Computer Science Department

USER MANUAL

Alterdroid

Tool for twarting obfuscated malware

Leganés, Febrero de 2015

Index

Introduction

Alterdroid is a dynamic analysis tool for detecting hidden or obfuscated malware components distributed as parts of an app package. The key idea in Alterdroid consists of analyzing the behavioral differences between the original app and a number of automatically generated versions of it where a number of modifications (*faults*) have been carefully injected. Observable differences in terms of activities that appear or vanish in the modified app are recorded, and this signature is finally analyzed through a pattern-matching process driven by rules that relate different types of hidden functionalities with patterns found in the differential signature.

Installation

1.1 Requirements

- *Ubuntu Server or Desktop* (it can be ported to Windows and Mac as well).
- *Android*
- *Python 2.7*
- Librería *PIL* python para procesado de imágenes.
- Librería *ImageMagik* para la transformación de imágenes
- Librería *PyPa* python
- Librería *Levinshtain* python
- Librería *Libmagic*

Mercury, lzma, http://tukaani.org/xz/

1.2 Installing the dependencies

Alterdroid doesn't need installation. However, it depends on a number of dependencies. The instalation of all required libraries is subsequently described:

1.2.1 Android over Ubuntu Desktop

Follow instractions here: https://developer.android.com/sdk/installing/index.html

1.2.2 Android over Ubuntu Server

```
wget http://dl.google.com/android/android-sdk_r22.6-linux.tgz
tar -xvzf android-sdk_r20-linux.tgz
cd ~/android-sdk-linux/tools
android update sdk --no-ui
vim ~/.bashrc
export PATH=${PATH}:~/android-sdk-linux/tools
export PATH=${PATH}:~/android-sdk-linux/platform-tools
sudo apt-get install libc6:i386 libstdc++6:i386 ia32-libs
android update sdk --filter android-10 --no-ui
```

1.2.3 Install Androguard

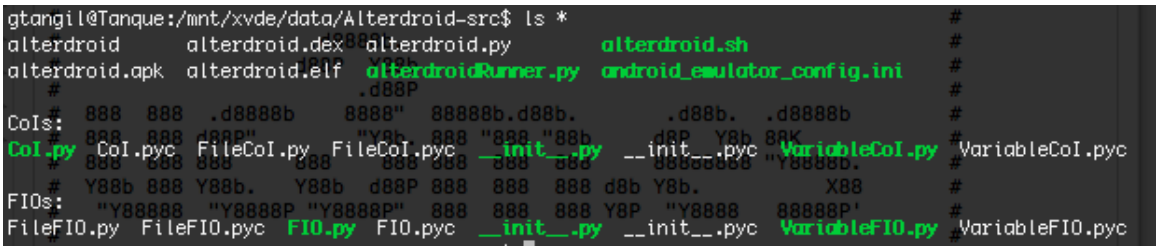
Follow the instructions here: https://code.google.com/p/androguard/

1.2.4 Other dependencies

```
sudo apt-get install python-imaging
sudo apt-get install python-levenshtein
sudo apt-get install python-numpy python-scipy python-matplotlib
sudo apt-get install python-magic
sudo apt-get install imagemagick
```

Alterdroid

1.3 Components



1.4 API

TotalNumber of lines of code: 1904

- Alterdroid.py:
  - main
  - alterdroid
  - init_sandbox
  - create_and_start_sandbox
  - stop_and_delete_sandbox
  - get_apk
  - get_apk_info
  - display_dvm_info
  - get_apk_fios
  - get_files_types
  - get_apk_components
  - get_activity_signature
  - get_activity_signatures
  - get_diff_signature
  - match_rule
  - match_rules
  - get_summary_execution
  - get_summary_rep_injections
  - get_summary_coi
- InteractionThread
  - install
  - install_and_run
  - install_and_test
  - run_activity_callRunner
  - run_activty
  - run_activty_and_interact
  - interactDumpWindow
  - interactDumpCurrent

    - interactView
    - count_views
- FIO.py
    - get_apk
    - unpackage
    - repackage
    - cloneAPK
    - FioNotSupportedByAlterdroid
- FileFIO.py
    - FileFIO
        - get_fio_handler
        - select_fios
        - generic_mutation
        - image_mutation
    - GenericMutationFile
        - get_sub_type
        - inject_fault
    - ImageFile
        - get_sub_type
        - inject_fault
    - ScriptFile
        - get_sub_type
        - inject_fault
    - APKFile
        - get_sub_type
        - inject_fault
    - DEXFile
        - get_sub_type
        - inject_fault
    - ELFFile
        - get_sub_type
        - inject_fault
- COI.py
    - get_apk
    - get_type
    - shannonEntropy
- FileCoI.py
    - FileCoI
        - toString
        - get_attributes
        - get_file_name
        - get_extension
        - get_magic_key
        - get_magic_description
        - get_path
        - get_crc
    - ImageFileMatch
        - get_sub_type
        - check
    - ImageFileExtensionMismatch
        - get_sub_type
        - check

