DAI-Labor
TU Berlin

Mobile Endgeräte und Herausforderungen für den Selbstdatenschutz

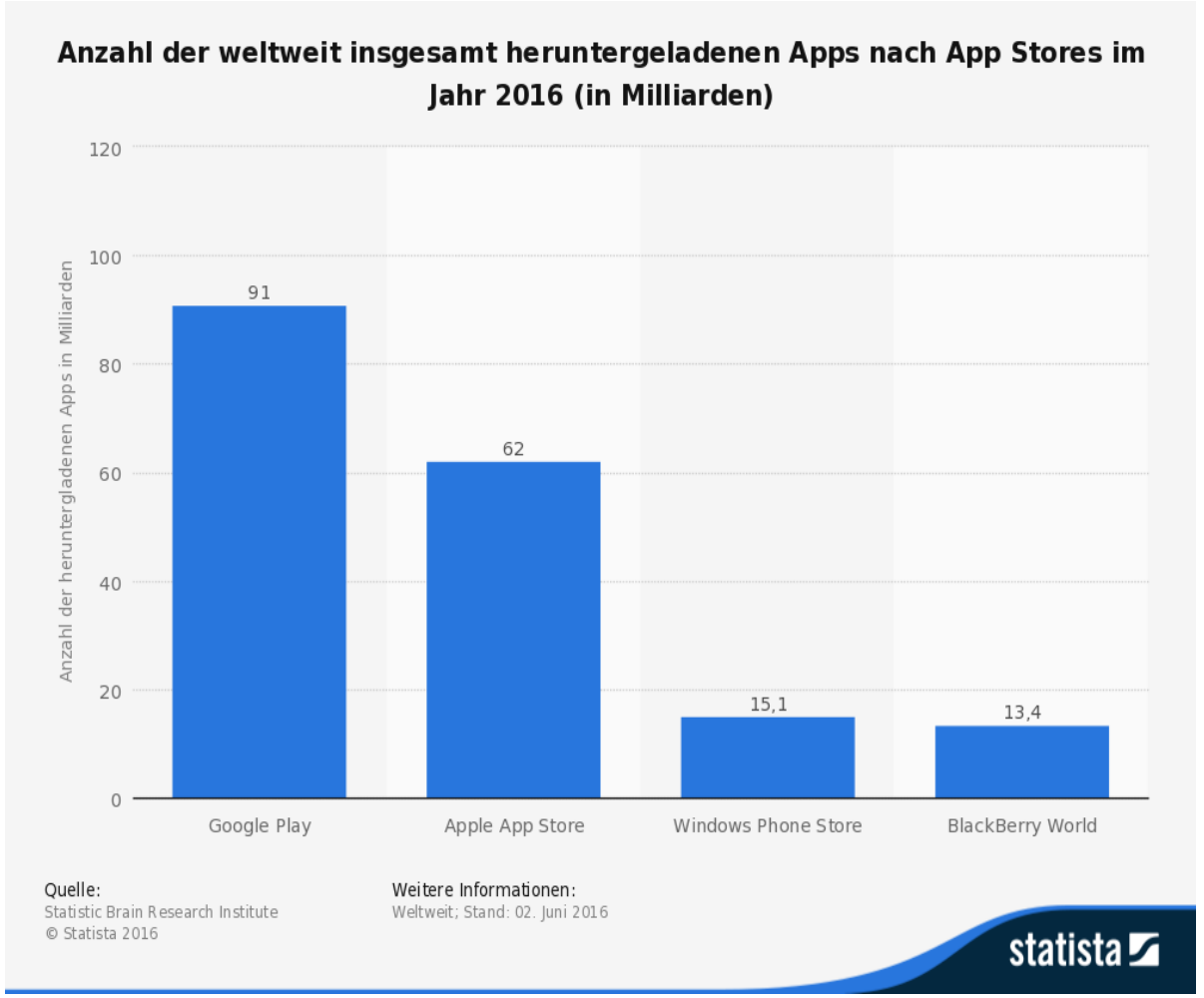
Prof. Dr. Sahin Albayrak

07.11.2016

Mobile Endgeräte und Datenhoheit

- **In 2016 über 180 Milliarden App-Downloads weltweit in allen App-Stores**
- Mobile Endgeräte spielen heutzutage eine zentrale Rolle
  - Smartphones, Tablets, Smartwatch, Smart-TV, Haushaltsgeräte, Autos, etc.
  - Kontinuierliche Internetverbindung
  - Wichtigstes Medium für Kommunikation
  - Produziert und speichert eine Vielzahl an Daten mit privaten und geschäftlichen Inhalten
  - Messinstrumente zum kontinuierlichen Tracking

→ Informationen können zweckentfremdet oder gar gestohlen werden



