>>> Android Malware

Name: Rob Brandon
Date: May 8, 2017

>>> Contents

>>> Malware on Phones?!

Android malware has been a problem for several years and is increasingly prevalent. Security firm G Data is currently finding 8400 new Android malware samples per day.[1]

[1] https://blog.gdatasoftware.com/2017/04/29712-8-400-new-android-malware-samples-every-day

>>> Why Android?

Android is currently by far the global market leader for smart phones.

Many phones are never updated from the OS they are running when sold - only 4.9% of Android users are running the current version according to Google statistics

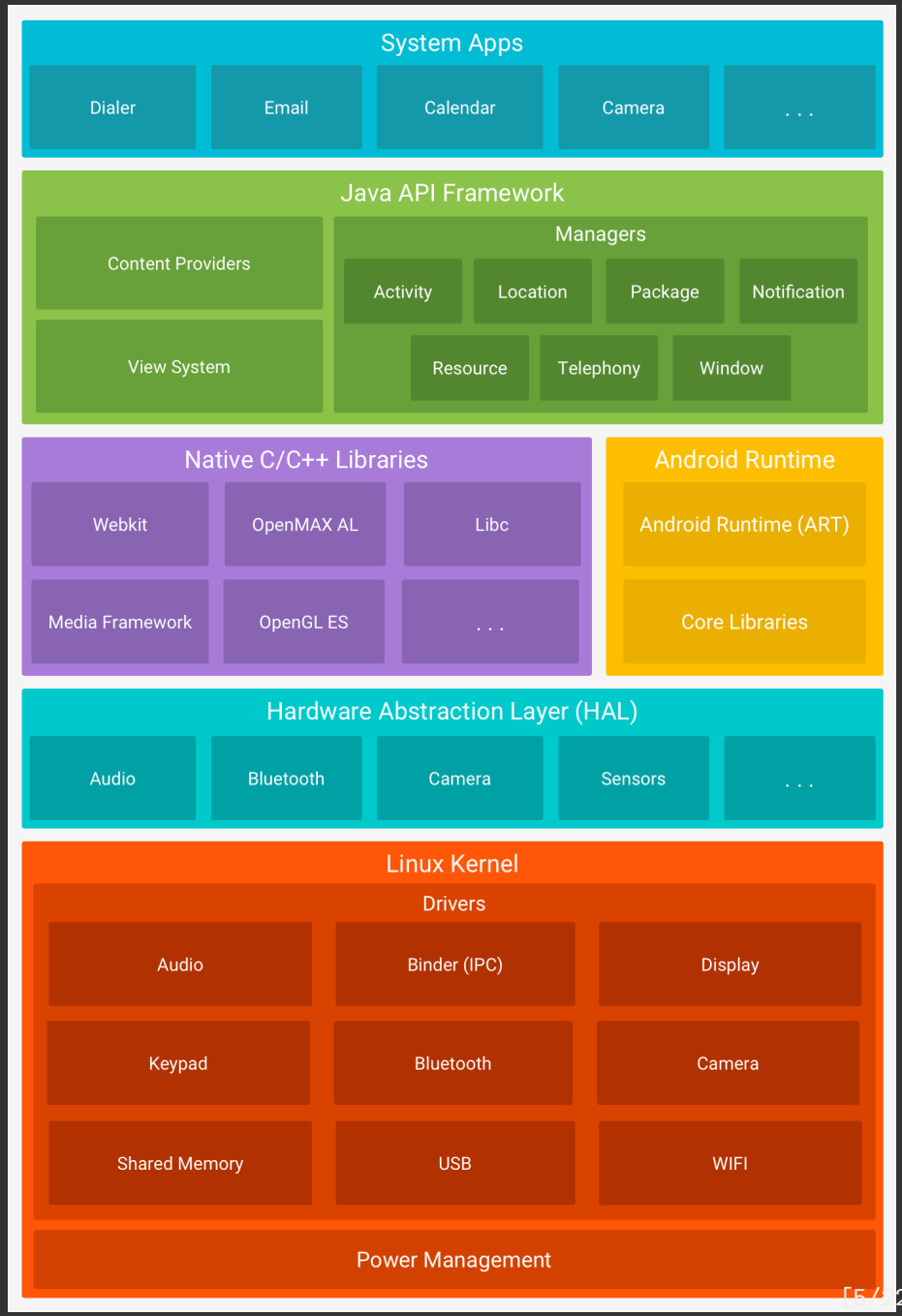
Vetted app stores are not available in all countries

