정보보호와 시스템보안

모바일 보안

전은아

목차

1. 모바일 운영체제의 역사
2. 모바일 운영체제의 보안과 취약점
3. 모바일 기기 보안의 문제점

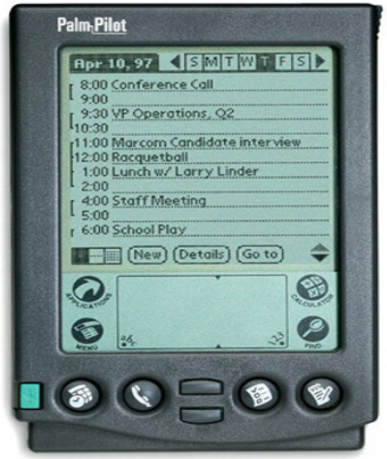
학습목표

- 모바일 운영체제의 발전사를 이해한다.
- 모바일 운영체제별 보안 체계를 이해한다.
- 모바일 운영체제별 취약점과 위협을 이해한다.
- 블루투스의 구조와 취약점을 이해한다.

01 모바일 운영체제의 역사

팜 OS

- 1996년에 개발된 운영체제
- 개인용 정보 단말기(PDA: Personal Digital Assistance)인 팜 파일럿에서 사용하기 위해 만든 것.
- 팜 OS에는 주소, 달력, 메모장, 할 일 목록, 계산기와 개인정보를 숨기기 위한 간단한 보안 툴이 포함되어 있음.



[그림 1] 팜 OS 1.0이 탑재된 팜 파일럿 5000

윈도 CE

- 마이크로소프트가 PDA나 모바일 장치 등에 사용하기 위해 만든 운영체제
- 1MB 이하의 메모리에서도 동작이 가능하도록 설계
- 초기에는 PDA의 운영체제로 주로 사용
- 이후에는 AutoPC, 스마트폰 등의 기기에 사용

[그림 2] 윈도우 CE 1.0이 탑재된 카시오 A-11

01 모바일 운영체제의 역사

블랙베리 OS

- RIM(Research In Motion)에 의해 만들어진 모바

  일 운영체제
- 메시지와 E-Mail 전송과 관련한 기능과 보안에

  초점을 둔 제품

[그림 3] 초기의 블랙베리 5790

iOS

- 애플의 아이폰과 아이패드에 사용되는 모바일 운영체제
- 처음부터 iOS로 불렸던 것은 아님.
  - 2007년 6월 29일에 4GB/8GB의 용량으로 출시된 아이폰의 첫 번째 버전인 아이폰 오리지널의 운영체제는 OS X였음.
  - OS X는 당시 맥북의 운영체제를 모바일로 바꾼 것.

[그림 4] 아이폰 오리지널

01 모바일 운영체제의 역사

안드로이드

- 구글과 핸드폰 업체들이 연합하여 개발한 개방형 모바일 운영체제
- 2007년 11월에 최초의 구글폰인 HTC의 Dream(T-Mobile G1)에 안드로이드 1.0이 탑재된 것이 시작.

[그림 5] HTC Dream (T-Mobile G1)

