FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Analyse der Kommunikation von Android-Apps

Spioniert mein Handy mich aus?

Andreas Galauner und Michael Stahl
Lehrgebiet Datennetze

IT Forensik
FH Aachen

Agenda

- Einleitung
- Herangehensweise
- Analyse von Applikationen
- Erstes Fazit
- Automatisierung und Verschlüsselung
- Auswertung

Problemstellung

Smartphones:

- Helfer im alltäglichem Leben
- Alle Informationen eines Notizbuches
- Weitere Funktionen, um Daten über Nutzer zu sammeln (GPS)
- Internetzugriff (Soziale Netzwerke)
- Unzählige Programme sind verfügbar, selten von bekannten Herausgebern

Problemstellung

„26 Prozent der Nutzer sorgen sich um die Sicherheit im mobilen Internet bei der Nutzung von Apps. 82 Prozent fühlen sich von App-Anbietern nicht ausreichend über die Verwendung ihrer persönlichen Daten informiert“
(Pressemitteilung 35 vom 07.02.2012 des Ministeriums für Verbraucherschutz)

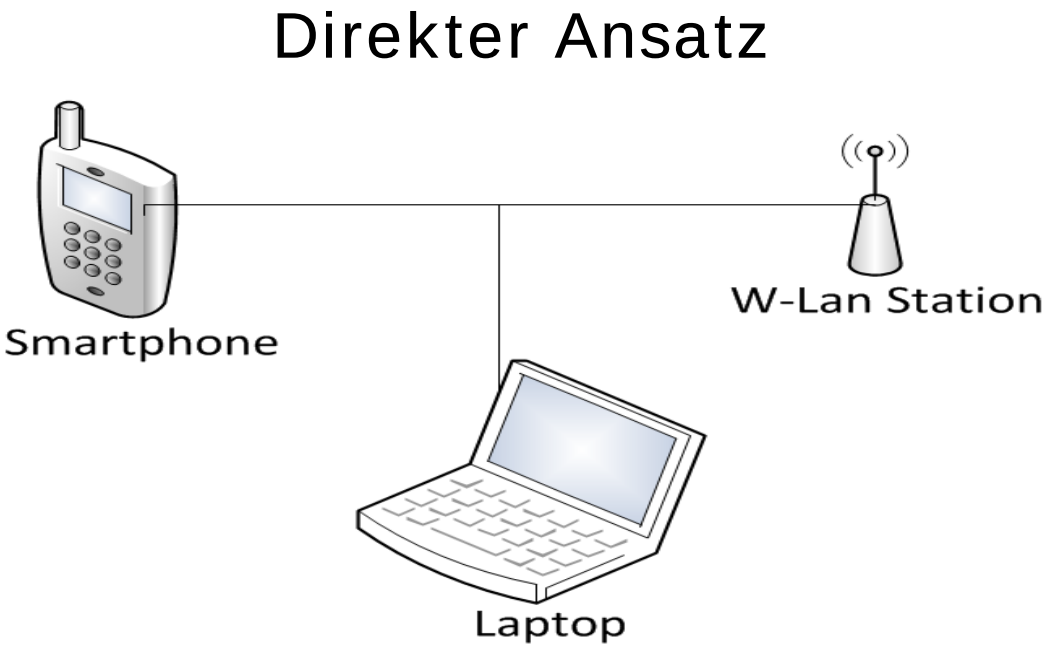
„Apple iPhone zeichnet alle Nutzer-Geodaten auf“
(Heise Online 21.04.2011)

Ziel

- Vollständiges Verfolgen des Sendens von sensitiven Daten
- Zuverlässige Auswertung der ermittelten Daten
- Zielsystem: Android

