SMARTPHONE (ANDROID) MALWARE

Developments, Analysis methods, Research@IAIK

Peter Teufl
IAIK/Graz University of Technology
peter.teufel@iaik.tugraz.at
New dangers/possibilities

Android malware developments, examples, conclusions

Research@IAIK

Malware analysis methods
• Peter Teufl (peter.teufl@iaik.tugraz.at)

• Research, lectures (networks, cloud, smartphones)

• Smartphone security, cloud security, knowledge mining, machine learning, audits

• Finishing my PHD (knowledge mining)
Introduction
Possibilities vs. Threats
Malware Evolution
Malware Analysis
Research @IAIK

IAIK / GRAZ

Institute for Applied Information Processing and Communications
- Application oriented research
- Academic teaching activity
- Independent information center
- Support secure information society

IAIK

Graz University of Technology

Security focus

Thursday, July 14, 2011
IAIK/A-SIT

• Prof. Reinhard Posch: head of institute, CIO of Austria, e-Government

• Cryptography, RFID, chip design, design and verification

• e-Government: Citizen card, e-identity, secure signatures, cloud

• A-SIT (Vienna): security audits together with Austrian national bank (OENB), other audits in public institutions
A-SIT - IAIK
SMARTPHONES

Introduction
Possibilities vs. Threats
Malware Evolution
Malware Analysis
Research @IAIK

Thursday, July 14, 2011
## SMARTPHONES TODAY

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>approx. 1 Ghz (dual cores)</td>
</tr>
<tr>
<td>GPU</td>
<td>OpenGL</td>
</tr>
<tr>
<td>RAM</td>
<td>512MB-1GB</td>
</tr>
<tr>
<td>Storage</td>
<td>16-64 GB</td>
</tr>
<tr>
<td>Network</td>
<td>GSM, UMTS, WiFi, Bluetooth, NFC, LTE</td>
</tr>
<tr>
<td>Sensors</td>
<td>GPS, Accelerometer, Gyroscope, Compass</td>
</tr>
<tr>
<td>Sensors</td>
<td>Camera(s), Microphone, Flash light, Light</td>
</tr>
<tr>
<td>Displays</td>
<td>up to 960 × 640</td>
</tr>
<tr>
<td>OS</td>
<td>Highly sophisticated, comparable to Desktop OS</td>
</tr>
<tr>
<td>Applications</td>
<td>App Stores</td>
</tr>
<tr>
<td>Interface</td>
<td>Multitouch (Usability!!!)</td>
</tr>
<tr>
<td>Internet</td>
<td>HSDPA 2-3 MBIT, LTE</td>
</tr>
</tbody>
</table>

**Introduction**

**Possibilities vs. Threats**

**Malware Evolution**

**Malware Analysis**

**Research @IAIK**

Thursday, July 14, 2011
POSSIBILITIES

• New applications (Android, IOS), UI
• Navigation (car, maritime...)
• Augmented Reality
• Multimedia
• Games
• Cloud, social networks
POSSIBILITIES COME ALONG WITH NEW THREATS

- New technologies
- Mobility (!) and applications
- Mixing of private and business use cases
NEW TECHNOLOGIES

Introduction
Possibilities vs. Threats
Malware Evolution
Malware Analysis
Research @IAIK

Attacker

UMTS
WLAN

Desktop OS
Permanent Internet connection
SMS/MMS
Phone

Sensors
Applications

Microphone A-GPS Camera NFC Browser Many...

Thursday, July 14, 2011
MOBILITY AND APPLICATIONS

• Available data: Position, microphone, camera!

• Easy access to phones (beer after work: iPhone 4 prototype)

  • private area: installing spy ware

  • business/private area

• Apps are used for every private/business area

  • Sport, Navigation, Augmented Reality, SPYING!!!
MIXING OF PRIVATE AND BUSINESS USE CASES

• Other mobile devices (laptops, netbooks) not comparable

• Current security policies are not adapted (Companies are not aware of the need!)

• Used in all private areas: what about the sensitive data?

