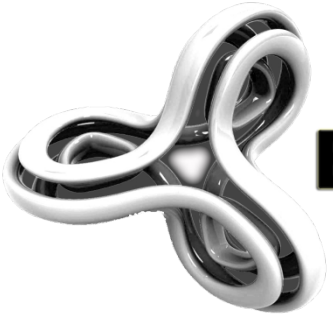


BGA

BİLGİ GÜVENLİĞİ AKADEMİSİ

www.bga.com.tr

Mobile Application Pentest Eğitimi

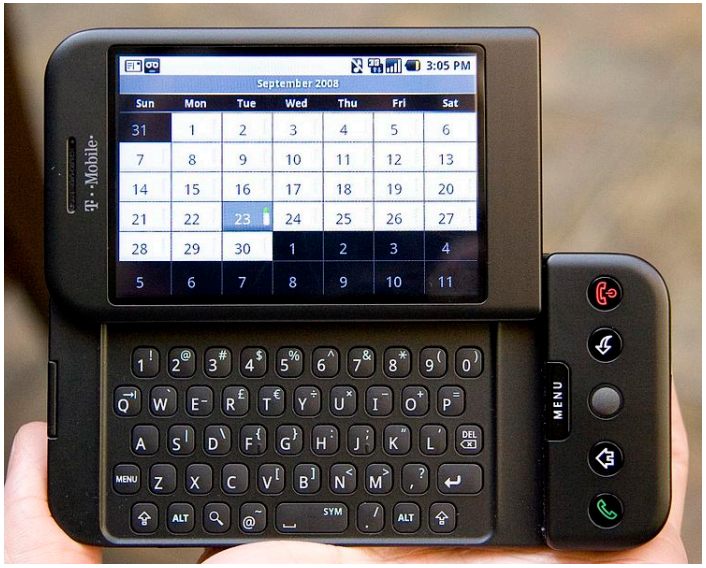
ANDROID

@2013

http://www.bga.com.tr
bilgi@bga.com.tr

Android

- 2003: Android Inc.'in kuruluşu
- 2005: Google'a geçişi
- 2008: İlk ticari mobil Android cihaz

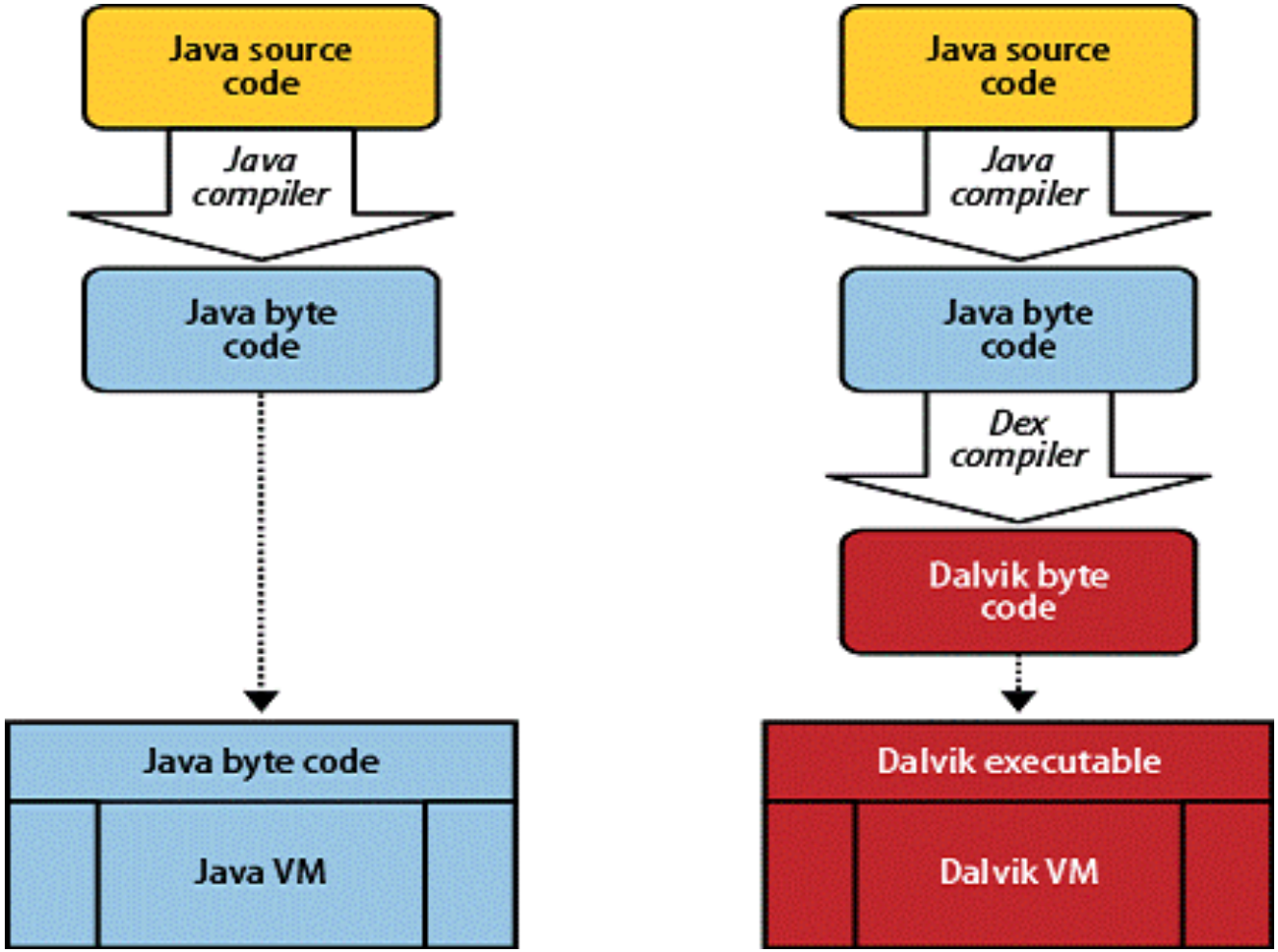


Sayılarla Android

- 900 milyon cihazı aktivasyonu
- 1.5 milyon günlük cihaz aktivasyonu
- >50 milyar uygulama kurulumu *Google Play*


Applications
Home
Contacts
Phone
Browser
...
Application Framework
Activity Manager
Window Manager
Content Providers
View System
Notification Manager
Package Manager
Telephony Manager
Resource Manager
Location Manager
XMPP Service
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
Bluetooth Driver
Flash Memory Driver
Binder (IPC) Driver
USB Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Java VM vs. Dalvik VM



Android SDK

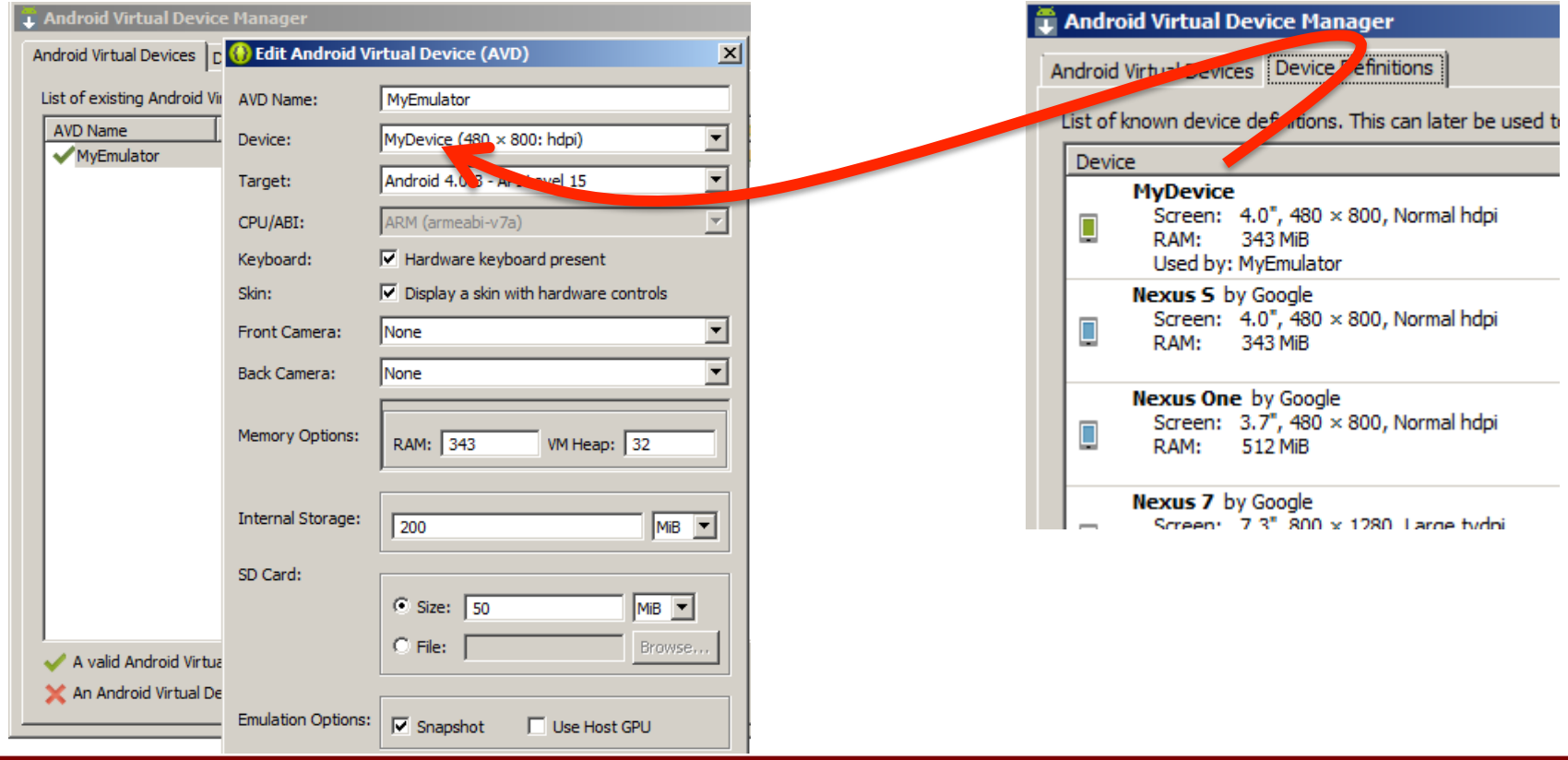
- Android Yazılım Geliştirme Kiti
- Android SDK Bileşenleri;
  - SDK Manager: *Farklı Android SDK'larını yönetme aracı*
    - *Android 2.3.3 (Gingerbread, 2010) API Level 9*
    - *Android 3.2 (Honeycomb, 2011) API Level 13*
    - *Android 4.0.3 (Ice Cream Sandwich, 2011) API Level 15*
    - *Android 4.1 (Jelly Bean, 2013) API Level 18*
  - Emulator: *Test Android simulatorü*
  - AVD Manager: *Android Emulator yapılandırma aracı*

Android Emulator

- Sanal Android mobil cihazlardır.
- Geliştirme ve test amaçları için kullanılır.
- Cihaz tipleri ve içinde çalışacak Android versiyonları emulatorü oluşturur.

AVD Manager

- Android versiyonu ve cihaz tipi, bir sanal cihazı oluşturur.



Yeni Android Device Definition

Çözünürlük

Keyboard yok

Directional Pad

Emulator RAM büyüklüğü

Edit Device

Name: MyDevice
Screen Size (in): 4.0
Resolution (px): 480 x 800

Sensors: Accelerometer, Gyroscope, GPS, Proximity Sensor

Cameras: Front, Rear

Input: Keyboard; No Nav, DPad, Trackball

RAM: 343 MiB

Size: normal
Screen Ratio: long
Density: hdpi

Buttons: Hardware

Device States:
Portrait: Enabled, Navigation
Landscape: Enabled, Navigation
Portrait with keyboard: Enabled, Navigation
Landscape with keyboard: Enabled, Navigation

Override the existing device with the same name

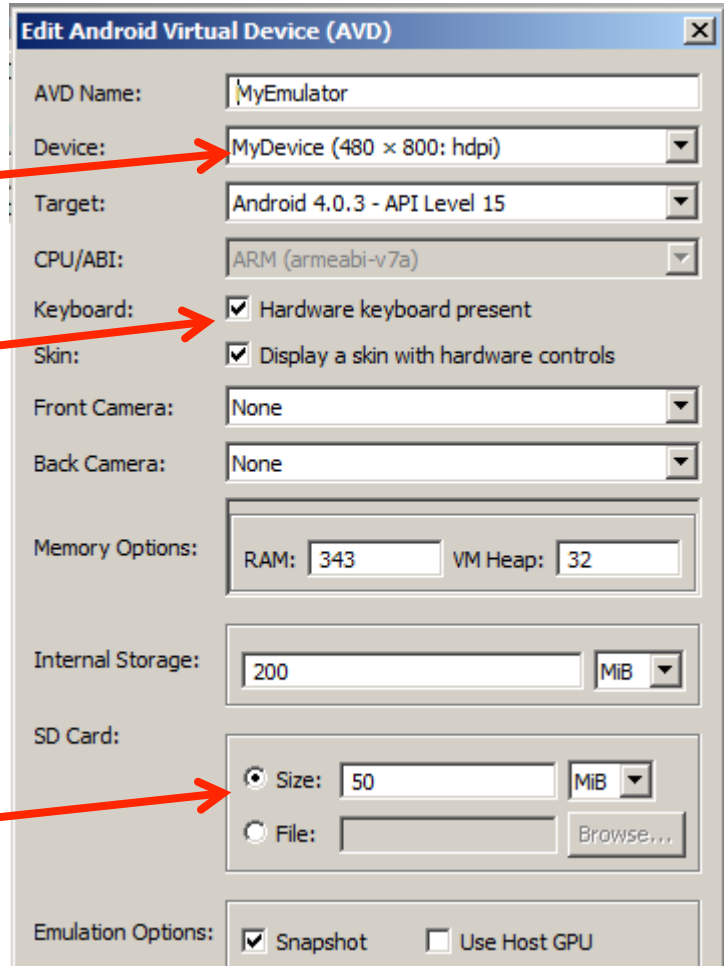
Edit Device | Cancel

Yeni Android Virtual Device

Device Seçimi

Hardware Keyboard

SD Card Büyüklüğü

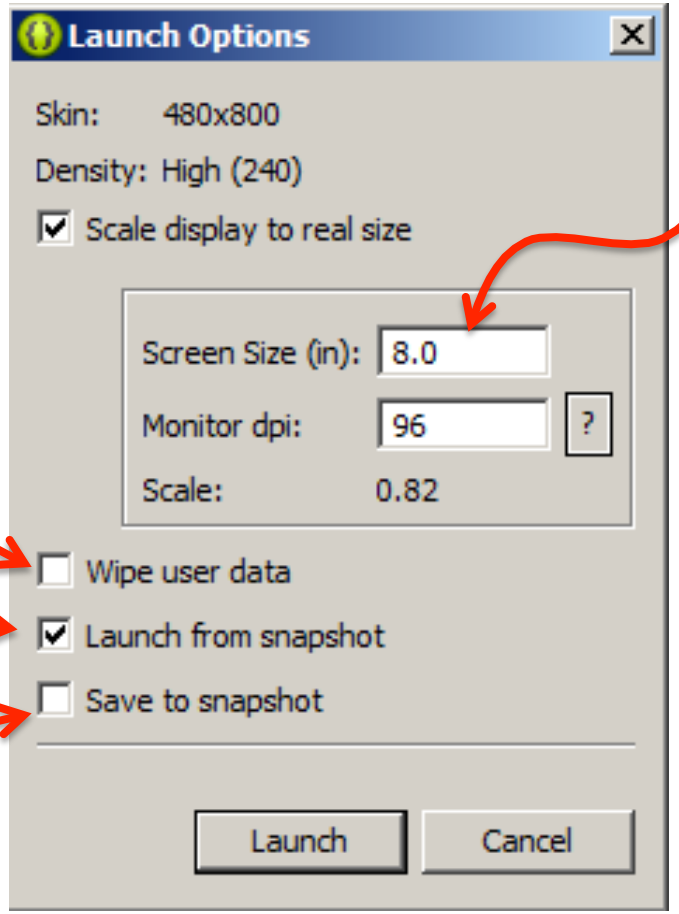


Emulator w/ Snapshot

Eski kaydedilmiş snapshot kullanılmaz

Eski kaydedilmiş snapshot kullanılır

Değişiklikler snapshot 'a kaydedilir



Sanal cihazın boyutunun belli bir oranda küçültülmesi

Android Debug Bridge - adb

- Android cihazlar veya emulatorler ile iletişimi sağlayan zengin komut satırı aracıdır.
- <SDK>/platform-tools/adb

```
adb install uygulama.apk
adb push <yerel> <uzak>
adb pull  <uzak> <yerel>
adb shell
adb logcat
```

