https://commons.wikimedia.org/wiki/File:Hacker_-_Hacking_-_Symbol.jpg

How to mess with Android Intents

Răzvan-Costin IONESCU, Cristina Ştefania POPESCU

Intel OTC Security, Romania

Speakers

Răzvan
Security QA Engineer @Intel
geocacher, trekker, squash player

Ştefania
Security QA Intern @Intel
open-minded, optimistic, resourceful

Agenda

Motivation

Existing solutions

intents.fuzzinozer

Research

Intent Fuzzer: Crafting Intents of Death – crashes in native code for top apps

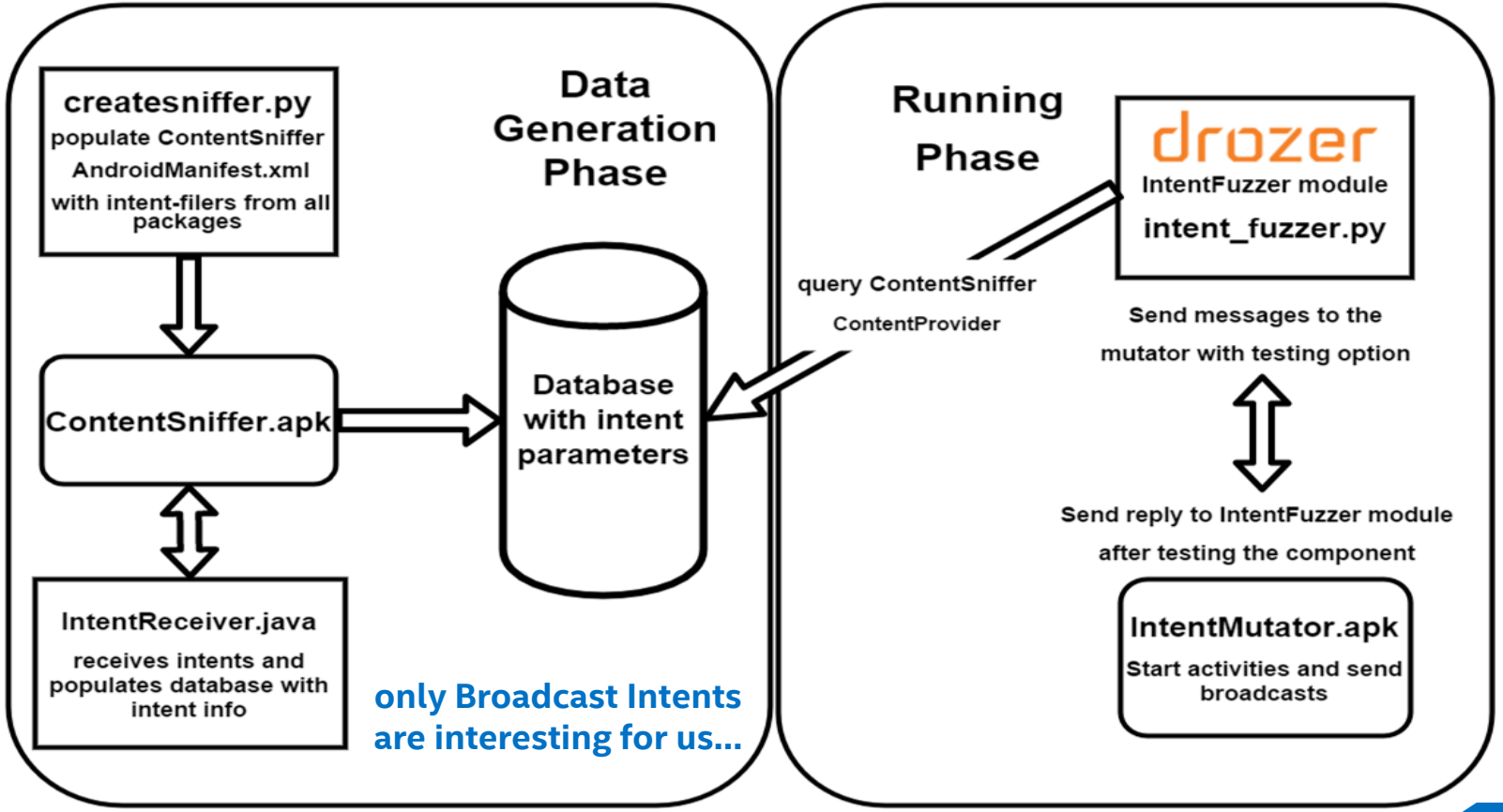
DroidFuzzer: Fuzzing the Android Apps with Intent-Filter Tag

