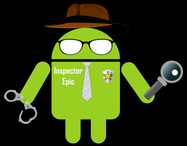
Oh Noes, Another Android Malware Talk

Thomas Eder Michael Rodler

2012-04-18



Malware on my Android Phone?

Malware on my Android Phone?

Who in here has an Android based smartphone?

Malware on my Android Phone?

Who in here has an Android based smartphone?

That's why Android is interesting for malware authors

Agenda... NOT

DON'T ROOT
ROBOTS!

APPLICATIONS
Home
Contacts
Phone
Browser
...
APPLICATION FRAMEWORK
Activity Manager
Content Providers
View System
Notification Manager
Package Manager
Telephony Manager
Resource Manager
Location Manager
XMPP Service
LIBRARIES
Surface Manager
Media Framework
OpenGL|ES
FreeType
SGL
libc
ANDROID RUNTIME
Core Libraries
Dalvik Virtual Machine
LINUX KERNEL
Display Driver
Camera Driver
Bluetooth Driver
Binder (IPC) Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

Actual Agenda

- Malware analysis on Android
  - static
  - dynamic
- "Tools of the Trade"
- Research overview
- A very simple example
- Our own project: EPIC

Android Malware is skyrocketing

```
+                             *
|                            *
|                           *
|                          *
|                         *
|                        *
|                      *
|                    *
|                  *
|               *
|           *
|      *
| *
+------------------------------+
```

[1]

---

[1] no actual data, graphs just look good

Android is a high risk asset because...

- ... it contains sensitive data
  - location, pictures, contacts
  - login credentials
- ... it can access services that cost money
  - sms, mms, calls to `0900[0-9]+` -> we will come to that! ;)
  - in-app billing
- ... people depend on it
  - reachability
  - navigation
  - who remembers phone numbers?

New attack vectors

- Return of the Dialer! (after a decade or so)
- DDoS on Callcenters and Network Operators
  - via sms
  - via calls
- Bad for critical infrastructure
  - aka. 112, 122, 133, 144, etc.
  - yeah, they do (sometimes) depend on GSM

Android Malware

This is a serious threat!

Android Malware

This is a serious threat!

Actual malware capabilities

- Botnets (controlled via SMS, IRC, HTTP)
- Backdoors
- e-banking trojans
- Dialer
- root exploits

Android Malware

This is a serious threat!

Actual malware capabilities

- Botnets (controlled via SMS, IRC, HTTP)
- Backdoors
- e-banking trojans
- Dialer
- root exploits

Get samples and analysis reports from:
https://code.google.com/p/androguard/wiki/DatabaseAndroidMalwares
http://contagiominidump.blogspot.com/

Identifying Malware – the static analysis way

Static analysis steps

- Get sample apk
- Unpack the apk file
- Extract and analyse `AndroidManifest.xml`
- Disassemble/Decompile `classes.dex` and ELF binaries
- Look for suspicious code and resources

Suspicious resources in `FoncySms.apk`

```
sh-4.2$ file *.png
border01.png: Zip archive data, at least v2.0 to extract
footer01.png: ELF 32-bit LSB executable, ARM, version 1 (SYSV), dynamically linked (uses shared libs), not stripped
ghthouse.png: PNG image data, 1550 x 465, 8-bit/color RGB, non-interlaced
ght.png:      PNG image data, 1550 x 465, 8-bit/color RGB, non-interlaced
gtho.png:     PNG image data, 1550 x 465, 8-bit/color RGB, non-interlaced
header01.png: ELF 32-bit LSB executable, ARM, version 1 (SYSV), dynamically linked (uses shared libs), not stripped
h.png:        PNG image data, 1550 x 465, 8-bit/color RGB, non-interlaced
sh-4.2$
```

header01.png: ELF 32-bit LSB executable,

Static Analysis Example

Existing Tools

Tools:

- AXMLPrinter2
- aapt
- smali/baksmali
- dex2jar
- jad/jd-gui
- your favourite ELF/ARM disassembler (e.g. IDA, objdump...)
- (dedexer, dexdump)

Toolkits:

- apktool
- androguard
- APKInspector (GUI)

Why static analysis can be a pain in the a**

- Obfuscation
- Packing
- Encryption

Why static analysis can be a pain in the a**

- Obfuscation
- Packing
- Encryption

- Hard to automate
- Good analysis must be done manually
- Time consuming

Dynamic Analysis Tools I

- Run sample inside Android emulator
- watch what it does

Dynamic Analysis Tools II

Existing free tools focus on privacy flaws

- Taintdroid and associates
  - dynamic taint tracking
  - TaintdroidRunner, DroidBox

Dynamic Analysis Tools III

Other academic approaches

- Crowdroid
- Android Application Sandbox
- Paranoid Android
- ...

