http://dx.doi.org/10.14400/JDC.2016.14.12.183

NFC 서비스 보안 위협 분석 및 대응방안 연구

김형욱, 김형주, 강정호, 전문석
숭실대학교 컴퓨터학과

A Study on Analysis and Countermeasure of Security threat in NFC

Hyung-Uk Kim, Hyung-joo Kim, Jung-ho Kang, Moon-seog Jun
School of Computer Science & Engineering, Soongsil University, Seoul, Korea

요 약 최근들어 스마트폰에서 NFC 기능을 지원함에 따라 스마트폰을 정보의 송·수신을 위한 매개체로 활용하여 결제, 의료, 개인인증 등 다양한 분야에서 융·복합된 형태의 서비스로 NFC 서비스가 전개되고 있다. 또한 기존 서비스에 NFC 기술이 융합됨에 따라 기존 서비스 구조에서 찾아볼 수 없던 신규 사업자가 기존 서비스에서 취급되던 개인정보를 취급하거나 기존 사업자가 NFC 사업자로 전환됨에 따라 기존에 취급하던 개인정보 이외의 다양한 개인정보를 취급할 수 있다. 이러한 서비스적 배경 및 시대적 배경을 바탕으로 NFC서비스 환경을 구축하기 위해 보안위협 분석 및 대응방안을 마련하고자 한다.

주제어 : 비접촉식 근거리 무선 통신 기술, 무선 주파수 인식 기술, 취약점, 모바일, ISO/IEC표준

Abstract Most recent trend reveals broader state of provision of NFC service as NFC technology was applied on smartphones which has become core communication tools by providing integrated services such as payment, medical, and personal authentication. Moreover, with integration of original service and NFC technology, new service providers now can handle personal information of original service or can handle other personal information with transition of previous service provider to NFC service provider. Considering current state of security industry along with NFC technology and service, we would like to analyze current stage of security threats and plan the counter strategies to create NFC service structure.

Key Words : Near Field Communication, Radio Frequency Identification, Vulnerability, Mobile, ISO/IEC standard

1. 서론

최근 인터넷의 발달로 새로운 IT 신기술과 다양한 서비스들의 등장에 따라 신규 IT시장을 기반으로 하는 서비스가 형성되고 있다.

NFC(Near Field Communication)은 비접촉식 근거리 무선 통신 기술로 스마트 단말기와 같은 모바일 단말기에 쉽게 적용할 수 있어 스마트 단말기 보급 확대와 국내외 기업, 정부등의 참여를 통해 시장이 급격하게 성장 할 것으로 전망된다.

이러한 NFC서비스는 NFC사업자가 서비스 제공 시 다양한 정보에 대한 분석을 통하여 맞춤형 서비스가 제

Received 26 September 2016, Revised 31 October 2016
Accepted 20 December 2016, Published 28 December 2016
Corresponding Author: Moon-seog Jun(School of Computer Science & Engineering, Soongsil University, Seoul, Korea)
Email: mjun@ssu.ac.kr

ISSN: 1738-1916

공될 경우 다양한 정보의 취급이 증가하고 있는 추세이다.

따라서 NFC의 보안 위협 분석 및 대응방안을 연구하여 향후 안전한 NFC 서비스 제공이 이루어 질 수 있도록 보안위협 분석 및 대응방안에 대한 연구가 필요하다.

2. NFC 개요

2.1 NFC 등장배경

NFC는 13.56MHz 대역 비접촉식 근거리 무선 통신 기술을 의미한다. 2002년 소니와 NXP에 의해 개발되었고 2003년 NFC 통신규격에 대한 국제표준제정(ISO/IEC 18092)과 2004년 NFC Forum의 설립으로 그 용어가 공식적으로 정의되었다. 그러나 NFC기술 이전에도 RFID(Radio Frequency Identiciation)라는 무선주파수 인식 기술이 보급되고 사용되고 있었다. RFID의 경우 인식에 초점을 둔 기술인 반면 NFC는 통신에 중점을 둔 기술이라는 점이다. 또한 NFC는 13.56MHz대역에서 동작하기 때문에 동일 주파수 영역의 RFID와의 호환이 용이하며 처음 제안된 NFC는 P2P(Peer to Peer)통신 위주의 기술이었으나 현재는 무선주파수 대역의 RFID 기술을 포괄하는 기술로 NFC의 기술 표준이 정의된다 [1].

과거에는 비용 등의 문제로 NFC를 적용한 단말기 보급이 어려웠지만 최근 보급되는 다수의 스마트 단말기는 NFC 및 NFC서비스를 위한 인프라가 빠르게 갖추어지고 있어 스마트 단말기의 빠른 보급이 NFC기술 확산의 배경이 되고 있다. 특히 NFC기술은 결제 서비스, 광고 및 간편한 데이터 전송등 다양한 분야의 서비스가 가능하며, TSM(Trust Service Manager)등을 통한 사용자 맞춤형 서비스를 제공할 수 있어 기술의 활용분야가 매우 다양하지만 이해관계자간의 서비스 주도권 경쟁을 놓고 아직까지 합의가 원만하게 이루어지지 않아, 현재 기술의 확산에 걸림돌이 되고 있는 실정이다.