Android Sandbox Modeli - ps

```
radio     165   37    647984 35900 ffffffff 40011384 S com.android.phone
app_9     178   37    650104 52736 ffffffff 40011384 S com.android.launcher
app_20    235   37    659192 53428 ffffffff 40011384 S android.process.acore
app_4     294   37    632752 30328 ffffffff 40011384 S android.process.media
app_11    319   37    641888 33416 ffffffff 40011384 S com.android.email
app_22    324   37    632992 32512 ffffffff 40011384 S com.android.inputmethod.la
app_21    358   37    634140 28700 ffffffff 40011384 S com.android.exchange
app_25    385   37    633368 32404 ffffffff 40011384 S com.android.mms
app_31    413   37    632576 29512 ffffffff 40011384 S com.android.providers.cale
app_8     429   37    630736 29068 ffffffff 40011384 S com.android.deskclock
system    442   37    641768 43128 ffffffff 40011384 S com.android.settings
app_32    457   37    634556 29540 ffffffff 40011384 S com.android.calendar
app_17    518   37    630964 27572 ffffffff 40011384 S com.android.defcontainer
app_23    533   37    628872 27104 ffffffff 40011384 S com.svox.pico
app_29    546   37    631404 28540 ffffffff 40011384 S com.android.quicksearchbox
app_42    591   37    643060 39840 ffffffff 40011384 S org.owasp.goatdroid.fourgo
app_1     633   37    637928 31724 ffffffff 40011384 S com.android.browser
app_18    654   37    628852 27184 ffffffff 40011384 S com.android.sharedstorageb
root      718   45    704    308   c014ea24 4000c438 S /system/bin/sh
```

Android Sandbox Modeli - ls

```
# pwd
/data/data
# ls -al
drwxr-x--x app_34   app_34          2012-03-28 18:08 com.android.backupconfirm
drwxr-x--x app_1    app_1           2012-03-28 18:11 com.android.browser
drwxr-x--x app_12   app_12          2012-03-28 18:07 com.android.calculator2
drwxr-x--x app_32   app_32          2012-03-28 18:08 com.android.calendar
drwxr-x--x app_7    app_7           2012-03-28 18:07 com.android.camera
drwxr-x--x app_24   app_24          2012-03-28 18:08 com.android.certinstaller
drwxr-x--x app_20   app_20          2012-03-28 18:08 com.android.contacts
drwxr-x--x app_2    app_2           2012-03-28 18:07 com.android.customlocale2
drwxr-x--x app_17   app_17          2012-03-28 18:14 com.android.defcontainer
drwxr-x--x app_8    app_8           2012-03-28 18:08 com.android.deskclock
drwxr-x--x app_10   app_10          2012-03-28 18:07 com.android.development
drwxr-x--x app_11   app_11          2012-03-28 18:08 com.android.email
drwxr-x--x app_30   app_30          2012-03-28 18:08 com.android.emulator.connec
drwxr-x--x app_19   app_19          2012-03-28 18:08 com.android.emulator.gps.te
drwxr-x--x app_21   app_21          2012-03-28 18:08 com.android.exchange
drwxr-x--x app_13   app_13          2012-03-28 18:07 com.android.fallback
drwxr-x--x app_4    app_4           2012-03-28 18:07 com.android.gallery
drwxr-x--x app_39   app_39          2012-03-28 18:08 com.android.gesture.builder
```

Kurulu Bir Android App İçinde

- cache/ : cache'lenen nesneler
- databases/ : kullanılan veritabanı
- shared_prefs/ : basit veri saklama

```
# pwd
/data/data/org.owasp.goatdroid.fourgoats
# ls -al
drwxrwx--x app_42   app_42           2013-05-17 21:07 cache
drwxrwx--x app_42   app_42           2013-05-17 21:07 databases
drwxr-xr-x system   system           2013-05-17 21:06 lib
drwxrwx--x app_42   app_42           2013-05-17 22:53 shared_prefs
#
```

databases/

- Android SQLite veritabanı sistemi ile gelir.
- Hassas veriler açık saklanmamalıdır;
  - kimlik bilgileri, şifreleme anahtarları, kredi kartları

```
# pwd
/data/data/org.owasp.goatdroid.fourgoats/databases
# ls -al
-rw-rw---- app_42   app_42       4096 2013-05-17 22:53 userinfo.db
-rw-rw---- app_42   app_42          0 2013-05-17 22:53 userinfo.db-journal
# sqlite3 userinfo.db
SQLite version 3.7.4
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
android_metadata  info
sqlite> select * from info;
1|60d65a7fe07cee7e48d94c5f8fc85a548c20cef55f2bf5b35a3f07de74adbd3c4e4a422fe
6236503a695b775ce85c76b846|test|true|true|false
sqlite>
```

shared_prefs/

- Basit key:value çiftlerini saklamak içindir.
- Hassas veriler açık saklanmamalıdır;
  - kimlik bilgileri, v.b.

```
# pwd
/data/data/org.owasp.goatdroid.fourgoats/shared_prefs
# ls -al
-rw-rw-r-- app_42   app_42        187 2013-05-17 22:53 credentials.xml
-rw-rw-r-- app_42   app_42        142 2013-05-17 22:48 destination_info.xml
-rw-rw-r-- app_42   app_42        140 2013-05-17 21:07 proxy_info.xml
# cat credentials.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="password">test</string>
<boolean name="remember" value="true" />
<string name="username">test</string>
</map>
#
```

LogCat

- İşlemler için kullanılan kayıt mekanizması
- Hassas veriler açık bir şekilde kayıt altına alınmamalıdır;
  - kimlik bilgileri, şifreleme anahtarları, kredi kartları

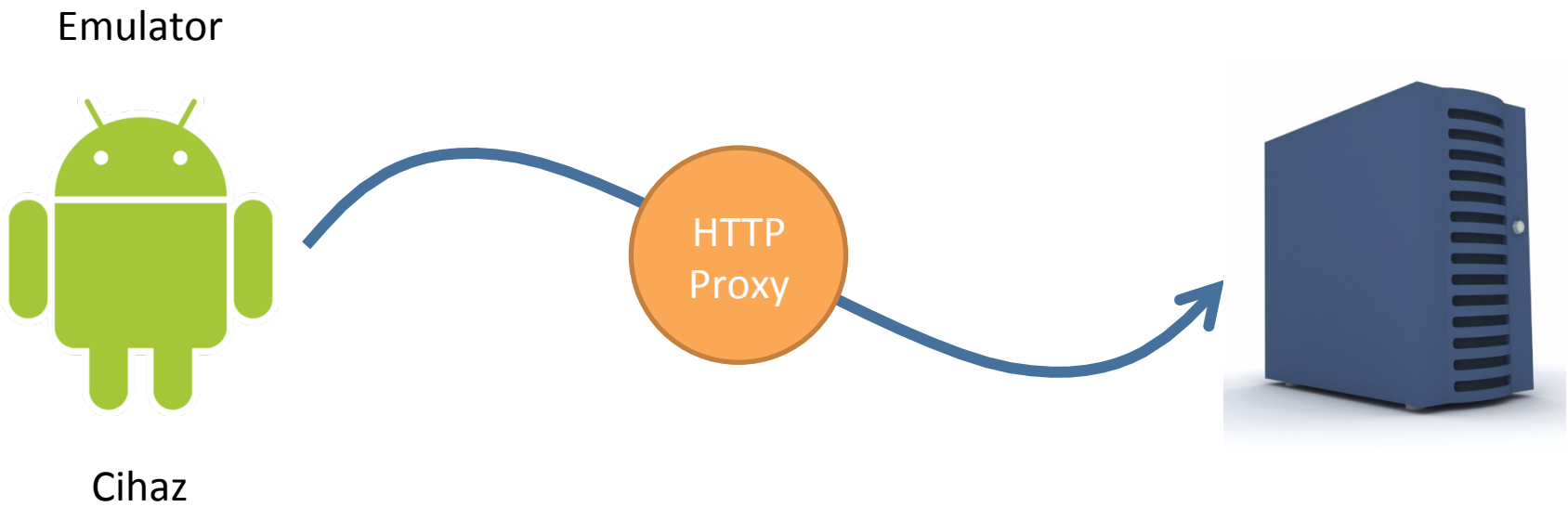
```
E/Cursor  (  827):      at org.owasp.goatdroid.herdfinancial.services.StatementUpdateS
ervice$1.run(StatementUpdateService.java:33)
E/Cursor  (  827): Finalizing a Cursor that has not been deactivated or closed. databa
se = /data/data/org.owasp.goatdroid.herdfinancial/databases/userinfo.db, table = info,
 query = SELECT accountNumber FROM info
E/Cursor  (  827): net.sqlcipher.database.DatabaseObjectNotClosedException: Applicatio
n did not close the cursor or database object that was opened here
E/Cursor  (  827):      at net.sqlcipher.database.SQLiteCursor.<init>(SQLiteCursor.jav
a:217)
```

SD Card'lar

- Android dahili veya harici depolama ihtiyacını SD Card'lar ile sağlar
- Ancak SD Card üzerindeki kaynaklar geniş dosya hakları ile kullanılırlar

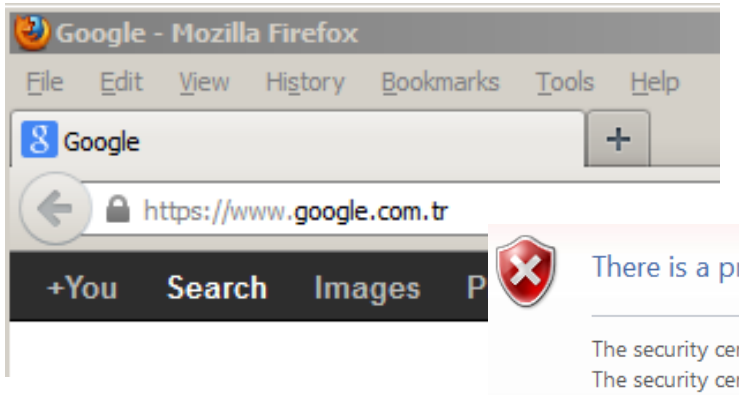
```
# pwd
/mnt/sdcard
# ls -al androidlabs/
----rwxr-x system   sdcard_rw      164 2013-05-17 20:50 1368813057416.html
#
```

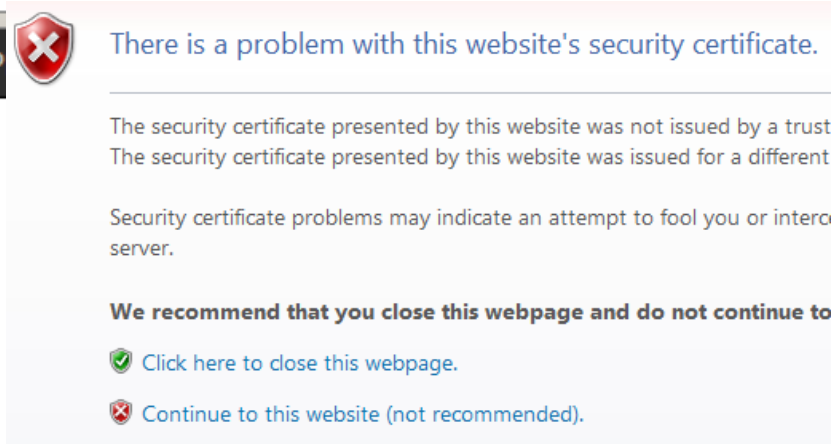
Proxy



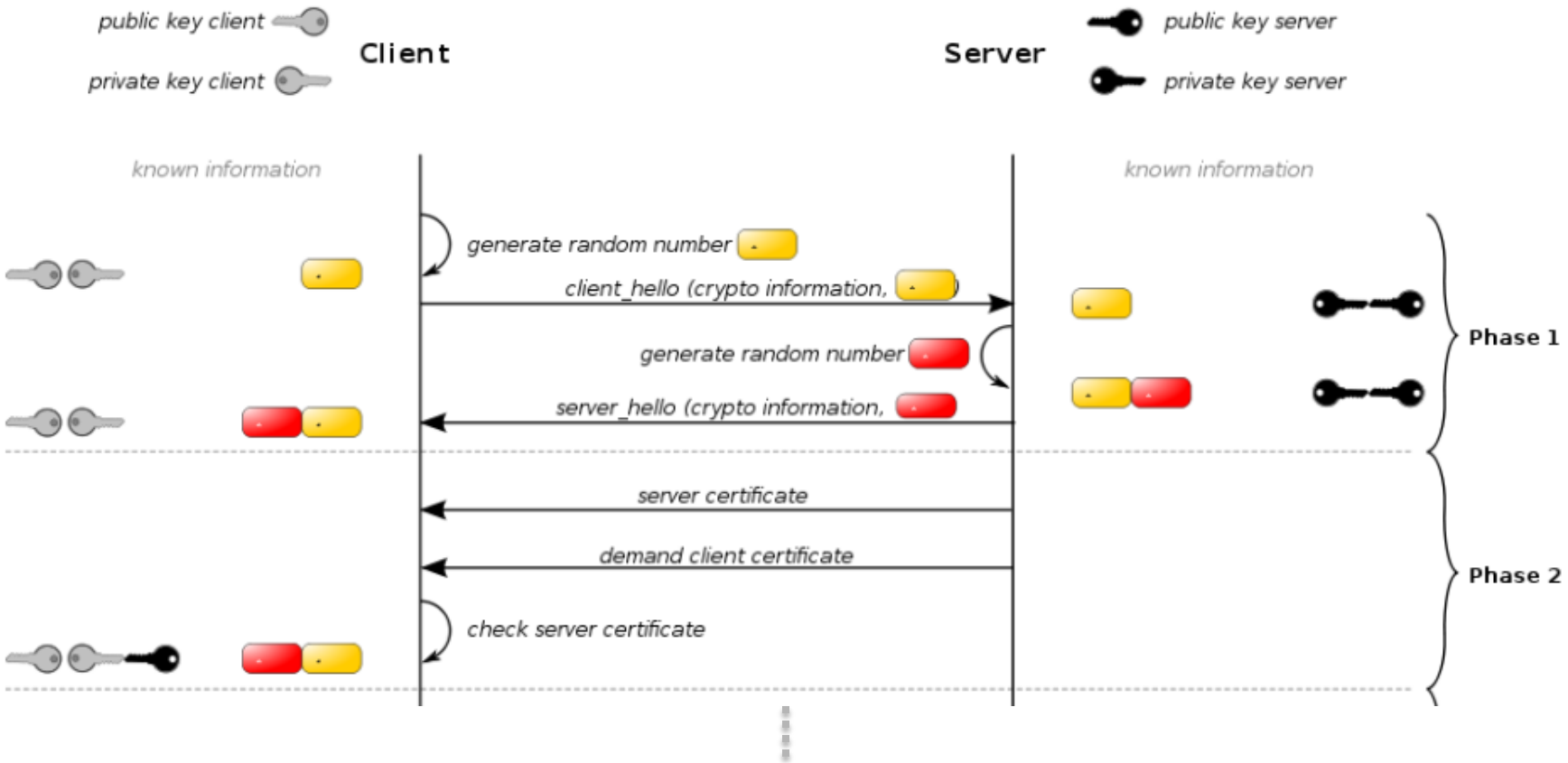
SSL/TLS

- SSL/TLS protokolü, HTTP trafiğinin gizliliğini sağlayan en temel unsurdur.

