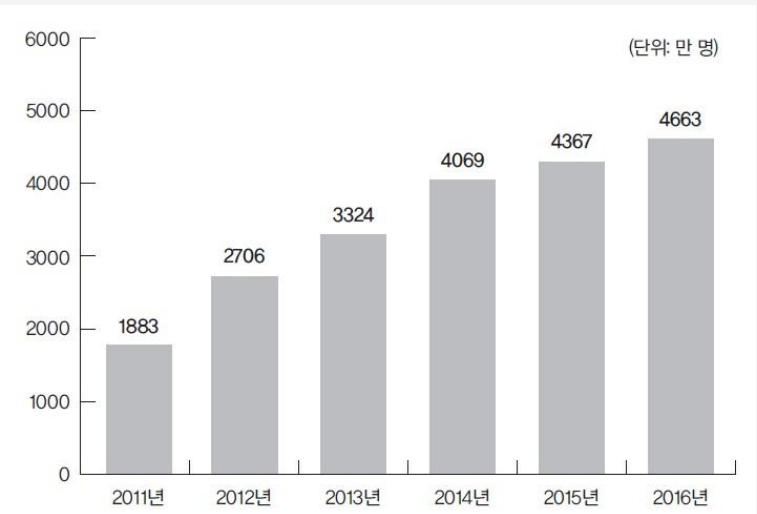
1 모바일 보안의 개요

1 모바일 환경의 성장

- 모바일 보안의 중요성은 아이폰이 세상에 나온 후 스마트폰 열풍이 불기 시작하면서부터 시작(아이폰)

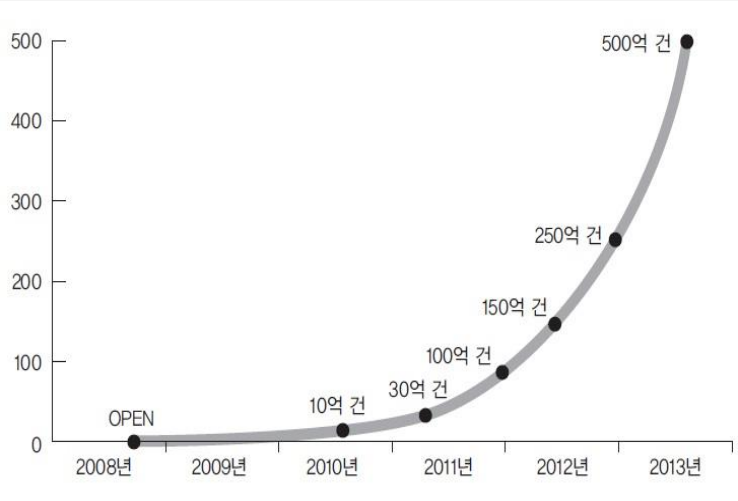


[국내 무선통신 (스마트폰) 가입자 수 (출처:방송통신위원회]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

1 모바일 환경의 성장

현재 모바일 앱을 다운로드할 수 있는 곳은
애플 앱 스토어와 구글 플레이로 양분되어 있음



[누적 다운로드 수로 살펴본
안드로이드 마켓의 성장세]

※ 출처 : 인터넷 해킹과 보안,
김경곤, 한빛아카데미, 2017

2 안드로이드와 iOS의 보안

- 현재 모바일 앱을 다운로드할 수 있는 곳은 애플 앱 스토어와 구글 플레이로 양분되어 있음

[안드로이드와 IOS의 보안관련 사항 비교]

속성	구글 안드로이드	애플 iOS
Openness	개방형 소스 플랫폼	비개방형 소스 플랫폼
Trusted Computing System	리눅스 커널 및 Core libraries	XUN 커널 및 Core libraries
Trusted Programming Language Used	자바 언어	오브젝티브-C 언어
Core applications	루트 권한으로 실행	루트 권한으로 실행
Application process	샌드박스식 격리, 자신의 메모리 영역에서 실행	샌드박스식 격리, 자신의 디렉터리 영역에서 실행

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 안드로이드와 iOS의 보안

- 현재 모바일 앱을 다운로드할 수 있는 곳은 애플 앱 스토어와 구글 플레이로 양분되어 있음

[안드로이드와 IOS의 보안관련 사항 비교]