• Malware, phishing, theft, malware, spy apps? tracking? microphone? get data (emails, business applications)?
EXAMPLE FOR DATA

• Looking at emails
  • Sensitive information (financial data, project data)
  • Social network (private and business)
  • Account data (passwords, social engineering)
• Appointments (when and where)
• Example: Attack on Twitter in 2009...
SECURITY FUNCTIONS

• Many built into the smartphone OS however:
  • PIN/Password length?
  • Working encryption?
  • Theft?
  • Application sources?
  • Update frequency? Delta updates?
IMPLICATIONS

• All new... (Apple, Google)
• New ideas (e.g. mobile payment via NFC) smartphone distribution on the increase
• New malware
• Laptop vs Feature Phone vs Smartphone
• Current policies, analysis frameworks partly (not) applicable
SMARTPHONE MALWARE

• Why writing malware for smartphones?

• Location (organized crime, botnets??), NFC payments, NFC locks, microphone, camera (extortion??)

• Mobile banking, social information, data...

• Business vs. private use! Very sensitive data (emails, etc.)

• Cyberwar (look at recent examples, RSA and Lockheed)
SMARTPHONE MALWARE

• Industrial spying (much easier with smartphone)
• Established trust in downloads... (Walled garden?)
• Exploit trust of users in app stores, sources
• Currently, open system (Android) is pounded with malware
SMARTPHONE MALWARE

• Android: under attack every day, many examples..., many users, cheap phones, easy to use

• IOS: not more secure (in certain areas even less), BUT WALLED GARDEN!

• Blackberry OS: very secure architecture, many options, proprietary, not based on well known OS, code

• Windows Phone: Also walled garden market share currently very small
FOCUS ON ANDROID

Dynamic analysis of Golddream.A Trojan: This is a recent malware that targets the Android platform. This Trojan...
3 hours ago

Android Malware Found in Angry Birds Add-On Apps -
http://j.mp/pJ0Wrn
23 hours ago

- Huge increase in the last months
- Creating bots, targeting private information
- Malware evolves
- Seems like arms race on PC
MALWARE TRENDS...

- Source: topsy.com, Twitter search interface
WALLED GARDEN

• Apple/Microsoft/RIM

• Identification of developer

• Strict rules: API access, content, limitation to what the application has access

• Limited possibilities: no deep system integration

• Very strict approval process
GOOGLE’S APPROACH

• Open approach

• No identification of developer, just register and deploy apps

• Remove afterwards approach: Remote (UN)INSTALL

• If necessary install removal tool

• What does the open approach imply?
OPEN APPROACH

• Much deeper system integration for apps:
  • SMS catching, sending without the user’s knowledge
  • Rooted phones (everything is possible)
  • Background services, hiding in the system, access to everything
• Untrusted sources!!!
• And then there is “security software”...
ANDROID MALWARE HISTORY

• Simple apps with too many permissions reading private data
• Alternative sources (links on emails, websites)
• Relying on the user, not exploiting system vulnerabilities
• Exploiting some weaknesses (research: e.g. install package permission on Android)
• Legitimate spyware/security software (huge issue)
SECURITY SOFTWARE?  SPYWARE?

• Security software: remote wipe, remote commands, show phone on map etc. (rooted vs. standard phone), scan for viruses, deeply integrate into the system

• Spyware: show phone on map, read emails, forward SMS, switch on microphone (Faceniff!)

• Covers a lot of the same functionality: private and business area

• Just depends on who installs the software
**Title: Wife Tracker**

Know your wife's position anytime and anywhere. Just install this app on her phone, and track her, via Web, or with our free tracker viewer. In a future version we will add a notification feature, that alarms via email for position changes.
ANDROID MALWARE HISTORY

• Changing nature

• Malware attacks the system (root kits)

• Meaning: No need to rely on permissions etc., since root access is there

• After basic malware is installed, other apps are downloaded
ANDROID MALWARE HISTORY

- Bots, private data, premium numbers
- Problem: Google Kill Switch/remote installation does not work anymore, since malware modifies the system
- So Google cannot remove everything
- Problem: Malware adapts to new detection mechanisms
ANDROID MALWARE HISTORY