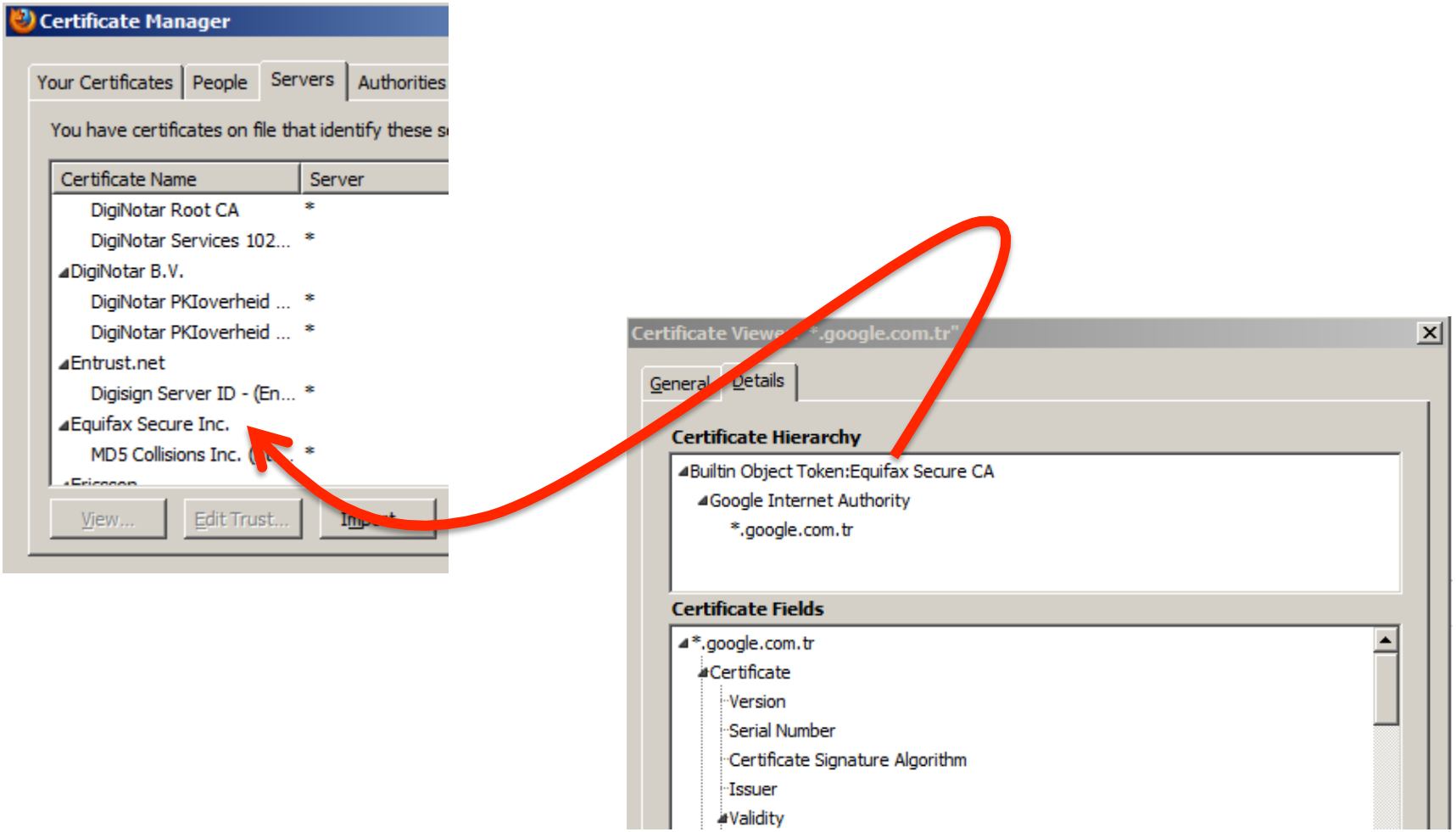




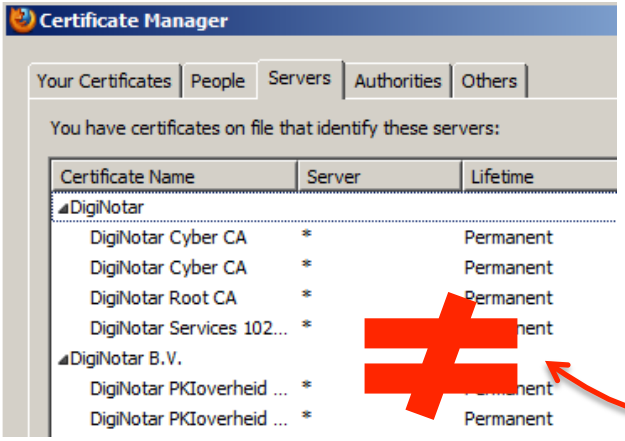
SSL Tokalaşması

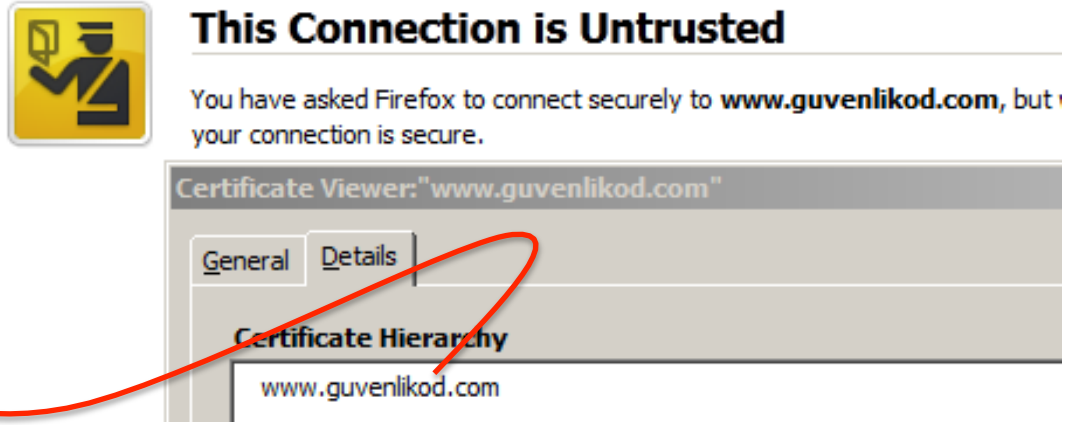


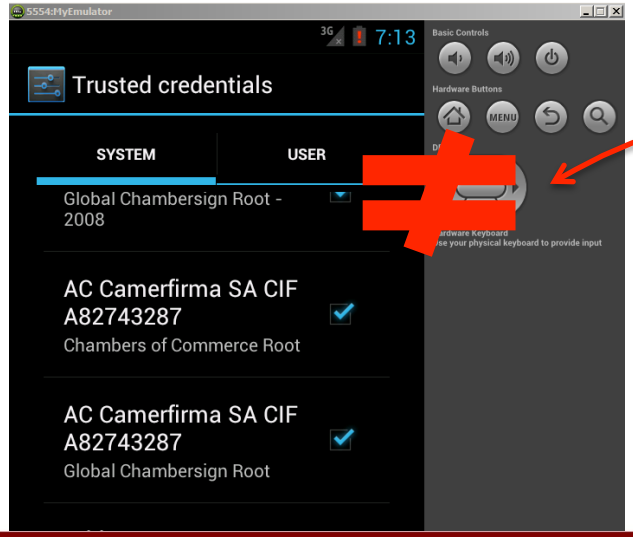
Güvenilir Sertifikalar - Browser



HTTPS Bağlantılar








```
URL url = new URL("https://www.guvenlikod.com/");
con = (HttpsURLConnection)url.openConnection();
```

```
W/System.err( 1634): javax.net.ssl.SSLPeerUnverifiedException:
W/System.err( 1634):     at
org.apache.harmony.xnet.provider.jsse.SSLSessionImpl.getPeerCe
W/System.err( 1634):     at org.apache.http.conn.ssl.AbstractVe
W/System.err( 1634):     at
org.apache.http.conn.ssl.SSLSocketFactory.createSocket(SSLSock
W/System.err( 1634):     at
org.apache.http.impl.conn.DefaultClientConnectionOperator.open
```

Güvenilir Sertifikalar - Android

- Android sisteminde güvenilir sertifikalar

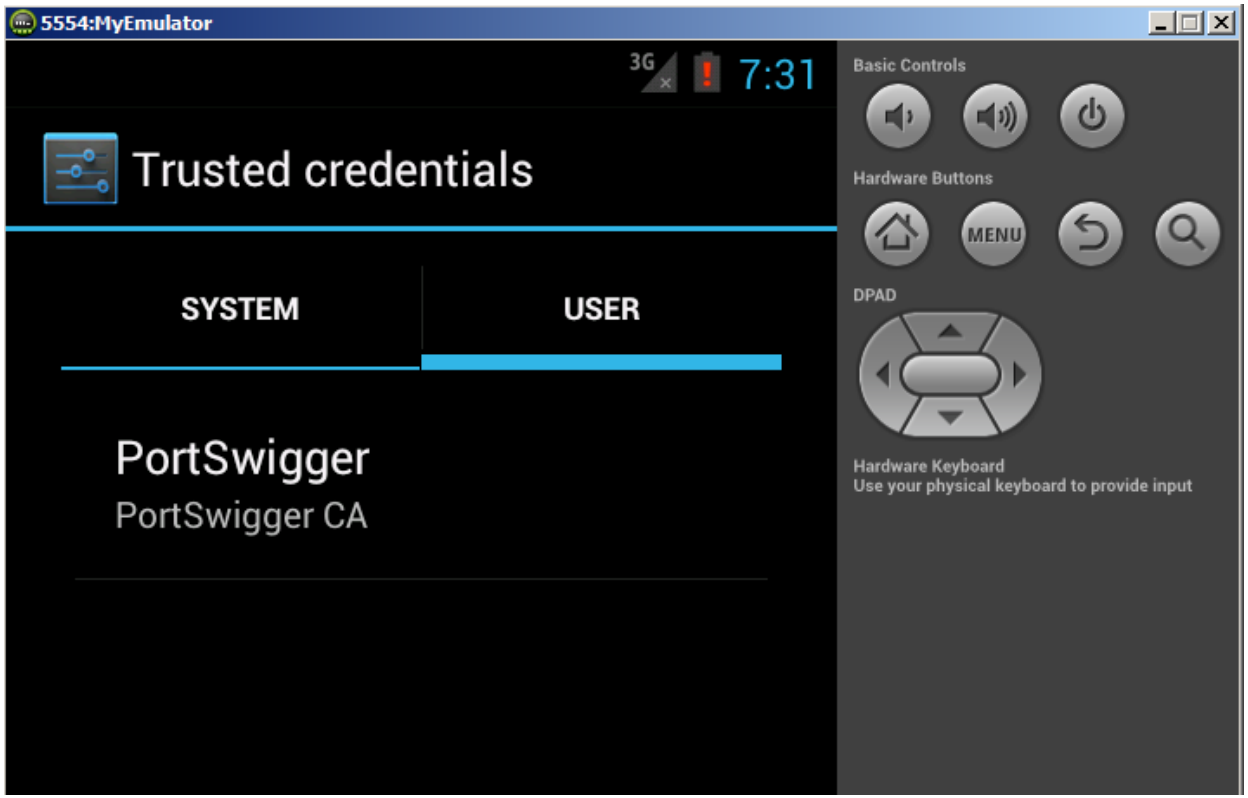
/etc/security/cacerts.bks

- Burp SSL sertifikasını yüklemek için;

1. Browser'da https://hedefsunucu:hedefport açılması
2. CA sertifikasının **der** dosyası olarak export edilmesi
3. **der** dosyasının uzantısının **cer** olarak değiştirilmesi
4. adb push burp.cer /sdcard/burp.cer
5. Emulator/Cihaz'da Settings->Security->Install from SDCARD

Yüklenen Sertifika

- Settings->Security->Trusted credentials



Android APN

Settings

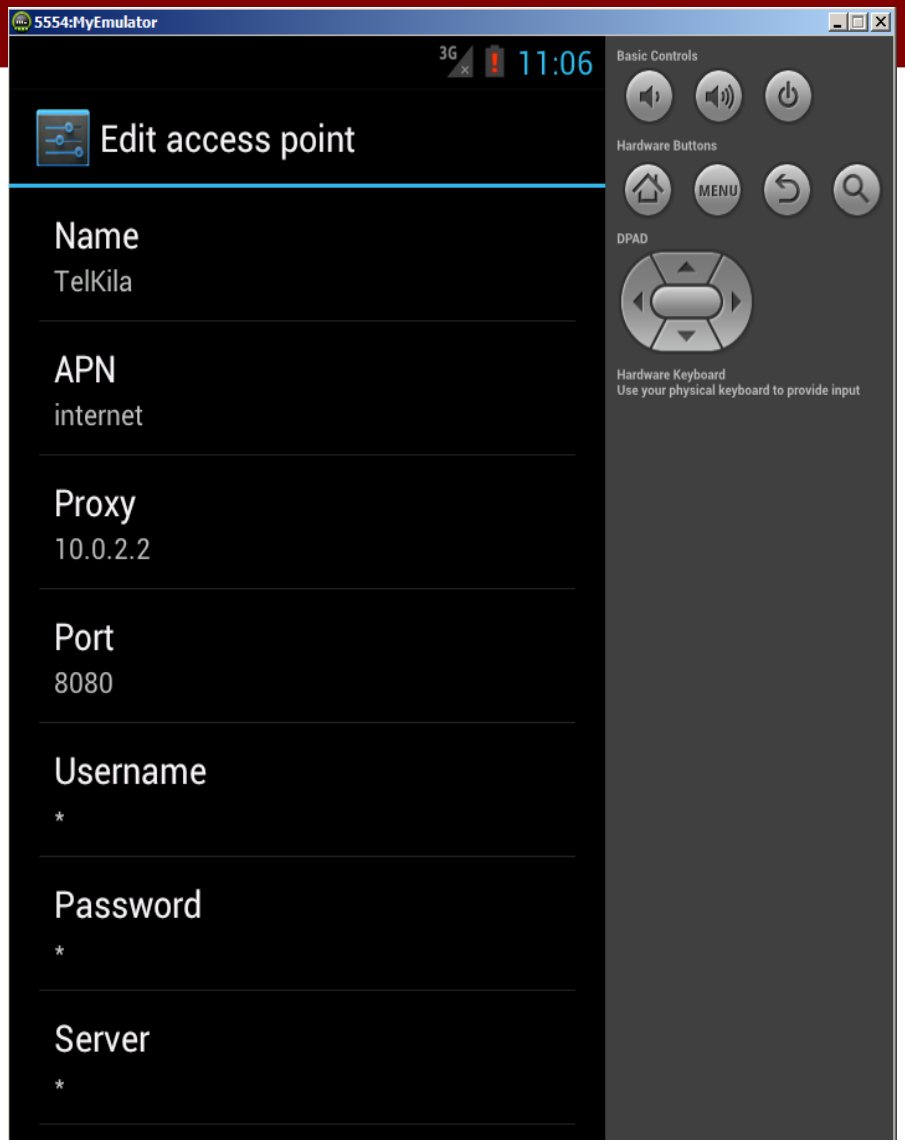
Wireless & Networks

More

Mobile Networks

Access Point Names

Telkila



Dikkat adb bağlantısı kopabilir!

 # adb kill-server

 # adb start-server

Android WIFI

Settings

Wireless & Networks

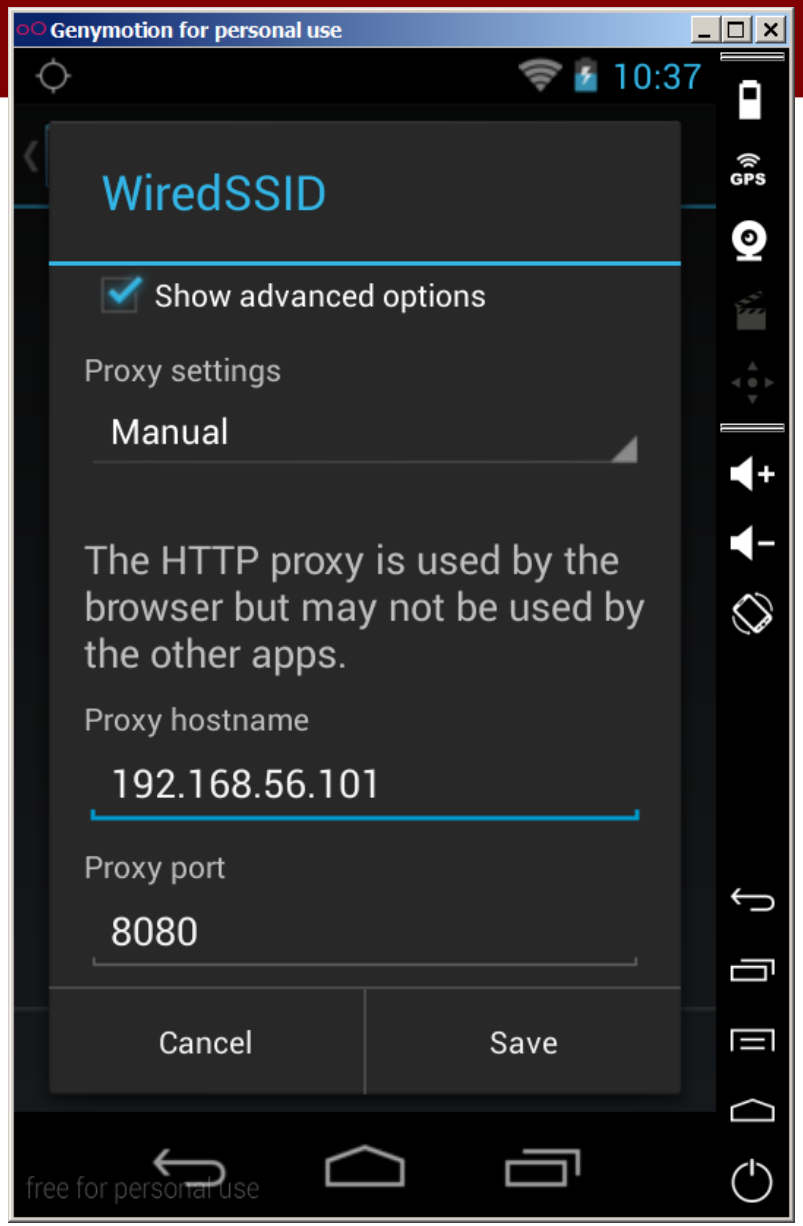
WIFI

WiredSSID*

Modify Network

Show Advanced Opt.

