Advanced Malware Analysis Training Series

Introduction to Android

Swapnil Pathak

www.SecurityXploded.com

Disclaimer

The Content, Demonstration, Source Code and Programs presented here is "AS IS" without any warranty or conditions of any kind. Also the views/ideas/knowledge expressed here are solely of the trainer’s only and nothing to do with the company or the organization in which the trainer is currently working.

However in no circumstances neither the Trainer nor SecurityXploded is responsible for any damage or loss caused due to use or misuse of the information presented here.

Acknowledgement

- Special thanks to **Null** community for their extended support and co-operation.
- Special thanks to **ThoughtWorks** for the beautiful venue.
- Thanks to all the trainers who have devoted their precious time and countless hours to make it happen.

Advanced Malware Analysis Training

This presentation is part of our **Advanced Malware Analysis** Training program. Currently it is delivered only during our local meets for FREE of cost.

For complete details of this course, visit our Security Training page.

Who am I?

Swapnil Pathak

- Security Researcher
- Reversing, Malware Analysis, Exploit Analysis etc.
- E-mail: swapnilpathak101@gmail.com

Agenda

- Introduction
- Architecture
- Security Features
- Application Format
- Permissions
- Dalvik bytecode
- Analysis lab setup
- Q & A

Introduction

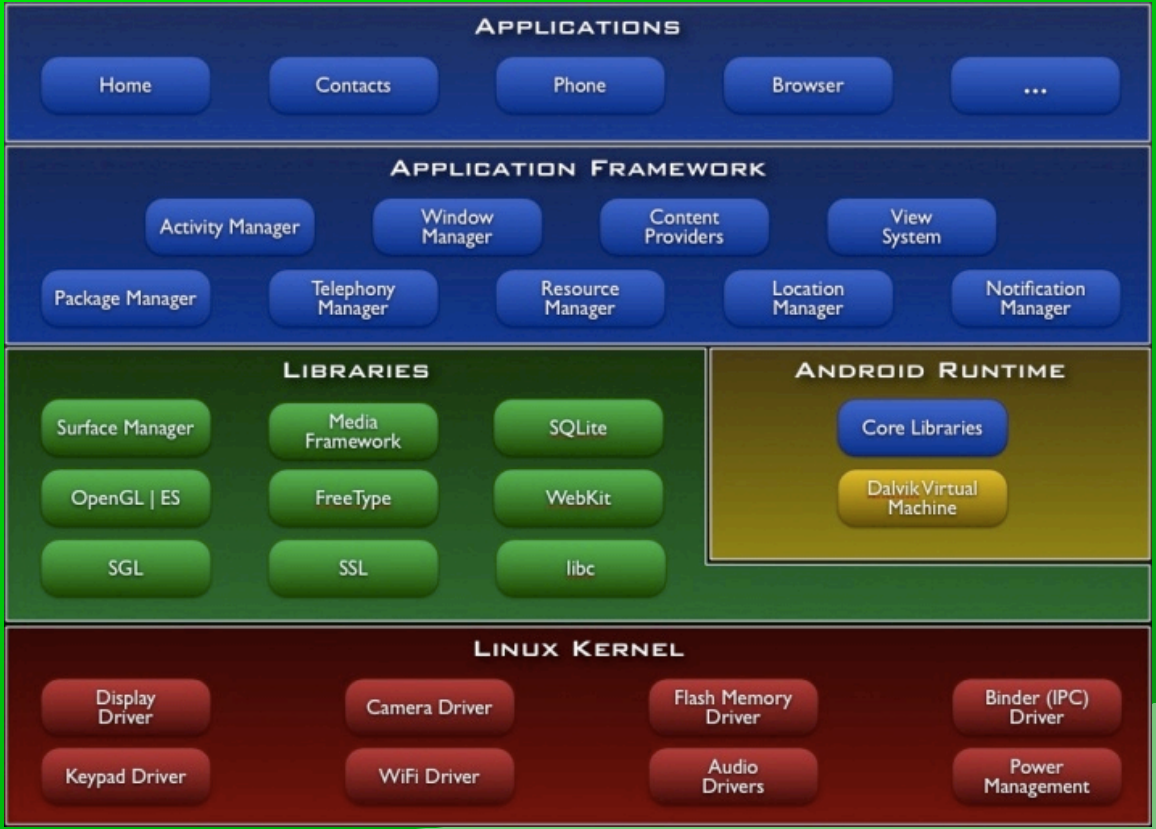
- Linux based OS designed for mobile devices such as smartphones and tablets.
- 500 million devices activated
- 1.3 million activations per day by Q3 of 2012
- 1+ million apps available for download at Google Play Store

