(IN-)SECURITY OF SMARTPHONE ANTI-VIRUS AND SECURITY APPS

Stephan Huber, Siegfried Rasthofer,

Steven Arzt, Michael Tröger, Andreas Wittmann, Philipp Roskosch,
Daniel Magin, Joseph Varghese

Who are we

Stephan

- Mobile Security Researcher at Fraunhofer SIT
- Enjoys teaching students in Android Hacking
- @teamsik

Siegfried

- 4th year PhD Student at TU Darmstadt/ Fraunhofer SIT
- Static and Dynamic Code Analysis
- @teamsik

Vulnerabilities in antivirus tools: What does it mean for enterprises?

übergizmo Search this site Features Phones Computers Tutorials Events More

Google Security Researcher Slams Antivirus Software For Its Vulnerabilities

Research shows antivirus products vulnerable to attack

A Google researcher has been reporting severe vulnerabilities in

s tools, such as

Security App Features on Mobile

Security App Features on Mobile

Secure Browsing

Security App Features on Mobile

Secure Browsing

Signature Update

Security App Features on Mobile

Secure Browsing

Signature Update

Realtime Monitoring

Security App Features on Mobile

Secure Browsing

Signature Update

Premium Features

Realtime Monitoring

Security App Features on Mobile

Secure Browsing

Theft Protection

Signature Update

Premium Features

Realtime Monitoring

Security App Features on Mobile

SPAM Protection

Secure Browsing

Theft Protection

Signature Update

Premium Features

Realtime Monitoring

Outline

- **Analyzed** Apps
- Excerpt of Implementation **Flaws** and **Attack** Types
  - Business Model
  - Local Denial of Service
  - Man-in-the-Middle Attacks
- Overview of **All Findings**
- Our **Experiences** during the **Responsible Disclosure** Process
- Summary

Analyzed Android Apps

App	GooglePlay Downloads
AndroHelm	1-5m
Malwarebytes	5-10m
ESET	5-10m
Avira	10-50m
Kaspersky	10-50m
McAfee	10-50m
CM Security	100-500m

Bussines Model Attack


AndroHelm Security
AntiVirus app
AndroHelm Security
Virenschutz
AndroHelm Security
9,99 €
AntiVirus for Tablet
AndroHelm Security
10,99 €
AntiVirus Security
AndroHelm Security
129,99 €
AntiVirus Android
AndroHelm Security
20,85 €
AntiVirus Android
AndroHelm Security
99,99 €

Client Side License Verification

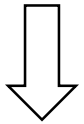
```
…
this.toast("Thank you for upgrading to PRO!");

//shared pref value set to true
this.prefs.putBoolean("isPro", true);
…
```

Client Side License Verification

```
…
this.toast("Thank you for upgrading to PRO!");

//shared pref value set to true
this.prefs.putBoolean("isPro", true);
…
```



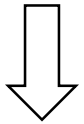
write value to .xml file

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <int name="dialogShowTimes" value="1" />
    <boolean name="hasDatabase" value="true" />
    <string name="lastFragment"></string>
    <boolean name="isPro" value="true"
</map>
```

Client Side License Verification

```
…
this.toast("Thank you for upgrading to PRO!");

