Mobile Security
(Android OS)

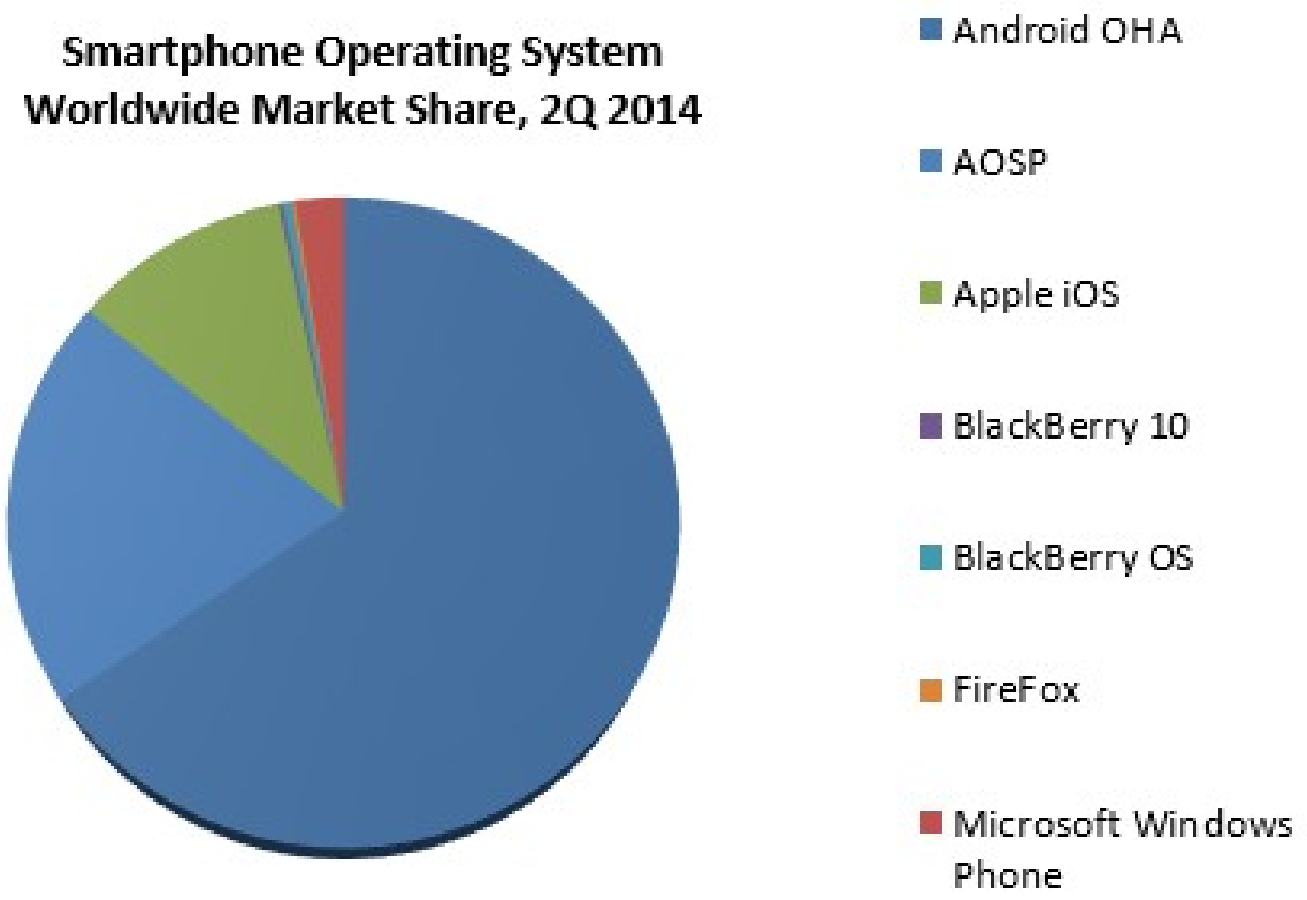
Ein Vortrag zur Sensibilisierung eines Benutzers im Umgang mit Smartphones und Tablets mit dem Android OS.

Inhaltsverzeichnis

Was ist Android?

