WORKSHOP
PENETRATION TESTING ANDROID APPS

Sahil Dhar

xen1thLabs

SMART AND SAFE DIGITAL

Whoami

Sahil Dhar

Security researcher

My area of expertise include Web and Mobile application security. Prior to joining Xen1thLabs, I have worked on numerous projects involving the security assessment of Web, Mobile, Thick clients and Network and Cloud Infrastructure for multiple fortune 500 companies.

@0x401

A former

- Security Engineer
- Security Consultant
- Bug Bounty Hunter

Currently

- Security researcher
- @Xen1th Labs

Content

01
Introduction

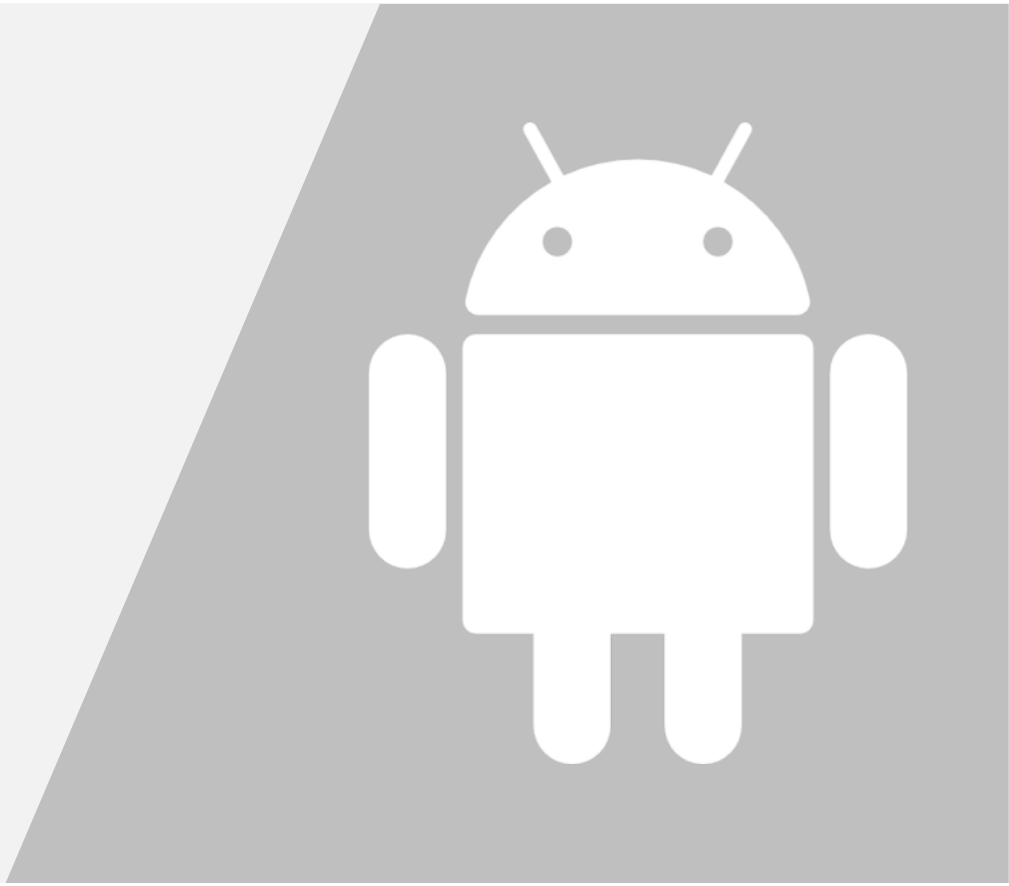
Why Android

Mobile Operating System developed by Android Inc. bought by Google in 2005.

