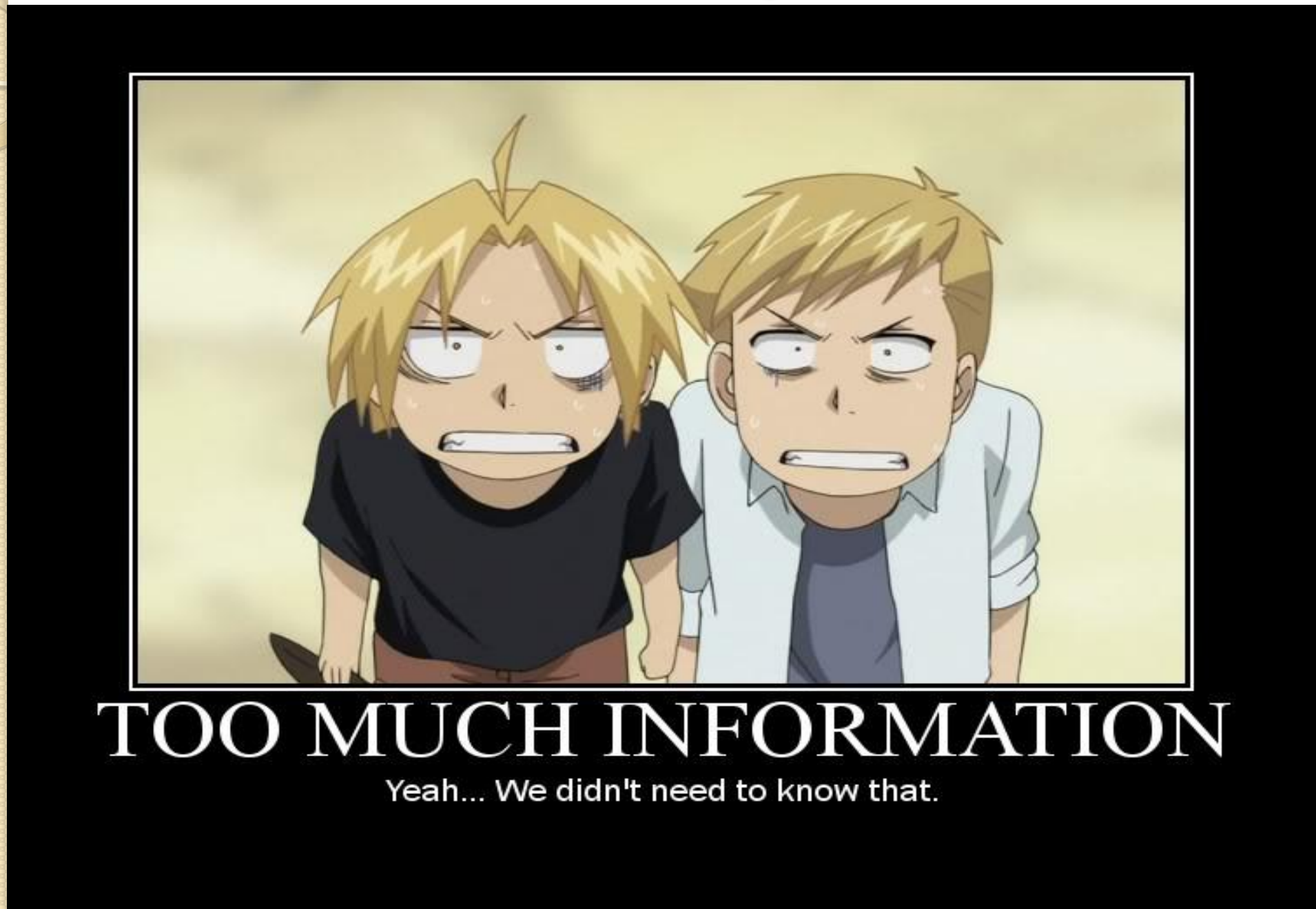
InfoMAR

REVERZNI INŽENJERING ANDROID APLIKACIJA

Dinko Korunić @ InfoMAR

Previše informacija!



Što čini Android platformu

- Application framework:
  - modularnost, komponentni dizajn, laka izmjena i/ili nadogradnja komponenti
  - **Views** (gradivne jedinice tipa text-boxevi I sl.), **Content Providers** (pristup informacijama i dijeljenje istih), **Resource Manager** (pristup datotekama koje nisu dio koda projekta tipa layouti i sl.), **Notification Manager** (notifikacije na status baru), **Activity Manager** (navigacija aplikacije i životni ciklus aplikacije)

