디지털산업정보학회 논문지 제14권 제1호-2018년 3월
http://dx.doi.org/10.17662/ksdim.2018.14.1.045

모바일 앱 서비스 이용 증가로 인한 보안 위협 분석*

최 희 식** · 조 양 현***

Analysis of Security Threats from Increased Usage of Mobile App Services

Choi Heesik · Cho Yanghyun

〈Abstract〉

Recently, because the arrival of the fourth industrial revolution era, many information and telecommunication services have grown rapidly in the mobile business market. So, companies are based Mobile Apps on user customized services and expanding their services. From the standpoint of the business, to generate revenue, the company needs to maintain the existing current computer environment and develop Mobile Apps to offer convenience in various areas such as finance, admiration, e-commerce and sales support. However, as the number of users increase due to expansion of various Mobile services, security threats that are related to Mobile Apps are increasing and its damage is also increasing. Due to the rapid technological transformation of Mobile devices using the Internet, the level of security threats to Smartphones are rising and getting more advance, so this thesis is structured as follows. In Chapter 2, it will look at the overall trends of Mobile Apps as related research. In Chapter 3, it will discuss various security concerns that related to the latest Mobile Apps and learn about the threatening factors. In Chapter 4, it will compare and analyze the threatening factors. Then it will find and suggest the possible plan. In Chapter 5, it will end with conclusion. Finally, to protect mobile devices from security threats, the environment of operating system which manages the resources and data of Apps needs to be protected. Also, it is important that users to have awareness and check activation FinTech technology security in the process of simple payment with fingerprint or IC card.

Key Words : Mobile App, Security Threats, Smart Phone, Mobile Device

Ⅰ. 서론

최근 4차 산업혁명 시대가 도래되면서 많은 정보통신 기반의 서비스가 모바일 비즈니스 시장의 급속한 성장에 따라 고객들의 모바일 사용 패턴이 모바일 앱 기반으로 이동되면서 기업들은 사용자 맞춤형 서비스로 앱 개발을 확대하여 운영되고 있다. 이는 기존 하드웨어 플랫폼의 기본적인 서비스 기반에서

* 본 연구는 2016년 삼육대학교 교내 연구비 지원으로 수행된 연구임(The Research Foundation of Korea funded by the Ministry of Education, No. 2017R1D1A1B03030759)
** 경민대학교 IT경영과 외래교수
*** 삼육대학교 컴퓨터학부 교수(교신저자)

스마트폰기기와 같은 이동성 특징을 고려하여 생활에 필요하고 편리한 기능을 모바일 앱을 통해 비즈니스 창출을 얻기 위한 새로운 서비스의 변신이라고 볼 수 있다. 현재, 각국 정부기관을 비롯하여 대부분의 기업, 통신사, 학교, 은행, 병원 등에서 고객 서비스 및 새로운 수익 창출을 기대하여 하드웨어 기반에 추가적으로 기관 성격에 부합되는 편리하고 새로운 기능이 추가된 다양한 모바일 앱을 개발하여 지원하고 있다. 특히, 스마트폰 및 태블릿 PC와 같은 모바일 이동 기기의 대량 보급과 함께 모바일 앱 서비스가 경쟁사들 사이에서 이원화적인 서비스로 동시에 지원되고 있기에 모바일 앱 개발 경쟁은 치열할 수밖에 없다. 이런 이유로 사용자들은 앱스토어를 이용하여 자동차의 네비게이션, 모바일 지도 찾기, 철새의 이동경로, 교통 흐름 정보, 질병의 원인 파악 등 다양한 분야에서 적용되고 있다[1]. 다양한 소비자의 욕구를 충족시킬 수 있는 디지털콘텐츠를 자유롭게 다운로드하여 모바일을 이용하게 된다. 이러한 뜨거운 앱 시장 경쟁 속에서 해커들은 각종 변종된 다양한 앱 등을 개발하여 시중에 유포한 후, 소비자의 개인정보 및 금전 갈취를 시도하는 앱 등을 유통시키고 있으므로 이와 관련하여 정보보안에 대한 예방과 대책 마련은 매우 중요하다고 하겠다[2].

본 논문에서는 모바일 앱 개발과 관련된 사용자들의 환경 변화와 모바일 사용에 따른 취약적인 위험 유형을 분석하여 논문을 구성한다. 2장에서는 관련 연구로 모바일 앱과 관련된 전반적인 사항에 대해서 살펴보고, 3장에서는 모바일 앱과 관련된 위협적인 유형에 대해서 알아보고, 4장에서는 문제점을 검토하고 문제점에 대한 방안을 제시하고, 5장에서 결론으로 마무리하고자 한다.

