service)을 수행하고, 공유된 비밀키를 이용해 세션키를 생성하여 암호화 통신(SCH : Secure Channel Service)을 수행한다. 키교환 시 사용되는 알고리듬은 ECDH (Elliptic Curve Diffie Hellman) 이며, 암호화 통신 시 사용되는 알고리듬은 AES가 사용된다[6][7].

이외에도 안전한 Tag 기반 서비스 제공을 위해 인증서를 이용할 수 있도록 NDEF (NFC Data Exchange Format) Signature Record Type이 NFC 포럼을 통해 개발 되었다[8].

〔표 1〕 NFC 기능 및 이용 분야

구분	Card Emulation	Reader/Writer	P2P
특징	디바이스가 기존 신용카드의 기능 수행	디바이스가 기존 리더기 역할을 수행	두 대의 NFC 디바이스간 양방향 통신
분야	모바일 신용카드, 교통카드 등	스마트포스터, 스마트주문 등	명함교환, P2P 결제 등

2.2 NFC 표준 현황

NFC 관련 표준은 비접촉식 근거리 무선통신 기술 표준을 개발하는 ISO/IEC를 통해 13.56MHz 대역을 사용하고 10cm 이내의 근접형 거리에서 통신이 가능한 표준 개발을 시작으로 이루어졌다. ISO/IEC 14443이 바로 그 표준으로 우리가 잘 알고 있는 스마트카드에 적용되는 기술이다. 또한 동일한 주파수대역을 사용하며 인식거리가 약 1m 정도까지 가능한 ISO/IEC 15693 표준도 개발이 되었다. 하지만 실제적으로 NFC라는 용어를 사용하고 NFC 표준이라 불리는 표준은 2004년에 개발한 ISO/IEC 18092 표준이다. 본 표준은 ECMA(European Computer Manufacturers Association)에서 개발한 ECMA-340 표준(NFCIP-1)을 ISO/IEC 표준으로 제정한 것으로 NFC 인터페이스와 데이터 교환 프로토콜 등을 정의하고 있다. 주요 내용으로는 변조방식, 코딩방식, 전송속도(106~424 kbps) 및 데이터 충돌 제어 방식 등이 기술되어 있으며, Passive 및 Active 통신 모드를 정의하여 NFC 주요 특징이라 할 수 있는 Read/Write 모드, Card emulation 모드, P2P 모드 등이 사용될 수 있는 기반을 마련하였다. 2005년에는 기존 13.56MHz 대역을 사용하는 비접촉식 카드 표준 3가지를 포괄하는 ISO/IEC 21481을 개발하였다.

〔표 2〕 NFC 인터페이스 관련 표준 현황

구분	NFC 인터페이스	비접촉 근접식 (Contactless Proximity)	비접촉 원격식 (Contactless Vicinity)
표준명	ISO/IEC 18092 (NFCIP-1)	ISO/IEC 14443	ISO/IEC 15693
내용	NFC 디바이스간 통신을 위한 표준	비접촉 근접식 카드와 리더기간 통신 표준	비접촉 원격식 카드와 리더기간 통신 표준
ISO/IEC 21481 : NFCIP-2 (기존 NFC 인터페이스 관련 표준 통합)			

본 표준은 ECMA-352(NFCIP-2)를 적용하여 개발한 표준이다. ISO/IEC 21481 표준은 이전에 개발된 표준이 명시하는 모드를 모두 지원하고 있으며 해당 모드를 포괄하기 위한 통신 규약 및 모드 선택 과정 등이 기술되어 있다. 이외에도 테스트 방법을 정의하는 ISO/IEC 22536, 23917 등이 2005년도에 개발되었으며, 유선인터페이스와 NFC 디바이스간의 통신규약을 정의한 ISO/IEC 28361 표준이 2007년 개발되었다.

NFC 보안 관련 표준의 경우, 최초 NFC 표준 개발 시 고려하고 있지 않다가 무선통신 보안에 대한 중요성을 인식하고 2010년에 ISO/IEC 13157 표준을 개발하였다. 본 표준은 ECMA-385(NFC-SEC), ECMA-386 (NFC-SEC-01) 표준을 각각 ISO/IEC 13157-1, 13157-2로 개발하였다. ISO/IEC 13157-1은 NFC 보안 서비스 및 프로토콜을 정의하는 표준으로 SSE(Shared Secret Service)와 SCH(Secure Channel Service) 등의 보안 서비스, 프로토콜 메커니즘, NFC-SEC PDU 등을 정의하고 있다. 또한, ISO/IEC 13157-2 표준은 NFC 보안서비스(SSH, SCH) 적용 시 필요한 암호알고리즘 정의, 키 교환, 비밀키 생성, 데이터 암복호화, 데이터 Conversion 등의 방법을 정의한다.

ISO/IEC, ECMA를 통해 NFC 서비스 기반인 인터페이스 및 프로토콜 표준을 개발하였다면, 실질적으로 NFC 응용서비스 제공에 필요한 주요 기술은 NFC Forum을 통해 개발되었다. 노키아, 소니, 필립스를 중심으로 2004년 설립된 NFC Forum은 NFC 기술 발전 및 서비스 활성화를 위해 기존 표준을 기반으로 Card Emulation 모드, Read/Write 모드, P2P모드 등 실질적인 NFC 서비스에 필요한 기술명세서를 개발하였다.

주요 기술 명세서는 NDEF[9], NFC Forum Tag Type[10], Record Type Definition (RTD)[11], Protocol(LLCP[12], SNEP[13]) 등이 있다. NFC 보안 관련한 기술 명세서로는 NFC Tag 서비스 이용 시 Tag 데이터의 무결성 보장을 위한 NFC Signature RTD를 2009년에 개발하였다[8].