While most malware targets Android today, malware for iOS and other mobile OSes does exist

>>> Android Basics

Android system has more levels of abstraction than desktop operating systems

Malware can target any of these levels



>>> Mobile Malware

Phone malware comes in all the same varieties as PC malware

Mobile also introduces new possibilities for malicious behavior

* GPS tracking
* Accelerometer
* SMS C&C
* and more

>>> Mobile Constraints

Mobile malware has same constraints as other mobile software

* Limited power
* Limited bandwidth
* Limited permissions, without exploits

>>> Infection Vectors

Similar to PC malware, with some important differences

Usually requires side-loading to be enabled on device

* Phishing
* Third party app stores
* Exploit kits

>>> APK Format

APKs are Zip files with a defined structure

All APK files contain the following, at a minimum:

* Hashes of all files in APK
* Signer certificate (Can be self-signed)
* AndroidManifest.xml
* classes.dex

APK will also contain any other files needed by the app, such as icons, HTML, etc

>>> Android Manifest

Contains required permissions for app

Also contains default activity for the app aka. program entry point and intent handlers

>>> Classes.dex

Old Android runtime used the Dalvik VM to run bytecode.

Current Android RunTime (ART) compiles the classes.dex when the app is installed.

>>> Mobile AV

AV software for mobile devices has significant limitations

Unlike PC AV, mobile AV runs in a sandbox with limited privileges - it cannot observe other apps as they run

>>> Decompilers

Can usually decompile Dalvik bytecode

Commercial decompiler: JEB

Free Options: dex2jar with JD-GUI, apktool, jadx, many others

>>> Packing

Proguard bundled with SDK from Google

More sophisticated packers available, such as Dexguard

Dynamic loading/packing often required due to limits of Android file format (primarily 16k method limit in DEX format)

>>> Packing - continued

Code can also be packed at the assembly level.

Towelroot exploit was initially delivered using code obfuscated with O-LLVM to increase the time it would take for outsiders to repurpose the exploit.

Lack of dynamic analysis tools makes this kind of obfuscation tedious to break

>>> Limited Dynamic Analysis Tools

Qemu-based emulator is the most common. Only solution for running ARM

Other emulators are available, none are focused on malware analysis

None allow easy introspection or debugging

>>> Lab Setup Is Challenging

A full lab requires a working, instrumented mock-up of both the cell network and wifi

Requires EM isolation to avoid interfering with other users

>>> Operation Emmental

Used combination of spearphishing to get banking creds along with Android app to intercept 2FA sent by SMS [2]

[2] http://www.bankinfosecurity.com/malware-bypasses-2-factor-authentication-a-7090

>>> Dualtoy

Windows malware that pushes Android malware onto phones connected to the PC [3]

[3] http://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

And the reverse: Android malware that uses USB Autorun to infect Windows machines [4]

[4] https://blog.avast.com/2013/02/08/malware-infects-android-and-windows-at-the-same-time/

>>> Orbot malware

Android malware that uses TOR .onion domains for C&C [5]

[5] https://securelist.com/blog/incidents/58528/the-first-tor-trojan-for-android/

>>> Godless Exploit Kit

Able to infect over 90% of Android phones as of December 2016 [6]

[6] http://blog.trendmicro.com/trendlabs-security-intelligence/godless-mobile-malware-uses-multiple-exploits-root-devices/