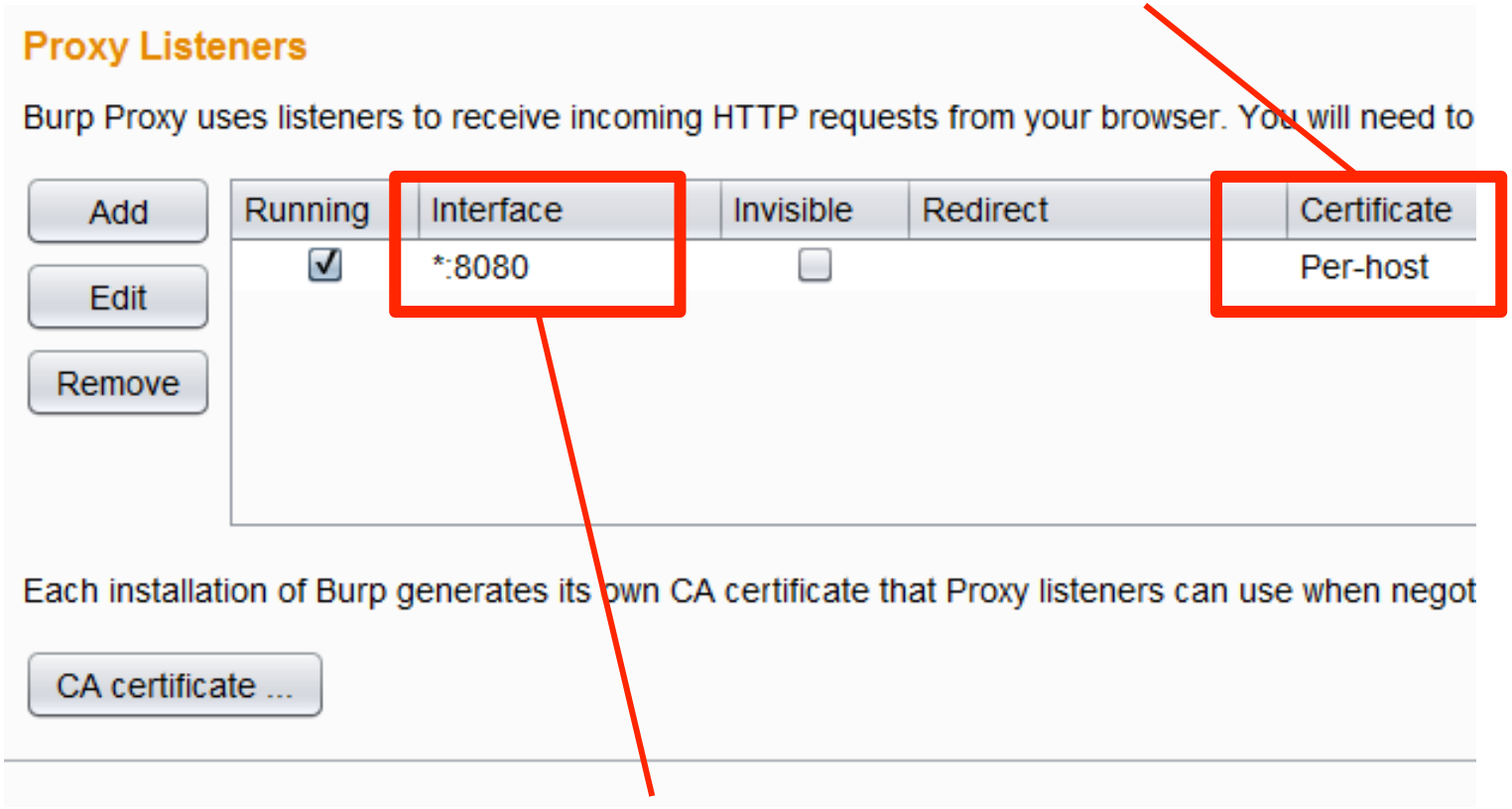
Manual



* **WiredSSID üzerine mouse ile basılı tutularak**

Burp Proxy Ayarları

Her Host için ayrı CA imzalı sertifika



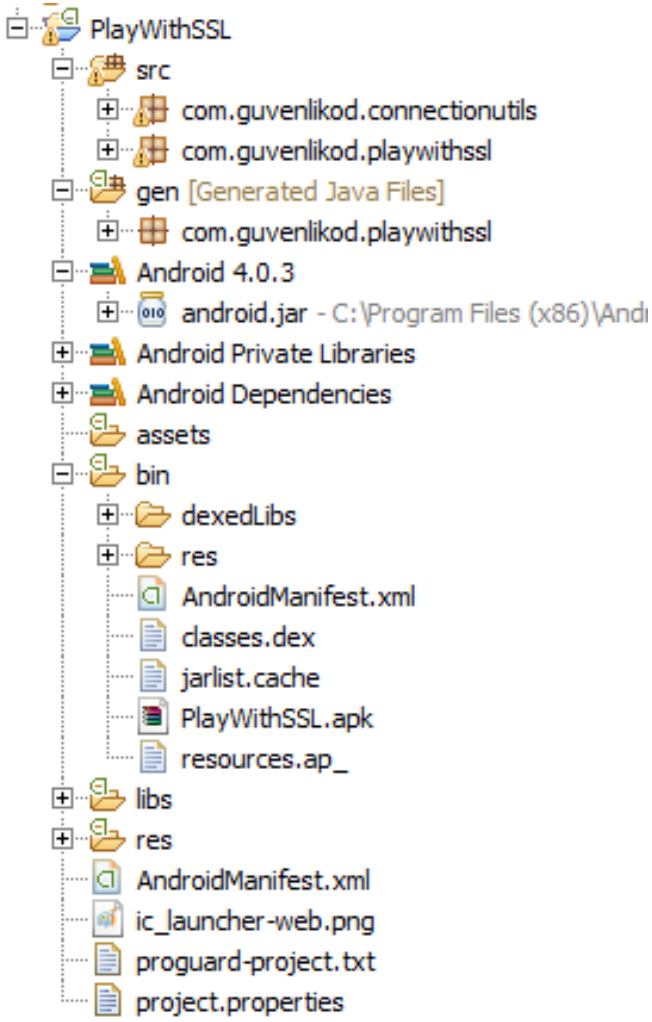
Bütün interfacelerden dinler

Emulatör Komut Satırı

- AVD manager arayüzünün yanısıra Android emulatör komut satısı aracılığı ile de çalıştırılabilir
- HTTP Proxy cihaz başlatılırken komut satırından da tanıtılabilir

```
emulator -avd MyEmulator -http-proxy http://127.0.0.1:8081
```

Android Proje Dizin Yapısı



src/

Kaynak kodlar; java,aidl dosyaları

gen/

Otomatik üretilen java dosyaları

bin/

APK'yı oluşturan derlenmiş dosyalar; dex, xml

libs/

Harici kütüphaneler

res/

Kaynaklar; imajları, yapılandırma XML'leri

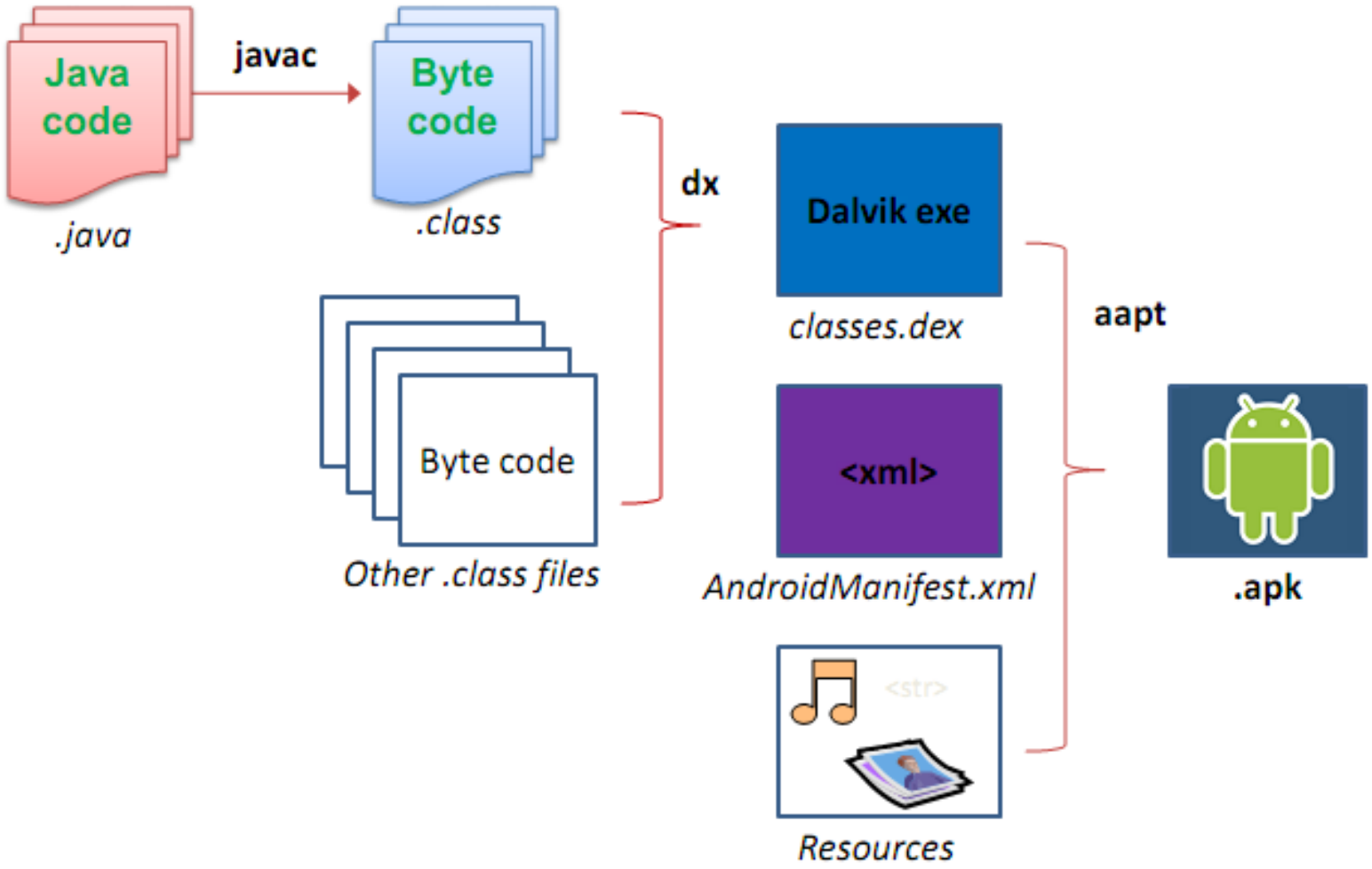
project.properties

Hedef Android versiyonu

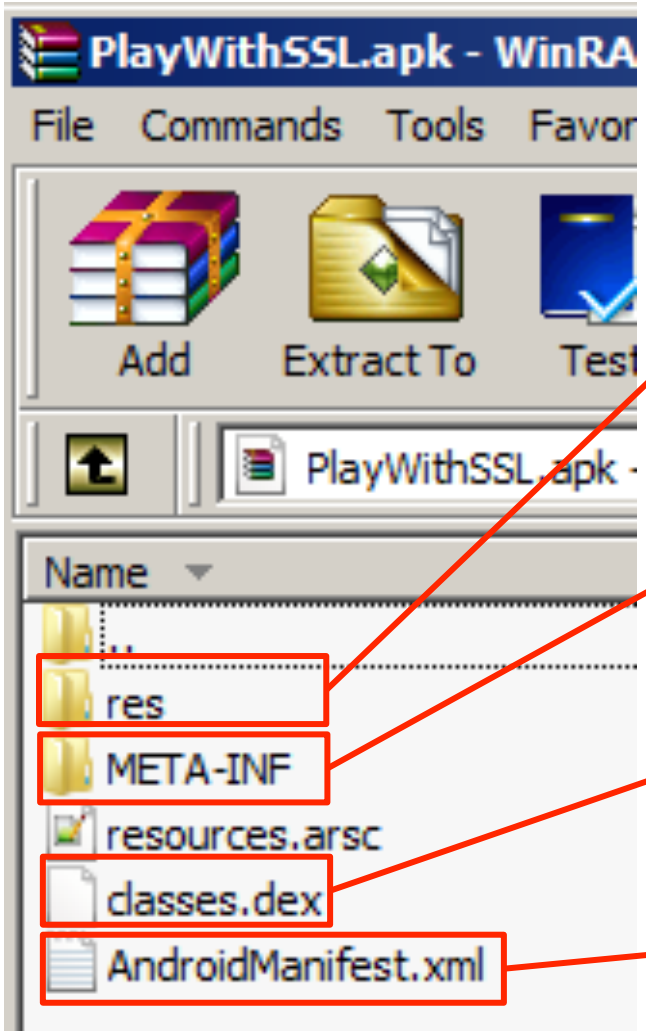
AndroidManifest.xml

Uygulama bileşenleri, kullanılacak izinler, v.b.

Java → APK


Java code
.java
javac
Byte code
.class
Byte code
Other .class files
dx
Dalvik exe
classes.dex
<xml>
AndroidManifest.xml
Resources
aapt
.apk

Android Package - APK



UI ile ilgili XML yapılandırma dosyaları, resimler

Kriptografik imzalanmış sertifikalar

Java class dosyalarının dex formatına derlenmiş hali

Binary formatında uygulama bileşenleri, kullanılacak izinler, v.b.

APK Dosyasının İmzalanması

- APK kurulum dosyası, release öncesinde kriptografik olarak imzalanmalıdır.
  - dijital imza sertifikası self-signed olabilir
  - sertifikanın geçerlilik süresi kurulum/yenileme zamanında kontrol edilir
  - keytool/jarsigner araçları imzalama işlemi için kullanılırlar
  - imzalar, cihaz üzerinde koşan uygulamalar arası güvenli iletişimin en önemli kaynaklarındandır

İmzalama İşlemleri

1

- Yoksa self-signed sertifikasının oluşturulması

```
keytool.exe
        -genkey
        -keystore mykstr
        -alias myalias
        -keyalg RSA
        -validity 10000
```

sertifikanın saklanacağı keystore dosya ismi

keystore içindeki sertifikanın alias'ı

10000 gün geçerlilik süresi

İmzalama İşlemleri

2

- APK'nın imzalanması

```
jarsigner.exe
        -verbose
        -keystore mykstr
        HelloWorld.apk
        myalias
        -sigalg MD5withRSA
        -digestalg SHA1
```

imzalayacak sertifikayı barındıran keystore

imzalanacak APK

keystore içinde imza için kullanılacak sertifikanın alias'ı

İmzalama İşlemleri

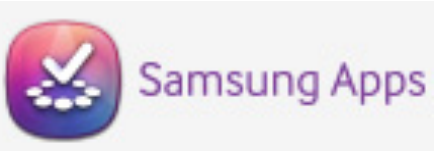
- APK imzasının kontrolü

```
jarsigner.exe
        -verbose
        -verify
        HelloWorld.apk
```

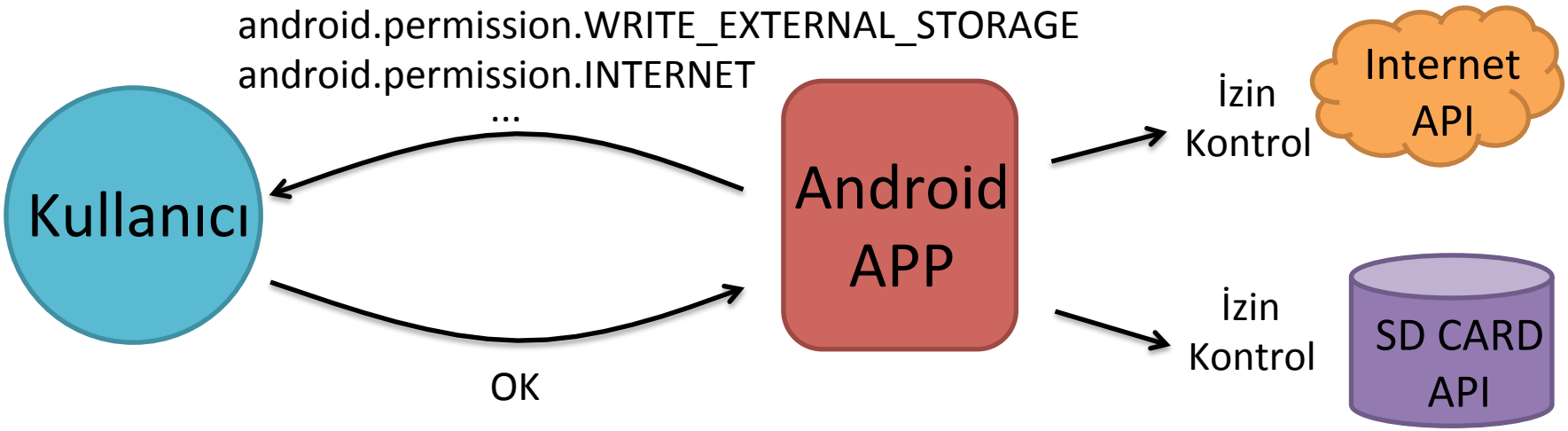
imzası kontrol edilecek APK

Android Market

- Android uygulamaların indirildiği bazı popüler web portallar



Android Uygulama İzinleri



- Kurulma/Yenileme esnasında uygulamalar kaynaklara erişmek için kullanacakları izin listesini kullanıcının onayına sunarlar.
- Onay sonrası uygulama, kaynaklara erişim esnasında bir daha bu izinleri kullanıcıya sormaz.