2.2 NFC 개요

NFC는 비접촉식 근거리 무선 통신 기술로 RF(Radio Frequency)주파수를 이용하여 NFC단말기 간 또는 NFC 단말기와 NFC Tag간에 정보를 전송하는 기술이다. NFC는 13.56MHz 주파수 영역에서 동작하며, 통신 거리는 약 10cm이하이다. RF를 이용한다는 점에서 NFC는 RFID의 한 범주가 될 수 있으나 NFC는 P2P모드의 통신이 가능하다는 점이다. NFC는 <Table 1>과 같이 3가지 모드로 동작한다 [2,3].

<Table 1> Three features of the NFC

Operating mode	Features	Applicable services
P2P	Peer to Peer mode between NFC device that can exchange data with each other	Electronic business card exchange, P2P payments, End-to-end data exchange
Read/Write Reader	Reader mode that is capable of reading and writing that can read NFC Tag	Smart posters, Tourist Information, Simple NFC
Card Emulation	Operaing with NFC terminal, NFC Tag, etc. which make it possblie to exchange data with exteral reader	Traffic Card, Mobile Credit Card

NFC는 2004년 NFC Forum이 설립되면서 그 용어가 널리 사용되었으며 최근 스마트폰의 보급과 함께 NFC기능을 지원하는 스마트폰이 널리 보급됨에 따라 더욱 주목을 받고 있다.

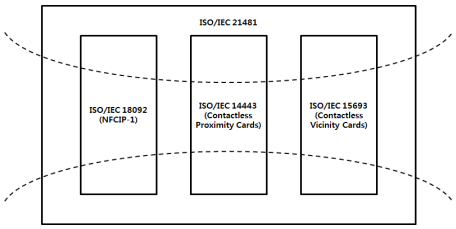
이용자는 NFC단말기를 이용하여 다른 NFC단말기 또는 NFC 태그에 간단히 터치하는것만으로 NFC기능을 이용하여 NFC서비스를 제공받을 수 있다. <Table 2>는 NFC와 다른 근거리 통신 기술과의 차이점을 나타내는 Table이다 [4].

<Table 2> Short-range wireless communications technology comparison

Communication specifications	Frequency	Features	Effective distance
NFC	13.56Mhz	Bidirectional read / write communication is possible	Within 10cm
Bluetooth	2.4Ghz	It is developed to replace the cable for communication between mobile devices and PC	Within 10cm
ZigBee	2.4Ghz	It refers to one of the IEEE 802.15.4 standard that supports short-range communications	10~20m
WiFi	2.4Ghz	Wireless LAN standard	Up to 500m
RFID	134Khz, 13.56Mhz,433 Mhz, 860 ~960Mhz , 2.45Mhz	It refers to an IC chip and recognition technology to manage the information of the various objects over the air.	Tens of cm

2.3 NFC 표준

NFC와 관련된 다수의 국제 표준은 2003년부터 ISO/IEC 18092시작으로 2004년 NFC Forum의 설립과 함께 NFC라는 용어가 공식적으로 사용되기 시작하였다. 2005년 NFC 응용서비스 분야의 확산 및 보급 확대를 위해 ISO/IEC 21481표준을 통해 기존의 RFID기술인 ISO/IEC 14443과 15693을 포함하게 되었다. [Fig. 1]은 NFC 관련 ISO/IEC 국제 표준들의 관계를 보여준다.



[Fig. 1] ISO/IEC 21481

NFC와 관련된 ISO/IEC표준은 ECMA의 표준이 ISO/IEC의 Fast Track절차를 통하여 ISO/IEC표준으로 등록된 표준이 존재하며, 이는 <Table 3>과 같다[5].

<Table 3> Relationship between ISO / IEC standard and ECMA standard

ISO / IEC standard	ECMA standard
ISO/IEC 18092	ECMA-340 (NFCIP-1)
ISO/IEC 21481	ECMA-352 (NFCIP-2)
ISO/IEC 13157-1	ECMA-385 (NFC-SEC)
ISO/IEC 13157-2	ECMA-386 (NFC-SEC-01)

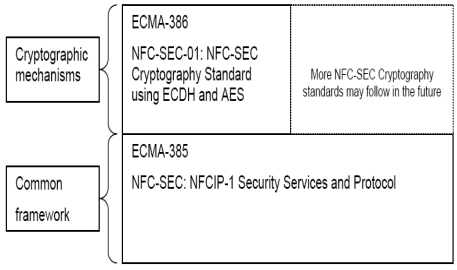
ISO/IEC 14443은 13.56MHz대역의 비접촉식 근거리 무선통신 기술의 하나로 10cm이내 근접형(Proximity)에서 카드의 인식이 가능하다. 스마트 카드에 적용되는 대표적인 비접촉형 근접형 무선통신기술이다[6,7].

ISO/IEC 15693은 13.56MH대역의 비접촉식 근방형(Contactlee Vicinity) 무선통신기술의 하나로 1m범위까지 카드의 인식이 가능하다. 인식범위가 ISO/IEC 14443의 10cm보다 넓어서 출입증 및 항공화물인식 등의 스마트 레이블에 주로 활용되고 있다[8].