Existing solutions

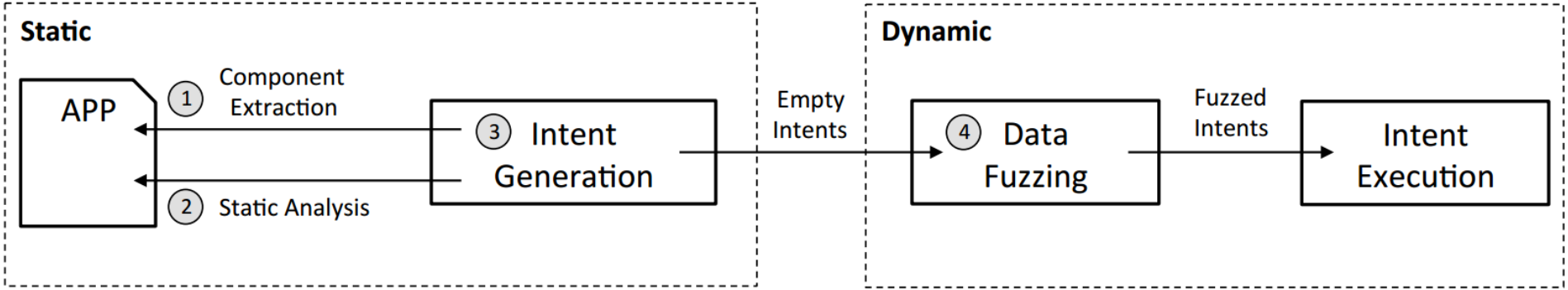
intent_fuzzing - https://github.com/cbthomas/drozer

DroidFuzzer – not public

intent_fuzzing - design

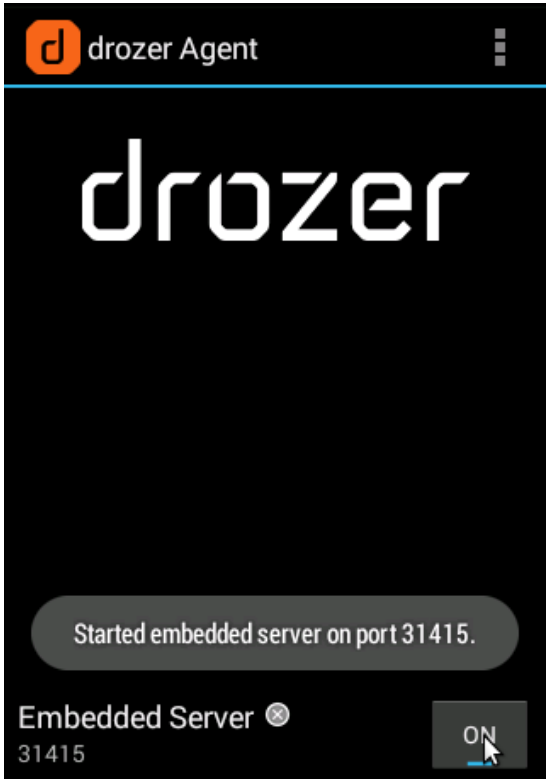


A little bit of theory…




```
Intent intent = new Intent(Intent.ACTION_SEND);
intent.setType("text/plain");
intent.putExtra(android.content.Intent.EXTRA_TEXT, "Hello!");
startActivity(intent);
```

