



Android Application Security Assessments

By Michael Born

Overview

- **Platform Terminology**
 - Component Names
 - Component Purpose
 - Activating Components
- **Lab Setup**
 - Physical Device
 - Android Virtual Device
- **Process**
- **Tools**
- **What To Look For**
- **Demo Assessment**

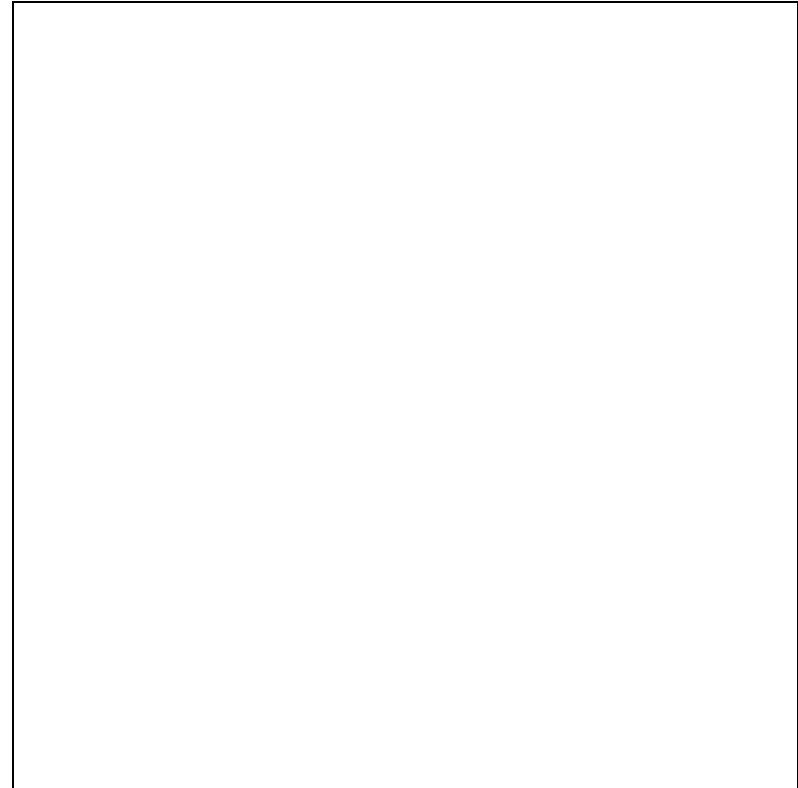
Platform Terminology

- **Components**
 - Activity
 - Content Provider
 - Service
 - Broadcast Receiver



