secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

32. AIK-Symposium

Android: auf dem Weg zu einer sicheren Plattform und sicheren Apps

Sebastian Fritsch, secuvera GmbH

28.10.2016

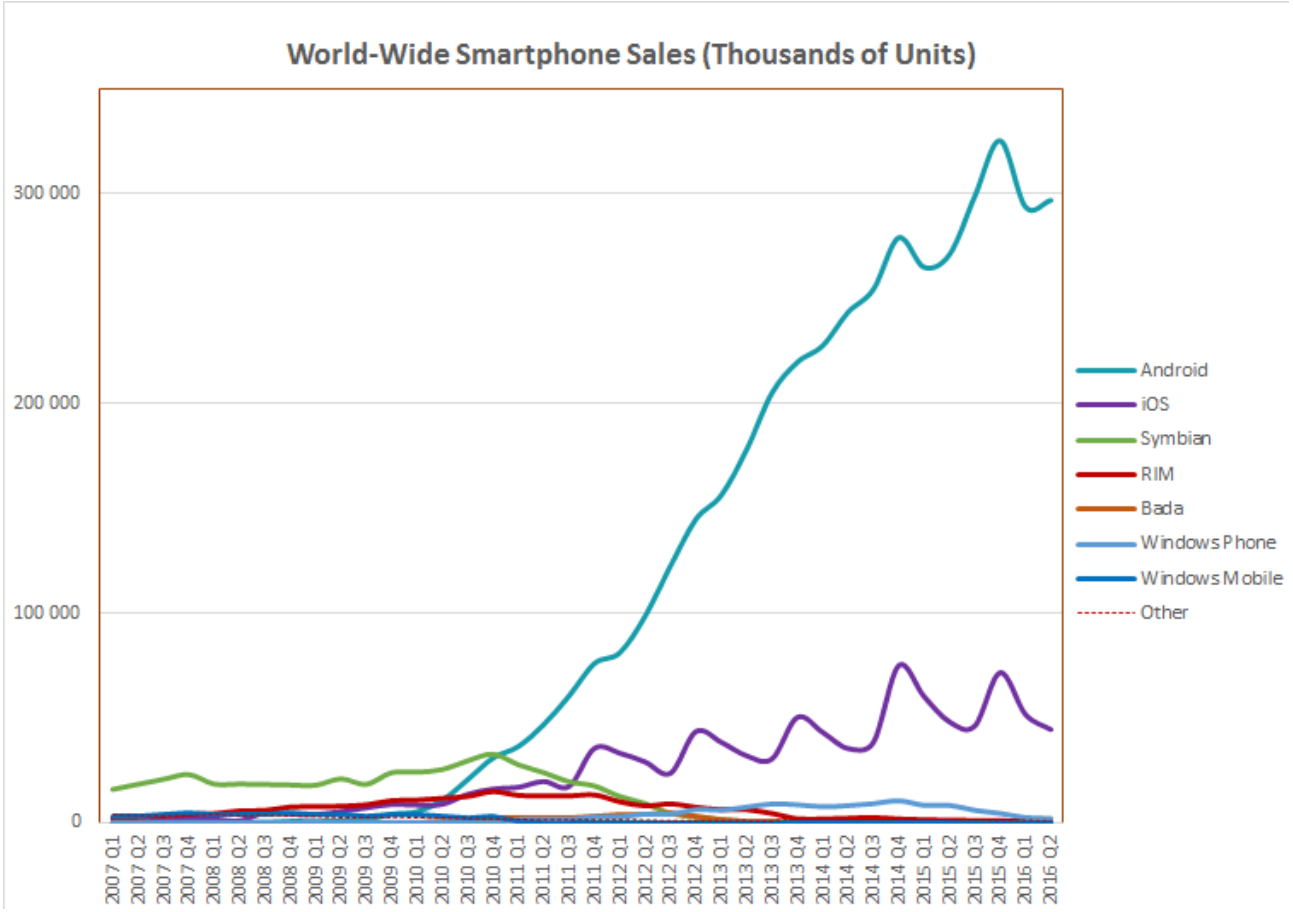
- Android Kontext und Historie
- Security & Privacy Probleme
- Basisproblem: die sichere Plattform
- Anwenderproblem: die Sichere App
- BMBF-Projekt *AndProtect*

- Android Kontext und Historie
  - iPhone mit iOS 1.1: 27.06.2007
  - Android 1.0 auf HTC Dream: 23.09.2008
  - davor: Nokia, Blackberry, Symbian

