디지털산업정보학회 논문지 제14권 제4호-2018년 12월
http://dx.doi.org/10.17662/ksdim.2018.14.4.219

# 안전한 NFC 서비스 활용 활성화를 위한 보안 위협 대책 마련을 위한 고찰*

최 희 식** · 조 양 현***

# *The Study for Establishment of Security Threat Measures for Secure NFC Service*

Choi Heesik · Cho Yanghyun

〈Abstract〉

The utilization of NFC has been continuously increasing due to the spread of smart phones and the development of short-range wireless communication networks.

However, it has been suggested that stability and security of convenient NFC short-range wireless communications can be unstable and problematic. The unstable causes for NFC are the lack of security technologies for NFC, the controversy about personal information infringement, and the lack of social awareness on security breach against data settlement.

NFC service can be conveniently used by simply touching other NFC devices and NFC tags through the NFC device. This thesis analyzes that NFC authentication technology, which is convenient for user are one of the unstable causes of security of NFC.

This thesis suggest that ministry should research countermeasures and promote how users can use NFC safely. It also suggests that users should have awareness when they use payment and authentication service through NFC to prevent from security threat.

Key Words : NFC, Mobil Security, Security Threat, NFC Device

## Ⅰ. 서론

[1)]

최근 우리 생활을 윤택하게 도와주는 IT 기술들이 속속히 개발되어 출시되고 있는데 그 중 대표적인 기술이 NFC 기술이다. 근거리 무선통신인 NFC 인증 기술은 애플 페이, 삼성 페이 등 스마트폰 결제 시스템에 도입되면서 더욱 알려지게 되었다. 특히, 국내 안드로이드 계열 스마트폰에 NFC가 탑재되어 젊은 직장인들 사이에 편리함과 함께 활용도가 높아서 더욱 주목을 받고 있다. 또한, 근거리에서만 통신이 가능하기에 기존의 RFID 기술보다 보안성이 우수하다는 장점과 편의성으로 앞으로 높은 사용률은 꾸준하게 증가할 것으로 전망되고 있다. 그러나 무선 통신망에서 이루어진 NFC 사용에 대한 보안이 다소 불안하고 문제가 발생할 수 있다는 의견이 제시되면서 NFC에 대한 보안기술 부족과 개인정보 침해 논란, 데이터 결제에 대한 보안 침해가 대표적이다 볼 수 있다.

본 논문에서는 NFC와 관련된 기술적 방향과 NFC

* 본 연구는 2018년 삼육대학교 교내공모과제 연구비 지원으로 수행됨
** 경민대학교 IT경영과 외래교수
*** 삼육대학교 컴퓨터 · 메카트로닉스공학부 교수(교신저자)

보안 이슈에 대해서 이를 고찰하여 논문을 구성하고자 한다. 2장에서는 관련 연구로 NFC 정의 및 기술, 사용분야에 대해서 살펴보고, 3장에서는 보안과 관련된 위협적인 부분에 대해서 알아보고 NFC 인증 시스템과 관련된 보안 위협에 문제점을 고찰하여 4장에서 검토 사항에 대한 방안을 제시하고, 5장에서 결론으로 마무리하고자 한다.

## Ⅱ. 관련연구

### 2.1 NFC 정의

NFC는 근거리 무선통신(Near Field Communication)의 약자로 10cm 이내의 거리에서 데이터를 무선으로 주고받을 수 있는 근거리 통신 기술이다. NFC는 13.56MHz의 주파수 영역에서 작동되며 최대 초당 424kb의 속도로 데이터를 전송시킨다[1].

NFC는 2002년에 네덜란드의 NXP 사와 일본 소니(Sony) 사가 공동으로 개발하였다. 2003년 NFC는 ISO/IEC 표준이 승인되었으며 2004년 NXP 사와 소니 사 등이 중심으로 NFC 포럼(NFC Forum)을 구성하였다. 현재 NFC 포럼에 삼성, 구글, 애플 등과 같은 IT 대기업뿐만 아니라 은행, 무선 통신 업체 등 다양한 분야의 기업들이 회원으로 가입되어 있다. NFC 포럼에서는 NFC 기술의 동향, 미래, 표준 등이 논의되고 있다[2].

