




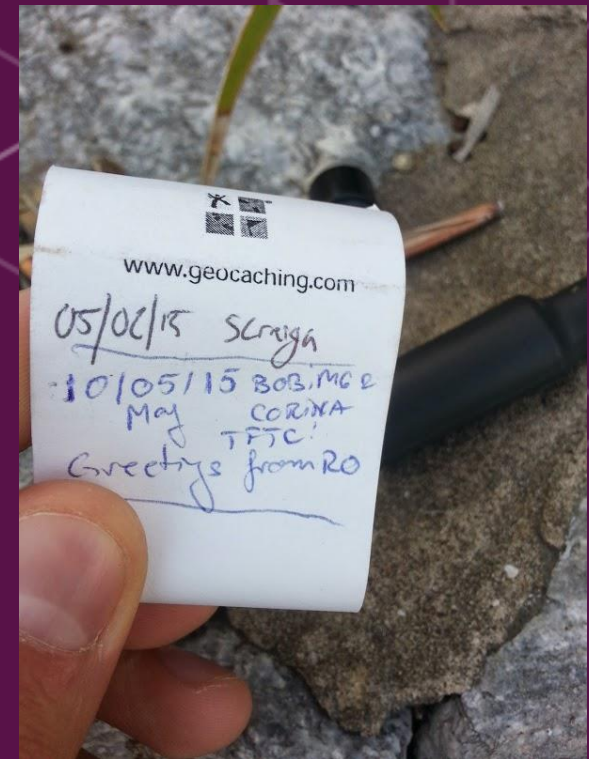
Dev(Talks):

 11 JUNE, ROMEXPO C1, BUCHAREST

+ Răzvan



+ Răzvan (bobim6)



Dev(Talks): // Mobile & IoT stage

+

+

Broadcast Intent Fuzzing Framework for Android

Răzvan-Costin IONESCU

Security QA Engineer, Intel Romania

+

Why ?

What ?

How ?

Who ?

Where ?



Why ?