• Current malware:
  • Encrypting exploits, payloads to avoid detection
  • Switching from Java to native code to make reverse engineering more difficult
  • Typical infection: Still over the user by copying existing apps and repacking them
ANDROID MALWARE HISTORY

• More sophisticated attacks

• Attacking the browser, services other vulnerabilities

• Exploiting bugs in the security architecture (sandboxes) etc. if root access is not that easy to achieve, circumventing the permission system

• Injecting malware in open WLANs

• Attacking the stores directly
ANDROID MALWARE HISTORY

• We are at the beginning
• As analysis/security methods get better, malware evolves
• More sophisticated attacks to come (targeted attacks)
• Currently, focus on Android
• Same arm’s race as in the PC area (P2P botnets now!)
MALWARE CONCLUSIONS

• Increase in sophistication
• Installation by user
• Exploits simple publication in market, some security holes
• Some malware that attacks custom ROMs
• Stealing information, setting up bots
• Sophisticated malware that hides itself is just emerging...
RECENT MALWARE

• DroidDream
• DroidKungfu
• Others...
• VERY IMPORTANT: legitimate spyware/security software
DROIDDREAM

• Also: DroidDream, RootCager, and myournet

• March 2011

• Over 50 infected apps on Android Market

• 50,000 to 200,000 downloads!

• Copies of legitimate apps infected with malware
DROIDDREAM

- Replaces manifest file with its own activity
- Starts malicious activity, which starts a background service called **Setting**
- Then starts original application
DROID DREAM

• [http://blogs.iss.net/archive/Examining%20the%20recent.html](http://blogs.iss.net/archive/Examining%20the%20recent.html)

• Setting service starts up and:
  • attempt to get root access via two exploits
  • udev exploit (CVE-2009-1185)
  • rageagainstthecage exploit (ADB bug is exploited)
DROIDDREAM

- Sending IMEI, IMSI, ProductID to URL
- Installs download manager
- Download manager contacts command server periodically
- Installs any other package
DROIDKONGFU

• Mai 2011
• Uses the same two exploits as DroidDream
• Found in 8 alternative Chinese Android markets
• Sends private information
DROIDKONGFU

• Exploit code is encrypted
• More code moves from Java to native C
• Conclusions? Malware evolves quickly on Android
• Arms race as we know it from the PC?
OTHERS

• Golddream, Plankton, Crusewind

• Capturing SMS/MMS, call history, SMS relays, bots...

• Pretending to be a racing game

• The list goes on and on...
Summary: New opportunities and problems in private and business areas

Giving support to public institutions in Austria (A-SIT)

Raise awareness, highlight threats, analyze platforms, analyze smartphone infrastructures, also mGovernment
• In order to gain knowledge:

• PHDs, students, projects, lectures, research at IAIK

• Focus on security
• Generic threats

• Secure elements on smartphones

• Mobile signatures on smartphones

• NFC (upcoming)

• Malware (sophisticated attacks, detection)
• Malware focus (since Oct. 2010)

• Market analysis (metadata)

• Sophisticated attacks: Circumventing permissions

• Static analysis, network traffic analysis

• How to attack secure elements? NFC?
MARKET ANALYSIS

• Use metadata from store to learn more about apps

• Knowledge mining

• Description, permissions, download counts, category

• Detect anomalies (e.g. wallpapers with GPS permissions)

• Find relations (e.g. term “position” is related to “husband, wife”)

• Clustering applications (terms, permissions)
MARKET ANALYSIS

- Description terms related to “position”
• Permissions related to wife, husband
MARKET ANALYSIS

• Currently working on automated download of new apps every day

• Automated analysis? Filters (e.g. certain permission)?

• Getting an overview of new apps?

• Retrieving APKs and doing static analysis?
CIRCUMVENTING PERMISSIONS

• Permissions for GPS, SEND SMS, CALL PHONE etc.

• Shown to the user (assuming expert user)

• Permission system conveys level of trust

• The context is important! READ CONTACTS and INTERNET together?
CIRCUMVENTING PERMISSIONS

• Assuming you install a wallpaper with READ CONTACTS, GPS, INTERNET permissions

• No description that could explain this...