사용자들은 NFC 기기를 통하여 다른 NFC 기기 및 NFC 태그에 간단히 터치하는 것만으로도 NFC 서비스를 사용할 수 있다. NFC 태그는 NFC 칩과 안테나로 이루어져 있으며 휴대폰 하나로 스마트카드와 RFID Reader/Write를 하나로 합쳐 놓은 것 같은 기능을 수행할 수 있다[3]. NFC 칩은 소량의 데이터와 통신할 수 있는 기술이 포함된 마이크로 칩이 탑재된 유심이며 안테나는 두께가 수 밀리미터 정도 되는 코일이나 와이어 루프로 이루어져 있다. NFC 태그는 보통 ISO 14443 표준에 호환되게 제작되어 있다[4].

NFC는 동작 방식에 따라 읽기/쓰기 모드(Reader/Writer mode), 피어 투 피어 모드(Peer-to-Peer mode), 카드 에뮬레이션 모드(Card Emulation mode)로 3가지 모드로 분류한다[5].

#### 2.1.1 읽기/쓰기 모드 (Reader/Writer Mode)

읽기 모드(Reader Mode)에서는 NFC 기기가 ISO 14443와 FeliCa 체계와 호환되는 태그에서 정보를 읽어 들일 수 있다. 만약 기기가 두 가지 이상의 태그를 감지했을 경우 충돌 방지 알고리즘을 통하여 하나의 태그만을 선택한다. 쓰기 모드(Writer Mode)에서는 읽기 모드와 반대로 사용자가 NFC 기기를 통하여 NFC 태그에 정보를 입력할 수 있다.

#### 2.1.2 피어 투 피어 모드 (Peer to Peer Mode)

피어 투 피어 모드(Peer to Peer Mode)에서는 두 개의 NFC 기기가 서로 통신하여 정보 및 파일을 공유할 수 있다.

#### 2.1.3 카드 에뮬레이션 모드 (Card Emulation Mode)

카드 에뮬레이션 모드(Card Emulation Mode)에서는 NFC 기기가 기존의 비접촉식 스마트카드와 같이 작동되며 사용자는 이를 통하여 NFC 기기를 교통카드, 신용 카드, 스마트폰에 탑재된 페이 결제 시스템 등으로 활용할 수 있다.

① NFC 결제 서비스

현재 NFC 기술이 가장 많이 사용되고 있는 분야 중 하나이다. 많은 스마트폰 제작 회사들과 통신사들이 각자의 NFC 결제 서비스를 제공하고 있으며 스태

티스타(Statista)의 조사에 의하면 모바일 결제를 이용하는 2018년에 사용자가 1억 6600만 정도 추정했다. 2016년에 미국의 모발일 결제 시장이 약 280억 달러 정도였으며 2020년에는 미국의 모바일 결제 시장이 약 3140억 달러 정도로 성장할 것으로 예상하였다[6].

대표적인 예로 애플이 2014년도부터 도입한 애플 페이(Apple Pay), 구글이 기존의 구글 월렛(Google Wallet)과 안드로이드 페이(Android Pay)를 통합한 구글 페이(Google Pay), 삼성의 삼성 페이(Samsung Pay) 등이 대표적이다.

② 의료 산업

의료 산업에서 또한 NFC 기술을 도입하고 있다. 병원은 스마트폰 같은 기기들을 통하여 환자의 진료 기록, 투약 기록, 처방 기록 등과 같은 정보를 쉽게 추적 및 기록할 수 있으며, 응급 환자의 경우, 응급환자가 NFC 기기나 태그를 소유하고 있으면 응급환자의 필요 정보를 신속하게 얻을 수 있다[7].

③ 관광

사용자들은 박물관, 미술관, 관광 명소 등에 있는 NFC 태그를 통해 관련 정보를 쉽고 신속하게 접할 수 있다. 런던 박물관은 노키아(Nokia)와 협력하여 2011년도부터 NFC 서비스를 도입하였다. 사용자는 NFC 서비스를 통하여 박물관의 티켓, 박물관 상점의 물건을 구입할 수 있으며. 전시품의 NFC 태그를 통하여 사용자는 전시품의 정보를 접할 수 있다[8].

④ 광고 산업

광고주들은 스마트포스터(Smart Poster) 등과 같이 NFC 기술을 이용하여 광고를 효율적으로 이용할 수 있다. 광고의 NFC 태그에는 제품의 웹사이트 링크, 할인 쿠폰 등을 포함할 수 있으며 사용자는 관심이 있는 제품의 정보를 즉석에서 접하는 것이 가능하다.

⑤ 출입 통제

ITC 관련 회사 및 정부, 학교와 같은 건물에서 내부 직원 출입과 관련된 현황 및 외부인 출입 통제를 위해 이미 NFC 기술이 널리 활용되고 있다. 또한, 정교한 애플리케이션을 통해 개인 정보나 보안을 요하는 학술 자료에 대한 직원의 접근을 관리하는데도 사용되고 있다.

