Android Application Security Assessments

By Michael Born

Overview

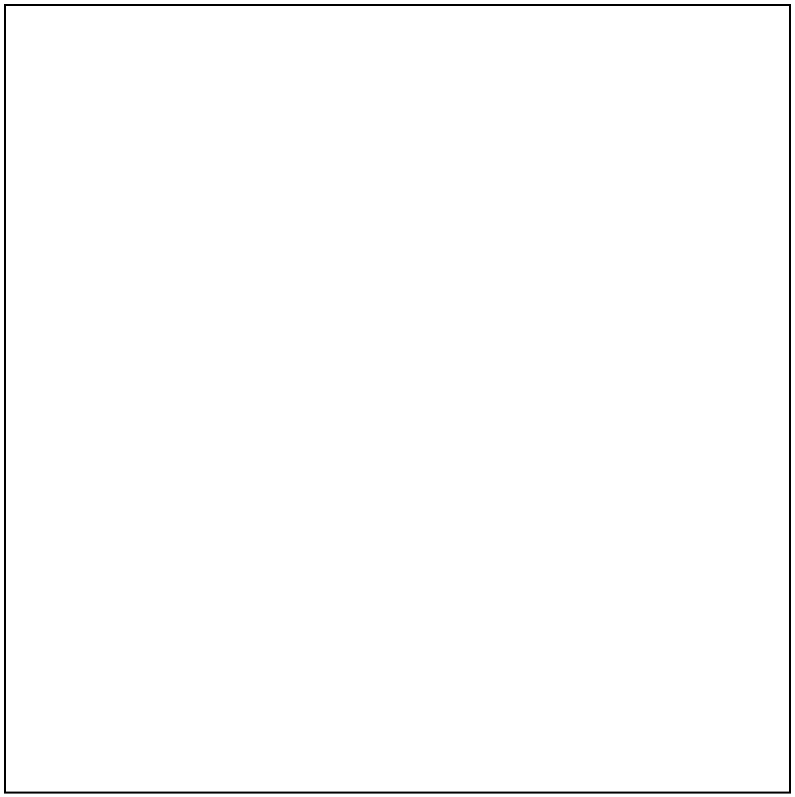
- **Platform Terminology**
  - Component Names
  - Component Purpose
  - Activating Components
- **Lab Setup**
  - Physical Device
  - Android Virtual Device
- **Process**
- **Tools**
- **What To Look For**
- **Demo Assessment**