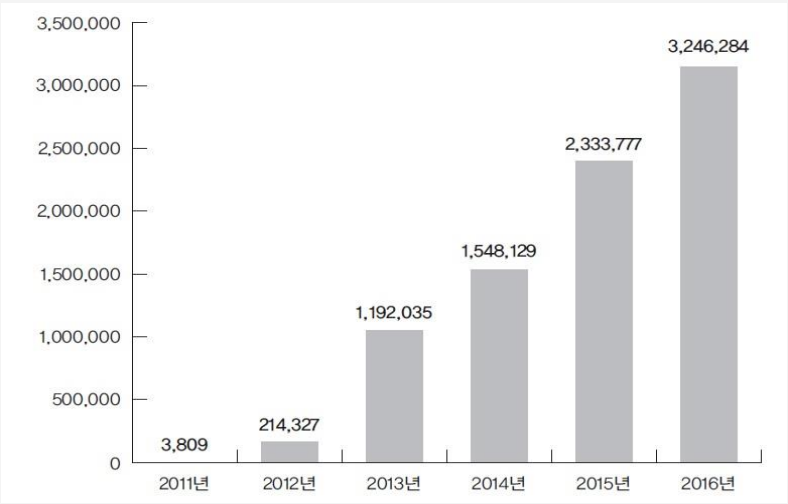
속성	구글 안드로이드	애플 iOS
Application permissions	서명 확인 및 사용자 승인	서명 확인
File Data Protection	암호화 키 사용	암호화 키 사용
File Sharing(default)	권한 부여하에 가능	불가능
Device Security	사용자 패스워드 및 원격 조정 삭제 기능	사용자 패스워드 및 원격 조정 삭제 기능

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 안드로이드와 iOS의 보안

- 안드로이드의 개방적인 특성을 이용한 리패키징 기법이 알려지면서 모바일 악성 앱이 증가하는 추세(역공학)

[전 세계의 안드로이드 악성 샘플 수]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 모바일 보안 위협 요소

1 모바일 보안 위협의 유형

분류	공격 유형	공격 방법
플랫폼 공격	• 바이러스/웜 • 시스템 언록 • 키보드 해킹	• 와이파이/블루투스/웹 이용 전파 • 탈옥(아이폰), 루팅(안드로이드), Security Off(WM) • 플랫폼 취약점 • 루트킷(백도어, 트로이 목마 등의 해킹 프로그램)
네트워크 공격	• 와이파이 도청/변조 • DoS 공격	• 와이파이/블루투스 네트워크 공격
애플리케이션 공격	• Malicious App. • 피싱 앱	• 웹 다운로드 • PC 동기화
단말기 공격	• 도난 및 분실 • Malicious App.	• 도난 및 분실 • 이동 저장 매체 감염

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

1 모바일 보안 위협의 유형

[스마트폰을 대상으로 한 주요 악성코드]

구분	발견 시기	운영체제	특성
Cabir.A	2004년 6월	심비안	• 최초의 웜 바이러스로 심비안에서 발견 • 블루투스를 통해 전파되며 단말기 배터리 수명 단축
InCE.Duts	2004년 7월	윈도우 모바일	• 단말기 루트 폴더의 모든 파일 감염
Skulls	2004년 11월	심비안	• 단말기 아이콘을 해골 모양으로 변경 • 동작 정지 및 해당 프로그램 삭제
WinCE. Brador	2005년 8월	윈도우 모바일	• 사용자 모르게 설치되어 단말기 원격 제어
Red Browser	2006년 3월	공통(자바)	• 사용자 모르게 불특성 다수에게 SMS 발송
FlexiSpy	2006년 3월	심비안	• 사용자 모르게 통화 기록, SMS, 콘텐츠, 개인 정보를 빼내어 판매

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

1 모바일 보안 위협의 유형

[스마트폰을 대상으로 한 주요 악성코드]

구분	발견 시기	운영체제	특성
InfoJack	2008년 3월	윈도우 모바일	• 인터넷 연결 시 단말기의 시리얼 번호, OS 정보를 빼가고 파일 설치 유도
Ikee	2009년 11월	아이폰	• 아이폰 단말기 간에 감염되어 사용자 바탕화면 교체
iPhone/Privacy	2009년 11월	아이폰	• 감염된 단말기에서 무선 랜 접속 시 개인 정보를 원격지로 전달
Duh Worm	2009년 11월	아이폰	• 감염된 단말기로 은행 사이트 이용 시 패스워드 유출 및 원격 제어
Stagefright	2015년 7월	안드로이드	• 문자 메시지를 수신만 해도 감염

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 5대 모바일 보안 위협(2018)

- 모바일 보안은 요즘 모든 기업들이 가장 걱정하는 문제로 그럴만한 타당한 이유가 있음, 거의 모든 직원들이 이제 스마트폰으로 기업 데이터에 주기적으로 접근하기 때문임, 이는 민감한 정보가 엉뚱한 사람의 손에 넘어가지 않게 하는 것이 점점 어려워진다는 것을 의미함(BYOD)

- 손실의 위험이 그 어느 때보다 큼,

  포네몬 연구소(Ponemon Institute)
  2016년 보고서에 따르면, 기업 데이터 침해에 따른 평균 비용은 '하루에' 2만 1,155달러라고 함

2 5대 모바일 보안 위협(2018)

