안드로이드 취약점 분석 및 대응방안 연구

지도교수 : 이강호
연 구 자 : 박지훈

< 목 차 >

요 약

21세기의 우리는 가정에서 사용하던 PC의 기능을 스마트 폰이라는 작고 가벼운 기기를 통하여 공간의 제약 없이 사용할 수 있게 되었다. 우리에게 가장 가깝고 편리한 기기임은 분명하나 그만큼 개인의 다양한 정보를 담고 있는 것도 스마트 폰이다. 이러한 스마트 폰에 가장 많은 비중으로 사용되고 있는 운영체제가 바로 안드로이드(Android)이다. 안드로이드는 세계에서 가장 대표적인 오픈 소스 플랫폼으로써 비단 스마트 폰만이 아닌 여러 디바이스에서 사용되고 있는 운영체제이다. 하지만 안드로이드는 다른 폐쇄적 운영체제와는 달리 상대적으로 많은 보안 취약점을 지니고 있다. 이러한 취약점이 계속될 경우, 사용자는 안드로이드에 대한 거부감을 느낄 수 있으며 나아가 신뢰를 잃을 수도 있다. 본 연구는 안드로이드의 취약점에 대한 분석과 그 취약점으로 인해 발생할 수 있는 여러 문제점을 분석하고 그에 맞는 대응 방안을 모색하고 나아가 보안 정책과 기준 수립에 도움이 될 것으로 기대한다.

주요어 : 안드로이드(Android), 취약점, 어플리케이션(Application)

1. 서론

1.1 안드로이드(Android)란

초창기의 안드로이드는 디지털 카메라의 운영체제로 개발을 진행하고 있었으나 iPhone 등 스마트 폰의 등장으로 개발 방향을 전환하여 지금의 대중적인 모바일 OS인 안드로이드가 되었다고 한다. 안드로이드는 리눅스(Linux) 커널을 기반으로 구글(Google)사에서 제작하고 있는 모바일 운영체제이다. 안드로이드는 세계에서 가장 대표적인 오픈 소스 플랫폼이며 세계 최다 사용자를 보유한 운영체제이다. 2021년 기준 안드로이드의 모바일 OS 점유율은 72.19%로 다음으로 점유율이 높은 iOS(Apple 사의 모바일 OS)의 26.99%와 비교하여도 압도적인 점유율 차이를 보인다. 호환성이 매우 뛰어난 OS로써, 스마트 폰뿐만 아니라 ARM 프로세서, 태블릿 컴퓨터, TV에도 적용이 가능하며 PC에서도 적용하여 사용 가능하다. 가장 대표적인 예로 셋톱박스와 내비게이션에도 안드로이드가 적용되어 사용되고 있으며 구글사에서 공개한 자료에 의하면 안드로이드의 사용자 수는 전체 인구의 7분의 1인 10억 명 정도라고 한다.

[사진 1] 안드로이드 마스코트

안드로이드는 여러 분야에서 사용되고 있는 만큼 많은 사용자를 보유하고 있지만, 여러 가지 취약점을 가지고 있으며 그것을 악용한 사례는 꾸준히 발표되고 있다. 그중에서도 안드로이드는 스마트 폰에서의 사용 비율이 굉장히 높은데 스마트 폰은 공간의 제약이 없이 사용할 수 있는 편리한 기기이지만 개인의 민감한 정보를 포함하고 있는 기기이므로 보안이 매우 중요하다고 할 수 있다. 하지만 안드로이드는 다른 폐쇄적인 운영체제에 비해 매우 개방적인 방식으로 운영되고 있으므로 많은 취약점을 가진다.

논문의 구성은 안드로이드가 가지는 취약점에서 대표적인 사례를 예로 작성될 예정이다. 2.1.1장에서는 가장 최근 이슈였던 구글 웹 뷰 이슈에 대해 서술할 것이며, 2.1.2장에서는 안드로이드의 개발자들에게 가장 큰 피해를 끼치고 있는 불법 복제 및 무단 수정 이슈에 대해 기술하고 2.1.3장에서는 사용자 입력값 거증 부재 취약점에 대해 서술하고 대응방안을 제시하며, 마지막으로 2.1.4장에서 권한상승 취약점에 대해 서술하며 대응방안도 제시할 것이다.