//shared pref value set to true
this.prefs.putBoolean("isPro", true);
…
```



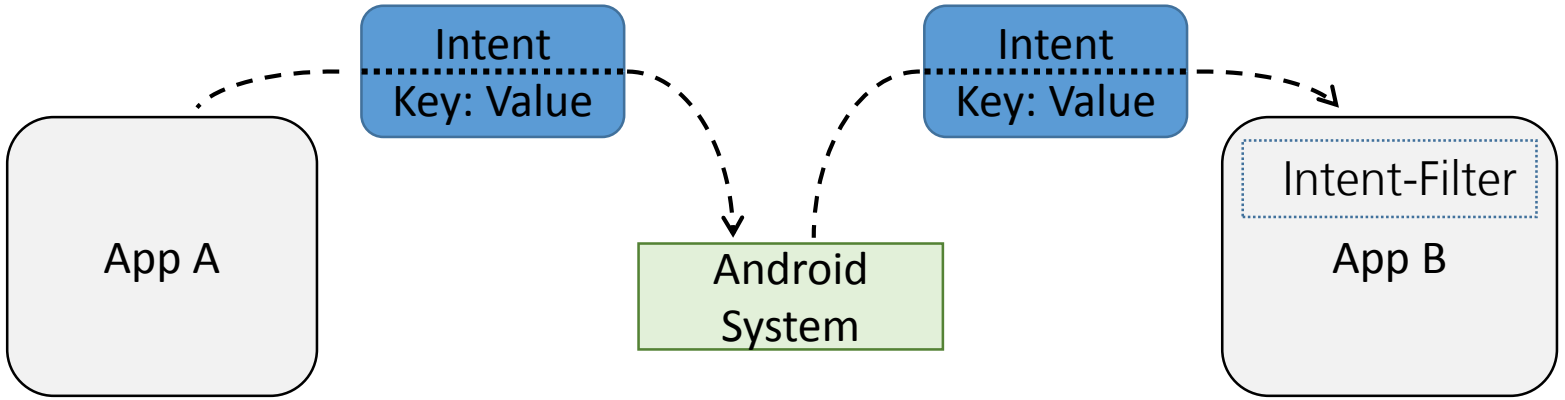
write value to .xml file

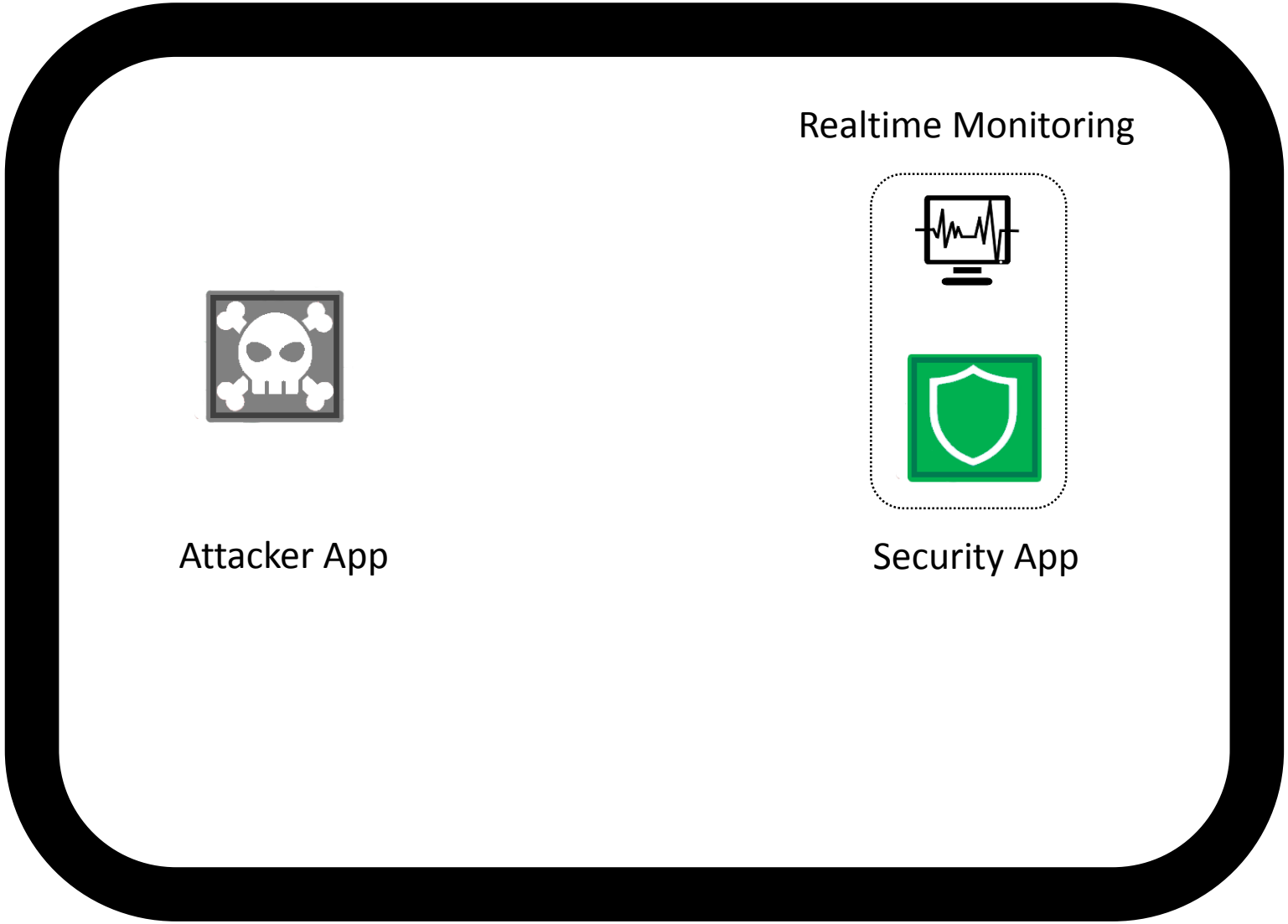
```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <int name="dialogShowTimes" value="1" />
    <boolean name="hasDatabase" value="true" />
    <string name="lastFragment"></string>
    <boolean name="isPro" value="true"
</map>
```

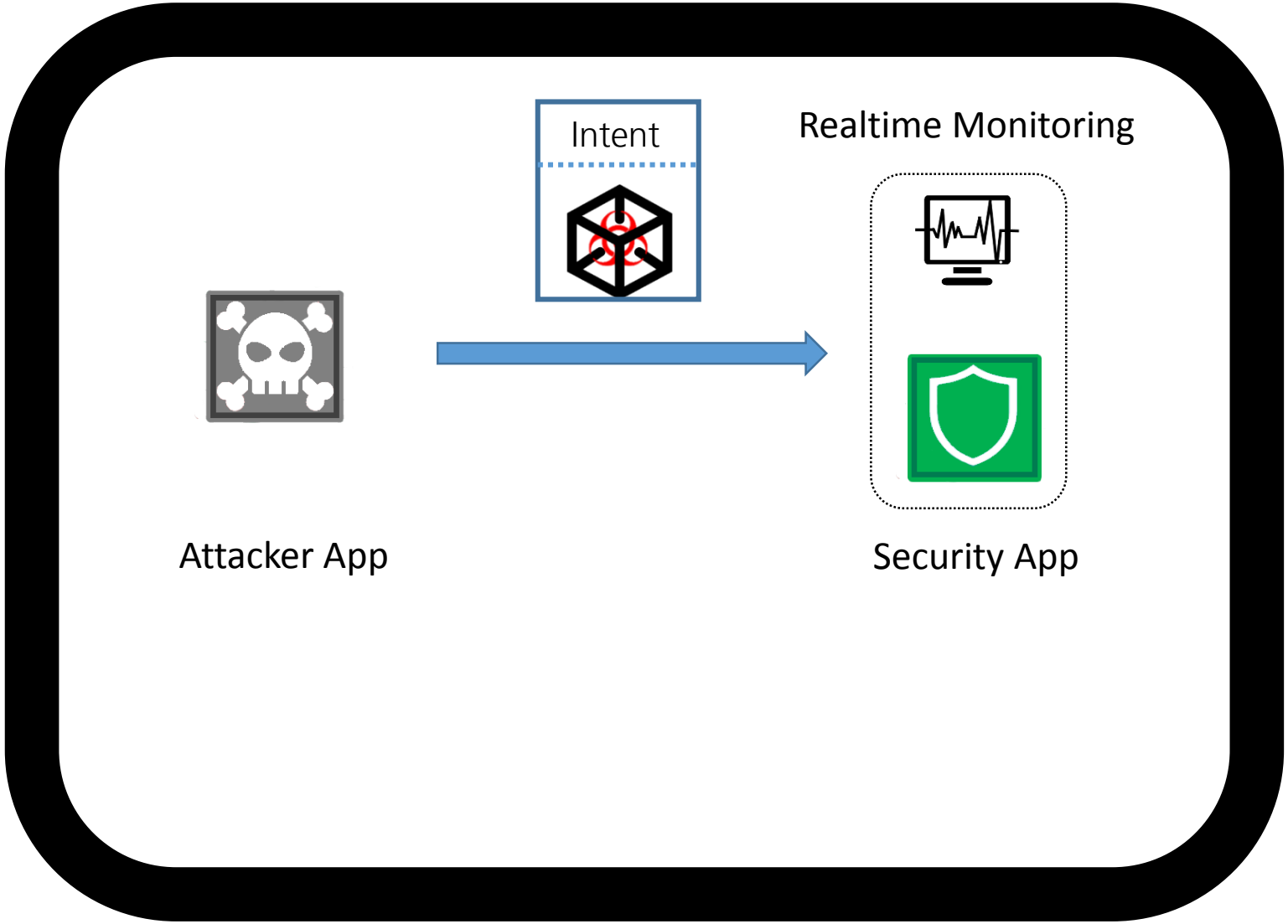