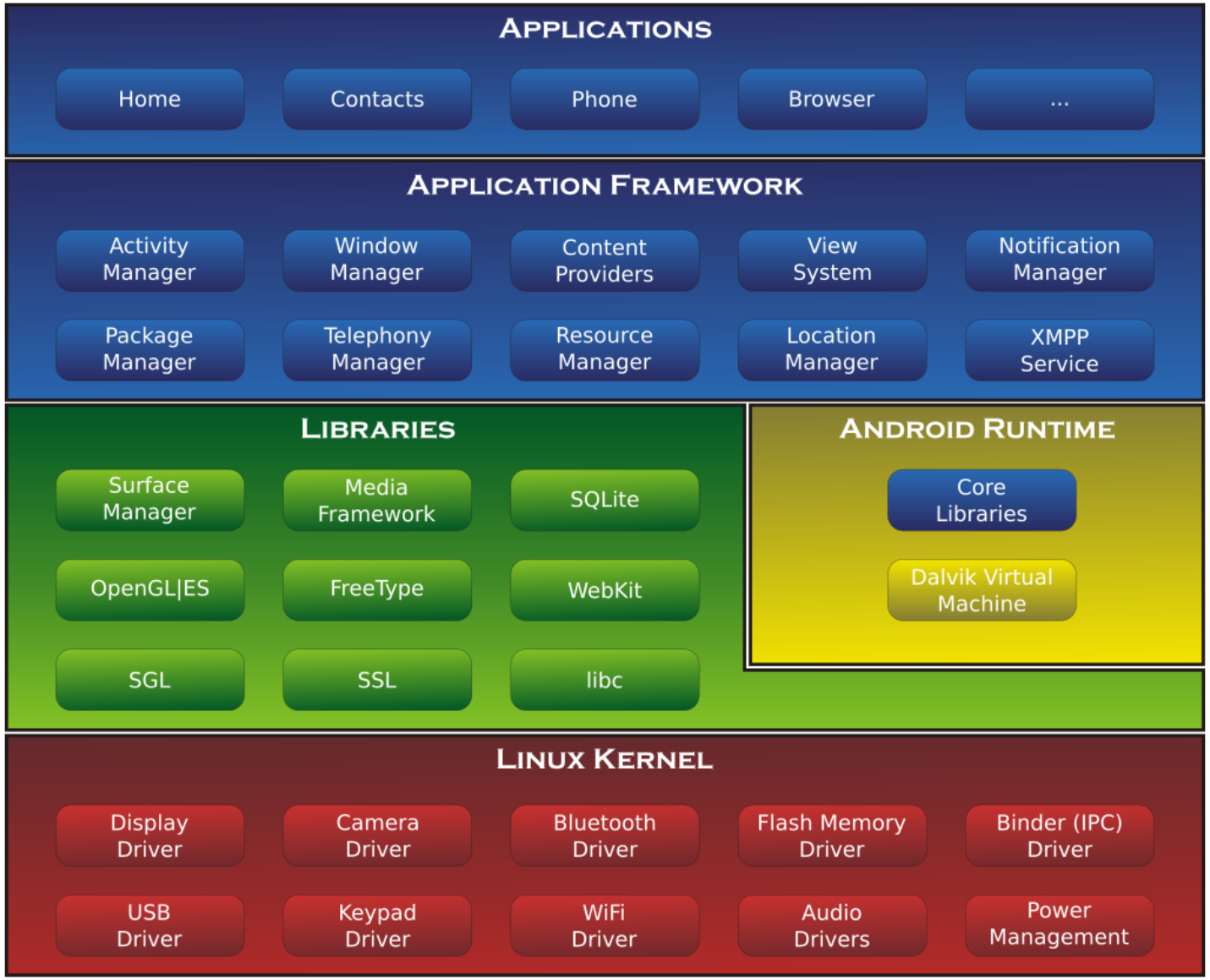
Holds 76.23 % of operating System market share worldwide.

Some of the key security features:

App Sandbox	App Signing	App Permissions
Secure Storage	Biometric Authentication	
Keystore	TEE	SE-Linux



Android System Architecture



Types of Android Apps

Android App Sandbox

- This simply means that the app A cannot directly access the data or resources of app B.
- Uses User unique ID (UID) to setup kernel-level application sandbox.
- As the segregation is implemented at kernel level, both the code running natively in the app and interpreted code abides by this.

```
vbox86p:/ # ps -A|grep -i messa
u0_a64        1404   331 1180564 111276 ep_poll      f2072ba9 S com.android.messaging
vbox86p:/ # ps -A|grep -i email
u0_a47        1360   331 1175420 108972 ep_poll      f2072ba9 S com.android.email
vbox86p:/ # ls -l /data/data/com.android.messaging/
total 16
drwxrws--x 2 u0_a64 u0_a64_cache 4096 2019-07-26 05:10 cache
drwxrws--x 2 u0_a64 u0_a64_cache 4096 2019-07-26 05:10 code_cache
drwxrwx--x 2 u0_a64 u0_a64       4096 2019-07-26 05:10 databases
drwxrwx--x 2 u0_a64 u0_a64       4096 2019-09-29 12:29 shared_prefs
vbox86p:/ # ls -l /data/data/com.android.email/
total 20
drwxrws--x 2 u0_a47 u0_a47_cache 4096 2019-07-26 05:10 cache
drwxrws--x 2 u0_a47 u0_a47_cache 4096 2019-07-26 05:10 code_cache
drwxrwx--x 2 u0_a47 u0_a47       4096 2019-09-29 12:27 databases
drwxrwx--x 2 u0_a47 u0_a47       4096 2019-07-26 05:10 files
drwxrwx--x 2 u0_a47 u0_a47       4096 2019-07-26 05:10 shared_prefs
```

Important File System Locations

PATH	DESCRIPTION
/data/data/<app_name>	Application specific data (accessible with root access only)
/data/app/<app_name>	Application binaries, libraries and framework files (accessible with non-rooted device as well)
/data/local/tmp	Similar to /tmp in unix file systems (only write access in non-rooted devices)
/system/app	System applications (accessible in non-rooted devices as well)
/data/system_ce/0/recent_images	Contains the snapshot of applications in background state.

Important File System Locations

PATH	DESCRIPTION
/data/data/<app_name>/shared_prefs	Application specific configuration, credentials etc.
/data/data/<app_name>/files	Can have any app specific files (depends on dev)
/data/data/<app_name>/databases	SQLite databases (app specific and third party as well)
/data/data/<app_name>/cache	WebView cache files
/data/misc/keystore/user_0	Any data stored by the application in android KeyStore

02
Lab Setup

Walk-through
ANDROID-STUDIO

Mobile Pentest Tools - Configuration

Copy the android-tools folder from the pendrive/<**network share**> to your **$HOME** directory.