- 세상을 떠들썩하게 하는 악성코드 문제에 초점을 맞추기 쉽지만 사실 현실에서 모바일 악성코드 감염은 믿어지지 않을 정도로 드뭄

  한 통계 자료에 따르면, 모바일 악성코드에 감염될 확률은 벼락맞을 확률보다 훨씬 낮음, 이는 모바일 악성코드의 속성 덕분이며 모바일 운영체제 내에 구축된 고유한 보호 기능 덕분이기도 함(샌드박스)

2 5대 모바일 보안 위협(2018)

1. 데이터 유출
   - 데이터 유출은 2018년에 가장 우려되는 기업 보안 위협 가운데 하나로 널리 인식되고 있음, 이 문제가 특히 짜증나는 이유는 악의적인 성격인 경우는 별로 없고 사용자들이 정보 동의 표시와 전송에 사용할 앱을 부주의하게 잘못 선택해 발생하기 때문(부주의)

2 5대 모바일 보안 위협(2018)

1. 데이터 유출
   - 가트너(Gartner)의 모바일 보안 연구 책임자 디오니시오 주멀은 "주요 과제는 앱 검사 프로세스를 이행하는 데 있어 관리자에게 부담을 주지 않고 사용자에게 불만이 생기지 않게 하는 것"이라고 말함 (부담/불만)

2 5대 모바일 보안 위협(2018)

1. 데이터 유출
   - 주멀은 모바일 위협 방어(MTD) 솔루션 활용을 추천함, 예를 들면 시만텍(Symantec)의 엔드포인트 프로텍션 모바일(Endpoint Protection Mobile), 체크포인트(CheckPoint)의 샌드블래스트 모바일 (SandBlast Mobile), 짐페리움(Zimperium)의 Zips 프로텍션(Zips Protection)과 같은 제품들 (MTD)

2 5대 모바일 보안 위협(2018)

1. 데이터 유출
   - 주멀의 설명에 따르면, 이런 유틸리티들은 "유출 행위"가 없는지 앱을 검사하며 문제 있는 프로세스 차단을 자동화할 수 있음
   - 물론, 사용자의 공공연한 실수로 인한 유출은 막을 수 없음, 예를 들면 기업 파일을 퍼블릭 클라우드 스토리지 서버에 전송한다든가, 기밀 정보를 엉뚱한 곳에 붙여넣기 한다던가, 이메일을 의도치 않은 수신자에게 전달한다든가 하는 간단한 실수만으로도 데이터가 유출됨(Public vs. Private Cloud)

2 5대 모바일 보안 위협(2018)

1. 데이터 유출
   - 이는 현재 의료 업계에서 극복하기 위해 애쓰고 있는 문제임, 전문 보험업체인 비즐리(Beazley)에 따르면, 2017년 1~3분기 동안 의료 업체들이 신고한 데이터 침해 가운데 "의도치 않은 정보 공개"에 의한 것이 41%에 달하며 이 비율은 그 다음 많은 원인보다 2배 이상 높음

2 5대 모바일 보안 위협(2018)

1. 데이터 유출
   - 이런 종류의 유출을 가장 효과적으로 방지할 수 있는 것은 데이터 손실 방지(DLP) 도구일 것(DLP)
   - 민감한 정보가 돌발적인 상황 등에서 노출되는 것을 방지할 목적으로 설계된 소프트웨어이기 때문

2 5대 모바일 보안 위협(2018)

2 소셜 엔지니어링

- 효과가 있는 것으로 검증된 소셜 엔지니어링 사기 수법은 데스크톱에서나 모바일에서나 골칫거리임(사회 공학)
- 소셜 엔지니어링 사기꾼들을 쉽게 피할 수 있다고 생각하겠지만 여전히 놀라울 정도로 활개를 치고 있음

2 5대 모바일 보안 위협(2018)

2 소셜 엔지니어링

- 버라이즌(Verizon)의 2017년도 데이터 침해 실태 조사 보고서에 따르면, 엔터프라이즈 솔루션 부문에서 관찰한 데이터 침해 가운데 무려 90%가 피싱(Phishing) 때문인 것으로 나타났음(피싱, 파밍, 스미싱)

2 5대 모바일 보안 위협(2018)

2 소셜 엔지니어링

- 버라이즌은 피싱 시도에 걸린 사용자 비율은 7%에 불과하지만 이들과 같이 잘 속는 사람들이 상습범인 경향이 있다고 밝혔음(상습범)
- 버라이즌의 보고서에 따르면, 일반적인 조직에서 성공적으로 피싱 당한 사용자 가운데 15%가 같은 해에 '최소한' 한 번 이상 또 피싱을 당하게 됨

2 5대 모바일 보안 위협(2018)