Source: https://en.wikipedia.org/wiki/File:HTC_Dream_Orange_FR.jpeg

- Android Kontext und Historie
  - danach Siegeszug des Smartphones
  - kurzer Auftritt
    - Symbian, Windows Mobile, Palm OS, webOS, ...
  - aktuell noch Konkurrenten, aber wie lange noch?
    - Blackberry, Windows 10, …
  - Stand 2016
    - ein Duopol aus iOS und Android

- # Android Kontext und Historie



Source: https://en.wikipedia.org/wiki/File:World_Wide_Smartphone_Sales.png

- Android Kontext und Historie
  - Geräte Hersteller von **Smartphones**: Samsung, HTC, Huawei, LG, Motorola, Sony, Xiaomi, ASUS
  - aber weit mehr Geräteklassen:
    - Tablet
    - Android Auto
    - Android TV
    - Android Wear
    - TV Set-Top Boxes
    - Industrial Control / HMI
    - …
  - aktuell Version 6.0 (Marshmallow), Oktober 2015
    - Version 7.0 (Nougat) bereits veröffentlicht, August 2016
    - hohe Divergenz bzgl. Versionen und Hersteller

- Android Kontext und Historie
  - Android Sonderentwicklungen
    - SiMKo3 (Deutsche Telekom)

Quelle: Deutsche Telekom

- Android Kontext und Historie

  Fazit

  – extrem komplex gewordenes Umfeld
  – offene Plattform wird ähnlich wie Linux stark adaptiert
  – stark getaktete Weiterentwicklungen

  Frage: Auswirkungen auf Privacy und Security?

- Security & Privacy Probleme
  - Digitalisierung des Alltags
  - mobil oft über das Smartphone realisiert

  einige Stichworte:
  - mobile payment
  - Fitness-Tracking
  - Benutzer-Tracking (Standort, Nutzungsverhalten, Daten überhaupt)
  - Zugriff auf Firmendaten (privates Gerät → Firma)

- Security & Privacy Probleme

  zugrundeliegende Fragestellungen, was schützen?

  – Apps erzeugen, speichern und versenden Daten
    - personenbezogen, privat
  – Kontrolle der Erzeugung und Verarbeitung von Daten
  – Verlust von Daten (Zugriff verhindern)
  – Remote Angriff auf Smartphone
  – Schutz der Plattform (Ausführumgebung für alle Apps)

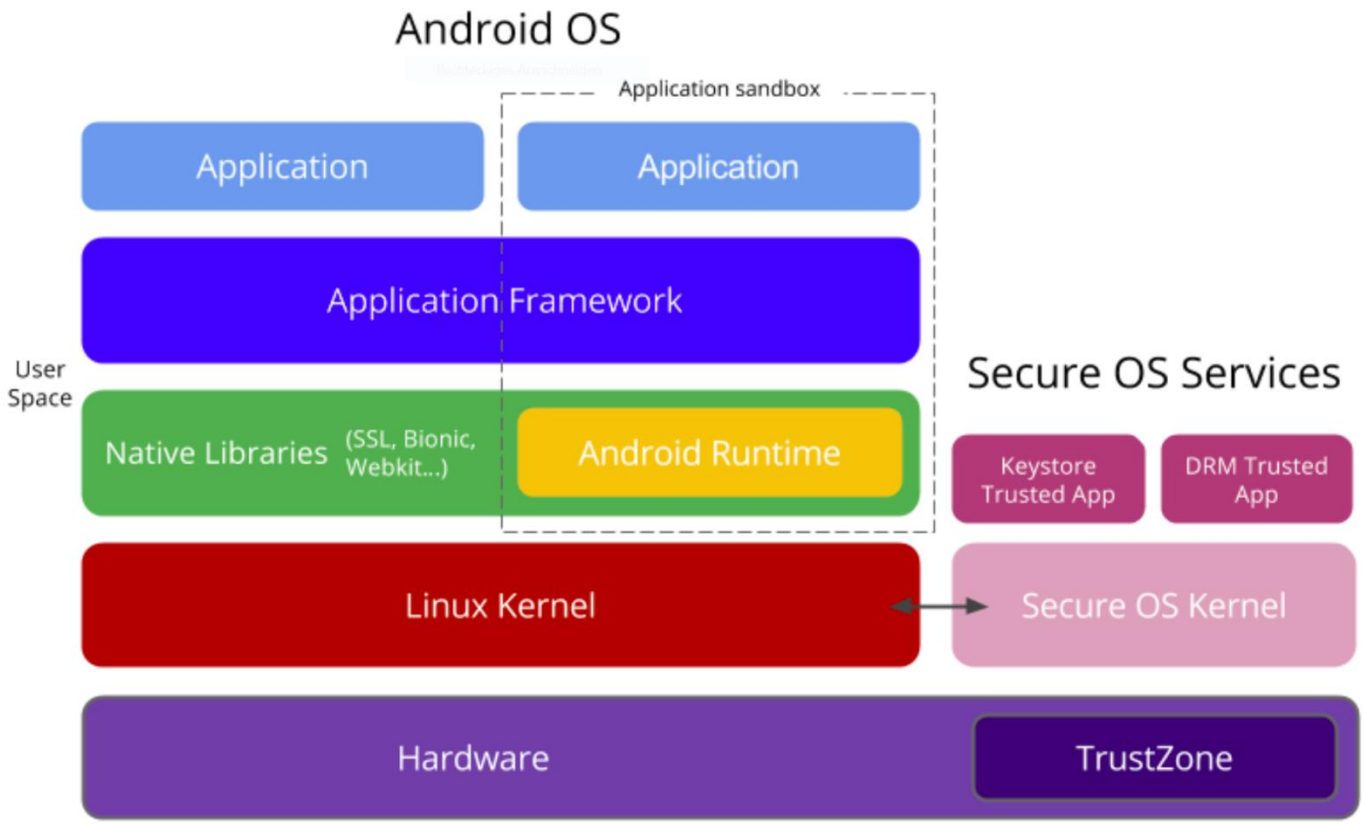
  Frage: Welche Schutzmaßnahmen existieren? Welche Maßnahmen fehlen eventuell noch?