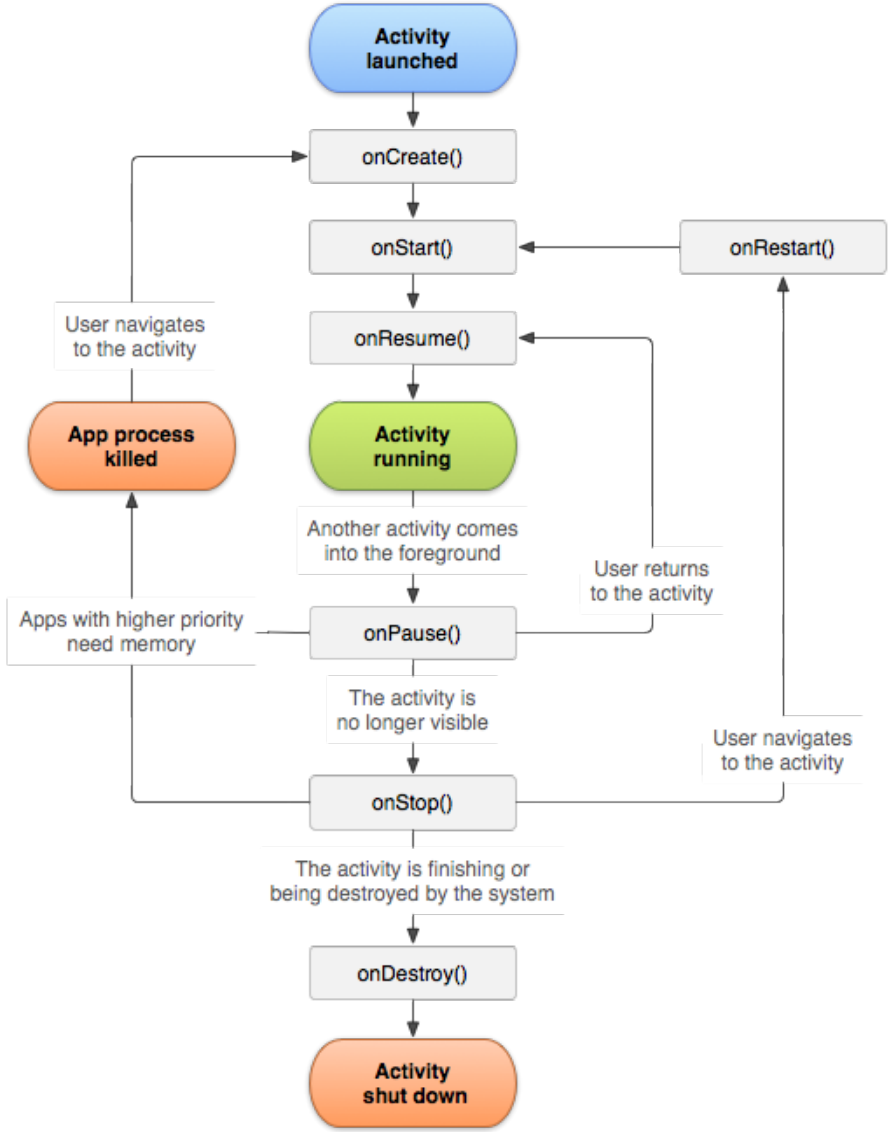
Open the terminal and navigate to the **$HOME/android-tools** folder.

Execute **". setenv.sh"** file.