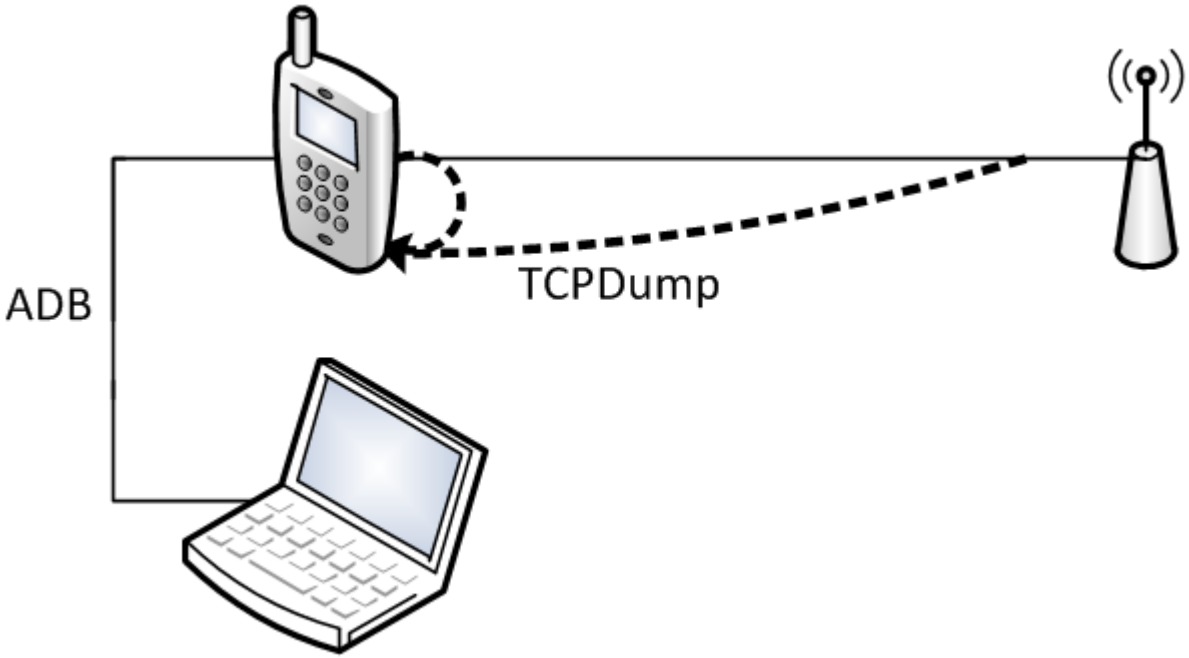
- Entwicklung eines Verfahrens, um zu verfolgen, was für Daten vom Smartphone aus wirklich versendet werden.

Herangehensweise



- Teile der Kommunikation fehlen (GPRS/UMTS)
- Umständlich, da man nicht immer mit offenen Netzwerken arbeiten möchte

Herangehensweise



- Eigene Applikation steuert TCPDump um Internetverbindung zu belauschen (automatische Erkennung der Schnittstelle)
- Applikation liefert eine Auswertung
- Detaillierte Auswertung mit Wireshark

Analyse von Applikationen

Fruit Ninja

- Installationen: 1.000.000 – 5.000.000
- Berechtigungen:
  - ungefährer Standort
  - Telefonstatus
  - Internetzugriff
  - aktive Apps abrufen
- Bewertung durch eigene Applikation
  - 5 x IMEI
  - 6 x AndroidID
  - 5 x MCC+ MNC