Platform Terminology

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

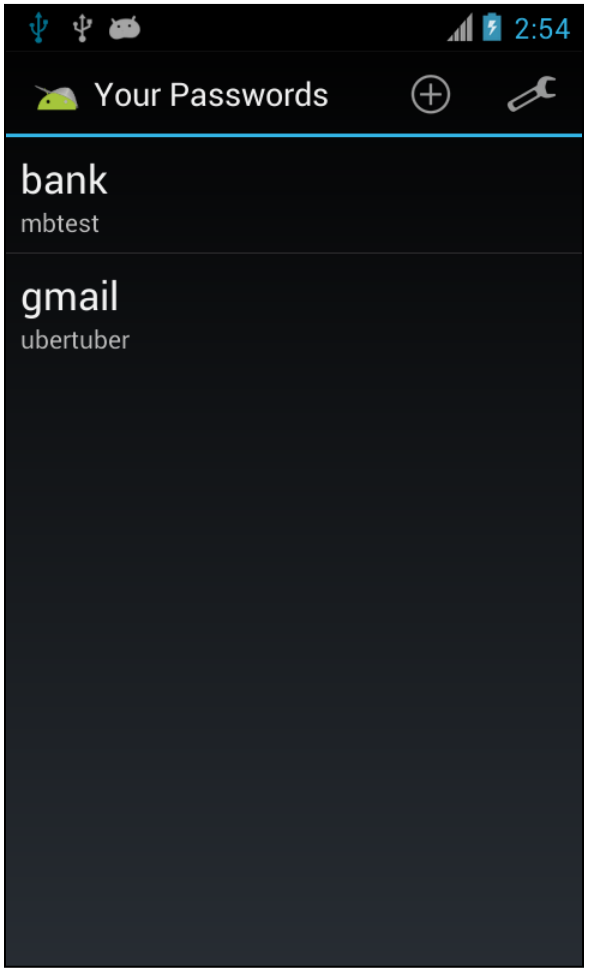
Platform Terminology

- **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

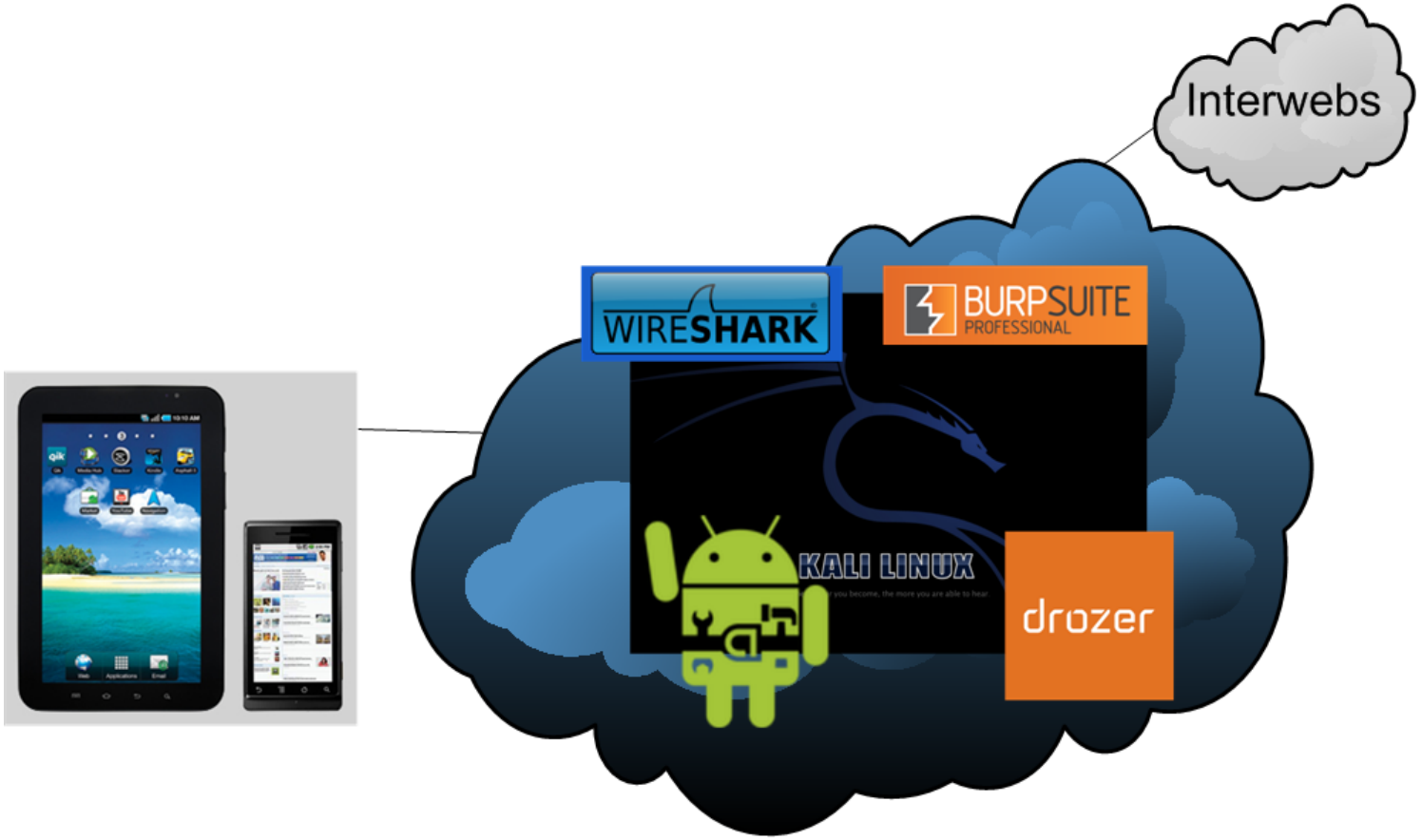


Platform Terminology

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

```
<activity android:name=
    <intent-filter>
        <action androi
        <category andr
        <data android:r
    </intent-filter>
</activity>
```