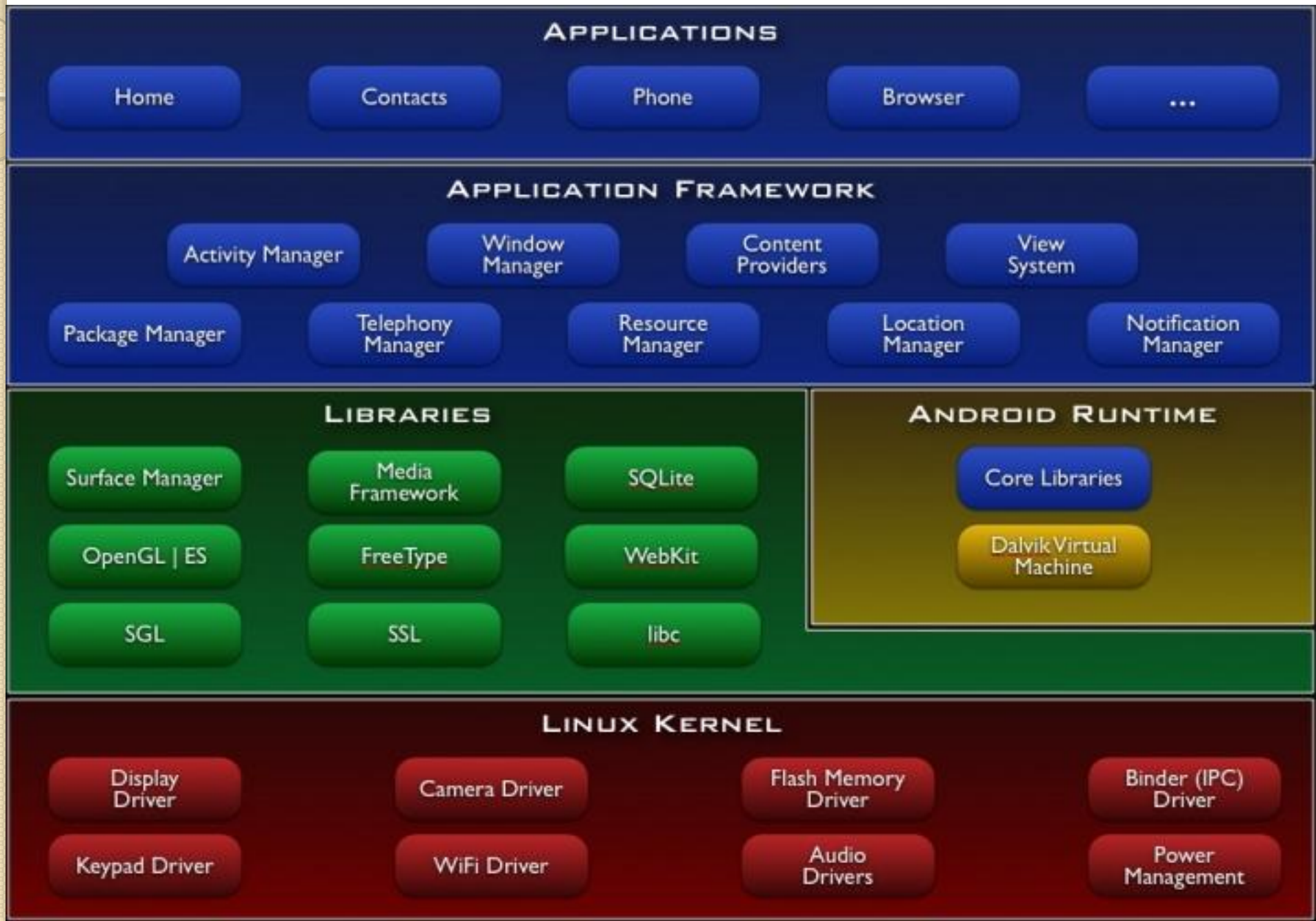
Što čini Android platformu (2)

- **Dalvik VM**
- **Linux kernel 2.6**!
- Web preglednik – **WebKit**
- grafički custom 2D i 3D (OpenGL ES) podsustav
- **SQLite** za spremište
- multimedija (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)
- GSM, Bluetooth, EDGE, 3G, WiFi

Što čini Android platformu (3)

- kamera, GPS, kompas, akcelerometar
- IDE, alati za debugiranje, profiliranje, emulator (**Qemu**)
- dodaci za Eclipse, Netbeans
- CLI alati: **adb**, **fastboot**, zipalign, itd.
- niz gotovih Google aplikacija (**Gapps**) u svakoj standardnoj instalaciji

Android arhitektura



Biblioteke

- Java classlib:
  - **Apache Harmony**
  - clean-room implementacija
- System C lib / libc:
  - **Bionic**
  - BSD derivat (dlmalloc, itd.)
  - Glibc prevelik, uClibc ima LGPL “problem”
  - nije POSIX compliant!
  - vrlo lagan i optimiziran za ARM i x86
  - djelomična / nepotpuna multicore podrška

Biblioteke (2)

- System C lib / libc:
  - nešto Linux kernel headera zbog ioctl-ova
  - nema C++ exceptiona, nema STL
  - poseban libpthread (kernel futexi!)
  - nema passwd i groups datoteke
  - UID/GID >10000 za svaku pojedinu aplikaciju, <10000 su sistemski servisi
  - **properties** kao globalni key/value store umjesto environment varijabli
  - poseban DNS resolver (nema NSS, npr.)

Biblioteke (3)

- Media libs:
  - PacketVideo **OpenCORE**
  - različiti audio/video formati, statičke datoteke, itd.
- **LibWebCore**:
  - WebKit baziran WebView i preglednik
- ostalo:
  - SGL, OpenGL ES
  - **FreeType**, **SQLite**

Dalvik VM

- **process VM**
  - instancira i gasi se sa aplikacijom
- **register-based VM**
- aplikacije
  - u Dalvik EXecutable .dex obliku
  - optimizirano za mali prostor i spori CPU
- **dx** alat:
  - prevodi iz Java u .dex format (kompresija, 4-bajtno poravnanje + Dalvik bytecode)
  - više klasa u jednoj .dex datoteci

Dalvik VM (2)