2 소셜 엔지니어링

- 피시미(PhishMe)의 정보 보안 및 피싱 방지 전략가 존 렉스 로빈슨은 "전반적으로 모바일 사용이 늘어나고 BYOD 업무 환경이 지속적으로 성장함에 따라 모바일 감염 가능성이 대체적으로 높아지고 있다"고 지적했음(BYOD)
- 피시미는 피싱 시도 인식과 대처에 대한 직원 교육을 위해 실제 상황 시뮬레이션을 활용하는 업체임(Simulation)

2 5대 모바일 보안 위협(2018)

2 소셜 엔지니어링

- 로빈슨은 업무용과 개인용 컴퓨팅 사이의 경계선이 계속해서 흐릿해지고 있다고 말했음
- 업무용 계정과 개인용 계정에 연결된 여러 개의 받은 편지함을 모두 스마트폰에서 확인하는 직원들이 점점 많아지고 있다고 전제하고 근무 중에 온라인으로 모종의 개인 업무를 처리하지 않는 사람은 거의 없다고 덧붙였음
- 그 결과, 업무 관련 메시지와 함께 개인 이메일처럼 보이는 것을 받는 것이 표면적으로는 이상할 것이 없어 보임, 그러나 사실은 계략일 수도 있음(계략)

2 5대 모바일 보안 위협(2018)

3 와이파이 중간자 공격

- 모바일 기기의 안전은 데이터가 전송되는 망의 안전에 달려 있음, 이 시대는 우리 모두가 공용 와이파이(Wi-Fi) 망에 늘 연결되어 있음
- 즉, 우리의 정보는 생각보다 안전하지 않음

2 5대 모바일 보안 위협(2018)

3 와이파이 중간자 공격

- 이런 우려는 얼마나 중요할까? 기업 보안업체 완데라(Wandera)가 발표한 신규 조사 결과에 따르면, 기업 모바일 기기들의 와이파이 사용은 셀룰러 데이터 사용의 거의 3 배임, 공개되어 있고 안전하지 않을 가능성이 있는 와이파이 망에 연결 되어 있는 기기가 거의 ¼에 달함, 누군가 악의적으로 양자간 통신 내용을 가로채는 중간자(Man-in-the-middle) 공격을 최근 한 달 안에 당한 비율도 4%나 됨(이블 트윈)

2 5대 모바일 보안 위협(2018)

3 와이파이 중간자 공격

- 스마트폰 보안 전문가이자 시라큐스 대학교 (Syracuse University) 컴퓨터 과학과 교수인 케빈 두는 "요즘에는 트래픽 암호화가 어렵지 않다"며, "VPN이 없다면 자신의 구역에 많은 문을 열어 놓는 셈"이라고 지적했음(VPN)

2 5대 모바일 보안 위협(2018)

3 와이파이 중간자 공격

- 그러나 제대로 된 엔터프라이즈급 VPN을 선택하는 것은 그렇게 쉽지 않음, 대부분의 보안 관련 사안을 고려할 때 그러하듯 타협이 필요할 수밖에 없음(비용)
- 가트너의 주멀은 “VPN의 서비스 제공은 모바일 기기에서는 더욱 스마트해야 함, 배터리 등 자원 소모를 최소화하는 것이 무엇보다 중요하기 때문” 이라고 설명했음(자원 소모)

2 5대 모바일 보안 위협(2018)

3 와이파이 중간자 공격

- 효과적인 VPN이라면 단순히 사용자가 새로운 사이트에 접속할 때가 아닌 절대적으로 필요할 때라든가 믿을 수 있고 안전하고 알려진 앱 내에서 사용자가 작업하고 있을 경우에만 활성화할 줄 알아야 함(활성화)

2 5대 모바일 보안 위협(2018)

4 패치가 되지 않는 인터넷 연결 기기

- 스마트폰, 태블릿, 소형 인터넷 연결 기기 (흔히 사물인터넷(IoT))는 기업 보안에 새로운 위험 요소임(IoT)
- 이들 기기는 전통적인 업무 기기와 달리 제때 지속적으로 소프트웨어 업데이트가 보장되지 않는 경우가 일반적이기 때문임(업데이트)

2 5대 모바일 보안 위협(2018)

4 패치가 되지 않는 인터넷 연결 기기

- 이는 안드로이드(Android) 기기의 경우 특히 심함
- 대다수의 제조업체들이 제품을 최신 상태로 유지하는 것에 당혹스러울 정도로 비효율적임
- 운영체제 업데이트는 물론 중간 중간의 월간 보안 패치도 마찬가지임
- IoT 기기들은 말할 것도 없음, 애초에 업데이트를 받을 수 있게 설계되지 않은 것조차 많기 때문임

2 5대 모바일 보안 위협(2018)

4 패치가 되지 않는 인터넷 연결 기기

- 케빈 두는 “패칭 메커니즘조차 내장되지 않은 경우가 많음, 요즘 그것이 점점 더 위협이 되고 있다”고 지적했음(가장 기본 → 패치)
- 이번에도 강력한 정책이 도움이 됨, 지속적인 업데이트를 제때 안정적으로 받는 안드로이드 기기가 없지 않음, IoT 환경에 질서와 안정이 찾아올 때까지는 각 회사가 IoT 주변에 자체적인 보안망을 만드는 수밖에 없음