〔표 3〕 NFC 포럼 주요 기술 명세서(Specification) 현황

구분	기술명세서
Data Exchage Format	NFC Data Exchange Format(NDEF) Technical Specification
NFC Forum Tag Type	NFC Forum Type 1 Tag Operation Specification 1.1
	NFC Forum Type 2 Tag Operation Specification 1.1
	NFC Forum Type 3 Tag Operation Specification 1.1
	NFC Forum Type 4 Tag Operation Specification 2.0
Record Type Definition	NFC Record Type Definition (RTD) Technical Specification
	NFC Text Record Type Definition (RTD) Technical Specification
	NFC URI Record Type Definition (RTD) Technical Specification
	NFC Smart Poster Record Type Definition (RTD) Technical Specification
	NFC Generic Control Record Type Definition (RTD) Technical Specification
	NFC Signature Record Type Definition (RTD) Technical Specification
Protocol	NFC Logical Link Control Protocol (LLCP) 1.1 Technical Specification
	NFC Digital Protocol Technical Specification
	NFC Activity Technical Specification
	NFC Simple NDEF Exchange Protocol (SNEP) Technical Specification
	NFC Controller Interface (NCI) Candidate Technical Specification

Ⅲ. 국내 · 외 NFC 기반 모바일 서비스 현황

NFC 기술은 기존의 RFID 기술을 발전시킨 기술로써 기존 카드에뮬레이션 기능이외에도 읽기/쓰기 기능, P2P 기능 등을 통해 양방향 데이터 전송이 가능하기 때문에 모바일 결제 이외에도 교통, 항공, 극장, 박물관, 스포츠경기장 등 다양한 분야에서 서비스 제공이 가능하다. NFC 기반 서비스는 영국, 프랑스, 미국, 일본 등에서 시범 및 상용서비스를 제공하였으며, 한국에서는 2011년 11월부터 서울 명동지역에 NFC Zone을 설치

하고 3개월간 시범서비스를 추진하였으며 2012년에는 여수엑스포에 NFC 서비스를 제공 중에 있다.

3.1 국외 NFC 서비스 현황

국외 NFC 서비스 중 가장 대표적인 것은 구글에서 제공하는 구글 지갑(Google Wallet) 서비스이다. 구글 지갑 서비스는 2011년 5월부터 8월까지 뉴욕과 샌프란시스코를 우선적으로 하여 시범서비스를 추진하였으며, 2011년 9월부터 정식서비스를 출시하였다.

〔그림 2〕 구글 월렛 서비스 개념도
출처 : 구글 월렛 홈페이지

본 서비스는 서비스명에서 보면 알 수 있듯이 모바일 결제 서비스이며 쿠폰, 멤버십 등의 서비스가 부가적으로 포함 되어져있다. 서브웨이, 메이시스, 월그린, 아메리칸 이글 아웃 등 대형 백화점 및 체인점과 계약체결을 맺어 서비스를 제공하고 있다. 하지만 단일 종류의 NFC 폰(넥서스 S), 단일 이통사, 단일 신용카드 기반으로 서비스를 제공함에 따라 활성화 측면에서 어려움이 있으며, 올해 초 구글 월렛 서비스의 해킹 문제가 제기됨에 따라 서비스 활성화에 난항을 겪고 있다. 구글 월렛의 보안 취약성은 크게 두 가지로 볼수 있는데 루팅(해커가 만든 루팅 도구를 통해 스마트폰의 OS를 변경하여 최고 권한 획득 및 관리 가능)된 안드로이드 폰에서의 PIN 번호 유출 가능성과 구글 월렛 어플리케이션 자체에 대한 보안 문제이다. 첫 번째 보안문제의 경우 루팅 된 폰에서 PIN번호 해킹을 위한 프로그램 설치를 통해 PIN 번호 획득이 가능하지만, 두 번째 문제의 경우 별도의 해킹 프로그램 없이도 타인의 구글 월렛 계정을 이용하여 결제가 가능하기 때문에 문제가 더 심각하다. 이러한 보안문제의 제기로 구글이NFC 기반 모바일 결제 서비스 선도를 위해 야심차게 준비한 구글 월렛 서비스가 어려움을 겪고 있다.

이외에도 미국의 3대 이통사(버라이즌, AT&T, T모바일)에서 약 1억 달러 투자해 설립한 ISIS를 통해 NFC 기반 모바일 결제서비스를 진행하고 있다. 구글월렛과는 경쟁관계이며 2012년 상반기부터 솔트레이크시티, 텍사스 오스틴 등에서 NFC 기반의 모바일 결제 서비스 사업을 진행 중에 있다. 구글 월렛보다는 시기적으로 늦게 시작을 하였지만 미국 3대 이통사, 아메리칸 익스프레스 등 3개 신용카드사 및 다양한 단말기 제조업체(HTC, LG, 모토롤라, 림, 삼성, 소니에릭슨 등)의 참여를 이끌어내며 NFC 기반 모바일 결제 시장을 주도하기 위해 노력 중에 있다.

일본의 경우, 2004년부터 FeliCa 라는 자체 비접촉 통신기술을 기반으로 자국 내에서 '오사이후케이타이' 라는 모바일 결제 서비스를 추진하였으며, 약 90% 보급률을 보이며 크게 성공하였다. 하지만 '오사이후케이타이' 서비스는 피처폰 기반의 모바일 결제 서비스이기 때문에 해당 서비스를 제공했던 NTT 도코모에서는 NFC기반 서비스로 전환을 추진 중에 있다.

