스마트폰에서 NFC를 이용한 융·복합 하이브리드 취약점

박창민* · Park Neo** · 박원형***

요 약

스마트폰의 최근 보급 확대와 함께 비접촉식 초단거리 무선통신 기술인 NFC(Near Field Communication)기술이 탑재된 모바일 NFC 단말기가 주목을 받고 있다.

본 논문은 모바일 NFC 단말기의 개방형 특성과 다양한 서비스, 통신 기술과의 접목으로 인한 보안 취약성 발생 가능성을 알아보고자 한다. 해커는 악성코드가 포함된 URL을 기록한 NFC 태그를 대중 교통 단말기 근처 숨겨진 장소에 부착한다. 이는 온·오프라인이 결합된 융·복합 하이브리드 성격의 공격시도로서 스마트폰은 NFC 운용모드 중 하나인 Reader/Writer 모드를 통해 악의적으로 부착된 NFC 태그를 인식하여 악성코드에 감염이 된다. 다음으로 단말기 사용자는 NFC 운용모드 중 하나인 Peer-to-Peer 모드 이용으로 불특정 다수에게 무의식적인 악성코드 확산을 돕고, 마침내 지정된 D-day에 모바일 DDoS의 형태로 최종 목표지점을 공격한다는 취약점에 대해서 연구한다.

A Hybrid Vulnerability of NFC Technology in Smart Phone

Park Chang Min* · Park Neo** · Park Won Hyung***

ABSTRACT

Smartphones have all the recent technology integration and NFC (Near Field Communication) Technology is one of them and become an essential these days. Despite using smartphones with NFC technology widely, not many security vulnerabilities have been discovered. This paper attempts to identify characteristics and various services in NFC technology, and to present a wide range of security vulnerabilities, prevention, and policies especially in NFC Contactless technology. We describe a security vulnerability and an possible threat based on human vulnerability and traditional malware distribution technic using Peer-to-Peer network on NFC-Enabled smartphones. The vulnerability is as follows: An attacker creates a NFC tag for distributing his or her malicious code to unspecified individuals and apply to hidden spot near by NFC reader in public transport like subway system. The tag will direct smartphone users to a certain website and automatically downloads malicious codes into their smartphones. The infected devices actually help to spread malicious code using P2P mode and finally as traditional DDoS attack, a certain target will be attacked by them at scheduled time.

Key words : NFC, Smart Mobile Phone, Malware

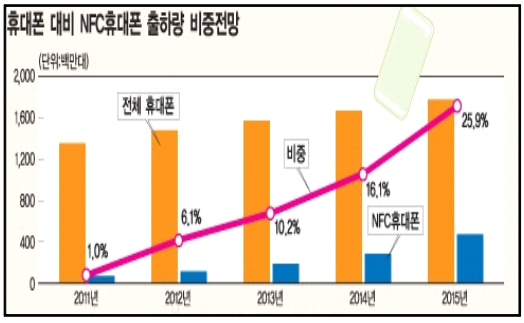
접수일(2012년 8월 6일), 수정일(1차: 2012년 8월 29일), 게재확정일(2012년 8월 30일)

* 서울과학기술대학교 글로벌융합산업공학과
** 극동대학교 유비쿼터스 IT학과
*** 극동대학교 정보경영학과(교신저자)

1. 서 론

NFC(Near Field Communication)는 13.56Mhz의 주파수 대역을 사용하는 비접촉식 근거리 무선 통신 규격으로 10cm 이내의 거리에서 낮은 전력으로 무선 통신을 할 수 있는 기술이다.

무선 네트워크 기술들의 비약적인 발전과 함께 2002년 소니사와 NXP사에 의해 최초로 개발된 NFC 기술은 2003년 ISO 국제표준통신 규격으로 등록되었다. 그리고 2004년 NFC Forum이 설립되면서 그 용어가 널리 사용되기 시작하였다. 2010년 이후 NFC 기술은 기존 스마트 기기의 보급 확대와 동시에 NFC 기능을 지원하는 스마트폰 또한 기하급수적으로 보급됨에 따라 더욱 주목 받고 있다.[1] 하지만 이러한 순기능의 뒷면에 역기능 또한 발생할 수 있다. NFC를 모바일 단말기에 적용하여 사용하는 경우 단말기의 개방형 특성과 다양한 서비스, 통신 기술과의 융합으로 NFC 프로토콜 이외의 영역에서 새로운 사회공학적 기술을 이용한 사이버공격 발생 가능성이 높다.[2]