1.2 안드로이드 버전 업그레이드

안드로이드의 취약점을 설명하기에 앞서 안드로이드는 2007년 안드로이드 0.5를 발표한 이래로 꾸준히 취약점을 발견, 패치하여 업데이트를 제공하고 있다. 각 안드로이드

버전의 특징에 대해 살펴보자.

안드로이드는 10.0 이전까지 1.0을 제외한 버전별 코드 네임이 전부 디저트 이름으로 되어있다. 최초의 안드로이드인 0.5버전은 전화, 인터넷, 지도 등의 기능만 존재하였다.

다음으로 발표된 안드로이드 0.9버전은 알람, 계산기, 갤러리, 카메라, 메시지, 음악과 같은 사용자 친화적인 애플리케이션이 다수 등장하고, '위젯'이라는 개념이 도입되었다.

[사진 2] 시계 위젯이 적용된 안드로이드 0.9 화면

정식으로 최초 배포된 안드로이드는 1.0 버전으로 구글 플레이 스토어의 원조인 안드로이드 마켓을 지원했다.

[사진 3] 초창기 안드로이드 아이콘

다음으로 발표된 안드로이드 1.5 컵케이크에서는 iOS보다 2개월 빠르게 복사/붙여넣기를 구현하였으며 안드로이드 2.0에서는 여러 개의 구글 계정을 동시에 사용할 수 있게 되었다. 2.1에서는 블루투스와 멀티 터치를 지원하게 되었다.

안드로이드 2.2는 실행 속도가 기존에 비해 2~5배 증가하였고 메모리 회수 기능의 개선으로 속도가 20배 정도 증가하였다. 안드로이드 9.0 이후의 버전은 지금까지 부족하던 안드로이드의 보안을 지속적으로 보완하여 현재 안드로이드 10 버전까지 업데이트가 배포되었다.

2. 본론

2.1 안드로이드 취약점

안드로이드는 커널부터 실제 폰과 비슷한 환경에서 본인이 제작한 프로그램을 돌려볼 수도 있는 에뮬레이터까지 모두 무료로 사용할 수 있는 OS이다. 오픈 소스로 모두에게 공개하는 만큼 응용 프로그램을 개발할 수 있는 환경이 효율적이며 다양한 응용 프로그램을 개발하기에 유용하지만 여러 소프트웨어 취약점에 쉽게 노출될 수 있다.

2.1.1 구글 웹 뷰(WebView) 이슈

최근 안드로이드는 2021년 3월 23일, 전 세계적으로 커다란 이슈가 있었다. 안드로이드의 '웹 뷰(WebView) 애플리케이션'이 업데이트 과정에서 문제를 일으켜 전 세계의 모든 안드로이드 스마트 폰의 애플리케이션 실행이 먹통이 되었던 것이다. 이 이슈는 삼성전자에서도 급히 해결법을 공지할 만큼 커다란 이슈였다. 이 이슈는 구글이 만든 웹 뷰 애플리케이션이 업데이트 과정에서 기존 애플리케이션들과의 충돌을 일으켜 발생하였다고 추정되고 있으며 원초적인 문제를 가진 웹 뷰 앱을 제거하거나, 사용을 중지해준다면 해결이 가능한 이슈였다.