03

Hello World – Android

Android Activity Life Cycle



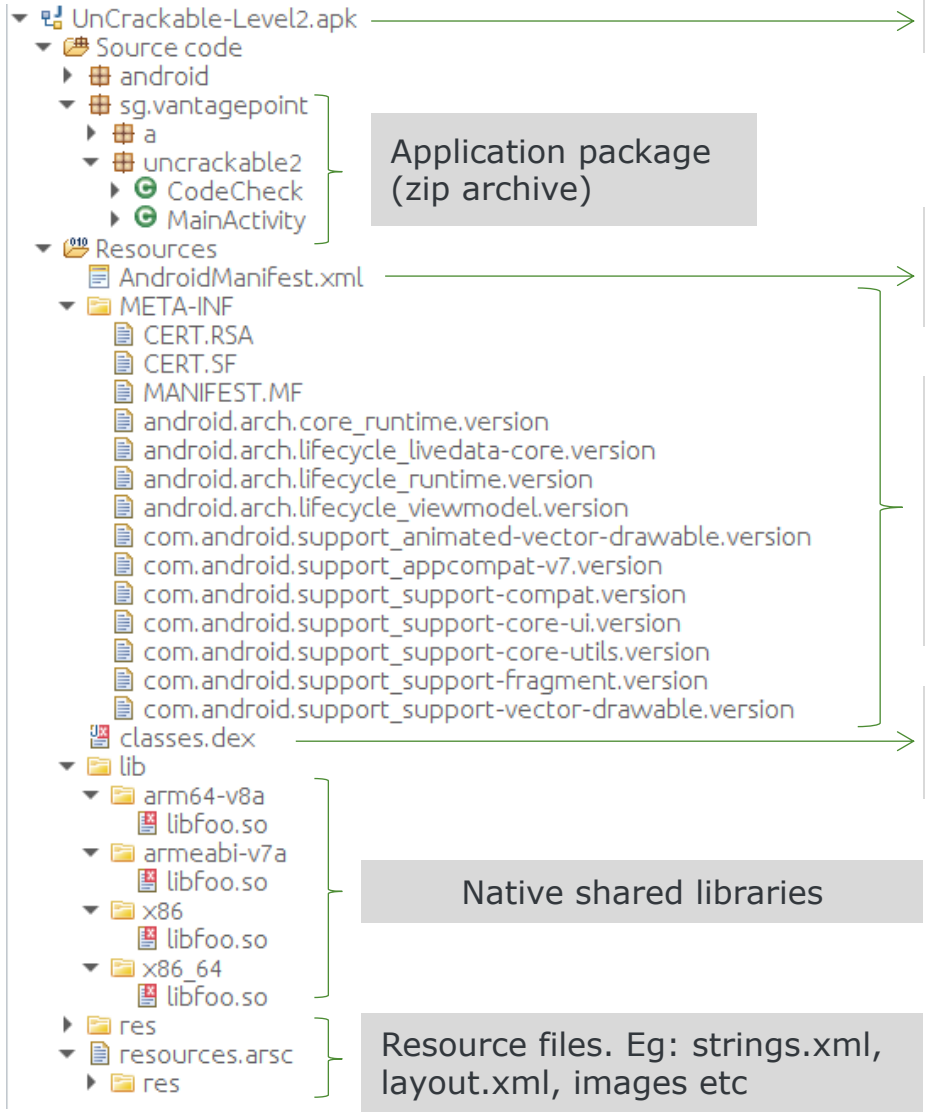
WALK-THROUGH

04
APK Structure

Understanding APK Structure

DESCRIPTION	COMMAND
Unpacking APK as zip file	unzip –e uncrackable-level2.apk –d unzipped_apk
Decompiling APK using apktool	apktool d uncrackable-level2.apk –o decompiled_apktool
Decompiling APK with jadx-gui	./jadx-gui uncrackable-level2.apk

Android APK Structure



Application package (zip archive)

Application package (zip archive)

Compiled XML file, contains entry point, permissions of application components

- MANIFEST.MF: contains sha1 hashes of application files.
- CERT.RSA: Developer's public signature
- CERT.SF: contains sha1 hashes of lines in MANIFEST.MF files and lines.

Compiled classes executed by Android (DVM/ART) runtime as odex or oat.

Native shared libraries

Resource files. Eg: strings.xml, layout.xml, images etc

Understanding APK Structure

DESCRIPTION	COMMAND
Unpacking APK as zip file	unzip –e **??** –d **??**
Decompiling APK using apktool	apktool d **??** –o **??**
Decompiling APK with jadx-gui	./jadx-gui **??**

05

Understanding Android App Components

Android App Components

ACTIVITIES

- A graphical user interface provided by the app that a user can interact with and perform relevant operations. Example: Dialing the number on a phone app.
- Any android app will often have more than activities which will get triggered based on events generated by the user or system.

SERVICES

- App services runs in background and does not have any GUI.
- An app can start or stop services based on the events generated by the user or system.

CONTENT PROVIDERS

- Content Providers provides a way to store and share app data locally and with other applications installed on the device.

BROADCAST RECEIVERS

- Uses publish-subscribe design pattern to send or receive messages to and from the android system or other apps installed on the device.

06

Exploiting Android Components

Understanding Android App Manifest

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="jakhar.aseem.diva" platformBuildVersionCode=
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="26"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBackup="true" an
        <activity android:theme="@style/AppTheme_NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
        <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
        <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
        <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
        <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
        <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
        <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
        <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
        <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
        <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d10" android:name="jakhar.aseem.diva.AccessControl2Activity"/>
        <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APICreds2Activity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <provider android:name="jakhar.aseem.diva.NotesProvider" android:enabled="true" android:exported="true" android:authorities="jakhar.aseem.diva.provider.notesprovide
        <activity android:label="@string/d11" android:name="jakhar.aseem.diva.AccessControl3Activity"/>
        <activity android:label="@string/d12" android:name="jakhar.aseem.diva.Hardcode2Activity"/>
        <activity android:label="@string/pnotes" android:name="jakhar.aseem.diva.AccessControl3NotesActivity"/>
        <activity android:label="@string/d13" android:name="jakhar.aseem.diva.InputValidation3Activity"/>
    </application>
</manifest>
```

Understanding AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="jakhar.aseem.diva" platformBuildVersionCode=
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="26"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBackup="true" an
        <activity android:theme="@style/AppTheme_NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
        <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
        <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
        <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
        <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
        <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
        <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
        <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
        <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
        <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d10" android:name="jakhar.aseem.diva.AccessControl2Activity"/>
        <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APICreds2Activity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <provider android:name="jakhar.aseem.diva.NotesProvider" android:enabled="true" android:exported="true" android:authorities="jakhar.aseem.diva.provider.notesprovide
        <activity android:label="@string/d11" android:name="jakhar.aseem.diva.AccessControl3Activity"/>
        <activity android:label="@string/d12" android:name="jakhar.aseem.diva.Hardcode2Activity"/>
        <activity android:label="@string/pnotes" android:name="jakhar.aseem.diva.AccessControl3NotesActivity"/>
        <activity android:label="@string/d13" android:name="jakhar.aseem.diva.InputValidation3Activity"/>
    </application>
</manifest>
```