- 2003 gründete Andy Rubin das Unternehmen Android
- 2005 kaufte Google Android
- Ab 2007 entwickelt Google mit 33 anderen Mitgliedern der Open Handset Alliance ein Mobiltelefon-Betriebssystem namens Android
- 22.10.2008 erstes Gerät mit dem AOS verfügbar (HTC Dream)

Marktanteil



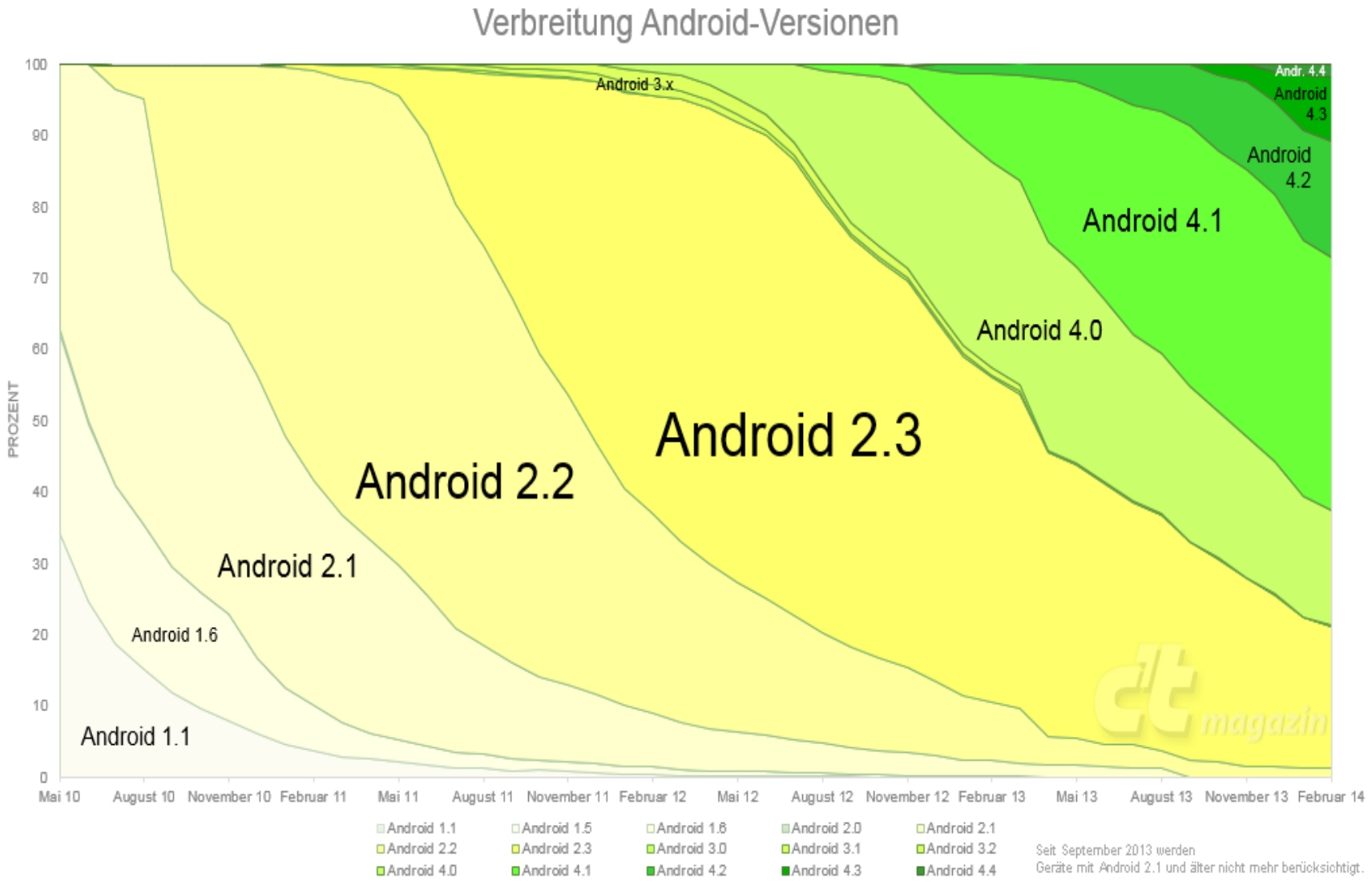
Schwächen des AOS
(Schlüsselrollen im AOS Ökosystem)

- Google
- CPU Manufactorers
  - ARM, Intel x86, MIPS
- SoC's = System on Chip Manufacturers
  - OMAP, Tegra, Exynos, Snapdragon
- ODM/OEM = Original Device/Equipment Manufacturers
  - Samsung, HTC, LG, ...
- Carriers
  - Telekom, Vodafone, O2, 1&1, ...

Schwächen des AOS
(schlechter Update-Mechanismus)

- Hardwarehersteller-/Mobilfunkanbieteraufsatz ausgeliefert
  - OS wird modifiziert/gebrandet
- keine Supportverträge zwischen Kunden und Herstellern
- Kein Backporting
- Längere Wartezeiten bei Updates/ bis gar keine Updates
- Ausnahme → Nexus-Serie
  - erhalten aktuelle Updates nach nur kurzer Verzögerung

Schwächen des AOS



Grundlegende Sicherheitskonzepte im AOS

- 1. Sandbox (übernommen von Linux)

  - ermöglicht Anwendungen den Zugang zu Dateisystem, RAM und anderen Ressourcen

  - Schränkt jedoch die IPC stark ein

- 2. App Permissions

  - schränken die Zugriffsberechtigungen einer App ein

  - sind meistens beim Installationsvorgang sichtbar

  - werden vom Entwickler gesetzt

• Apps sind das Einfallstor für Schadsoftware

- Zugriffsberechtigungen(Permissions) erlauben den Zugriff auf sensible Daten bzw. Hardware wie

  (Kontakte, int./ext. Speicher, SMS, Mikrofon , Kamera, GPS-Modul...)

