Module 51
(Mobile Device Fundamentals - Android)

• In this Module, we'll briefly discuss the general landscape of mobile devices. You will then learn about the underlying structure and security properties of Android devices. You'll also know how most trojan apps are developed. You'll be able to identify several of the common categories of security vulnerabilities to which current Android mobile devices are subject.
Mobile Devices

• Targets of interest:
  – Smartphones
  – Tablet Computers

• Most popular platforms
  – Android OS (Google)
  – IOS (Apple)
Android Devices

• Android started in 2003 and acquired in 2005 by Google.

• What is it? Software stack including
  – Operating system (linux)
  – Framework
  – Middleware
  – Applications
Android Software Structure

- Linux OS at lowest layer
- Libraries to provide access to
  - Device functionality (camera, graphics, sound, GPS, phone network, wifi network)
  - System underpinnings (SQLite database with no encryption that records all system and application settings and information)
  - Dalvik Virtual Machine
- Application Framework
- Applications
Android Security Measures

- Application sandbox uses Linux user protection scheme to isolate app resources. Unique uid assigned to each process so processes cannot interact.
- Full system encryption using AES 128 is available, but the system partition is read-only and will not be encrypted.
- Address Space Layout Randomization (ASLR) and no-execute permission on memory areas used to avoid stack and heap attacks.
- Permission model controls access to camera, location, data, telephony, SMS.MMS. Apps request such permission on installation. But it is given as all-or-none.
- All applications must be signed with a cert signed by the app developer. (But certificate may be self-signed. No need to be signed by a Certificate Authority.)
Android Development Tools

- System Development Kit (SDK) for Linux, Mac, Windows. Includes
  - Emulator for ARM (from ARM holdings) mobile devices
    - Can't send phone calls or real SMS except to another instance of the emulator
    - No bluetooth or camer/video
    - No Google apps (gmail, maps) or telephone carrier apps.
  - Android Debug Bridge
  - Dalvik Debug Monitor Server
Rooting a mobile device

- Rooting (Android nomenclature) or jail-breaking (iOS nomenclature) refers to an escalation privilege attack in which you increase your privilege so you can gain access to all phone resources. (Normal phone access is less privileged.)

- Rooting is arranged by
  - Exploiting a vulnerability in the underlying software of the device, or
  - Replacing your entire ROM with one supporting superuser access.
Benefits and Drawbacks of Rooting

- **Drawbacks:**
  - May brick your device
  - Voids manufacturer warranty
  - May open yourself up to new malware attacks

- **Benefits:**
  - Full control of the device
  - Access to the latest software versions (fewer vulns)
  - Can run SuperUser.apk which controls access to root privileges for other processes
Android App Structure

- Android applications (apk files) are just PK files (Phil Katz – developer of zip). Contents:
  - Manifest
    Encoded XML file defining software components, services, activities, permissions, etc.
  - Classes.dex
    Dalvik executable code that implements the application.
    - Broadcast receivers (event handlers)
    - Services (that run in background with no GUI elements)
Trojan Development

• Common Vector of Infection is the Downloading of a *Trojan App*. Behaves as normally expected, but provides a special malware component.

• Development plan:
  - Start with legitimate application
  - Disassemble dex code
  - Decode manifest
  - Include malicious code
  - Assemble dex code
  - Encode the (possibly modified) manifest
  - Sign the final apk
Android Master Key Vulnerability

- On installation, android checks the integrity of the application by using a checksum calculated on the apk dex components.
- These components are unpacked from the PK file one at a time.
- If any redundant components are encountered they are ignored.
- But when the apk execution occurs, the dex components are unpacked in such a way that the most recently redundant component is used.
- Upshot: you can replace a valid component with a malicious one and use the original certificate and signature.
- Patch released by Google in July 2013.
How Do These Apps Get on Your Device?

- One estimate is that 30% of smartphone users have no password.
- Consider this app:
- Have you ever downloaded an app from anywhere except the Android Marketplace?
- Malware has been hosted on the Marketplace as well.
SMS Abuse Malware

- More common in eastern Europe.
- SMS charges are immediately applied rather than being billed monthly.
Phishing Attacks

- Apps imitating legitimate banking apps are linked via email sent to unsuspecting recipients.
- Clients using these applications provide their banking credentials.
Poorly Written Applications

• Many apps are written without encryption.
  – If users connect via wifi, data can be compromised.
• Many applications use hard-coded passwords.
  – Discover the password on your device and you can use it on another one.
Protections

- Upgrade, upgrade, upgrade
- Use a password on your device
- Encrypt your user data
- Don't download software from anywhere except the Google Marketplace
- (Don't) Root Your Device
- Make software developers write better code!?!?