안드로이드OS 보안 위협 및 대처 방안

지도교수 : 한 상 훈
연 구 자 : 김 준 석

< 목 차 >

요 약

국내 대다수의 사람은 스마트폰을 사용하고 있다. 스마트폰은 단순히 통화, 문자만이 아닌 은행 및 증권 등과 같은 금융업무, 기업에서는 스마트폰을 통해 업무를 진행하곤 한다.
스마트폰의 기술은 나날이 발전하며 일상생활에 필수 요소로 자리 잡고 있다. 그래서 스마트폰 보안기술 동향에 대해 알아보고자 한다.

주요어 : 안드로이드, 삼성, KNOX, 악성코드

1. 서론

1.1. 스마트폰 개요

기존의 휴대폰은 단순히 통화, 문자를 위해 사용되었고, 이후에는 MP3 재생, DMB 감상 등 다양한 편의 기능이 추가되었으며, 현재의 스마트폰은 단순한 휴대전화뿐만이 아닌 휴대가 가능한 소형 컴퓨터의 기능을 수행해내고 있다. 기존에도 PDA와 같이 휴대전화와 컴퓨터를 결합한 기기는 있었으며, 1992년에 만들어진 최초의 스마트폰이라 하는 IBM의 사이먼도 있다. 스마트폰이란 명칭을 사용하지는 않았지만, 과거 1990년대부터 스마트폰이라 볼 수 있는 휴대전화 + 컴퓨터의 기능을 수행하던 기기는 존재해왔다. 2007년 애플의 스티브 잡스가 공개한 아이폰이 현재의 스마트폰 시장을 만들어냈다고 볼 수 있으며, 아쉽게도 국내에서는 이동통신 주파수, WIPI 탑재 의무화, 화이트리스트 제도 등의 이유로 아이폰과 같은 많은 외산 핸드폰들이 국내에 출시되기는 많은 어려움이 있었고, 국내에서는 주로 피처폰을 사용하였으나, 2009년 아이폰의 국내 출시로 인하여 스마트폰 시장에 불이 붙으며, 이때부터 많은 제조사에서 다양한 스마트폰을 개발하기 시작하였으며 애플, 삼성, 블랙베리, 노키아, LG, 마이크로소프트 등 다양한 제조사에서 만들어진 스마트폰을 사용할 수 있게 되었다. 스마트폰 시장 초기에는 안드로이드, iOS 두 운영체제뿐만 아닌 노키아의 심비안 OS, 블랙베리 OS, MS사의 윈도우 모바일, 삼성의 타이젠, 바다 등 다양한 모바일 운영체제의 스마트폰을 사용해왔지만, 현재의 국내외 모바일 운영체제 점유율은 안드로이드와 iOS가 대부분을 차지하고 있으며, 국내 시장의 경우 기존에는 삼성뿐만 아닌 LG, 팬택 등 다른 제조사도 있었지만, 경영난 및 다양한 이유로 인하여 현재 국내 시장은 iOS를 사용하는 아이폰과 안드로이드를 사용하는 갤럭시 만이 남아있다고 볼 수 있다.

스마트폰 사용자	사례수 (명)	현재 사용 스마트폰 브랜드							
		갤럭시	노트	삼성 (계)	애플 아이폰	LG	팬택	기타	모름 응답 거절
2012년 8월 27~28일	416			59%	13%	12%	8%	6%	2%
2013년 11월 25~28일	894	49%	12%	61%	13%	15%	7%	1%	3%
2014년 8월 12~14일	792	43%	15%	58%	10%	21%	7%	1%	3%
2016년 7월 12~14일	879	44%	12%	56%	17%	19%	2%	1%	4%
2017년 2월 7~9일	912	47%	11%	58%	17%	19%	2%	1%	3%
10월 24~26일	910	49%	14%	63%	18%	16%	2%		2%
2018년 7월 26~28일	931	46%	15%	61%	17%	16%	2%		4%
2019년 7월 30일~8월 1일	933	47%	16%	63%	19%	15%	2%		2%
2020년 8월 4~6일	934	42%	19%	61%	18%	17%	2%		2%
2021년 6월 1~3일	947			63%	20%	13%	1%		3%
2022년 6월 28~30일	**971**			**66%**	**20%**	**10%**	**2%**		**2%**

[사진 1] 국내 스마트폰 브랜드 점유율
(출처 : 한국갤럽조사연구소, “2012-2022 스마트폰 사용률 & 브랜드, 스마트워치, 무선이어폰에 대한 조사,” 2022.07.)