MCC = Mobile Country Code
MNC = Mobile Network Code

Analyse von Applikationen

Fruit Ninja

```
Hypertext Transfer Protocol
  [truncated] GET /?p=android&i=46397573-C748-4CD5-BFCD-DB612D04A52D&s=320x50&rt=mcnative&rtv=0&av=1.6.2.10
  Cookie: \r\n
  User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.4; de-de; Nexus S Build/GRJ22) AppleWebKit/533.1 (KHTML, l
  Host: ads.mobclix.com\r\n
  Connection: Keep-Alive\r\
  \r\n
  [Full request URI [truncated]: http://ads.mobclix.com/roid&i=46397573-C748-4CD5-BFCD-DB612D04A52D&s
```

```
0050  2d 43 37 34 38 2d 34 43  44 35 2d 42 46 43 44 2d   -C748-4C D5-BFCD-
0060  44 42 36 31 32 44 30 34  41 35 32 44 26 73 3d      .10&u=35 59210401
0070  32 30 78 35 30 26 72 74  3d 6d 63 6e 61 74 69      54211&an did=8b79
0080  65 26 72 74 76 3d 30 26  61 76 3d 31 2e 36 2e      223818e0 bae0&v=3
0090  2e 31 30 26 75 3d 33 35  35 39 32 31 30 34 30
00a0  35 34 32 31 31 26 61 6e  64 69 64 3d 38 62 37
00b0  32 32 33 38 31 38 65 30  62 61 65 30 26 76 3d
00c0  2e 31 2e 31 26 63 74 3d  77 69 66 69 26 64 6d
00d0  4e 65 78 75 73 2b 53 26  68 77 64 6d 3d 63 72
00e0  73 70 6f 26 73 76 3d 32  2e 33 2e 34 26 75 61 3d   spo&sv=2 .3.4&ua=
00f0  4d 6f 7a 69 6c 6c 61 25  32 46 35 2e 30 2b 25 32   Mozilla% 2F5.0+%2
0100  38 4c 69 6e 75 78 25 33  42 2b 55 25 33 42 2b 41   8Linux%3 B+U%3B+A
0110  6e 64 72 6f 69 64 2b 32  2e 33 2e 34 25 33 42 2b   ndroid+2 .3.4%3B+
0120  64 65 2d 64 65 25 33 42  2b 4e 65 78 75 73 2b 53   de-de%3B +Nexus+S
0130  2b 42 75 69 6c 64 25 32  46 47 52 4a 32 32 25 32   +Build%2 FGRJ22%2
0140  39 2b 41 70 70 6c 65 57  65 62 4b 69 74 25 32 46   9+Applew ebKit%2F
0150  35 33 33 2e 31 2b 25 32  38 4b 48 54 4d 4c 25 32   533.1+%2 8KHTML%2
0160  43 2b 6c 69 6b 65 2b 47  65 63 6b 6f 25 32
0170  56 65 72 73 69 6f 6e 25  32 46 34 2e 30 2b          3.1&o=0& ap=0&l=d
0180  62 69 6c 65 2b 53 61 66  61 72 69 25 32 46
0190  33 2e 31 26 6f 3d 30 26  61 70 3d 30 26 6c          e_DE&mcc =262&mnc
01a0  65 5f 44 45 26 6d 63 63  3d 32 36 32 26 6d
01b0  3d 30 33 20 48 54 54 50  2f 31 2e 31 0d 0a          =03 HTTP /1.1..Co
```

Analyse von Applikationen

Fruit Ninja verschlüsselt

627	122.013642	207.171.163.152	https	192.168.178.21	60194	TCP	54 https > 60194 [ACK] Seq=5663 Ack=263 Win=523904 Len=0
628	122.014013	207.171.163.152	https	192.168.178.21	60194	TLSv1	97 Change Cipher Spec, Encrypted Handshake Message
629	122.014151	192.168.178.21	60194	207.171.163.152	443	TCP	54 60194 > https [ACK] Seq=263 Ack=5706 Win=17520 Len=0
630	122.156166	192.168.178.21	60194	207.171.163.152	443	TLSv1	493 Application Data
631	122.285424	207.171.163.152	https	192.168.178.21	60194	TCP	54 https > 60194 [ACK] Seq=5706 Ack=702 Win=523456 Len=0
632	122.344130	207.171.163.152	https	192.168.178.21	60194	TCP	1514 [TCP segment of a reassembled PDU]
633	122.344501	192.168.178.21	60194	207.171.163.152	443	TCP	54 60194 > https [ACK] Seq=702 Ack=7166 Win=20440 Len=0
634	122.345121	207.171.163.152	https	192.168.178.21	60194	TCP	1514 [TCP segment of a reassembled PDU]
635	122.345372	192.168.178.21	60194	207.171.163.152	443	TCP	54 60194 > https [ACK] Seq=702 Ack=8626 Win=23360 Len=0
636	122.345959	207.171.163.152	https	192.168.178.21	60194	TCP	1514 [TCP segment of a reassembled PDU]
637	122.346249	192.168.178.21	60194	207.171.163.152	443	TCP	54 60194 > https [ACK] Seq=702 Ack=10086 Win=26280 Len=0
638	122.346834	207.171.163.152	https	192.168.178.21	60194	TCP	1514 [TCP segment of a reassembled PDU]
639	122.347138	192.168.					
640	122.347995	207.171.	https	192.168.178.21	60194	TLSv1	1514 Application Data
641	122.348280	192.168.178.21	60194	207.171.163.152	443	TCP	54 60194 > https [ACK] Seq=702 Ack=13006 Win=32120 Len=0
642	122.348900	207.171.163.152	https	192.168.178.21	60194	TCP	1514 [TCP segment of a reassembled PDU]
643	122.349149	192.168.178.21	60194	207.171.163.152	443	TCP	54 60194 > https [ACK] Seq=702 Ack=14466 Win=35040 Len=0
644	122.349982	207.171.163.152	https	192.168.178.21	60194	TLSv1	336 Application Data
645	122.350201	192.168.178.21	60194	207.171.163.152	443	TCP	54 60194 > https [ACK] Seq=702 Ack=14748 Win=37960 Len=0
646	122.350614	207.171.163.152	https	192.168.178.21	60194	TCP	1514 [TCP segment of a reassembled PDU]
647	122.350870	192.168.178.21	60194	207.171.163.152	443	TCP	54 60194 > https [ACK] Seq=702 Ack=16208 Win=40880 Len=0
648	122.351317	207.171.163.152	https	192.168.178.21	60194	TCP	1514 [TCP segment of a reassembled PDU]
649	122.351558	192.168.178.21	60194	207.171.163.152	443	TCP	54 60194 > https [ACK] Seq=702 Ack=17668 Win=43800 Len=0
650	122.351970	207.171.163.152	https	192.168.178.21	60194	TCP	1514 [TCP segment of a reassembled PDU]