02 모바일 운영체제의 보안과 취약점

현재 모바일 흐름

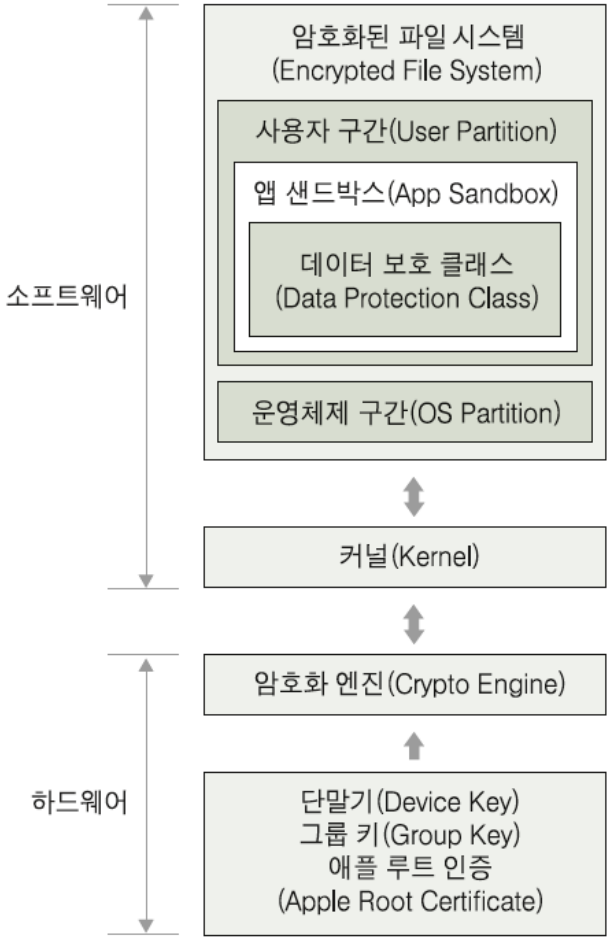
- 애플의 iOS와 구글의 안드로이드

iOS의 보안과 취약점

- iOS는 맥 OS인 OS X의 모바일 버전에서부터 시작
- 맥 OS는 Darwin UNIX에서 파생하여 발전된 것으로 iOS의 원래 틀은 유닉스라고 생각할 수 있음.

- iOS의 보안 체계
  - iOS는 보안에 대한 기본적인 통제권을 애플이 소유하고 있음.

02 모바일 운영체제의 보안과 취약점



[그림 7] iOS의 보안 모델

02 모바일 운영체제의 보안과 취약점

iOS의 보안과 취약점

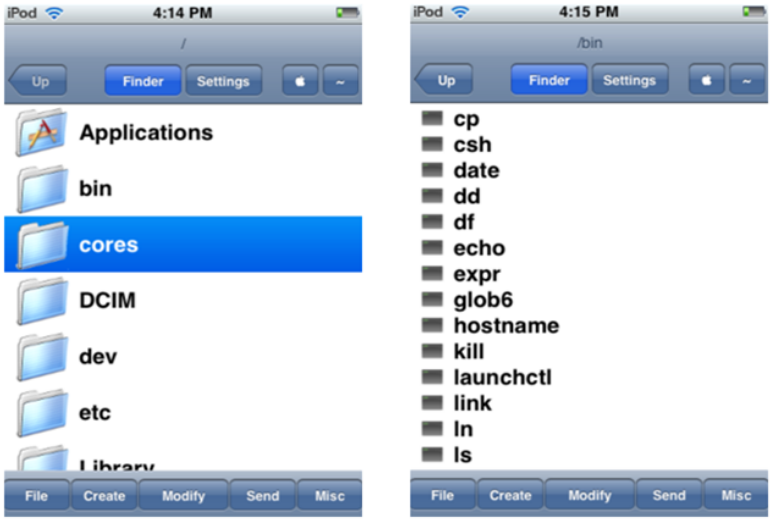
- 애플은 보안 모델을 기초로 4가지의 시스템 보안 체계를 가짐.
  - **안전한 부팅 절차 확보**
    - iOS를 사용하는 모바일 기기에서 모든 소프트웨어는 애플 암호화 로직의 서명된 방식에 의해 무결성이 확인된 후에만 동작함.
  - **시스템 소프트웨어 개인화**
    - 애플은 모든 소프트웨어를 애플의 아이튠즈를 통해 일괄적으로 배포.
    - 소프트웨어를 설치/업데이트 시에는 이전 버전으로 다운그레이드할 수 없도록 함
      - 이를 시스템 소프트웨어 개인화라는 절차를 통해서 통제하고 있음.
  - **응용 프로그램에 대한 서명**
    - 애플은 iOS에 설치되는 모든 앱에 대해서 코드 무결성 사인(Code Signature)을 등록하게 하고 있음.
      - 이 코드 무결성 사인은 앱에 대한 일종의 해시 값으로 등록된 앱의 코드 무결성 사인이 다를 경우 앱을 설치하지 못하게 하는 것임.
      - 또한 개인이 각각의 iOS에 설치한 어플리케이션이 문제가 있을 경우 네트워크에 연결된 iOS를 강제로 삭제할 수 있음.
  - **샌드박스 활용**
    - 사용자 앱의 경우 기본적으로 앱끼리 데이터를 주고 받을 수 없고, 시스템 파일에도 접근할 수 없음.
    - 앱끼리 문서나 음악 사진 등을 전송하는 것은 시스템 API에서 기능을 제공하는 경우에만 가능.