II. 관련연구

기존 하드웨어 플랫폼 컴퓨팅 환경에서는 이용자가 데이터를 이용하기에는 정보적인 활용 면에서 여러모로 불편하고 다양한 서비스를 활용하는데도 제약적이었으며 하나의 소프트웨어를 설치하더라도 직접 구매하여야만 하는 번거로운 사항도 있었다. 하지만 무선영역의 네트워크 서비스가 확대되고 모바일 기기가 활용되면서 다양한 서비스가 하드웨어 플랫폼에서 모바일 플랫폼으로 이동하게 되었다. 뿐만 아니라 모바일 컴퓨팅 환경에서는 실시간적인 모든 자원을 가상화된 형태로 인터넷을 통해 제공받을 수도 있게 되었다. 사업자 입장에서도 수익 창출을 위해 기존 컴퓨터 환경을 유지하면서 새로운 비즈니스 및 서비스 측면에서 모바일 앱을 개발하여 금융, 행정, e커머스, 결제, 판매 등 다양한 분야에서 편리성 제공과 함께 수익 창출을 위해 앱 활용이 자리를 잡아가고 있다.

2.1 모바일 앱

모바일 앱이란 Mobile Application의 약어로 스마트폰, 태블릿 PC 등과 같은 이동기기를 모바일 환경에서 이용할 수 있도록 개발된 응용 소프트웨어로 모바일 앱은 단말이 출시될 때 탑재되어 출시되는 '탑재형 앱(Preload App)'과 사용자가 마켓을 통해 설치할 수 있는 '설치형 앱(Download App)'으로 구분한다. 탑재형 앱은 단말 출시 전 단말 제조사에서 각 기능 모듈 검증, 앱의 취합 및 검증을 수행하고, 솔루션 제공사에서 플랫폼 기능 검증, 플랫폼 호환성 검증 등이 이루어진다. 또한, 설치형 앱은 단말 출시 후 서비스사업자의 주관 하에 사업정책에 의한 평가 및 검증, 배포가 이루어진다[3].

2.2 모바일 운영체제 방식

모바일 환경의 OS 종류에는 크게 3가지 환경에서 개발되어 보급되는데 아이폰(iOS) 방식, 안드로이드 <표1 > 방식, 윈도우를 지원하는 방식으로 구분한다.

① 아이폰(iOS) 방식 : 아이폰을 사용하는 사용자를 위해 개발사가 앱이 개발되게 되면 앱스토어에 업로드를 하는데 iOS방식은 업로드 되기 전에 애플사의 엄격한 심사를 받는다. 심사 후, 애플이 허락하는 앱만을 유통시키므로 사용자들은 가급적 유해한 악성코드 앱으로부터 보호받을 수 있다는 것이 장점이다. 또한, iOS는 하드웨어를 직접 생산하는 업체에서 탑재시키므로 보안 측면에서도 우수함을 평가받고 있다[4].

② 안드로이드 계열 : 안드로이드의 장점은 오픈소스로 모바일에 최적화된 앱으로 빠르고 쉽게 앱을 개발할 수 있으며 이식성이 뛰어나다는 장점이 있다. 뿐만 아니라 아이폰에 비해 필요한 앱을 좀 더 쉽게 구할 수 있으며 <표 1>과 같은 제품에 탑재되어 서비스되고 있다.

<표 1> 안드로이드 계열 제품 [5]

	안드로이드 계열 스마트폰
제조사	삼성 터치위즈
	소니 모바일 소니 레이첼
	KT테크 테이크 UI
	샤오미 MIUI
	모토로라 모토블러
	팬택 플럭스 UI
	LG전자 LG UX
	샤프전자 Feel UX
	HTC Sense
	화웨이 Emotion UI
	Jide Remix OS
	vivo FunTouch OS

③ 윈도우 계열 : 마이크로소프트사에서 개발한 스마트폰으로 윈도우10과 연동성이 뛰어나며 PC, 서페이스 태블릿, 스마트폰에 자체 윈도우 운영체제를 기반으로 서비스하고 있다. 그러나 후발주자이면서도 애플과 안드로이드폰 제품들에 비해 다양하고 편리한 앱에 대한 공급이 부족하고 성능과 다양성 측면에서 까지 경쟁사에 밀리면서 소비자들의 경쟁력 확보가 쉽지 않고 있다.

2.3 모바일 앱 개발 방식

모바일 앱은 이용자가 사용하는 해당 기기의 OS에 맞추어 개발되어 빠른 속도와 API구현, 웹과의 뛰어난 연동성으로 사용자에게 필요한 정보를 제공한다.

① 모바일 앱 : 모바일 앱을 사용하면 카메라, GPS, 블루투스, 생체인식 등 스마트폰 하드웨어가 제공하는 기능을 활용한 서비스를 만들 수 있다는 점이 가장 큰 장점이다. 특히, 푸시 알림은 사용자들을 유지시키고, 참여도를 높일 수 있는 검증된 방법이며, 단점으로는 모바일 앱에만 올라간 콘텐츠는 구글이나 네이버에서 검색되지 않는다는 것이다[6].

② 네이티브앱 : 특정 모바일 OS로 맞추어져 있어서 가장 빠르고 UI 등, 앱 제작에 필요한 다양한 요소가 패키지화되어 있다. 편리한 개발 툴과 라이브러리를 제공하여 개발 쉽고 유지보수도 쉽다. 프로그램 구동 시에 매우 빠르고 안정적이지만 플랫폼별로 어플리케이션을 별도로 개발해야 하는 것은 단점으로 지적된다.