1.2. 스마트폰 보안의 중요성

무선 이동통신 기술의 발전에 따라 현재는 5세대 이동통신 기술인 5G를 사용하며 그에 대응하여 하드웨어의 성능 또한 빠르게 발전되고 있다. 스마트폰을 통해 금융 업무를 보며, 모바일신분증을 통해 신원을 증명하고, 지갑 없이도 결제를 할 수 있으며, 5G의 발전에 따라 사물인터넷(IoT) 활용 범위가 커지며 기존에 통신 영역이 필요 없었던 다양한 사물들이 사람과 연결되고 있고, AR(증강현실), VR(가상현실), 자동차 자율 주행 등 일상생활에 접하는 모든 행위가 스마트폰을 통한 제어가 가능한 시대가 되었다. 과학기술정보통신부의 <무선통신서비스 가입 현황>에 따르면 2022년 7월 말 기준 국내 이동전화 가입 회선은 약 7,454만 개로 그 중 스마트폰 회선은 약 5,402만 개에 달하며, 같은 달 행정안전부 주민등록 된 총인구수는 약 5,157만 명으로, 국민 1명당 1대의 스마트폰을 사용하고 있다고 볼 수 있다. 대다수 사람들이 스마트폰을 사용하며 스마트폰의 특성상 24시간 통신망과 연결되어 있으며, 스마트폰의 보안 사고는 단순히 정보 유출의 위협뿐만이 아닌 내 주변의 모든 일상에 있어 안전을 위협받는 것이기 때문에 스마트폰에서의 보안의 필요성에 대해 우리는 상기시킬 필요가 있으며, 스마트폰 보안 기술과 보안 위협 공격에 대해 알아보고 일반적인 사용자 입장에서의 보안 위협 대처 방안에 대해 알아보고자 한다.

(단위 : 만명)

구분	2018.12	2019.12	2020.12	2021.7	2021.11	2022.3	2022.7
이동전화 가입자	6535	6793	6954	7080	7164	7291	7454
스마트폰 가입자	4944	5113	5222	5341	5340	5377	5402

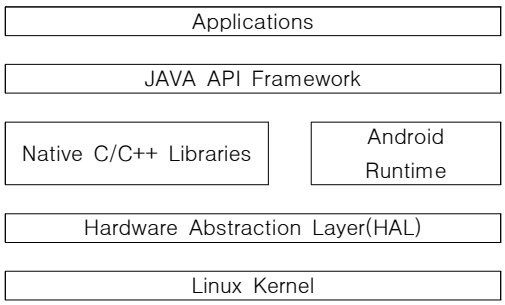
[표 1] 스마트폰 가입자 현황

2. 안드로이드 OS

2.1. 구글 안드로이드 OS

2.1.1. 안드로이드 OS 개요

2003년 앤디 루빈이 설립한 안드로이드(Android Inc.)는 2005년 구글에 매각하게 되어 현재는 구글 안드로이드라고 불리며, 안드로이드 OS는 Linux 커널을 기반으로 만들어진 모바일 운영체제로 가장 대표적인 오픈소스로 볼 수 있다. 스마트폰 OS 점유율 3위에 WIndows Mobile이 모바일 OS 시장에서 철수하면서 사실상 iPhone을 제외한 모든 스마트폰에 탑재된 OS라고 볼 수 있다. 안드로이드 OS는 초기 쿼티폰에 최적화되어 물리 버튼을 통해 조작이 가능한 모바일OS였으나, 애플의 iPhone이 출시된 후부터 터치스크린을 통해 조작이 가능한 모바일 OS로 발전되며 현재의 안드로이드 OS로 자리 잡게 되었다. 현재 안드로이드는 13버전까지 나와 있으며 기존에 버전별 코드네임을 알파벳순으로 디저트 이름으로 사용했으나, 버전 10.0부터는 숫자로 OS의 이름을 정하는 특이점을 볼 수 있다. 안드로이드는 최신버전의 Linux 커널을 사용하지 않으며, 출시 후 충분히 검증되어 안정된 커널을 사용한다. 안드로이드 OS의 경우 애플리케이션, Java API 프레임워크, 네이티브 C/C++ 라이브러리, Android 런타임, HAL(하드웨어 추상화 계층), Linux 커널로 구성되어 총 6개의 계층으로 분류되어 있다.



[표 2] 안드로이드 계층

2.1.2. 안드로이드 OS 보안 취약점

1) 권한(Permission) 요청에서 오는 문제점

안드로이드 OS에서 애플리케이션을 사용하게 될 때 사용자에게 직접 권한을 요청하게 되는데 이때 해당 앱이 요구하는 권한을 확인하여 승인 또는 거부할 수 있게 된다. 사용자가 권한을 요청을 직접 승인, 거부함으로써 보안 수준을 자유롭게 선택할 수 있는 장점이 될 수 있으나 일반적인 사용자는 이때의 권한을 중요하게 생각하지 않고 쉽게 승인해버리는 경우가 많으니 이로 인한 보안 취약점이 발생하게 된다. 예를 들어 플레이스토어를 통해 받은 단순히 온·오프 버튼만 존재하는 손전등 앱을 받게 되었을 때 이 앱에서 과도한 권한(위치, 저장소, 주소록, 문자 등)을 요청하게 되고 사용자가 이를 승인할 때 사용자의 개인정보가 탈취되는 보안 취약점이 발생할 수 있다.