ISO/IEC 18092는 13.56MH대역에서 자기장 커플링 방식의 기기 간 통신 인터페이스 및 프로토콜을 정의하고 있으며, 이는 장치(Reader)와 카드 등으로 구성된 다른 비접촉식 스마트카드 기술과 차별화된 점이다. 이 표준은 초기화 방식 및 초기화 과정에서의 데이터 충돌 제어에 필요한 조건, 변조 방식, 코딩, 전송속도, RF 인터페이스의 프레임 형태 등을 기술하고 있다.

ISO/IEC 21481은 13.56MHz에서 동작하는 근거리 통신 프로토콜인 ISO/IEC 14443, ISO/IEC 15693, ISO/IEC 18092의 세가지 표준을 모두 수용한다. 이러한 세가지 표준은 RF신호 인터페이스, 초기화, 충돌방지와 근접하게 붙어있는 장치들과의 무선 상호접속을 위한 통신규약, 13.56MHz에서 동작하는 비접촉식 집적회로 타드에 대하여 기술되어 있다[9].

ISO/IEC 13157은 ECMA표준인 ECMA-385(NFC-SEC)와 ECMA-386(NFC-SEC)이 ISO/IEC의 Fast Track절차를 통해 ISO/IEC 13157-1, ISO/IEC 13157-2로 비준을 받은 표준이다. NFC-SEC표준은 [Fig. 2]와 같은 구로조이루어져 있다. 일반적인 프레임워크인 NFC-SEC은 NFC단말기 간 보안 서비스와 프로토콜을 정의하고 있다. NFC-SEC-01은 암호 메커니즘의 구현으로 ECDH (Elliptic curve Diffie-Hellman)와 AES(Advanced Encryption Standard)를 이용한 암호 표준을 정의하고 있다[10].



[Fig. 2] NFC-SEC standard series structure

2.4 NFC 서비스 동향

국내 NFC서비스는 이동통신사를 중심으로 서비스 관련 업체들이 이동통신사와 제휴를 통하여 서비스 중에 있다. 하지만, 아직까지 제공되는 대다수의 서비스가 NFC이외의 기술을 통하여 제공되고 있으며, NFC기술이 접목되어 사용되는 서비스는 간단한 결제서비스 등과 같은 시범적 단계의 서비스만 제공되고 있는 설정이다[11].

또한 NFC서비스와 관련하여 서비스 활성화를 위한 다양한 시범사업을 진행하였다. 이러한 시범사업 중 정

부주도하의 대표적 사업으로 '명동 NFC Zone'과 '스마트 RFID존 구축' 그리고 '여수 엑스포 NFC시범사업'등이 있다. 하지만, 시범사업 역시 서비스 이용이 번거롭고 불편하여 크게 활성화가 되지 못했다는 평가가 있다.

즉, 아직까지 국내 NFC서비스는 걸음마 단계에 있다고 할 수 있으며 NFC서비스와 관련된 다양한 이해당사자들(이동통신사, 카드사, 은행, 제휴업체 등)의 주도권 다툼 및 NFC서비스 관련 인프라 투자 등의 문제 등이 해결되어야 서비스가 활발히 제공될 것으로 예상된다.

SK는 'SK플래닛'이라는 자회사를 통하여 'Smart Wallet'이란 NFC서비스를 제공하고 있다. 본 서비스는 'Smart Wallet'이라는 모바일지갑 애플리케이션을 이용하여, 다양한 멤버십 카드의 적립·조회·사용, 지불결제, 쿠폰 및 상품권의 수신·사용 등의 서비스를 제공하고 있다.

KT는 'Olleh myWallet'이란 서비스를 제공하고 있다. Olleh myWallet서비스는 올레클럽을 비롯한 다양한 멤버십, 쿠폰 서비스를 플라스틱 카드없이 하나의 어플을 통하여 제공하는 서비스이다. SKT의 Smart Wallet과 비슷한 개념이라 할 수 있다. 교통카드, 신용카드, 터치형 멤버십·쿠폰 서비스 등에 NFC기술이 결합되어 서비스 중이다. 특히, 스마트 결제와 관련하여 'UbPay'라는 회사와 제휴를 통하여 NFC를 이용한 모바일안심결제 서비스를 제공하고 있다.

LG U+sms 'USIM/NFC 서비스'라는 이름으로 NFC 기술이 접목된 다양한 서비스를 제공하고 있다. 다른 통신사와 비슷하게 'USIM Wallet'이란 모바일지갑 서비스를 제공하고 있으며, 스마트 Tag, 모바일 티머니등 다양한 NFC서비스를 제공하고 있다. 하지만, 다른 통신사와 마찬가지로 NFC 기술을 활용한 서비스보다 USIM을 중심으로 한 서비스가 주를 이루고 있다.

NFC서비스 활성화를 위한 정부주도하의 대표적인 사례는 Grand NFC Korea Alliance, 지식경제부의 스마트 RFID존 구축과 방송통신위원회의 여수엑스포 NFC시범사업이 있다.