③ 하이브리드앱 : 모바일 앱의 단점을 해결하기 위하여 앱의 성격이 비교적 간단하여 구동 속도가

모바일 앱 보다 빠르며 하나의 소스로 모든 모바일 플랫폼에서 실행 가능하다. 하드웨어 기능을 사용할 수 있으며, 앱스토어를 통해 배포되나 한번 다운받은 앱은 항상 고정되어 변하지 않는 요소들을 앱으로 만들어서 사전에 배포하고 변동되는 콘텐츠만 그때그때 다운로드 받으면 된다. 그러나 모바일 플랫폼이 제공하는 모든 기능을 사용하지 못하며 네이티브앱 보다는 속도가 떨어진다[7].

2.4 모바일 앱 개발 구성

모바일 앱을 개발하는 데 있어서 기능적으로 이용자에게 필요한 정보 및 콘텐츠를 제공하기 위해 아래와 같은 4개의 중요한 구성요소가 필요하다.

① 활동(Activities) : '활동' 요소는 앱이 사용자와 상호 작용을 하려는 시작점을 일컫는다. 주로 사용자 인터페이스를 포함하고 있는 단일 화면으로 이루어져 있다. 이 '활동'들의 조합이 사용자의 편리성을 증가시키나, 각 '활동'들은 서로 독립적으로 작용한다. 만약, 이메일 앱이 허용하는 경우 다른 앱이 이메일 앱의 '활동' 중 하나를 통해 시작 할 수 있다. 사진 앱의 경우 이메일 앱의 첨부 기능의 사진 첨부를 통해 시작 할 수 있다.

② 서비스(Services) : '서비스' 요소는 앱이 다양한 기능으로 백그라운드 상태에서 실행되기 위한 범용적 시작점이다. 이 요소는 앱이 백그라운드에서 장기 작업 또는 원격 프로세서 실행 등을 담당한다. '서비스'는 '활동'과 다르게 사용자 인터페이스를 제공하지는 않는다. 예를 들어 사용자가 다른 앱을 사용하고 있는 동안 백그라운드에서 음악을 재생하거나 사용자의 다른 앱을 통한 활동을 방해하지 않고도 백그라운드에서 데이터를 네트워크로부터 가져올 수 있는 기능을 수행한다. 또한, '서비스' 요소는 앱이 작업이 완료 될 때까지 실행하도록 시스템에 알리는 기능도 수행한다. 이로 인하여 사용자는 앱을 사용한 후에도 앱의 데이터를 동기화하거나 음악을 재생 할 수가 있게 된다.

③ 브로드캐스트 수신(Broadcast receivers) : '브로드캐스트 수신' 요소는 시스템이 이벤트 등을 일반 사용자 흐름 외부의 앱에 전달할 수 있게 하며 앱이 시스템의 전체 브로드캐스트 공지에 응답할 수 있도록 허락한다. 또한, '브로드캐스트 수신'은 시스템이 현재 실행되고 있지 않은 앱에서도 브로드캐스트 공지를 전달 할 수 있게 한다. 예를 들어, 앱에서 알림을 설정하여 향후 이벤트에 대해 사용자에게 알릴 수 있으며 '브로드캐스트 수신' 요소를 통해 알람이 울릴 때까지 앱이 실행되고 있지 않아도 된다. '브로드캐스트 수신'의 예로는 배터리 부족 알림, 스크린샷 알림 등에 대한 알림 서비스가 있다.

④ 콘텐츠 제공(Content providers) : '콘텐츠 제공'요소는 앱 개발을 위한 요소 중에서 가장 중요한 항목이다. 기능적 중요 역할로는 파일 시스템, 데이터베이스, 모바일 웹과 같은 영구 저장장치에 저장할 수 있는 공유된 앱 데이터를 관리한다. 예를 들어 안드로이드 시스템은 다른 앱이 '콘텐츠 제공' 요소를 통하여 허가 하에 특정 정보를 조회하거나 수정할 수 있게 한다[8].

Ⅲ. 모바일 앱 보안 위협

각종 모바일 서비스의 확대로 인해 사용자가 늘어남에 따라 모바일 앱 관련 보안 위협으로 인한 피해도 늘어나고 있다. 최근, 인터넷을 활용한 모바일

디바이스의 빠른 기술적 변환에 따라 모바일 악성코드로 인해 스마트 폰에 대한 보안 위협 수준도 고도화 되고 있다. 최근 이슈된 보안 위협중 하나는 스팸 메시지를 이용자에게 전송하여 해당 앞을 추가적으로 다운로드하여 설치하도록 유도하는 방식의 악성코드가 전송되고 있다. 특히, 사용자 대부분의 스마트폰이 24시간 외부 인터넷과 연결되어 있으므로 보안 위협은 항상 노출되어 있다고 볼 수 있다. 시간이 지날수록 많은 사용자가 필요한 모바일 앱을 계속해서 선호함에 따라 모바일 앱에 대한 악성코드와 관련된 보안 위협은 계속해서 증가할 것으로 보여 진다.

3.1 스마트TV 정보 유출 위협

최근 3~4년 전부터 보급되고 있는 대부분의 UHD급 스마트TV에서 해커들이 TV를 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 가정이 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[9].