- „dreiste“ ZB sind manchmal erkennbar
  - Taschenlampenapp, Kompassapp

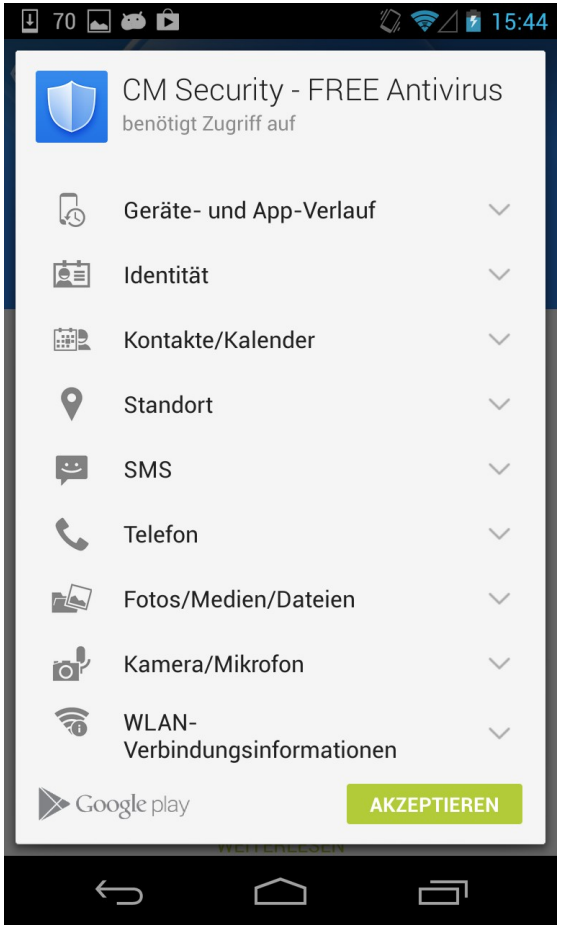
- Was ist mit komplexeren Apps ?

  - Antivirus, Multimedia, die im Normallfall viele ZB benötigen um ihre Dienste auszuführen

Bsp. Für Zugriffsberechtigungen

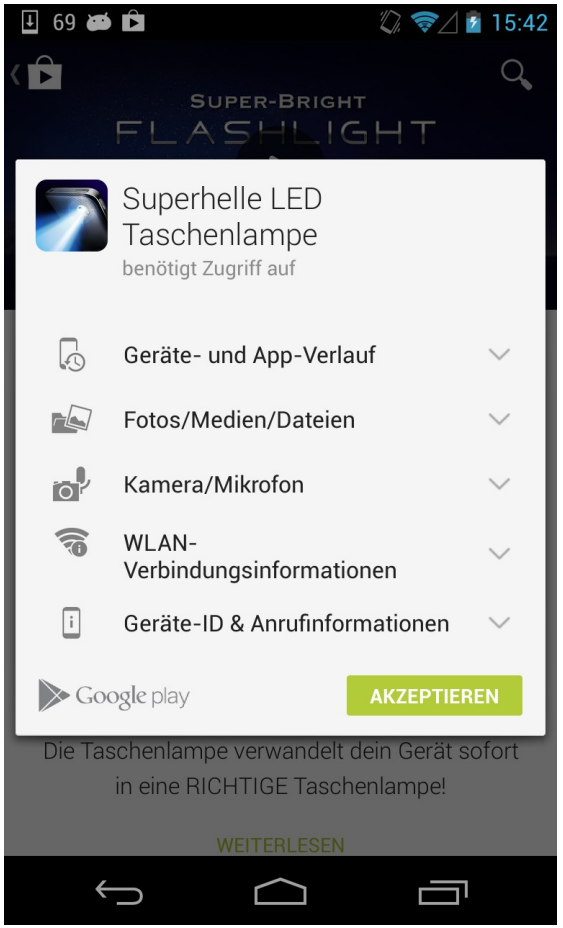
```
15      <uses-permission android:name="android.permission.GET_ACCOUNTS" />
16      <!--<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />  -->
17
18      <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
19      <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
20      <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
21
22      <uses-permission android:name="android.permission.READ_PHONE_STATE" />
23
24      <uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS" />
25
26      <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
27
28
29      <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
30
31      <uses-permission android:name="android.permission.INTERNET" />
32
33
34      <uses-permission android:name="android.permission.RECORD_AUDIO" />
35
36      <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
37
38      <uses-permission android:name="android.permission.CAMERA" />
39      <uses-feature android:name="android.hardware.camera" />
40
41
42      <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
```