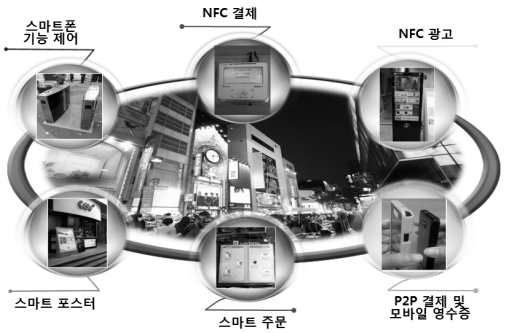
영국에서는 2012년 런던 올림픽에 NFC 기반 모바일 결제 서비스 범용화를 위해 O2 등 영국 이통사를 중심으로 2011년부터 NFC 기반 모바일 결제 서비스를 준비하였으며, 교통, 소매체인점, 올림픽 경기장 주변 등에 약 6만여 개 결제 단말기를 설치하고 NFC 기반 모바일 결제 및 응용 서비스를 제공하고 있다. 또한, 2011년 8월에는 Nokia 기술을 이용하여 런던 박물관내의 전시품 정보, 티켓구매, 소셜 서비스 등을 이용할 수 있는 NFC기반 서비스를 제공하였다. 프랑스에서도 2010년 5월부터 니스 지역에서 Cityzi 라는 프로젝트를 통해 NFC 기반 모바일 서비스를 제공하고 있다. 다른 국가의 프로젝트와는 달리 프랑스에서는 정부기관 및 시의회가 적극 참여하고 있다.

〔그림 3〕 NFC 기반 모바일 서비스(Cityzi 프로젝트)

이외에도 유럽, 아시아 등의 여러 국가에서 NFC 기반 모바일 서비스 개발 및 구축에 많은 노력을 기울이고 있다.

3.2 국내 NFC 서비스 현황

국내 NFC 기반 모바일 결제 서비스는 2011년 11월 방송통신위원회, KISA가 중심이 되고 3개 이통사, 11개 신용카드사, VAN사 등이 참여하여 추진한 명동 NFC 존 시범사업이 최초 서비스라 할 수 있다. 2011년 초반부터 명동 NFC존 시범사업 추진을 위한 기술 개발, 가맹점 확보, 결제 단말기 개발 및 구축 등을 통해 명동 지역 주요 200여개 가맹점(편의점, 화장품 매장, 커피숍, 음식점, 패스트푸드 매장 등)에서 NFC 디바이스 기반 모바일 결제 상용 서비스를 약 3개월간 제공하였으며 현재까지도 편의점, 주유소, 대형마트 등 전국 체인점에서도 NFC 기반 모바일결제 서비스 이용이 가능하다. 또한, 모바일 결제 서비스 이외에도 NFC 기반 모바일 주문, 버스도착 정보 제공, 모바일 광고, 입출입 통제 등 다양한 Tag 기반 시범서비스도 추진하였다[3].



〔그림 4〕 명동 NFC 존 주요 서비스

2012년 1월부터는 방통위와 여수 세계엑스포조직위원회가 업무협약을 통해, 여수세계엑스포내에서 NFC 기반 결제 서비스 및 Tag 서비스 제공을 위한 기술 개발 및 구축을 추진하였으며, 2012년 5월부터 3개월간 NFC 기반 상용서비스를 추진하고 있다.

이렇듯 국내에서는 정부와 민간이 협력하여 NFC 기반 서비스 활성화에 많은 노력을 기울이고 있다. 향후 NFC가 탑재된 디바이스가 보급 확산되고 교통카드 등과 같은 생활 밀착형 킬러서비스가 개발될 경우 수년내에 NFC기반 서비스가 대중화 될것으로 생각된다. 국외 리서치 업계에서도 2016년에는 NFC 결제 서비스가 대중화가 이루어질 것이며 휴대전화의 약 50%가 NFC가 탑재된 스마트폰이 될 것이라고 전망하고 있다. 또한, Gartner에서는 NFC기반 결제건수가 2010년 3억 1,6000만 건에서 2014년 35억 7,200만 건으로 11배 이상 증가할 것으로 전망하고 있다[3].

이에 따라, 국내에서도 이통3사를 중심으로 NFC 기반 모바일 결제 및 응용서비스 활성화를 위해 적극 노력하고 있으며, 현재 이통3사 모두 모바일 지갑 서비스를 제공하고 있다. 또한, SKT의 경우 2011년에 NFC 내장 USIM카드를 자체 기술로 개발하였으며, 2012년에는 일본 이통사 KDDI와 함께 모바일 아시아 엑스포(MAE) 2012에서 현재 인천 문학구장에서 상용화되어 있는 NFC 티켓서비스를 시연하였다. 또한 중국 차이나 모바일과도 NFC 기반 모바일 결제 서비스에 대해 협력하기로 하였다. KT는 일본 NTT 도코모와 협력을 통해 2012년 4월부터 NFC 로밍 서비스를 추진하고 있다. 국내 사용자가 일본에 가서 쿠폰을 통한 할인 및 결제가 가능한 서비스로 내년까지 양국 간의 다양한 상호 로밍 서비스가 제공 될 예정이다. LGU+에서는 기존 스마트카드 형태의 출입증을 NFC 기반 출입증으로 전환하는 사업을 추진중에 있으며, 2012년 10월 시범운영할 예정이다. 또한, LG Tag+를 통해 자동차, 사무실, 수면 시 필요한 기능을 활성화 시켜주는 서비스를 제공 중에 있다. 예를 들어, 자동차내에서 NFC Tag를 접촉하면 운전에 필요한 네비이게이션, GPS, 블루투스 등이 자동으로 실행되는 방식이다.

이와 같이 국외 뿐 아니라 국내에서도 NFC기반 모바일 서비스에 대한 관심과 기대가 높다. NFC 기반 서비스는 현재 개발 및 적용된 서비스 이외에도 의료, 항공/철도, 자동차, 스포츠, 게임, 티켓 등 우리 일상생활에 필요한 다양한 산업 분야에 적용할 수 있기 때문에 지금보다는 미래가 더 기대되는 기술이라 할 수 있다.