(그림 1) 휴대폰 대비 NFC휴대폰 출하량 비중전망[3]

최근 스마트 기기에서 NFC 기능을 지원하는 기기가 늘어남에 따라 스마트 기기를 정보의 송·수신을 위한 매개체로 활용하여 다양한 분야에서 융·복합된 형태의 서비스로 확대하고 있다. 기존의 비접촉식 스마트카드 응용 서비스가 아닌 모바일 단말기에 적용된 NFC 기술은 다양한 응용 서비스에 접목이 가능하다. 위 (그림 1)에서는 휴대폰 대비 NFC휴대폰에 대한 출하량 비중전망치를 보여주고 있다. 이를 통해 본다면 향후 NFC 시장은 급속도로 성장하고 그 규모 또한 확대 될 것으로 보인다.

이처럼 스마트 기기에 NFC 기술이 융합됨에 따라 종전의 무선 보안에서 찾아볼 수 없던 새로운 보안 취약점의 발생과 동시에 기존에 알려진 공격기법과는 다른 사이버 공격 시도가 예상된다. 또한 스마트 기기의 보급과 함께 제공되는 다양한 서비스에서 점차 무의식적으로 사용자의 개인정보 유출 또는 경제적 손실을 입히는 침해 사례 발생이 빈번하게 일어나고 있다. 따라서 본 논문에서는 온·오프라인과 NFC 기술이 결합된 새로운 개념의 하이브리드 취약점을 이용한 공격 예상과 향후 대응책을 제시할 목적을 가지고 있다.

2. 관련 연구

2.1 NFC 보안 취약성

NFC 기술은 실생활과 연계된 다양한 정보활동을 위해 모든 타입의 사용자 기기에 대해 "Touch-and-Start" 방식으로 직관적 연결이 가능하다. 여기서 직관적 연결이라 함은 사용자가 두 개의 NFC 장치들을 가까이 접촉하여 복잡한 환경 설정 과정을 사용자 개입 없이 상호작용을 통하여 필요한 정보를 전송할 수 있는 것을 의미한다.[4] 다음의 〈표 1〉에서는 그동안 알려진 NFC 단말기 주요 운영 모드의 발생 가능 취약점과 그 대책을 보여주고 있다.[5]

<표 1> NFC 기술적 취약점 분류[5]

분류	취 약 점	대 책
물리적	도청(Eavesdrop)	보안채널 이용
	데이터 변조 (Data Corruption)	보안채널 이용, RF 필드 체크
논리적	데이터 수정 (Data Modification)	보안채널 이용, RF 필드 체크
	데이터 삽입 (Data Insertion)	보안채널 이용, RF 필드 체크
	중계 공격(Relay Attack)	타이밍 체크, 위치 체크
	중간자 공격 (MITM Attack)	사전비밀 공유, RF 필드 체크
	스마트 포스터 URI 스푸핑 (Smart Poster URI Spoofing)	URI 검증, URI 문법 체크
	NDEF Signature RTD 취약점	헤더필드에 대한 전자서명 지원

이 중에서 도청, 전송 데이터 파괴, 전송 데이터 위변조 공격, 그리고 중간자 공격 등에 관한 취약성을 노린 공격 가능성은 충분히 발생 가능한 것으로 이미 많이 다루어져 왔다.[6][7][8]

본 논문에서는 앞서 다룬 취약점과는 달리 사회 공학적 요소와 사용자의 무의식적 태깅(Tagging)을 통한 취약점 도출에 그 차이점이 있다.

2.2. NFC의 운영 모드

아래 <표 2>와 같이 NFC 단말기의 주요 운영 기능 모드는 3가지로 정의할 수 있다. 먼저 기존의 카드 대신 휴대폰을 갖다 대며 비접촉식 지불이 가능한 Card Emulation 모드가 있다. 두 번째로 NFC 단말기로 NFC 트랜스폰더에 저장된 데이터를 읽고 쓸 수 있는 Reader/Writer 모드, 그리고 마지막으로 두 대의 단말 또는 기기 간 서로 통신하며 데이터 송수신이 가능한 Peer-to-Peer 모드의 3가지 운용 모드로 이루어져 있다.[8]

<표 2> NFC의 주요기능

모 드	내 용	예
Card Emulation	NFC 장치가 기존의 비접촉식 카드로 동작	모바일 신용카드, 교통카드, 카드키
Reader /Writer	NFC 장치가 카드 리더기와 라이터기로 동작	태그 기반 광고, 영화포스터, NFC 메모
Peer-to-Peer	두 대의 NFC 장치가 서로 통신하는 모드	사진, 문서, 연락처 공유