drozer




```
cristina@cristina-OptiPlex-7010: ~/Documents/fuzzer-module
cristina@cristina-OptiPlex-7010:~/Documents/fuzzer-module$ drozer console connec
t INV133601437 --server localhost:31415
            ..                    ..:.
           ..o..                  .r..
            ..a..  . ....... .  ..nd
              ro..idsnemesisand..pr
              .otectorandroidsneme.
           .,sisandprotectorandroids+.
         ..nemesisandprotectorandroidsn:.
        .emesisandprotectorandroidsnemes..
      ..isandp,..,rotectorandro,..,idsnem.
      .isisandp..rotectorandroid..snemisis.
      ,andprotectorandroidsnemisisandprotec.
     .torandroidsnemesisandprotectorandroid.
     .snemisisandprotectorandroidsnemesisan:
     .dprotectorandroidsnemesisandprotector.

drozer Console (v2.3.4)
```

drozer - setup

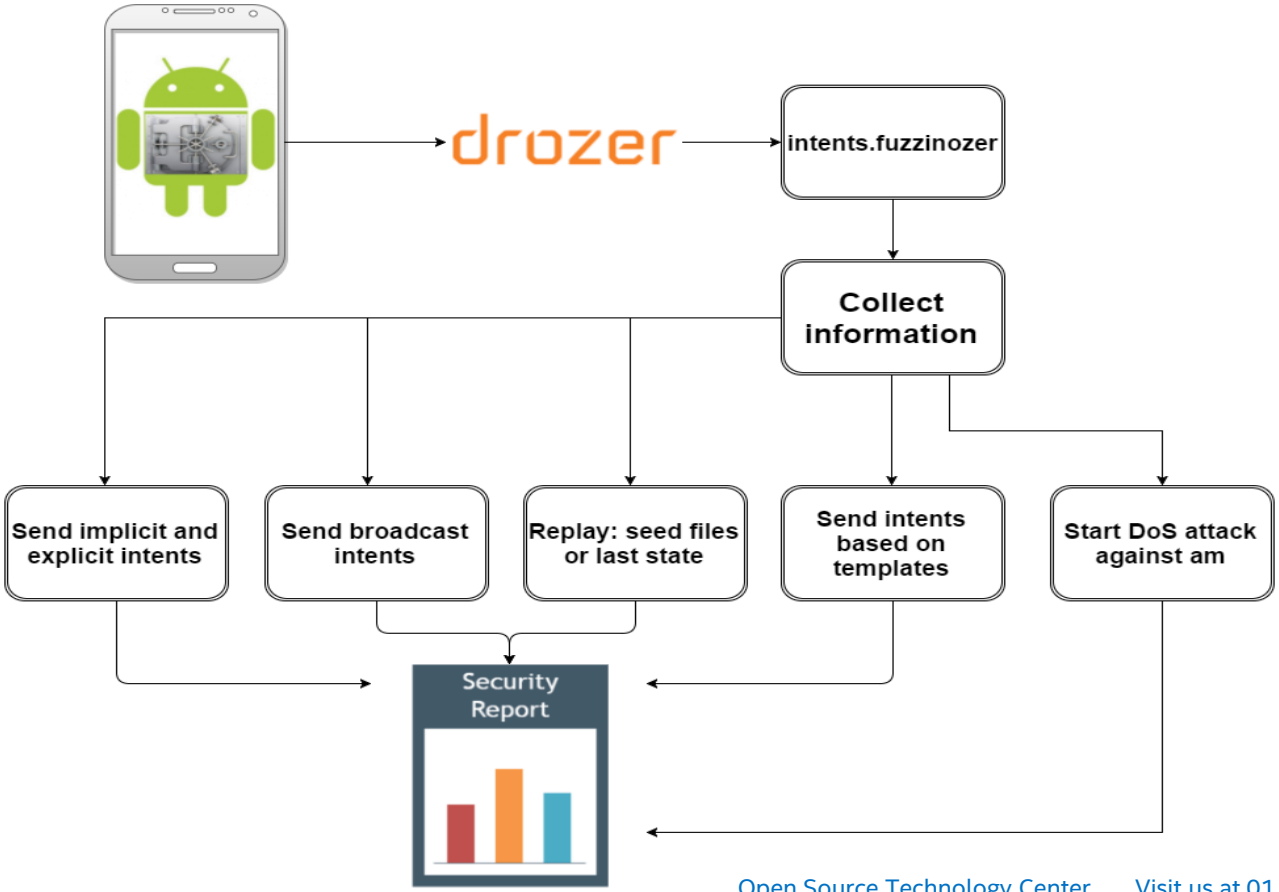
```
$  adb forward tcp:31415 tcp:31415
$  drozer console connect
dz>  module repository enable /path/to/your/repository
dz>  ls
dz>  help <name_of_the_module>
dz>  run <name_of_the_module>
```