2) 개방적인 앱 설치 환경에서 오는 문제점

안드로이드 OS는 기본 탑재된 구글 플레이스토어뿐만 아닌 통신사 마켓, 제조사 마켓 등 다양한 앱마켓이 존재하고 있다. 국내 안드로이드 사용자들은 주로 플레이스토어, 원스토어를 사용하며, 이 두 앱마켓은 검증 단계를 통해 검증되어진 앱들이 등록되어 있는데 이 검증 단계를 교묘하게 속여 악성 앱이 등록된 경우가 있으며, 블로그와 같은 웹사이트에 업로드되어 있는 출처를 알 수 없는 앱을 직접 내려받아 설치하게 되는 경우도 있는데 이 앱 파일(APK)이 악성 앱일 가능성이 매우 크다. 이렇게 개방적인 앱 설치 환경으로 인한 보안 취약점이 존재한다.

3) 루트 권한 획득에서 오는 문제점

안드로이드 OS의 경우 일반적인 사용자는 중요한 시스템파일에 접근할 수 없게 권한이 설정되어 있는데 이때 최고 관리자 권한인 루트 권한을 획득하는 행위를 루팅(rooting)이라고 한다. 일반적인 사용자의 경우 루트 권한에 대해 알지 못하는 경우가 대부분이지만, 카메라 촬영음을 없애기 위해, 통신사 앱을 삭제하기 위해, 휴대폰을 꾸미기 위해 루팅을 하는 경우가 있으며 이때 루트 권한을 획득한 상태로 악성코드가 설치된다면 시스템 권한을 공격자가 획득하게 된다. 이때 기존의 사용자 권한으로는 접근할 수 없던 금융 앱의 공인인증서와 패스워드 등에 접근할 수 있게 되며, rm ?rf / 명령어(LINUX 기반의 안드로이드에서 이 명령어가 실행되면 모든 파일과 디렉터리를 삭제되게 된다.)가 실행될 수도 있다. 또한 루팅 흔적이 발견되면 제조사 약관 위반이기에 AS를 거부당할 수 있다.

2.1.3. 안드로이드 OS 보안기술

1) 애플리케이션 샌드박스

안드로이드 OS는 Linux 사용자 기반 보호 기능을 활용하여 앱을 식별하고 분리하게 된다. 이때 각 애플리케이션은 고유한 UID(사용자 ID)를 할당받은 샌드박스 공간을 가지게 된다. 이러한 샌드박스 공간에서 앱이 실행됨으로써 내부 시스템과 분리되어 악영향을 받을 것을 미리 방지할 수 있게 된다. 애플리케이션 샌드박스는 커널에 있으므로 이 보안 모델은 네이티브 코드와 OS 애플리케이션으로 확장된다. OS 라이브러리, 애플리케이션 프레임워크, 애플리케이션 런타임 및 모든 애플리케이션과 같은 커널 상위에 있는 모든 소프트웨어는 애플리케이션 샌드박스 내에서 실행되기에 일부 플랫폼에서는 개발자가 특정 개발 프레임워크, API 세트 또는 언어로 제한된다. 안드로이드 OS에서는 보안을 강화하기 위해 애플리케이션을 작성하는 방법에 제한이 없습니다. 이러한 점에서 네이티브 코드에는 해독된 코드처럼 샌드박스가 설정되게 된다.

2) 애플리케이션 서명

안드로이드 OS에서는 인증서를 사용해 디지털 방식으로 서명된 앱 파일(APK)만을 기기에 설치하거나 업데이트할 수 있다. 개발자는 앱을 개발할 때 서명을 하게 되고 이때의 개인키는 개발자가 소유하게 된다. 인증서를 통해 개발자를 식별하여 개발자와 애플리케이션 사이의 신뢰가 연계된다. 애플리케이션 서명은 애플리케이션 샌드박스에 배치하기 위한 우선 단계로 서명 보호 수준에서 보안 권한을 선언하여 액세스를 같은 키로 서명된 애플리케이션으로 제한하는 동시에 고유한 UID 및 애플리케이션 샌드박스를 유지할 수 있다.