Ⅳ. NFC 기반 모바일 서비스 보안 위협 및 취약성

NFC 기술 표준에 보안기능이 포함되어 있고 실질적으로 5Cm 이내의 짧은 거리에서 사용이 되기 때문에 기존 모바일 결제 및 RFID 서비스에 비해 보안성이 높다는 것은 사실이지만, 응용서비스의 특성, 어플리케이

션 자체 취약성, Tag 보안 취약성, 스마트폰 사용자의 관리 소홀 등 전방위적인 보안 위협 대책이 마련되어야 비로소 안전성이 보장된 NFC 기반 서비스 제공이 가능하다. NFC기술 자체의 보안성만을 신뢰하고 그 외의 보안 취약성을 간과할 경우 NFC 기반 서비스가 대국민 서비스로 확산된 이후의 피해규모는 가히 상상을 초월할 수 있을 것이다. 특히, NFC 기반 서비스의 주축이 모바일 결제임을 고려한다면, 최근 사회적으로 큰 문제로 부각되고 있는 대기업의 개인정보 유출보다 국민들이 체감하는 피해수준은 보다 직접적이고 높을 것으로 예상된다. 이는 비단 NFC 기반 서비스에 국한되는 것이라 향후 우리 일상생활에 일부가 될 모바일 디바이스 기반 서비스에 대한 보안 문제와도 일맥상통한다고 할 수 있다.

4.1 무선(RF) 통신 구간에서의 보안 위협

NFC 기술은 기존의 RFID기반으로 개발되었기 때문에 기본적으로 RF 통신 기반으로 서비스가 제공된다. 이에 따라, 기존 무선 통신 상에서의 위협들이 NFC 기술에도 동일하게 적용 된다고 할 수 있다. 특히, NFC 기반 모바일 결제 서비스의 경우 RF 통신을 통해 계좌정보, 비밀번호, 쿠폰정보 등 민감한 정보들이 전송되기 때문에 해당 보안 위협에 대한 대책은 매우 중요하다. RF 통신 보안 위협에는 도청, 데이터 손상, 데이터 위변조, 중간자(Man-in-the-middle) 공격 등이 대표적이라 할 수 있다. 또한, 기존 ISO/IEC 14443 비접촉식 스마트카드 기반 서비스의 경우 디바이스간 Relay attack이 가능하다[14][15].

데이터 도청의 경우 Passive mode에 비해 Active mode에서 쉽게 이루어질 수 있다. 물론 도청을 위해서는 공격자의 안테나, 리시버, RF 신호 디코더 등이 준비되어야 하며 각 기기에 대한 성능에 따라 도청의 범위가 결정된다. 일반적으로, Active mode의 경우 약 10m 범위 내에서 도청이 가능하며, Passive mode는 이보다 약 10배 정도 거리가 감소된다[16]. 이는 기존 부채널 공격 시 스마트폰 CPU의 전력 사용 정보를 10m 내외의 거리에서 도청하는 것과 유사하다고 할 수 있다.

데이터 손상의 경우 데이터 위변조와는 달리 전송되는 데이터를 수신자가 이해하지 못하게 하는 것으로 데이터 스펙트럼의 정확한 전송 주파수만 알 수 있다면 가능하다. 데이터 손상 공격의 경우 전송되는 데이터가 유효한 데이터가 아니기 때문에 단순 서비스 거부 공격(DoS)의 일종이라 할 수 있다.

데이터 위변조 위협은 위의 위협들에 비해 발생확률이 적고 공격도 어렵긴 하지만 실제 유효한 변조된 데이터가 전송되기 때문에 피해는 심각할 수 있다. 데이터 위변조 공격이 가능하기 위해서는 인코딩 방식 및 데이터 변조 방식(100% ASK, 10% ASK 등)에 따라 공격 가능성이 달라진다. 이러한 위협들 때문에 일반적으로 NFC 기술이 근접한 거리에서 데이터를 송수신하기 때문에 안전하다고 믿는 것은 잘못된 생각이다. 특히, NFC 기반 모바일 서비스 이용 시 비밀번호, 계좌정보, 신원확인 정보 등 주요한 개인정보가 전송되기 때문에 무선 통신 구간에서의 보안에 더욱 신경 써야 할 것이다.

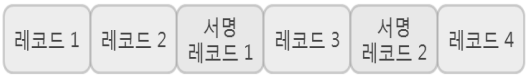
4.2 어플리케이션 보안 위협

일반적으로 NFC 기술은 NFC 컨트롤러 칩, Secure Element, 안테나 등 하드웨어를 기반으로 동작된다. 하지만 모바일 결제, 신분증, 도어락, 스마트 주문 등 다양한 응용서비스를 위해서는 어플리케이션이 반드시 필요하다. 그리고 해당 어플리케이션을 어떻게 개발하느냐에 따라 보안 위협의 강도는 차이가 클 수밖에 없다. 일례로, 2011년 9월 구글이 구글 월렛 상용서비스를 시작하고 얼마 지나지 않아 보안성 문제에 제기되 어려움을 겪었었다. 보안 취약점은 크게 두가지 인데 하나는 루팅된 안드로이드 폰에서 비밀번호 해킹 프로그램 설치 후 PIN 번호를 유출할 수 있다는 것이고, 다른 하나는 스마트폰 분실, 도난 시 이전 사용자의 구글월렛 선불카드를 이용하여 결제가 가능하다는 것이다. 안드로이드 폰을 루팅하여 발생하는 보안 위협은 이미 아이폰 탈옥 시에 발생하는 문제와 유사하고 이미 어느 정도 인지하고 있는 것이고, 사용자 선택에 따라 이루어지는 것이기 때문에 어쩔 수 없다 해도, 어플리케이션 구현 상의 실수로 인해 모바일 결제 서비스에서 존재해서는 안되는 오류를 범한 것은 문제라 할 수 있다. 특히, 습득한 스마트폰의 어플리케이션 메뉴에서 구글월렛 어플리케이션을 찾아 관련 정보를 삭제하고 다시 구글월렛을 구동하면 초기화가 되면서 패스워드 재입력이 가능하고 이를 통해 새로운 패스워드로 이전 사용자의 선불카드 이용이 가