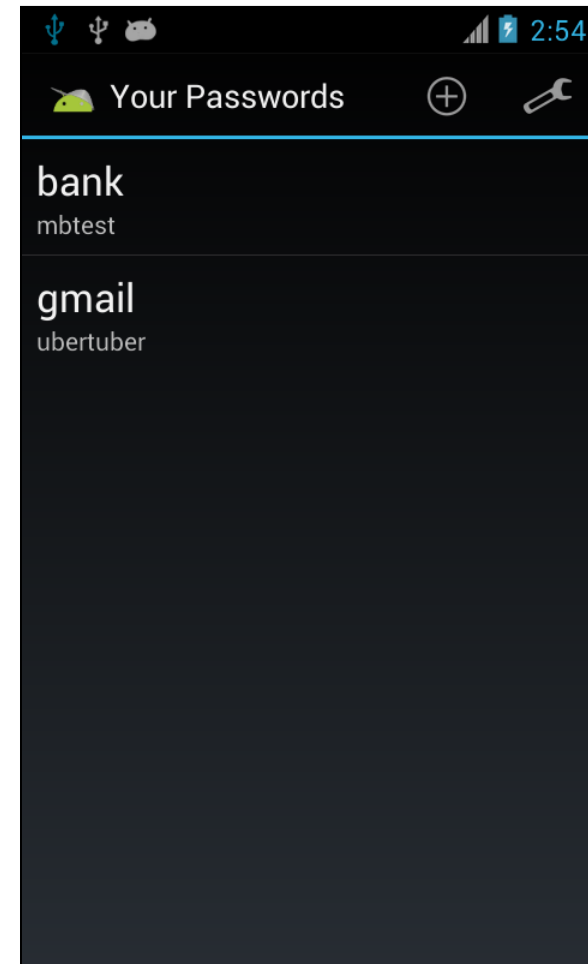
Platform Terminology

- **Activity**
 - Screen Task
- **Content Provider**
 - Structured Data Task
- **Service**
 - Background Task
- **Broadcast Receiver**
 - System Broadcast Responder Task



Platform Terminology

- **Activation**
 - Intent
 - Intent Filters
- **Intent**
 - Explicit
 - FQCN
 - Own App
 - Implicit
 - General Action
 - Another App