[사진 4] 문제가 되었던 구글의 WebView 어플리케이션

2.1.2 불법 복제 및 무단 수정 이슈

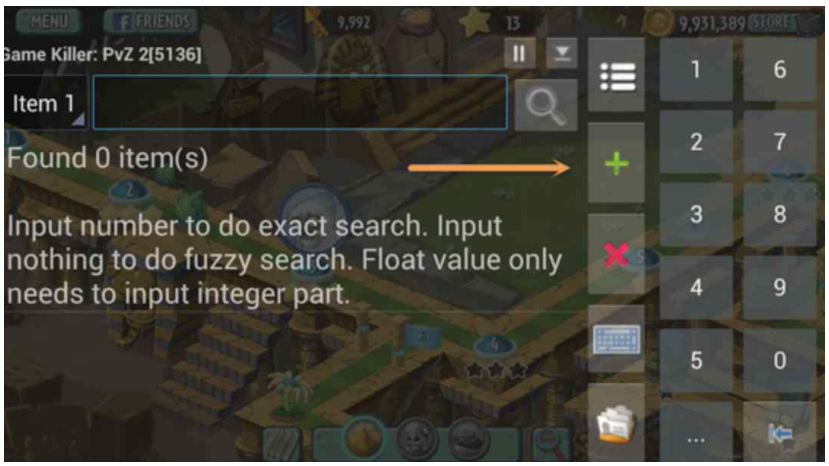
안드로이드는 개방성이 매우 높은 모바일 OS이다. 그로 인해 접근이 편리하다는 장점도 있지만 개인이 자유롭게 누군가가 개발한 애플리케이션을 무단으로 복제하여 배포, 사용하거나 애플리케이션을 변형하여 시스템에 혼란을 줄 수도 있다. 예를 들어 개발자나 기업이 안드로이드 환경에서 개발하여 플레이 스토어[1](Play Store)에서 판매중인 게임 A가 있다고 가정한다. A 게임에는 기업의 이익을 위한 상점 시스템이나 게임 머니 시스템이 존재할 것이다. 이 시스템을 어느 한 개인이 A 게임 애플리케이션을 무단 복제하여 게임의 상점 시스템과 게임 머니 시스템에 접근, 상점의 모든 아이템을 무료로 구매할 수 있게 수정한다거나 자신의 게임 머니를 무한정으로 늘리는 등의 행위가 불가능한 일이 아니라는 의미이다.

---

1) 플레이 스토어(Play Store) : 플레이 스토어는 구글에서 제작 배포하는 안드로이드 OS에서 사용되는 애플리케이션의 장터(마켓)

[사진 5] 구글에서 ‘안드로이드 게임 치트’ 검색어를 입력한 모습

실제로 위의 사진과 같이 구글에 ‘안드로이드 게임 치트’라는 검색어를 입력하면 어렵지 않게 게임의 시스템에 접근하여 시스템을 무단으로 수정하는 방법을 개인이 자유롭게 학습하고 시행할 수 있다. 가장 대표적인 예로 ‘게임 킬러(GameKiller)’라는 애플리케이션이 있는데 게임의 시스템에 접근하여 일정 시스템값을 수정, 게임에 적용시킬 수 있는 애플리케이션이다.



[사진 6] 게임 킬러를 실행한 모습

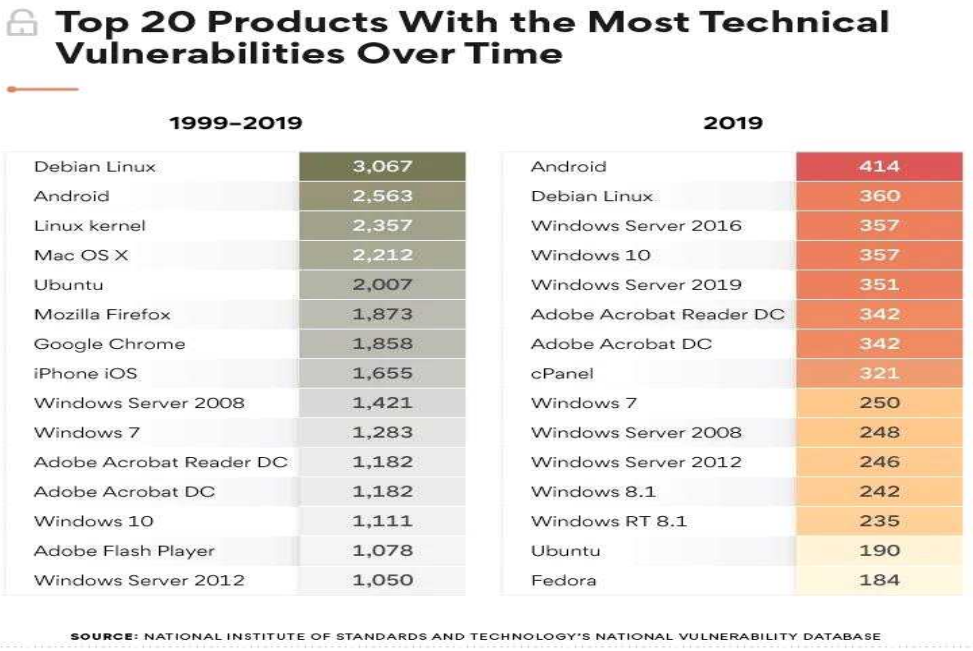
게임 킬러는 게임의 데이터에 자신이 원하는 값을 검색한 후, 일치하는 값을 발견하면 그 값을 수정하여 적용시키는 방식이다. 예를 들어 본인의 게임 머니가 14,353원이 있다고 가정한다. 게임 킬러에 14,353이라는 값을 입력하여 일치하는 값을 찾아낸다. 하지만 게임은 수많은 코드가 집합되어 있는 집합체이기 때문에 14,353이라는 값만으