Erstes Fazit

- Mitschnitte sind vollständig
- Auswertung scheint zuverlässig
- Ohne großen Aufwand mobil einsetzbar

- 30 Applikationen untersucht
- Bei 20 Applikationen konnte das Versenden von sensitiven Daten nachgewiesen werden. 15 von diesen an Dritte

Kommunikation oft mit SSL verschlüsselt und daher mit diesem Verfahren nicht zu verfolgen

Automatisierung und Verschlüsselung

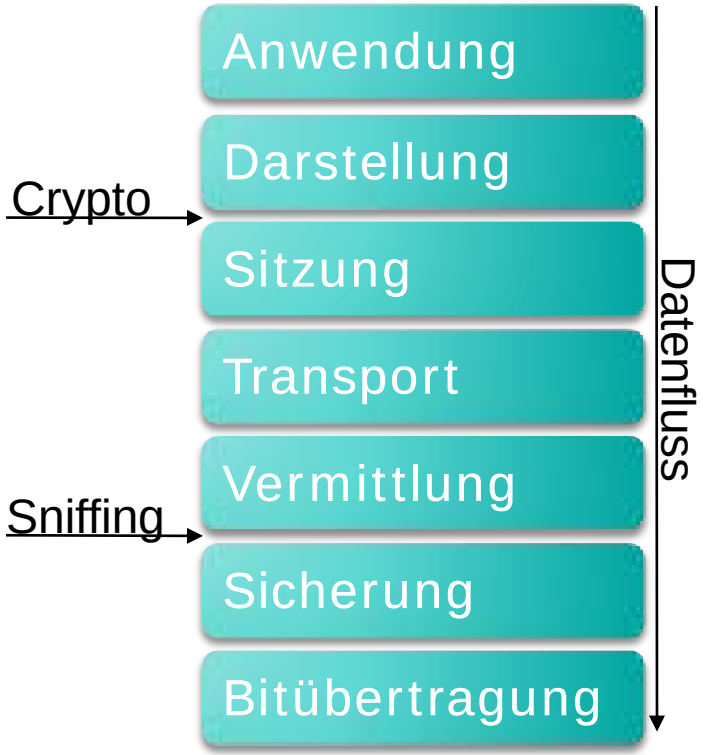
Automatisierter Vorgang

Neuer Ansatz: Automatisierung (inklusive Analyse verschlüsselter Daten)

- 2 in Python geschriebene Scripts:
  1. Script zum Sammeln von Netzwerkdaten
  2. Script zur anschließenden Auswertung durch Suche nach Schlüsselwörtern
- Nutzen adb (Android Debugging Bridge) zur De-/Installation von zu untersuchenden Applikationen
- Daten werden durch tcpdump und sslsniff auf einem unbeteiligten Rechner gesammelt

Verschlüsselung

- Weit verbreitetes Protokoll zur sicheren Verschlüsselung von Datenverbindungen ist TLS (früher SSL)
- Durch ARP-Spoofing ist der gesamte Traffic auf der Sicherungsschicht (Schicht 2) einsehbar
- TLS (SSL) arbeitet aber auf Darstellungsschicht (Schicht 6)
  - Darunter bekommt man nur noch bereits verschlüsselte Daten