- Basisproblem: die sichere Plattform
  - AOSP = Android Open Source Project
  - Basis Sicherheitskonzepte

  - isolated app concept = UID (app sandboxing)
  - IPC concept → Android permissions
  - no root user → device rooting
  - app signing (self-signed certificate, app update)

- Basisproblem: die sichere Plattform
  - Security Evolution des Android Betriebssystems
    - NX Bit (ARM Erweiterung) (Android 2.3)
    - dm-crypt Full Disk Encryption (Android 4.0)
    - Address Space Layout Randomization (ASLR) (Android 4.0/4.1)
    - Credential storage/Android Key Store (Android 4.3)
    - Hardware credential storage (Android 4.3)
      - Secure Element, TPM or ARM TrustZone
    - SE Linux (Android 4.3/4.4/5.0)
    - New permission Model: Runtime Permissions (Android 6.0)

- Basisproblem: die sichere Plattform
  - Android Referenz-Plattform (Stand 2015)



Source: Android security white paper, Google, May 2015

- Basisproblem: die sichere Plattform
  - Einige Sicherheitsprobleme der letzten Jahre
    - Exynos Abuse (Samsung Galaxy with SoC Exynos 4210 and 4412) → Hardware
    - FakeID: Fehlerhafte Prüfung der App-Signatur (Android 2.1-4.3) → Software
    - Stagefright: Verarbeitung von SMS/MMS verwundbar (Android -5.1) → Software
    - Extracting Qualcomm's KeyMaster Keys - Breaking Android Full Disk Encryption (Google Nexus with QSEE (Qualcomm Secure Execution Environment)) → Hardware/Software

- Anwenderproblem: die sichere App
  - Quelle der App
  - Vertrauenswürdigkeit der App (App Logik)
  - benötigen sichere und vertrauenswürdige Plattform

- Anwenderproblem: die sichere App
  - Quelle der App
    - App Store vs. Side-loading (Plattform)
    - Prüfungen des App Stores (Freigabe einer App)
    - Regelmäßiges Scannen auf Schwachstellen
  - Vertrauenswürdigkeit der App (App Logik)
    - statische und dynamische App Analysen
      - Projekt *AndProtect*
    - Zuverlässige Bibliotheken für App-Entwickler
  - benötigen sichere und vertrauenswürdige Plattform
    - Was kann die App prüfen?
    - Gerät gerootet?
    - Attestation?