Security Apps

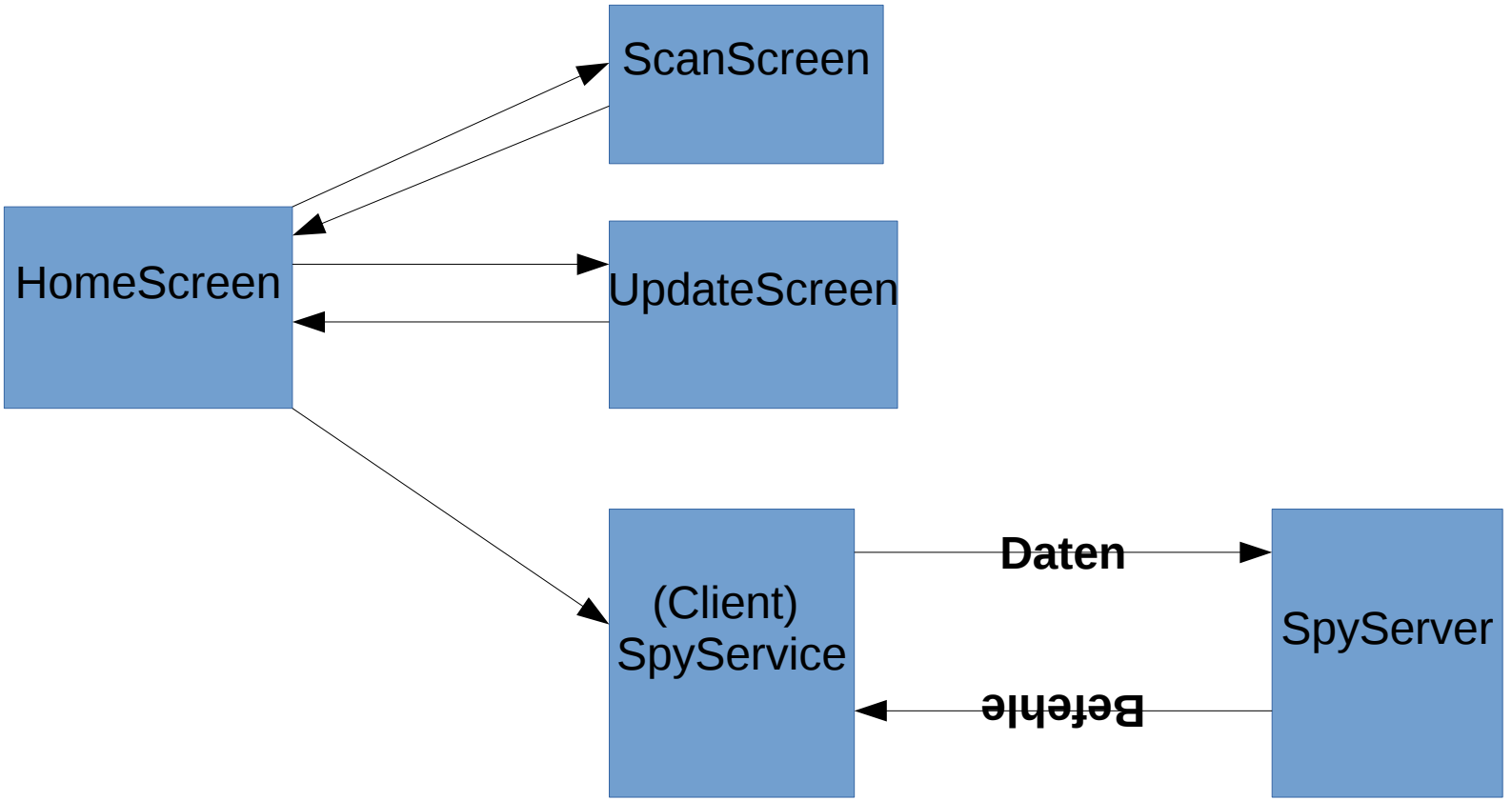


Taschenlampe aus dem Playstore

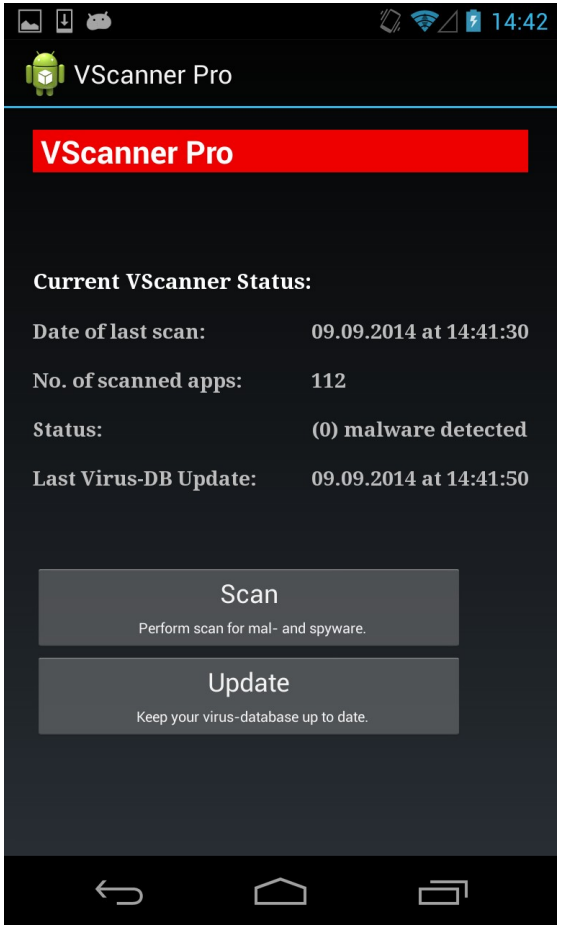
www.heise.de/security/meldung/Millionenfach-installierte-Android-App-schnueffelte-Nutzerdaten-aus-2062105.html