• Expert user would probably not install this app

• ==> Trust in the permission system (if understood)
CIRCUMVENTING PERMISSIONS

• But probably the user would install an app with GPS alone and a second one with INTERNET alone?

• How to break the permission context?

• Use IPC (Intents, Broadcasts, Services, Log files, side channels)
CIRCUMVENTING PERMISSIONS

• Distribute permissions over two or more apps:
CIRCUMVENTING PERMISSIONS

• Where is the malicious code?

• E.g. GPS service provided by one app and used by another with INTERNET permission?

• Where to find the malicious code?

• So we cannot rely on permission screening in the market

• Backdoors, injection of source code in well known apps, apps with no permissions (acquired from other apps)
CIRCUMVENTING PERMISSIONS

• Based on these insights: Thinking more about malware detection

• Which methods?

• What can be detected?

• Doing further research
MALWARE, DETECTION?

- Current Malware: Typically simple to detect
- But that won’t stay that way
  - Look at botnet evolution: latest one p2p!
- Detection, analysis?
- Methods...

Thursday, July 14, 2011
MALWARE ANALYSIS

- User
- Expert User
- Security tool (virus scanner)
- Security Analyst:
  - dynamic, static, network traffic analysis, market analysis
- Market provider (e.g. Google, Apple)
PROPERTIES, ENVIRONMENT FOR SCANNING

• Analysis depends on the environment

• E.g. avg user:
  • Standard phone
  • Installed application
  • Store App Metadata

### Table

<table>
<thead>
<tr>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
</tr>
<tr>
<td>One App</td>
<td>Some Apps</td>
<td>Arbitray Apps</td>
</tr>
</tbody>
</table>
STANDARD PHONE

- Standard installation
- Not rooted
- No modified ROM
- Average user

<table>
<thead>
<tr>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
</tr>
<tr>
<td>One App</td>
<td>Some Apps</td>
<td>Arbitrary Apps</td>
</tr>
</tbody>
</table>
ROOTED PHONE

• Standard installation, but rooted
• Much deeper system integration
• Hidden applications
• Access to more data
• Original OS
MOD PHONE

- Changed ROM
- Very deep system changes
- Kernel, APIs, OS, API calls
- Getting every information
- Modifying information: tainting etc.

<table>
<thead>
<tr>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
</tr>
<tr>
<td>One App</td>
<td>Some Apps</td>
<td>Arbitray Apps</td>
</tr>
</tbody>
</table>
USER INTERACTION

• User/analysis interacts with app
• Executes functions
• Goes trough the UI
• Generates traffic, plays a game etc.
STORE APP METADATA

- Data from the market, accessible to everyone
- Description
- Permissions
- Ratings, reviews
- Download counts, versions, release dates, links
EXT METADATA

• Data available in the application package
• IPC interfaces
• Activities
• Intent filters etc.
• Available on local phone, within the APK

<table>
<thead>
<tr>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
</tr>
<tr>
<td>One App</td>
<td>Some Apps</td>
<td>Arbitray Apps</td>
</tr>
</tbody>
</table>
WHERE IS THE APPLICATION?

- Installed application: on the phone
- Installation package: package available
- Network traffic: access to traffic generated by phone/application
ACCESS TO HOW MANY APPS?

• Just a single app: e.g. as package, installed

• Some apps: e.g. on a phone, multiple packages for combined analysis

• Arbitrary apps: access to a large number of apps (e.g. the market provider, or downloaded meta-data from a store)
Now to the analysis methods

From

First line of defense: User

To

Dynamic information flow analysis
USER

• USING the smartphone and its apps!
• First line of defense (best option?)
• Where does the app come from?
  • Market
  • URL in emails etc.
• Alternative Market