- 애플은 이 외에도 멀티태스킹과 원격지에서 iOS 로그인을 금지함.

02 모바일 운영체제의 보안과 취약점

iOS의 보안과 취약점

- iOS의 취약점
  - iOS의 보안상의 문제점은 대부분 탈옥(Jailbreak)한 iOS 기기에서 발생

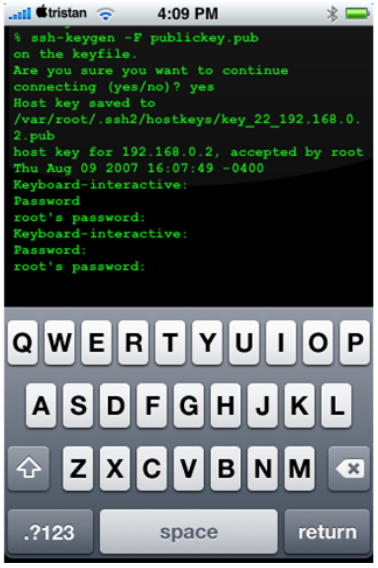


[그림 8] 탈옥한 iOS로 내부 파일 접근

02 모바일 운영체제의 보안과 취약점

iOS의 보안과 취약점

- iOS의 취약점
  - 탈옥된 iOS에서 SSH 서버를 실행할 경우 로컬이나 원격지에서 로그인하는 것도 가능



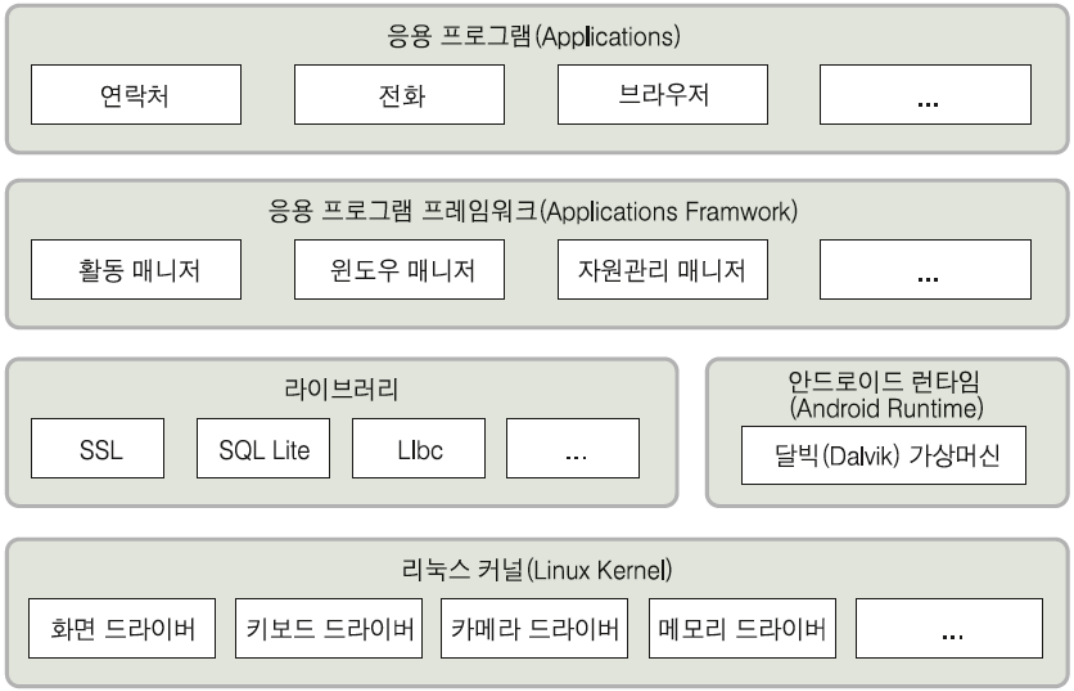
[그림 9] 탈옥한 iOS에서 SSH 서버 실행

  - 사용자가 iOS를 탈옥할 경우에 반드시 적용해야 할 보안 사항은 바로 기본 패스워드 변경
  - iOS에서는 root의 패스워드가 'alpine'으로 설정되어 있음
    - 탈옥을 해놓은 상태에서 SSH 서버 등을 실행시켜놓으면 임의의 접속자에 의해 iOS에 있는 정보들이 유출될 수 있음.