국외 NFC서비스 시장은 국내보다 먼저 시장이 형성되었다. 영국에서는 최초로 NFC기반 모바일 결제 서비스를 시행하였고, 글로벌 기업인 Google에서 'Google Wallet'을 발표하면서 NFC서비스 시장이 점차 증가하고 있다. 일본의 경우 기존 근거리 통신 기술을 이용한 인프라가 형성되어 있어서 NFC서비스를 제공하기 용이한 기반이 잘 마련되어 있다. 하지만 국내 NFC서비스와 마찬가지로 국외 사례에서도 아직까지 뚜렷하게 성공적이라 할 수 있는 NFC서비스는 제공되지 않는 것으로 보인다.

2011년 5월 20일 영국의 이동통신사인 오렌지(Orange) UK(United Kingdom)가 신용카드사인 Barclaycard와 협력하여 영국에서 첫 NFC기반 비접촉식 모바일 결제서비스인 'Quick Tap'을 출시하였다.

'Quick Tap'은 결제 기능과 잔액 및 최근 거래 내역 조회 기능, 보안기능 등을 제공한다. 현재 'Quick Tap'은 패스트푸드, 마켓 등에서 소액결제 용도로 사용 중에 있으며, 20파운드 미만일 경우 단순 소액결제로 사용 가능하며, 50파운드 초과 시 본인인증 후 사용이 가능하다.

NTT 도코모에선 비접촉 통신기술인 FeliCa기반으로 제공되어 오던 '오사이후케이타이' 서비스를 NFC로 확장하였으며 Felica칩을 내장한 단말기 및 서비스로 2004년에 서비스 시작하였다.

현재 오사이후케이타이의 보급률은 약 90%에 해당하며, 일본 모바일 E-Money시장 규모의 약 50%의 비율을 차지하고 있다.

편의점, 쇼핑센터, 도서·문구, 음식점 등 이용 가능 서비스도 50여종으로 사회에 전반적으로 사용 가능하도록 성장하였으며, 2004년 이후 생산된 거의 모든 피처폰(Feature phone)에 오사이후케이타이 기능을 기본적으로 탑재되어 나왔다.

Google은 NFC 기술을 이용한 Smart Wallet 애플리케이션인 'Google Wallet'의 서비스를 2011년 9월 19일부터 실제 서비스를 시행중에 있다.

Google Wallet 서비스는 Google과 함께 여러 회사가 참여하여 제공하고 있다. 사용자에 대한 다양한 개인정보를 각 금융·카드사, 이통사, 상점 등에서 수집을 수행한다. Google Wallet서비스의 TSM업체는 First Data가 참여하고 있다.

3. NFC 취약점 분석

NFC 취약점은 RF전파의 특성에 따른 물리적 취약점과 NFC응용계층에서의 논리적 취약점 등으로 구분 할 수 있다. <Table 4>는 NFC기술적 취약점에 대한 요약이다[12].

<Table 4> NFC technology vulnerability classification

Class	Vulnerability	Measures
Physical	Eavesdrop	Secure channel
	Data Corruption	Secure channel, RF field check
	Data Modification	Secure channel, RF field check
	Data Insertion	Secure channel, RF field check
Logical	Relay Attack	Timing check, Location check
	MITM Attack	Pre-shared secret, RF field check
	Smart Poster URI Spoofing	URI Validation, URI syntax check
	NDEF Signature RTD Vulnerability	Electronic signature support for the header field

3.1 도청(Eavesdrop)

NFC는 다른 무선 통신과 마찬가지로 무선 통신의 특성 상 도청공격이 가능하다. 두 기기가 RF시그널(Signal)을 사용 해 데이터를 주고 받을 때 공격자는 안테나를 사용하여 RF시그널을 도청 할 수 있다. 도청된 RF시그널의 퀄리티(Quality) 및 도청 가능한 거리는 정확한 수치로 표현 할 수 없다. 도청 대상 NFC기기의 RF필드 특성, 공격자의 안테나 특성 및 환경, 공격자가 도청한 RF시그널의 퀄리티, 공격자의 RF시그널 디코드 능력 및 디코더 기기의 퀄리티, 기기의 파워등과 같은 변수에 따라 달라질 수 있다. 일반적인 공격가능 거리는 능동모드의 경우 10m이며 수동모드의 경우 1m이다[13].

도청 공격에 대한 대책으로 전송되는 데이터를 암호화 하여 기밀성을 확보하는 방법이 있다. 즉, 보안 채널을 형성하여 데이터를 전송하면 도청 공격이 일어나도 해당 데이터의 내용을 알 수 없다.

3.2 데이터 변조(Data Corruption)

데이터 변조 공격은 NFC단말기 간 통신 시 통신 방해, RF시그널 송출, 데이터 전송 등의 방법을 사용하여 Data의 변질 도는 변형을 일으키는 공격으로 서비스 거부 공격(Denial of Service, DoS)과 비슷하다.

데이터 변조 공격에 대한 대책으로 보안채널의 이용 또는 Rf필드를 체크하여 주변에 방해 전파가 있는지 확인하는 방법 등이 있다.