Source : Wikipedia

Introduction

- Mobile malware on the rise, Android most at Risk - McAfee
- Android users are prime target for malware – PC World
- New Android malware app turns phone into surveillance device - ThreatPost
- New Android Trojan app exploits previously unknow flaws, researchers say – Computer World

Android Architecture



APPLICATIONS

Home | Contacts | Phone | Browser | ...

APPLICATION FRAMEWORK

Activity Manager | Window Manager | Content Providers | View System

Package Manager | Telephony Manager | Resource Manager | Location Manager | Notification Manager

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 | Flash Memory Driver | Binder (IPC) Driver

Keypad Driver | WiFi Driver | Audio Drivers | Power Management

Security Features

System and Kernel Security

- Application Sandbox

Each application assigned a unique user id (UID) and executed as a separate process

Implemented in kernel, all software above the kernel are run inside the sandbox

Memory Management

- Hardware based NoExecute (NX) to provide code execution on stack and heap

- Address Space Layout Randomization to randomize key locations in memory

Permissions

Application Signing

Application Format

- .apk file extension
- Similar to archive file can be extracted using 7-zip
- Archive contains
  - AndroidManifest.xml
  - Classes.dex (Compiled source code)
  - Res directory
  - Asset directory
  - META-INF directory

Application Format

- Basic elements of Applications
  - AndroidManifest.xml : Specifies the permissions requested by the application
  - Activities : Represents a single screen with user interface
  - Services : Executes in background in its own process or in the context of another applications process.
  - Content Providers : Provides access to private and shared data
  - Broadcast receivers : Code that responds to system wide events
  - Intent – Actions that activate activity, service and broadcast receivers

http://developer.android.com/guide/components/fundamentals.html

Permissions

Permissions updated with each OS release.

CALL_PHONE – Initiate phone call
CAMERA – To access camera on the device
INTERNET – To open network sockets.
INSTALL_PACKAGES – To install packages.
READ_CONTACTS – To read users contact data
READ_LOGS – Low level system log files.
READ_PHONE_STATE , READ_PROFILE
READ_SMS, RECEIVE_SMS,SEND_SMS, WRITE_SMS
WRITE_APN_SETTINGS
RECORD_AUDIO
ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION

Dalvik Virtual Machine and Bytecode

- Applications programmed in java are compiled into java bytecode (.class files)
- dx tool compiles the java bytecode into dalvik bytecode (classes.dex) which is executed on Dalvik virtual machine.
- Dalvik VM, an open source software, responsible for running apps.
- Register based VM, optimized for low memory requirements.
- Consist of virtual registers

Dalvik Virtual Machine and Bytecode

```
.method public add(II)I
.limit registers 4
; this: v1 (Ltest2;)
; parameter[0] : v2 (I)
; parameter[1] : v3 (I)
add-int v0,v2,v3 ; v0=v2+v3
return  v0
.end method
```

Analysis Setup – Tools of the Trade

- Android Emulator
- Smali(assembler)/Baksmali(dissasembler), dedexer
- Apktool
- Dex2Jar
- JD-GUI
- Androguard
- Tcpdump-arm
- Android Reverse Engineering Virtual Machine

Research Projects

- Malgenome Project
- Appanalysis.org
- Sandia MegDroid
- HoneyDroid
- Understanding the Dalvik bytecode with Dedexer tool – Gabor Paller

Reference

Complete Reference Guide for Advanced Malware Analysis Training

[Include links for all the Demos & Tools]

Thank You !

www.SecurityXploded.com