Our own project: EPIC

FH Hagenberg project in cooperation with Fraunhofer AISEC

EPIC team:
Thomas Eder, Christian Nösterer,
Michael Rodler, Thomas Traunmüller

EPIC supervisors:
Dieter Vymazal, Martin Brunner

Our own project: EPIC

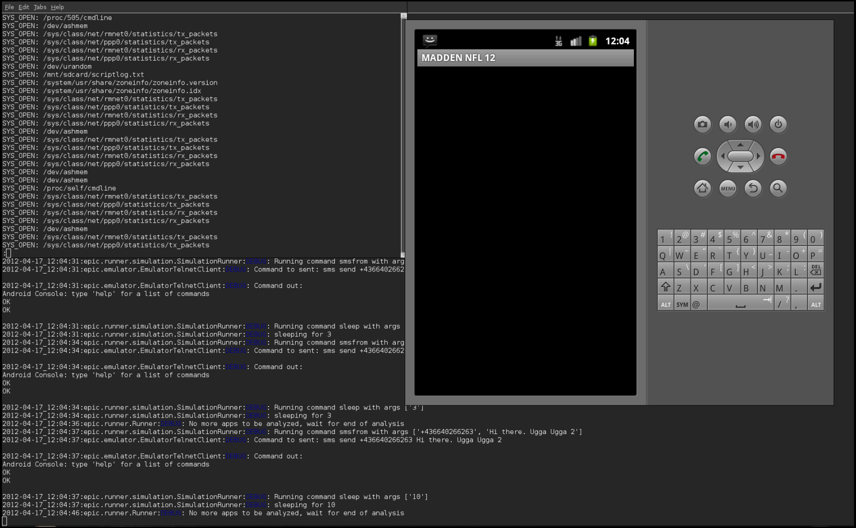
- Dynamic Anlysis Tool
- Fork of TaintdroidRunner
- Combination of several approaches
- Simulation of User Interaction and Phone Events
- Analysis report (machine and human readable)
- In development

State at the moment: unfinished and unreadable log $\rightarrow$ work-in-progress ;)

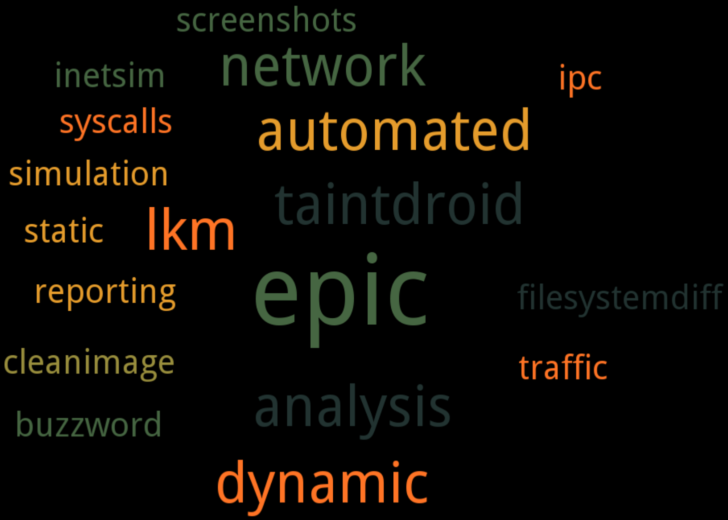
Approaches

- Basic static analysis
- Syscall tracing via Kernel Module
- Network Traffic Analysis
- Privacy flaw detection via Taintroid
- Filesystem-Diff

“Development Preview” Screenshot



Buzzword Cloud



Contact

- Thomas Eder (thomas.eder@students.fh-hagenberg.at)
- Michael Rodler (michael.rodler@students.fh-hagenberg.at, @f0rki)

Thanks for the attention!

References

- http://source.android.com/tech/security/index.html
- https://developer.android.com/guide/topics/security/security.html
- http://contagiominidump.blogspot.com/
- https://code.google.com/p/androguard
- https://code.google.com/p/android-apktool/
- Taintdroid http://appanalysis.org/
- https://github.com/dbaeumges/taintdroid_runner
- Crowdroid https://www.ida.liu.se/~rtslab/publications/2011/spsm11-burguera.pdf