- Vorstellung Projekt *AndProtect*
  - „Selbstdatenschutz durch statische und dynamische Analyse zur Validierung von Android-Apps“
  - Projektzeitraum: 11/2015-10/2016
  - BMBF-gefördert
  - Projektpartner
    - secuvera
    - DAI-Labor (TU Berlin)
    - Allgemeine und Arbeitspsychologie (TU Chemnitz)

- Vorstellung Projekt *AndProtect*
  - Zielsetzung
    - Entwicklung eines benutzerfreundlichen Werkzeuges
    - Mit Hilfe des Werkzeuges sollen Laien in der Lage sein Informationsflüsse einer App nachzuvollziehen und zu bewerten
    - Geschäftsmodelle für App Prüfung

- Vorstellung Projekt *AndProtect*
  - Statische Analyse
    - Aufbauend auf „Androlyzer“ der TU Berlin
    - Identifiziert Informationsflüsse innerhalb der App und nach außen
    - Analysegraph optimiert
    - Aussagekraft ist jedoch beschränkt (nachgeladener Code, Verschleierungstechniken)
  - Dynamische Analyse:
    - Ergebnisse der statischen Analyse sollen als Input verwendet werden (z.B. Permissions, Views)
    - Automatisierte Bedienung der App
    - Analyse des Datenflusses während der Bedienung

- Vorstellung Projekt *AndProtect*
  - Nutzerforschung
    - Erhebung von Privatsphärenbedenken im mobilen Kontext (Befragung)
    - Benutzerfreundliche Gestaltung der Nutzerschnittstellen von statischer und dynamischer Analyse (Labortest)
    - Evaluation des integrierten Systems (Feldversuch)

- Vorstellung Projekt *AndProtect*
  - Befragung
    - Zielsetzung: Wie bewerten Benutzer potentielle Bedrohungen für verschiedene Datentypen von Apps?
      - Karten, Messaging, Wetter, Shopping
    - Laufzeit 02/2016 – 05/2016 (10 Wochen)
    - Einladung per: Studenten/Mitarbeiter, persönliche Kontakte der Projektpartner, Testteilnehmer der Professur, Einladung an bekannte Projekte, TUC Facebook Post.
    - Teilnehmer der Befragung, vollständige Fragebögen
      - N = 227; n = 81 weiblich (36%), n = 146 männlich (64%)

- Vorstellung Projekt *AndProtect*
  - Ergebnisse der Befragung

Mobile privacy concerns have nothing to do with: the age, the gender, the knowledge, technical affinity, the experience of the user…

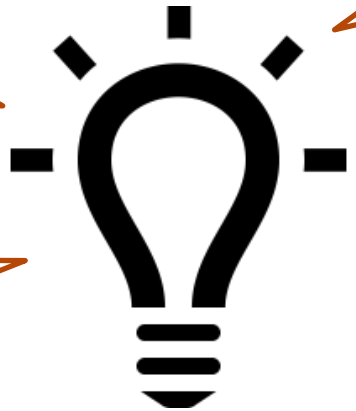
… nor the installation process, or the relevance of respective service of the app.

…and if the use of the data is not necessary for providing the respective service of the app.

The users request for measures and functions they can actively apply to protect their privacy…

…especially if an app uses data continuously in the background…

…or at least increase the transparency about the usage of their data.



Smartphone users are concerned about their mobile privacy…

- Vorstellung Projekt *AndProtect*
  - Nächste Schritte
    - Ende-zu-Ende Umsetzung der dynamischen Prüftechnologie
    - Instrumentierung
    - Test-Automatisierung (gar nicht so einfach)
    - Sammlung von Rohdaten (transparent machen: was tut die App)
    - Bewertung der Daten
      - grün, gelb, rot? (Rückfluss der Ergebnisse der Befragung)
  - Nächster (öffentlicher) Meilenstein
    - Nationale Konferenz IT-Sicherheitsforschung 2017: „Selbstbestimmt und sicher in der digitalen Welt“, 14.-16.02.2017, Berlin
    - Demonstrator

- Fazit
  - Reifegrad der Plattform steigt
    - aber Android- und Hardware-basierte Probleme bleiben
    - Update der Plattform (Android Version) für jeden Hardware-Hersteller ein Problem
    - neue Geräteklassen (ohne Erfahrung) kommen hinzu
    - Sicherheitsergänzungen (SE for Android, Samsung KNOX, SRT AppGuard)
  - App Sicherheit bleibt schwierig
    - Sicherheit auf dem Gerät ist schwer umsetzbar
    - außer Plattform ist unter gemanagter Kontrolle
      - technisch (MDM) und organisatorisch (Policies)
    - Vorgelagerte App-Prüfung (App Store Filter)

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Vielen Dank!