AndroidManifest.xml ve İzin Tanımları

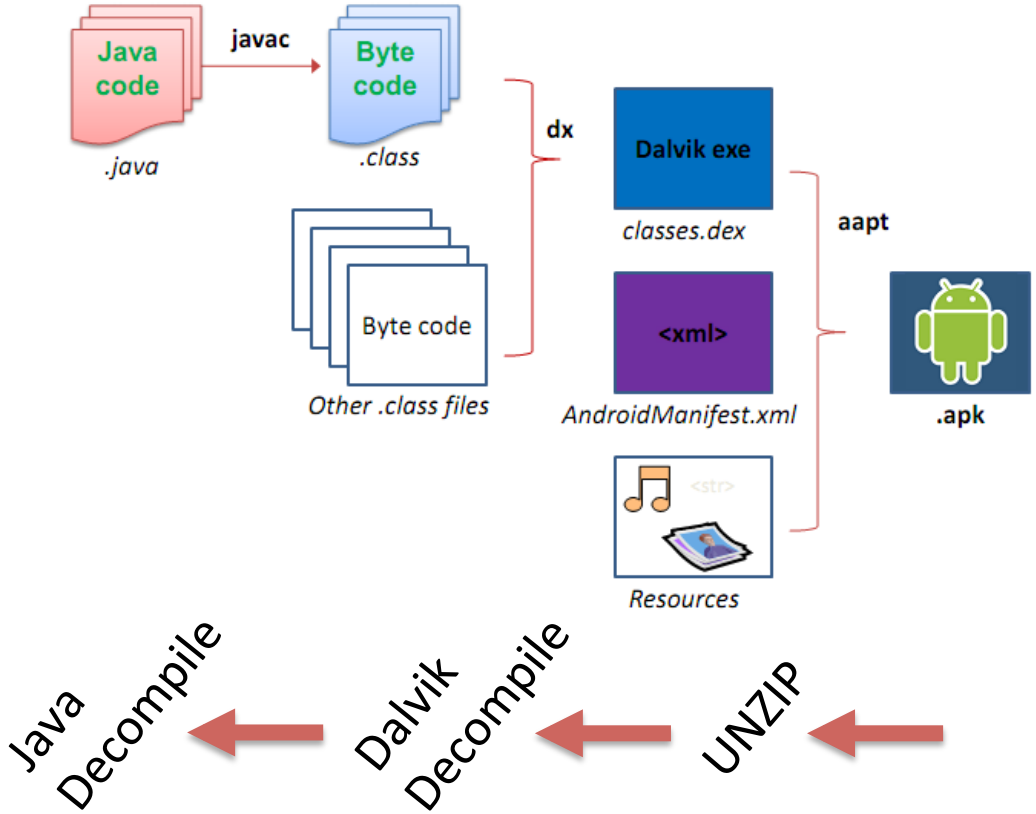
```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.owasp.goatdroid.herdfinancial"
    android:versionCode="1"
    android:versionName="1.0" >

    <uses-sdk android:minSdkVersion="8" />

    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />

    <application
        android:icon="@drawable/icon"
```

 # aapt.exe dump permissions HerdFinancial.apk

package: org.owasp.goatdroid.herdfinancial
uses-permission: android.permission.READ_PHONE_STATE
uses-permission: android.permission.INTERNET
uses-permission: android.permission.WRITE_EXTERNAL_STORAGE

Reversing APK

- Dalvik executable (classes.dex) -> Java kaynak kodlarına dönüşüm



Reversing APK - dex2jar

```
# d2j-dex2jar.bat PlayWithSSL.apk
```

1

Java Decompiler - MyHttpClient.class

File Edit Navigate Search Help

PlayWithSSL-dex2jar.jar

- android
  - annotation
  - support.v4
- com.guvenlikod
  - connectionutils
    - CustomSSLSocketFactory
    - MyHttpClient
      - MyHttpClient
        - response : String
        - target : String
        - Execute() : void
        - MyHttpClient(String)
        - getResponse() : String
        - readStream(InputStream) : String
    - RequestMethod
    - RestClient
  - playwithssl
    - BuildConfig
    - MainActivity
    - R

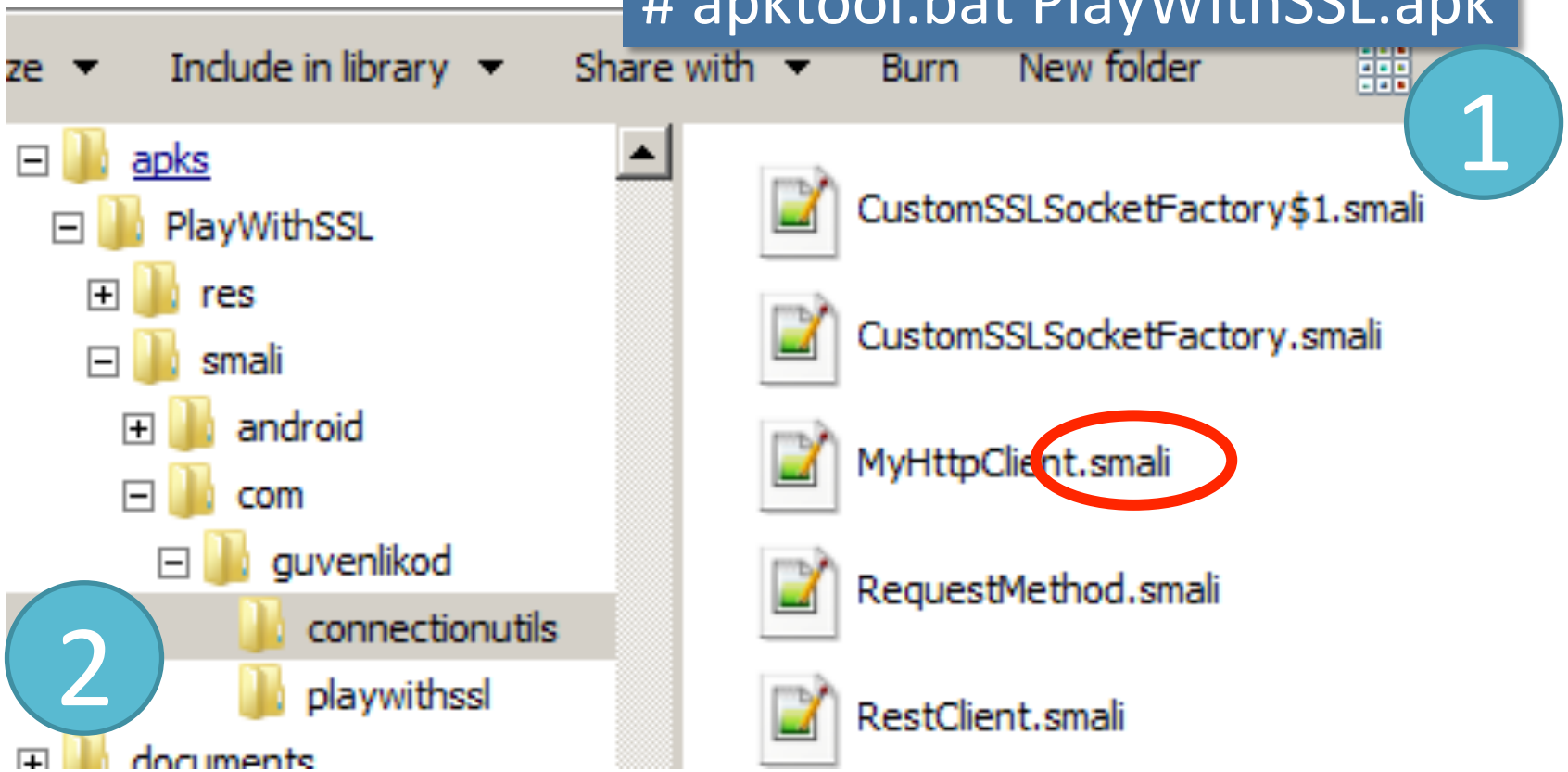
MyHttpClient.class

```
}

public void Execute()
{
  Log.i("PlayWithSSL MyHttpClient", "Ir
  try
  {
    this.response = readStream(((HttpsU
    Log.i("PlayWithSSL MyHttpClient", "
    return;
  }
  catch (Exception localException)
  {
    localException.printStackTrace();
  }
}

public String getResponse()
{
```

2

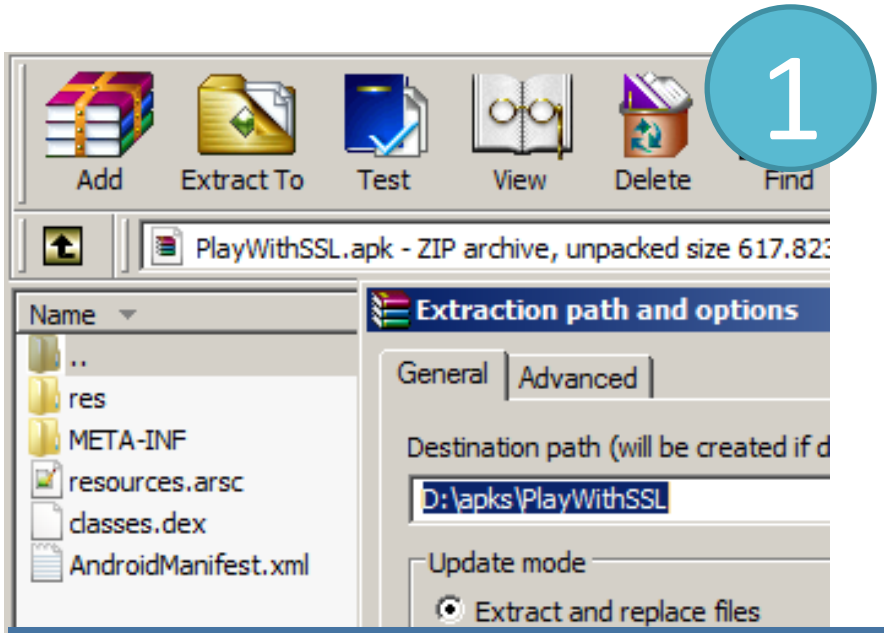
Reversing APK - apktool

apktool.bat PlayWithSSL.apk



smali?

- Dex için üretilen assembly/disassembly aracı
- Aynı zamanda assembly diline verilen isim



2

```
java -jar baksmali-1.4.2.jar PlayWithSSL\classes.dex -o smali
```

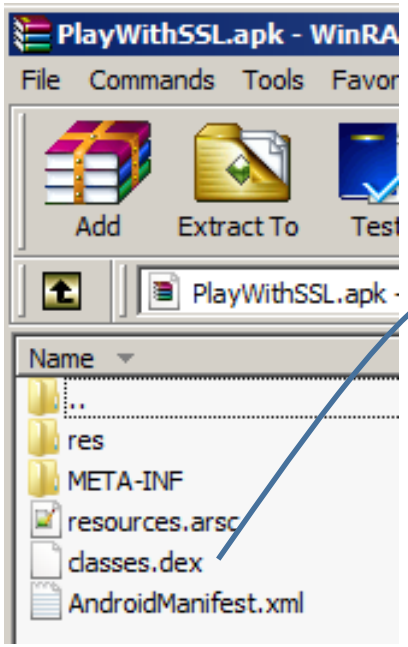
java - HelloWorld

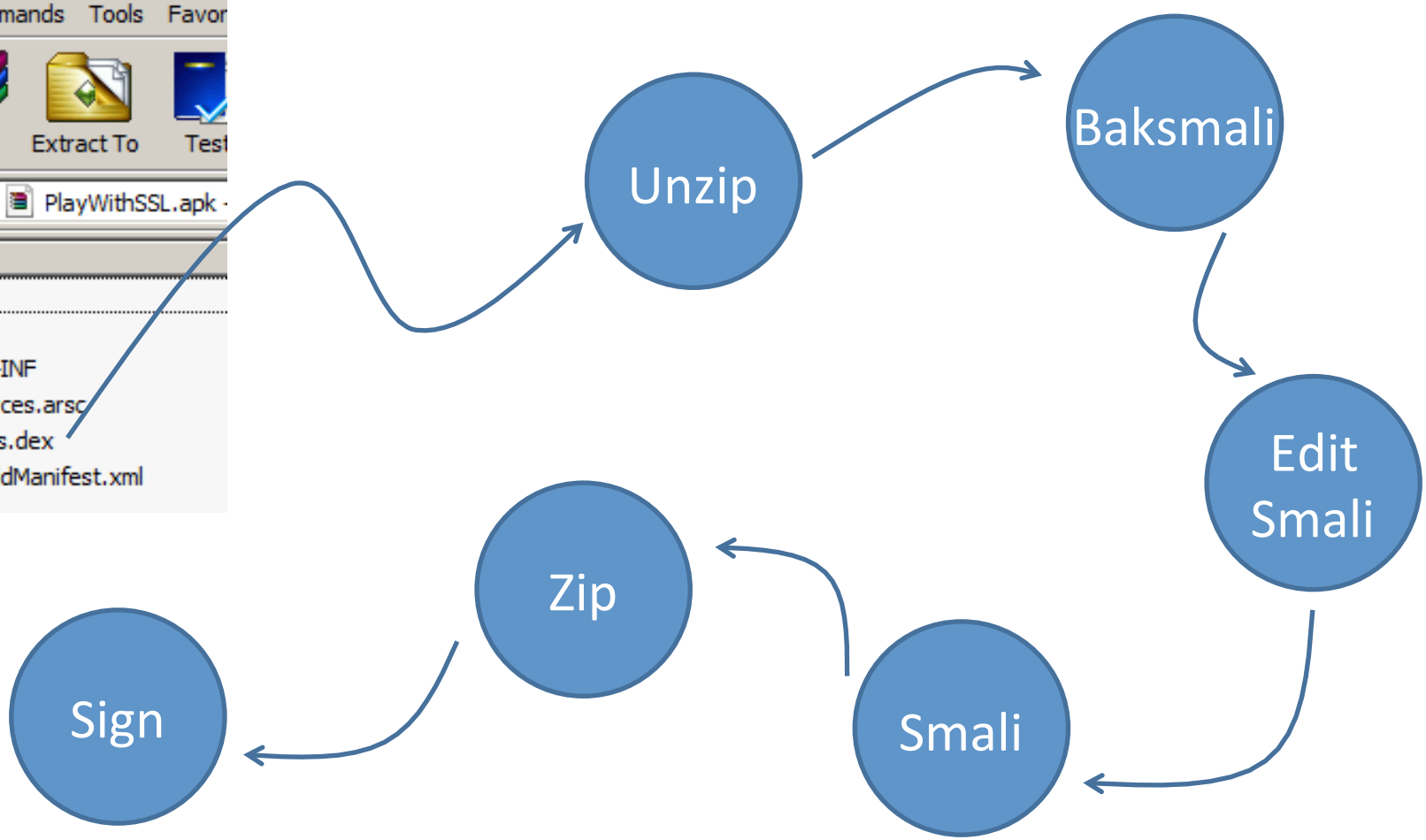
```
import java.io.PrintStream;

public class HelloWorld
{
  public static void main(String[] paramArrayOfString)
  {
    System.out.println("Hello World!");
  }
}
```

smali - HelloWorld

```
.class public LHelloWorld;

.super Ljava/lang/Object;

.method public static main([Ljava/lang/String;)V
   .registers 2

   sget-object v0, Ljava/lang/System;->out:Ljava/io/PrintStream;
   const-string v1, "Hello World!"

   invoke-virtual {v0, v1}, Ljava/io/PrintStream;->println(Ljava/lang/String;)V

   return-void
.end method
```