- 16-bitni instrukcijski set i radi isključivo na **lokalnim varijablama**
- varijable – 4-bitni virtualni registar
- **JIT** – od 2.2 Androida naviše
- VM ne odlučuje o sigurnosti već samo OS, jedino provjerava bytecode radi optimizacija
- Gabor Paller: Understanding the Dalvik bytecode with the Dedexer tool: http://goo.gl/ck16

Dalvik VM (3)

```
26 0x62 const/4 v10 , [#+ 0] , {0}
27 0x64 if-lt v10 , v9 , [+ 16]
28 0x68 return-void
29 0x6a aget-object v9 , v8 , v1
30 0x6e check-cast v9 , [type@ 319 [B]
31 0x72 invoke-static v9 , [meth@ 172 Landroid/telephony/gsm/SmsMessage; ([B) Landroid/telephony/gsm/SmsMessage;
createFromPdu]
32 0x78 move-result-object v9
33 0x7a aput-object v9 , v7 , v1
34 0x7e add-int/lit8 v1 , v1 , [#+ 1]
35 0x82 goto [+ -20]
36 0x84 aget-object v5 , v7 , v10
37 0x88 invoke-virtual v5 , [meth@ 173 Landroid/telephony/gsm/SmsMessage; () Ljava/lang/String; getDisplayOrigina
tingAddress]
38 0x8e move-result-object v6
39 0x90 const-string v11 , [string@ 72 '10086']
40 0x94 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
41 0x9a move-result v11
42 0x9c if-nez v11 , [+ 42]
43 0xa0 const-string v11 , [string@ 70 '10000']
44 0xa4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
45 0xaa move-result v11
46 0xac if-nez v11 , [+ 34]
47 0xb0 const-string v11 , [string@ 71 '10010']
48 0xb4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
49 0xba move-result v11
50 0xbc if-nez v11 , [+ 26]
51 0xc0 const-string v11 , [string@ 75 '1066185829']
52 0xc4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
53 0xca move-result v11
54 0xcc if-nez v11 , [+ 18]
55 0xd0 const-string v11 , [string@ 74 '1066133']
56 0xd4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
57 0xda move-result v11
58 0xdc if-nez v11 , [+ 10]
59 0xe0 const-string v11 , [string@ 73 '106601412004']
60 0xe4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
61 0xea move-result v11
62 0xec if-eqz v11 , [+ 5]
```

Android aplikacije

- **SDK** – Java kao frontend
- **NDK** – C/C++ & Bionic
- sastoje se od kompiliranog koda i resursa
- komponente:
  - komuniciraju kroz **Intentove**
  - Activity, Broadcast Receiver, Service, Content Provider
- **Reference Monitor** – MAC enforce
  - komponente imaju različite dozvole

Android aplikacije (2)

- komunikacija
  - aplikacija provjerava listu dozvola za odredište
  - među komponentama ili broadcast (globalno slanje poruke) koju framework prenosi prema pojedinoj komponenti
  - ovisno o akciji sistem poziva pojedine komponente za izvršenje
- AndroidManifest.xml
  - razvijatelj: Permission, Intent-Filters
  - za **PackageManager** i **ActivityManager**

Sigurnosni model

- jedinstveni UID i GID za svaku aplikaciju prilikom instalacije
- dozvole kroz korisnikovu ručnu potvrdu ili negaciju (ili sve ili ništa)
- **Linux Process Sandbox** – po aplikaciji
- multi-process system
- dijeljenje informacija / komunikacija – jedino kroz interakciju komponenti odnosno **Intentove** (asinkroni IPC)

Sigurnosni model (2)

- nema pristupa datotekama između aplikacija (osim za specifične ovlasti)
- potpisane developerovim ključem, nažalost može biti self-signed ☹
- dozvole se provjeravaju tijekom:
  - sistemskih poziva
  - početka aktivnosti (Activity)
  - upravljanjem javne objave (Broadcast)
  - povezivanjem ili startanjem servisa
  - pristupanja/korištenja Content Providera

Zaštitni nivoi dozvola

- **Normal**
  - VIBRATE
  - SET_ALARM
- **Signature**
  - FORCE_STOP_PACKAGES
  - INJECT_EVENTS
- **Dangerous**
  - SEND_SMS
  - CALL_PHONE
- **SignatureOrSystem**
  - ACCESS_USB
  - SET_TIME

Potencijalni problemi

- Activity
  - problem sa “zlim” podacima iz Intentova
  - sa predavanjem osjetljivih podataka
- Intent Filter
  - nije sigurnosna granica - problem izvora
  - nužna je ručna validacija ulaza
  - kategorije sužuju skup za dostavu, međutim ne garantiraju sigurnost
- **Pending Intents**
  - kasnije izvršavanje pod originalnim ID-jem

Potencijalni problemi (2)

- aplikacije
  - self-signed, ne koristi se PKI/CA
  - ne postoji samoprovjera potpisa ☹
  - aplikacije “rade” i prepakirane, modificirane, potpisane testnim ključevima
  - problem crnih izvorišta: **Applanet, Mobilism, BlackMart, SnappzMarket, ApkTor**
  - Google nema automatizirani malware scan svih uploadanih aplikacija ☹
- kao i uvijek... PEBKAC!