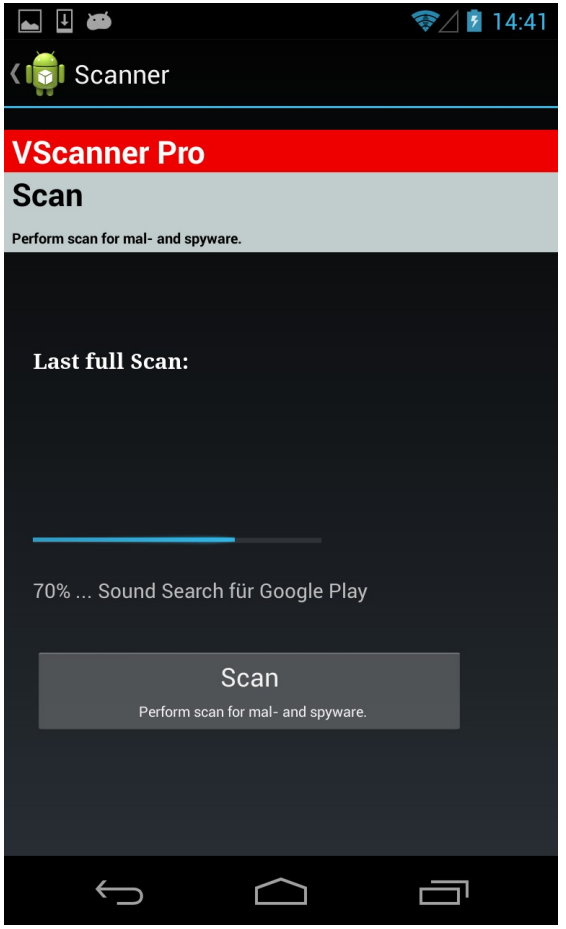


Aufbau meiner Virus App

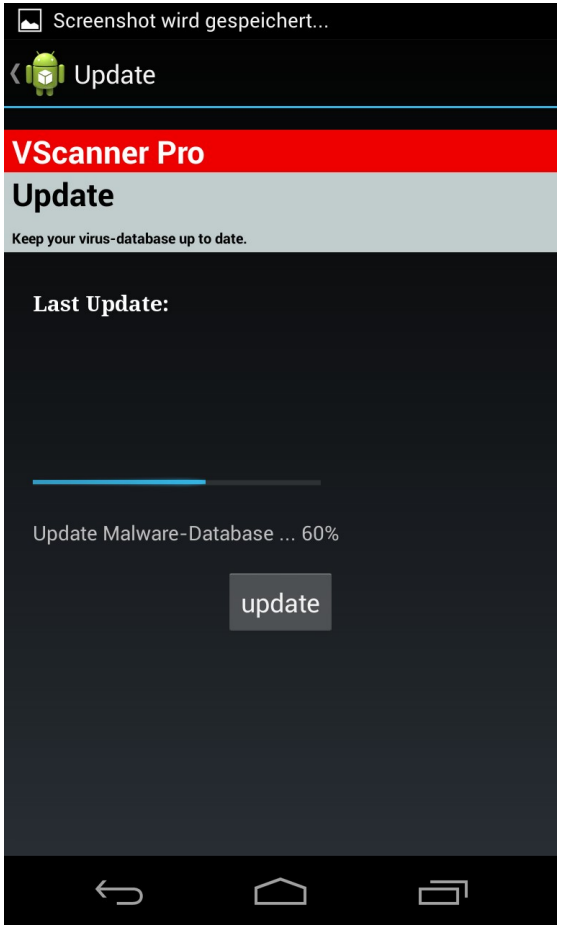


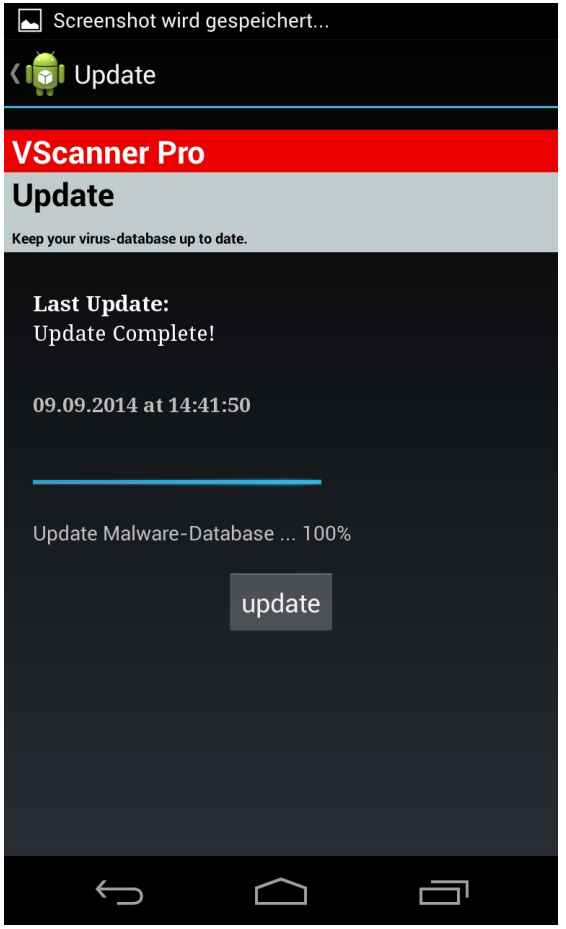
VirusDoc in der Ausführung
(sichtbarrer Teil)





VirusDoc in der Ausführung
(sichtbarrer Teil)





Ausblick

- Untersuchung des WLAN Tracking
- Schwachstellensuche in anderen apps mit Hilfe von speziellen Tools
- Erweiterung der App bzw. deren Aufteilung in separate Module und Einschleusung dieser in den Playstore