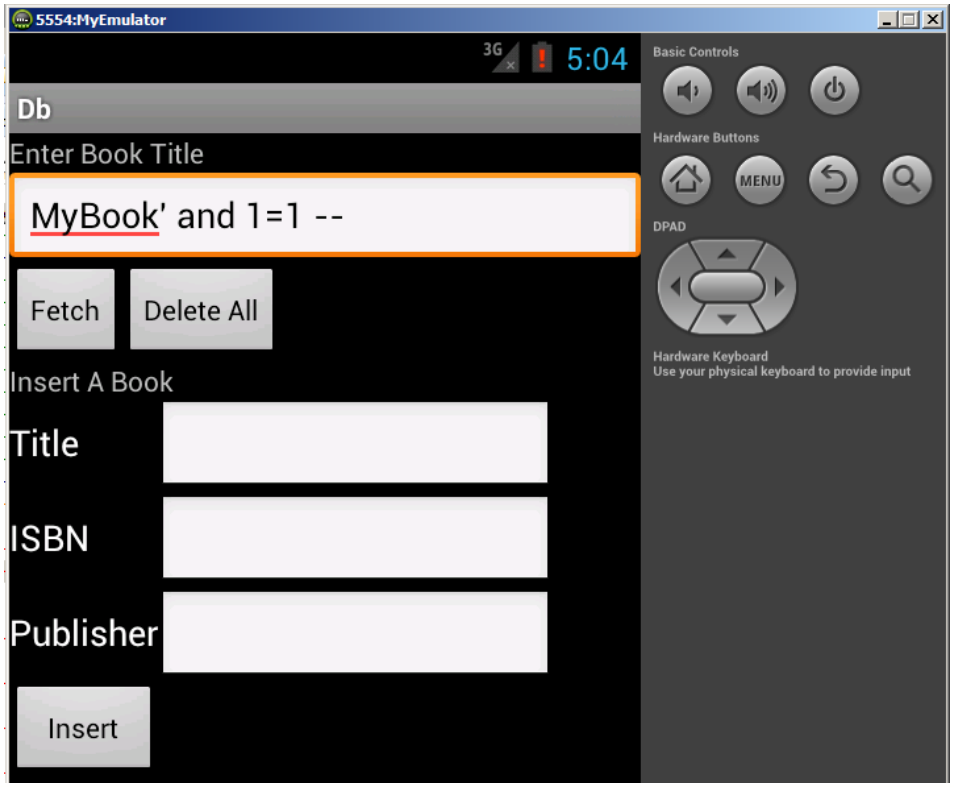
apk -> smali ->apk





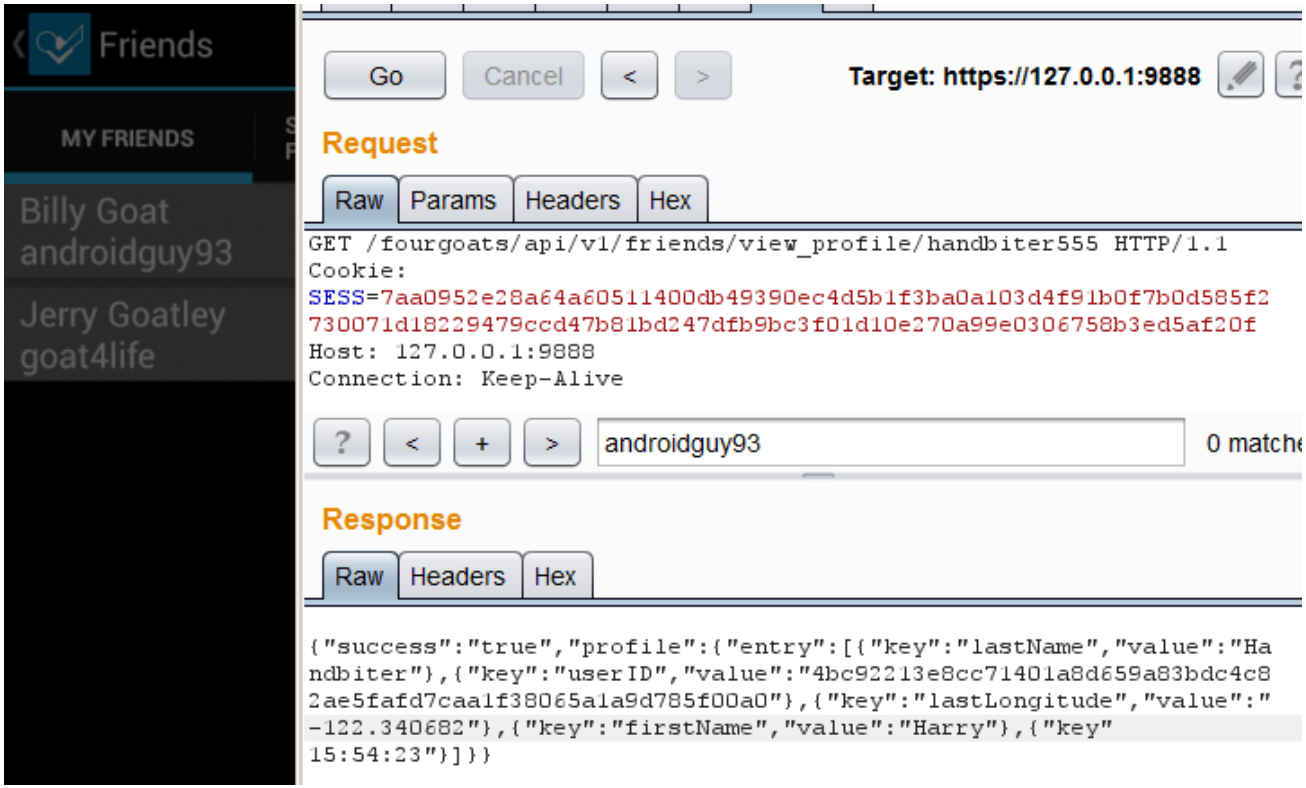
Enjeksiyon - İstemci

- SQL enjeksiyonu Android uygulamalarda da bulunabilecek bir zafiyet çeşididir.



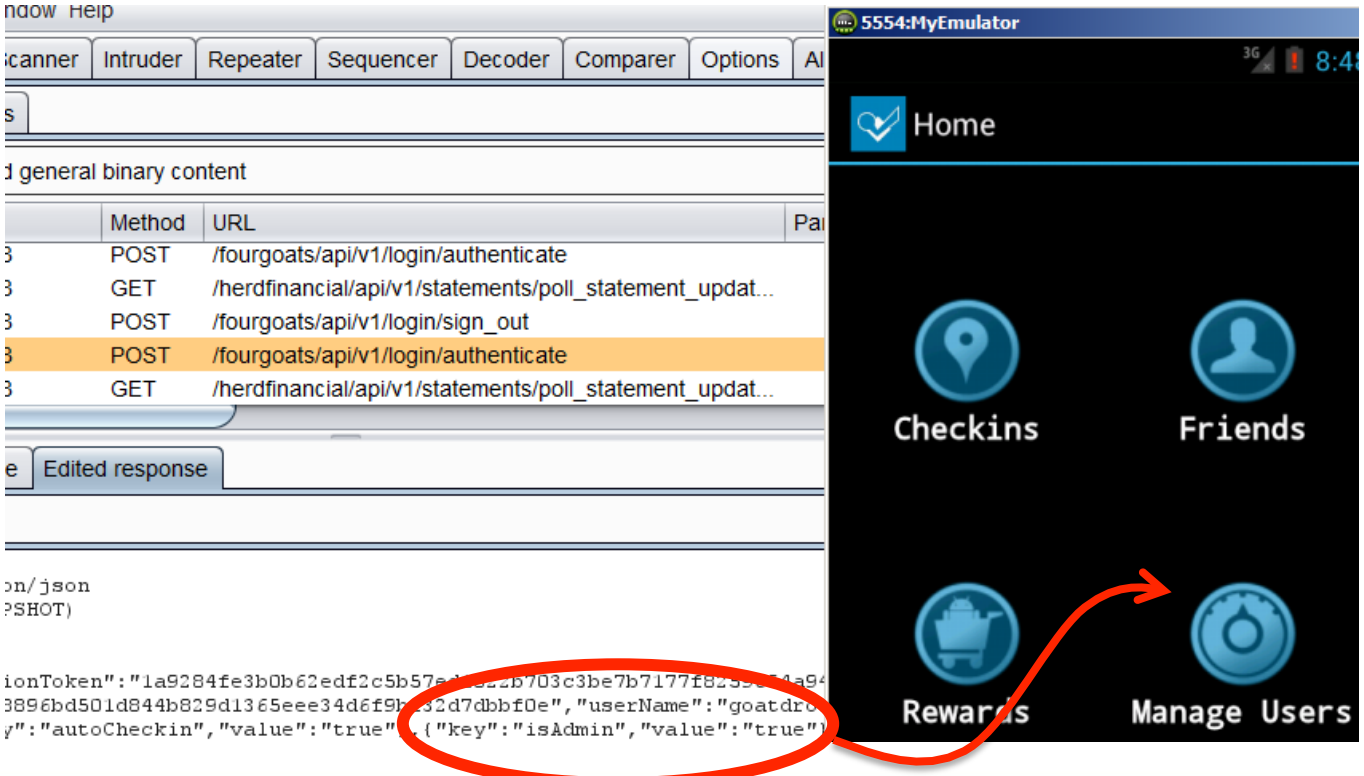
Yetersiz Yetkilendirme - Sunucu

- Yetkilendirme kontrolleri sunucu tarafında eksiksiz gerçekleştirilmelidir.



Yetersiz Yetkilendirme - Sunucu

- Yetkilendirme kontrolleri sunucu tarafında eksiksiz gerçekleştirilmelidir.



LogCat Bilgi Sızdırma

- Yapılan işlemler sonucu hassas bilgiler LogCat mekanizmasında kayıt altına alınmamalıdır.

```
I 06-2...  dalvikvm  Wrote stack traces to '/data/anr/traces.txt'
I 06-2...  Trans...  Member Accounts [123456789 (debit): 169.0] [987654321 (credi
                     t): 931.0]
I 06-2...  Trans...  Response code for transfer: -1
I 06-2...  Trans...  Transferred $12.0 from account 123456789 to account 98765432
                     1
I 06-2...  Banki...  Accounts:
I 06-2...  Banki...  123456789 (debit): 157.0
I 06-2...  Banki...  987654321 (credit): 943.0
D 06-2...  dalvikvm  GC_CONCURRENT freed 357K, 7% free 9845K/10567K, paused 6ms+3
                     4ms
D 06-2...  webvi...  nativeDestroy view: 0x33a350
```

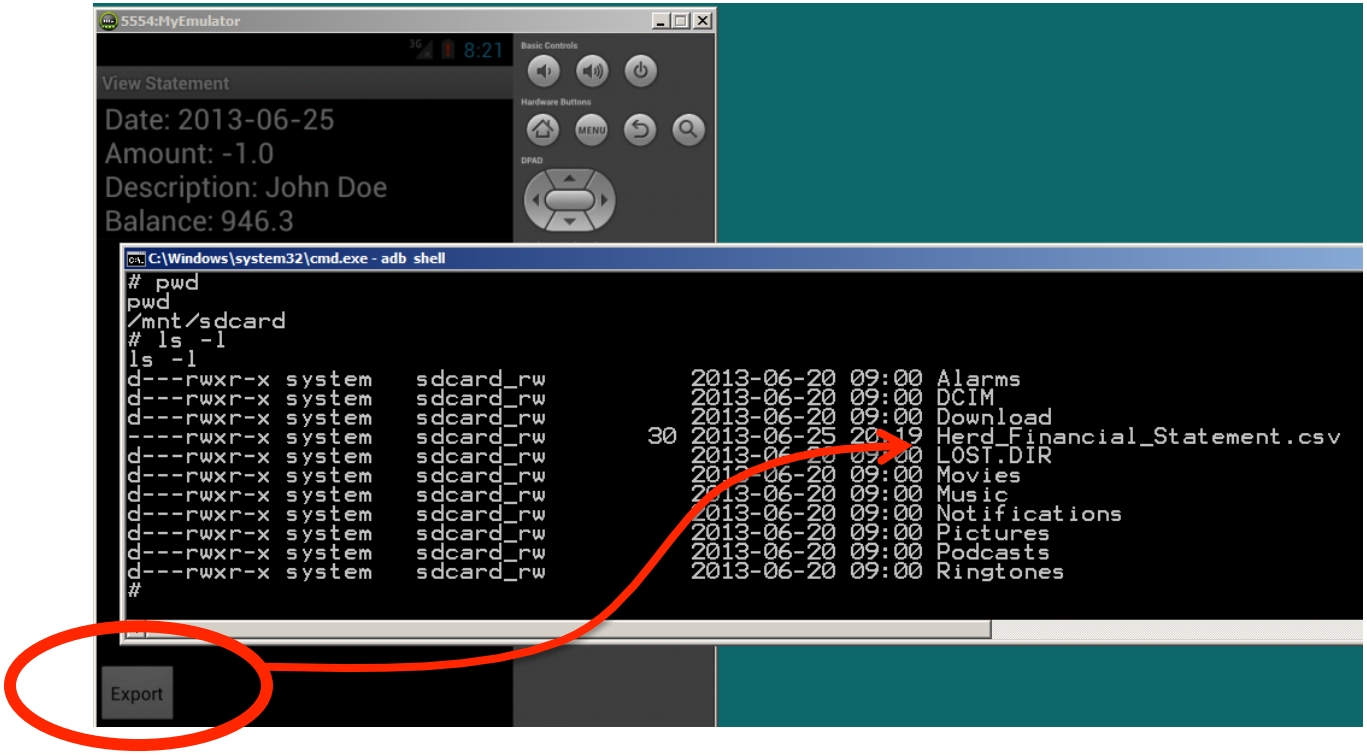
Güvensiz Veri Saklama

- Kullanıcı şifreleri, kredi kartı numaraları, kişisel bilgiler shared_prefs gibi yapılar açık saklanmamalıdır.

```
# pwd
pwd
/data/data/org.owasp.goatdroid.fourgoats/shared_prefs
# cat credentials.xml
cat credentials.xml
<?xml version='1.0' encoding='utf-8' standalone='yes'
<map>
<string name="password">goatdroid</string>
<boolean name="remember" value="true" />
<string name="username">goatdroid</string>
</map>
```

Güvensiz Veri Saklama

- SDCard Android sandbox'ının uygulanmadığı güvensiz bir veri alanıdır.



Güvensiz Veri Transferi

- Hassas bilgiler HTTP üzerinden iletilmemelidir.
- SSL bağlantı problemler nedeniyle özel sınıflar kullanılmamalıdır.

```
try {
    KeyStore trustStore = KeyStore.getInstance(KeyStore.getDefaultType());
    trustStore.load(null, null);
    SSLSocketFactory sf = new CustomSSLSocketFactory(trustStore);
    sf.setHostnameVerifier(SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER);
    SchemeRegistry registry = new SchemeRegistry();
    registry.register(new Scheme("https", sf, 443));
```

1

2

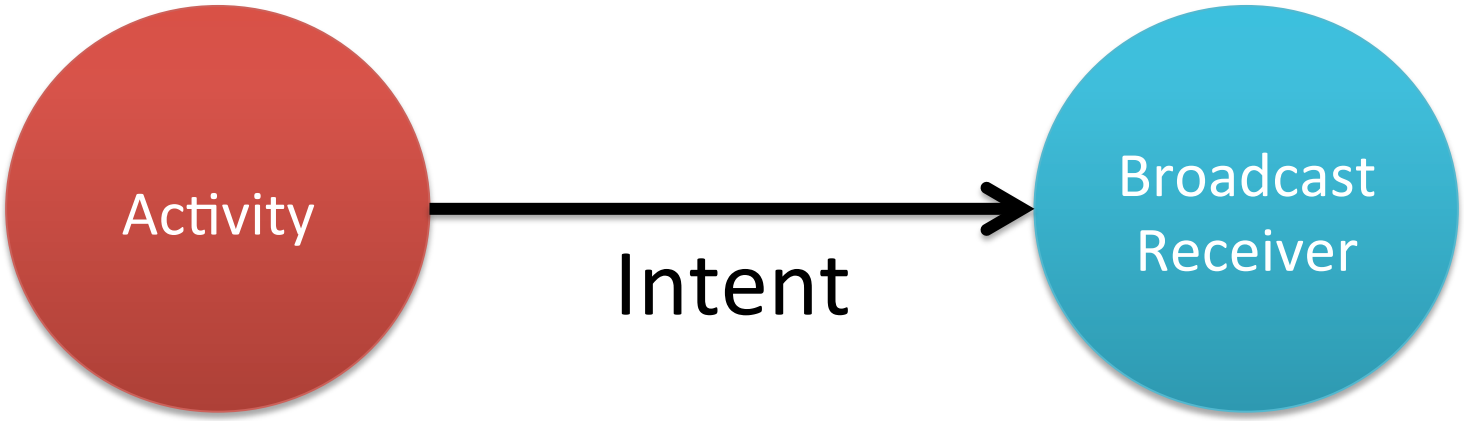
```
try {
    AllowAllHostnameVerifier aahv = new AllowAllHostnameVerifier();
    URL url = new URL(target);
    HttpsURLConnection con = (HttpsURLConnection) url.openConnection();
    con.setHostnameVerifier(aahv);
```

Android Bileşenler

- Android uygulamalarında dört temel bileşen
  - Activity
    - kullanıcıların iletişim kurduğu arayüz
  - Service
    - arkaplanda iş yapan bileşen
  - Content Provider
    - veri sunan servisler, veritabanı
  - Broadcast Receiver
    - iş için komut bekleyen bileşen

Intent

- Bileşenler arası iletişim Intent'ler ile sağlanır



Özel veya Açık Bileşenler

- Uygulamalar bileşenlerini sisteme AndroidManifest.xml dosyası ile tanıtırlar
- Bileşen tanımlarında
  - export attribute'unun değeri True ise veya
  - extra Intent tanımları içeriyorsa,

  ilgili bileşeni diğer uygulamalar da çağırabilir
- Özel bir bileşen sadece aynı uygulamadan çağrılabilir

Örnek Bileşen Tanımı 1

- .mydb Content Provider bileşeni export attribute'u True olduğundan diğer uygulamalar tarafından çağrılabilir

```
<manifest ...>
   <provider android:name=".mydb" android:exported="true">
         <intent-filter>
         </intent-filter>
   </provider>
</manifest>
```

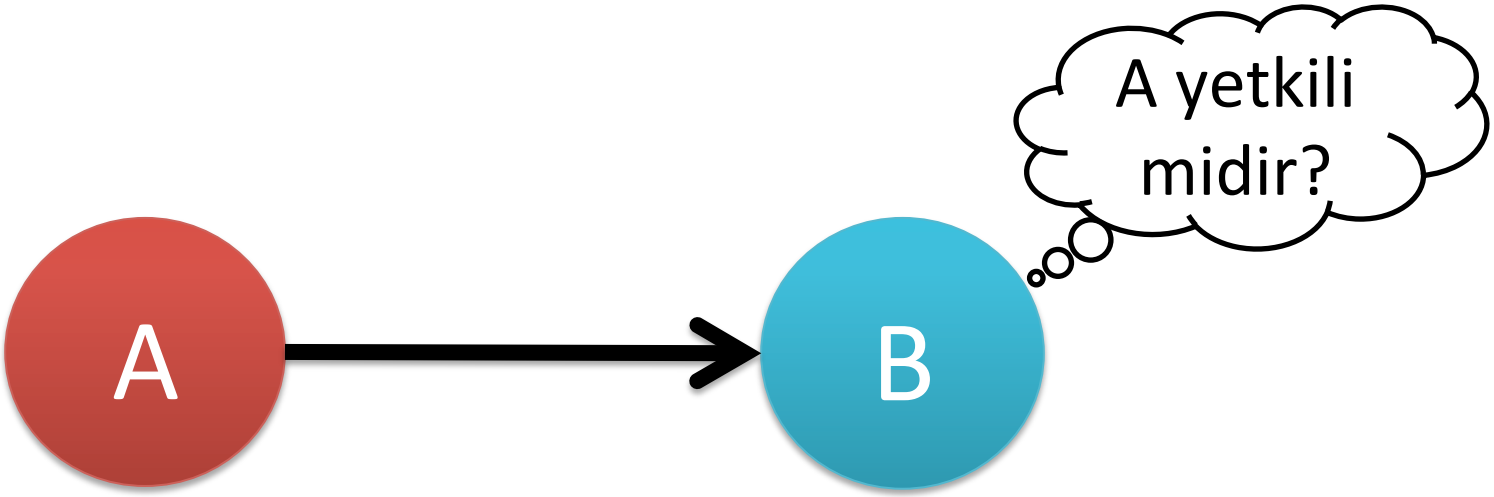
Örnek Bileşen Tanımı 2

- .mysmssender Broadcast Receiver bileşeni export attribute'u True olmasa da, bir Intent ile tetikleneceğini beyan ettiği için açıktır

```
<manifest ...>
  <receiver android:name=".mysmssender">
    <intent-filter>
      <action android:name="android.intent.sendSMS"/>
    </intent-filter>
  </receiver>
</manifest>
```

Bileşenlerin Yetki Kontrolü

- Dolayısıyla hassas işlem yapan Açık (Export=True) bir bileşen, diğer uygulamalar tarafından çağrıldığında yetki kontrolü yapmalıdır



Güvensiz IPC

- Componentlar arasındaki gerekli yetkilendirme kontrolleri gerçekleştirilmelidir.

