Introduzione ad Android

Lezione 4
Android security

Ruggero Donida Labati

Laboratorio di Sistemi Operativi
Università degli Studi di Milano
Dipartimento di Informatica
A.A. 2022/2023

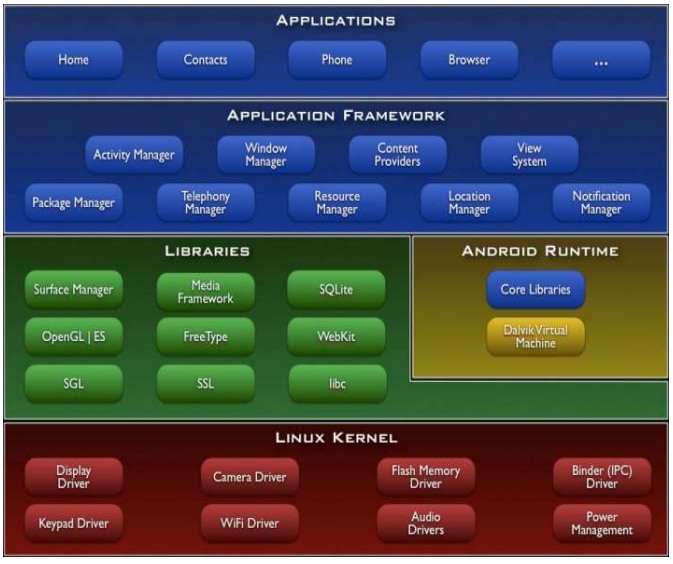
Sommario

1. Android OS
2. Android security
3. Security analysis

Android OS (1/3)

- System Architecture
  - Linux Version 2.6 or 3.0.1
  - Dalvik Virtual Machine (VM)
  - Application Framework

Android OS (2/3)



Android OS (3/3)

- Applications
  - Applications are written in Java or Python
  - Applications are run on the Dalvik Virtual Machine
  - Development done in the Android SDK
  - Development is open to all
  - User driven Android Market

Android security (1/8)

- Security triad applicability
  - Confidentiality
  - Integrity
  - Availability

Android security (2/8)

- Android Security
  - Relies on security of its foundations: Linux, Dalvik, and Java.
  - Security Goal: "*A central design point of the Android security architecture is that no application, by default, has permission to perform any operations that would adversely impact other applications, the operating system, or the user*."

Android security (3/8)

- Enforcement strategy
  - Application signing and certification
  - Linux username base access restriction
  - Capability permissions

Android security (4/8)

- Application Sandboxes
  - All Applications run as their own Linux user
  - Several Inter-Process Communication methods
    - Activities
    - Services
    - BroadcastReceiver
    - ContentProvider
    - Intent
  - Applications utilize a capability like model to protect the system and the user

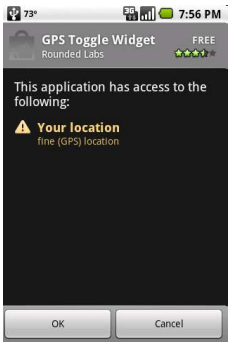
Android security (5/8)

- Android capabilities and permissions
  - Capabilities default to safe state
  - Must be explicitly defined to enable capabilities
  - Permissions are static on install
  - Users have open view of permissions

Android security (6/8)

String	ACCESS_COARSE_LOCATION	Allows an application to access coarse (e.g., Cell-ID, WiFi) location
String	ACCESS_FINE_LOCATION	Allows an application to access fine (e.g., GPS) location

http://developer.android.com/reference/android/Manifest.permission.html



http://www.simplehelp.net/images/quick_gps/img06.png

Android security (7/8)

- Security concerns for developers
  - Protect your application, use least privilege principle
  - If you expose, mediate IPCs
  - Provide maximum availability
    - Minimize memory footprint
    - Minimize battery usage

Android security (8/8)

- Security concerns for users
  - Do your research
    - Read reviews.
    - Analyze capabilities/permissions before installing
    - Use common sense
    - http://www.downloadsquad.com/2010/06/28/understanding-the-android-market-security-system/

Security analysis (1/3)

- Security Analysis
  - Mediation
  - Verifiability
  - Integrity of TCB

Security analysis (2/3)

- Principles of Secure Design
  - Least privilege
  - Fail safe defaults
  - Economy of mechanism
  - Complete mediation
  - Defense in depth
  - Open design
  - Separation of privilege
  - Least common mechanism
  - Psychological acceptability

Security analysis (3/3)

- Secure architecture
- Reliance on trust
- As with all things, use your head

Credits

- Daniel Angelis, Michael Rothstein, „Android™ OS Security - A brief synopsis of the Android Operating System and its security”