Verschlüsselung

Lösungen: AES oder RSA cracken, SSL Stripping oder SSL Sniffing

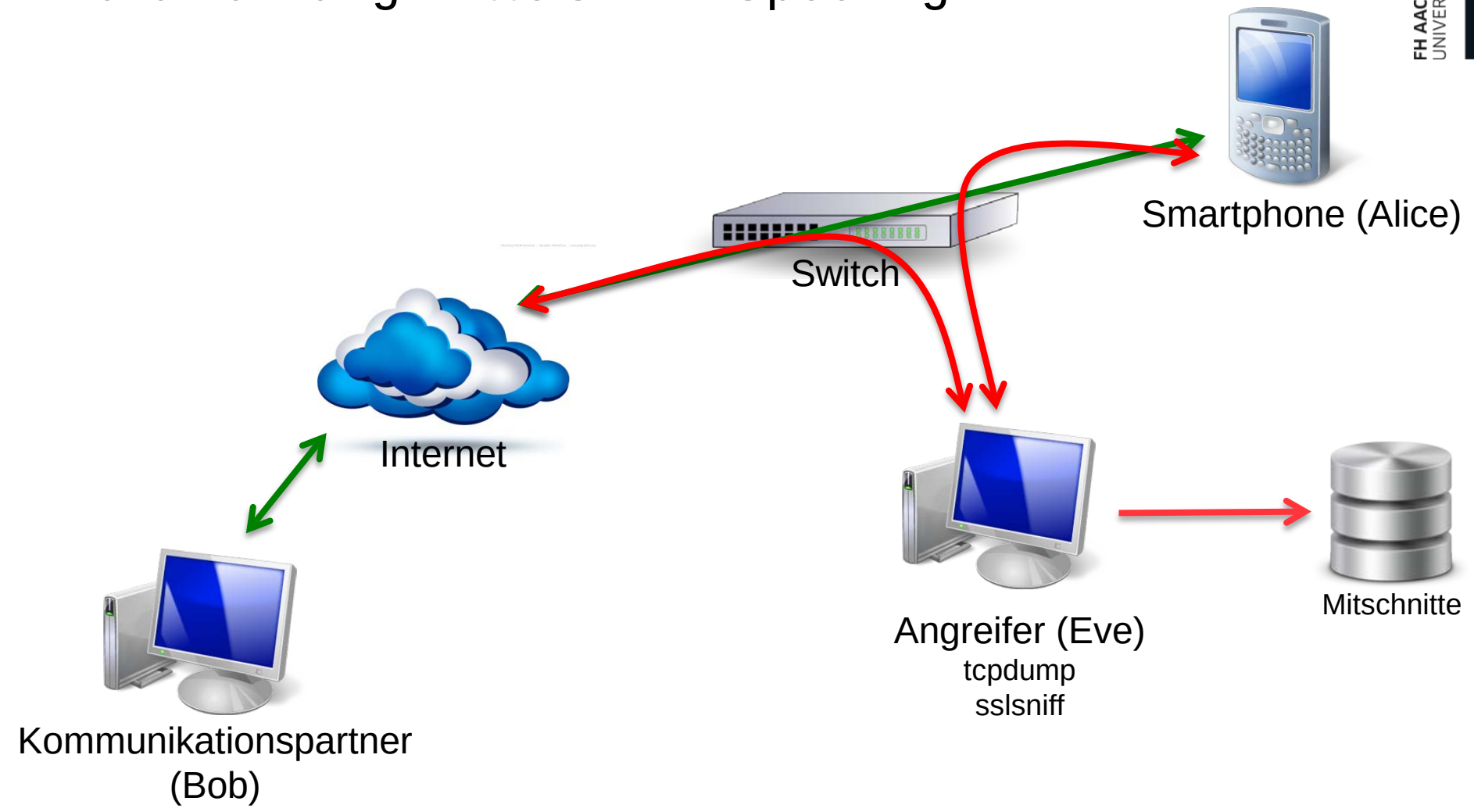
- AES oder RSA cracken: Eher nicht, nach heutigem Stand sicher

- SSL Stripping entfernt einfach jede Verschlüsselung und schickt Daten im Plaintext weiter

- SSL Sniffing entschlüsselt die Daten, verschlüsselt sie mit eigenem private Key und schickt sie weiter
  - Möglich in unserer Laborumgebung

Mitschneidevorgang

Durchführung mittels ARP-Spoofing



Auswertung

- FruitNinja
  - Verschickt Android-ID zusätzlich nochmal verschlüsselt
- Wind-Up-Kinght
  - Verschickt nichts unverschlüsselt
  - Verschickt verschlüsselt:
    - Providername
    - Providerkennung
    - Android ID
    - IMEI
- Kalorienzähler
    - Versendet Handynummer unverschlüsselt