Every user can set this value !

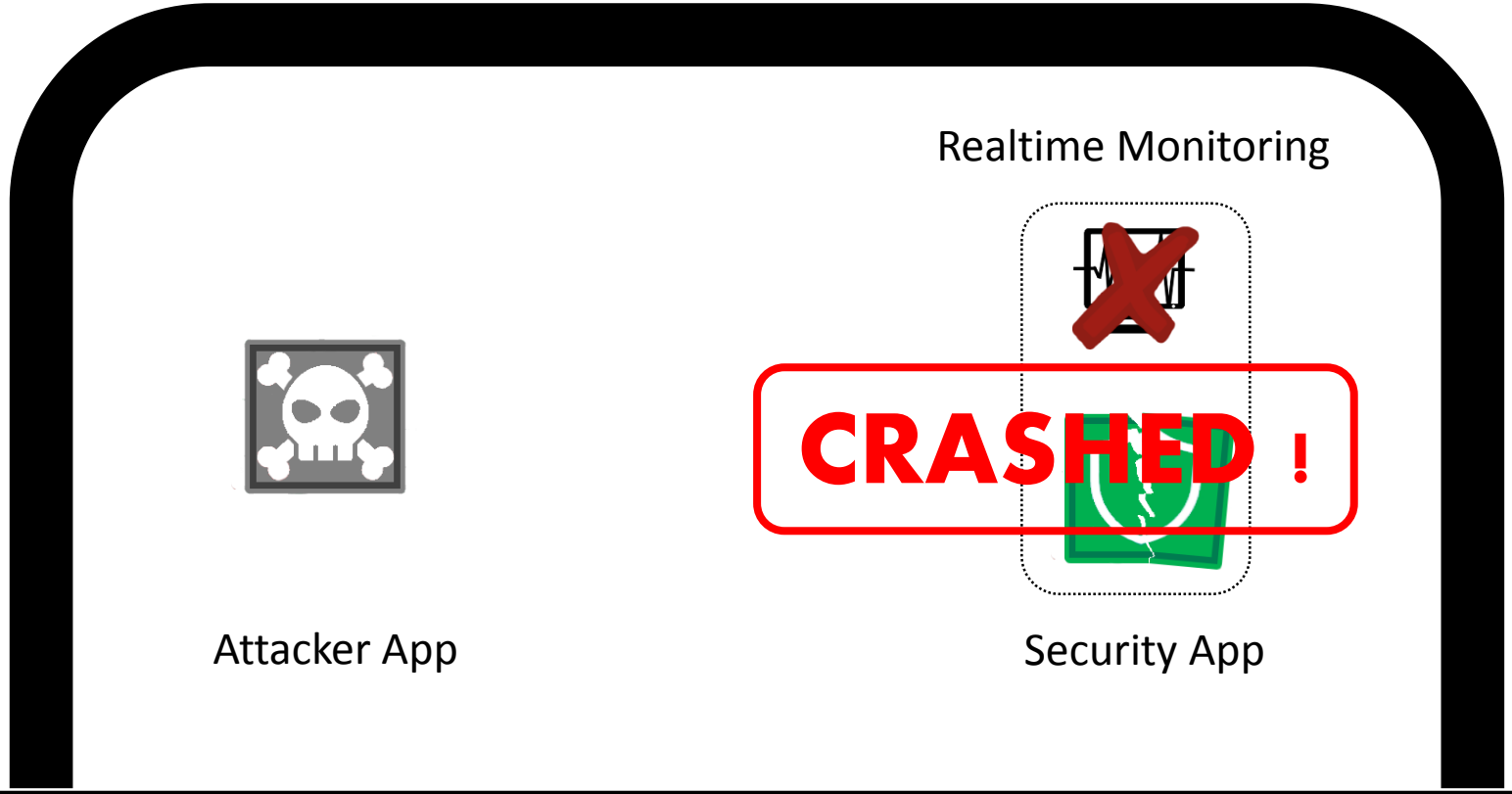
Local Denial of Service

Inter App Communication




Realtime Monitoring
Attacker App
Security App


Intent
Realtime Monitoring
Attacker App
Security App