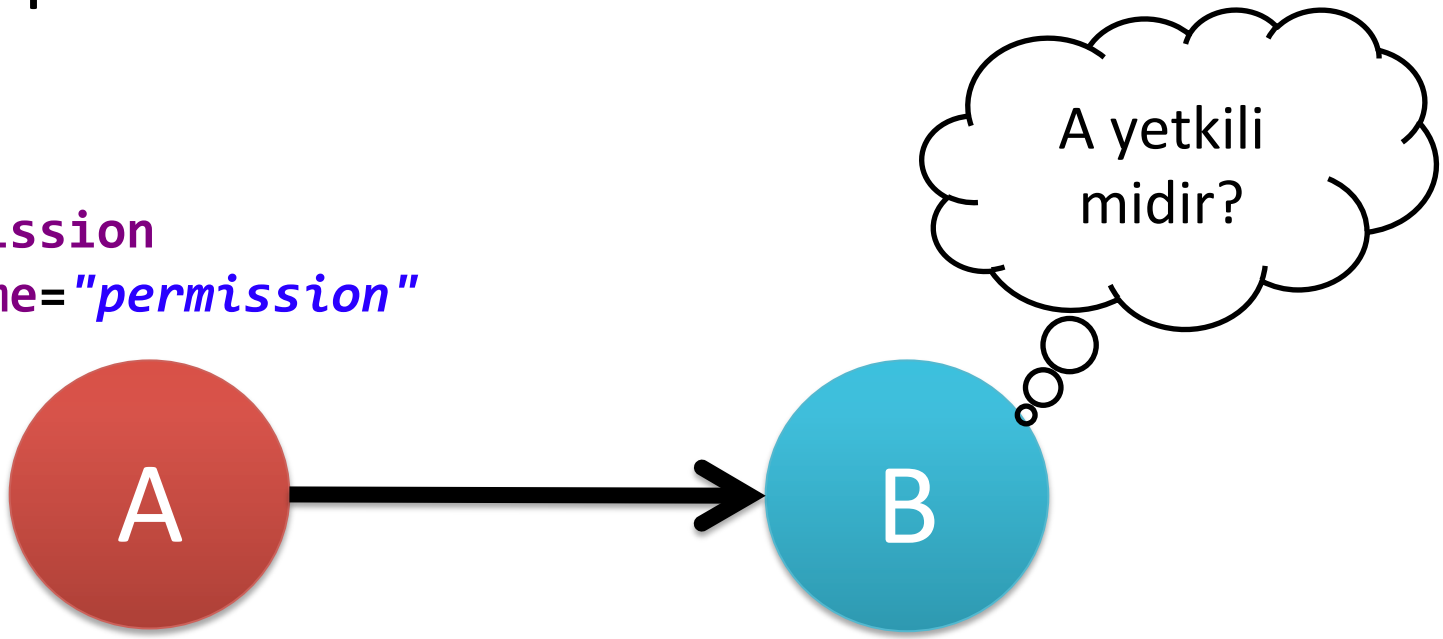
```
    <service android:name=".services.LocationService" >
        <intent-filter>
            <action android:name="org.owasp.goatdroid.fourgoats.services.Locat
        </intent-filter>
    </service>

    <receiver
        android:name=".broadcastreceivers.SendSMSNowReceiver"
        android:label="Send SMS" >
        <intent-filter>
            <action android:name="org.owasp.goatdroid.fourgoats.SOCIAL_SMS" />
        </intent-filter>
        >
    </receiver>
</application>
```

Güvensiz IPC Önlem 1

- normal permission kontrolü

3

```
<uses-permission
android:name="permission"
```



1
```
<permission
android:name="permission" />
```

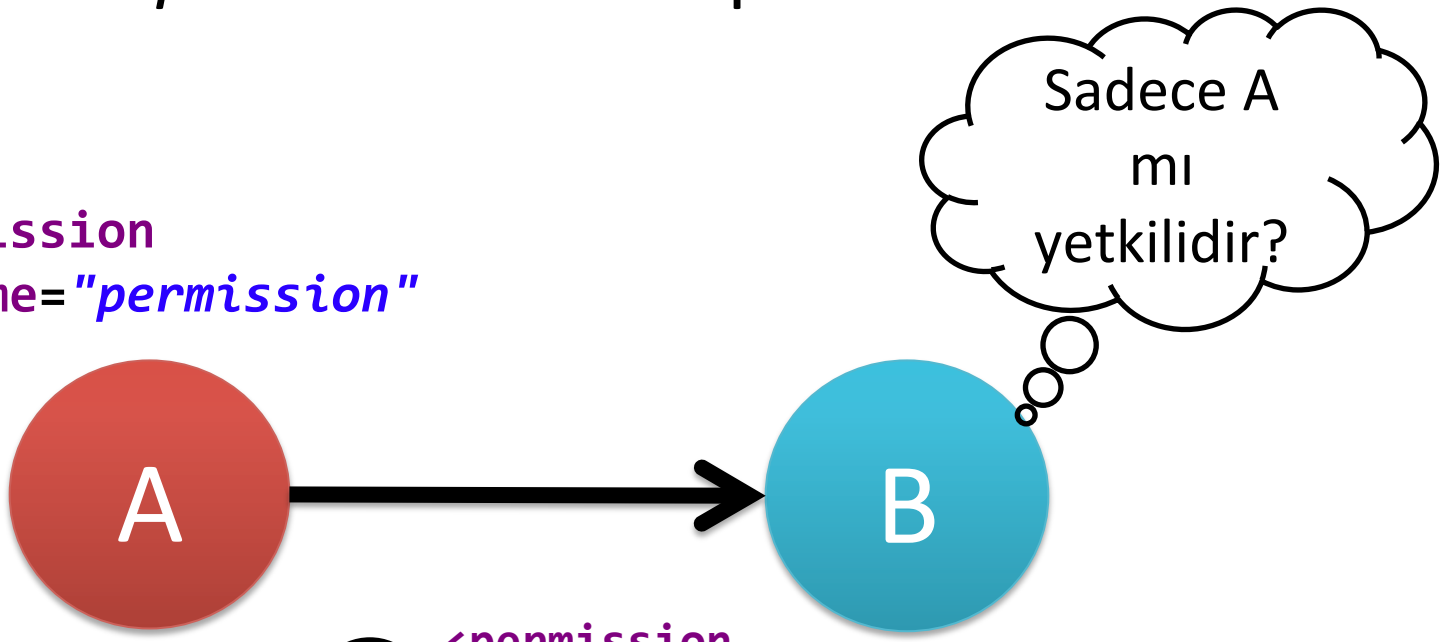
2
```
<receiver
android:permission="permission"
```

Güvensiz IPC Önlem 2

- permission *protectionLevel* ipucu

3

```
<uses-permission
android:name="permission"
```



1

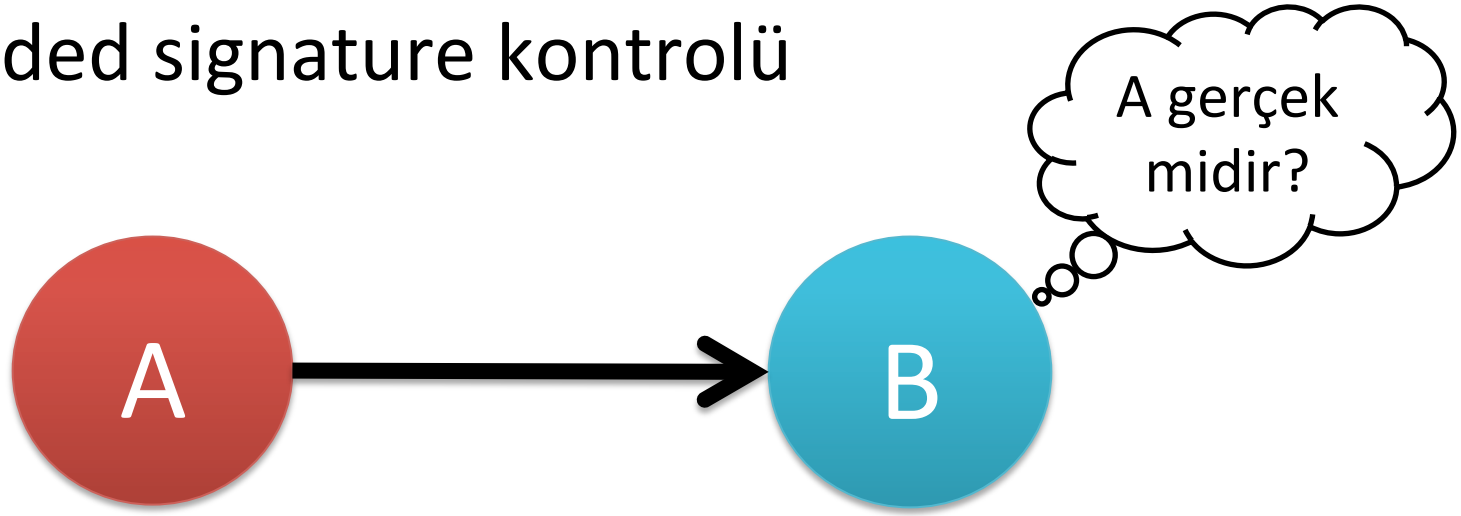
```
<permission
android:name="permission"
android:protectionLevel="signature" />
```

2

```
<receiver
android:permission="permission"
```

Güvensiz IPC Önlem 3

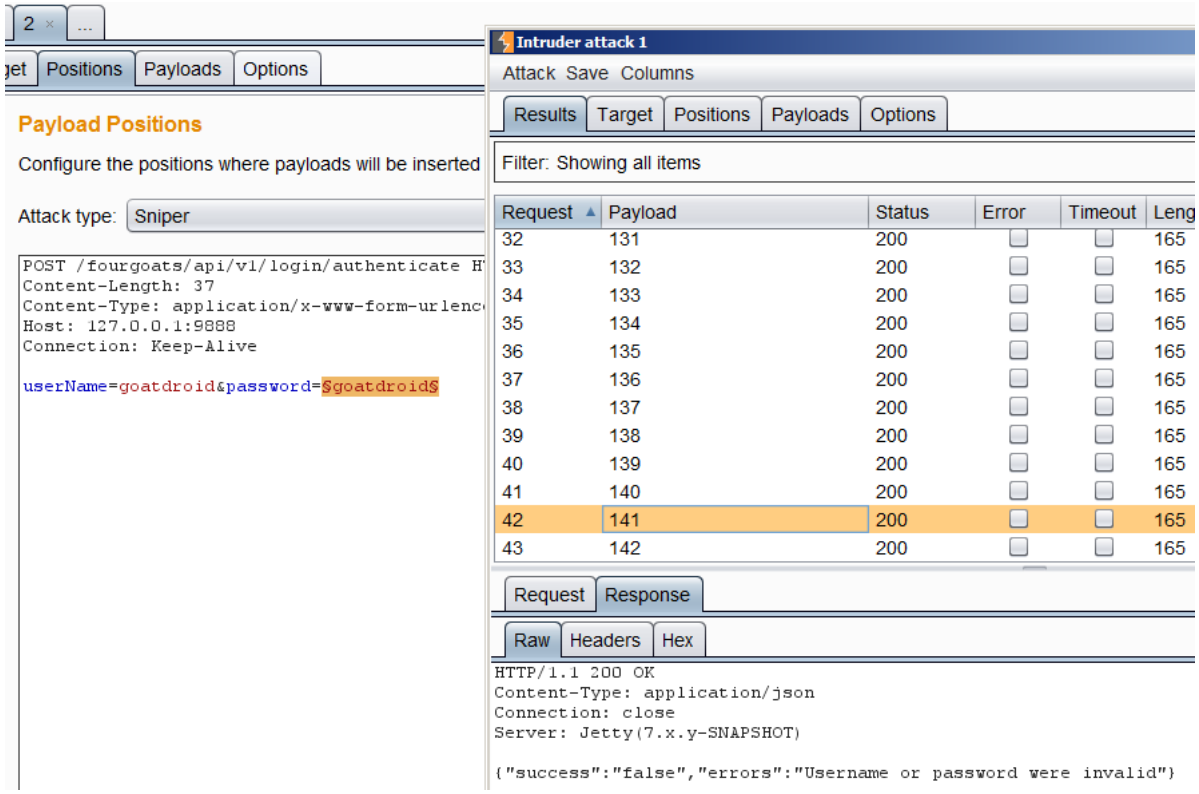
- hardcoded signature kontrolü




```
packageInfo = pm.getPackageInfo(A_PkgName,
                PackageManager.GET_SIGNATURES);

String A_SIGNATURE = "308202...";

for (Signature signature : packageInfo.signatures)
   if (signature.toCharsString().equals(A_SIGNATURE)) {
   }
```

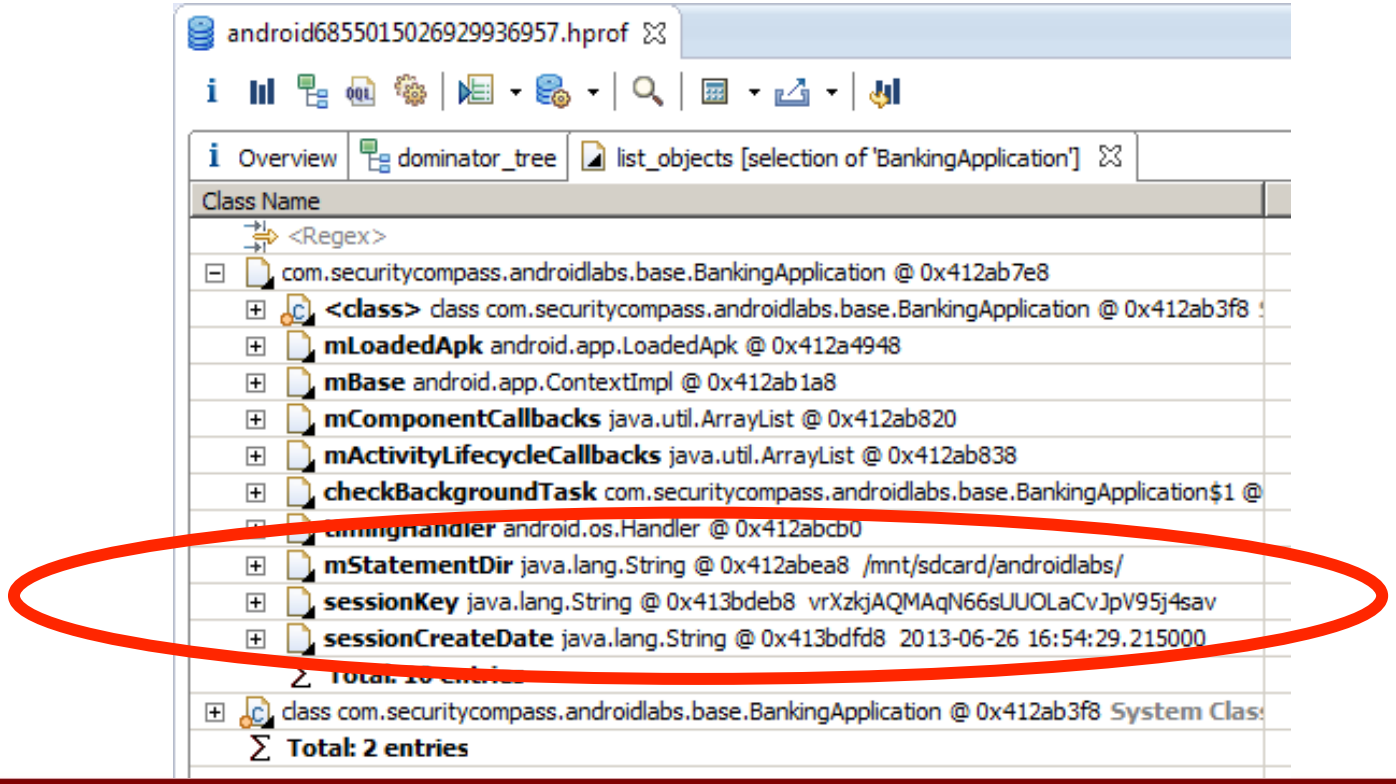
Yetersiz Anti-Otomasyon

- Özellikle login işlemleri, deneme-yanılma saldırılarına açık olmamalıdırlar.