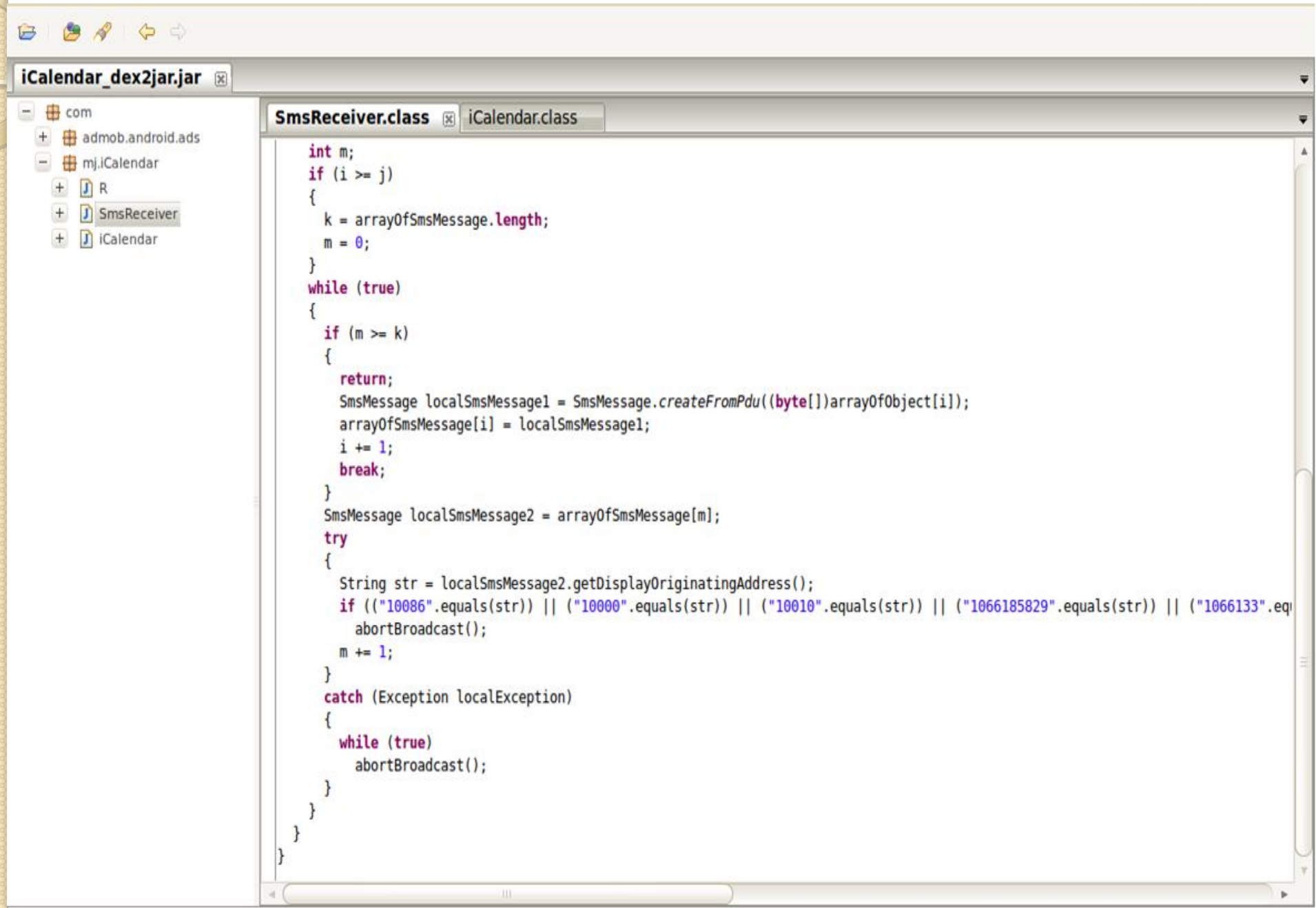
Potencijalni problemi (3)

- nužnost ručnih provjera IPC-a
- razno:
  - curenje osjetljivih informacija u log ring
  - curenje informacija kroz IPC i broadcastove
- VFAT
  - vanjsko spremište
  - nema pristupne kontrole
  - osjetljivi podaci iz aplikacija bi se morali kriptirati

Statička analiza: Dex2Jar

- koristi se sa Java decompilerom poput JD-Core/JD-GUI/JD-Eclipse
- translacija iz dex u jar (http://goo.gl/Qd4MZ), optimizacija, prikaz
- trivijalni dolazak do praktički izvornog koda aplikacije, malwarea, itd.
- što sa modifikacijama, editiranjem, repakiranjem?

Statička analiza: Dex2Jar (2)



Statička analiza: Apktool

- praktički standard.. za krekanje ☺
- nadogradnja na **smali/baksmali**
- **deodex**
  - micanje BOOTCLASSPATH ovisnosti o specifičnom uređaju
- dekodiranje i deodex, ponovna izgradnja / pakiranje, debuggiranje koda, očuvanje strukture, izmjena koda i resursa, korištenje frameworka
- debug + povezivanje sa DDMS

Statička analiza: Apktool (2)

```
vampirella:~/work/android/analiza/apktool $ ./apktool d -f Dontpanic.apk
I: Baksmaling...
I: Loading resource table...
I: Loaded.
I: Loading resource table from file: /home/kreator/apktool/framework/1.apk
I: Loaded.
I: Decoding file-resources...
I: Decoding values*/* XMLs...
I: Done.
I: Copying assets and libs...
vampirella:~/work/android/analiza/apktool $ grep -i "network" Dontpanic/smali/hr
/mireo/dp/common/DpAppService.smali
    const-string v3, "network"
    const-string v1, "network"
    const-string v1, "network"
vampirella:~/work/android/analiza/apktool $ PATH=`pwd`:$PATH ./apktool b Dontpan
ic dp-new.apk
I: Checking whether sources has changed...
I: Smaling...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs...
I: Building apk file...
vampirella:~/work/android/analiza/apktool $                          % 15:28
```