3.3 데이터 수정(Data Modification)

데이터 수정 공격은 NFC단말기 간 통신 시 주파수를 수정하여 데이터를 고치는 방법으로 데이터를 변형하는 공격이다. 데이터의 유효성 체크를 하지 않는 서비스의 경우 의미 없는 데이터가 전송되어 일종의 서비스 거부 공격(Denial of Service, DoS)이 될 수도 있다. 또한 보안 채널을 이용하지 않은 경우 데이터의 수정으로 인하여 잘못된 데이터가 전송되어 서비스가 공격자의 의도로 변형되어 제공될 수 있다.

데이터 수정 공격에 대한 대책으로 보안채널의 이용 또는 RF필드를 체크하여 주변에 방해 전파가 있는지 확인하는 방법등이 있다.

3.4 데이터 삽입(Data Insertion)

데이터 삽입 공격은 두 NFC 단말기 간 데이터 전송 시 공격자의 메시지를 전송하여 삽입시키는 공격 방법이다. 본 공격은 어느 한 NFC 기기에서 응답 데이터를 전송하는데 오랜 시간이 걸릴 때 유효한 공격이다.

데이터 삽입 공격에 대한 대책으로 보안채널의 이용 또는 RF 필드를 체크하여 주변에 방해 전파가 있는지 확인하는 방법 등이 있다.

3.5 중간자 공격(Man in the Middle Attack)

전형적인 중간자 공격은 Alice와 Bob간의 통신 시 공격자인 Eve가 각각의 사용자인 Alice와 Bob인 것처럼 가장하여 중간에서 데이터를 취득하는 것이다.

유럽 컴퓨터 제조 협회(ECMA, European Computer Manufacturers Association)에 따르면 NFC는 10cm이내의 거리에 있는 두 기기 사이에서 동작하기 때문에 중간자 공격에 안전하며, RF필드의 체크를 통한 중간자의 개입을 확인하여 중간자 공격의 성공률은 극히 낮다고 설명하고 있다.

하지만, 10cm라는 거리상의 문제는 도청 공격과 마찬가지로 데이터 송신자와 수신자 그리고 공격자의 안테나 기하학적 구조, 안테나 성능 및 환경에 의해 언제든지 그 상황이 변경 될 수 있다.

중간자 공격에 대한 대책으로 사전 비밀의 공유를 통한 보안채널을 형성하여 이용하는 방법 또는 Rf필드를 체크하여 주변에 공격자가 있는지 확인하는 방법 등이 있다.

3.6 중계 공격(Relay Attack)

RF시그널(Signal)을 사용하는 NFC는 기존의 RFID(Radio Frequency Identification) 시스템(System)의 공격 방법 중 하나로 사용되고 있는 중간자 공격과 유사한 개념의 중계 공격이 가능하다[14].중계 공격은 공격자가 단순히 데이터 전송에 사용되는 데이터를 중계만 해주기 때문에 보안채널 형성 등을 통한 데이터의 기밀성, 무결성을 유지하여도 그 속성들과 무관하게 공격이 가능하다.

중계 공격에 대한 대책으로 전송되는 데이터의 타이밍을 체크하여 일정 시간 이내에 데이터가 전송되는지 확인하는 방법 또는 현재 위치 정보에 대한 정확한 응답 등을 통한 근접거리 인증 등의 방법이 있다.

3.7 스마트 포스터 URI 스푸핑 (Smart Poster URI Spoofing)

NFC단말기는 스마트 포스터에 부착된 NFC태그로부터 스마트 포스터의 URI정보를 읽어 간편한 영화예매 등의 서비스 이용이 가능하다. 이때 영화정보는 URI형태로 전송이 된다. 실제 URI스푸핑 공격에 대한 예제는 [Fig. 3]과 [Fig. 3]에 나타나 있다[15].

```
Title: Bank of Germany
URL:   https://www.bankofgermany.de
```

(a) Original Smart Poster

```
Title: Bank of Germany\rhttps://www.
         bankofgermany.de\r\r\r\r\r.
URL:   http://www.attacker.com
```

(b) Malicious Smart Poster

[Fig. 3] URL Spoofing

```
Title: Tourist Information
URL:   tel:08001234567
```

(a) Original Smart Poster

```
Title: Tourist Information\r080012345
        67\r\r\r\r\r\r\r.
URL:   tel:09009996668
```

(b) Malicious Smart Poster

[Fig. 4] Telephony URI Spoofing

이러한 스푸핑 공격에 대한 대책으로 NFC태크로부터 전송받은 데이터에 대한 위·변조 확인을 위한 URI검증 또는 URI문법체크를 통하여 "\r"와 같은 특수 문자에 대하여 사용을 금지하는 등 데이터 검증과정을 통하여 스푸핑 공격을 예방할 수 있다.

NFC Forum에서는 NDEF 데이터에 전자서명을 지원하는 NDEF Signature RTD라는 TS를 제공하여 NDEF 데이터에 대한 무결성을 보장한다. 하지만 이러한 방법도 다음의 취약점이 존재한다.

