Arthur Liou
CS373

Week 9-10 Writeup

Prompt: Submitting a write-up of your thoughts, impressions, and any conclusions based on the material from the week. Each week will have its own assignment in the grades page.

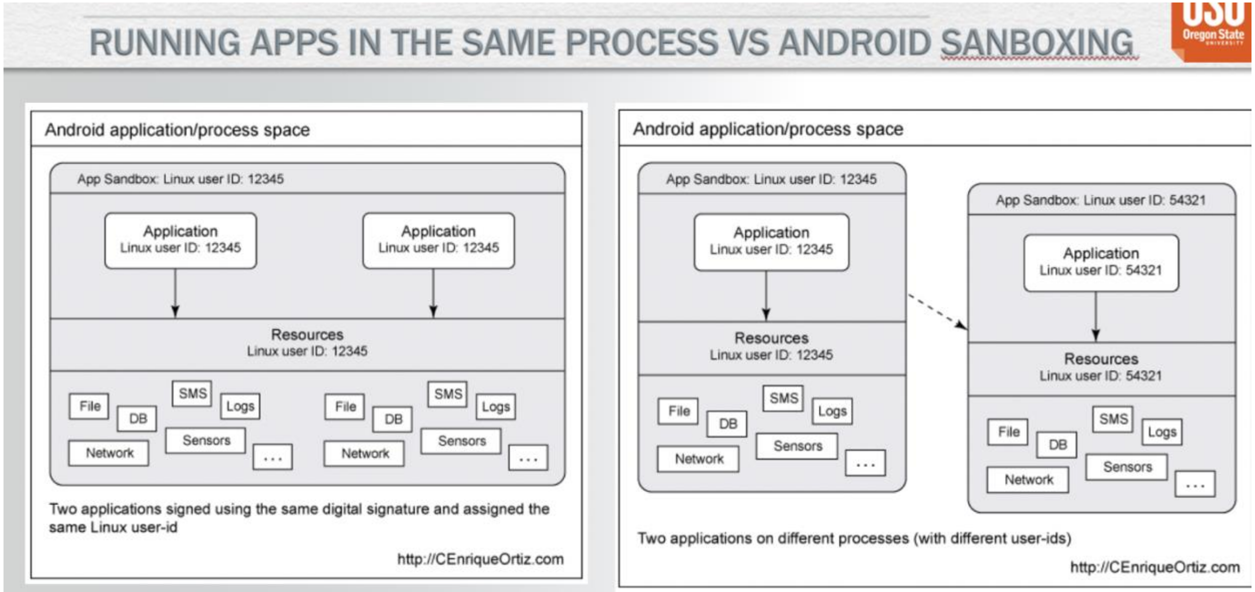
For the first part of this week's writeup, I'm reflecting on the topic – Mobile Security. I originally thought this week would be very engaging material, similar to how I found the material last week. Unfortunately, I found this week's material (concepts and labs) rather dull, disengaging, and an incredible letdown to end the course, having not yet taken the final.

For a brief summary of what we covered and learned, see my lecture notes below.

Lecture Notes

Lesson 1 – Mobile Security

- History of Mobile Devices, Mobile OS History.
- World-wide Smartphone Sales. Android takes way off.
- Apple iOS Slide, Microsoft Windows Phone, Google Android, also other mobile OS
- Mobile OS Executable environments, security features
- Running Apps in the Same Process vs. Android Sandboxing



RUNNING APPS IN THE SAME PROCESS VS ANDROID SANBOXING

Two applications signed using the same digital signature and assigned the same Linux user-id