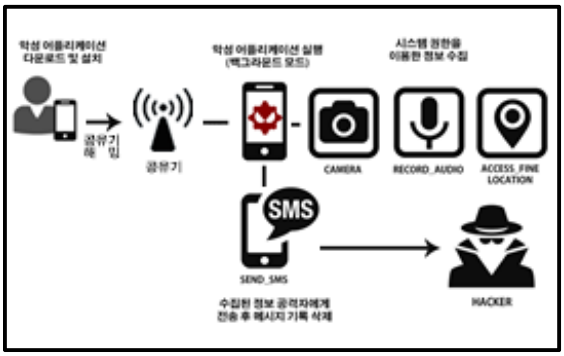
3.2 특정 스마트폰 기기 플랫폼 위협

대부분의 모바일 악성 코드는 특정 기기를 대상으로 개발되어 유포되는데 특히, 안드로이드 기기 사용자를 타깃으로 만들어진 유형으로 피싱(Phishing), 라이크잭킹(Likejacking), 웹사이트 리디렉션(Redirection), 랜섬웨어 공격 등이 포함된다. 랜섬웨어 중 위험도가 높은 것은 스마트폰 관련 앱을 설치했다가 악성 랜섬웨어에 감염되어 사용자 스마트폰을 Lock시켜서 더 이상 사용할 수 없도록 하는 경우도 있다. 스마트폰 랜섬웨어에 감염되게 되면 사용자 동의 없이 원격 조정으로 특정 앱을 강제 실행시키는 것은 물론 스마트폰에 저장된 모든 정보를 유출해 갈 수도 있다. 특히, 안드로이드 공식 앱마켓에서 악성코드가 포함된 앱을 직접 등록하여 모바일 악성코드 유통 경로를 확대하여 유통시키고 있으므로 안드로이드 관련 스마트폰 사용자의 각별한 주의가 필요하다. 뿐만 아니라 스마트폰 특정 폴더에 데이터 파일을 일반 파일인 것처럼 숨기고 속여서 코드가 실행하게 되면 악성코드를 실행시켜 스마트폰을 감염시키는 유형도 있다[10].

3.3 센서 기반 위치 추적 보안 위협

모바일 기기의 위치기반 서비스는 위치결정시스템과 위치정보 서버 사이의 연결이나 위치정보 서버와 정확한 정보를 수신하는 중재자인 위치기반 서비스 제공자 사이의 네트워크 연결이 진행되면서 제공된다[15]. 사용자 위치 추적에 대한 보안 위협 공격 시나리오는 <그림 1>과 같이 우선적으로 불특정 다

수의 취약한 공유기를 모색하여 선점한 후, 해킹을 시도한다. 해킹으로 접수한 스마트폰을 허위의 포털 사이트로 접속하도록 유도하여 백그라운드 모드에서 악성 앱을 설치하여 감염시키게 된다.

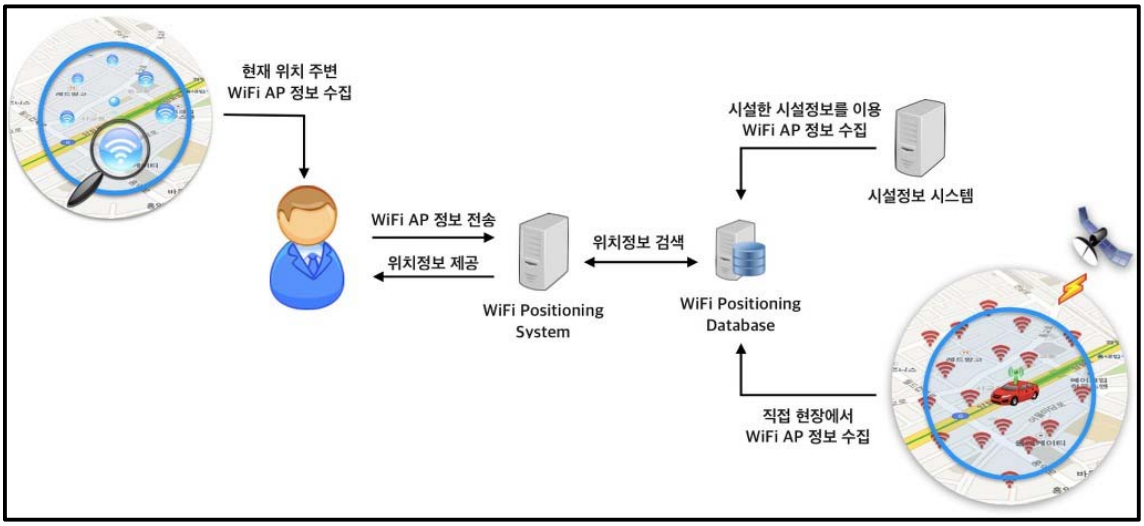


<그림 1> 시스템 권한 공격도 [12]

감염된 스마트폰은 공격자가 공격에 필요한 포털 가입에 필요한 인증번호나 위치기반에 필요한 동의하는 승인 인증 정보를 득하게 된다. 사용자 동의 없이 공격자가 유도한 대로 필요한 정보를 득한 후, 위성으로부터 사용자 위치 이동에 따른 이동 추적을 받기 위해 수신 GPS, 카메라, 마이크 장치에 따른 관련 디바이스 앱이 사용자 스마트폰에 자동으로 설치되어 외부의 해커로 부터 전달된 명령을 원격으로 위치 정보를 입수하고 수집하는 역할을 전달받게 된다.