intents.fuzzinozer – source code (sample)

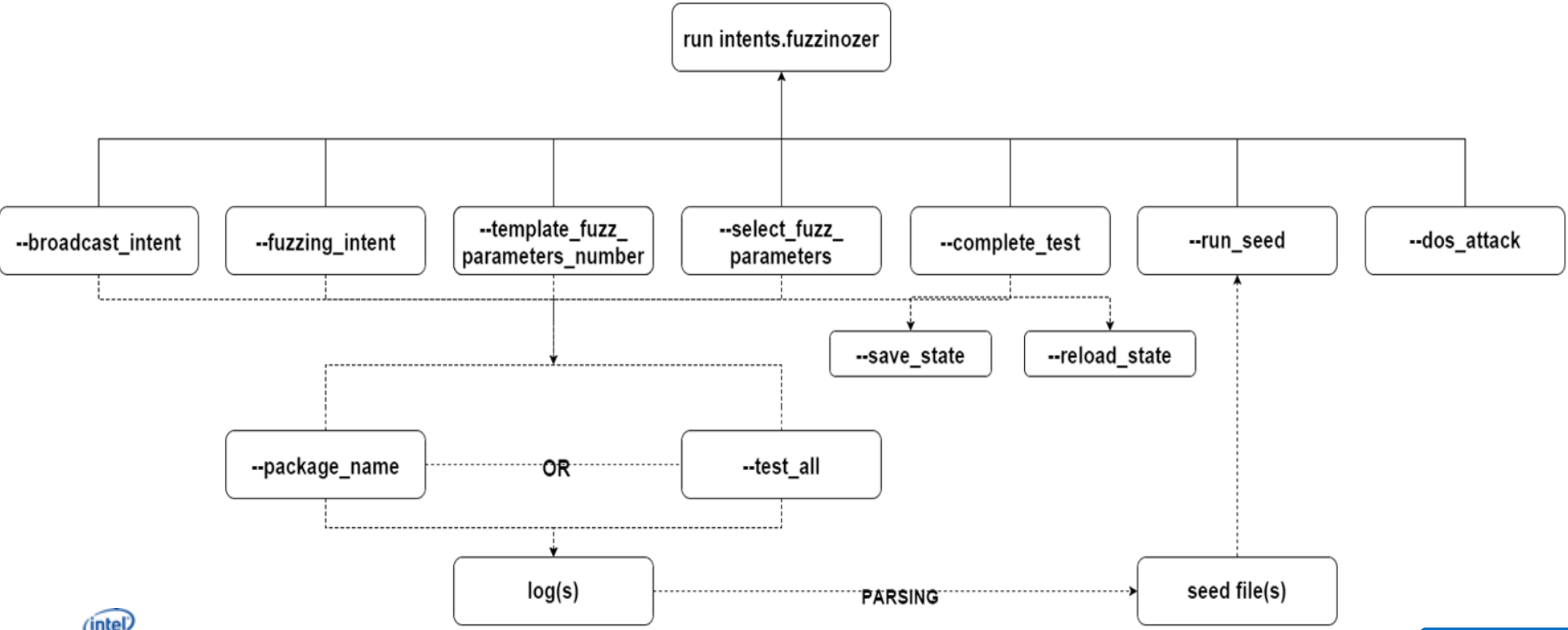
```
class Fuzzinozer(Module,common.PackageManager):
    name = "fuzzinozer"
    author = "Popescu Cristina Stefania"
    date = "2015-10-08"
    license = "3 clause BSD"
    path = ["intents"]

    def add_arguments(self, parser):
        parser.add_argument("--package_name", help="specify name of package to test ")
        parser.add_argument("--test_all", action='store_true', help="test all packages")
        parser.add_argument("--broadcast_intent", action='store_true', help="send ...")
        parser.add_argument("--fuzzing_intent", action='store_true', help="send intent...")
        parser.add_argument("--complete_test", action='store_true', help="test with...")
        parser.add_argument("--select_fuzz_parameters", help="give the parameters ...")
        parser.add_argument("--save_state",action='store_true', help="save the running ...")
        parser.add_argument("--reload", help="reload the running state parameters in ...")
        parser.add_argument("--run_seed", help="select the seed file you want to run")
        parser.add_argument("--device", help="used only for automated tests")
        parser.add_argument("--template_fuzz_parameters_number", help="give the ...")
        parser.add_argument("--dos_attack", help="give the number of intents you want to send")
```