3) 파일 기반 암호화(FBE)

안드로이드 7.0 이상에서 지원하는 기술로 개별적으로 암복호화가 가능한 여러 키를 사용하여 여러 파일을 암복호화할 수 있게 된다. 파일 기반 암호화가 설정된 기기에서는 기기의 각 사용자가 두 개의 저장소 위치를 애플리케이션에서 사용할 수 있게 된다. 사용자 인증 정보 암호화(CE) 저장소와 기기 암호화(DE) 저장소가 있다.- 사용자 인증 정보 암호화(CE) 저장소 : 기본 저장소 위치로 사용자가 기기의 잠금을 해제한 경우에만 사용할 수 있다.- 기기 암호화(DE) 저장소 : 직접 부팅 모드 시 그리고 사용자가 기기의 잠금을 해제한 경우 모두 사용할 수 있는 저장소 위치이다.

4) Play Integrity API

Play Integrity API는 기존에 안드로이드에서 사용하던 SafetyNet Attestation API를 대체하기 위해 구글에서 제공하는 API로 소프트웨어(앱)와 하드웨어(기기)의 무결성과 라이선스를 검증할 수 있다. 이 API를 통해 대표적으로 3가지의 검증이 가능하다.

- 정품 앱 바이너리 : Google Play에서 인식하는 변조되지 않은 바이너리와 상호작용하는지 확인한다.- 정품 Play 설치 : 현재 사용하고 있는 사용자 계정에 라이선스가 부여되어있는지를 확인하여 정상적으로 Google Play를 통해 앱을 설치하였고, 비용을 지불했음을 검증할 수 있다.

- 정품 안드로이드 기기 : Google Play 서비스에서 제공하는 검증된 Android 기기에서 앱이 실행되고 있음을 확인할 수 있다.

2.2. 삼성 KNOX

2.2.1. 삼성 KNOX 개요

삼성전자에서 출시한 기업 및 개인용 보안 플랫폼으로 스마트폰뿐만 아닌 삼성에서 제조되는 대부분 디바이스가 제공되며, 외부로부터의 침입, 악성 소프트웨어 및 악의적인 위협으로부터 데이터를 보호하는 다중 방어 및 보안 메커니즘으로 구성되어 있다. KNOX는 현재 미국과 유럽 등 각국의 정부 기관으로부터 보안 인증을 획득하였으며, 국내 금융권에서도 현재 KNOX를 도입하여 사용 중에 있다. 삼성 스마트폰에서의 KNOX를 살펴보면 삼성 스마트폰 내부 메인보드에는 Efuse라는 회로가 존재한다. 스마트폰이 부팅 단계에 있을 때 'Secure Boot', 'Trusted Boot'와 같은 기술로 시스템의 커널, 부트로더 등이 변조되었는지 확인하게 되는데 이때 검사를 통과하지 못하게 된다면 Efuse가 끊어져 버린다. Efuse가 끊어지면 메인보드를 교체하는 방법 외에는 복구할 수 없으며, 이때 KNOX Warranty가 깨지게 되며 KNOX와 연계된 모든 서비스를 실행할 수 없게 된다. 이때 KNOX와 연계된 서비스는 삼성에서 제공하는 삼성페이, 삼성 헬스, 보안 폴더 등이 있다.

[사진 2] 삼성 KNOX 구조
(출처 : Samsung KNOX Security Solution, Whitepaper, 2015.09.)

2.2.2. 삼성 KNOX 연계 서비스

1) 보안 폴더

KNOX 2.7버전에 추가된 보안 솔루션으로 안드로이드 7.0 이상의 삼성 갤럭시 디바이스에서 지원된다. KNOX의 보호를 받는 디바이스 내의 별도의 분리된 공간으로 안드로이드 OS

에서 사용되는 애플리케이션 샌드박스에 유사하다. 보안 폴더 내부에는 애플리케이션뿐만 아닌 사용자 개인 파일 또한 보관할 수 있으며 보안 폴더 내의 앱 및 파일 삭제 시에는 영구히 삭제되어 복구할 수 없다. 또한 시스템의 커널 및 부트로더 변조로 인해 KNOX Warranty가 깨지게 되면 보안 폴더 기능이 차단되어 접근할 수 없게 된다. 보안 폴더의 암호의 경우 삼성 계정을 통해 재설정이 가능하여 암호를 분실하더라도 보안 폴더에 접근이 가능하지만, 설정을 통해 '삼성 계정으로 잠금 초기화' 기능을 비활성 한다면 암호 없이는 어떠한 방법으로도 잠금을 해제하는 것이 불가능해진다.