Android Security

Intent Fuzzing

Important Target

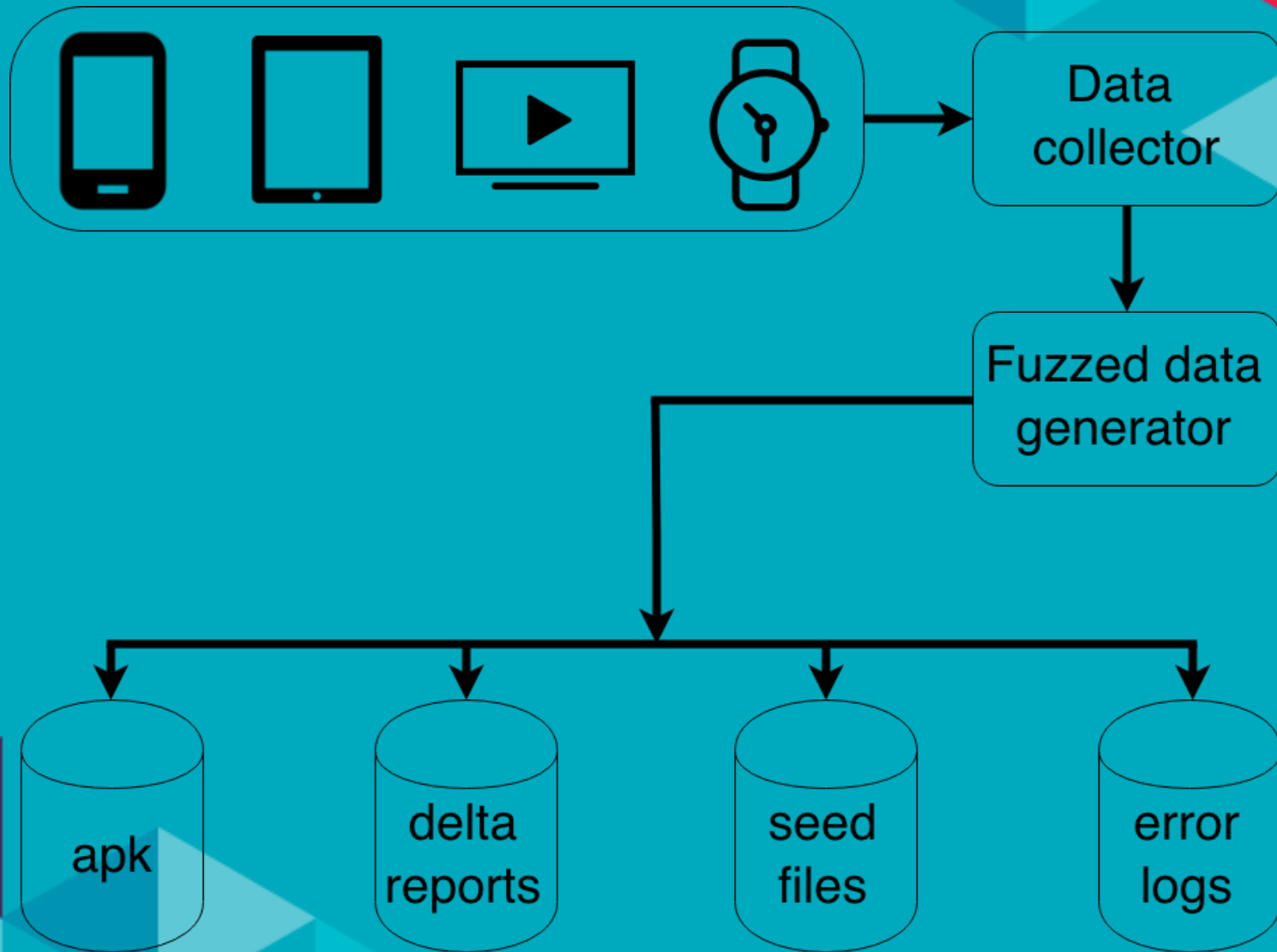
Broadcast Intents

Android Apps

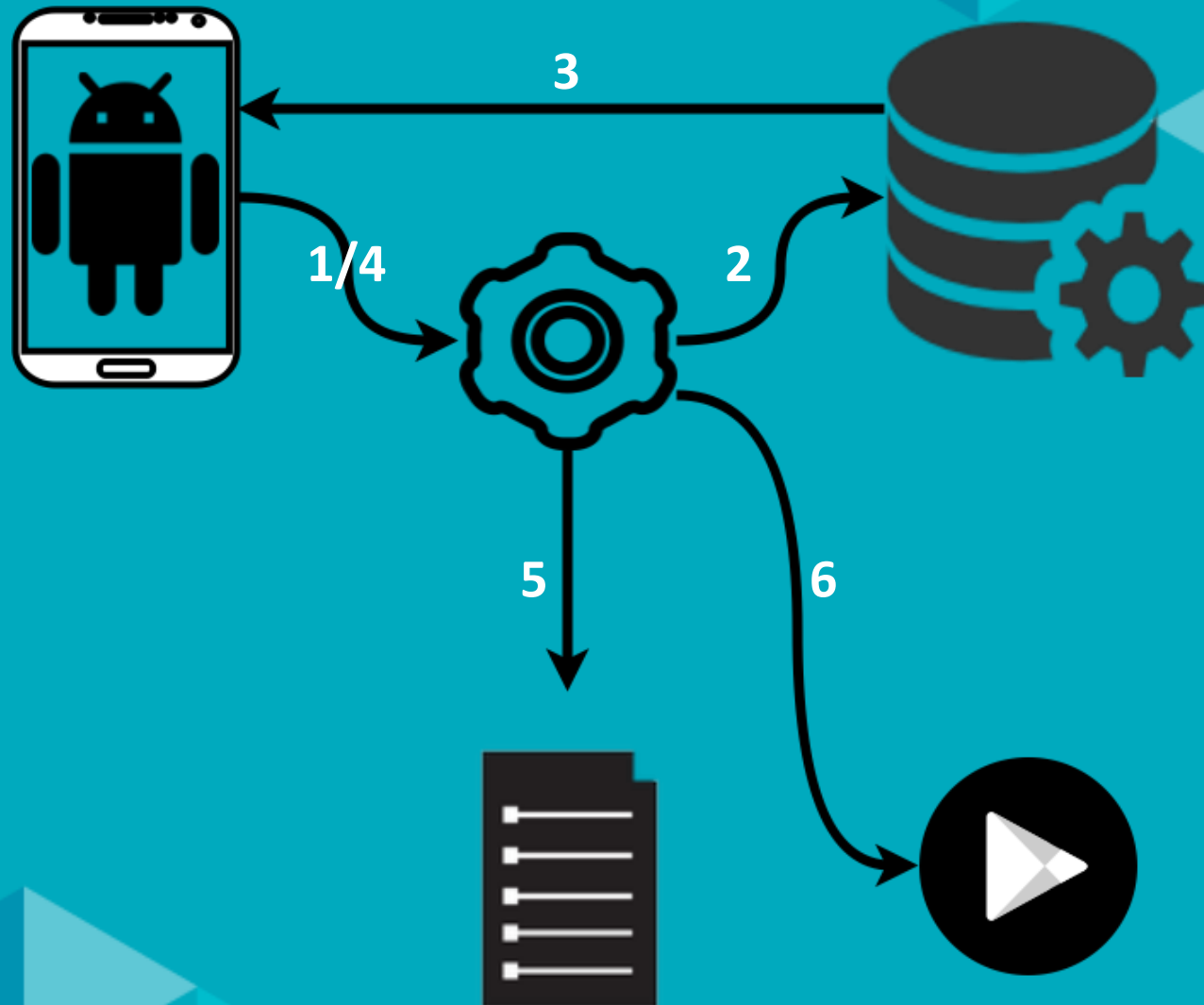
What ?



What else?



What else?



How ?

```
= = = = = = = = = = = = = = = = =
### # #### # # ####
# # # # # # ##
### # #### # # ##
# # # # # # #
### # # #### ###
= = = = = = = = = = = = = = = = =
```

Select one option from below

1. Select Devices Under Test
2. Generate Broadcast Intent calls for the DUT(s)
3. Generate Fuzzed Intent calls
4. Generate a delta report between 2 fuzzing sessions
5. Run existing generated intents from file
6. SQL injections for specific apk
7. Generate apk
8. DoS against Activity Manager - requires userdebug image
9. Smart fuzzing - using a template
- Q. Quit

Broadcast Intent -+example

```
adb -s 12qw34er56ty78ui shell am broadcast  
-n com.google.earth/  
com.google.analytics.tracking.android.Campai  
gnTrackingReceiver
```

Fuzzed Intent – using templates

tem_000000.tem – example

#Do not add lines to this template; possible options for each item: fuzz, nofuzz; if nofuzz, then a list might be expected

action nofuzz ["ACT_1","ACT_2"]

category nofuzz

data_uri nofuzz

e_key nofuzz

e_val nofuzz

flag nofuzz

Fuzzed Intent – using templates

tem_000000.tem – intent example

```
am start -n com.google.android.gms/.car.FirstActivity
```

```
-f 0x00400000
```

```
-a ACT_1
```

```
-c android.intent.category.ALTERNATIVE
```

```
-d DEFAULT
```

```
-e android.intent.extra.DOCK_STATE_LE_DESK 0
```

or

```
am start -n com.google.android.gms/.car.FirstActivity
```

```
-f 0x00400000
```

```
-a android.app.action.ADD_DEVICE_ADMIN
```

```
-c android.intent.category.ALTERNATIVE
```

```
-d DEFAULT
```

```
-e android.intent.extra.DOCK_STATE_LE_DESK 0
```