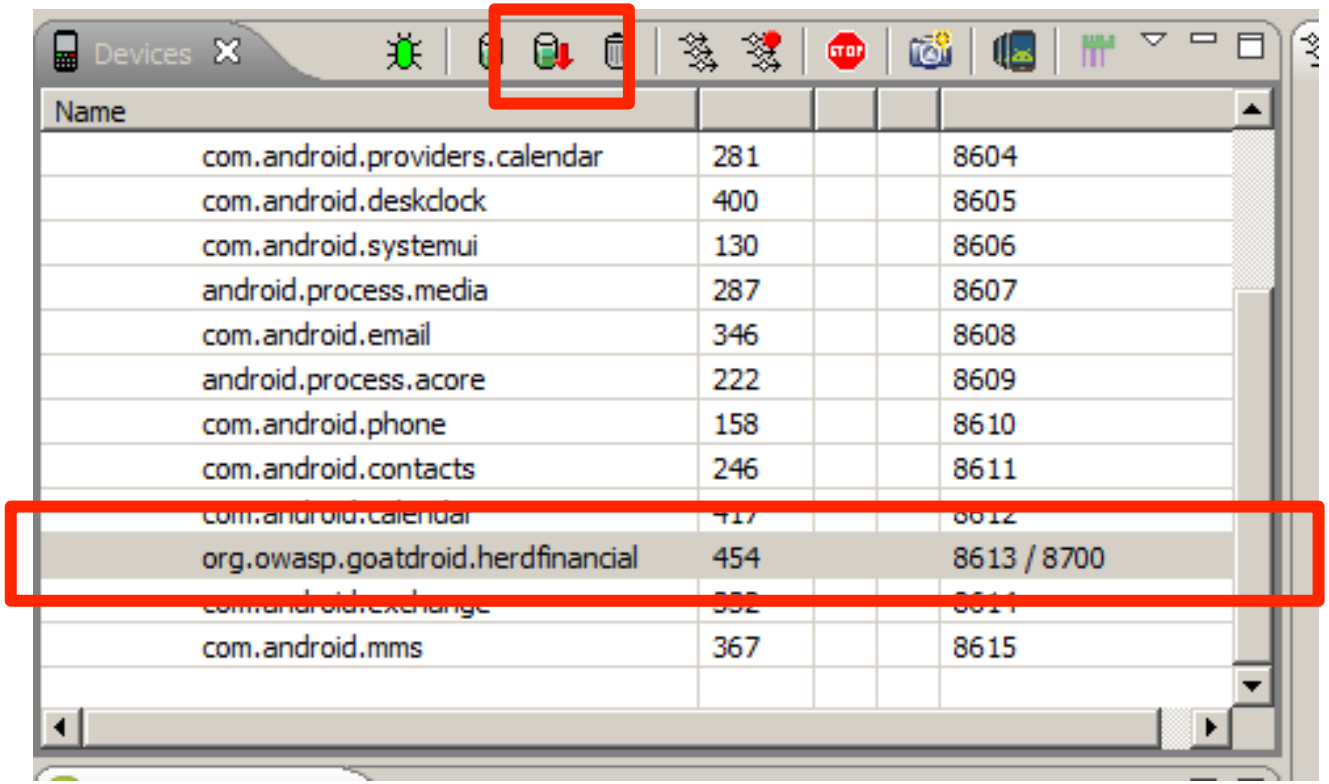


Memory Analizi

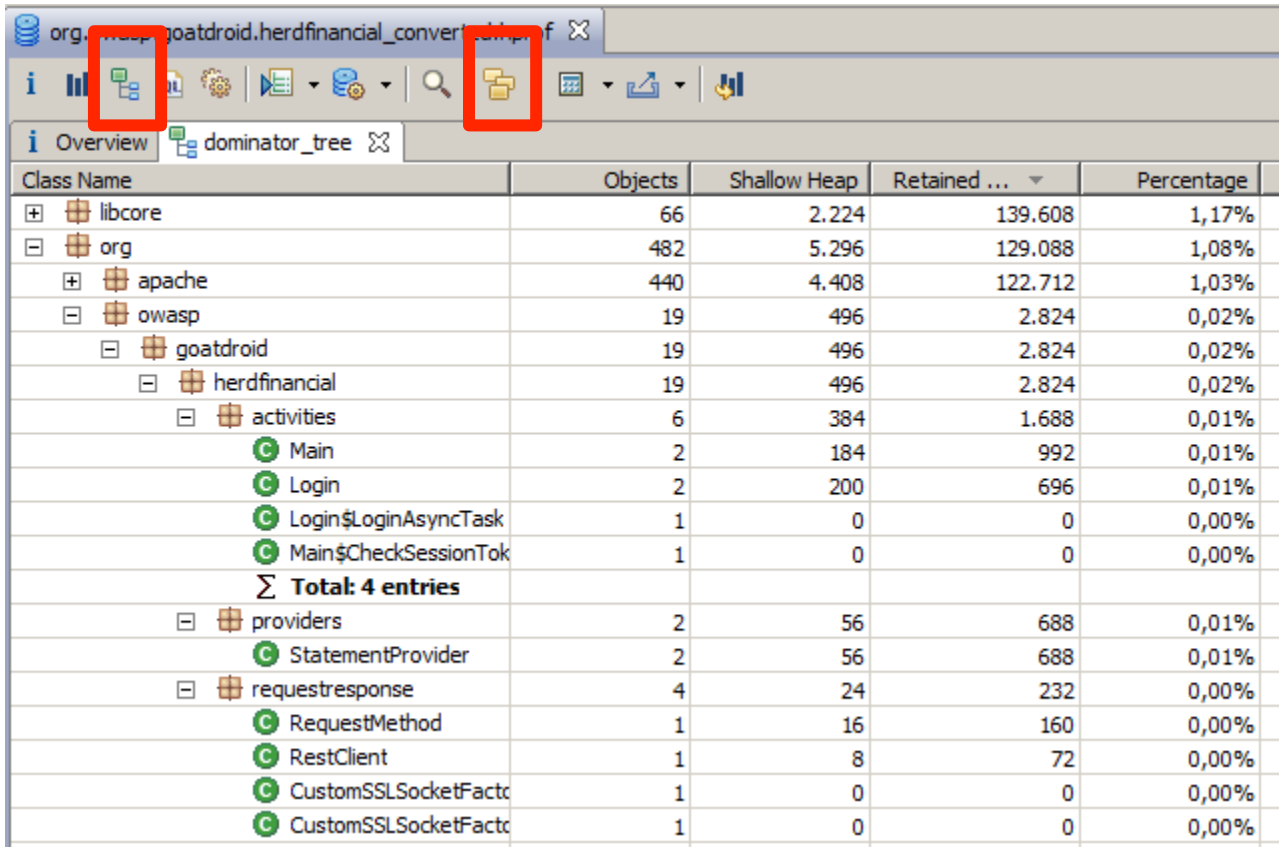
- Eclipse MAT ile uygulamaların heap memory analizi gerçekleştirilebilir.



DDMS Ekranı - Hprof Dump



MAT Ekranı - Dominator Tree



Overview | dominator_tree

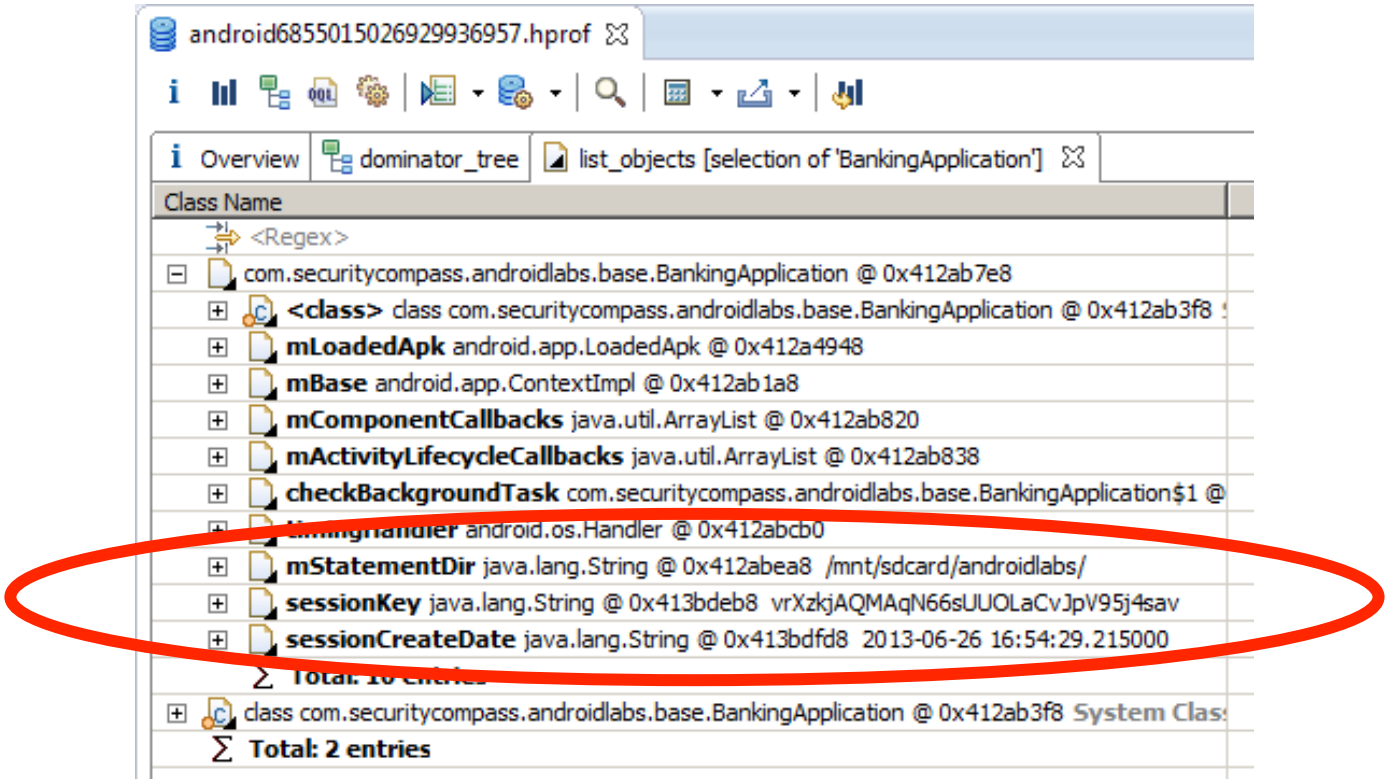
Class Name	Objects	Shallow Heap	Retained ...	Percentage
libcore	66	2.224	139.608	1,17%
org	482	5.296	129.088	1,08%
apache	440	4.408	122.712	1,03%
owasp	19	496	2.824	0,02%
goatdroid	19	496	2.824	0,02%
herdfinancial	19	496	2.824	0,02%
activities	6	384	1.688	0,01%
Main	2	184	992	0,01%
Login	2	200	696	0,01%
Login$LoginAsyncTask	1	0	0	0,00%
Main$CheckSessionTok	1	0	0	0,00%
Total: 4 entries				
providers	2	56	688	0,01%
StatementProvider	2	56	688	0,01%
requestresponse	4	24	232	0,00%
RequestMethod	1	16	160	0,00%
RestClient	1	8	72	0,00%
CustomSSLSocketFactc	1	0	0	0,00%
CustomSSLSocketFactc	1	0	0	0,00%

MAT Ekranı - DT - List Objects

org	482	5.296	129.088	1,08%
apache	440	4.408	122.712	1,03%
owasp	19	496	2.824	0,02%
goatdroid	19	496	2.824	0,02%
herdfinancial	19	496	2.824	0,02%
activities	6	384	1.688	0,01%
Main	2	184		
Log				
Log				
Ma				
Total				
provide			688	0,01%
Sta			688	0,01%
reques			232	0,00%
Re			160	0,00%
Re			72	0,00%
Cu			0	0,00%
Cu			0	0,00%
Total				
db			216	0,00%
base			0	0,00%
Re			0	0,00%
Ba			0	0,00%
Total: 2 entries				

- List objects
  - with outgoing references
  - with incoming references
- Show objects by class
- Merge Shortest Paths to GC Roots
- Java Basics
- Java Collections
- Leak Identification
- Immediate Dominators
- Show Retained Set
- Copy
- Search Queries...
- Calculate Minimum Retained Size (quick approx.)
- Calculate Precise Retained Size
- Columns...

MAT Ekranı - DT - List Objects



SMALI - Log Injection

- APKSmash iki amaç için kullanılabilir;
  - Hedef APK içerisinde telefon numaraları, IP adresleri, URL'leri ve kayıt işlemlerine ait incelenebilecek bazı bilgileri
  - Hedef uygulamayı patchleyerek runtime'da LogCat mekanizmasına bir çok kayıt atılmasını sağlar. Bu şekilde uygulama hakkında detaylı bir çok dinamik bilgi elde edilebilir

SMALI - Log Injection

- APKSmash için iLogger ve APKTool araçları gerekmektedir
- Hedef uygulamanın APK'sı belirlendikten sonra;
  1. apktool ile decode edilir
  2. apksmash.py, decode edilen dizinde, kod içerisinde aşağıdaki değişiklik ile çalıştırılır

JonestownThisAPK = ~~False~~True

SMALI - Log Injection

3. Aynı dizinde oluşturulan apk-ig-info.txt dosyası ilginç bazı bulgular için analiz edilebilir
4. Kayıt enjeksiyonu için iglogger.smali dosyası smali dizinine kopyalanır
5. apktool kullanılarak dizin build edilir ve imzalanır
6. Elde edilen apk, emulator'e kurulduktan sonra çalıştırmadan önce incelenmek için adb logcat açılır
7. adb logcat çıktıları, uygulama kullanıldıkça izlenir

SMALI - Log Injection

- apksmash ile enjekte edilen log metotları, logcat ile hassas bazı bilgileri açığa çıkarabilir

```
rnal.view.IInputMethodClient$Stub$Proxy@4158c638 (uid=10013 pid=593)

o -2
02): !!! IGTraceLogger in Method: org.webguvenligi.db.DbActivity$1->onClick
: !!! IGTraceLogger in Method: org.webguvenligi.db.DBAdapter-><init> Line 20
Line 15( 1302): !!! IGTraceLogger in Method: org.webguvenligi.db.DBAdapter$
!!! IGTraceLogger in Method: org.webguvenligi.db.DBAdapter->open Line 35

2): !!! IGTraceLogger in Method: org.webguvenligi.db.DBAdapter->getTitle Line
02): SELECT DISTINCT _id, isbn, title, publisher FROM titles WHERE title='a'

!!! IGTraceLogger in Method: org.webguvenligi.db.DBAdapter->close Line 21
```

CCRAWL - Kaynak Kod Analizi

- Kaynak kodu elde olan veya decompile edilebilen Android uygulamalar için kaynak kod analizi ile hızlı bir denetim gerçekleştirilebilir
- Açık kaynak kodlu CCRAWL Android uygulamalarında probleme yol açabilecek bazı API'ları otomatik olarak göstermektedir

CCRAWL - Android APIs

- Privacy Violation
  - Log
- SQL Injection
  - rawQuery, query
- Eksik BroadcastReceiver İzinleri
  - registerReceiver, sendBroadcast, sendOrderedBroadcast
- Kod Enjeksiyonu
  - DexClassLoader

CCRAWL - Android APIs

- SDCard Dosya İşlemleri
  - android.permission.WRITE_EXTERNAL_STORAGE
  - android.permission.READ_EXTERNAL_STORAGE
  - getExternalStorageDirectory
- Şüpheli Geo-Lokasyon İşlemleri
  - android.permission.ACCESS_COARSE_LOCATION
  - android.permission.ACCESS_FINE_LOCATION
  - requestLocationUpdates, getLastKnownLocation

CCRAWL - Android APIs

- Süpheli SMS İşlemleri
  - android.permission.SEND_SMS
  - android.permission.WRITE_SMS
  - sendTextMessage(
  - content://sms/inbox
- Özel SSL Denetimi
  - SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER
  - checkServerTrusted, checkClientTrusted
  - setHostnameVerifier, AllowAllHostnameVerifier

CCRAWL - Android APIs

- Bilgi İfşası
  - setData, getData, putExtra, getExtras
- XSS
  - setJavaScriptEnabled, addJavaScriptInterface
- Hassas İşlemler
  - getCallState, getCellLocation, getDeviceId, getLine1Number, getSimSerialNumber, Intent.ACTION_CALL, SmsManager, ContactsContract, LocationManager