능하다는 점은 해당 어플리케이션 구현상의 문제라고 할 수 있다. 이렇듯 NFC 기반 모바일 서비스는 결제 정보나 주요한 개인정보를 다루기 때문에 해당 어플리케이션 구현 시 개인정보 입력 시부터 저장, 이용 등 데이터 관리의 전반적인 부분에 대해 보안 취약성을 최소화하여야 한다. 만약, 이러한 어플리케이션 보안 취약성을 간과할 경우 최근 크게 이슈가 되는 개인정보의 유출 뿐 아니라 서비스 이용자에게 직접적인 금전적 피해까지 발생 시킬 수 있다. 사소한 코딩 문제나 어플리케이션 관리 문제로 인해 보안 사고가 발생할 경우 피해보상도 문제지만 해당 보안 사고로 인한 기업 이미지 손실은 금액으로 환산할 수 없을 정도가 될 수도 있기 때문에, 어플리케이션 개발 초기부터 보안에 각별히 유념하여 서비스를 준비하는 것이 투자비용 대비 효과가 가장 높다.

4.3 Tag 서비스 보안 위협

현재 NFC 기반의 모바일 서비스는 모바일 결제, 쿠폰, 멤버십 등 주로 결제 분야에 주로 적용되어져 있지만, 향후에는 Tag 기반의 서비스가 활성화 될 것으로 예상된다. Tag 기반 서비스란 영화관, 음식점, 카페, 버스정류장 등 누구나 손쉽게 접근할 수 있는 장소에서 간단한 태깅만으로 예약, 주문, 정보 확인 까지 가능한 서비스를 말한다. 일상생활에 편리함을 줄 수 있는 서비스에 많이 적용될 수 있다. Tag 기반 서비스를 위해서는 물리적으로 Tag가 필요하며 NFC Tag의 종류에는 4가지가 있다[10]. 각 종류별로 메모리 크기, 호환성이 각기 다르기 때문에 서비스 특성에 맞게 Tag 선택이 필요하다. 이러한 Tag 기반 서비스에서 Tag와 스마트 디바이스간의 데이터 교환 시 필요한 규격은 NFC Forum에서 제공하는 NDEF(NFC Data Exchange Format) 규격[9]과 RTD(Record Type Definition) 규격[11] 등이다. RTD에는 텍스트 RTD, URI RTD, 스마트포스터 RTD 등이 있으며, 보안 관련 규격은 이전에는 존재하지 않다가 2009년에 NFC 서명 레코드 타입(Signature Record Type Definition) 규격을 제정하였다. NFC Forum의 보안 관련 규격은 이것이 유일하다. 하지만 NFC 서명 레코드 타입 규격은 Optional 규격으로 실제 필드에서는 거의 적용이 되지 않고 있으며, 또한 본 규격 자체에도 Tag 정보가 위변조 될 수 있는 취약점이 존재한다[17].



- 서명 레코드 1 : 레코드 1, 2에 대한 서명
- 서명 레코드 2 : 레코드 3에 대한 서명
- 레코드 4 : 무서명 레코드

〔그림 5〕 서명 레코드가 포함된 NDEF 메시지 형태

해당 규격에서 NDEF 메시지 서명 시 모든 필드를 서명하는 것이 아니라 일부 필드만 서명하도록 규정하고 있고, 복수개의 레코드를 포함한 NDEF 메시지 서명 시 복수의 인증서로 서명이 가능하다[18].

〔표 4〕 NDEF Records 서명 방식

필드명	서명여부
Message Begin (MB)	×
Message End (ME)	×
Chunk Flag (CF)	×
Short Record Flag (SR)	×
ID-length present Flag (IL)	×
Type Name Format (TNF)	×
Type-length	×
Payload-length	×
ID-length	×
Type	○
ID	○
Payload	○

Tag 기반 서비스 적용 시 Tag 정보 보호를 위한 기술을 적용하지 않을 경우 쉽게는 실제 서비스에 접근할 수 없게 하는 서비스 거부공격(DoS)이 가능하며 그 외에도 URI 스푸핑, 웜 바이러스 유포, Fishing 등을 통한 개인정보 유출도 가능하다. 향후 Tag 기반 상용서비스가 활성화될 경우 해당 취약성 기반으로 공격도 증가할 것으로 예상된다.