사용자 이동에 따른 대부분의 위치 정보는 <그림 2>와 같이 사용자 스마트폰의 가장 가까운 이동통신사 기지국과 교신하며 사용자가 전화를 하는 수·발신의 신호나, 문자 메시지를 주고받는 신호를 통해 사용자가 가까이 있는 기지국으로부터 정보를 수집하게 된다. 또한, 스마트폰 사용자 위치를 반경 수백 미터 수준으로 위성으로부터 추적하여 게 된다.

특히, 기지국이 촘촘하게 있는 도시의 경우 더 정확한 위치 추적이 더 가능하게 된다. 이러한 사용자 위치 정보를 입수하여 전달받은 악성 앱은 주기적 혹은 특정 조건이 만족되면 특정 명령 서버에 접속하여 감염된 스마트폰의 정보를 남기고 공격자가 유도하는 정보를 받아와 공격자가 제공받는 특정 서버로 정보를 전송받게 된다. 전송되는 중요한 정보에



<그림 2> 사용자 위치 정보 [14]

는 주로 사용자의 통화기록, 시간별 이동에 따른 행적 기록, 문자 메시지, 이메일 내용, 저장되어 있는 전화번호 목록, 사진 정보에 수록되어 있는 각종 이미지 등을 유출하게 된다. 해커에 의해 유출된 정보는 웹을 통해 필요한 사람에게 돈을 받고 거래되기도 하며 제 3의 가상 인물로 아바타와 같은 새로운 공격자가 탄생하여 또 다른 공격에 가담하기도 한다. 공격에 주로 사용되는 앱의 유형은 Android용 Tapsnake, flexispy, ADRD, PJAPPS, GEINIMI 등이 공격에 사용되었던 앱으로 알려져 있다[11].

3.4 금융 앱 보안 위협

최근 스마트폰을 이용하여 모바일 뱅킹, 간편 결제, SNS 사용자 끼리 현금을 이체할 수 있는 생활편의 금융 거래가 빈번함에 따라 이에 따른 금융서비스의 위협이 나날이 증가하고 있다. 가장 큰 이유는 스마트폰이 보편화 되면서 모바일 앱을 이용하는 편리성이 인터넷에 접속하여 금융거래를 이용하는 편리함이 가장 큰 이유일 수도 있다. 그러나 일상에서 너무도 잘 유용하게 이용되고 있는 스마트폰이 각종 해커들이 설치해 놓은 악성 앱 설치에 유도되어 금융 위협에 피해를 입는 사례도 증가하고 있다. 대부분의 악성 앱 유포 방법은 크게 2가지 유형으로 근거리 무선망 사용 시 공유기 해킹 후 해당 공유기에 연결된 모바일 기기에 악성 앱을 감염시키는 방법, 이메일 및 SMS 또는 큐싱 등으로 사용자가 공식적인 금융기관 어플리케이션으로 오인케하고 다운로드 하게 하여 금융정보를 탈취하는 방법 등이다[12]. 만약, 사용자가 악성 앱을 설치하게 되면 스마트폰에 저장된 개인정보는 물론 사용자가 입력하는 값(계좌번호, 비밀번호, 공인인증서 번호 등)은 모두 키로깅(Keylogging)되어 공격자의 서버로 정보가 전송되기도 하며, 추가로 악성 어플리케이션이 설치된 단말기가 루팅 또는 탈옥된 상태라면 공격자가 최고 권한(root)을 가지기 때문에 그 피해는 더욱 커질 수밖에 없다[13].

3.5. 공격자 제어 기반 악성 행위

사용자가 특정 앱을 사용하기 위해 관련된 특정 앱을 구동하게 되면 일정 시간이 지난 후 악성행위를 시작하도록 하는 앱의 유형이다. 이 앱은 특정 시점 이후에만 악성행위를 시작하도록 하는 등 단순히 시간을 지연시키며 공격자로부터 명령을 받거나 특정 키워드가 삽입된 문자 수신시에만 악성행위를 시작하도록 되어 있다. 즉, 공격자 제어 기반으로 악성행위를 시작하는 형태이므로 사용자가 앱 구동 시, 바탕화면 페이지 전환 시, 네트워크 환경 설정 변경 시, 사용자가 지리적 정보를 사용하기 위해 GPS 정보를 이용 시 단말 동작이 탐지되어 악성행위를 시작하도록 하는 형태 이므로 사용자는 어떤 앱이 악성코드에 감염되어 본인의 개인정보를 유출하고 있는지를 전혀 모르기 때문에 피해에 대한 문제를 파악하기란 쉽지가 않다[14].