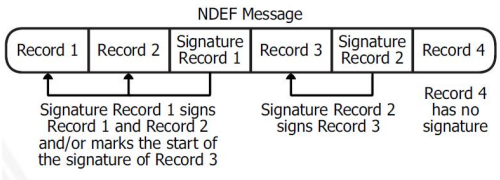
3.8 NDEF Signature RTD 취약점

NFC Forum은 NFC단말기 간 데이터 교환 포맷인 NDEF(NFC Data Exchange Format)의 무결성 검증을 위하여 NDEF Signature RTD(Record Type Definition)라는 명세서를 제공한다. 하지만 NDEF Signature RTD는 기존 NDEF RTD와의 호환성 등을 고려하여 NDEF 메시지의 모든 부분에 대한 서명을 지원하지 않는다. <Table 5>는 현재 NDEF Signature RTD에 대한 각 필드의 서명여부와 필드별 서명 유효성을 나타낸다 [16].

<Table 5> NDEF Signature function availablilities

Field name	Signature validity	NDEF Signature RTD
Message Begin	Not required	Impossible
Message End	Not required	Impossible
Chunk Flag	Importance	Impossible
Short Record Flag	Importance	Impossible
ID Length Present Flag	Importance	Impossible
Type Name Format	Essential	Impossible
Type Length	Essential	Impossible
Payload Length	Essential	Impossible
ID Length	Essential	Impossible
Type	Essential	Possible
ID	Essential	Possible
Payload	Essential	Possible

또한, 하나의 NDEF메시지(message)는 여러 독립적인 사인 값들을 포함하는 형태로 구성이 가능하다. NDEF 메시지에 서명 데이터가 삽입된 예는 [Fig. 5]과 같다.



[Fig. 5] NDEF Message Format

서명 레코드 1(Signature Record 1)은 레코드 1과 2에 대한 데이터를 서명하고 서명 레코드 2는 레코드 3에 대한 데이터를 서명한 값을 가지고 있으며, 레코드 4는 서명 레코드 값을 갖고 있지 않다. 따라서 NDEF메시지 헤더의 조작 및 동일한 서명자의 서명 위조 등을 통하여 NDEF메시지가 위조된 NFC태크를 배포할 수 있다.

NDEF Signature RTD취약점에 대한 대책으로 헤더 필드에 대한 서명 지원 등이 가능하다. 즉, <Table 5>에서 제시한 MB(Message Begin)와 ME(Message End)필드를 제외한 모든 필드를 서명하여, 서명된 데이터의 위·변조를 막을 수 있다.

4. NFC 보안위협 시나리오

4.1 Active-Attack 보안 위협 시나리오

Active-Attack 기반 보안 위협은 공격자가 공격 시점에 직접 참여를 함으로써 발생하는 보안 위협으로, 무선 주파수 특성을 이용하여 RF신호를 훼손시켜 서비스를 제공할 수 없는 Dos공격을 수행하는 보안 위협과 NFC 기능이 활성화 되어 있는 경우 근거리에서 해당 Tag의 정보를 중계하여 발생하는 Relay-Attack과 관련된 보안 위협이 발생 할 수 있다.

NFC Tag를 이용한 단말기 상태 변경 보안 위협으로 NFC Generic Control RTD은 NFC단말기 제어를 위한 규격을 나타내며 이를 이용하여 NFC단말기의 기능을 제어 할 수 있다. 사용자의 편의를 위해 NFC Tag를 이용하여 단말기의 다양한 기능을 제어하는 NFC Generic Control RTD를 사용하고 있으며 이를 악의적으로 사용할 수 있으며, 검증할 수 없다.

위협으로는 상태 변경과 악의적인 AP 로 인한 피해가 있다. 상태 변경은 단말기의 소리 모드 설정 변경, 알람 설정, 특정 기능의 On/Off변경 등 여러 가지 상태를 변경할 수 있으며, 이를 이용한 공격이 가능하다. 악의적인 AP에 정상적인 사용자가 접속하여 통신하였을 때 ID나 Password, 카드 정보, 통신 내용 등이 도청 될 수 있다.

대응방안으로는 NFC Forum에서 보안 문제로 Specification에서 제외한 NFC Generic Control RTD은 사용하지 않아야 한다. NFC Tag를 이용하여 단말기의 기능을 제어하는 경우 주요 단말기 기능은 제한하며 Tag 내 단말기 제어 정보를 사용자가 인지한 후 수행하도록 하는 것이 비교적 안전하다. 사용자가 Tag를 읽을 때, 변경되지 않은 정상적인 Tag인지 검증 할 수 있도록 해야 한다.

4.2 Passive-Attack 기반 보안 위협 시나리오

NFC Tag 기반 스마트 포스터를 이용한 Spoofing 공격으로 사용자를 공격자가 미리 만들어 놓은 악의적인 웹 사이트로 접속을 유도할 수 있다. 이러한 악의적인 사이트를 이용한 2차 피싱공격 혹은 악성코드 감염으로 사용자에게 추가적인 피해가 발생할 수 있다. 다수의 NFC 단말기가 스마트 포스터로 읽어온 정보들 중 일부만 사용자에게 보여주고 있다. 서비스 제공자의 확인이나 URL검증을 수행하지 않는다.

