Android Internals Training

Table of content:

Introduction - The Android Architecture

- Android features
- Android vs. Linux vs. Embedded Linux
- Filesystem layout and directories
- The Runtime Environment
- The Frameworks
- Dalvik (Java)
- Version differences - 1.5 through L (5.0) to Android S (12.0)
- User-Mode and Kernel-Mode Architecture
- Android Kernel modifications
- Recompiling the Kernel

Android's Hardware Abstraction Layer

- The need for a hardware abstraction layer
- The basic devices
- The User Event Daemon
- HAL stubs
- The last stretch - from HAL to the driver
- Android O HAL modifications ("Project Treble")

Partitions & Filesystems

- UFS vs. eMMC devices
- Device Partition Layout and the GPT
- Android standard partitions
- Vendor Specific Partitions (QCom, Samsung, MTK)
- A tour of the Android filesystems (/system, /vendor, /data)

Booting

- The Boot loader, and FastBoot
- Samsung Odin
- ARM TrustZone (32-bit) and ELx (64-bit)
- Kernel Startup
- User mode init - /init and /init.rc
- Boot-to-root: Rooting techniques by unlocking the bootloader

Native Servicesadbd

- servicemanager
- healthd (K +)
- logd (L +)
- lmkd (L +)
- keystore
- keymaster (M +)
- zygote/app_process

- debuggerd

Android IPC

- IPC and RPC basics
- The servicemanager
- Other communication mechanisms: Sockets and socketpairs

The Input Architecture

- The Linux Kernel Input Model
- The EventHub
- The InputReader
- The InputDispatcher
- The Activity Views

Dalvik

- The Dalvik VM architecture
- The DEX file format
- The DEX OpCode and instruction format
- Optimizing DEX
- Reversing DEX
- Obfuscating DEX
- The JNI model

ART

- The concepts behind ART
- Advantages over Dalvik
- The evolution - from 5.0 to the present day
- Reversing ART
- ART Memory Management
- Return of the (profiled) JIT
- The JNI implementation

Android Kernel tweaks

- ASHmem - Android's Anonymous Shared Memory mechanism
- PMem - Physical contiguous memory for non scatter/gather capable hardware
- Low memory killer - Allowing customized Linux OOM behavior from user space
- Wakelocks - and the enhancements to Power Management
- The RAM Console and pstore - Used in Android to save Panic data across reboot
- Timed GPIO/Output
- Recompiling the kernel
- Kernel level debugging and tracing

Security

- Java level modifiers: Private and Public
- Java level Permissions
- UNIX/native level Permissions
- Digital Signatures (code signing, etc)
- Key storage and encryption

- Service Hooks
- Protected APIs
- Extensions and improvements in Oreo, Pie and 10 (e.g. seccomp-bpf, Webview-Zygote)
- Why it all fails - Android Exploitation