2 5대 모바일 보안 위협(2018)

5 물리적 기기 침해

- 마지막은 바보같아 보이지만 여전히 충격적으로 현실적인 위협으로 남아 있는 것, 분실하거나 제대로 간수하지 않은 기기는 중대한 보안 위협이 될 수 있음(분실 → 2차 피해)
- 강력한 PIN이나 비밀번호가 없거나 전체적인 데이터 암호화가 되어 있지 않은 경우는 특히 그러함

2 5대 모바일 보안 위협(2018)

5 물리적 기기 침해

- 다음 내용을 생각해 보자
- 2016년도 포네몬 연구소 조사에서 전문직 종사자 가운데 35%가 자신의 업무용 기기에 접근 가능한 기업 데이터를 안전하게 보호할 수 있는 필수 조치가 되어 있지 않다고 답변했음(기기 보호)

2 5대 모바일 보안 위협(2018)

5 물리적 기기 침해

- 더 심각한 것은 설문 조사 대상자 가운데 거의 절반이 기기를 보호할 만한 비밀번호, PIN 또는 생체 보안 기능이 없다고 답했다는 것
- 약 2/3는 암호화를 사용하지 않는다고 답했음
- 응답자 가운데 68%는 자신의 모바일 기기를 통해 접속되는 개인 계정과 업무 계정에 같은 암호를 쓴 적이 있다고 답변했음(All or nothing)

2 5대 모바일 보안 위협(2018)

- 스마트폰 탈옥(Jailbreak) 및 루팅(Rooting)에 관련된 정보가 인터넷을 통해 공유되면서 많은 사람이 자신의 취향에 맞게 스마트폰을 변경하여 이로 인한 악성 코드 감염도 급증(탈옥-아이폰, 루팅-안드로이드)

2 5대 모바일 보안 위협(2018)

- 탈옥
  : 애플의 통제를 벗어나
  임의의 소프트웨어를 설치할 수 있도록 하는 것

- 루팅
  : 안드로이드 운영체제를 사용하는 스마트폰에서
  시스템 잠금 장치를 해체하여 운영체제 관리자의
  권한을 얻는 것

2 5대 모바일 보안 위협(2018)

- 탈옥과 루팅
  - 탈옥과 루팅은 모두 보안 취약점을 이용함
  - 시스템 커널이나 라이브러리의 취약점을 해킹해 운영체제의 최고 관리자 권한을 얻을 수 있는 자동화 툴 형태로 배포됨(권한 상승)
  - 안드로이드의 경우 루팅이 가능한 운영체제를 직접 배포하기도 함

2 5대 모바일 보안 위협(2018)

- 탈옥과 루팅
  - 아이폰의 경우 탈옥툴이 나오면 애플이 새로운 iOS 패치 버전을 내놓고 다시 탈옥툴이 나오는 과정이 반복되는데, 탈옥툴에 사용된 보안취약점을 역추적해 애플이 이를 보완하면 기존 탈옥툴로는 탈옥할 수 없어 다시 새로운 취약점을 찾기 때문임 (창과 방패)

2 5대 모바일 보안 위협(2018)

- 탈옥과 루팅
  - 제조업체의 제약이 사라지면
    사용자 입장에서는 많은 장점이 있음
  - 사용자 인터페이스를 사용자가 원하는 대로
    바꿀 수 있고 이를 패키지 형태로 설치할 수 있는
    앱도 나와 있음
  - 듀얼 모니터처럼 애플이 정책적으로 지원하지
    않는 기능을 이용해 아이패드를 마치 맥 노트북의
    서브 모니터처럼 활용하는 것도 가능함

2 5대 모바일 보안 위협(2018)

- 탈옥과 루팅
  - 기기 구매 시 기본 설치됐지만 사용하지 않는 앱들을 삭제해 추가 공간을 확보할 수 있고 시스템 지연을 관리해 앱을 통해 전반적으로 성능을 높일 수도 있음

2 5대 모바일 보안 위협(2018)

- 탈옥과 루팅
  - 그러나 탈옥과 루팅을 하기 전에 이에 따른 위험도 함께 고려해야 함, 전문가들은 운영체제의 최상위 권한으로 스마트폰을 사용한다는 것은 자칫 해킹을 당할 경우 모든 것이 뚫릴 수 있다는 의미라고 지적
  - 제조업체의 제한은 보안을 위한 최소한의 안전장치이기도 하다는 것(권한 상승이 목적인데 원래부터 권한 상승 되어 있음)

2 5대 모바일 보안 위협(2018)