로는 본인이 원하는 게임 머니 값에 접근하기가 쉽지 않을 것이다. 이때, 게임으로 돌아가 게임 킬러 사용자는 본인의 게임 머니를 조금 더 추가하여 14,355원으로 게임 머니에 변화를 준다. 이 과정을 진행하면 미리 구해두었던 14,353의 값을 가진 코드 안에서 14,355로 변화가 있었던 코드를 찾아낼 수 있게 된다. 그 값이 시스템에서의 게임 머니 값인 것이다. 이 값을 개인이 원하는 값으로 수정하여 적용하면 게임 내에도 개인이 원하는 값으로 게임 머니를 적용할 수 있게 되는 원리이다. 이러한 문제점은 개발자와 기업에게도 막대한 손해를 끼칠 수 있는 중대한 문제이다. 이 문제는 지금도 꾸준히 제기되고 있는 안드로이드의 가장 큰 이슈 중 하나이다.

2.1.3 사용자 입력값 검증 부재 취약점 및 대응 방안

위의 2.1.2 불법 복제 및 무단 수정 이슈에서 서술한 내용과 같이 안드로이드가 가지는 취약점은 개발자나 기업에게 막대한 피해를 줄 수 있지만, 사실은 개인에게도 막대한 피해를 줄 수 있다. 안드로이드가 개인에게 가장 많이 사용되고 있는 분야는 당연 스마트 폰이다. 스마트 폰은 개인의 민감한 정보를 포함하고 있는 기기로써 보안이 매우 중요하다고 할 수 있다. 하지만 안드로이드는 오픈 소스로 모두에게 무료로 제공되며 개방성이 매우 높은 모바일 OS로써 여러 가지 취약점에 취약할 수밖에 없다.

취약점은 보안의 결함을 의미하고 악의적인 공격에 이용될 가능성이 높다. 안드로이드는 2019년 보안에 가장 취약한 운영체제 1위로 선정되었다. 미국표준기술연구소(NIST)가 공개한 '국가취약점 데이터베이스(NVD)'에 따르면 2019년 한 해 안드로이드에서 발견된 취약점은 총 414건으로 다른 OS에 비해 가장 높다.

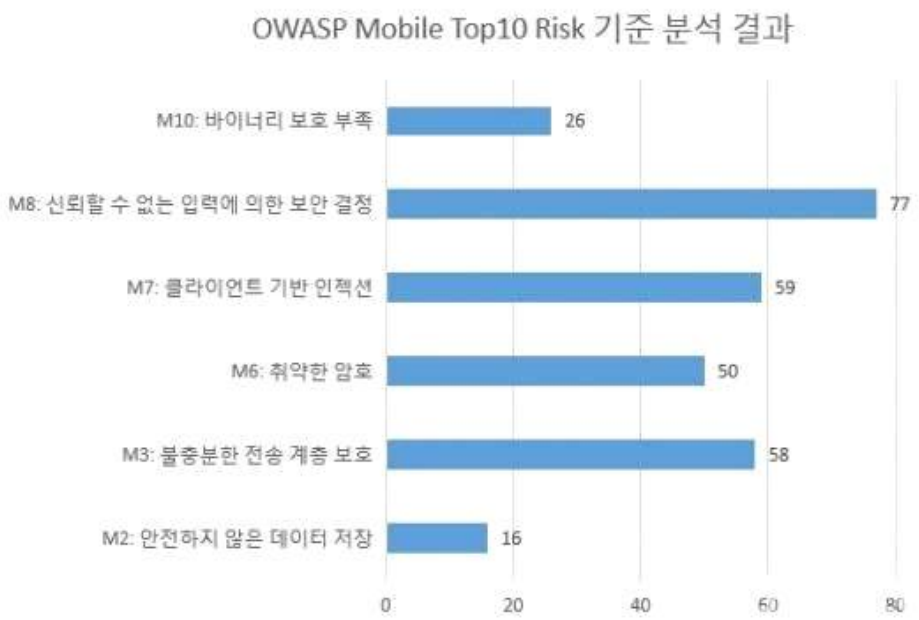


[사진 7] 안드로이드는 2019년 보안에 가장 취약한 운영체제 1위로 선정되었다

안드로이드는 오픈 소스로 모두에게 배포하는 모바일 OS인 만큼 취약점을 발견할 가능성이 높다고 판단하는 경향이 있는데 위의 조사 결과를 보면 결코 그렇지 않다.