## 2.2 NFC 구성요소

NFC 기능을 제대로 구현하기 위해서는 위에서 설명한 3가지 동작방식 외에도 아래와 같은 필수 구성요소가 <그림 1>과 같이 NFC 칩, 안테나, SE(Secure Element, USIM/SD카드) 등과 같은 메모리가 필요하다[10].


<그림1> NFC 구성요소 [9]

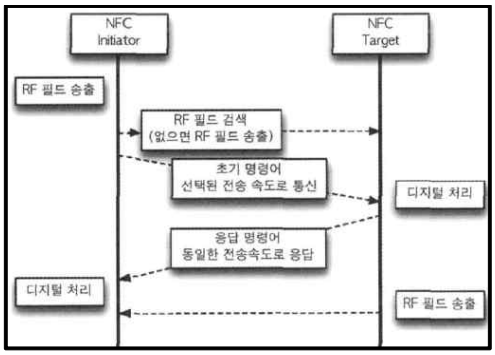
## 2.3 NFC 통신 모드

NFC 통신 모드는 <그림 2>와 같이 수동 모드와 능동 모드로 나누게 되며 이니시에이터 NFC 단말기는 주기적으로 RF를 송출해 RF 필드를 검색하고, RF 필드가 검색되면 초기 작업을 수행하여 타겟 단말기와 통신을 시작한다. 타겟 단말기의 역할은 이니시에이터 단말기로 부터 받은 데이터에 대해 응답하고,

응답을 받은 이니시에이터 단말기에 데이터를 송신하는 과정을 반복하게 된다.

① 수동모드 : 이니시에이터 단말기에서 먼저 RF 필드를 제공하여 통신을 시작한다.

② 능동모드 : 이니시에이터 단말기와 타겟 단말기 모두가 RF 필드를 동적으로 생성하여 통신한다.




<그림 2> NFC 통신 프로토콜 [10]

# Ⅲ. NFC 보안 위협

## 3.1 NFC 보안의 위협요소

일상생활에서 물건 구매와 관련된 금융 결제 서비스 영역 등 다양하게 활용되고 있는 NFC 기술은 여러 유형의 보안 위협에 노출되고 있다.

### 3.1.1 Tag 보안 위협

현재 NFC 기반 서비스는 모바일 결제, 모바일 쿠폰, 모바일 멤버쉽 앱과 관련한 결제 분야 등 다양한 분야에 사용되고 있다. Tag 서비스는 점차적으로 국내 통신사의 신제품 개발과 함께 새로운 결제 기능이 탑재된 기능과 함께 젊은이들 사이에 활용에 따른 인기가 매우 높으며, 이를 활용하기 위해 폰을 바꾸기도 한다. 활용적 이용 분포에 따르면 주로 택시, 카페, 소액 결제 등 많은 이용자 들이 Tag 이용을 통해 결제 서비스 등에 이용하고 있다. 하지만 Tag과 관련된 편리한 결제 서비스가 이용되고 있는 과정에서 위·변조될 위협적 요소도 포함되어 있다. Tag 유형은 크게 <표 1>과 같이 4개의 서비스로 구분한다.

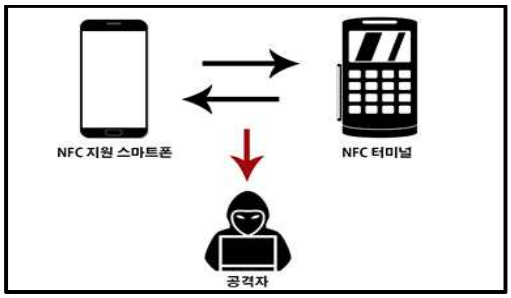
<표 1> NFC Tag Category [11]

| | Type1 | Type2 | Type3 | Type4 |
|---|---|---|---|---|
| RF Interface | ISO 14443A | ISO 14443A | ISO 18092 | ISO 14443 |
| Speed | 106 Kbps | | 212 Kbps | 106-424Kbps |
| Protocol | Self-instruction | | FeilCa | ISO 14443-4 |
| | | | Protocol | ISO 7816-4 |

### 3.1.2 도청(Eavesdropping)

NFC 또한 다른 무선 통신 기술과 마찬가지로 도청 공격에 보안 위협에 노출되어 있다. 직접 현물을 거래하던 전통적인 거래 방식과는 달리, NFC 거래의 특성은 <그림 3>과 같이 사용자 기기와 결제 터미널 간의 전자 데이터를 전송한다는 점에서 정보 보안에 대한 탈취가 용이하다는 것이 문제점으로 나타나고 있다. NFC 공격은 사용자가 단말기와 기기간의 데이터를 이용하는 짧은 시간에 공격자는 데이터를 통해 침투하여 은행 관련 세부 정보, 사용자의 개인 정보 등을 탈취하게 된다.