Quellenverzeichniss

- http://www.androidnext.de/news/android-forks-20-prozent-aller-smartphones-laufen-ohne-google-apps-tendenz-steigend/
- Google-Playstore
- http://www.heise.de/newsticker/meldung/Android-Verteilung-Updates-ziehen-langsam-an-2133882.html

Mobile Security
(Android OS)

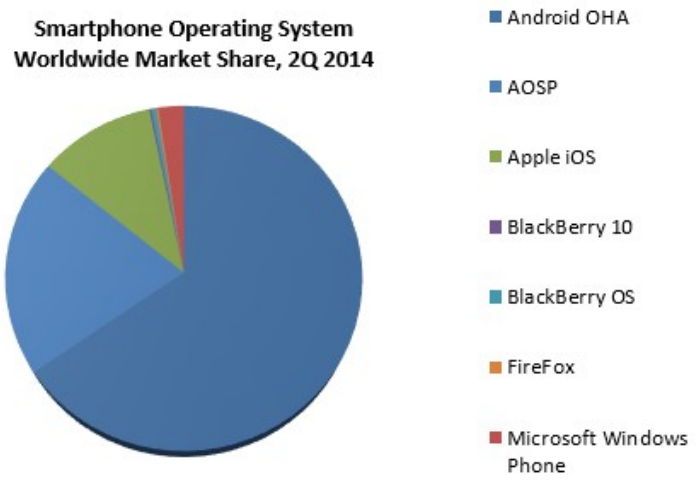
Ein Vortrag zur Sensibilisierung eines Benutzers im Umgang mit Smartphones und Tablets mit dem Android OS.

Inhaltsverzeichnis

Was ist Android?