VI. 문제점 방안 검토

모바일 앱 위협으로 부터 우선적으로 모바일기기를 보호하기 위해서는 앱들의 리소스와 데이터를 관리하는 운영체제 환경이 보호되어야 한다. 최근에는 모바일 앱의 활용도가 높아지면서 사용자 스마트폰 백그라운드 모드에서 모바일 기기를 공격자가 유도하는 형태로 변경하여 조작이 가능하고 앱스토어를 비롯하여 외부에서도 원격 조종 제어가 가능해 졌다. 4장에서는 3장 모바일 앱에 관련된 위협과 피해적 사례를 참조하여 사용자가 피해를 최소화할 수

있는 여러 방안을 검토하여 방안을 제시한다.

4.1 위치 추적 앱 검토

최근 출시되는 대부분의 스마트폰에서는 강력한 GPS 기능이 탑재되어 사용자의 위치를 파악하여 대중교통 정보, 택시, SNS 이용 시 편리한 위치 정보를 사용자에게 제공하고 있다. 뿐만 아니라 연인들끼리 서로의 위치 소재를 파악하여 끊임없는 관심과 상대방이 어디에서 무엇을 하고 있는지를 궁금해 하고자 한다. 스마트폰 위치 추적은 사생활 유출로 인한 개인정보 유출 논란에 심각한 사회적 논란으로 이어지고 있다. 더욱 심각한 것은 스마트폰 위치 추적을 통해 사진, 문자 메시지, 지리적 정보, 전화 도청 등으로 악용되고 있다는 것이다. 가장 우선적으로 사용자의 이동 거리 및 현재의 위치 장소 파악이 쉽게 노출될 수 있으며, 더욱 놀라운 사실은 사용자의 자세한 시간별 이동 경로와 주변 환경에서 일어난 사용자의 일상 대화 내용까지 녹음되고 있다. 위치 추적은 해당 기기 사용자를 광범위하게 감시하여 위치 추적을 통해 획득한 정보를 해커의 특정 서버로 실시간 전송이 가능하다. 대부분의 사용자가 스마트폰 기능에서 제공하는 Location 정보를 간과하는 경우가 많은데 이러한 위험에 대한 경각심을 갖고 예방하기 위해서는 Location 정보를 필요시만 On으로 설정하고 대부분 Off로 설정해 두는 것이 좋다. 또한, 센서와 관련해서 카메라 렌즈 부분의 탈부착 스티커를 이용하여 주변 환경과 다른 사람의 신상이 녹화되어 전송하는 것을 사전에 방지하는 것이 좋다. 또, 다른 추가적 예방으로 녹음 기능에 대한 부분도 세세한 관심을 가지고 주기적으로 확인해 보는 것이 좋다. 이는 본인의 통화 내용과 주변 사람들과의 대화 내용을 도청하여 자료가 전송됨을 주지하기 위해서이다.

4.2 생활 필수 앱 검토

대부분의 생활 필수 앱들은 무심코 그냥 지나쳐 버릴 수 있고 믿고 이용할 수 있는 앱들이 대부분이므로 이러한 악성 앱들은 대기업을 사칭해서 문자를 보내기 때문에 사용자들은 의심하지도 않고 바로 클릭해 버려서 피해를 입는 경우가 많다. 모바일 환경에서 사용자들이 무심코 당할 수 있는 생활에 필요한 필수 앱 서비스에서 다양한 보안 위협 요인을 검토해 보자.

① 스파이앱 : 보안 업데이트를 하라는 문자를 보내는 정상적인 앱으로 위장을 한 앱 이므로 설치 권장을 요구할 경우 무조건 삭제하는 것이 좋다.

② 게임 앱 : 최근 대중들의 인기를 끌고 있는 게임 앱이 불법 복제되거나 악성코드가 숨겨진 가짜 앱이 많으므로 앱 설치 시 사용자 리뷰, 다운 조회 수 등을 참조하여 신중하게 판단하는 것이 좋다.

③ 쿠폰 문자 : 스타벅스(Starbucks), 커피빈(CoffeeBean), 엔젤인어스(AngelInUs)와 같은 유명 커피 브랜드를 사칭하여 멤버에 가입한 사용자의 정보를 파악하여 무료 음료, 커피 쿠폰을 다운받도록 변조된 링크 문자 메시지를 전송한다. 사용자가 해당 링크를 클릭하여 무료 쿠폰을 다운받는 순간 악성 앱이 깔리게 되어 악성 코드에 감염되게 된다. 이러한 공짜 쿠폰은 해당 업체에서 정식 홈페이지에 로그인하여 다운로드하는 방식이므로 공짜 쿠폰 링크는 영원히 Blocking하여 스팸 처리하도록 한다.

④ 소액결제 : 스카이프, 핸드폰 소액결제, 커피 주문 시 결제에 관한 에러 메시지를 전송하여 금전적 이득을 취한다. 사용자는 오류로 인식하여 다시 결제를 시도하기 위해 전송된 문자 메시지 링크를 무심코 클릭하게 되면 결제하고자 하는 소액결제서비스 형태가 아닌 사용자 개인 및 금융정보가 빠져

나가게 된다. 최근에는 변종 악성코드가 스마트폰에 등록된 주소록이나 연락처(이메일, 전화번호)외에 통화 내역 등을 가리지 않고 유출해 가고 있으므로 더욱 경각심을 가져야 한다. 특히, 소액결제 시 인증번호를 탈취하는 해커의 IP 발생은 여러 장소에서 우후죽순으로 나오고 있으므로 추적이 매우 어려워지고 있다.