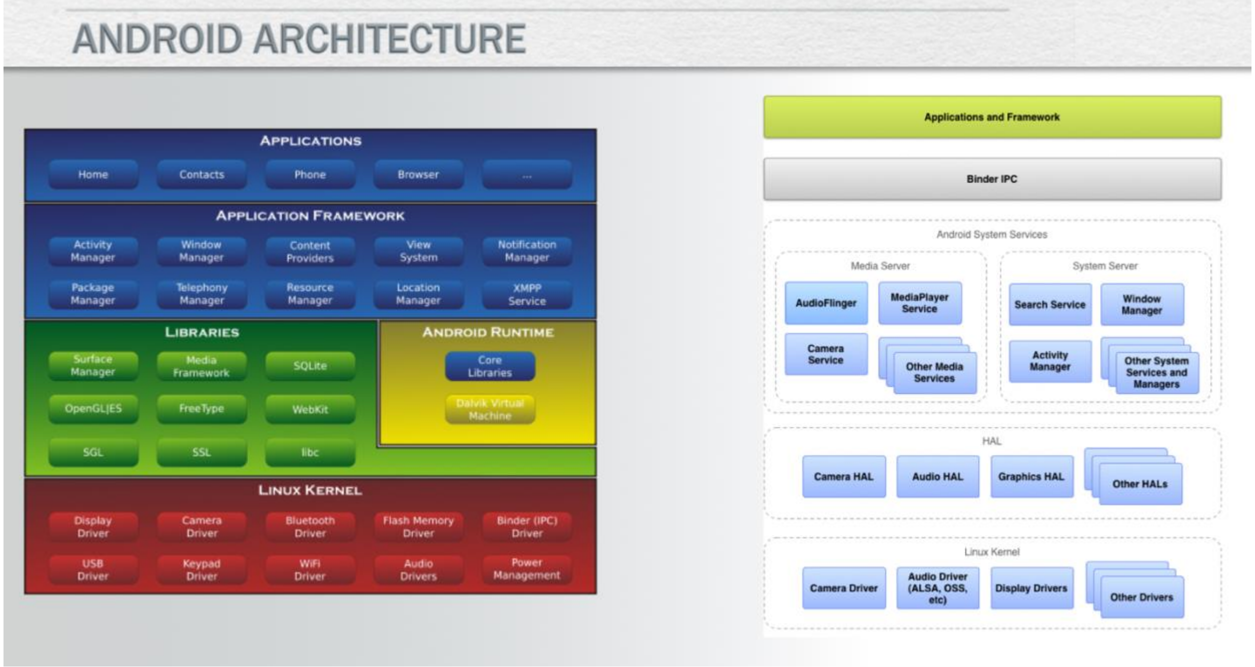
http://CEnriqueOrtiz.com

Two applications on different processes (with different user-ids)

http://CEnriqueOrtiz.com

- System Security Bypasses – Jailbreaking, Rooting in Android, Security Enhancements
- Mobile Malware Genesis, started in 2000-2004
- Middle Ages – 2005-2006, 2006-2008
- Calm Before the Storm – 2008-2010, New Platforms with Smartphone revolution, market share changed, new capabilities
- Symbian Worm YXES: First Mobile Botnet
- Ikee – first Ios malware. Jailbroken phones (2009)

- First Android Malware in the wild. Fakeplayer, Tapsnake
- Andrew Malware Revolution – exponential increase
- Geimini – first android botnet – 2010, China, Leaks sensitive info to a remote server
- PJApps – Interception of SMS messages, Found 2011 targeting Chinese users
- Droiddream – android market nightmare, 2011, many apps, XOR obfuscation (embeded key), attempts to root device using two public exploits
- Google Action – Remote Kill Switch
- Android Fundamentals



ANDROID ARCHITECTURE

APPLICATIONS
Home
Contacts
Phone
Browser
...

APPLICATION FRAMEWORK
Activity Manager
Window Manager
Content Providers
View System
Notification Manager
Package Manager
Telephony Manager
Resource Manager
Location Manager
XMPP Service

LIBRARIES
Surface Manager
Media Framework
SQLite
OpenGL|ES
FreeType
WebKit
SGL
SSL
libc

ANDROID RUNTIME
Core Libraries
Dalvik Virtual Machine

LINUX KERNEL
Display Driver
Camera Driver
Bluetooth Driver
Flash Memory Driver
Binder (IPC) Driver
USB Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Applications and Framework

Binder IPC

Android System Services
Media Server
AudioFlinger
MediaPlayer Service
Camera Service
Other Media Services
System Server
Search Service
Window Manager
Activity Manager
Other System Services and Managers

HAL
Camera HAL
Audio HAL
Graphics HAL
Other HALs

Linux Kernel
Camera Driver
Audio Driver (ALSA, OSS, etc)
Display Drivers
Other Drivers

- Android Runtimes, Dalvik architectures
- Application sandboxing in android vs linux
- Android application components: Activities, Services, Broadcast Receivers, Content Providers
- Android interprocess communication: official and nonofficial
- Intents – messages between components
- Sticky Broadcasts
- Android application permissions
- Android Manifest.xml encoded inside the APK file.
- Labs and Slides related to the labs, tools
- Appendix Slides
- Analog Systems (1G), Digital Cellular Networks (2G), Mobile Broadband Data (2.5G-3G), IP Networks (3.5G & 4G)