NFC 거래는 공중 인터페이스 신호 캡처, 통신 채널 디코딩 그리고 캡처된 데이터 분석이라는 크게 세 가지 측면으로 나누어진다. 이 중 공중 인터페이스 신호 캡처 부분이 도청 위험에 노출되어 있다. 공격자는 안테나 등으로 NFC 기기 간의 통신을 도청할 수 있다. NFC 통신이 근접한 기기 간에서 발생한다는 점에도 불구하고 공격자들은 최대 5m의 거리에서도 도청에 성공했다는 주장이 보고되었다[12-13].



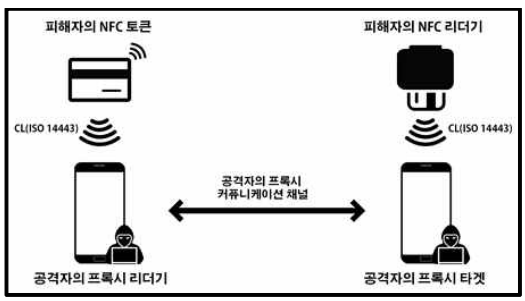

<그림 3> NFC 도청 공격 방식 [12]

3.1.3 데이터 수정(Data Modification)

데이터 수정은 공격자가 교환되고 있는 무선 주파수 장치를 통하여 캡처 및 수정이 가능한 경우다. 공격자의 기기는 NFC 데이터 교환을 잠시 금지할 수 있으며 금지된 동안 공격자는 바이너리 코딩을 변경할 수 있다. 이러한 유형의 공격은 구현하기가 매우 어렵지만 드물게, 데이터 수정이 실현 가능한 경우가 있다. 공격자들은 NFC 데이터 교환을 방해하기 위해 가장 일반적인 방법으로 RFID 전파 방해기를 사용한다. 송신자는 NFC 데이터 교환 중에 주파수 강도를 측정할 수 있다면 이와 같은 유형의 공격을 어렵지 않게 감지할 수 있다[12]. 원격으로 조정할 수 있는 여러 가지 문제점이 파악됐다. 특히, 스마트TV의 경우 다양한 콘텐츠를 인터넷과 연결하여 TV에 VOD 콘텐츠 앱을 클릭하여 영화를 다운로드 받는 과정, 특정 콘텐츠 서비스를 공급받는 과정에서 악성코드가 유입하여 멀웨어와 같은 악성 바이러스에 감염되게 된다. 지난해 미국에서 판매된 전체 TV 가운데 69%가 스마트TV로 밝혀진 자료만 보더라도 스마트TV는 국내·외 통틀어 가정에 필수품이 되었지만 보안 위협으로 노출될 수 있다는 문제를 인식하고 있는 소비자들은 그리 많지가 않다. 각 스마트TV 제품 기능에는 스마트폰으로 제어할 수 있는 다양하고 편리한 앱이 출시되어 서비스되고 있다. 그런데 편리한 서비스를 TV와 연계하여 이용하는 과정에서 소비자들의 이메일과 IP, 콘텐츠 구매 이력에 대한 정보 등이 노출되게 된다. 스마트TV는 TV 디바이스만으로 기능과 서비스를 제공하는 것이 아니라 인터넷 망, 앱스토어 운영을 위한 WAS, 빌링 서버, 프로비저닝 서버 등의 다양한 서버들과 결합해서 운영되기 때문에 서비스를 제공하는 모든 곳에서 보안 위협이 발생하게 된다[14].

3.1.4 릴레이 공격(Relay Attack)

공격자는 피해자의 스마트카드 소유자로 가장하여 사용자의 요청을 피해자에게 전달하고 사용자에게 실시간으로 응답을 되돌린다. 이 공격 기법은 <그림 4>와 같이 스마트카드와 같은 NFC 토큰과 NFC 리더기 사이의 범위를 확장하는 것이 중요하다. 공격자는 두 개의 NFC 기기에 필요하며 하나는 NFC 리더기로서 작동하고 하나는 카드 에뮬레이터로 작동되게 되어있다. 피해자의 NFC 시스템은 카드가 실제로 앞에 있다고 인식하기에 공격을 탐지할 수 없다. 일반적으로 공격자는 피해자의 스마트카드 근처에서 NFC 리더기를 보유하여 다른 통신 채널을 통해 피해자의 NFC 리더기에 근접한 곳에 있는 스마트카드를 모방할 두 번째 NFC 기기에 데이터를 송신한다. 이 공격은 타이밍 문제에 크게 제약을 받는다. 공격자의 두 NFC 기기 간의 물리적 거리로 인해 데이터 전송시간이 일반적인 NFC 데이터 전송시간보다 더 오래 걸린다는 제약을 가지고 있다[12-13].