Fuzzed Intent – using templates

tem_111111.tem – example

#Do not add lines to this template; possible options for each item: fuzz, nofuzz; if nofuzz, then a list might be expected

action fuzz

category fuzz

data_uri fuzz

e_key fuzz

e_val fuzz

flag fuzz

Fuzzed Intent – using templates

tem_111111.tem – intent example

```
am start -n com.google.android.gms/.games.ui.client.requests.  
ClientPublicRequestActivity  
-f -1388136854  
-a 4GPHAI3LEG7Q76V0_fuzzy  
-c NHIL2ZJNBGCFYKQ_fuzzy  
-d 7RBNY6L30_fuzzy  
-e L33BC79I7HDE00A_fuzzy 1KQGYRV86AUTBV84G_fuzzy
```

Did it crash ? Yes, it did ! ☺

I/ActivityManager(3993): START u0 {act=U6K26ZP2Q0PAZ9_very_large_and_fuzzy
E/JavaBinder(3993): !!! FAILED BINDER TRANSACTION !!!

....

F/ActivityManager(3993): Exception thrown launching activities in
ProcessRecord{37d55748 20303:com.android.bluetooth/1002}

F/ActivityManager(3993): **android.os.TransactionTooLargeException**

F/ActivityManager(3993): at android.os.BinderProxy.transactNative(Native Method)

F/ActivityManager(3993): at android.os.BinderProxy.transact(Binder.java:496)

F/ActivityManager(3993): at android.app.ApplicationThreadProxy.scheduleLaunchActivity
(ApplicationThreadNative.java:797)

F/ActivityManager(3993): at

com.android.server.am.ActivityStackSupervisor.realStartActivityLocked
(ActivityStackSupervisor.java:1181)

F/ActivityManager(3993): at

com.android.server.am.ActivityStackSupervisor.attachApplicationLocked
(ActivityStackSupervisor.java:551)

....

+ F/ActivityManager(3993): at android.os.Binder.execTransact(Binder.java:446)

Bifuz

Generate Broadcast Intent calls

Generate Fuzzed Intent calls

Run existing generated intents from file

SQL injections for specific apk

Generate Broadcast Intent calls

Select package name and then select receiver activity

Select package to test Broadcast

Select receiver to broadcast

Back

com.htc.customappinstaller

com.htc.sense.ime

com.vodafone.addressbook

com.android.phone

com.htc.widget.profile

com.htc.f...

Select package to test Broadcast

Select receiver to broadcast

Back

Generate Broadcast Intent calls

Select package name and then select receiver activity

com.vodafone.addressbook

```
Fuzz ----- beginning of /dev/log/mainF/  
BIFUZ_BROADCAST(18813): am broadcast -n  
com.vodafone.addressbook/  
com.voxmobili.app.service.BootObserver F/  
BIFUZ_BROADCAST(18818): am broadcast -n  
com.vodafone.addressbook/  
com.vodafone.lib.sec.receiver.ConnectivityR  
eceiver
```

SQL injections for specific apk

com.mwr.example.sieve

Select content provider

com.mwr.example.sieve.DBContentProvider

com.mwr.example.sieve.FileBackupProvider



SQL injections for specific apk

com.mwr.example.sieve

yahoo

stefania

<ByteArray size=24 at 0x1750144752>

stefania@yahoo.com

google

stefania26

Back

<ByteArray size=25 at 0x1750144752>

stefania26@gmail.com

Results

javaNullPointerException

javaClassNotFoundException

DoS attack

SQL injection

NumberFormatException

IllegalArgumentException

SecurityException

IllegalStateException

ClassCastException



Thank you to...



Andreea Brîndușa Proca
Security QA Engineer
Intel Romania



Cristina Stefania Popescu
"open-minded, optimistic,
resourceful"
Student



Alexandru Bogdan Ungureanu
"amateur programming poet,
a lot more amateur than anything else"
Software Engineer, Intel Romania

Where ?



<https://github.com/fuzzing/bifuz>