- 2003 gründete Andy Rubin das Unternehmen Android
- 2005 kaufte Google Android
- Ab 2007 entwickelt Google mit 33 anderen Mitgliedern der Open Handset Alliance ein Mobiltelefon-Betriebssystem namens Android
- 22.10.2008 erstes Gerät mit dem AOS verfügbar (HTC Dream)

Marktanteil



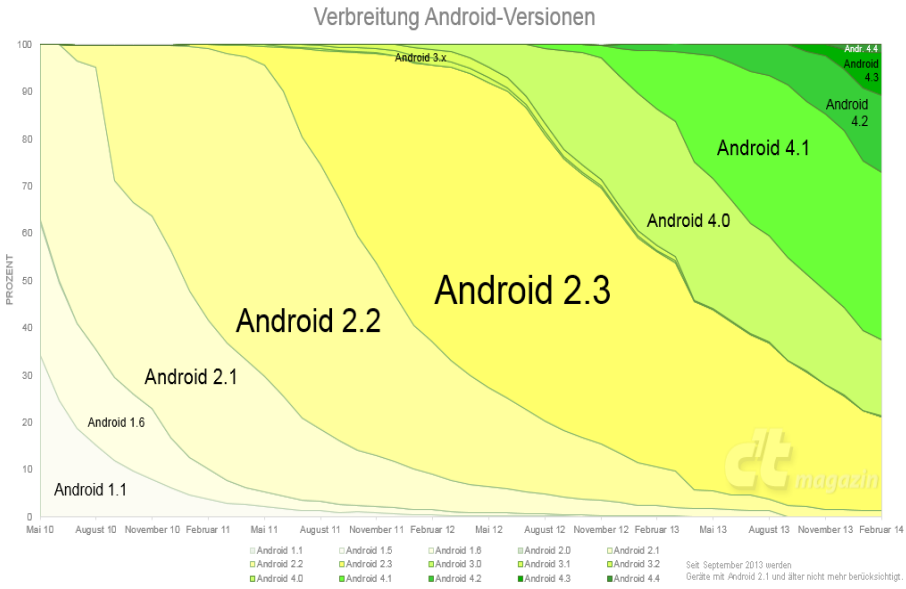
Schwächen des AOS
(Schlüsselrollen im AOS Ökosystem)

- Google
- CPU Manufactorers
  - ARM, Intel x86, MIPS
- SoC's = System on Chip Manufacturers
  - OMAP, Tegra, Exynos, Snapdragon
- ODM/OEM = Original Device/Equipment Manufacturers
  - Samsung, HTC, LG, ...
- Carriers
  - Telekom, Vodafone, O2, 1&1, ...

Schwächen des AOS
(schlechter Update-Mechanismus)

- Hardwarehersteller-/Mobilfunkanbieteraufsatz ausgeliefert
  - OS wird modifiziert/gebrandet
- keine Supportverträge zwischen Kunden und Herstellern
- Kein Backporting
- Längere Wartezeiten bei Updates/ bis gar keine Updates
- Ausnahme → Nexus-Serie
  - erhalten aktuelle Updates nach nur kurzer Verzögerung

Schwächen des AOS



Grundlegende Sicherheitskonzepte im AOS

- 1. Sandbox (übernommen von Linux)
  - ermöglicht Anwendungen den Zugang zu Dateisystem, RAM und anderen Ressourcen
  - Schränkt jedoch die IPC stark ein
- 2. App Permissions
  - schränken die Zugriffsberechtigungen einer App ein
  - sind meistens beim Installationsvorgang sichtbar
  - werden vom Entwickler gesetzt

• Apps sind das Einfallstor für Schadsoftware

- Zugriffsberechtigungen(Permissions) erlauben den Zugriff auf sensible Daten bzw. Hardware wie

  (Kontakte, int./ext. Speicher, SMS, Mikrofon , Kamera, GPS-Modul...)

- „dreiste“ ZB sind manchmal erkennbar
  - Taschenlampenapp, Kompassapp

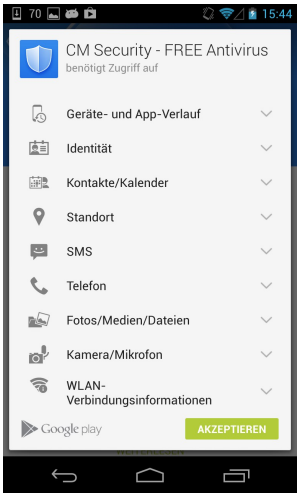
- Was ist mit komplexeren Apps ?

  - Antivirus, Multimedia, die im Normallfall viele ZB benötigen um ihre Dienste auszuführen

Bsp. Für Zugriffsberechtigungen

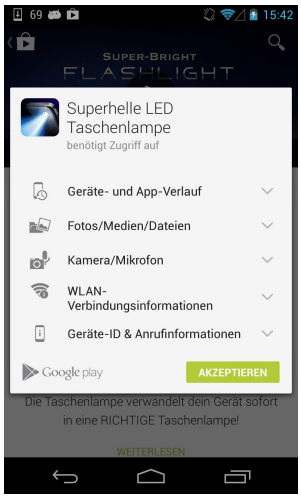
```
15      <uses-permission android:name="android.permission.GET_ACCOUNTS" />
16      <!--<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />  -->
17
18      <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
19      <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
20      <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
21
22      <uses-permission android:name="android.permission.READ_PHONE_STATE" />
23
24      <uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS" />
25
26      <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
27
28
29      <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
30
31      <uses-permission android:name="android.permission.INTERNET" />
32
33
34      <uses-permission android:name="android.permission.RECORD_AUDIO" />
35
36      <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
37
38      <uses-permission android:name="android.permission.CAMERA" />
39      <uses-feature android:name="android.hardware.camera" />
40
41
42      <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
```