02 모바일 운영체제의 보안과 취약점

안드로이드의 보안과 취약점

- 안드로이드(Android)는 리눅스 커널(2.6.25)을 기반으로 한 모바일 운영체제
  - 2005년 : 구글이 안드로이드사를 인수
  - 2007년 11월 : 안드로이드 플랫폼을 휴대용 장치 운영체제로 무료 공개한다고 발표
- 안드로이드의 보안 체계
  - 안드로이드는 리눅스 커널을 기반으로 함.



[그림 10] 안드로이드 운영체제의 구조

02 모바일 운영체제의 보안과 취약점

안드로이드의 보안과 취약점

- 안드로이드는 개방형 운영체제로서의 보안 정책을 적용
  - 응용 프로그램의 권한 관리
    - 안드로이드에 설치된 모든 응용 프로그램은 일반 사용자 권한으로 실행됨.
  - 응용 프로그램에 대한 서명
    - 안드로이드 역시 애플과 마찬가지로 설치되는 응용 프로그램에 대해 서명을 하고 있음.
      - 하지만 애플이 자신의 CA를 통해 각 응용프로그램을 서명하여 배포하는 반면, 안드로이드는 개발자가 서명하도록 하는 차이점이 있음.
      - 안드로이드에서의 전자서명은 보안보다는 응용 프로그램에 대한 통제권을 개발자가 가지게 하는 것이 목적.
  - 샌드박스 활용
    - 안드로이드는 특정 형태를 갖추어 권한을 요청하는 것을 허용
    - iOS에 비해 상대적으로 어플리케이션 간 통신과 데이터 전달이 자유로움.

  - 안드로이드의 취약점
    - 안드로이드는 사용자의 선택에 따라 보안 수준을 선택할 수 있음.
      - 이런 이유로 각종 바이러스와 악성코드가 유포되었으며 이로 인해 백신이 보급되고 있음.

[그림 11] 안드로이드 백신

02 모바일 운영체제의 보안과 취약점

■ 안드로이드의 보안과 취약점

[표 1] iOS와 안드로이드의 보안 체계 비교

	iOS	안드로이드
운영체제	Darwin UNIX에서 파생하여 발전한 OS X의 모바일 버전	리눅스 커널(2.6.25)을 기반으로 만들어진 모바일 운영체제
보안 통제권	애플	개발자 또는 사용자
프로그램 실행권한	관리자(root)	일반 사용자
응용 프로그램에 대한 서명	애플이 자신의 CA를 통해 각 응용프로그램을 서명하여 배포	개발자가 서명
샌드박스	엄격하게 프로그램 간 데이터 통신 통제	iOS에 비해 상대적으로 자유로운 형태의 어플리케이션의 실행이 가능
부팅 절차	암호화 로직으로 서명된 방식에 의한 안전한 부팅 절차 확보	-
소프트웨어 관리	단말 기기별 고유한 소프트웨어 설치 키 관리	-

03 모바일 기기 보안의 문제

■ 이동성으로 인한 문제점

- 모바일 기기 보안의 가장 큰 문제는 모바일 기기의 이동성에 있음.
- 무선랜의 경우 노트북을 수신율이 높은 안테나를 붙여서 차를 타고 보안이 취약한 무선 랜을 탐색하며 해킹을 시도할 수 있는데 이를 워 드라이빙(Wardriving)이라고 함.

[그림 12] 워 드라이빙

03 모바일 기기 보안의 문제

블루투스의 취약점과 위협

- 블루프린팅
  - 블루프린팅(Blueprinting)은 블루투스 공격 장치의 검색 활동을 의미
    - 블루투스는 장치 간 종류를 식별하기 위해 서비스 발견 프로토콜(SDP : Service Discovery Protocol)을 보내고 받음.
    - 공격자는 이를 이용해 공격이 가능한 블루투스 장치를 검색하고 모델을 확인할 수 있음.
- 블루스나프
  - 블루스나프(BlueSnarf)는 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격
    - 공격자는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환할 수 있는 OPP(OBEX Push Profile)를 사용하여 정보를 열람
- 블루버그
  - 블루버그(BlueBug)는 블루투스 장비 간 취약한 연결 관리를 악용한 공격
    - 블루투스 기기는 한 번 연결되면 이후에는 다시 연결해주지 않아도 서로 연결됨.
    - 이 인증 취약점을 이용하여 공격.

Q&A