Understanding AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="jakhar.aseem.diva" platformBuildVersionCode=
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="26"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBackup="true" an
        <activity android:theme="@style/AppTheme_NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
        <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
        <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
        <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
        <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
        <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
        <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
        <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
        <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
        <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d10" android:name="jakhar.aseem.diva.AccessControl2Activity"/>
        <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APICreds2Activity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <provider android:name="jakhar.aseem.diva.NotesProvider" android:enabled="true" android:exported="true" android:authorities="jakhar.aseem.diva.provider.notesprovide
        <activity android:label="@string/d11" android:name="jakhar.aseem.diva.AccessControl3Activity"/>
        <activity android:label="@string/d12" android:name="jakhar.aseem.diva.Hardcode2Activity"/>
        <activity android:label="@string/pnotes" android:name="jakhar.aseem.diva.AccessControl3NotesActivity"/>
        <activity android:label="@string/d13" android:name="jakhar.aseem.diva.InputValidation3Activity"/>
    </application>
</manifest>
```

Understanding AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="jakhar.aseem.diva" platformBuildVersionCode=
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="26"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBackup="true" an
        <activity android:theme="@style/AppTheme_NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
        <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
        <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
        <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
        <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
        <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
        <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
        <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
        <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
        <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d10" android:name="jakhar.aseem.diva.AccessControl2Activity"/>
        <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APICreds2Activity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <provider android:name="jakhar.aseem.diva.NotesProvider" android:enabled="true" android:exported="true" android:authorities="jakhar.aseem.diva.provider.notesprovide
        <activity android:label="@string/d11" android:name="jakhar.aseem.diva.AccessControl3Activity"/>
        <activity android:label="@string/d12" android:name="jakhar.aseem.diva.Hardcode2Activity"/>
        <activity android:label="@string/pnotes" android:name="jakhar.aseem.diva.AccessControl3NotesActivity"/>
        <activity android:label="@string/d13" android:name="jakhar.aseem.diva.InputValidation3Activity"/>
    </application>
</manifest>
```

ADB Primer

DESCRIPTION	COMMAND
List connected devices/emulators	adb devices
Install android apk on the device	adb install diva.apk
Get list of installed apps on the device	adb shell pm list package
Get path of installed applications on the device	adb shell pm path info <package_name>
Copy files from device to your local machine	adb pull /device/local/path /machine/local/path
Copy files from local to device	adb push /machine/local/path /device/local/path
Port Forwarding	adb forward tcp:31415 tcp:31415
View device and app debug logs	adb logcat

Getting Started – Drozer

Follow setup instructions from Notes/drozer_installation.md file

Exploiting Exported Activities

DESCRIPTION	COMMAND
Open the apk with jadx-gui	jadx-gui diva.apk
[**Drozer**] Enumerate app attack surface	run app.package.attacksurface jakhar.aseem.diva
[**Drozer**] Start the vulnerable activity	run app.activity.start --action <action> --category <category> –component <package_name> <component_name>
[**Drozer**] Exploiting APICredsActivity from Diva	run app.activity.start --component jakhar.aseem.diva jakhar.aseem.diva.APICredsActivity

Exploiting Content Providers

DESCRIPTION	COMMAND
Open the apk with jadx-gui	jadx-gui diva.apk
[**Drozer**] Enumerating Content Provider URIs	run app.provider.finduri jakhar.aseem.diva
[**Drozer**] Extracting data from vulnerable content providers Content Provider URI	run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes
[**Drozer**] Get Specific data using projection and selection args	• run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes --selection "_id=5" • run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes --projection "note"

Exercise: Exploiting Vulnerable Broadcast Receivers

DESCRIPTION	COMMAND
Open the apk with jadx-gui	jadx-gui exploitBroadcast.apk
[**Drozer**] Enumerate exported broadcast receivers	run app.broadcast.info -a com.example.broadcastreceiver
[**Drozer**] Interacting with exported broadcast receivers	run app.broadcast.send --action com.sendBroadcast.Action --extra string com.sendBroadCast.extra_msg " hello"

Exercise: Exploiting Vulnerable Services

DESCRIPTION	COMMAND
Open the apk with jadx-gui	jadx-gui service_example.apk
[**Drozer**] Enumerating exported services	run app.package.attacksurface com.example.serviceexample
[**Drozer**] Stopping a service	run app.service.stop --component com.example.serviceexample .MyService
[**Drozer**] Starting a service	run app.service.start --component com.example.serviceexample .MyService

07

Client-side App Defense Mechanisms

Common App Defense Mechanisms

Root Detection Bypass – Manual Patching

DESCRIPTION	COMMAND
Decompile the app with apktool	apktool d ./UnCrackable-Level1
Recompile the app with apktool	apktool b UnCrackable-Level1
Sign the application	sign UnCrackable-Level1.apk
Zipalign the application	zipalign –v 4 UnCrackable-Level1.s.apk UnCrackable-Level1.aligned.apk
Install the patched app on the device	adb install UnCrackable-Level1.aligned.apk

Getting Started – Frida

Follow setup instructions from Notes/frida_installation.md file

Frida Internals

Hijack remote thread - **ptrace()**

Allocating memory for Bootstrapper:
frida_resolve_library_function - mmap()