탈옥과 루팅

- 과도한 멀티태스킹을 일으키는 앱은
  배터리 급격히 소모시킬 수 있고,
  앱 안정성에 문제가 생길 수도 있음
- 보안 문제 때문에 은행 앱 중 상당수는
  탈옥 혹은 루팅한 스마트폰에서는 사용할 수 없음

3 모바일 환경에서 주의해야 할 위협 요소 10가지

[OWASP의 상위 10가지 모바일 보안 위협 요소]

코드	위협 요소
M1	적절하지 않은 플랫폼 사용(Improper platform usage)
M2	안전하지 않은 데이터 저장(Insecure data storage)
M3	안전하지 않은 통신(Insecure communication)
M4	안전하지 않은 인증(Insecure authentication)
M5	불충분한 암호화(Insufficient cryptography)

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 모바일 환경에서 주의해야 할 위협 요소 10가지

[OWASP의 상위 10가지 모바일 보안 위협 요소]

코드	위협 요소
M6	안전하지 않은 권한(Insecure authorization)
M7	클라이언트 코드 품질(Client code quality)
M8	코드 변조(Code tampering)
M9	역공학(Reverse engineering)
M10	관련 없는 기능(Extraneous functionality)

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 M1. 적절하지 않은 플랫폼 사용

- 위협 대상
  : 안드로이드 인텐트, 플랫폼 퍼미션, TouchID,
  그 외 모바일 운영체제의 한 부분인 보안 통제가
  해당(플랫폼)

- 공격 요인 : 공격 벡터(다양한 입력)

- 보안 취약성
  : 모바일 앱에서 제공하는 API 또는
  웹 서비스가 노출되어 있어야 함(노출)

4 M1. 적절하지 않은 플랫폼 사용

- 기술적 영향
  : 모바일 장치에 대한 공격으로 기존
  'OWASP Top 10' 취약점과 같은 기술적 영향이 발생

- 비즈니스 영향
  : 기술적 영향과 동일한 영향이 발생하지만
  비즈니스 측면에서 고려할 수 있음

5 M2. 안전하지 않은 데이터 저장

- 위협 대상
  : 분실하거나 도난 당한 모바일 장치를 습득하여 공격하는 경우

- 공격 요인
  : 개인정보가 포함된 파일이나 민감한 정보가 포함된 파일, 제삼자의 디렉터리 내용 등을 볼 수 있고, 정보 자산을 훔치지 위해 등록된 앱을 수정하거나 악성 코드를 만들 수 있음(개인정보/정보자산)

5 M2. 안전하지 않은 데이터 저장

- 보안 취약성
  : 루팅이나 탈옥 상태에서는
  암호화된 보호가 무력화될 수 있음(루팅/탈옥)

- 기술적 영향
  : 데이터를 잃어버릴 수 있을 뿐만 아니라
  수많은 사용자의 데이터가 삭제될 수 있음(분실/삭제)

- 비즈니스 영향
  : 조직에서는 신원 도용, 부정, 브랜드 손상, 외부 정책
  위반(PCI 등), 자료 손실 등의 리스크가 발생할 수 있음

6 M3. 안전하지 않은 통신

- 위협 대상
  : 로컬 네트워크를 공유하는 악의적인 공격자, 통신 제공사, 네트워크 장치 제공자, 모바일 장치에 있는 악성 코드 등(통신)

- 공격 요인
  : 안전하지 않은 통신 범위를 모니터링 할 수 있는 부분(스니핑)

6 M3. 안전하지 않은 통신

- 보안 취약성
  : 모바일 애플리케이션은 인증이 필요할 때만
  SSL/TLS를 사용하기 때문에 중요한 데이터나
  세션 아이디와 같은 정보가 노출될 수 있음(정보 노출)

- 기술적 영향
  : 개인 사용자의 데이터와 계정 정보가
  노출될 수 있음(노출)

- 비즈니스 영향
  : 사용자의 개인 정보 유출이 기업의 신원 도용,
  부정, 브랜드 손상으로 이어질 수 있음

7 M4. 안전하지 않은 인증

- 위협 대상
  : 전형적으로 자동화된 툴을 이용하여 공격 수행

- 공격 요인
  : 모바일 악성 코드나 봇넷으로 인증 체계의 취약점을 발견하면 모바일 앱 백 엔드 서버에게 서비스 요청을 전달하여 인증 또는 모바일 앱의 특정 요청을 우회 (우회)

- 보안 취약성
  : 보통 모바일 장치의 입력폼에서 발생

7 M4. 안전하지 않은 인증

- 기술적 영향
  : 공격자가 다른 사용자에게 특정 행위를 할 수 있음

- 비즈니스 영향
  : 브랜드 손상, 정보 유출, 데이터에 대한
  불법적인 접근 등의 결과 초래(불법 접근)

8 M5. 불충분한 암호화

- 위협 대상
  : 부적절하게 암호화된 데이터에 물리적으로
  접근할 수 있는 모든 행위자 또는 모바일에
  설치된 악성 코드(암호화)