Statička analiza: Androguard

- švicarski nož za rev engineering:
  - interaktivna analiza class, dex, apk, jar i axml datoteka – dakle koda i resursa
  - direktno manipuliranje iz interaktivnog shella
  - usporedba sličnosti/diff, izračun potpisa, mjerenje rizika, vizualizacija, ...
- jednostavan i brz, radi iz prompta, nema GUI
- daleko najpotpuniji alat za analizu

Statička analiza: Androguard (2)

```
26 0x62 const/4 v10 , [#+ 0] , {0}
27 0x64 if-lt v10 , v9 , [+ 16]
28 0x68 return-void
29 0x6a aget-object v9 , v8 , v1
30 0x6e check-cast v9 , [type@ 319 [B]
31 0x72 invoke-static v9 , [meth@ 172 Landroid/telephony/gsm/SmsMessage; ([B) Landroid/telephony/gsm/SmsMessage;
createFromPdu]
32 0x78 move-result-object v9
33 0x7a aput-object v9 , v7 , v1
34 0x7e add-int/lit8 v1 , v1 , [#+ 1]
35 0x82 goto [+ -20]
36 0x84 aget-object v5 , v7 , v10
37 0x88 invoke-virtual v5 , [meth@ 173 Landroid/telephony/gsm/SmsMessage; () Ljava/lang/String; getDisplayOrigina
tingAddress]
38 0x8e move-result-object v6
39 0x90 const-string v11 , [string@ 72 '10086']
40 0x94 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
41 0x9a move-result v11
42 0x9c if-nez v11 , [+ 42]
43 0xa0 const-string v11 , [string@ 70 '10000']
44 0xa4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
45 0xaa move-result v11
46 0xac if-nez v11 , [+ 34]
47 0xb0 const-string v11 , [string@ 71 '10010']
48 0xb4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
49 0xba move-result v11
50 0xbc if-nez v11 , [+ 26]
51 0xc0 const-string v11 , [string@ 75 '1066185829']
52 0xc4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
53 0xca move-result v11
54 0xcc if-nez v11 , [+ 18]
55 0xd0 const-string v11 , [string@ 74 '1066133']
56 0xd4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
57 0xda move-result v11
58 0xdc if-nez v11 , [+ 10]
59 0xe0 const-string v11 , [string@ 73 '106601412004']
60 0xe4 invoke-virtual v11 , v6 , [meth@ 1167 Ljava/lang/String; (Ljava/lang/Object;) Z equals]
61 0xea move-result v11
62 0xec if-eqz v11 , [+ 5]
```

Statička analiza: Androguard (3)

```
Do you really want to exit ([y]/n)? y
vampirella:~/work/android/analiza/androguard $ ./androlyze.py -s        % 16:24
Androlyze version 0.2

In [1]: a, d, dx = AnalyzeAPK("../droidbox/BloodvsZombie_com.gamelio.DrawSlasher
_1_1.0.1.apk")
WARNING: module psyco not found

In [2]: perms = dx.tainted_packages.get_permissions([])

In [3]: show_Path(perms['SEND_SMS'])
Lcom/GoldDream/zj/zjService; bg_sendSms (Ljava/lang/String; Ljava/lang/String; I
)Ljava/lang/String; (@bg_sendSms-BB@0x0-0x0)  ---> Landroid/telephony/SmsManager
; getDefault ()Landroid/telephony/SmsManager;
Lcom/GoldDream/zj/zjService; bg_sendSms (Ljava/lang/String; Ljava/lang/String; I
)Ljava/lang/String; (@bg_sendSms-BB@0x18-0x18)  ---> Landroid/telephony/SmsManag
er; sendTextMessage (Ljava/lang/String; Ljava/lang/String; Ljava/lang/String; La
ndroid/app/PendingIntent; Landroid/app/PendingIntent;)V

In [4]: perms
Out[4]:
{'READ_PHONE_STATE': [<analysis.PathP instance at 0x26d4fc8>,
                      <analysis.PathP instance at 0x26d5050>,
                      <analysis.PathP instance at 0x26d5290>],
 'SEND_SMS': [<analysis.PathP instance at 0x28193f8>,
              <analysis.PathP instance at 0x2819518>]}

In [5]:
```

Dinamička analiza: Atrace

- potencijalno koristan ali nedovršen projekt
- omogućava syscall trace kroz posebno patchirani Android emulator/Qemu
- općenito praćenje ponašanja aplikacije, nema filtera, poluupotrebljivo