- APKFileExtensionMismatch
  - get_sub_type
  - check
- RAtCFileMatch
  - get_sub_type
  - check
- TextScriptMatch
  - get_sub_type
  - check
- ELFExecutableMatch
  - get_sub_type
  - check
- DEXFileMatch
  - get_sub_type
  - check
- APKFileMatch
  - get_sub_type
  - check
- EncryptedOrCompressedMatch
  - get_sub_type
  - check

Execution

```
Usage: alterdroid.py [options]

Options:
  -h, --help            show this help message and exit
  -i INPUT, --input=INPUT
                        file : inject faults in this apk
  -v, --version         version of the API
  -d DIRECTORY, --directory=DIRECTORY
                        directory : use this directory, test all apks
  -t TIME, --time=TIME  time : time of the dynamic analysis
  -f, --fast            fast : applies all the injections at once
```

Examples

```
./alterdroid.sh -d samples
./alterdroid.sh -d samples -t 120
./alterdroid.sh -d samples -t 120 -f
./alterdroid.sh -i samples/ahw-giyum-ghkrmsgksahepf-1-5111313-
8ef4a02fc4681795f8a967ca7e1b2e64.apk -d 120
```

Ouptut

```
################################################################################
# Author: Guillermo Suarez de Tangil - guillermo.suarez.tangil@uc3m.es   #
# (c) 2013, COmputer SEcurity (COSEC) - Universidad Carlos III de Madrid #
################################################################################
#                                                                              #
#   .d8888b .d88b.  .d8888b   .d88b.   .d8888b                                 #
#  d88P"   d88""88b 88K      d8P  Y8b d88P"                                    #
#  888     888  888 "Y8888b. 88888888 888                                      #
#  Y88b.   Y88..88P      X88 Y8b.     Y88b.                                    #
#   "Y8888P "Y88P"   88888P'  "Y8888   "Y8888P                                 #
#                                                                              #
#                    .d8888b.                                                  #
#                   d88P  Y88b                                                 #
#                        .d88P                                                 #
#  888  888  .d8888b    8888"  88888b.d88b.       .d88b.  .d8888b        #
#  888  888 d88P"        "Y8b. 888 "888 "88b     d8P  Y8b 88K            #
#  888  888 888     888    888 888  888  888     88888888 "Y8888b.       #
#  Y88b 888 Y88b.   Y88b  d88P 888  888  888 d8b Y8b.          X88       #
#   "Y88888  "Y8888P "Y8888P"  888  888  888 Y8P  "Y8888   88888P'       #
#                                                                              #
############################## COSEC Alterdroid ###############################
============================
[SAMPLE] samples/DroidKungFuSapp/8f85dbb8f3b58c40d1c5cabe2f72f7a9480a460f.apk
[DURATION] Static: 17.4794111252
[DURATION] Dynamic: 1607.9387939
[COIs] 5
 + [COI] FileCoI(RAtCFileMatch): assets/ratc - data
 + [COI] FileCoI(EncryptedOrCompressedMatch): assets/ratc - data
 + [COI] FileCoI(EncryptedOrCompressedMatch): res/raw/linphonerc - ASCII
 + [COI] FileCoI(EncryptedOrCompressedMatch): assets/gjsvro - data
 + [COI] FileCoI(EncryptedOrCompressedMatch): assets/killall - ELF Executable

[FIOs] 5
 + [FIO]GenericMutationFile
 + [FIO]GenericMutationFile
 + [FIO]GenericMutationFile
 + [FIO]ExecutableFile
 + [FIO]GenericMutationFile

[ORIGINAL SIGNATURE] ['service', 'service', 'service', 'service', ...]

[REPACKAGED APP] sample_GenericMutationFile_26f7f3c9-df76-4ace-8031-
4d8f21124900.apk
 + [REPACKAGED SIGNATURE] ['file-write', 'service', 'service', …]
 + [DIFFERENTIAL SIGNATURE] [['insert', 'service'], ['insert', 'service']...
 + ...
...
```