<그림 4> 릴레이 공격 방식 [9]

3.1.5. 데이터 손상(Data Corruption)

NFC 데이터 손상 공격은 서비스거부(DoS) 공격과 매우 유사하다. 공격자는 데이터 전송을 방해하거나 수신자가 정보를 해독하지 못하게 데이터의 흐름을 방해하여 전파교란으로 RF 신호를 방해하여 사용자의 정상적인 데이터 수신을 차단하는 공격을 시도한다. 공격자는 공격을 시도하기 위해 전송된 데이터에 직접 접근할 필요는 없으며, 공격자는 신호를 방해하여 무선신호를 송신하는 것만으로도 데이터를 손상하는 공격을 할 수 있게 된다. 또한, 공격의 유형이 서비스거부공격과 비슷하므로 사용자 NFC 기기에 대한 정상적인 데이터 수신 동작을 방해하기 위해 공격자가 준비한 여러 대의 공격 시스템으로 데이터를 집중적으로 보내는 공격을 이행한다[12].

3.1.6 스푸핑(Spoofing)

스푸핑 공격은 NFC가 아닌 일반적인 보안 위협 요소에서도 널리 알려진 보안 위협 요소이기는 하나 NFC 기기에서도 공격 위협에도 노출되어 있다. NFC 근거리 통신에서 스푸핑 공격은 공격자가 사용자가 정상적인 태그인 것처럼 가장하여 사용자가 자신의 NFC 기기를 태그에 탭 하도록 유도한다. 공격자는 악성코드가 포함된 NFC 태그를 통하여 사용자가 NFC 기기로 악성코드가 포함된 태그를 탭 할 경우 자동으로 기기에 악성코드를 자동으로 다운로드하도록 하게 한다. 이러한 유형의 공격에 대한 주요 대책으로 사용자는 자신의 기기를 NFC를 통해 명령이 실행되기 전에 메시지를 표시하여 자동으로 실행되지 않게 설정할 수 있다[12].

# Ⅳ. 보안 위협 문제점 검토 방안 마련

NFC 서비스가 보편화되면서 보안에 대한 취약점은 계속 제기되어 왔었지만, 국내에서는 NFC 사용에 따른 부정사용, 금융정보 유출 및 명의도용, 결제도중 사용자정보 낚아채기 등 일반인이 전혀 인지하지 못하는 심각한 보안상의 문제점이 지적되었다. 그중 가장 많은 보안적 문제점은 NFC 무선 환경에서 개인정보에 대한 유출 위협이었다. 우선적으로 NFC 태블릿 PC, 스마트폰과 같은 모바일 서비스에 대한 사용 억제를 막는 것이 가장 최우선이기는 하지만 생활 속의 편리함을 추구하는 모바일 기기 사용 억제를 막는 것은 너무도 안일한 방법이다. 프랑스와 같은 서구 선진국에서는 NFC 기반 모바일 서비스 사용을 위해 정부기관 및 시의회에서 적극적으로 참여하고 있으며 보안과 관련된 경각심을 일반인에게 홍보하고 널리 알리어 사회적 문제에 따른 심각성을 최소화하기 위해 적극 노력하고 있다.

## 4.1 태그 사용에 따른 안전한 보안 마련

최근 강남 일대 및 홍대, 이대 부근, 서울 중심의 시내에는 스타벅스와 같은 유명 카페를 너무도 쉽게 볼 수 있다. 많은 직장인, 젊은 대학생들이 카페에서 일상생활에 필요한 바쁜 만남을 갖고 음료 문화를 즐기고 있다. 하지만 스타벅스 결제 어플을 통해 NFC 결제 시스템을 이용하는 가운데 안전에 따른 문제적 이슈가 발생할 수 있다. 스타벅스는 국내보다는 해외에서 더 많은 이용자들이 이용하고 있지만, 현재 국내에서도 많은 카페가 생겨나고 이를 이용하는 사람들이 많아지고 있기에 이미 우리나라에서도 스타벅스는 자리매김한 것으로 보여지고 있다. 카페를 즐기는 사람들에게는 빠르고 편리한 NFC 결제시스템이 야말로 젊은이들 사이에서는 대단한 인기를 한 몫 하고 있다. 하지만 Tag와 관련된 논란은 이미 물류, 재