본 논문에서 제시하는 공격은 NFC의 3가지 운용 모드 모두가 유기적으로 연관되어 스마트 기기가 보안 위협에 노출되게 만드는 것이다. 사용자는 NFC의 Card Emulation 모드를 이용하여 교통카드 결제를 위한 태깅을 시도할 때, 결제기 근처에 교묘하게 감춰진 NFC 태그는 또 다른 모드인 Reader/Writer 기능으로 함께 인식되어 공격자가 의도한 특정 URL로 이동을 유도하게 한다. 사용자는 화면에 도출된 피싱사이트를 통해 무의식적으로 업데이트나 다운로드를 하게 되고 이 후 악성코드에 감염된다. 그리고 악성코드의 잠복기 중 사용자는 NFC의 Peer-to-Peer모드로 다른 사용자와 데이터를 교환함으로서 악성코드의 확산 속도는 기하급수적으로 증가하게 된다.

앞서 다룬 공격 과정에서 NFC의 각 운영 모드는 Card Emulation 모드 실행 이 후 Reader/Writer 모드로 넘어간다거나 그 반대의 실행 경우처럼 모드의 선, 후 프로세스가 순차적으로 이루어지는 구조를 가지고 있다.

3. NFC 취약점 공격 시나리오

3.1. 공격 흐름도

스마트폰 사용자는 NFC 단말기의 3가지 운용모드를 통해 다양한 정보의 송·수신 매개체로 하여 여러 분야에 융·복합된 NFC 서비스 이용이 가능하다. NFC 프로토콜 이외의 부분에서 새로운 보안 취약성 발생 가능성을 알아보고자 한다.

새로운 과금 유발 공격이 어떻게 이루어지는지 살펴보면 다음의 (그림 2)와 같다.

(그림 2) 스마트 기기에서 NFC를 이용한 하이브리드 공격 흐름도

3.2. 단계별 분석

본 절에서는 다음 (그림 2)의 공격 흐름도를 감염 및 전파 단계, 피해 단계, 피해 인지 및 대응 단계로 구분한 뒤 순차적으로 분석한다.

3.2.1. 감염 및 전파 단계

① 공격자는 악의적인 목적을 가지고, 악성코드가 포함된 URL을 NFC 태그에 기록한다.

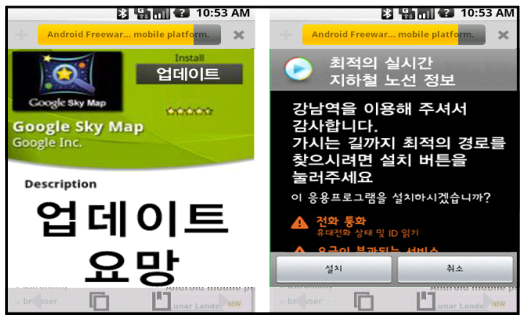
② (그림 3)과 같이 시내버스의 교통카드 단말이나 지하철 개찰구 측면에 잘 보이지 않도록 몰래 NFC 태그를 부착한다. 특히 버스나 지하철 이용자들은 반드시 교통카드 단말 인식 후 통과할 수 있기 때문에 NFC모듈과 교통카드 기능이 탑재된 스마트폰 사용자, 그리고 NFC모듈이 활성화 되어 있는 스마트폰으로 단말에 태깅하려는 사람들은 위험에 노출될 가능성이 크다. 또한, 음란물, 경품 제공 이벤트, 티저 광고 등 사람들의 호기심을 자극할 수 있는 포스터나 전단지에 NFC 태그를 부착하여 감염 숙주를 다양화 할 수 있다.

(그림 3) 지하철 개찰구에 붙여진 NFC 태그를 인식하는 스마트폰

③ 피해자는 버스에 탑승하거나, 지하철 개찰구를 통과할 때 교통카드 단말기에 스마트폰을 가져간다. 이 때 공격자가 부착해 놓은 NFC 태그를 인식 한다.

④ NFC 태그를 읽은 피해자의 스마트폰은 URL 확인절차 없이, 공격자가 만들어 놓은 특정 웹페이지로 이동한다.