4.3 금융 앱 검토

최근 스마트폰과 같은 모바일 기기를 사용하는 일반인일 경우 가장 편리한 기능 중의 하나가 아마도 금융 관련 앱일 것이다. 금융 앱의 주요 기능은 특정 금융기관에서 제공하는 앱을 앱스토어나 금융기관에서 직접 다운로드하여 설치하여 온·오프라인을 통해서 현장 또는 원격으로 결제가 가능하다는 편리함이다. 뿐만 아니라 핀테크 앱을 비롯하여 금융 관련 앱은 인터넷 뱅킹을 대신하여 무통장 송금, 신용카드 결제, 지로 납부 등도 가능해지고 있다. 특히, 젊은 세대와 30,40대 직장인들 사이에서 핀테크 도입과 관련된 금융 서비스가 확대되면서 새로운 영역의 보안 위협이 대두되고 있다. 사용자들이 널리 이용하고 있는 결제 송금 서비스로는 카카오페이, 네이버페이, 삼성페이 등이 널리 이용되고 있으며 모바일을 활용한 금융 서비스로는 새롭게 론칭한 카카오뱅크(Kakao Bank)와 케이뱅크(K Bank) 서비스가 있다. 두 서비스는 신규 금융 핀테크 산업 육성에 미래 지향적인 IT 금융 성장 산업으로 기대되고 있지만 인증 방식의 간소화로 해커들의 새로운 보안 위협 대상이 되고 있다. 우선적으로 무선 환경의 NFC 결제방식은 보안 취약에 대한 사고 우려가 높다. 무선 네트워크의 취약적 환경을 고려할 때 해커가 마음만 먹으면 거래 내역 및 부정 거래 결제를 유도할 수 있기 때문이다. 또한, 인터넷 은행 계좌 개설 시에도 대부분의 거래가 비대면 실명 인증으로 처리되고 있으므로 대포 통장과 불법 거래 탐지가 쉽지 않고 있다. 부정적 거래를 미연에 방지하기 위해 FDS(Fraud Detection System)이 금융사기, 불법 거래 등을 사전에 탐지하기 위해 가동된다고 하지만 이상 징후를 탐지하기는 여간 쉽지 않다. 금융 사기와 관련 위협으로부터 모바일 거래를 보호하기 위해서는 금융 앱이 실행되는 동안에는 멀티기능 실행에 대한 작동이 잠시 중지되도록 기술적 구현하는 방법과 활성화를 통해 2차적 인증을 필수적으로 해야 하는 방법 등이다. 이는 일반 전화에서 통화 중 대기 기능과 비슷한 기능으로 생각하면 이해가 쉽다. 또한, 간편 결제 과정에서도 지문인식이나 IC 카드 접촉 시에 보안 관련 핀테크 기술이 작동되고 있는지에 대한 사전 점검도 반드시 점검해 볼 필요성이 있다.

<표 2> 현행 문제점 분석 방안

구분	문제점 방안 제시
위치 추적	• 앱을 점검하여 GPS 정보와 연관성 없는 앱이 설정되었다면 제거하도록 한다. • 맥(MAC) 주소를 자동 변경하여 위치 추적을 방해하도록 한다. • 의심 카메라와 위치 추적에 관련된 센서 장치가 자동으로 작동되는지를 수시로 확인하여 문제점이 발견되면 공장 초기화를 시도한다. • 많이 사용되는 SNS 계정인 페이스북과 트위터 구글 검색엔진 등의 개인정보의 하나인 위치정보 제공 동의에 허락하지 않는다. • 최근에는 GPS 기능을 끄거나 와이파이 신호가 꺼져 있어도 사용자의 스마트폰 위치 추적이 가능하므로 사용자의 세심한 주의가 필요하다.
생활 필수	• 사용하지 않는 앱에 대한 권한이 자동으로 변경되어 정보의 유출이 위협될 수 있으므로 가급적 사용하지 않는 앱은 삭제하여 악성코드에 감염되지 않도록 예방한다. • 링크 관련 문자가 포함되는(http://)나 com, co.kr, net 등의 메시지는 통신사 차단 앱을 통해 완전 차단되도록 예방 조치를 취한다.