고, 유통 등 여러 분야에서 이용과 관련 데이터 유출 문제가 보고되었지만 스타벅스를 비롯한 NFC 결제 시스템에 이용에 따른 개인정보 유출 문제, 결제오류, 자금 이체 등에 대한 오류가 발생할 수 있다. 또한, 북적대는 많은 이용 고객들 사이에서 스타벅스 카페에서 이용하고 있는 무선 인터넷 통신망에 따른 이용 정보 가로채기와 같은 개인 정보 유출도 관리적인 측면에서 논란이 예상되고 있다. 사소한 피해를 막기 위해서는 가급적 카페 인터넷 공동망 사용을 자제하고 결제 시스템 이용 시에는 반드시 사용 내역에 따른 결제 내역을 스마트폰으로 전송받아 결제에 따른 정확성 진위여부를 반드시 확인하는 습관을 갖는 것이 좋다.

## 4.2 도청 방지 보안 마련

그럼, NFC 기기를 도청으로부터 안전하게 사용할 수 있는 방안을 살펴보도록 한다. 도청은 주로 유선전화나 무선전화, 무전기와 같은 주파수를 이용한 통신기기로 가까운 근거리 내에서만 도청이 가능한 것으로 알고 있지만 근거리를 포함해서 통신 전파를 이용하여 해커들의 필요한 정보를 얻기 위해서는 원격 도청도 가능해진 것으로 알려져 있다. 도청을 제공하는 요소는 NFC를 이용하는 기기에 악성코드가 감염된 경우나 사용자 기기의 주파수를 탐지하여 접근해 오는 방식이다. 가장 우선적으로 도청을 방지하기 위해서는 NFC 기기 간에 설정이 가능한 암호화된 보안 채널을 사용하고 음성 정보가 전달되는 과정에서 암호화되어 전송되는 신호를 복잡하게 혼선으로 도청을 못하게 하는 것이다. 이러한 예방적 방법으로 NFC 기기 간의 근접거리에서만 통신 된다는 점은 도청을 어렵게 만들어 우선적으로 예방에 대한 위협을 피할 수는 있지만, 여러 유형의 도청 공격에 대한 위험을 완전히 제거하지는 못하므로 도청 위협에 대한 경각심을 항상 갖는 것이 좋다.

## 4.3 NFC 안전성 무력화에 따른 보안 마련

비교적 안전하다고 여기는 스마트폰을 더욱 무력하게 만들어 NFC 시용 시 가장 많이 범하는 오류가 있다. 그것은 바로 사용자들이 상업적 어플을 정상적으로 돈을 지불하여 다운받지 않고 불법적인 블랫마켓을 통해 불법 루팅을 자행한 스마트폰을 노리는 공격 위협에 노출되어 있다는 것이다. 스마트폰 업체에서도 이를 염려하여 탈옥과 루팅을 사용자가 시도할 경우, 해킹을 당할 경우 위험으로부터 정보를 잃을 수 있다고 지적하고 있지만, 많은 사용자들이 불법 어플을 다운받아 성능을 높일 수 있다고 착각을 하고 있다. 하지만 이러한 행동은 정상적인 앱스토어의 마켓 경로를 통해 이루어진 다운 방식이 아니므로 심각한 문제를 일으킬 수 있을 뿐만 아니라 불법 어플에는 악성 코드가 감염되어 보안 기능을 무력화하여 NFC 결제 이용 시 공격자에게 공격할 수 있는 빌미를 제공하게 된다. 공격적 루트는 사용자가 NFC 기기로 서비스를 이용할 때 NFC 보안 프로토콜의 약해진 기능을 이용하여 안전한 금융 결제 시스템의 데이터를 도청, 중계 공격을 통해 필요한 사용자의 금융 정보 및 탈취가 이루어진다. 최근에는 안전을 고려하여 각 금융기관에서는 불법으로 루팅된 스마트폰에 금융 어플 서비스 지원을 중단하고 있지만, 여전히 위험 노출에 대한 부분은 잔재하고 있으므로 루팅 및 탈옥과 같은 스마트폰의 보안 기능을 떨어뜨리는 행동은 절대 하지 말아야 한다. 혹시나 불법적 루팅이 이루어졌다면 공장 초기화와 메인보드에 대한 교체 대비도 염두해 두는 것도 좋다.