<table>
<thead>
<tr>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
</tr>
<tr>
<td>One App</td>
<td>Some Apps</td>
<td>Arbitrarily Apps</td>
</tr>
</tbody>
</table>
• Should not care/understand
• permissions and implications
• problems of alternative sources
• implications of private spying
• User who employs malware deliberately?
• Security software installed on another phone?
• When is security software equal to spy ware?
• Just depends on the installation context...
Walled Garden has huge advantage here

- no security software also means no sophisticated spyware
- assumes that user does not know anything about security

But: other disadvantages
• most malware gets installed by the user

• at least means: that the systems are not that insecure

• Is not a defense...
  User does/should not care about security (e.g. permissions, relations, implications)

• User is deliberately installing malware...
EXPERT USER

• Check permissions
• Relation between text and permissions
• Understand sources
• Installs security tools (or spyware)
• Is security aware: phishing, trojans, malware, mobile banking, passwords etc.

<table>
<thead>
<tr>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
</tr>
<tr>
<td>One App</td>
<td>Some Apps</td>
<td>Arbitray Apps</td>
</tr>
</tbody>
</table>
EXPERT USER

• +++

• Knows about security

• Understands dangers

• Installs virus scanners, avoids dangerous sources etc.

• -- -- --

• Even experts cannot avoid everything

• Much more knowledge on how to distribute malware to others
SECURITY TOOL

- Access to ext. metadata of other apps
- Running, installed apps
- Security settings
- Features like remote wipe/locate
- On rooted phone: much more (packages, network traffic, additional measures)
SECURITY TOOL

•+++•

• Supports security on phone
• Simple checks (signatures)
• Complex tools do not help the user
• Analysis methods limited (plus?)
• Can be also used as malware/spyware by others

<table>
<thead>
<tr>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
</tr>
<tr>
<td>One App</td>
<td>Some Apps</td>
<td>Arbitray Apps</td>
</tr>
</tbody>
</table>
STATIC ANALYSIS

• Analyze application package
• No real execution
• Java: byte code, decompiled source
• C: disassemble (PC...)
• Wide range of analysis

<table>
<thead>
<tr>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
</tr>
<tr>
<td>One App</td>
<td>Some Apps</td>
<td>Arbitray Apps</td>
</tr>
</tbody>
</table>
STATIC ANALYSIS

• Android
  • Manifest: Permissions, Activities, IPC
  • DEX File: Decompile to get Java code
  • Extract API calls (e.g. getPhoneNumber())
  • Get called intents
STATIC ANALYSIS

• More sophisticated

• Information flow analysis

• Deep analysis of code, follow control flows, watch assignments

• Can get very complicated when countermeasures in place

• Better to do it dynamically then
STATIC ANALYSIS

• Current research

• Automated APK analysis

• Extracting method calls, intents, etc.

• Angry birds dump:
STATIC ANALYSIS

MethodExtractorOutput class_name=android.location.LocationManager class_is_used=true
getLatitude=MethodOutput [searched_for=true is_used=true
src_lines=[
    double d1 = location.getLatitude();
    double d1 = AdManager.d().getLatitude();
    double d1 = D.getLatitute();
    double d1 = a.android.location.Location fld.getLatitude();]]

getLatitude=MethodOutput [searched_for=true is_used=true
src_lines=[
    double d1 = location.getLatitude();
    double d1 = AdManager.d().getLatitude();
    double d1 = D.getLatitute();
    double d1 = a.android.location.Location fld.getLatitude();]]
STATIC ANALYSIS

• ++++

• automatic (no user interaction)

• signatures, quick overview

• ----

• countermeasures: encryption, obfuscation

• what does the code do?
**NETWORK TRAFFIC**

- **Network traffic**

- **Hosts**

- **URLs (HTTP vs. HTTPS)**

- **Data: IDs, Locations etc.**

```
POST /mobile/track_sdk_event HTTP/1.1
User-Agent: Dalvik/1.4.0 (Linux; U; Android 2.3.3; GT-I9000 Build/GINGERBREAD)
Host: android.heyzap.com
Connection: Keep-Alive
Content-Length: 134
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

POST /ad_source.php HTTP/1.1

"o":{"a":"url","u":"http://googleads.g.doubleclick.net/aclk?aid=1&ai=BY2f7KBMTh7W9G1msgbXtpGiCZmSk0kByYfMnxrAjbcBsNgEAEYASC32gFPaHR0cDovL2FuZHJvaWQuYWRtb21uYWxAcWZvcm1vYmlsZWZvcnkyY29t"}
```