구분	문제점 방안 제시
	• 가정이나 회사에서 사용하는 공유기의 암호를 초기 상태로 설정되어 있는지를 확인하고 공유기 사용에 따른 관리자 암호를 반드시 설정하여 해킹에 노출되는 사고를 미연에 방지하도록 한다. • 무료 쿠폰을 지급하겠다는 유도 문자 메시지에 현혹되지 말고 전송된 url이 포함되어 있는 메시지는 클릭하지 않고 자동으로 앱이 다운되지 않도록 주의도 기울인다.
금융 관련	• 서버로 전송되는 내용은 무조건 암호화 되도록 금융기관에서 제공하는 보안 솔루션을 필히 설치한다. • 앱 자체 개발 시 소스가 변조되거나 왜곡되지 않도록 무결성 보안 솔루션을 추가 설치한다. • 꾸준한 스마트폰 최신 백신 업데이트를 통해 악성코드의 침투 예방 및 스마트폰 루트권한을 넘겨지지 않도록 각별하고 세심한 보안 준수 원칙을 지키도록 한다. • 금융 기관에서 제공하는 간편 사용에 따른 4자리 비밀번호만 가지고 앱 결제를 진행하기에는 다소 위험이 존재할 수 있다. 최근에는 금융기관에서 2차 인증 수단으로 모바일 OTP와 같은 인증 결제 추가 수단을 확장하여 서비스되고 있으니 적극적으로 인증 추가 수단을 설정하길 권고한다. 통신사의 부가적인 기능을 통해 스마트폰 소액 결제 서비스에 대한 기능을 해제하는 것이 좋다.

Ⅴ. 결론

본 논문을 통해 다양하고 편리한 모바일 앱 보안 위협을 살펴보았다. 사용자 대부분은 일상에서 스마트폰을 24시간 끄지 않은 상태로 유지하고 있으며 이는 네트워크가 연결되어 있는 상태라면 보안 위협에 대한 노출은 더욱 위험하다. 많은 사용자들은 필요한 앱을 앱스토어를 이용하여 언제든지 자신의 모바일 기기로 다운받아 설치하여 이용하고 있으며 일부는 안정성으로 부터 검증되지 않은 변조된 가짜 앱들이 개인의 위치정보는 물론, 금융결제, 주변 정보, 연락처(주소록, 이메일)과 관련된 개인정보를 유출할 수 있다. 본 논문에서 살펴보았듯이 생활에 편리한 다양한 앱들의 자원을 유용하고 안전하게 사용하기 위해서는 사용자 각자가 우선적으로 내 모바일 기기가 보안 위협으로부터 위험에 노출될 수 있다는 경각심을 가져야 한다. 또한, 보안 사고가 발생하게 되면 경찰청 사이버대응센터와 인터넷진흥원과 같은 신고기관에 접수하여 빠른 대응을 할 수 있는 행동 강령과 스마트폰 최신 백신 프로그램으로 악성코드 유무를 수시로 검사하여 안전하게 사용하는 원칙이 무엇보다 중요하다. 또한, 일시적으로 사용자의 위치 추적을 방해하기 위해 맥(MAC) 주소 자동 변경과, 통신사의 기지국에서 전달받은 신호를 변조하여 내보내는 새로운 기술적 변화가 빨리 적용되어야 할 것이며, 무엇보다 정부의 보안사고 예방에 따른 관심과 의지가 적극적으로 필요할 때이다.

참고문헌

[1] 김영재, 오세종, 두일철, “모바일 실내위치기반 서비스를 활용한 해외 관광콘텐츠 정보 제공 연구,” 디지털산업정보학회, 제10권, 제3호, 2014, P.225.

[2] 김현진, “모바일앱 분석 플랫폼 동향,” 전자통신동향분석, 제 29권, 제 1호, 2014, p.51.

[3] 한정수, “모바일 클라우드 서비스 환경에서의 보안위협에 관한 연구,” “Journal of Digital Convergence,” 제 12권, 제 5호, 2014, p.267.

[4] http://donbada.tistory.com/27

[5] http://tcatmon.com/wiki/UI

[6] https://byline.network/2017/11/23-6/

[7] http://www.itworld.co.kr/news/95791

[8] https://developer.android.com/guide/compon

[9] 김남욱, 김성환, 엄정호, “보안 위협 및 정보보호 대상 분류에 관한 연구,” 보안공학연구회, 제 9권, 제 4호, 2012, p.330.

[10] htps://www.trendmicro.co.kr/kr/blog/

flocker-ransomware-crosses-smart-tv/index.html
[11] 이현정, 고갑승, 류찬호, 원동호, “모바일 클라우드 환경에서 스마트폰 악성 어플리케이션에 대한 동적 보안 검증 도구(ZPP-ZERVER) 개발,” 보안공학연구논문지, 제10권, 제 3호, 2013, p.337.
[12] http://www.igloosec.co.kr
[13] 김보, 인종인, 조용현, “모바일 앱 개인정보 침해현황 및 대응방안(금융, 안드로이드 운영체제 중심으로),” “The Journal of The Institute of Internet Broadcasting and Communication,” 제 14권, 제 6호, 2014, P.269.
[14] 김미주, 신영상, 이태진, 염흥열, “안드로이드 모바일 악성앱 동적분석 회피기술 동향,” 정보보호학회지, 제 25권, 제 6호, 2015, p.7.
[15] http://blog.naver.com/PostView.nhn?blogId=dkscjf89&logNo=150132379500
[16] 최희식, 조양현, 김정숙 “위치기반 서비스에 따른 개인정보보안 취약점의 사례분석,” 디지털산업정보학회, 제10권, 제3호, 2014, P.155.

■ 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 컴퓨터학부 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 2월 19일
수 정 일 : 2018년 3월 07일(1차)
2018년 3월 16일(2차)
게재확정일 : 2018년 3월 19일