4.4 디바이스 도난/분실에 따른 위협

최근 NFC가 전 세계적으로 각광받고 있고 관심의 대상이 되는 이유는 PC 수준의 연산능력을 보유하고 있고 언제 어디서나 항상 지니고 다니는 이동성과 편리성을 가지고 있는 스마트폰이 있기 때문이다. 이에 따라, 언제 어디서나 이용자가 위치한 곳에 적합한 서비스를 제공함에 따라 이용자의 경우 편리함을 제공해 줄 수 있다. 하지만 반대로 생각하면 개인의 중요한 정보들이

쉽게 외부에 노출된다는 위험도 동시에 존재한다. 그러므로 기존 PC 보다 외부 노출에 따른 보안 대책에 많은 고민이 필요하다. 현재 상용 서비스 되거나 될 예정인 서비스만 보아도 이용자의 금전이 오가는 결제/쿠폰 서비스, 집・회사・호텔 등에서의 출입통제 서비스, 티켓 주문/예약 서비스, 자동차 도어락 서비스 등이 있으며, 앞으로 점점 더 많은 서비스들이 이용 가능할 것으로 보인다. 이에 따라, 스마트폰의 분실, 도난(향후 도난 사고 급증 예상)에 따른 피해가 지금의 개인정보 유출 사고보다 더 큰 피해를 가져올 수도 있다. 스마트폰을 분실/도난당할 경우에는 신용카드, 쿠폰, 자동차키, 사무실/집 키 등을 동시에 잃어버린 것과 같은 피해가 발생하는 것이다. 조금의 편리함을 위해 보안을 고려하지 않기에는 이제는 너무나 큰 위협들이 존재한다.

Ⅴ. NFC 기반 모바일 서비스 보안 대책

앞 장에서 언급했던 것처럼 NFC 기반 모바일 서비스에서는 무선(RF)통신 구간부터 어플리케이션, Tag, 물리적 위협 등 많은 부분에서의 보안 위협이 존재한다. 이러한 보안위협에 대처하기 위해서는 기술적인 대응 방안 뿐 아니라 제도적인 대응 방안도 반드시 필요하다. 특히나 보안 위협들이 사용자의 부주의에 의해서 발생한다는 것은 최근 PC 기반 유선 서비스에서도 많이 강조되고 있다. 더욱이 무선기반 서비스에서는 스마트 디바이스가 가지고 있는 환경적 요소(항시 휴대)까지 더해지기 때문에 제도적으로 사용자의 보안 위협을 최대한 감소시켜주는 것이 중요하다고 할 수 있다. 대부분의 사용자들은 작은 불편함에도 사용을 꺼리는 특징이 있기 때문에, 제도적으로 안전성을 담보하기 위한 보안 대책 마련이 필요하다.

5.1 무선(RF) 통신 구간에서의 보안 대책

앞에서 언급했듯이 NFC 서비스 이용을 위한 실제 접촉 거리는 5cm 미만으로 아주 근접하지만 전송되는 정보를 도청하는 것은 최대 10m 거리에서도 가능하다. 이에 따라, 사용자의 민감한 정보(계좌정보, 비밀번호, 개인정보)를 보호하기 위해서는 무선 채널 암호화가 필요하다. 이를 위해서는 우선 RSA 또는 EC 기반의 Diffie-Hellmann 프로토콜을 통한 키 교환이 필요하고, 이후 AES 기반 암호키를 통해 암호화 통신을 수행할 수 있다. 현재 NFC 표준에서는 ECDH P-192를 통한 키 교환(SSE : Shared Secret Service) 후 AES 128 알고리즘을 통한 암호화(SCH : Secure Channel Service)를 수행하도록 하고 있다. 무선 통신 채널 암호화 방식 이외에도 NFC 콘트롤러 칩이나 SE(Secure Element)가 존재하는 USIM 등이 부채널 공격에 안전하도록 사전에 보안성을 고려한 칩 디자인이 필요하다. 하지만 이미 출시되고 사용되는 칩을 사용할 경우에는 칩의 보안기능을 이용하는 어플리케이션 개발 시 도청이나 부채널 공격에 노출되지 않도록 설계 단계부터 코딩, 디버깅 시까지 보안을 고려한 구현이 필요하다.

5.2 어플리케이션 보안 대책

모바일 결제, 출입통제, 티켓 예매 등 NFC 기반 모바일 서비스 제공 시 반드시 필요한 것은 해당 서비스를 위한 어플리케이션이다. 이에 따라, 물리적으로 보안 기능이 적용되어져 있다 해도 어플리케이션 자체에 취약성이 존재한다면 해당 보안기능이 무용지물이 될 수 있다. 구글 월렛 개인정보 유출 사고 역시 어플리케이션 구현 문제에서 비롯되었다고 할 수 있다. 따라서 민감한 정보를 입력할 때 사용하는 입력장치 보안 기능, 입력된 정보를 저장/관리하는 데이터 DB 관리 기능, 유효한 어플리케이션만이 NFC 칩이나 SE에 접근하도록 하는 기능, 개발된 어플리케이션 배포 이전에 보안 기능 구현 여부 검증, 어플리케이션 자체에 대한 보안 잠금 기능 등 다양한 보안요소가 고려되어야 한다. 특히, 많은 어플리케이션에서 사용자의 정보(민감한 정보 포함)를 스마트 디바이스 자체 저장 장치에 저장하도록 구현되어져 있는데, 민감한 데이터는 암호화하여 USIM 등과 같이 SE가 위치하고 있는 곳에 저장/관리하는 것이 필요하다. 또한, 공신력 있는 기관에서 구현된 어플리케이션에 대한 보안 기능 구현 적합성을 검증할 수 있는 제도적인 대책 마련도 필요하다. 또한, 서비스 제공자는 어플리케이션 배포 시 사용자가 유효한 어플리케이션인지 확인할 수 있는 기능을 제공하여야 하며, 사용자는 사전에 어플리케이션이 적합한 서비스 제공자로부터 배포되는 것인지 확인하고 이용하여야 한다.