2) 삼성페이(SamsungPay)

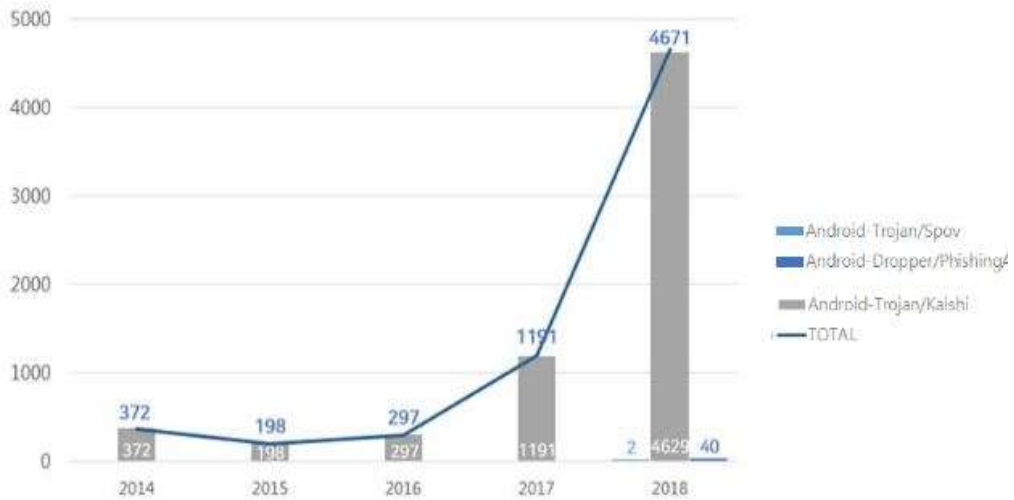
삼성페이는 2015년 3월에 삼성전자에서 공개된 간편 결제 서비스로 MST와 NFC 방식 모두를 동시에 지원하는 온/오프라인 결제 서비스로 단순히 결제를 위한 정보뿐만이 아닌 신분증, 블록체인 계좌, 차 키, 항공권 등 디지털화된 개인정보와 자산을 통합하여 관리할 수 있다. 이 때 삼성페이에 등록된 신용카드, 신분증 등을 사용하기 위해서는 지문인식, 홍채인식과 같이 사전에 등록된 인증방식을 통해 사용 가능하며, 모든 정보는 KNOX를 통해 보호된다. KNOX Warranty를 확인하는 Efuse와 삼성페이 MST 안테나는 직접적으로 연결되어 있어 Efuse가 깨지면 삼성페이 MST 결제를 사용할 수 없게 된다.

3. 안드로이드 보안 위협 공격 및 대처방안

3.1. 안드로이드OS 보안 위협 공격

3.1.1. 카이시 악성 앱을 통한 보이스피싱

2014년 처음 등장한 Android-Trojan/Kaishi(카이시) 악성 앱은 보이스피싱에 사용되는 앱이다. [사진 3]은 안랩 시큐리티 대응센터(ASEC)에서 공개한 보이스피싱 악성 앱 증가 추이로 2014년부터 2016년까지 꾸준히 증가하였으며 2017년과 2018년에는 4배 이상 증가하였다. 카이시 악성 앱은 금융사 웹사이트와 유사하게 제작된 피싱 사이트에 접속했을 때 '본인인증 프로그램을 설치 해야 한다며 악성 앱 설치파일(.APK)을 설치하게끔 유도한다. 악성 앱이 설치될 때 통화기능, 주소록, 문자메시지 등의 과도한 권한을 요청하게 되는데 이를 수락한다면 카이시 악성 앱이 스마트폰의 통화기능과 주소록, 문자메시지 정보를 유출한 후 스마트폰 상태를 모니터링하게 된다. 이후 사용자가 특정 금융사 대표 전화번호로 발신을 시도하면 이를 가로채 공격자의 전화번호로 재연결(리다이렉션) 하고, 이때 공격자는 해당 금융기관의 ARS 안내음을 재생한 후 통화연결을 하여 보이스피싱을 시도한다. 사용자는 기존의 보이스피싱 방식과 달리 실제 기관의 전화번호로 통화를 하였기에 피싱을 당했다는 사실을 알지 못하고 속수무책으로 속을 수밖에 없는 것이다.



[사진 3] 2014년 ~ 2018년 수집된 보이스 피싱 악성 앱 증가 추이
(출처 : AhnLab(안랩), 악성 앱과 결합한 보이스 피싱, 눈 뜨고 당한 이유 있다?, 2019.02.)