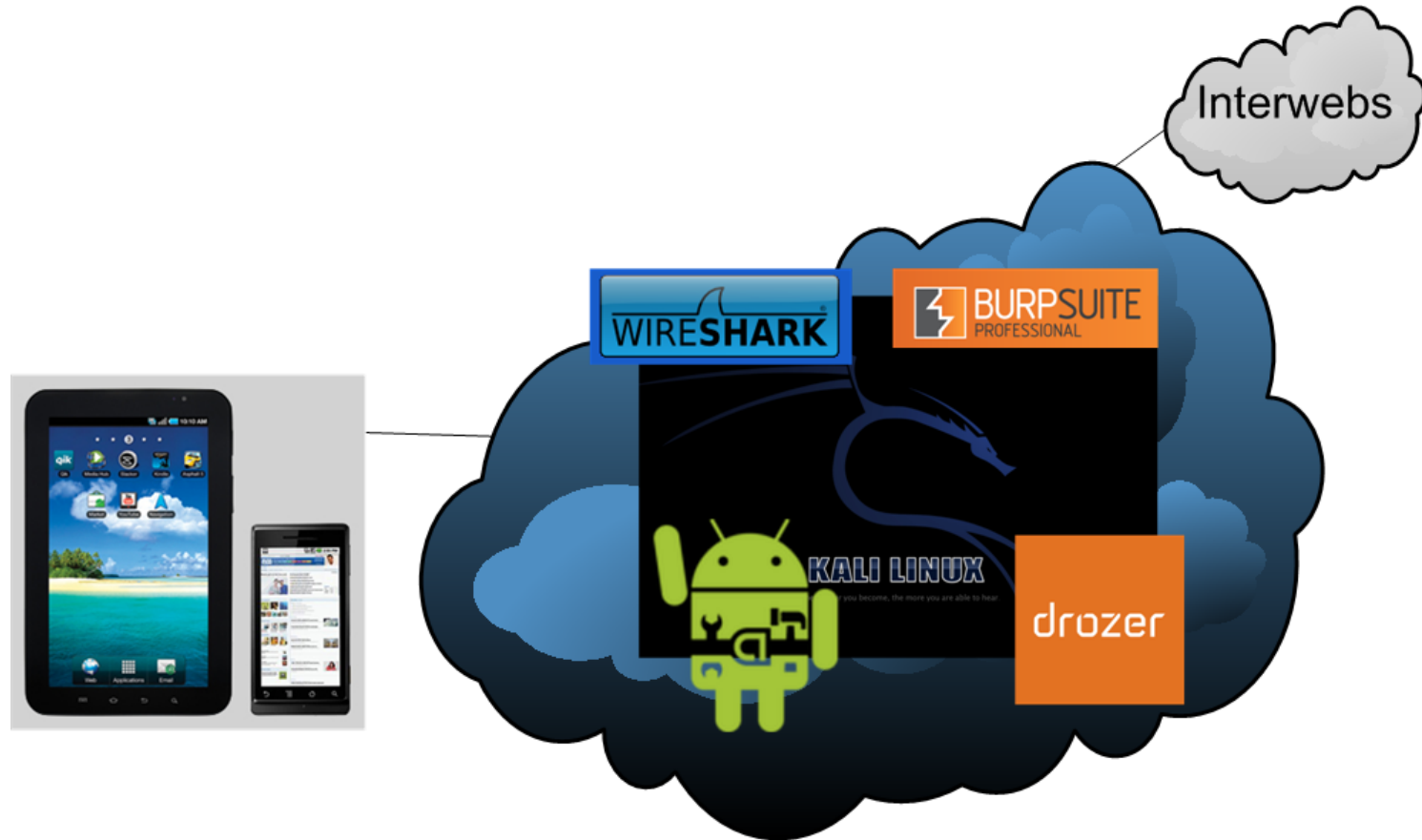


Platform Terminology

- **Intent Filters**
 - Implicit Only
 - Advertises Receivable Intents
 - Action
 - Data
 - Category
 - Per Component
 - Exception: Service

```
<activity android:name="..."  
    <intent-filter>  
        <action android:name="android.intent.action.MAIN" />  
        <category android:name="android.intent.category.LAUNCHER" />  
        <data android:scheme="http" />  
    </intent-filter>  
</activity>
```

Lab Setup – Physical Device



LAB – Physical Device

Lab – Android Virtual Device



LAB – Emulated Device

Assessment Process

- **File System Snapshot**
 - Pre-Installation
 - Post-Installation
 - Post-App Use
- **File System Review**
 - Cache
 - Logs
 - Configuration Files

Assessment Process

- **Application**
 - Authentication
 - Registration
 - Input Injection
 - Encryption
 - Information Storage
- **Web Services**
 - Server Configuration
 - Server Input Validation
 - Cipher Strength

```
ore: 211.0 MB.
lized files (Serialized files now loaded: 0 / Dirty serialized files: 0)
er: 211.8 MB.

is to reduce memory usage. Loaded Objects now: 3536.
lLiveObjects: 0.278970 ms CreateObjectMapping: 0.190384 ms MarkObjects: 3.486686 ms DeleteObj

ffects/heartbeat-01.mp3 - GUID: d20c556dda4e8be47a7ce2453b55a572...
0 ms]
cure/Extras/Military_LoneTrumpeteer_Loop.ogg - GUID: d72ed01aa34dc4a078b58117ac8827f2...
08 ms]
cure/FutureWorld_Resolution_Loop.ogg - GUID: e39f69181b3274f06aa80dbe740aaa13...
08 ms]
rupt.wav - GUID: e74fb1e77757ca14eb3d970a2a279304...
09 ms]
ffects/train-station-hall-1.mp3 - GUID: ea8c8ed24e1b6de469cfff40f4f12264...
0 ms]
rious Again - intro.wav - GUID: f333d5225f83d8f4ca409381ca2bce6e...
0 ms]
cure/FutureWorld_NewsReel_Loop.ogg - GUID: fc55e85438fe44522b95eb893c55a09f...
06 ms]
rious Again - Repeating.wav - GUID: ff922bf6447ff2547a8c20a02093ccd4...
01 ms]
ore: 211.6 MB.
lized files (Serialized files now loaded: 0 / Dirty serialized files: 0)
er: 211.8 MB.

is to reduce memory usage. Loaded Objects now: 3536.
lLiveObjects: 0.367556 ms CreateObjectMapping: 0.191886 ms MarkObjects: 3.595692 ms DeleteObj

time: 2945.366211s, Asset Import: 2941.584473s, CacheServerIntegrate: 0.000000s, CacheServer I

try/ScriptAssemblies/Assembly-CSharp-firstpass.dll, for buildtarget 13
try/ScriptAssemblies/Assembly-UnityScript-firstpass.dll, for buildtarget 13

tchBuildTargetEmulation.AndroidPlayer' in 2947 seconds

th: 'D:/Program Files (x86)/Unity422/Editor/Data/MonoEmbedRuntime;;D:\Development\Github\Uni
Windows;C:\Windows\system32;SRV*C:\websymbols*http://msdl.microsoft.com/download/symbols;', s
0x100-0x1
nity422\Editor\Unity.exe:Unity.exe (00400000), size: 27103232 (result: 0), SymType: 'PDB', PD
l.dll:ntdll.dll (77700000), size: 1404928 (result: 0), SymType: '-exported-', PDB: 'C:\Window
IEL32.DLL:KERNEL32.DLL (75FD0000), size: 1245184 (result: 0), SymType: '-exported-', PDB: 'C:\V
IELBASE.dll:KERNELBASE.dll (76680000), size: 679936 (result: 0), SymType: '-exported-', PDB: 'C
nity422\Editor\beast32.dll:beast32.dll (10000000), size: 1839104 (result: 0), SymType: '-expor
```