정보보안 전문 커뮤니티 시큐리티플러스라는 안드로이드의 애플리케이션에서 평균 4.8개의 취약점을 발견할 수 있다고 분석, 발표하였다. 그중에서도 가장 많이 발견된 보안 취약점은 신뢰할 수 없는 입력에 의한 보안 결정 취약점인 '사용자 입력값 검증 부재'이다. 사용자 입력값 검증 부재의 취약점을 가지게 되면, 모바일 애플리케이션의 비정상적인 상태(DoS) 유발뿐만 아니라 악의적인 코드 실행을 할 수 있는 메모리 오류 등이 발생할 수 있다.

이러한 취약점으로부터 개인의 민감한 정보를 보호하기 위해서는 모바일 앱 내에 민감한 정보를 저장하지 않는 방법이 가장 바람직하지만, 꼭 해야만 하는 경우 암호화 스토리지에 보관하는 방안 이외에도 ADB[3]에 의한 백업을 허용하지 않아야 한다.



[사진 8] 시큐리티플러스에서 발표한 *OWASP Mobile Top 10 Risk 기준 분석 결과

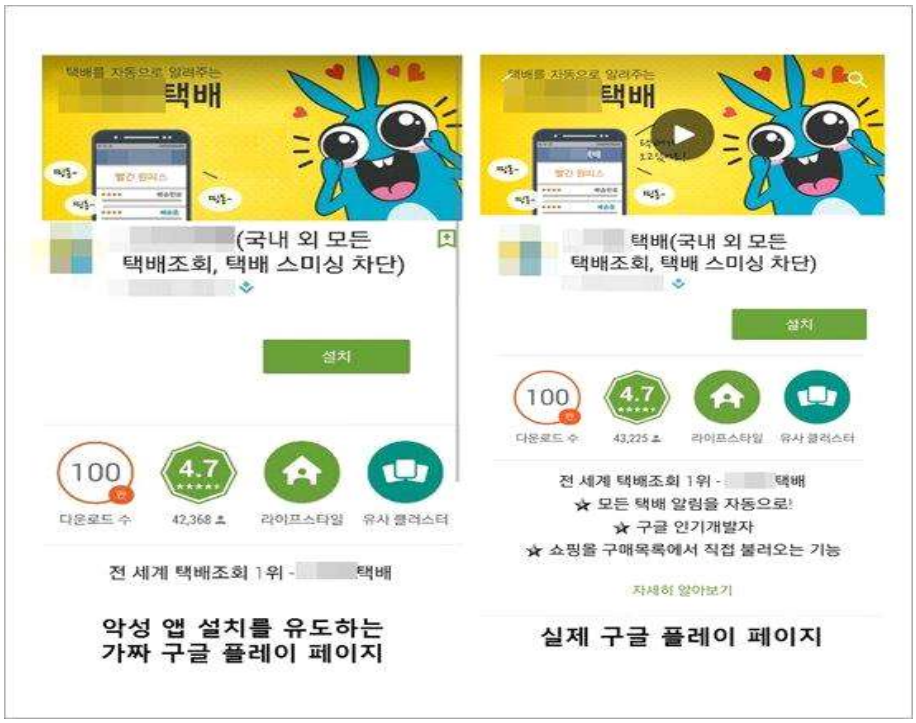
*OSWASP Mobile Top 10 Risk : 오픈소스 웹 애플리케이션 보안 프로젝트로써, 주로 웹에 관한 정보 노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구한 10대 웹 애플리케이션의 취약점

2) ADB : Android Debug Bridge의 약자로, PC와 스마트 폰 간에 통신을 할 수 있는 명령어 도구

2.1.4 권한 상승 취약점 및 대응 방안

또한 안드로이드는 권한 상승 취약점이 주기적으로 발표되고 있다. 권한 상승 취약점이란 해커가 루트 권한, 즉 기기의 모든 통제권을 악성 애플리케이션을 통하여 가지게 되는 취약점을 말한다. 해커로부터 여러 방법으로 악성 애플리케이션을 전달받아 설치하게 되면 해커는 악성 애플리케이션이 설치된 개인의 스마트 폰에 해커 자신의 권한을 루트로 설정, 부여하여 자신이 모두 통제할 수 있는 좀비로 만들 수 있으며, 스마트 폰 내부의 파일이나 개인정보에 접근할 수 있게 된다.