intents.fuzzinozer – design



intents.fuzzinozer – options



intents.fuzzinozer – running examples

```
dz> run intents.fuzzinozer --fuzzing_intent --package_name
com.google.android.gms --template_fuzz_parameters_number 6

dz> run intents.fuzzinozer --complete_test --package_name
com.google.android.gms

dz> run intents.fuzzinozer --run_seed
seedfile_com.google.android.gms_NullPointerException.txt

dz> run intents.fuzzinozer --broadcast_intent
--package_name com.google.android.gms

$ drozer console connect -c
"run intents.fuzzinozer --broadcast_intent -test_all"
```

Results

javaNullPointerException

SecurityException

javaClassNotFoundException

IllegalStateException

DoS attack

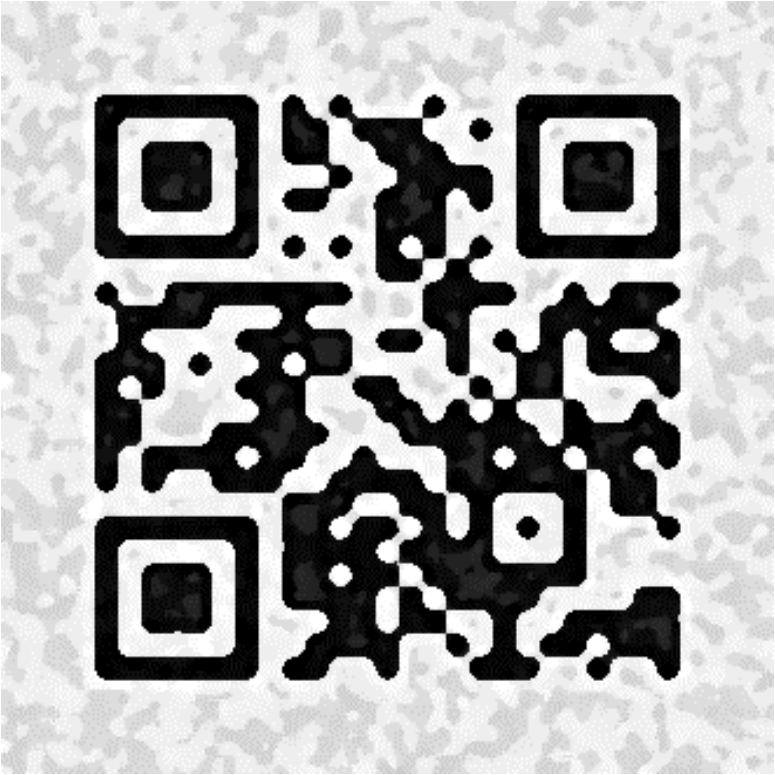
ClassCastException

NumberFormatException

ClassCastException

IllegalArgumentException

https://github.com/fuzzing



https://www.flickr.com/photos/codex41/9725166177


intel