Dinamička analiza: Atrace (2)

```
[ATRACE][][0x0][0][0] futex(0x426fb004, 0x1, 0x7fffffff, 0x0, 0x426fb004, 0x426f
b000) = 0x0
[ATRACE][][0x0][0][0] futex(0x4277e004, 0x1, 0x7fffffff, 0x0, 0x4277e004, 0x4277
e000) = 0x0
[ATRACE][][0x0][0][0] futex(0x4277e004, 0x1, 0x7fffffff, 0x0, 0x4277e004, 0x4277
e000) = 0x0
[ATRACE][][0x0][0][0] access(0x44e90c9c, 0x4) = 0xfffffffe
[ATRACE][][0x0][0][0] access(0x44e90c9c, 0x4) = 0x0
[ATRACE][][0x0][0][0] access(0x44e90cac, 0x4) = 0xfffffffe
[ATRACE][][0x0][0][0] access(0x44e90cac, 0x4) = 0x0
[ATRACE][][0x0][0][0] futex(0x4277e004, 0x1, 0x7fffffff, 0x0, 0x4277e004, 0x1) =
 0x0
[ATRACE][][0x0][0][0] futex(0x426fb004, 0x1, 0x7fffffff, 0x0, 0x426fb004, 0x1) =
 0x0
[ATRACE][][0x0][0][0] futex(0x4277e004, 0x1, 0x7fffffff, 0x0, 0x4277e004, 0x1) =
 0x0
[ATRACE][][0x0][0][0] futex(0x4277e004, 0x1, 0x7fffffff, 0x0, 0x4277e004, 0x1) =
 0x0
[ATRACE][][0x0][0][0] clock_gettime(0x1, 0x44e92e60) = 0x0
[ATRACE][][0x0][0][0] gettid() = 0x38
[ATRACE][][0x0][0][0] ioctl(0x17, 0x4601, 0x80c03260)[ATRACE][][0x0][0][0] clock
_gettime(0x1, 0x44f92d68) = 0x0
[ATRACE][][0x0][0][0] clock_gettime(0x1, 0x44f92d70) = 0x0
[ATRACE][][0x0][0][0] clock_gettime(0x1, 0x44f92d18) = 0x0
[ATRACE][][0x0][0][0] futex(0x3dada4, 0x0, 0xffff74d, 0x44f92d18, 0x3dada0, 0x3
dada4)
```

Dinamička analiza: TaintDroid

- projekt: http://goo.gl/TDLe9
- praćenje ponašanja aplikacija (curenje informacija i sl.) u realnom vremenu
- komunikacija dobiva oznake (**taint marking**) i prati se kroz aplikaciju te između aplikacija na razini varijabli, metoda, poruka i datoteka
- praćenje na razini instrukcija
- platforme: emulator i NexusOne

Dinamička analiza: TaintDroid(2)