권한 상승 취약점의 가장 위험한 점은 스마트 폰 내부에 저장되어 있는 개인의 정보이다. 스마트 폰은 개인이 편리하게 사용할 수 있는 만큼 개인의 모든 정보를 담고 있다고 하여도 과언이 아닐 정도로 많은 정보를 담고 있다. 예를 들어 은행 거래 정보, 연락처, 메일과 메시지 대화 내용, 개인의 사진 등의 유출된다면 매우 치명적일 수 있는 정보를 모두 담고 있다. 이러한 정보를 해커가 노리고 접근한다면 안드로이드 OS를 사용하고 있는 사용자는 쉽게 그 위험에 노출될 수 있는 것이다. 해커가 개인의 스마트 폰에 루트 권한을 획득하여 은행 정보에 접근한다면 개인의 은행 계좌를 악의적으로 이용할 가능성이 생기고 연락처나 개인정보에 접근한다면 사용자의 연락처에 저장된 다른 사용자에게도 해커가 접근할 수 있게 된다.



[사진 9] 대표적인 악성 안드로이드 어플리케이션의 예

위의 사진과 같이 해커는 안드로이드 사용자에게 악성 애플리케이션 설치를 유도하는 가짜 스미싱 애플리케이션 설치 페이지를 전송하여 사용자가 설치하도록 유도한 후, 루트 권한을 획득한다.

이러한 루트 권한을 획득하는 과정에는 사용자 본인의 부주의가 원인이 되는 경우가

다수이다. 안드로이드를 사용하는 사용자는 알 수 없는 연락처나 주소로부터 메일을 받게 된다면 읽지 않고 삭제하는 것이 가장 좋은 방법이며, 만약 읽었다고 하더라도 신뢰할 수 없는 URL 링크를 함부로 클릭하지 않으며 첨부파일을 열지 않고 개인의 정보는 가능한 스마트 폰 내에 저장하지 않는 것이 가장 바람직하다. 개인의 작은 실천으로부터 우리는 취약점에 노출되지 않고 안전하게 안드로이드를 이용할 수 있다.

3. 결론

안드로이드 시장 규모는 계속해서 증가하고 있지만 아직까지 다른 운영체제에 비해 많은 취약점이 존재한다. 우리의 일상 속에 수없이 많은 안드로이드를 적용하여 사용하는 기기들 중 역시 우리 개인에게 가장 가까운 분야는 스마트 폰이다. 스마트 폰에는 개인의 민감한 정보가 포함되어 있으므로 보안에 주의를 기울여야 한다. 스마트 기기들은 우리에게 편리함과 여러 이점을 가져다주지만 이는 양날의 검과도 같다. 우리가 어떻게 사용하느냐에 따라 득이 될 수도 해가 될 수도 있다. 우리는 개인의 노력으로도 충분히 안전하게 편리함을 누릴 수 있는 사용자가 되어야 한다. 그러기 위해서 취약점으로 인해 발생할 수 있는 문제점에 대해 조금 더 경각심을 가지고 보안에 유의하며 안드로이드를 사용하는 자세를 가지고 생활한다면 우리는 더욱더 편리하고 유익한 안드로이드를 활용할 수 있을 것이다.

참고문헌

1) 출처: https://namu.wiki/w/안드로이드(운영체제)#s-7
2) 출처: https://www.yna.co.kr/view/AKR20210323072800017
3) 출처: https://m.blog.naver.com/nicecan/70176999755
4) 출처: https://www.dailysecu.com/news/articleView.html?idxno=8206
5) 출처: https://ko.wikipedia.org/wiki/OWASP
6) 출처: https://www.ciokorea.com/news/133002
7) 출처: 조희훈, 원달수, 김종배 - A Study on the Security Vulnerability of Android 인문사회과학기술융합학회 2015년 12월