Load libpthread.so - **dlopen()**

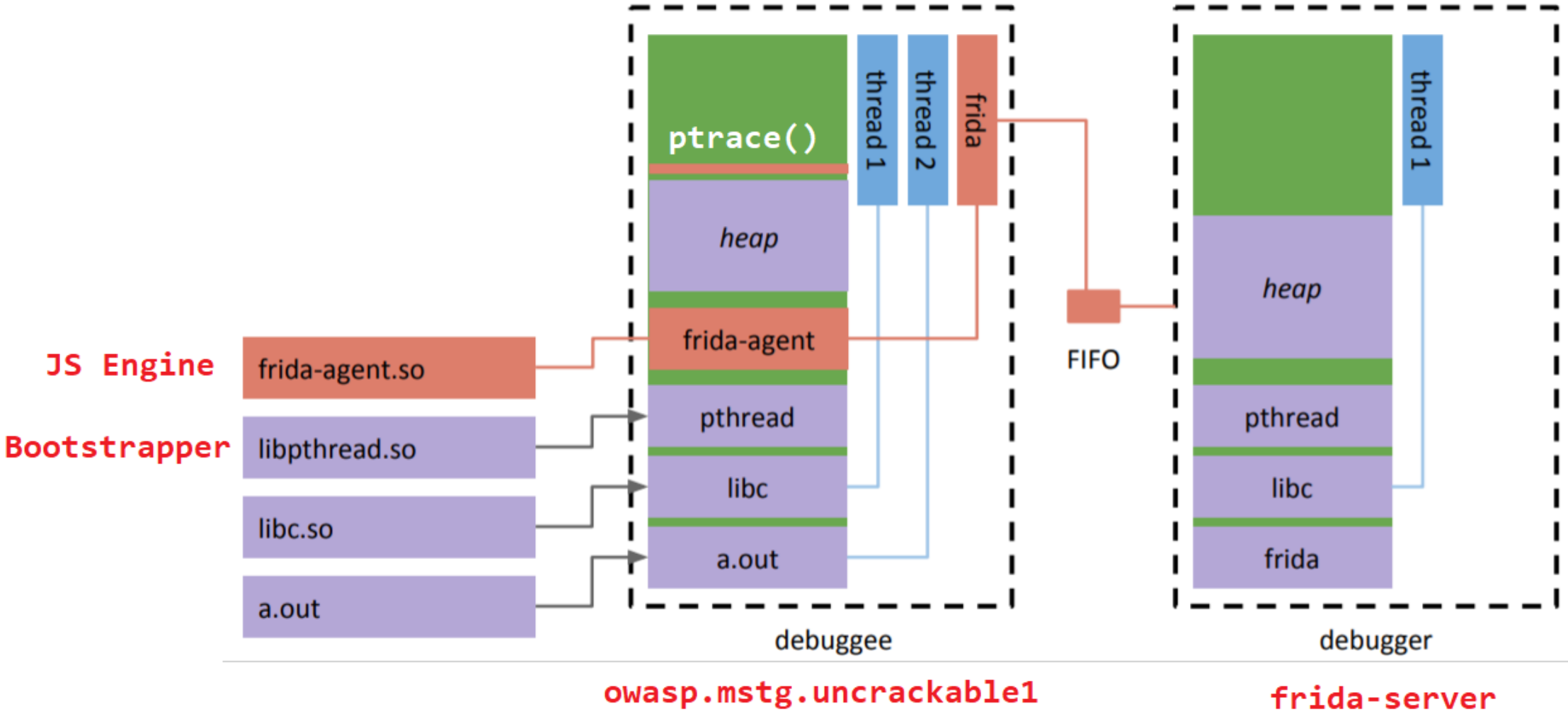
Create new thread - **thread_create()** - executing libpthread.so

Notify debugger
- Load frida-agent.so **dlopen()** in process memory
- Locate entry point of frida-agent

Resume hijacked thread execution
- Execute entry point of frida-agent

Resume execution

Frida Internals



Source: https://www.frida.re/docs/presentations/osdc-2015-the-engineering-behind-the-reverse-engineering.pdf

Automated Root Detection Bypass – Frida

```
Java.performNow(function(){

  var _system = Java.use("java.lang.System");
  _system.exit.implementation = function(){
    console.log("Exit called");
  }

});
```