3.1.2. 크립토재킹(Cryptojacking) 공격

크립토재킹(Cryptojacking) 공격이란 일반 사용자의 PC에 암호화폐 채굴을 위한 악성코드를 설치하여 사용자의 하드웨어를 통해 암호화폐를 몰래 채굴하여 공격자의 지갑으로 전송하는 사이버 범죄이다. 이러한 크립토재킹은 기존에는 PC를 공격대상으로 삼았지만, 정보보안업체 ESET의 발표에 따르면 플레이스토어에서 내려 받은 인기 게임 '버그 스매셔' 게임 앱에 크립토재킹 악성코드가 심어져 있어 사용자의 스마트폰을 통해 암호화폐 '모네로'를 채굴하는 것을 적발했다. '모네로'는 거래 기록 추적이 어렵고, 송금처를 알 수 없어 범죄 자금 은닉이 쉽기에 크립토재킹 대다수는 모네로 채굴을 목적으로 삼는다고 한다. 크립토재킹의 공격은 백그라운드에서 동작하기에 별다른 이유 없이 스마트폰 구동 속도가 느려지고 배터리 소모 속도가 빨라진다면 크립토재킹 공격을 의심해봐야 한다. 현재 크립토재킹 공격은 PC, 스마트폰뿐만 아닌 IoT(사물인터넷)를 공격대상으로 삼는다고도 한다.

3.1.3. 크립토락커(Cryptolocker) 공격

크립토락커(Cryptolocker) 공격이란 랜섬웨어의 일종으로 2013년 처음 발생했으며, 러시아 국적의 해커 евгений михай лович богачев (예브게니 미하일로비치 보가체프)가 만들었다고 알려져 있다. 2015년 안랩 시큐리티 대응센터(ASEC)에서 발표한 자료에 따르면 'Adobe Flash Player'를 위장한 'Addobe Flash' 악성 앱이 유포되었으며 해당 앱을 설치할 때 네트워크 통신, 전화 통화 등의 권한과 기기 관리자 권한을 요청하며 이를 수락하게 되면 운영체제 버전, 모델명, IMEI, 국가정보를 공격자에게 전송하게 되며 [사진 4]와 같은 감염화면이 나타나며 다른 조작이 불가능해진다. 다른 랜섬웨어와 마찬가지로 금전을 요구하고 있으며, 공격자에게 금전을 송금하더라도 암호화를 풀어준다는 보장이 없다. 이때 흥미로운 점으로는 크립토락커의 제작자가 러시아인이기에 국가 정보가 러시아면 크립토락커가 동작하지 않도록 설계되어 있다는 것이다. PC의 랜섬웨어의 경우 파일을 암호화하기 때문에 복호화하는 것이 불가능에 가깝지만, 스마트폰에서의 크립토락커의 경우 조작을 불가능하게 만드는 것이므로 안전모드

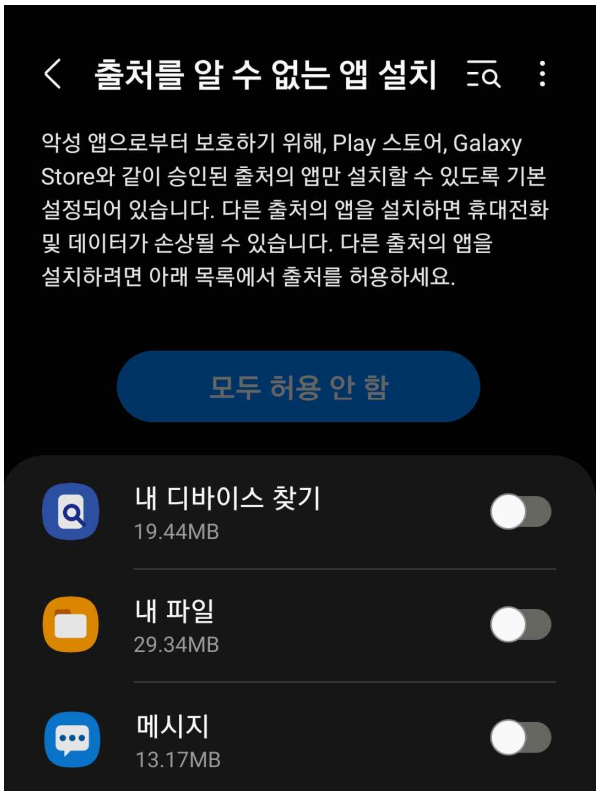
에 진입하여 해당 악성 앱을 제거할 때 크립토락커의 공격에서 벗어날 수 있다고 한다.

[사진 4] 크립토락커 감염 화면
(출처 : 삼성스마트폰카페, 스마트폰 랜섬웨어(크립토락커) 대응 방법, 2015.12.)