Security Apps

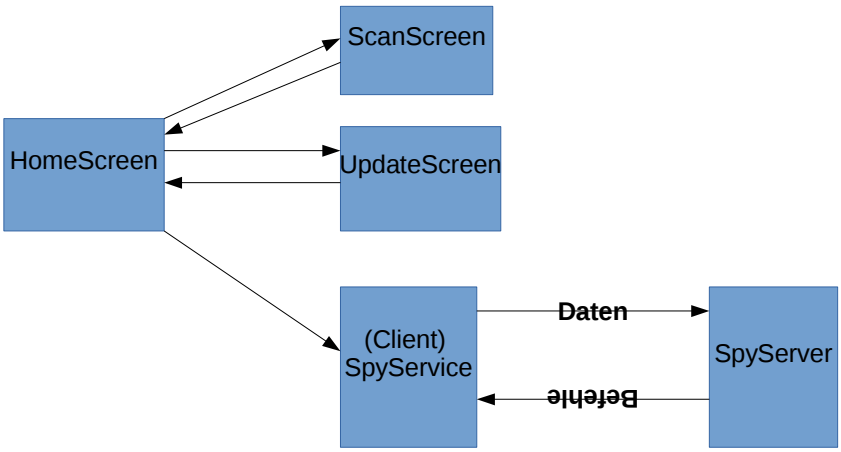


Taschenlampe aus dem Playstore

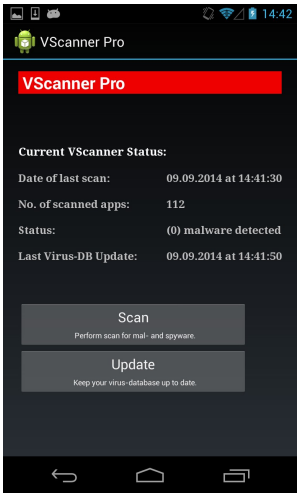
www.heise.de/security/meldung/Millionenfach-installierte-Android-App-schnueffelte-Nutzerdaten-aus-2062105.html

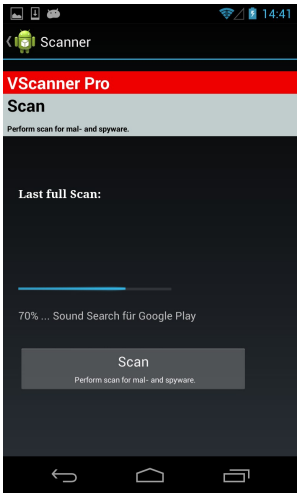


Aufbau meiner Virus App

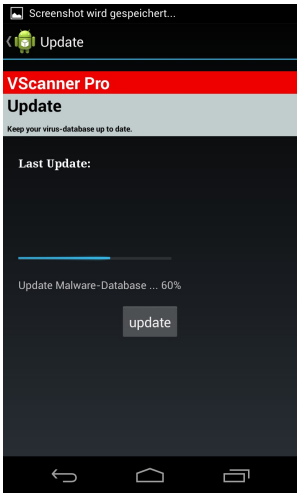


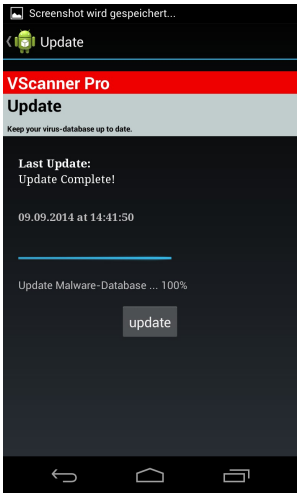
VirusDoc in der Ausführung
(sichtbarrer Teil)





VirusDoc in der Ausführung
(sichtbarrer Teil)





Ausblick

- Untersuchung des WLAN Tracking
- Schwachstellensuche in anderen apps mit Hilfe von speziellen Tools
- Erweiterung der App bzw. deren Aufteilung in separate Module und Einschleusung dieser in den Playstore

Quellenverzeichniss

- http://www.androidnext.de/news/android-forks-20-prozent-aller-smartphones-laufen-ohne-google-apps-tendenz-steigend/
- Google-Playstore
- http://www.heise.de/newsticker/meldung/Android-Verteilung-Updates-ziehen-langsam-an-2133882.html