- 공격 요인
  : 장치에 물리적으로 접근하여 데이터를 복호화하거나
  네트워크 트래픽을 캡처하거나 암호화된 데이터에
  접근할 수 있는 악성코드

8 M5. 불충분한 암호화

- 보안 취약성
  : 암호화된 코드를 복호화하거나 암호화 절차의 결함이나 취약한 암호화 알고리즘으로 원본 데이터를 복호화(암호화/복호화)

- 비즈니스 영향
  : 프라이버시 침해, 정보 유출, 코드 유출, 지식재산권 유출, 브랜드 손상과 같은 결과를 초래

- 기술적 영향
  : 민감한 데이터가 유출될 수 있음(유출 → 기밀성)

9 M6. 안전하지 않은 권한

- 위협 대상
  : 자동화된 툴을 이용하여 공격 수행(권한)

- 공격 요인
  : 권한 체계가 취약하다는 것을 공격자가 파악하면
  합법적인 사용자로 애플리케이션에 로그인하여
  성공적으로 권한 통제를 우회(우회)

- 보안 취약성
  : 낮은 권한을 가진 사용자가 높은 권한을 가진
  사용자만이 실행 가능한 기능을 실행할 수 있는지
  확인(권한 상승)

9 M6. 안전하지 않은 권한

- 기술적 영향
  : 관리자 권한으로 특정 명령어를 실행하거나
  시스템을 파괴하거나 민감한 데이터가 유출될 수 있음

- 비즈니스 영향
  : 브랜드 손상, 부정, 정보 유출과 같은
  다양한 비즈니스 영향이 발생

10 M7. 클라이언트 코드 품질

- 위협 대상
  : 모바일 코드에 의도치 않은 입력을 전달

- 공격 요인
  : 공격 대상 앱에 조작된 입력값을 전달하여 공격을 수행

- 보안 취약성
  : 정적 분석 도구 또는 퍼저를 이용하여
  모바일 코드의 취약점을 발견(퍼징)

10 M7. 클라이언트 코드 품질

- 기술적 영향
  : 공격자가 원하는 특정 코드를 실행하거나
  모바일 장치에 대한 서비스 거부 공격을 원격으로
  수행할 수 있음(DoS)

- 비즈니스 영향
  : 브랜드 손상, 지식재산권 유출, 정보 유출 등의
  결과를 초래

11 M8. 코드 변조

- 위협 대상
  : 앱스토어에 조작된 앱을 올리거나 피싱 공격을 통해
  코드가 변조된 악의적인 앱을 설치하도록 유도(역공학)

- 공격 요인
  : '애플리케이션 패키지의 핵심 바이너리에 대한
  바이너리 변경', '애플리케이션 패키지에 있는 리소스
  파일에 대한 바이너리 변경', '악의적 인 목적의 코드를
  실행하거나 데이터를 캡처하는 시스템 API 변경' 등

11 M8. 코드 변조

- 보안 취약성
  : 애플리케이션의 형태를 변경 (바이너리 패치, 로컬 자원 변경, 메소드 후킹 포함)(후킹)

- 기술적 영향
  : 일반적으로 새로운 기능을 추가하거나 정보를 유출

- 비즈니스 영향
  : 저작권 침해로 인한 수익 감소, 브랜드 손상 등의 결과를 초래

12 M9. 역공학

- 위협 대상
  : 앱스토어에서 공격 대상 앱을 내려 받아
  로컬 환경에서 분석(Reverse engineering)

- 공격 요인
  : IDA Pro, Hopper, otool, strings와 같은 바이너리
  검사 툴을 이용하여 핵심 바이너리 파일 분석

- 보안 취약성
  : 일반적으로 모바일 코드는 역공학에 취약(코드 크기)

12 M9. 역공학

- 기술적 영향
  : 백 엔드 서버 정보 추출, 암호화된 문자열 또는 암호화 키 추출, 지식재산권 정보 추출, 백 엔드 시스템에 대한 공격 수행과 같은 목적을 달성할 수 있음

- 비즈니스 영향
  : 지식재산권 유출, 브랜드 손상, 신원 도용, 백 엔드 시스템에 대한 침해 등의 결과를 초래

12 M9. 역공학

- 리버스 엔지니어링(영어: reverse engineering, RE) 또는 역공학(逆工學)은 장치 또는 시스템의 기술적인 원리를 그 구조분석을 통해 발견하는 과정임

- 이것은 종종 대상(기계 장치, 전자 부품, 소프트웨어 프로그램 등)을 조각내서 분석하는 것을 포함 함

  그리고 유지 보수를 위해, 또는 같은 기능을 하는 새 장치를 원본의 일부를 이용하지 않고 만들기 위해 대상의 세부적인 작동을 분석하는 것을 포함 함