3.2. 보안 위협 대처방안

3.2.1. 출처를 알 수 없는 앱 설치 기능 설정

안드로이드 OS의 경우 출처를 알 수 없는 앱 설치에 대해 기본적으로 '허용 안 함' 상태를 유지하고 있다. 일반적인 사용자의 경우 대부분의 앱을 플레이스토어나, 원스토어 등을 통해 설치하기에 APK 파일을 직접 설치하는 경우가 없다 봐도 무방하다. 악성 앱이 설치되는 대부분의 경로는 앱 마켓이 아닌 스미싱 문자, 검증되어 있지 않은 사이트에서의 APK 파일 설치로 출처를 알 수 없는 앱을 설치하는 것을 원초적으로 차단할 필요가 있다. 안드로이드 8.0 이상 버전에서는 개별의 앱마다 별도로 출처를 알 수 없는 앱 기능을 허용하므로 문자 앱에서의 APK 설치는 차단하고, 파일관리자에서의 APK 설치는 허용할 수 있다. 아래 [사진 5]는 안드로이드 12 버전에서의 출처를 알 수 없는 앱 기능을 '모두 허용 안 함'으로 바꾸는 그림이다.



[사진 5] 출처를 알 수 없는 앱 '모두 허용 안 함' 기능 설정

3.2.2. 앱 설치 시 권한 요청 확인

안드로이드 OS에서 앱을 설치하고 사용하게 될 때 사용자에게 해당 앱이 요구하는 권한을 요청하게 되고 사용자를 이를 허용 또는 거부할 수 있다. 대부분의 앱의 경우 설치 후 첫 실행에서 권한을 요청하게 되는데 사용자들은 본인이 사용하고자 하는 앱의 기능에서 필요가 없는 권한인지에 대해 각별의 주의할 필요가 있다. 예를 들어 계산기 앱을 설치하고 실행하는데 녹음 권한, 카메라 권한, 네트워크 권한 등을 요구한다면 이 계산기 앱은 계산기 앱으로 위장하여 사용자의 대화를 몰래 녹음하거나, 카메라를 동작시켜 불법 촬영을 하여 네트워크를 통해 공격자에게 전송하는 악성 앱일 가능성이 있는 것이다. 사용자는 앱이 권한을 요청하게 될 때 무작정 허용 버튼을 누르는 것이 아닌 권한 하나하나를 개별적으로 확인하고 허용해주는 것이 보안 위협을 대처할 수 있는 기본적인 방법이라고 생각한다.

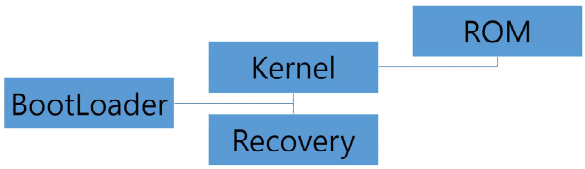
3.2.3. 모바일 백신 사용

모바일 보안에 대해 검색한다면 항상 빠지지 않고 등장하는 스마트폰 보안 수칙으로 '모바일 백신' 설치가 나올 것이다. 오늘날 스마트폰은 단순히 전화, 문자 기능을 넘어 카메라로 일상을 기록하고, 금융·증권 서비스를 이용하며, 회사 업무를 처리하는 등 우리 삶에 가까운 정보를 담고 있기에 스마트폰을 대상으로 한 공격은 꾸준히 증가하고 있어 모바일 백신의 중요성 또한 커지고 있다. 모바일 백신도 PC의 백신과 마찬가지로 악성코드 탐지가 주 기능이며 문자 탐지, URL 검사, 메모리 최적화, 임시파일 청소 등의 기능을 포함한다.
국내 모바일 백신은 대표적으로 이스트시큐리티의 '알약M'과 안랩의 'V3 모바일'이 존재한

다. ‘알약M’의 경우 자체적으로 악성코드를 검사하고 실시간 감시하며, 한국인터넷진흥원(KISA)과의 협력을 통한 스미싱 탐지 기능을 제공하며 국내에서 가장 많은 점유율을 보유하고 있다. 악성 앱 설치나, 개인정보 유출의 대부분은 스미싱 문자를 통해 이루어지기에 스미싱 탐지는 본 백신의 가장 큰 강점이다. ‘V3 모바일‘ 또한 ’알약M‘과 대부분 기능이 유사하며 국내 모바일 백신 점유율 2위를 차지하고 있다. 또한 글로벌 보안 인증 평가인 ’AV-TEST‘ 모바일 부문에서 인증받았으며, 국내 대다수의 금융 앱 사용 시에 동작하는 보안 솔루션인 ’V3 모바일’을 보유하고 있다. 모바일 백신 사용은 스마트폰 보안 위협에 대처하기 위해 안드로이드 OS 사용자라면 필수로 설치하길 바란다.

3.2.4. 부트로더 언락 자제

안드로이드OS의 부팅 순서를 살펴보면 아래 [사진6]과 같다.