Lab Setup – Physical Device



LAB – Physical Device

SOLUTIONARY

Lab – Android Virtual Device

LAB – Emulated Device

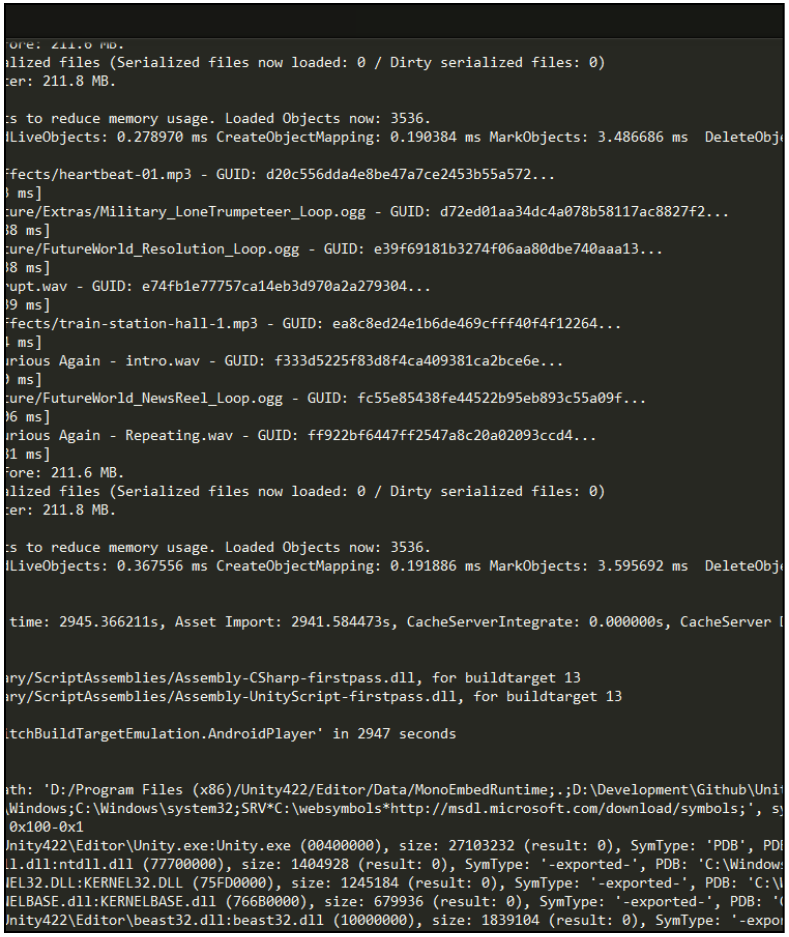
SOLUTIONARY

Assessment Process

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

Assessment Process

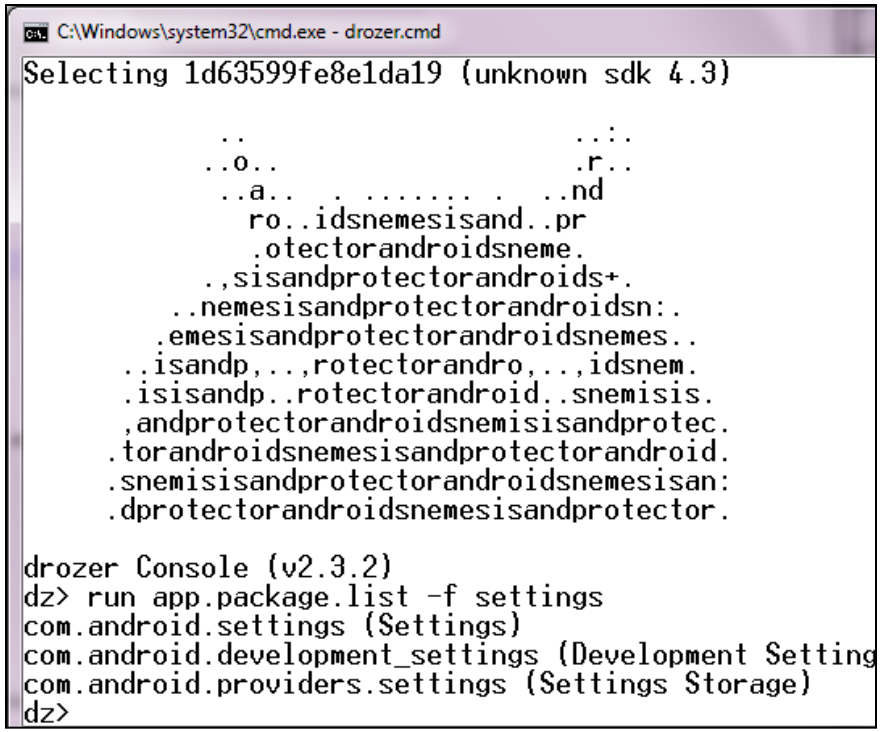
- **Application**
  - Authentication
  - Registration
  - Input Injection
  - Encryption
  - Information Storage
- **Web Services**
  - Server Configuration
  - Server Input Validation
  - Cipher Strength