12 M9. 역공학

- 리버스 엔지니어링의 기원은 상업적 또는 군사적으로 하드웨어를 분석한 것에서 시작되었음

  목적은 원본 생산의 절차에 관한 지식이 거의 없는 상태에서, 최종 제품을 가지고 디자인 결정과정을 추론하는 것

- 같은 기술이 레거시 소프트웨어 시스템을 응용하기 위해 현재 연구되고 있는데, 산업이나 국방이 아니고, 오류, 미완성, 접근 불가인 문서를 수정하기 위함

12 M9. 역공학

- 사용 이유
  - 소프트웨어 간의 상호 운용성
  - 사라진 문서
  - 상품 분석
  - 디지털 업데이트/수정
  - 호환성 부품개발 및 성능향상
  - 안전 감사
  - 군사 또는 산업 간첩
  - 복제 보호 해제

12 M9. 역공학

- 사용 이유
  - 허가되지 않은 불법 복제의 생성
  - 소프트웨어 불법 정품 인증 및 시리얼 코드 생성
  - 소프트웨어 키젠 및 크랙 생성
  - 학술/학문적 추구
  - 호기심
  - 경쟁사의 기술 정보 분석
  - 악성코드 분석
  - 소프트웨어 보안성 테스트

13 M10. 관련 없는 기능

- 위협 대상
  : 일반적으로 백 엔드 시스템에서 숨겨진 기능을 찾기 위해 모바일 앱의 기능을 분석

- 공격 요인
  : 로그 파일과 설정 파일을 살펴보거나 때로는 개발자가 실수나 고의로 특정 기능을 숨겨 놓기도 함

- 보안 취약성
  : 백 엔드 테스트 환경에 대한 정보나 사용자 환경 테스트 정보, API 관련 정보를 포함하는 기능 등은 공격자에게 유리하게 사용될 수 있음

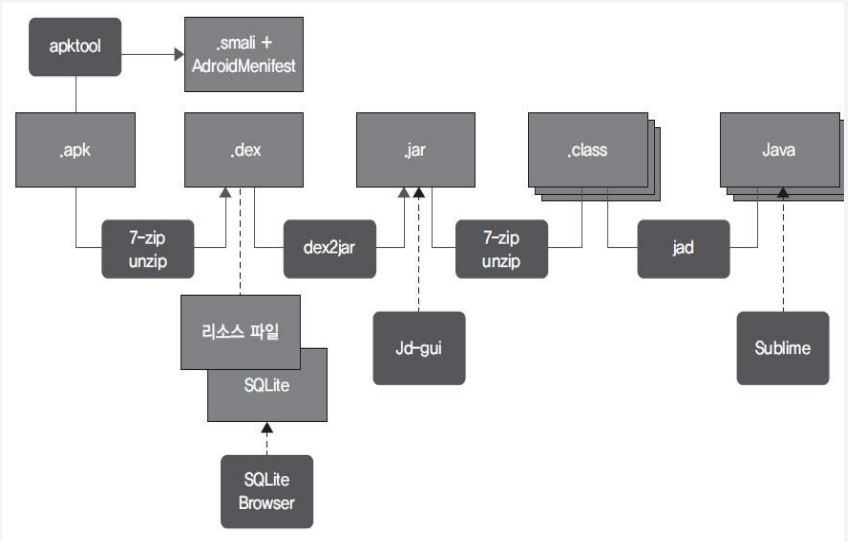
13 M10. 관련 없는 기능

- 기술적 영향
  : 백 엔드 시스템의 동작 내용 노출, 비인가자가
  높은 권한을 가지고 특정 기능을 수행하는 것 등

- 비즈니스 영향
  : 민감한 기능에 대한 불법적인 접근,
  브랜드 손상, 지식재산권 노출 등(불법 접근)

14 안드로이드 앱 분석 과정

[안드로이드 앱 분석 절차]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

14 안드로이드 앱 분석 과정

[안드로이드 앱 분석에서 생성되는 파일](달빅)

분석 단계	파일(확장자)	설명
1	.apk	안드로이드 앱 패키지 파일
3	.dex	달빅(Dalvik) 실행 파일
4	.smali	스마일리 파일
5	.jar	자바 클래스 압축 파일
6	.class	자바 클래스 파일
7	.java	자바 파일

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

14 안드로이드 앱 분석 과정

[안드로이드 앱 분석 단계와 사용 툴]

분석 단계	사용 툴	설명
해체 툴	7-zip	안드로이드 앱 패키지 파일
	unzip	달빅 실행 파일
	dex2jar	스마일리 파일
	jad	자바 클래스 압축 파일
	apktool	자바 클래스 파일
Viewer	SQLite Browser	sqllite 데이터베이스 파일 viewer
	Jd-gui	.jar 파일 viewer
	Sublime	.java 파일 viewer

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017