⑤ 해당 웹사이트에는 방금 통과한 지하철역과 관련된 유용한 정보(열차시각, 빠른경로, 혹은 운행중단 안내 등)가 담겨져 있고, 해당 정보를 이용하기 위해서는 앱을 다운로드 하게 되어 있다.



(그림 4) 드로퍼(Dropper) 다운로드를 유도하는 웹사이트

위 (그림 4) 처럼 해당 웹페이지는 피싱 사이트이다. 앱스토어의 어플리케이션 다운로드, 또는 업데이트와 유사한 화면으로 꾸며 피해자가 악성코드에 감염되어 드로퍼(Dropper)를 다운받도록 유도한다.

⑥ 스마트폰에 다운된 드로퍼(Dropper)는 악성코드가 담긴 파일을 특정 장소에 설치하고 드로퍼(Dropper) 자신은 삭제한다. 설치된 악성코드의 생성 날짜는 실제 날짜에서 의심하지 않을 만한 다른 날짜로 변경한다. 이것은 향후 수사기관에서 악성코드를 분석할 경우, 감염경로가 NFC 태그라는 사실과 드로퍼(Dropper)의 존재를 최대한 은닉하기 위함이다. 악성코드는 이후 스마트폰 안에서 특별한 징후 없이 잠복한다.

⑦ NFC기능 중 터미널 통신기능(Pear to Pear)기능이 있다. 이것을 통해 다른 스마트폰 사용자와 MP3파일, 사진, 명함 등의 정보 교환이 가능하다. 피해자는 이 기능을 이용해서 다른 스마트폰과 통신할 때, 잠복하고 있던 악성코드도 동시에 전송된다. 이러한 방식을 통해 악성코드가 여러 스마트폰으로 확산 및 감염된다.

3.2.2. 피해 단계

공격자가 설정한 특정한 시점이 되었을 때, 악성코드는 여러 가지 기능을 수행한다. 그 기능들은 크게 세 가지로 압축해 볼 수 있는데 스마트폰의 송수신 기능 제한, 이메일 계정 및 패스워드 정보 유출, 마지막으로 특정 서버를 DDoS(Distributed Denial of

Service)등의 공격기법으로 공격할 수도 있다. 이러한 스마트폰의 악성코드를 이용하면 피해서버의 과부하를 발생시켜 서비스 거부공격을 할 수 있다. 또한, 감염된 모든 스마트폰이 인터넷 서비스를 강제 이용하게 되어 피해자는 자신도 모르는 사이에 과도한 트래픽 사용에 따른 데이터 통신요금을 지불할 가능성도 있다. 이렇듯 스마트폰을 이용한 악성코드를 많은 사용자에게 전파 및 감염시킨다면 여러 가지 사회혼란을 야기 시킬 수 있다.[9][10]

3.2.3. 피해 인지 및 대응 단계

피해자는 과금 지불 후, 자신의 스마트폰에 뭔가 문제가 있다는 것을 인식하게 된다. 이후 피해자가 스마트폰을 안랩과 같은 백신업체에 샘플파일 및 로그 전송 등을 통해 보안점검을 의뢰할 경우 악성코드를 탐지하고 삭제하는 것은 어렵지 않지만 초기 생성 날짜를 변경하고 악성코드를 자동 삭제한 드로퍼(Dropper)의 존재를 파악하는 것은 쉽지 않다.

악성코드의 시그니처가 백신 엔진에 등록되었기 때문에 공격자는 추후 공격코드를 변형(난독화 또는 암호화, 메소드 이름 변경)하여 유포할 수도 있다. 이에 따라 악성코드의 지속적인 유포 또한 가능하다.

4. NFC 취약점 대응 방안

4.1 NFC 취약점 대책

다음 <표 3>은 앞서 다룬 내용들을 종합하여 기술적, 관리적, 제도적으로 나누어 본 NFC 서비스 취약점 및 대책이다.[5]

<표 3> NFC 서비스 취약점 및 대책[5]

구 분	취 약 점	대 책
기술적	모바일 APP 종료상태에서의 R Reader 기능	NFC 기능 On/Off 설정 지원
관리적	서비스 이용 시	서비스 이용 시
	추가 정보 요구	추가적으로 요구하는 정보에 대해서 이용자에게 명확히 알리고 동의를 받는 절차를 수립
제도적	모바일 APP에서 개인정보 과다 저장	NFC 단말기의 모바일 APP에는 최소한의 개인정보만을 저장하게 하고, 암호화하여 저장

추가적으로 온·오프라인이 결합된 융·복합 하이브리드적 성격을 가진 취약점을 이용한 시나리오 공격 기술에 대한 NFC 보안 예방책은 다음과 같다.