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Source IP</th>
<th>Protocol</th>
<th>Method</th>
<th>Path</th>
<th>User-Agent</th>
<th>Headers</th>
</tr>
</thead>
<tbody>
<tr>
<td>193.170.140.70</td>
<td>0.0.2.5</td>
<td>TCP</td>
<td>SYN</td>
<td>/mobile/track_sdk_event</td>
<td>Dalvik/1.4.0</td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>ACK</td>
<td>/mobile/track_sdk_event</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>0.0.2.5</td>
<td>TCP</td>
<td>SYN</td>
<td>/mobile/track_sdk_event</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>0.0.2.5</td>
<td>TCP</td>
<td>ACK</td>
<td>/mobile/track_sdk_event</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>93.170.140.70</td>
<td>TCP</td>
<td>SYN</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>ACK</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>SYN</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>ACK</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>SYN</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>ACK</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>SYN</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>ACK</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>SYN</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>ACK</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>SYN</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>ACK</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>SYN</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
<tr>
<td>193.170.140.70</td>
<td>10.0.2.5</td>
<td>TCP</td>
<td>ACK</td>
<td>/ad_source.php</td>
<td><em>null</em></td>
<td><em>null</em></td>
</tr>
</tbody>
</table>
NETWORK TRAFFIC

• Current research
• Analyze and visualize traffic generated by Android applications
• Get an idea on what the app is doing on the net
• Connections to servers, which URLs, private information

Thursday, July 14, 2011
NETWORK TRAFFIC

• ++++

• Just WLAN with network sniffer needed

• Traffic cannot be hidden (except enc.)

• -- -- --

• Mapping between apps an traffic

• Encryption

• User interaction

<table>
<thead>
<tr>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
</tr>
<tr>
<td>One App</td>
<td>Some Apps</td>
<td>Arbitray Apps</td>
</tr>
</tbody>
</table>
DYNAMIC ANALYSIS

- Information flow security
- Modified ROM required
- TaintDroid: tainting sensitive information and following the flow (e.g. when sent over network)
- Large number of sophisticated analyses
DYNAMIC ANALYSIS

• ++++

• Many detection methods

• Countermeasure against obfuscation

• -- -- --

• User interaction (with the app)

• Analysis takes a long time
STORE METADATA

• Use metadata from store to learn more about apps

• Description, permissions, download counts, category

• Detect anomalies (e.g. wallpapers with GPS permissions)

• Find relations (e.g. term “position” is related to “husband, wife”)

• Clustering applications (terms, permissions)
STORE METADATA

• Currently working on automated download of new apps every day

• Automated analysis? Filters (e.g. certain permission)?

• Getting an overview of new apps?

• Retrieving APKs and doing static analysis?
+++ STORE METADATA +++

• Overview of a large number of apps
• Learning about descriptions, permissions, relations
• Finding new types of applications (e.g. spyware)
• General knowledge mining

• No access to packages, only superficial analysis
STORE PROVIDER

- Google, Apple
- Resources, access to every app
- In-depth knowledge about system
- Relations between apps (IPC, intents), developers
- All kind of analyses

<table>
<thead>
<tr>
<th></th>
<th>Standard Phone</th>
<th>Rooted Phone</th>
<th>Modified ROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>User interaction</td>
<td></td>
<td>Ext. App Metadata</td>
<td>Store App Metadata</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Application Package</td>
<td>Network Traffic</td>
<td></td>
</tr>
<tr>
<td>One App</td>
<td></td>
<td>Some Apps</td>
<td>Arbitray Apps</td>
</tr>
</tbody>
</table>

Thursday, July 14, 2011
LINKS

• http://www.iaik.at

• http://www.a-sit.at

• https://sites.google.com/site/iaikmobisec/

• peter.teufl@iaik.tugraz.at