위협으로는 공격자 웹 사이트의 URL은 사용자가 A기업을 신뢰하는 수준과 같은 수준의 신뢰를 받는다. 따라서 공격자는 A기업의 신뢰를 악용함으로써 공격을 수월하게 수행 할 수 있다. URL Spoofing을 통한 공격자의 웹 사이트로 접속으로 사용자는 공격자의 피싱 웹 사이트에 접속하여 공격자가 요구하는 민감한 정보에 대해 입력할 시 해당하는 정보가 공격자에게 유출된다. 공격자가 해당 웹 사이트에 악성코드를 심어 놓았다면 공격자의 웹 사이트로 접속한 사용자들은 이 악성코드에 감염 될 수 있다.

대응방안으로는 NFC 단말기는 스마트 포스터로 읽어온 모든 정보를 보여주며 스마트 포스터가 \r과 같은 문자열을 포함하고 있을 경우, 해당 문자열을 특수하게 처리하지 않아야 한다. 서비스 제공자와 URL의 검증이 필요하며 사용자는 공격자의 공격 가능성을 인지하고 항시 URL을 확인해야 한다.

4.3 사용자 부주의에 따른 보안 위협 시나리오

NFC 동작 모드 중 하나인 P2P모드는 NFC단말기 간에 P2P연결을 이용하여 데이터를 교환할 수 있다. 이러한 P2P모드를 이용하여 교환자료에 악성코드가 삽입되어 있을 시 사용자의 권한이 탈취 될 수 있다. 공격자의 악의적인 코드가 삽입된 문서가 사용자에 의해 실행된다. 공격자가 문서파일뷰어와 권한 상승 관련 취약점을 통하여 트로이목마를 주입할 수 있다.

위협으로 공격자가 사용자의 NFC단말기에 저장되어 있는 모든 정보를 일어 올 수 있다. 정보는 이메일, 문자 메시지, 주소록, 사진 외에도 출입문 도어락의 인증정보나 결제, 계좌 이체에 필요한 정보, 전자쿠폰 등이 될 수 있다.

대응방안으로는 사용자는 신뢰되지 않는 파일에 대한 실행은 자제하며 타인에게 받은 파일은 Anti-Virus등의 백신으로 검사하여 악성코드의 존재유무를 확인하여야 한다. P2P모드의 자동페어링 기능을 사용자가 사용, 비사용 설정을 할 수 있어야 하며, 만약 자동페어링이 진행 중이라면 사용자가 인식할 수 있어야 한다.

4.4 NFC 서비스 제공업체에서의 보안 위협 시나리오

TSM에는 이동통신사, 금융 서비스 제공자(카드사, 은행, VAN사 등)로부터 정보를 제공 받고, 이 정보들을 공유하고 가공하여 사용자 패턴정보를 생성한다. 따라서 TSM에서 정보가 유출될 경우 그로 인한 파장이 타 서비스에 비해 클 수 있다. 한 업체의 기술적·관리적 문제로 보안 취약점이 발생하여 악성코드가 감염되면 전체 협력 업체와 데이터 공유를 위해 통신할 때 악성코드가 모든 협력 업체에 전송되어, 모든 업체들이 악성코드에 감염되는 형태로 작용한다. TSM에서 가공하여 보유하고 있는 개인의 패턴정보가 유출됨으로써 공격자는 2차 공격을 쉽게 할 수 있게 된다.

위협으로는 NFC서비스를 이용하는 사용자들이 개인정보 유출 및 TSM에서 유출되는 정보의 양, 사용자의 생활 패턴 정보와 같은 민감 정보 유출에 따른 2차 피해가 있다.

대응방안으로는 정보 유출과 악성코드 감염등의 피해를 예방하기 위해 방화벽, IDS, IPS등 물리적 보안과 암호화, 인증, 백신프로그램 사용 등 논리적 보안을 적용해야 한다. 또한, 신규 보안 취약점에 따른 보안 대책이 NFC 서비스를 제공하는 모든 서비스 제공자들에게 동시에 이루어져야 하며, 하나의 서비스 제공자에 공격기 수행되었을 때 타 서비스 제공자를 보호할 수 있는 방안이 필요하다. 관리적 문제로 인한 정보 유출을 막기 위해 내부 직원 관리 및 교육을 주기적으로 시행한다.

5. 결론

본 연구에서는 NFC서비스에서 안전한 환경 조성 및 산업 활성화를 위하여 다음과 같이 연구를 수행하였다.

첫째, NFC서비스의 기술특징과 서비스 동향을 분석하여 NFC서비스의 취약점을 도출하여 분석하였고 둘째, NFC서비스의 취약점 분석 결과를 기반으로 하여 서비스에 발생 할 수 있는 보안 위협과 그에 따른 시나리오를 도출하여 분석하였다. 셋째, 도출된 보안 위협 시나리오를 분석하여 발생 가능한 파장을 기술하였으며, 보안 위협 발생 원인과 그에 따른 대응방안을 마련하였다.

본 연구의 NFC취약점과 보안 위협 시나리오, 보안위협 시나리오별 대응방안을 기반으로 NFC사용을 바탕으로 하는 환경 및 산업에 활성화를 기대하고 있다.