NFC 기능은 필요하지 않은 경우 비활성화 하여야 한다. NFC 서비스는 근거리에서 무선방식으로 이루어지기 때문에 사용자가 모르는 사이 NFC 서비스 활성화 또는 추적 가능성을 이를 통해 방지 할 수 있다.

검증되지 않은 NFC 태그를 인식해서는 안되며, 이를 통한 위·변조된 앱을 설치하여서는 안된다. 또한, 앞서 연구한 공격 시나리오과 마찬가지로 검증되지 않은 NFC 태그가 자동으로 인식되거나 위·변조된 앱의 주소로 이동하여 다운로드나 업데이트와 유사한 화면에 속아 설치 시 단말기에 악성코드 및 바이러스가 유포될 우려가 있다.

NFC 단말기에 백신 프로그램 설치와 정기적인 검사를 하여야 한다. NFC의 P2P 기능은 개인의 연락처 전송에 유용한 기능인데 악성코드로 인하여 다른 이용자에게 전송되지 않아야 할 정보까지 전송될 수도 있다. 따라서 이를 방지 하기위해 항상 백신 프로그램은 최신버전으로 업데이트하고 정기적으로 검사를 해주어야 한다.[11]

5. 결 론

본 논문은 급증하고 있는 NFC 단말기의 취약점과 향후 보안위협 가능성에 대해 연구하였다. 국내에서

도 NFC 기술과 관련된 다양한 응용 서비스가 활성화되고 단말기의 수 또한 기하급수적 증가가 예상되는 가운데 보안상의 문제 또한 함께 발생할 것으로 예상 된다.

본 연구를 통해 NFC 서비스를 이용하는 사용자들이 침해사고 및 금전상의 피해 없이 NFC를 자유롭게 사용할 수 있는 환경이 구축되기를 기대한다. 또한 앞서 소개한 보안상의 문제점뿐만 아니라 새로운 사회공학적 공격기술에 대한 지속적인 연구와 취약점 연구가 필요 하다.

참고문헌

[1] 한국RFID/USN융합협회, NFC를 활용한 비즈니스 모델 기획, 2011

[2] Security aspects of mobile phone virus: a critical survey, Industrial Management & Data Systems Volume 108, 2008

[3] IMS Research, 휴대폰 대비 NFC휴대폰 비중전망, 2011

[4] 임선희 외 3인, NFC 보안 기술 분석 및 UICC 적용 효과 연구, 한국통신학회, 2011

[5] 숭실대학교 산학협력단, NFC 개인정보보호 대책, 한국인터넷진흥원, 2011

[6] Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones, International Conference on Availability, Reliability and Security, 2009

[7] Practical NFC Peer-to-Peer Relay Attack using Mobile Phones, RFIDSec, 2010

[8] 김선배 외 2인, NFC에서의 보안 취약점 분석, 한국인터넷정보학회, 2011

[9] 이수미 외 3인, 모바일 NFC기반 보안 동향, TTA Journal Vol.133, 2011. 7

[10] Practical Attack Scenarios on Secure Element-enabled Mobile Devices, 4th International Workshop on Near Field Communication, 2012

[11] Addressing Security and Privacy Risks in Mobile Applications, IT Professional, 2012

[저 자 소 개]

박 창 민 (Chang-min Park)

2009년 서울과학기술대학교 글로벌융합산업공학과 입학
현재 서울과학기술대학교 글로벌융합산업공학과 네트워크보안 Lab 연구원
KISA 대학정보보호동아리(KUCIS)서울·경기·강원권역 홍보부장

email : pcm0317@daum.net

Park Neo (Neo Park)

2002년 건국대학교 토목공학과 학사
2008년 미국 유타주립대학교 컴퓨터사이언스학과 2nd B.S.
2010년 미국 유타주립대학교 컴퓨터사이언스 대학원 M.S
현재 극동대학교 유비쿼터스학과 전임교수/정보관리처장

email : neopark2@gmail.com

박 원 형 (Won-hyung Park)

2002년 서울과학기술대학교 산업정보시스템공학과 공학사
2005년 서울과학기술대학교 정보산업공학과 공학석사
2009년 경기대학교 정보보호학과 이학박사
2011년 서울과학기술대학교 산업정보시스템공학과 겸임교수
현재 극동대학교 정보경영학과 전임교수

email : whpark@kdu.ac.kr