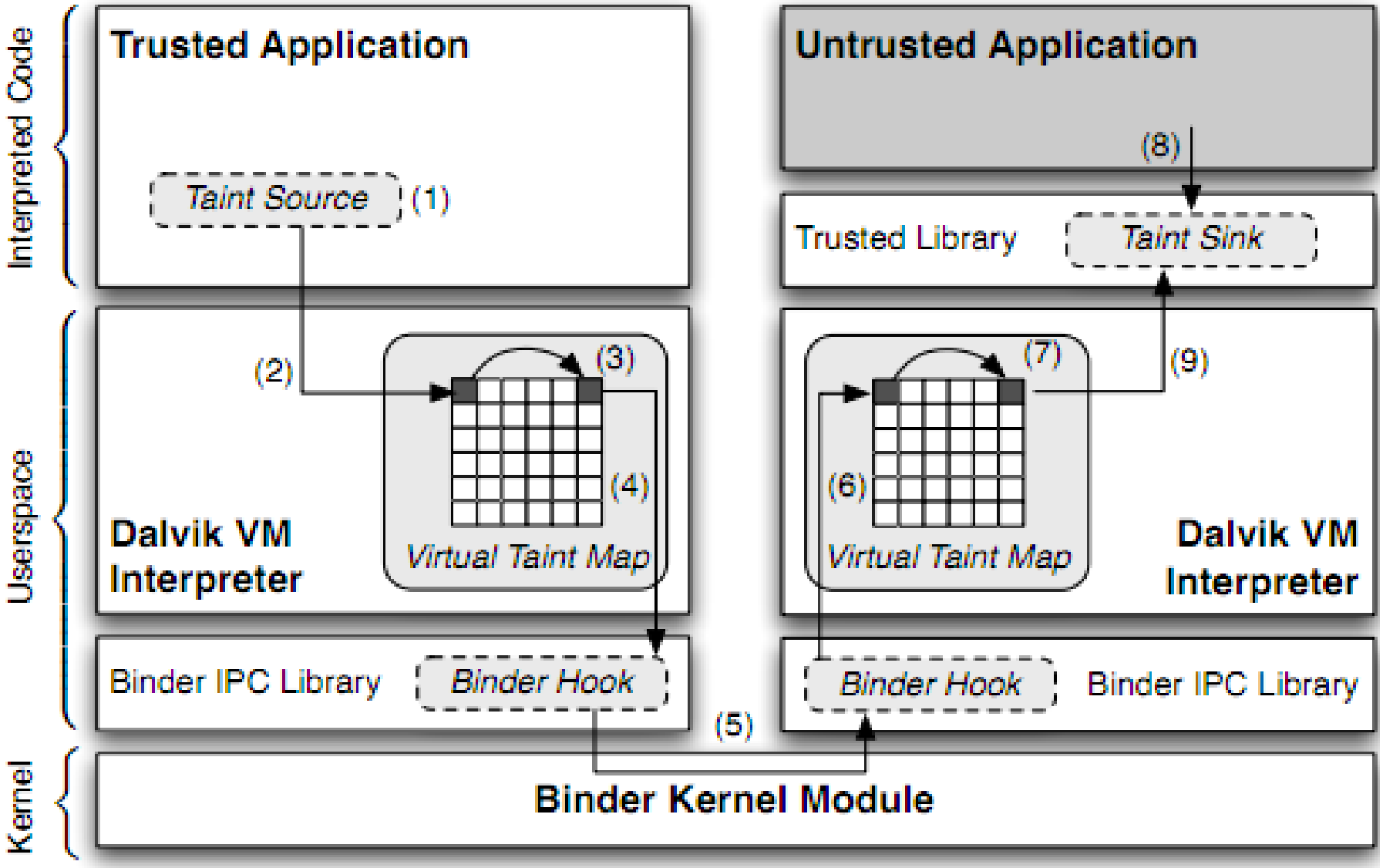
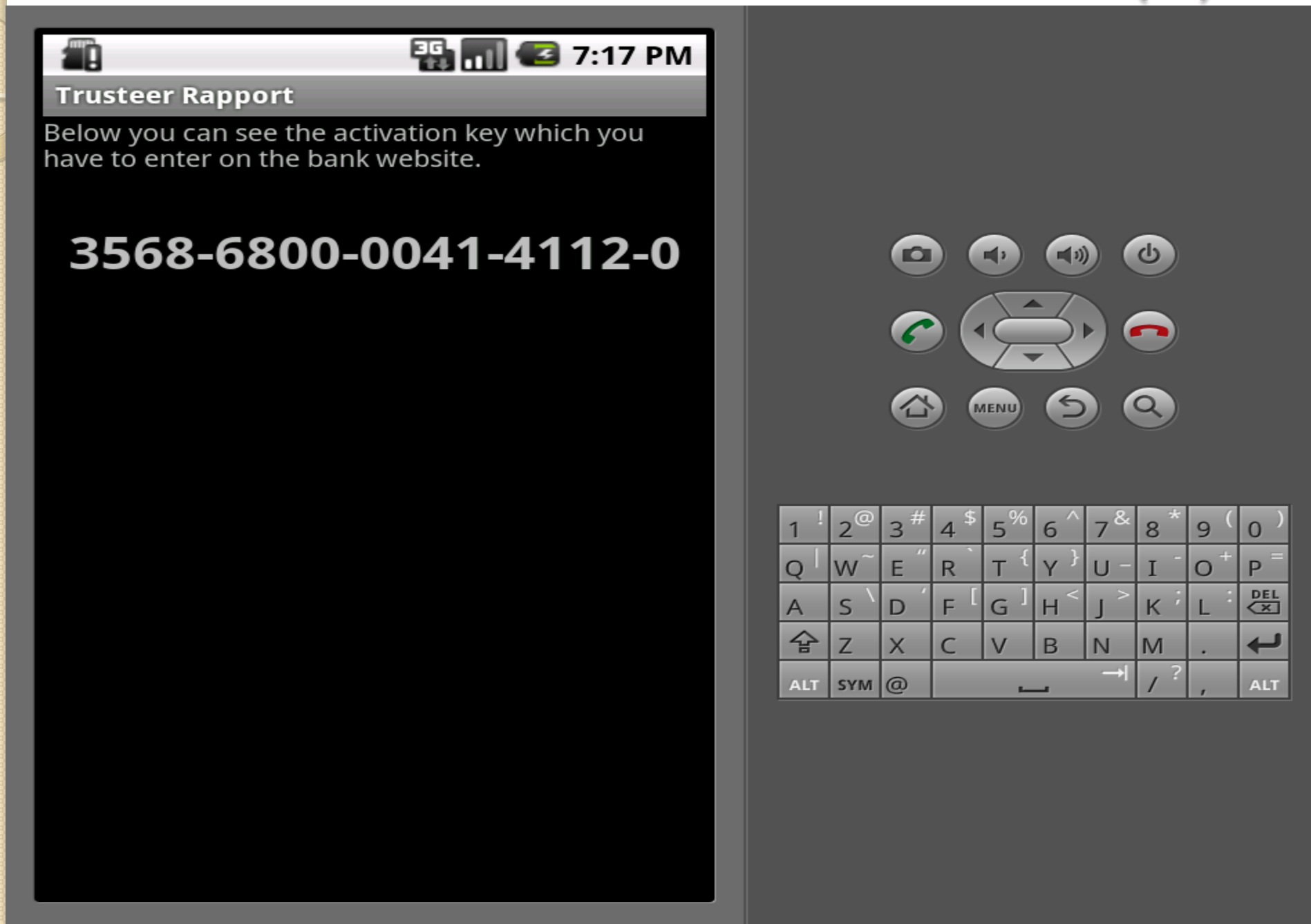


Figure 2: TaintDroid architecture within Android.

Dinamička analiza: DroidBox

- port TaintDroid platforme na emulator
- **sandbox** za testiranje i analizu individualnih aplikacija
- promatranje ponašanja malwarea
- dodaci:
  - sandboxing, automatizacija, vizualizacija, logging i log collector
- bitno za normalan rad!
  - *setprop dalvik.vm.execution-mode int:portable*