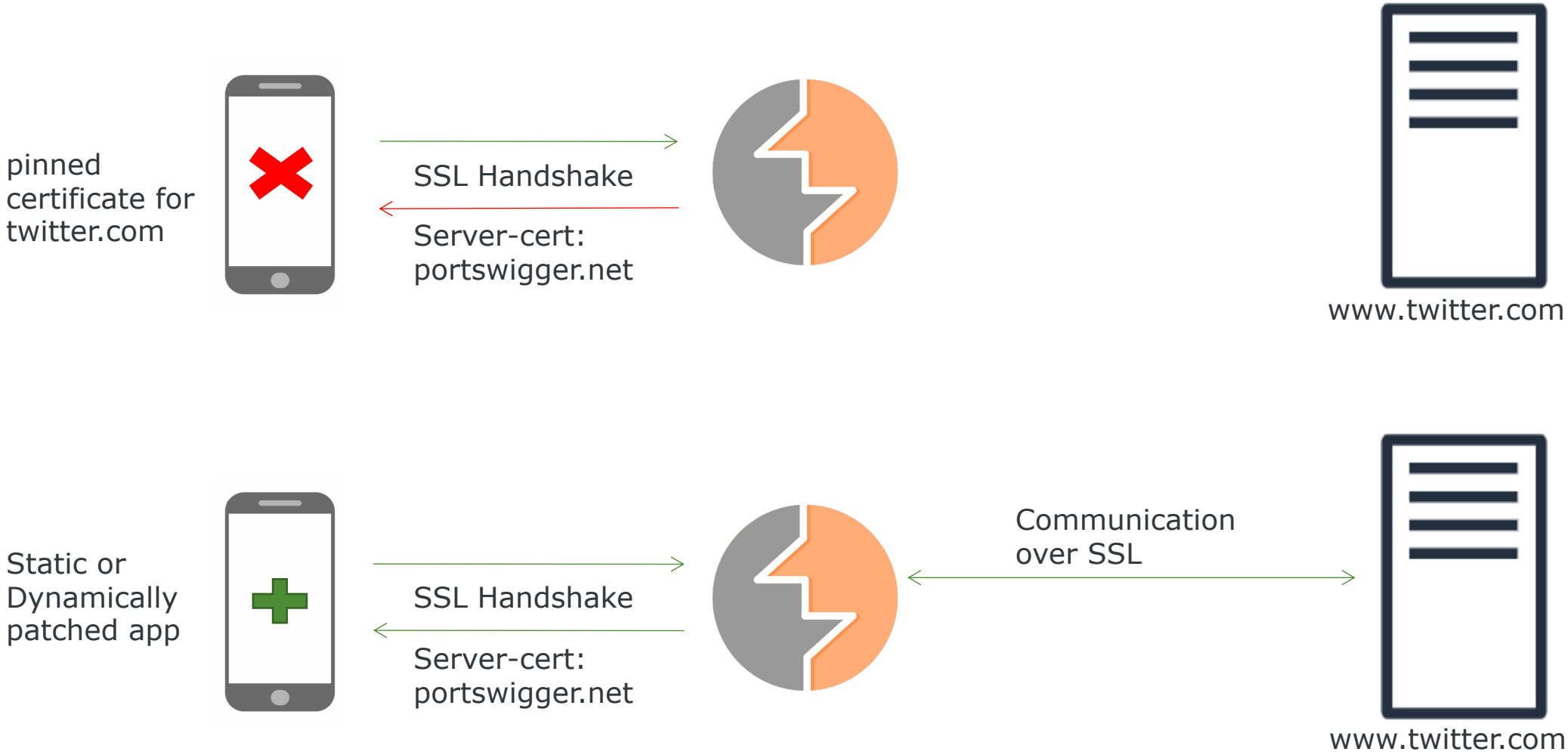
Automated Root Detection Bypass – Frida

DESCRIPTION	COMMAND
Open the app with jadx-gui	jadx-gui UnCrackable-Level1.apk
Copy frida server to the emulator	adb push frida-server-12.7.5-android-x86 /data/local/tmp
Run frida server on emulator	• adb shell • cd /data/local/tmp • chmod +x ./frida-server-12.7.5-android-x86 • ./frida-server-12.7.5-android-x86
Run the frida-script	frida -U –l rootBypass.js –f owasp.mstg.uncrackable1 –no-pause