Assessment Process

- **Component Tests**

- Exported Activities

- Permissions
 - Intent Filters

- Content Providers

- Permissions
 - Injection
 - Data Retrieval
 - URI Discovery

- Exported Services

- Permissions



```
C:\Windows\system32\cmd.exe - drozer.cmd
Selecting 1d63599fe8e1da19 (unknown sdk 4.3)

..o.. ..r..
..a.. ..nd
ro..idsnemesisisand..pr
..otectorandroidsneme.
..,sisandprotectorandroids+.
..nemesisisandprotectorandroidsn:.
..emesisisandprotectorandroidsnemes..
..isisandp,..,rotectorandro,..,idsnem.
..isisandp..rotectorandroid..snemesis.
..andprotectorandroidsnemesisandprotec.
..torandroidsnemesisandprotectorandroid.
..snemesisandprotectorandroidsnemesisan:
..dprotectorandroidsnemesisandprotector.

drozer Console (v2.3.2)
dz> run app.package.list -f settings
com.android.settings (Settings)
com.android.development_settings (Development Setting
com.android.providers.settings (Settings Storage)
dz>
```

Assessment Tools

- **Linux Commands**
 - tree
 - strings
 - diff
- **Intercepting Proxy**
 - Burp Suite Pro
 - Web Scarab
 - OWASP Zap

```
root@kali:/run# nmap 192.168.1.167

Starting Nmap 6.25 ( http://nmap.org ) at 1970-0
root@kali:/run# nmap --top-ports 10 192.168.1.1

Starting Nmap 6.25 ( http://nmap.org ) at 1970-0
Nmap scan report for ██████████ (192.16
Host is up (0.00076s latency).
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3
139/tcp   closed netbios-ssn
443/tcp   closed https
445/tcp   closed microsoft-ds
3389/tcp  closed ms-wbt-server
MAC Address: ██████████ (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1
root@kali:/run# █
```

Assessment Tools

- **Kali Tools**
 - Dex2Jar
 - Nmap
 - Wireshark
 - Metasploit
 - JD Gui
- **Drozer**
- **Drozer Agent**
- **Android SDK**



What To Look For

- **OWASP Top 10**
- **Components**
 - Exported Permissions
 - Input Injection
 - Data Retrieval
 - Authentication Bypass
- **Encryption**
 - Present
 - Cipher Strength
 - SSL/TLS Version
- **Sensitive Data**
 - Cache
 - Logs
 - Manifest
- **Application**
 - Input
 - Authentication
 - Password Strength
 - Certificate Pinning

What To Look For

- **Web Services**
 - Server Misconfiguration
 - Server Side Validation
 - Enumeration
 - Payment Type
 - Payment Info
 - Usernames
 - Other Sensitive Information



Further Reading

- **Android Developer Guides**
 - <http://developer.android.com>
- **Drozer User Manual**
 - <https://www.mwrinfosecurity.com/products/drozer>
- **Vulnerable Android App Sieve**
 - <https://www.mwrinfosecurity.com/products/drozer>
- **OWASP Mobile Top 10**
 - https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

Android Demo

DEMO



Thank You!