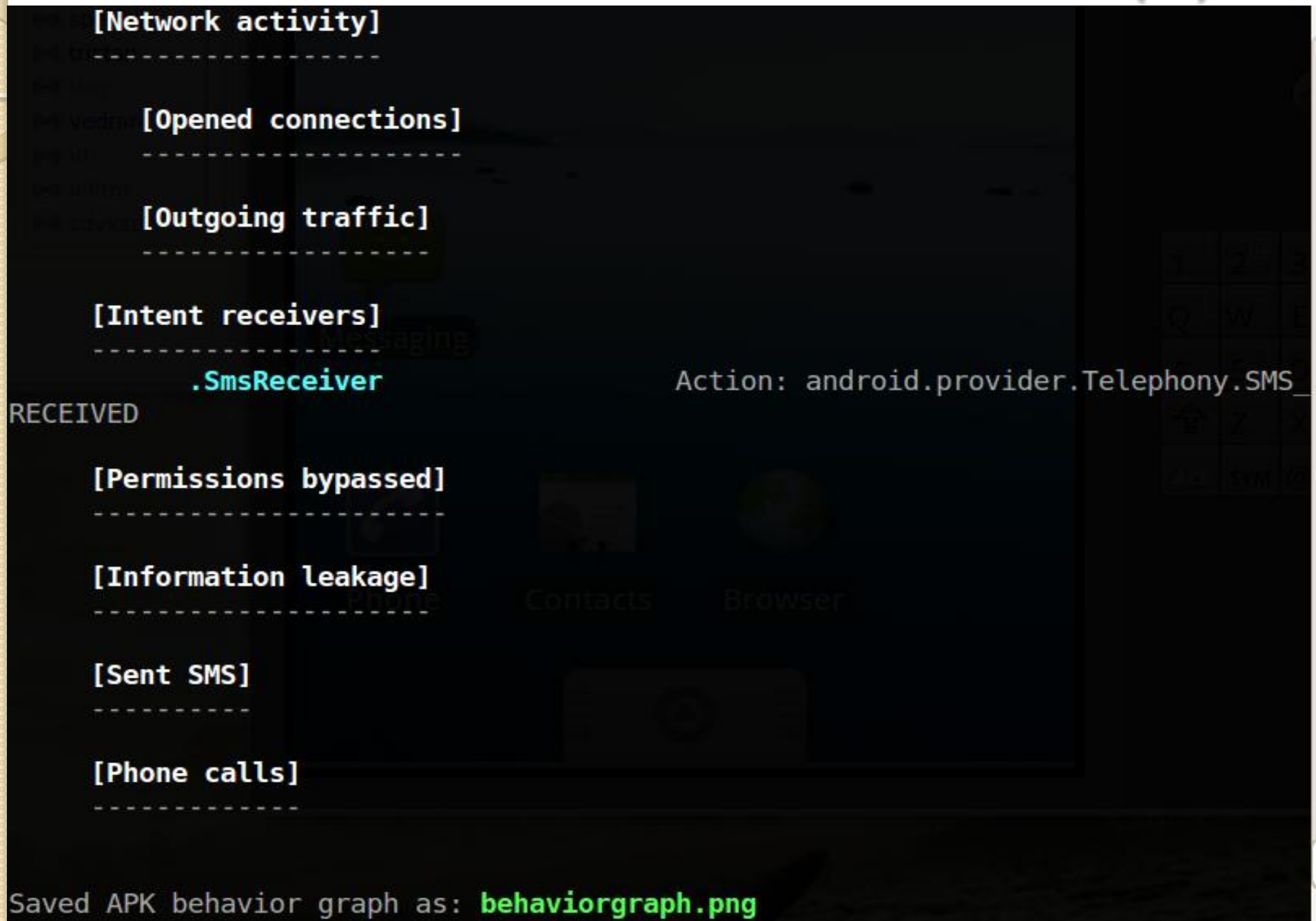
Dinamička analiza: DroidBox (2)



Dinamička analiza: DroidBox (3)

```
.. 13 more
^C    [*] Collected 6 sandbox logs

    [Info]
    ------
        File name:      Zitmo_tr_ECBBCE17053D6EAF9BF9CB7C71D0AF8D.apk
        MD5:            ecbbce17053d6eaf9bf9cb7c71d0af8d
        SHA1:           c9368c3edbcfa0bf443e060f093c300796b14673
        SHA256:         f6239ba0487ffcf4d09255dba781440d2600d3c509e66018e6a57249
12df34a9
        Duration:       90.041629076s


    [File activities]
    -----------------

        [Read operations]
        -----------------

        [Write operations]
        ------------------
            [4.05808711052]             /dev/pts/1[illegible] Fd: 2
            [4.06309318542]             /dev/pts/1 Fd: 2
            [4.90756416321]             /dev/pts/1 Fd: 1
            [4.90758895874]             /dev/pts/1 Fd: 1
            [6.35545015335]             /dev/pts/1[illegible] Fd: 1
            [6.35883307457]             /dev/pts/1 Fd: 1
```

Dinamička analiza: DroidBox (4)



Dinamička analiza: DroidBox (5)

```
     [Network activity]
     ------------------

        [Opened connections]
        --------------------
           [0.00077486038208]          Destination: www.searchwebmobile.com Po
rt: 80
           [1.64582395554]             Destination: www.searchwebmobile.com Po
rt: 80
           [5.03698396683]             Destination: localhost Port: 43182

        [Outgoing traffic]
        ------------------
           [0.000810861587524]         Destination: www.searchwebmobile.com Po
rt: 80
                                       Data: POST /ProtocolGW/protocol/command
s HTTP/1.1
           [0.108683824539]            Destination: www.searchwebmobile.com Po
rt: 80
                                       Data:

           [1.84798288345]             Destination: www.searchwebmobile.com Po
rt: 80
                                       Data: POST /ProtocolGW/protocol/command
status HTTP/1.1
           [2.27187991142]             Destination: www.searchwebmobile.com Po
rt: 80
                                       Data:

     [Intent receivers]
```

Kraj

- zahvale, pozdravi, pitanja, diskusija
- kontakt: dinko.korunic@infomar.hr
- hvala na pažnji!