```
Log output:
Java.lang.RuntimeException: Unable to start receiver
com.androhelm.antivirus.receivers.SMSMonitor: java.lang.NullPointerException
…
com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:793)
E/AndroidRuntime(16060): at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:560)
E/AndroidRuntime(16060): Caused by: java.lang.NullPointerException
com.androhelm.antivirus.receivers.SMSMonitor.onReceive(SMSMonitor.java:31)E/AndroidRuntime(16060): at
E/AndroidRuntime(16060): ... 10 more
```

Implementation Faults

- **Missing checks** of intent **payload**, cause ***exceptions***
- **Missing *exception*** handling will **crash whole** application

Implementation Faults

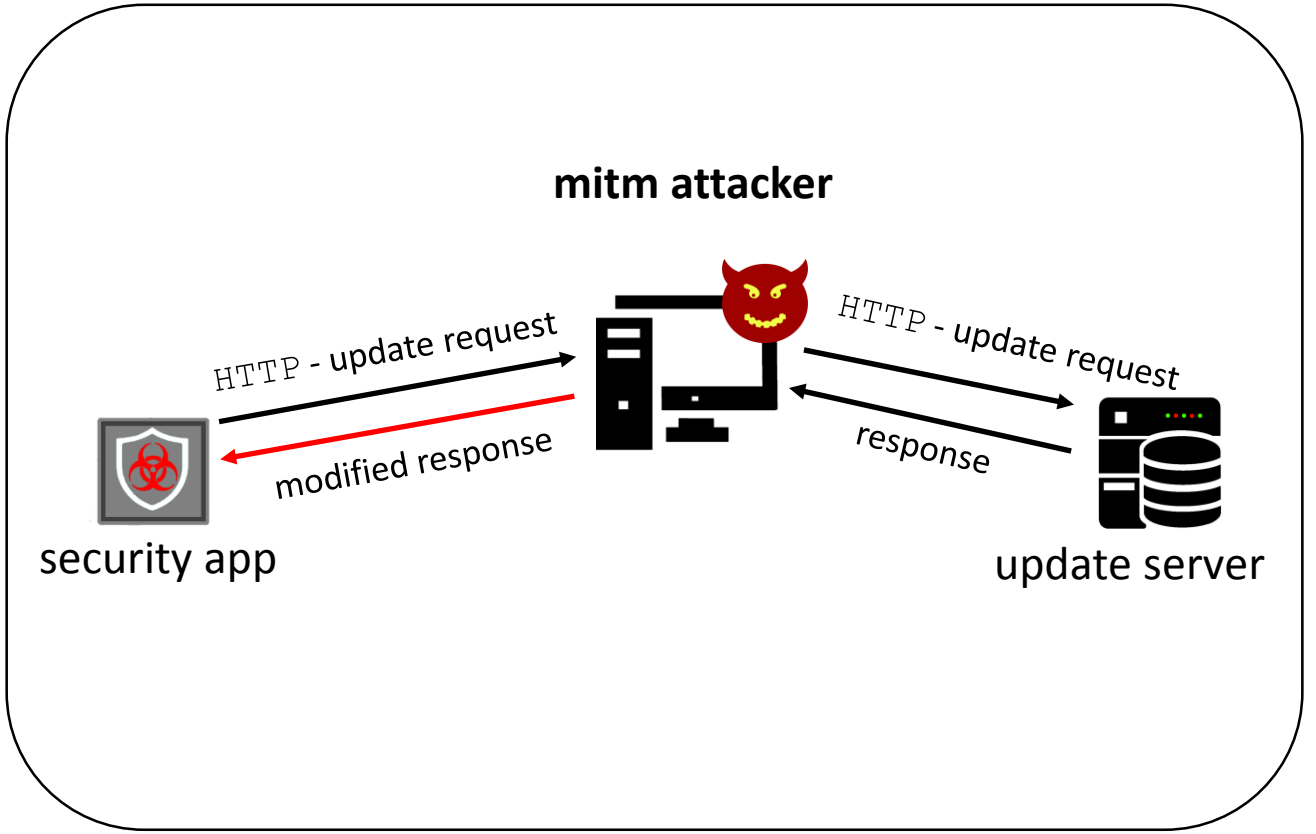
- **Missing checks** of intent **payload**, cause ***exceptions***
- **Missing *exception*** handling will **crash whole** application
- Example: `null-Intent`