## 4.4 중계 공격에 따른 보안 대책

릴레이 공격이라 불리는 중계 공격은 공격자가 사용자 단말기에 상호 연결된 통신 채널을 통해 메시지를 주고받는 형태이다. 이 때 사용자는 공격자의 공

격을 우선적으로 차단하기 위해 무선 통신 채널 신호를 변조하여 공격자의 공격 신호를 교란시키는 방법을 이용하도록 한다. 사용자가 사용하는 NFC 무선 환경에서 공격자는 사용자가 모르는 사이에 자신이 이미 확보해 놓은 무선 신호를 사용자와 연결된 통신 채널을 통해 사용자의 관련 정보와 메시지를 주고받게 된다. 당연히 사용자의 관련 정보가 고스란히 공격자 신호로 교신되어 유출되게 된다. 이를 방지하기 위해 앞서 소개한 변조 인증 프로토콜을 사용하여 BCDHE와 같은 키 교환값에 사용되는 암호 인증 프로토콜 <표 2>과 같은 기밀성, 무결성 인증에 사용되는 SCH 암호 인증 프로토콜을 서로 교차하여 사용하여 공격자의 공격을 역으로 이용하고 신호를 왜곡시켜 공격자의 메시지 전달을 사전에 차단하는 역할을 하게 된다. 또한 일정한 신호의 주기를 피하기 우해 SHA 해쉬 암호 방식을 사용하는 것도 좋은 방법으로 제시한다.

### 4.5 데이터 손상(Data Corruption) 보안 마련

무선 신호에 대한 통신 신호 교란은 왜곡이 되고 있어 심각한 문제를 안고 있다. 특히, 보안과 관련하여 일반 사용자가 이를 염려하고 두려워하여 사용을 그만두는 것은 좋은 방법이 아니다. 그렇다고 NFC 읽기/쓰기에 대한 기술을 무력화하여 사용을 기피하는 것 또한 바람직하지 못하다. 데이터 손상 공격에 대한 일반적인 대응책은 무선주파수 신호 검사를 지속적으로 체크하여 의미 없는 신호가 발생하고 송수신되고 있는지를 확인하는 것이다. 만약, 데이터 전송 중에 의미 없는 신호가 발생하는 것이 감지된다면, 사용자 기기를 무력화시키고 정상적인 데이터를 파괴할 수 있는 공격이 시도될 수 있으므로 공격자 태그 신호가 더 이상 접근하지 못하도록 전송을 차단하고 데이터 처리에 대한 이행을 회피해야 한다. 그리고 사고가 더 이상 확대되지 않도록 신속하고 안전한 강구 대책을 조속히 마련해야 한다.

### 4.6 NFC 스푸핑(Spoofing) 공격으로부터 보안 마련

NFC 스푸핑 공격은 사용자의 기기를 빠르게 공격자 자신의 기기로 NFC의 RF 신호를 순간적인 오작동으로 공격자의 기기를 사용자의 기기로 오인케하여 속이는 공격 수법이다. 우선, 선불형 충전식 NFC 기기를 가지고 대중교통 시스템을 이용하는 경우, 사용자가 태그 신호를 갖다 대어 무선 신호를 인식하는 순간 빠른 시간에 공격자 자신의 공격기기를 사용자 태그에 인식되도록 속이어 사용자 교통카드에 대한 금융 갈취를 시도하는 공격을 시도할 수도 있다. 또한, 카페에서 NFC 기기에 설치된 앱을 이용하여 사용자가 결제를 하는 과정에서 사용자의 무선신호를 인식하여 매장에서 판매하는 관련 상품을 홍보하는 이미지를 빠르게 전송시켜 사용자의 관심을 다른 곳으로 돌리게 한 후, 결제 시스템에 대한 정보를 빠르게 자신들이 마련해 놓은 별도의 기기에 신호를 복제하여 동시에 전달하는 공격을 취하게 된다. 만약, 카페에서 결제 내역보다 먼저 상품에 대한 홍보 이미지가 보인다면 이를 관계 매니저에게 확인하여 실제 이벤트 광고가 맞는지를 확인하도록 한다. 또한, NFC 단말기가 업체에 등록되어 사용할 수 있는 상호 신뢰할 수 있는 태그와 리더기기로만 데이터가 전달되고 있는지에 대한 인증 사실을 파악하여 사용자 입장에서 반드시 점검해 보는 것이 Spoofing 공격으로부터 피해를 줄일 수 있는 안전한 예방 방안이라 여겨진다.

또한, 많이 알려진 안정적인 방법으로 보안 수준을 높이기 위해 보안 채널을 확보하여 사용하는 것을 권장하며, 허용되지 않은 무선 신호 시그널 동작에 주의를 갖고 허가되지 않은 신호가 끼어드는 것에 각별히 유의할 필요성이 있다.