[사진 6] 안드로이드OS 부팅 순서

부트로더란 운영체제가 시동되기 전 미리 실행되어 커널을 메모리에 올려 실행시키는 프로그램으로 우리가 스마트폰을 사용하게 될 때 일반적으로 부트로더가 커널을 시동시키고 그 후 롬을 실행시켜 우리가 사용하는 안드로이드 OS로 부팅되는 것이다. 대부분의 제조사에서는 부트로더를 락한 상태로 기기를 제공하며, 제조사가 아닌 제3자가 커널과 롬을 수정하려 하면 부팅이 불가능하게 하여 데이터를 보호하도록 보안시스템이 구현되어있다. 이러한 부트로더를 언락하게 되면 삼성 갤럭시의 경우 KNOX Warranty가 깨지게 되어 모든 보안 기능이 무력화되며, 공격자가 시스템 자체를 수정할 수 있어 잠금 화면을 우회하여 기기에 접근할 수 있게 되었다는 것만으로도 OS를 더 이상 신뢰할 수 없게 된다. 또한 금융 앱과 같이 피해 규모가 큰 앱의 경우 부트로더가 언락 될 경우 실행조차 불가능하게 되며 사용자가 기기를 도난·분실했을 때 구글락, 삼성 원격 잠금 등의 기능을 쉽게 무력화시킬 수 있다.

3.2.5. 정기적 업데이트

안드로이드 스마트폰을 사용할 때 2개의 보안 업데이트를 지원받게 되는데 먼저 구글에서 제공하는 안드로이드 보안 패치 업데이트와 제조사에서 제공하는 보안 업데이트이다. 구글과 제조사는 지속해서 취약점을 테스트하고 분석하여 이에 대해 공유하고 사용자에게 보안 업데이트를 지원하고 있다. 구글에서는 안드로이드 OS의 취약점에 대해 이를 보완하여 업데이트를 제공하고, 제조사에서는 제조사 전용 앱, UI 등에서 발생하는 취약점을 보완하여 업데이트를 제공한다. 안드로이드 OS의 경우 많은 제조사에서 사용하기에 칩셋 및 안드로이드 버전별로 취약점이 상이하다. 또한 낮은 버전의 안드로이드를 사용할 때에도 보안에 취약하므로 최신 버전의 안드로이드로 업데이트하기를 권고한다.

4. 결론

지금까지 안드로이드 OS 구조와 보안 취약점 및 보안 위협 공격과 대처 방안을 소개하였다. 안드로이드 OS의 경우 다른 모바일 OS와 달리 어느 제조사나 가져다 쓸 수 있고, 앱 제작 또한 누구나 할 수 있다는 점에서 개방적이지만 그로 인한 위험을 감수해야 한다는 것을 알 수 있다. 현실에서와 마찬가지로 외부에서의 위협에 대해 보호받을 수 있는 완벽한 개방은 존재하지 않는 것이다. 안드로이드 OS의 자체 취약점은 보안 업데이트를 통해 해결할 수 있으나, 그 외에 악성코드에 감염되거나 스마트폰의 정보가 유출되는 경우는 사용자가 실수로 설치한 APK 파일, 악성 앱이 요구하는 권한을 승인하는 등 사용자의 부주의함으로 인해 발생한다는 것을 알 수 있었다. 본 논문을 통하여 사용자 입장에서의 3가지 보안 위협 대처 방안을 제안하였다. 국내 스마트폰 점유율의 반 이상의 점유율을 보유하고 있는 안드로이드 OS에서의 보안 위협을 최소화하기 위해서 향후 추가적인 보안 대처 방안에 대해 연구하고자 한다.

참고문헌

[1] 안드로이드 해킹 사례 및 향후 보안 대책, 임정관 외 3명, 2012년 4월 26일
[2] "Android 기기 보안.", Android 오픈소스 프로젝트, 2022년 9월 3일 검색, https://source.android.com/docs/security/overview.
[3] “진화하는 보이스피싱, 악성앱이 사용자를 노린다.”, AhnLab보안이슈, 2022년 9월 20일, https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=30254
[4] “스마트폰까지 노리는 랜섬웨어 ‘크립토락커(Cryptolocker)’.”, AhnLab보안이슈, 2022년 10월 23일, https://www.ahnlab.com/kr/site/securityinfo/asec/asecView.do?groupCode=VNI001&seq=23991
[5] 사용자 몰래 가상화폐채굴하는 스마트폰 악성앱 분석, 송지훤, 2014년 5월
[6] 모바일 보안 위협 및 보안 서비스 기술 동향, 강동호 외 2명, 2010년
[7] 모바일 백신 ‘V3 모바일’ vs.‘알약M’ 선두 경쟁에 ‘모바일가드’ 기웃, 테크M, 김가은 기자, 2021년 11월 12일, https://www.techm.kr/news/articleView.html?idxno=90738