5.3 Tag 서비스 보안 대책

Tag 기반 서비스는 향후 수년 내에 다양한 산업 분야에서 가장 널리 사용될 NFC 기반 모바일 서비스 중에 하나이다. Tag 기반 서비스에 적용되는 Tag에는 해당 서비스에 접근하기 위한 중요한 정보들이 저장되어 있기 때문에 해당 정보에 대한 위변조 위협으로부터 보호를 해야 한다. 그렇지 않을 경우 앞장에서 언급한대로 DoS 공격, Fishing 공격, 웜바이러스 유포 등의 위협이 존재한다[19]. 이러한 위협들로부터 보호하기 위해서는 우선적으로 정보의 무결성이 보장되어야 하며 이를 위해 Tag 서비스 제공자가 Tag내의 정보를 서명하여 원본 데이터와 함께 서명문을 Tag에 저장하여야 하며, 서비스 이용 시 해당 서명 검증을 통해 정보의 무결성을 검증할 수 있도록 하여야한다[20]. 이를 위해 NFC 포럼에서 Signature Record Type Definition 규격[8]을 개발하였지만 4.3절에서 언급한대로 보안 취약성을 가지고 있다. 따라서 국내에서만이라도 Tag 기반 서비스 적용 시 Signature Record Type을 사용하도록 제도적으로 권고 노력이 필요하다. 또한 기술적으로 현재 규격은 Tag의 제한된 메모리를 고려하여 서명문의 길이를 최소화하기위해 ID, Type, Payload 필드만 서명하도록 규정하고 있으나, 이럴 경우 공격자로 하여금 서명은 유효하지만 Tag내의 데이터를 의미없게 하거나, 원하는 데이터를 삭제할 수 있는 공격이 가능하다[17]. 이러한 공격을 방지하기 위해서는 최소한 Type-Length 필드와 ID-Length 필드를 추가로 서명에 포함하여야 한다[18]. 또한, Tag의 메모리 용량을 고려하여 서명문의 길이, 서명검증 시간, 인증서 길이 등을 고려한 보안 대책 마련도 필요하다. X.509 기반 RSA 인증서의 경우 서명 시간이 길고 인증서 크기가 크기 때문에 이에 대한 대안이 필요하다[21]. 이를 위해 인증서를 Tag 내에 보관하지 않고, 제3의 신뢰기관에 인증서를 보관하고 있다가 검증 시 사용하는 방안도 사용 가능하다. 이는 단순 NFC서비스 뿐 아니라 모바일 디바이스 기반의 인증서비스 이용 시 필요한 방식으로 다양한 분야에 적용 가능할 것으로 생각된다. 이와 관련한 세부 프로토콜에 대해서는 본 논문에서 논외로 한다. 또한, 기존의 X.509 기반 인증서[22]를 모바일 서비스에 적합하도록 인증서 필드를 경량화 하는 방안 연구도 필요하다.

5.4 제도적 보안 대책

스마트 디바이스 분실/도난 등 물리적인 위협에 대한 보안 대책으로는 기술적 대책보다는 제도적 대책 마련이 필요하다. NFC 기반 모바일 결제 서비스의 경우 스마트 디바이스를 켜지 않아도 바로 결제가 가능하기 때문에 모바일 결제 서비스(교통카드 포함) 제공 시 반드시 리더기에서 PIN 인증 또는 이와 유사한 보안 기능을 제공하도록 제도적 장치를 마련해야 한다. 또한, 쿠폰/멤버십, P2P 서비스, Tag 기반 서비스 이용 시 정당한 사용자 이외에는 사용이 어렵도록 각 어플리케이션별 PIN 설정을 의무화 하는 방안도 고려해야 한다. 또한, 사용자들의 보안 인식제고 노력을 통해 스마트 디바이스 자체에 대한 PIN 설정도 강력하게 권고해야 한다. 4.2절에서 언급한 구글월렛의 PIN 유출 위협 중에 하나인 안드로이드 기반 디바이스에 대한 루팅 문제에 대해서도 지속적인 사용자 인식제고를 통해 개선해야 하며, 추가적으로 루팅된 디바이스에서는 NFC 기반 어플리케이션의 동작을 제안해야 한다. 향후 스마트 디바이스의 용도가 늘어나면 늘어날수록 도난/분실 사고에 따른 1차적인 피해보다 이를 악용한 2차적인 피해가 훨씬 심각할 수 있기 때문에 기술적인 대책 마련과 동시에 제도적인 대책 마련이 시급하다. 또한, NFC 기반 서비스의 경우 모바일 결제, 쿠폰/멤버십 서비스, 스마트 포스터, 스마트 주문, 출입통제 등 이용자의 개인정보의 이용이 많은 분야에 적용이 되기 때문에 각 서비스별로 개인정보보호를 위한 제도적 대책 마련도 필요하다. 이를 위해, NFC 서비스 제공 시 필요한 개인정보 생성·관리를 특정 서비스 제공 업체가 아닌 신뢰된 제3기관에서 분산 관리할 수 있도록 관련 제도를 마련해야 한다[23].

Ⅵ. 결 론

작년부터 불기 시작한 NFC 기반 모바일 서비스의 관심이 수년 내에 국내 뿐 아니라 국제적으로 가장 널리 사용되는 모바일 서비스의 하나로 자리매김 할 것으로 예측된다. 이는 국외 리서치 업계로부터 이미 검증 받은 사실이며, 대부분의 리서치 업계에서 2016년에는 전 세계 약 50%가 NFC가 탑재된 스마트 디바이스를 사용할 것으로 내다봤다. 하지만 이러한 급격한 모바일 이용 환