SOLUTIONARY

Assessment Process

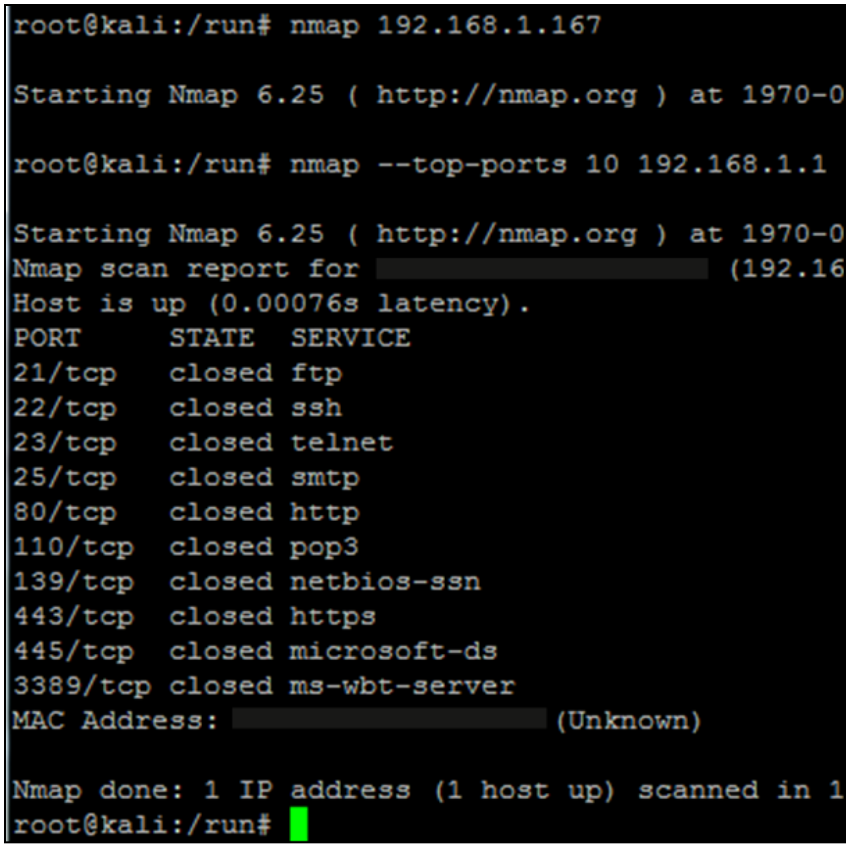
- **Component Tests**
  - Exported Activities
    - Permissions
    - Intent Filters
  - Content Providers
    - Permissions
    - Injection
    - Data Retrieval
    - URI Discovery
  - Exported Services
    - Permissions



SOLUTIONARY

Assessment Tools

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



SOLUTIONARY

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!

 ActiveGuard® U.S. Patent Nos 6,988,208; 7,168,093; 7,370,359; 7,424,743; 7,673,049: 7,954,159; 8,261,347 March 18, 2014