[표 2] 암호 인증 프로토콜

| 보안적 요소 | 암호 프로토콜 |
|---|---|
| 암호화 | SSL/TLS |
| 비밀 키 | SSE(Shared Secret Service) |
| 기밀성, 무결성 | SCH(Secure Channel Service) |
| 메시지 인증 | SHA |
| 블록 암호 인증 | CBC |
| 공유 비밀키 | ECDH, AES 128 |
| 키 교환 방식, | ECDHE |

## Ⅴ. 결론

본 논문에서 NFC 무선통신 서비스에 보안 대책이 다소 미흡한 상황에서 위협이 존재할 수 있는 상황에 대해 살펴보았다. NFC는 사용과 관련된 편의성과 활용도로 빠르게 시장이 성장하고 있는 만큼 NFC의 개인정보 유출과 서비스적인 측면에서도 보안 위협이 날로 증가하고 있다. 본 논문에서는 NFC 기기 간 RF 통신 구간에서 도청과 변조 위협으로부터 정보 유출을 방지하기 위해 가장 안전한 방법으로 사용 시 발생할 수 있는 위협적인 공격 상황에서 대처할 수 있는 예방 및 방안을 제시하였다.

앞으로도 NFC의 더욱더 안정적인 사용자 서비스 측면과 위협적 요소에 대비해야 할 것이다. 그러나 NFC의 보안적 위협요소는 항상 우리 주변에서 배제될 수 없기에 IT관련 부처 및 연구 기관에서는 NFC 활성화를 위한 대책 마련을 위해 보안 위협요소로부터 해킹 가능성을 차단할 꾸준한 연구와 노력이 지속되어야 한다고 본다.

## 참고문헌

[1] 이영교, 안정희, “스마트폰에서의 디지털 신용카드 관리 방법,” 디지털산업정보학회 논문지, 제 8권, 제 2호, 2012년, pp. 71[2] http://nearfieldcommunication.org/about-nfc.html

[3] 서장원, 이은영 “NFC를 이용한 스마트폰 상의 사회 공학적 공격 방지 기법 연구,” 디지털산업정보학회 논문지, 제 11권, 제 2호, 2015년, pp. 28.

[4] https://www.androidauthority.com/nfc-tags-expl-ained-271872/

[5] https://nfc-forum.org/what-is-nfc/what-it-does/

[6] https://www.websoptimization.com/blog/top-5-nfc-payment-apps/

[7] http://nearfieldcommunication.org/unexpected-uses.html

[8] https://www.techradar.com/news/phone-and-communications/mobile-phones/nokia-brings-nfc-technology-to-london-museum-991154

[9] 백종현, 염흥열, “NFC 기반 모바일 서비스 보안 위협 및 대책,” 정보보호학협회, 제 23호, 제 2호, pp. 56.

[10] 신상호, 윤은준, 유기영, “NFC 기술동향과 보안 취약점 분석,” 멀티미디어 학회, 제 16권, 제 3호, 2012년, pp. 34.

[11] 김경일, 전귀수, 채규수, “사용자 개인 정보 및 위치정보를 보호하기 위한 NFC 결제 시스템 모델,” 중소기업융합학회논문지, 제 5권, 제 2호, 2015년, pp. 22~23

[12] https://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/#gref

[13] https://www.cyberisk.biz/near-field-communication-security/

[14] http://www.epnc.co.kr/news/articleView.html?idxno=62128

## ■ 저자소개 ■

최 희 식
Choi Heesik

2008년 9월 ~ 현재
경민대학교 IT경영과 외래교수
2002년 2월 숭실대학교 컴퓨터학과(공학박사)
2006년 2월 숭실대학교
컴퓨터공학과(공학석사)

관심분야 : 정보보안, 클라우딩컴퓨터, IoT,
핀테크 금융보안
E-mail : dali3054@ssu.ac.kr

조 양 현
Cho Yanghyun

1997년 9월 ~ 현재
삼육대학교
컴퓨터·메카트로닉스공학부 교수
2011년 2월 광운대학교 전자통신학과
(공학박사)
1985년 2월 광운대학교 전자통신학과
(공학석사)
1982년 2월 광운대학교 전자통신학과(공학사)

관심분야 : 컴퓨터네트워크, 통신망(BcN),
GMPLS
E-mail : yhcho@syu.ac.kr

논문접수일 : 2018년 11월 21일
수 정 일 : 2018년 12월 3일
게재확정일 : 2018년 12월 11일