경의 변화 속에 보안에 대한 관심을 소홀히 할 경우 이에 따른 피해가 상상을 초월할 것이라는 사실은 자명하다. 이에 따라, NFC 칩 개발단계부터 어플리케이션 개발, NFC 기반 서비스별 이용 환경 구축(데이터 DB 관리, 개인정보 관리, Tag 정보 관리 등), 사용자 인식제고 등 NFC 기반 모바일 서비스 제공에 필요한 각 요소별 보안 대책 마련이 필요하다. 현재 국내 및 국외에서 추진되고 있는 NFC 기반 모바일 서비스의 경우 해당 서비스 활성화에 초점을 맞추어 추진하고 있는 것으로 보인다. 물론 초기에는 서비스 활성화가 우선적으로 필요하지만 구글월렛 사건에서도 보듯이 활성화 후 발생할 수 있는 보안 사고를 고려할 때 이에 대한 보안대책 마련도 병행해야 한다. 본 논문에서는 무선(RF) 통신 구간, 어플리케이션, Tag 서비스, 도난/분실 등 물리적 보안 위협 등에 대해 설명하고 이에 대한 보안대책을 제시하였다. 하지만, 추가적인 연구가 필요한 사항은 각 보안 대책에 대한 실질적인 프로토콜이나 구현 결과에 대해서 제시하는 것이다. 이에 따라, 향후 각 서비스별 기술적 보안 대책에 대한 구체적인 프로토콜 연구 및 구현을 통해 실효성 있고 실현가능한 보안 대책 마련이 필요하며, 이와 더불어 NFC 기반 모바일 서비스의 안전한 이용을 위한 제도적 가이드라인 연구도 필요하다. 특히, NFC 기반 모바일 서비스의 경우에는 기술적 보안 대책과 제도적 보안 대책이 공존할 때만이 사용자에게 편리성과 보안성을 모두 만족시킬 수 있는 서비스가 될 수 있을 것이다.

참고문헌

[1] ISO/IEC 18092:2004 Near Field Communication Interface and Protocol(NFCIP-1), ISO/IEC, 2004.

[2] ECMA-340 : Near Field Communication Interface and Protocol(NFCIP-1) 2nd Edition, ECMA, 2004.

[3] 백종현, “NFC 기반 시범서비스 추진 현황”, TTA NFC 표준기술전략 세미나, 2011.

[4] ISO/IEC 21481:2005 Near Field Communication Interface and Protocol-2 (NFCIP-2), ISO/IEC, 2005.

[5] ECMA-352 : Near Field Communication Interface and Protocol-2(NFCIP-2), ECMA, 2005.

[6] ECMA-385 : NFC-SEC : NFCIP-1 Security Services and Protocol 2nd Edition, ECMA, 2010.

[7] ECMA-386 : NFC-SEC-01 : NEC-SEC Cryptography Standard using ECDH and AES 2nd Edition, ECMA, 2010.

[8] NFC Signature Record Type Definition, NFC Forum Technical Specification, 2010.

[9] NFC Data Exchange Format(NDEF), NFC Forum Technical Specification, 2006.

[10] NFC Forum Tag Type Tag Operation Specification, NFC Forum Technical Specification, 2007.

[11] NFC Record Type Definition(RTD), NFC Forum Technical Specification, 2006.

[12] NFC Logical Link Control Protocol(LLCP) 1.1, NFC Forum Technical Specification, 2011.

[13] NFC Simple NDEF Exchange Protocol(SNEP), NFC Forum Technical Specification, 2011.

[14] M.Weib, “Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment,” Masters Thesis in Computer Science, 2010.

[15] Lishoy Francis, Gerhard Hancke, K. M., “Practical NFC Peer to peer Relay Attack using Mobile Phones,” Workshop on RFID Security-RFIDSec'10, 2010.

[16] E. Haselsteiner, K. Breitfub, "Security in Near Field Communication(NFC), Workshop on RFID Security RFIDSec, 2006.

[17] M. Roland, J. Langer, J. Scharinger, “Security Vulnerabilities of the NDEF Signature Record Type,” Third International Workshop on NFC, 2011.

[18] M. Q. Saeed, Colin D. Walter, “A Record Composition/Decomposition Attack on the NDEF Signature Record Type Definition, 6th International Conference on Internet Technology and Secured Transactions, 2011.

[19] C. Mulliner, “Vuluerability Analysis and Attacks on NFC-enabled Mobile Phones,” International Conference on Availability, Reliability and Security, 2009.

[20] M.Kilas, “Digital Signatures on NFC tags, Masters of Science Thesis, 2009.

[21] T. Rosati, G. Zaverucha, "Elliptic Curve Certificates and signatures for NFC Signature Records, RIM, Certicom Reseatch, 2011.
[22] R. Housley, T. Polk, W. Ford, and D Solo, “RFC3280 : Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile, IETF, 2002.
[23] NFC 개인정보보호 대책 연구, KISA. 2011.

〈著者紹介〉

백 종 현 (Jonghyun Baek)
정회원

1996년 2월 : 순천향대학교 전자공학과 졸업
1998년 2월 : 순천향대학교 전자공학과 석사
2008년 9월~현재 : 순천향대학교 정보보호학과 박사과정
2001년 4월 ~ 현재 : KISA 스마트인터넷팀장(‘11~’12), 무선인터넷팀장(‘10~’11), 전자인증팀장(‘08~’09)
2009년 2월 ~ 현재 : ITU-T SG17 Q6 의장(Rapporteur)
<관심분야> NFC 보안, PKI, 무선랜 보안, 무선인터넷 등

염 흥 열 (HeungYoul Youm)
종신회원

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 2월 : 한양대학교 전자공학과 석사
1990년 2월 : 한양대학교 전자공학과 박사
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사, 상임부회장, 회장(2011) 역임, (현) 명예회장
2004년 1월~현재 : 한국인터넷정보학회 이사, 논문지 편집위원
2004년 1월~현재 : OSIA 이사
2003년 9월~2004년 3월 : ITU-T SG17/Q10 Associate Rapporteur 부의장
2004년 3월~2008년 12월 : ITU-T SG17/Q9 Rapporteur
2009년 1월~현재 : ITU-T SG17 부의장
2006년 11월~2009년 2월 : 정보통신부 정책자문단 정보보호 PM
<관심분야> 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안