국내 NFC서비스는 기존 RFID 서비스와 달리 TSM기반의 통합결제 서비스로 확대될 전망이며, 국외의 경우 통합결제에서 처리되는 사용자의 개인정보를 기반으로 하는 사용자 맞춤형 서비스가 제공 예정 중에 있다 [17,18,19]. 따라서 TSM 기반서비스에서 활용될 수 있는 안전한 오픈 플랫폼 모델 및 사용자의 개인정보를 보호할 수 있는 보안 서비스 인프라 구축연구가 필요할 것으로 사료된다.

REFERENCES

[1] Ernst Haselsteiner, Klemens Breitfuß, "Security in Near Field Communication (NFC)", Workshop on RFID Security RFIDSec, 2006.[1] ECMA International : "ECMA-089 NFC-SEC White paper," Dec 9, 2008

[2] GSMA, "mobile NFC echnical guidelines V2.0," 2007

[3] GSMA, "mobile NFC Service V1.0," 2007

[4] EU, "Privacy and Data Protection Impact Assessment Framework for RFID Application", 2011.1.12.

[5] ECMA International : "ECMA-089 NFC-SEC White paper," Dec 9, 2008

[6] ISO/IEC 14443-3:2011, Identification cards - Contactless integrated circuit cards - Proximity cards - Part 3: Initialization and anticollision

[7] ISO/IEC 14443-4:2008, Identification cards - Contactless integrated circuit cards - Proximity cards - Part 4: Transmission protocol

[8] ISO/IEC 15693-1:2010, Identification cards - Contactless integrated circuit cards - Vicinity cards - Part 1: Physical characteristics
[9] ISO/IEC 21481:2005, Information technology - Telecommunications and information exchange between systems - Near Field Communication Interface and Protocol 2 (NFCIP-2)
[10] ISO/IEC 13157-2:2010, Information technology - Telecommunications and information exchange between systems - NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES
[11] NFC technology trends and certification, TTA Journal Vol.133, 2011
[12] Sun-Hee Lim, Jae-woo Jeon, Jung Imjin, Okyeon Yi, "Study on NFC Security Analysis and UICC Alternative Effect". J-KICS Vol36 No.1, 01.2011
[13] Ernst Haselsteiner and Klemens Breitfub, "Security in NFC", Workshop on RFID Security RFIDSec, 2006
[14] Gerhard P. Hancke, Markus G. kuhn, "An RFID Distance Bounding Protocol." Security and Privacy for Emerging Areas in Communications Networks, 2005.
[15] Collin Mulliner, "Vnlnerability Analysis and Attack on NFC-enabled Mobile Phones", International Conference on Availability, Reliability and Security, 2009.
[16] NFC Forum-TS-signature RTD-1.0, 2010-11-18
[17] C.H. Choi. "CPND ecosystem ICCT (Information, Communication, Contents Technology)." Journal of Digital Convergence. 12.3 (2014): 7-16.
[18] S.H. Won, and H.S. Yang. "Research and policy direction for the success of ICT-based company Fusion." Journal of Digital Convergence. 13.4 (2015): 39-50.
[19] J.H.Han, et al. "Effects of perceived usefulness and ease reliance on payment services and loyalty mall ." Journal of Digital Convergence 13.12 (2015): 75-87.
[20] Seong-Hoon Lee, "Actual Cases and Analysis of IT Convergence for Green IT", Journal of the Korea Convergence Society, Vol. 6, No. 6, pp. 147-152, 2015.
[21] Seong-Hoon Lee, Dong-Woo Lee, "FinTech - Conversions of Finance Industry based on ICT", Journal of the Korea Convergence Society, Vol. 6, No. 3, pp. 97-102, 2015.

김 형 욱(Kim, Hyung Uk)

- 2012년 2월 : 숭실대학교 정보과학대학원 정보보안학과 (공학석사)
- 2012년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정
- 2006년 9월 ~ 현재 : 한국전자인증 책임연구원
- 관심분야 : PKI, 컴퓨터통신, IoT
- E-Mail : ddarajaengi@gmail.com

김 형 주(Kim, Hyung joo)

- 2008년 8월 : 단국대학교 컴퓨터과학과(공학사)
- 2010년 8월 : 숭실대학교 컴퓨터학과(공학석사)
- 2015년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 관심분야 : IoT, Cloud Computing, 시큐어코딩
- E-Mail : hyungjoo.kim@ssu.ac.kr

강 정 호(Kang, Jung ho)

- 2000년 2월 : 서울과학기술대학교 컴퓨터공학과(공학사)
- 2002년 2월 : 서울과학기술대학교 컴퓨터공학과(공학석사)
- 2013년 12월 : 숭실대학교 컴퓨터학 (공학박사)
- 관심분야 : NFC, 시큐어코딩
- E-Mail : kjh7548@naver.com

전 문 석(Jun, Moon seog)

- 1989년 2월 : University of Maryland Computer Science(공학박사)
- 1991년 2월 : New Mexico State University physical Science Lab 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 정교수
- 관심분야 : RFID, PKI
- E-Mail : mjun@ssu.ac.kr