Setting up proxy in emulator/device

Follow setup instructions from Notes/proxy_setup.md file

Understanding SSL Pinning



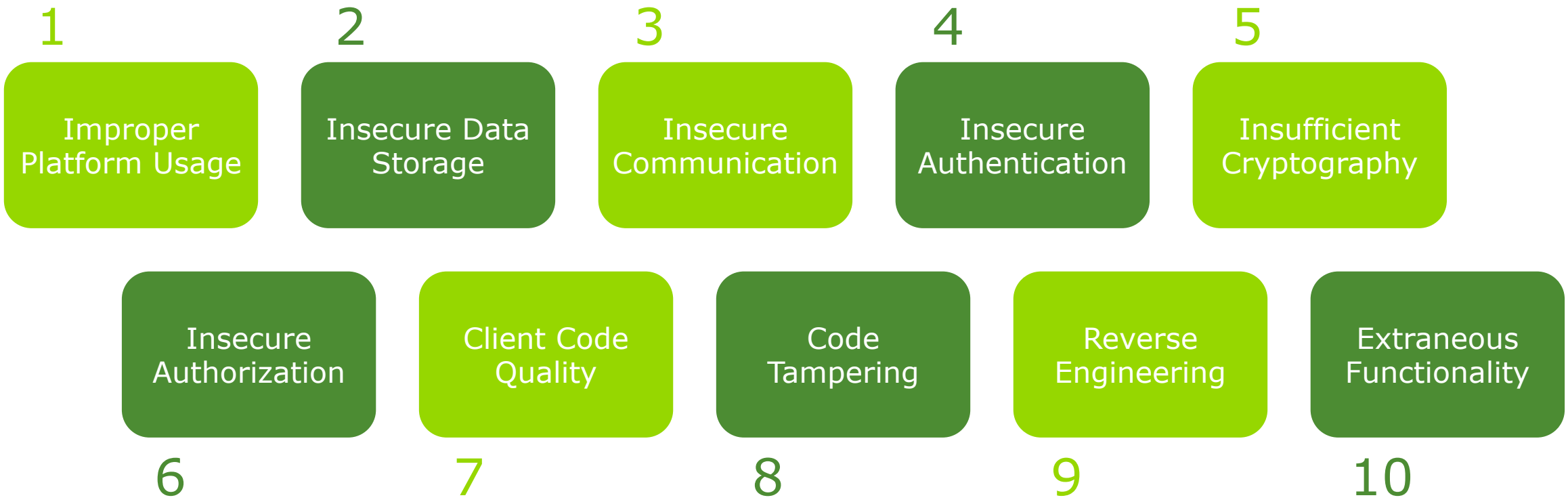
SSL Pinning Bypass using Frida

DESCRIPTION	COMMAND
Open the app with jadx-gui	jadx-gui Twitter.apk
Copy frida server to the emulator	adb push frida-server-12.7.5-android-x86 /data/local/tmp
Run frida server on emulator	• adb shell • cd /data/local/tmp • chmod +x ./frida-server-12.7.5-android-x86 • ./frida-server-12.7.5-android-x86
Run the frida-script	frida -U –l ssl-pin.js –f com.twitter.android --no-pause

08

Common Mobile App Vulnerabilities

OWASP Mobile Top 10



TASK 1 – Hardcoded Credentials

TARGET

ToasterBot.apk

Perform Static Reverse Engineering using apktool and find the flag.

TASK 2 – Hardcoded Credentials

TARGET
fast.apk

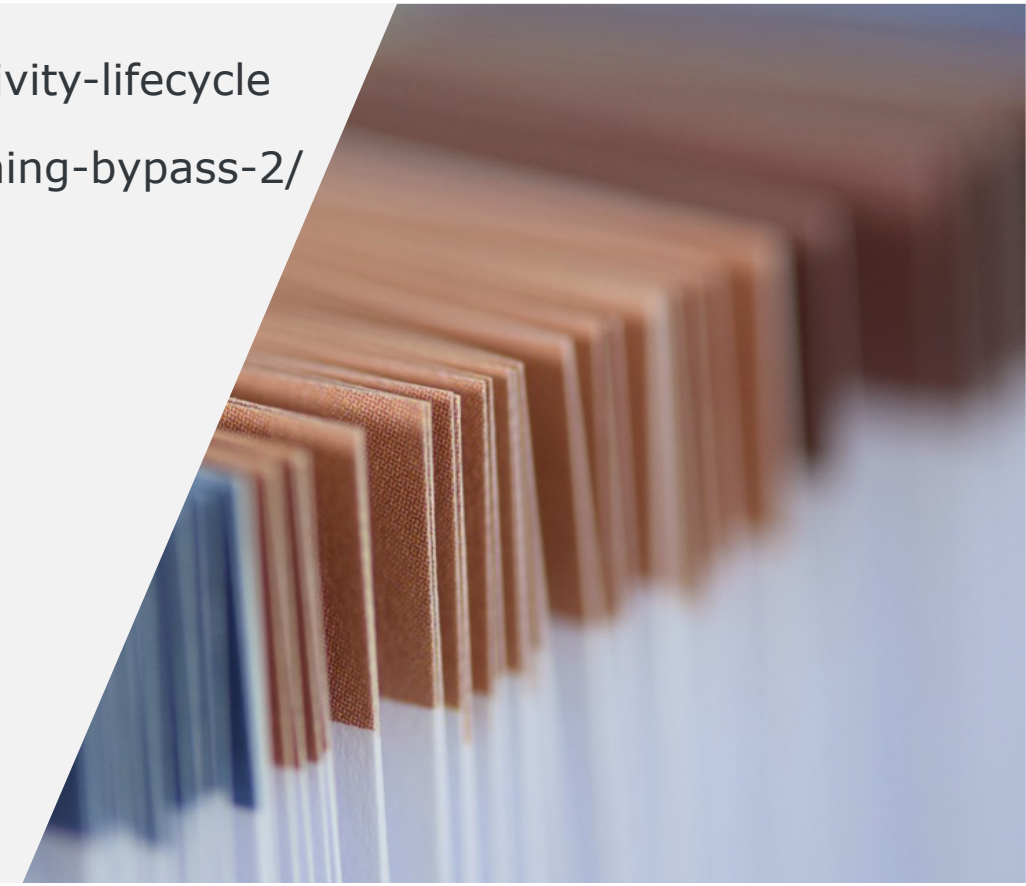
Perform Static Reverse Engineering using apktool and find the flag.

Awesome Learning Resources

- https://source.android.com/security/features
- https://github.com/tanprathan/MobileApp-Pentest-Cheatsheet
- https://github.com/xtiankisutsa/awesome-mobile-CTF
- https://github.com/ashishb/android-security-awesome
- https://appsecwiki.com/#/mobilesecurity

References

- https://developer.android.com/guide/components/activities/activity-lifecycle
- https://codeshare.frida.re/@sowdust/universal-android-ssl-pinning-bypass-2/
- https://www.frida.re/docs/javascript-api/
- https://ibotpeaches.github.io/Apktool/
- https://github.com/skylot/jadx
- https://github.com/payatu/diva-android
- https://labs.f-secure.com/tools/drozer/
- https://github.com/OWASP/MSTG-Hacking-Playground
- https://github.com/OWASP/owasp-mstg/tree/master/Crackmes



Questions?

THANK YOU

xen1thLabs

SMART AND SAFE DIGITAL