```
1)public void onReceive(Context c, Intent intent) {
2)     //missing check if intent is null
3)     Bundle bundle = intent.getExtras();
4)      if(bundle != null) {
5)            Object o = bundle.get("pdus");
```

Man-in-the-Middle Attacks

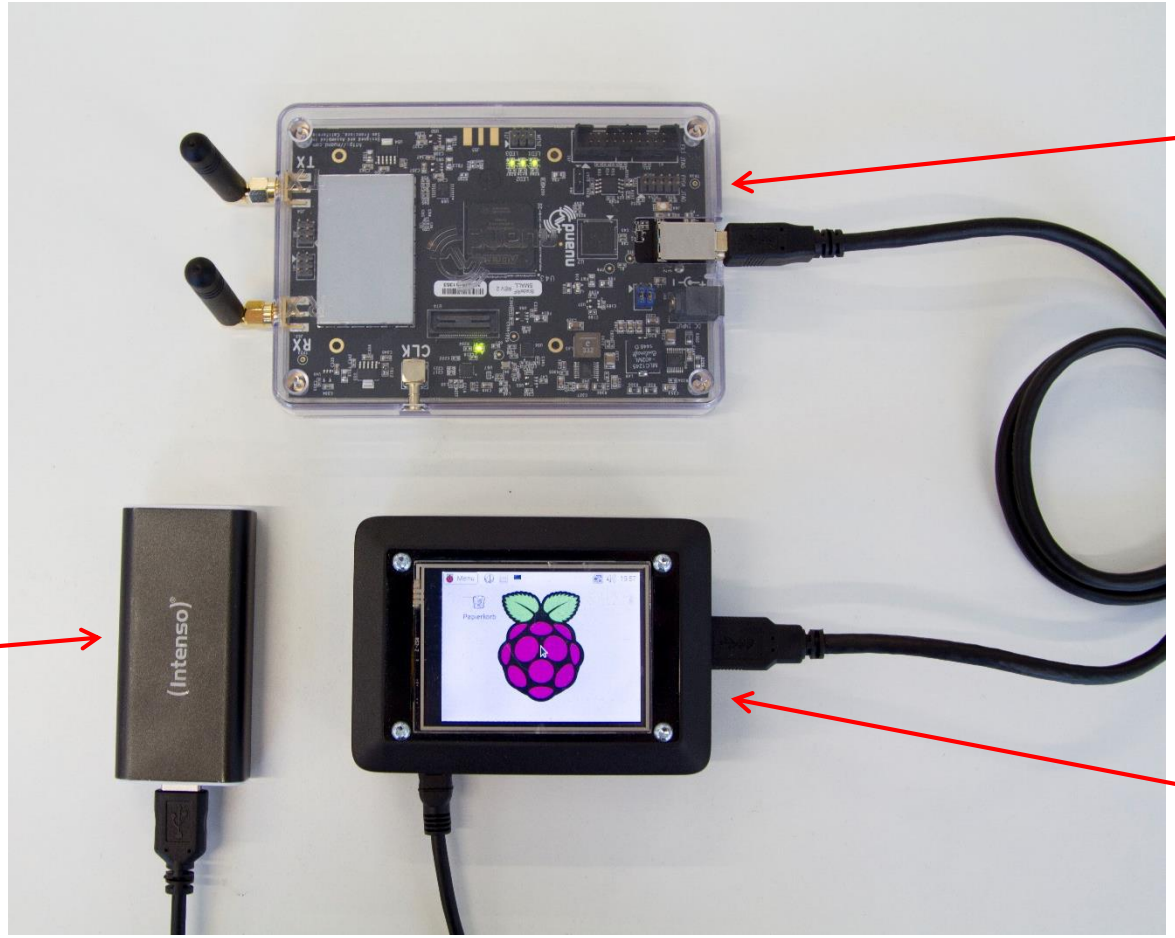
Man-in-the-Middle Attacks

- Smartphone is a **wireless medium**
- Communication over **HTTP**
  - **No authentication**
  - **Broken** self-made **integrity** protection
  - **Broken** self-made **encryption**
- Communication over **HTTPS**
  - **Broken certificate validation**



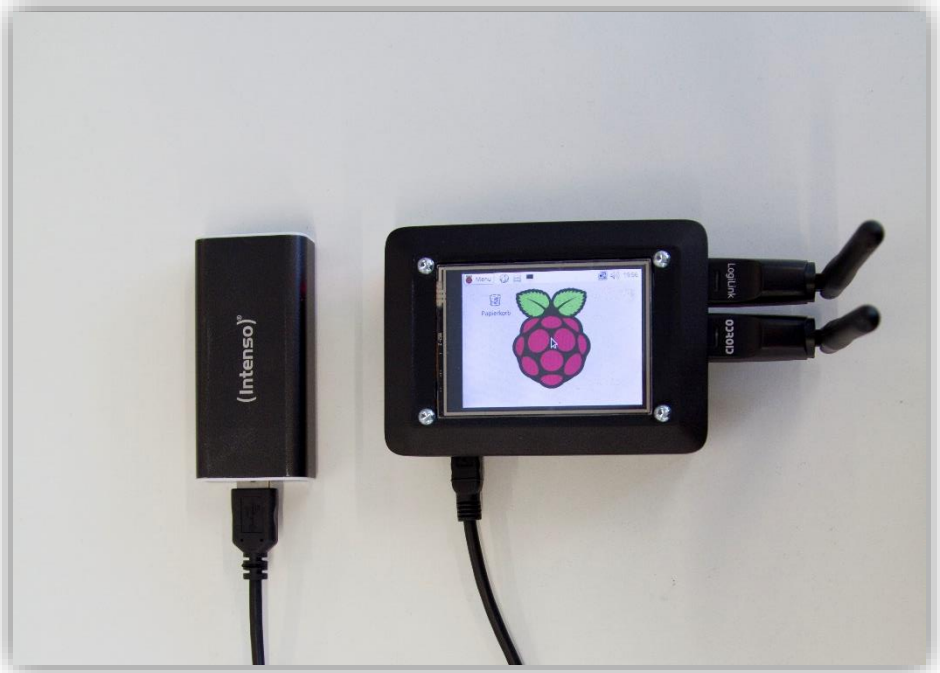
Rogue GSM Hotspot

- Cost: ~ 300 $



Mitm WI-FI Hotspot

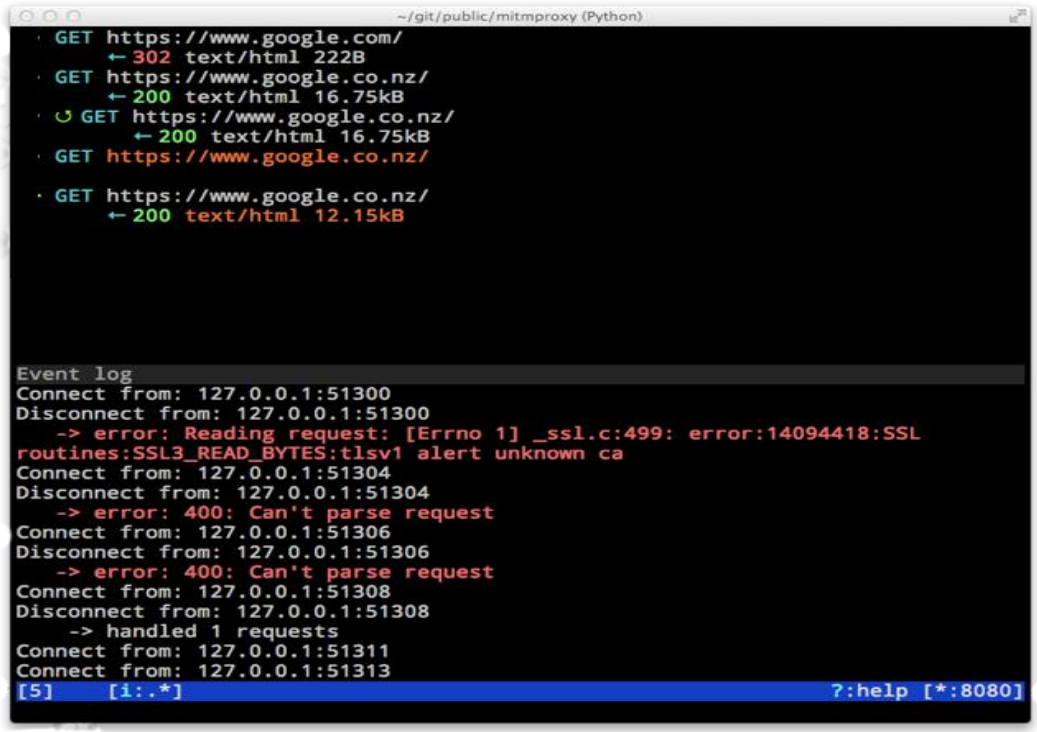
- Cost: ~60$



OR

Arp-Spoofing

- Cost: **arpspoof**, **iptables** and **(mitm)-proxy** are for free !



Remote Code Injection Example

Special zip Entry