Limitierungen

Immer noch Limitierungen vorhanden:

- Nach welchen Schlüsselwörtern sucht man?
  - Problem vor allem bei GPS-Location
    - Kommazahlen?
    - Welcher Dezimaltrenner? Punkt? Komma?
    - Wie viele Kommastellen
- Wie sind die Daten kodiert?
  - Momentan nur Suche nach ASCII möglich
  - Was ist mit Verschleierung von verschickten Daten?
  - Evtl. eigene Verschlüsselung genutzt
- False-Positives können immer entstehen
  - Manuelle Nachkontrolle nötig
- Ansatz ermöglicht kein Abhören mobiler Datenverbindungen

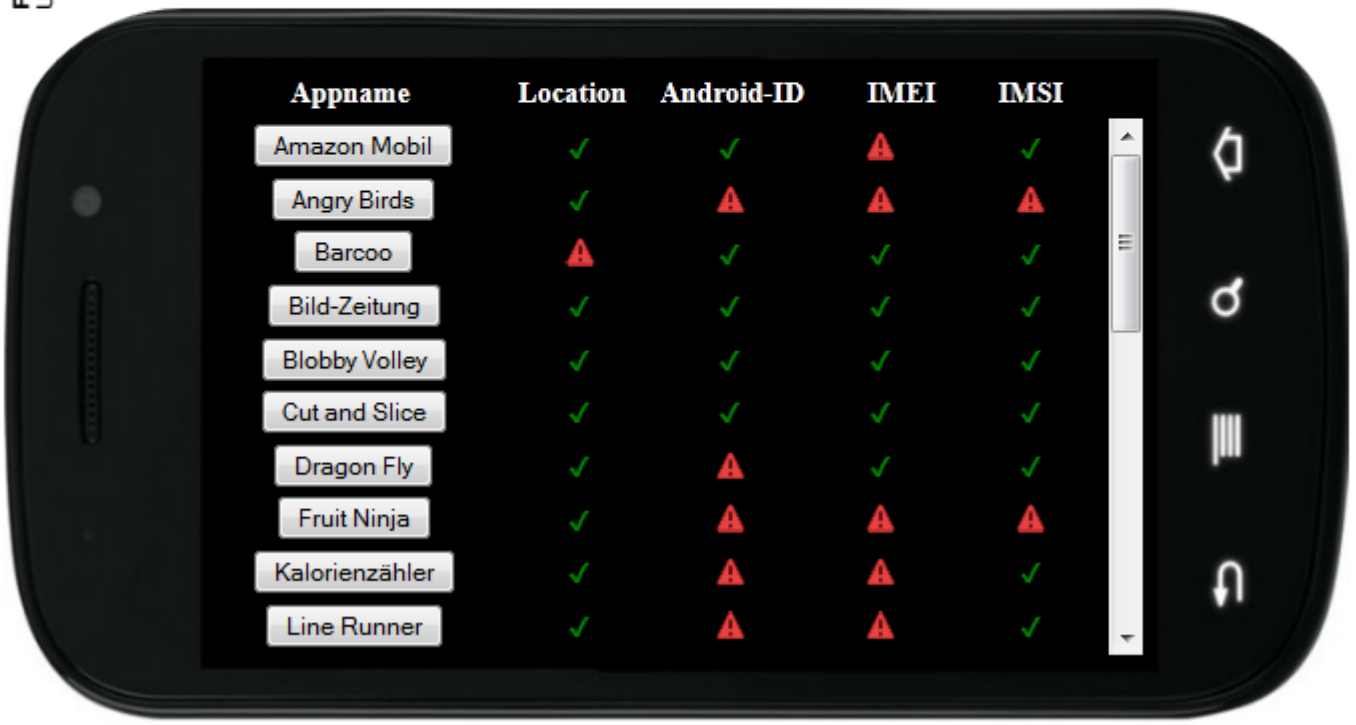
Internetpräsenz

FH AACHEN UNIVERSITY OF APPLIED SCIENCES

Spioniert mein Handy mich aus? – Hintergrund

Was bedeutet: Location, Android-ID, IMEI, IMSI?

IT Forensik FH Aachen



www.schuba.fh-aachen.de/appspy

Vielen Dank für Ihre Aufmerksamkeit!