```
/tmp$ unzip -l zipfile.zip
Archive:  zipfile.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
       22  2016-06-28 13:49   ../../../tmp/dir2/badfile.txt
       24  2016-06-28 13:43   file1.txt
---------                     -------
       46                     2 files
```

Unzip

```
/tmp$ unzip zipfile.zip -d ./dir1/
Archive:  zipfile.zip
warning:  skipped "../" path component(s) in ../../../tmp/dir2/badfile.txt
 extracting: ./dir1/tmp/dir2/badfile.txt
 extracting: ./dir1/file1.txt
```

Unzip

```
/tmp$ unzip zipfile.zip -d ./dir1/
Archive:  zipfile.zip
warning:  skipped "../" path component(s) in ../../../tmp/dir2/badfile.txt
 extracting: ./dir1/tmp/dir2/badfile.txt
 extracting: ./dir1/file1.txt
```

```
/tmp$ find /tmp/dir1/
/tmp/dir1/
/tmp/dir1/file1.txt
/tmp/dir1/tmp
/tmp/dir1/tmp/dir2
/tmp/dir1/tmp/dir2/badfile.txt
/tmp$
```

No escaping

```
/tmp$ unzip -: zipfile.zip -d ./dir1/
Archive:  zipfile.zip
 extracting: ./dir1/../../../tmp/dir2/badfile.txt
 extracting: ./dir1/file1.txt
```

No escaping

```
/tmp$ unzip -: zipfile.zip -d ./dir1/
Archive:  zipfile.zip
 extracting: ./dir1/../../../tmp/dir2/badfile.txt
 extracting: ./dir1/file1.txt
```

```
/tmp$ ls /tmp/dir1/
      file1.txt

/tmp$ ls /tmp/dir2/
      badfile.txt
```

Observed Update Traffic

Observed Update Traffic

GET-Requests of Application:

```
…
http://downloads7.xxxxxxxx-labs.com/bases/upd/upd-0607g.xml
http://ipm.xxxxxxxx.com/600eb07a-2926-4407-b014-d3e8c77b0086.zip
http://ipm. xxxxxxxx.com/eeea9321-5eac-4709-9046-8475ee951c82.zip
http://downloads7.xxxxxxxx-abs.com/bases/mobile/ksrm//rootdetector.jar
…
```

Observed Update Traffic

replace .zip file with attack file

GET-Requests of Application:

```
…
http://downloads7.xxxxxxxx-labs.com/bases/upd/upd-0607g.xml
http://ipm.xxxxxxxx.com/600eb07a-2926-4407-b014-d3e8c77b0086.zip
http://ipm.xxxxxxxx.com/eeea9321-5eac-4709-9046-8475ee951c82.zip
http://downloads7.xxxxxxxx-abs.com/bases/mobile/ksrm//rootdetector.jar
…
```

Content of the Attack File

```
unzip -l 600eb07a-2926-4407-b014-d3e8c77b0086.zip
Archive:  600eb07a-2926-4407-b014-d3e8c77b0086.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
       16  2015-09-15 18:57   ../../../../../../../../../../../../
../../../../../../../../../../../data/data/com.kms.free/app_bases/pdm.jar
     4042  2015-08-28 18:49   1000_768.css
     6078  2015-08-28 18:49   AntiVirus_Premium.html
      335  2015-08-28 18:49   [Content_Types].xml
      867  2015-08-28 18:49   meta.xml
     3216  2015-08-28 18:49   respond.min.js
```

Structure of Target App Folder

```
./app_bases/pdm.cfg
./app_bases/pdm.jar
.
.
.
.
./some_other_files
.
.
.
```

contains classes.dex
(executable)

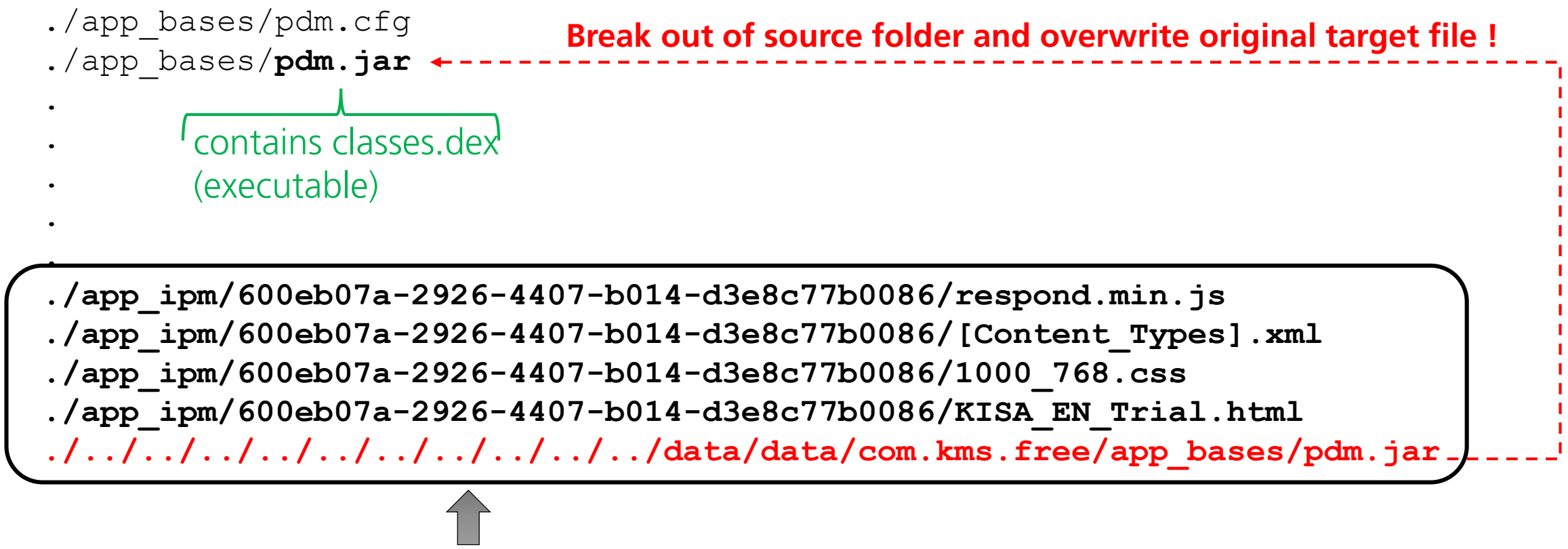
Unzip Received File

```
./app_bases/pdm.cfg
./app_bases/pdm.jar
.
.
.
.
.
./app_ipm/600eb07a-2926-4407-b014-d3e8c77b0086/respond.min.js
./app_ipm/600eb07a-2926-4407-b014-d3e8c77b0086/[Content_Types].xml
./app_ipm/600eb07a-2926-4407-b014-d3e8c77b0086/1000_768.css
./app_ipm/600eb07a-2926-4407-b014-d3e8c77b0086/KISA_EN_Trial.html
./../../../../../../../../../../data/data/com.kms.free/app_bases/pdm.jar
```

contains classes.dex (executable)

Advertisement files + attacker code extracted from zip archive !

Overwrite Original File



Injected Code

```
./app_bases/pdm.cfg
./app_bases/pdm.jar
.
.
.
.
.
```

contains classes.dex
with injected code

Injected File with attacker code !

```
./app_ipm/600eb07a-2926-4407-b014-d3e8c77b0086/respond.min.js
./app_ipm/600eb07a-2926-4407-b014-d3e8c77b0086/[Content_Types].xml
./app_ipm/600eb07a-2926-4407-b014-d3e8c77b0086/1000_768.css
./app_ipm/600eb07a-2926-4407-b014-d3e8c77b0086/KISA_EN_Trial.html
```

Advertisement files transfered by a zip archive !

Summary of Findings

	AndroHelm	Avira	CM	ESET	Kaspersky	McAfee	Malwarebytes
DOS	X	X				X	x
Premium	X			X			
Wipe/Lock	X						
HTTP		X	X		X		X
ScanEngine		X	X				X
Tapjacking			X				
RCE			X		X		
SSL Vuln				X			X
Crypto				X			X
XSS						X	

http://sit4.me/av-advisories

Responsible Disclosure

- 6/7 vendors fixed vulnerabilities

Responsible Disclosure

- 6/7 vendors fixed vulnerabilities

- Fails during RD:
  - Expired public key
  - PGP key was not matching with email address
  - No or less feedback about fixing

Responsible Disclosure

- 6/7 vendors fixed vulnerabilities

- Fails during RD:
  - Expired public key
  - PGP key was not matching with email address
  - No or less feedback about fixing

- One did not reply – but contacted at VB2015 ☺

Lessons learned…

- Do external code audits on your apps
- Room for improvement in the RD process
- Vulnerabilities in mobile apps can be also found in the PC counterpart (cross check)
- Also security software can contain vulnerabilites

sit4.me/av-advisories

Stephan Huber
Email: stephan.huber@sit.fraunhofer.de

Siegfried Rasthofer
Email: siegfried.rasthofer@sit.fraunhofer.de

Twitter: **@teamsik**
Website: https://team-sik.org