Quelle: https://de.statista.com/statistik/daten/studie/321649/umfrage/insgesamt-heruntergeladene-apps-pro-app-store-weltweit/

Beispiel 1: Diebstahl von Prototypen mit Hilfe von mobilen Endgeräten

- Einsatz von 3D-Druckern in der Prototypenentwicklung (z.B. im Maschinenbau oder Automobilindustrie) und Serienfertigung von Konstruktionen (z.B. in der Medizin)

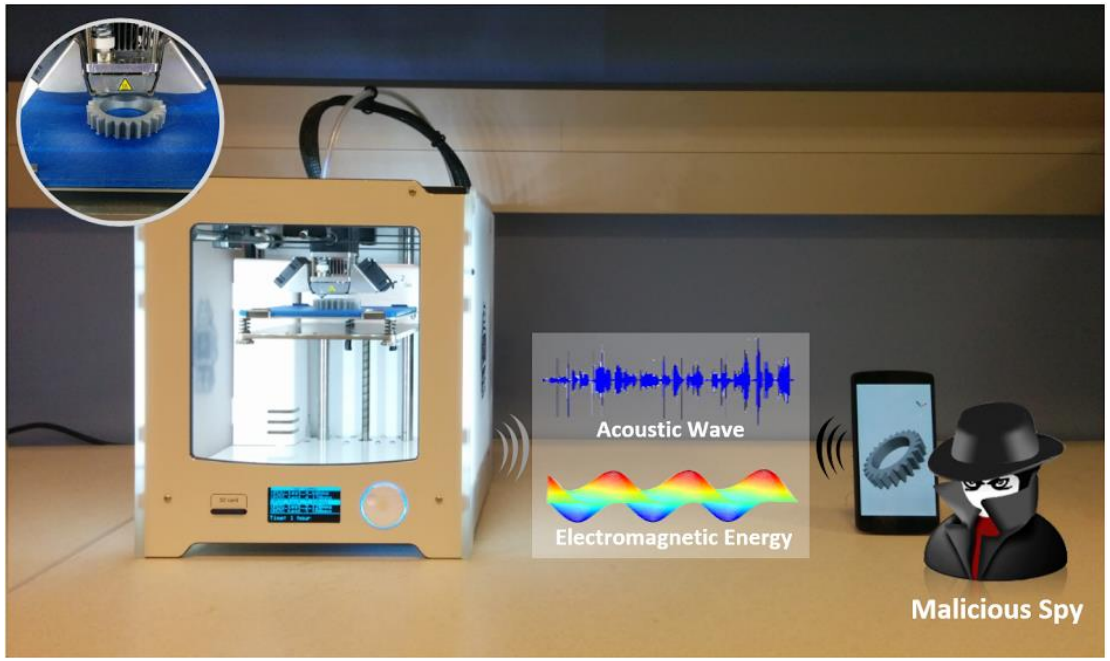
  → Geistiges Eigentum des Herstellers

- 3D-Drucker hat individuellen Sound und elektromagnetische Strahlung für jeweiligen Plan

- Smartphone-App kann Konstruktionsplan durch Mikrofon-Aufnahmen und Sensoren für magnetische Felder aufnehmen

  → Rekonstruktion des Prototpen als Druckplan

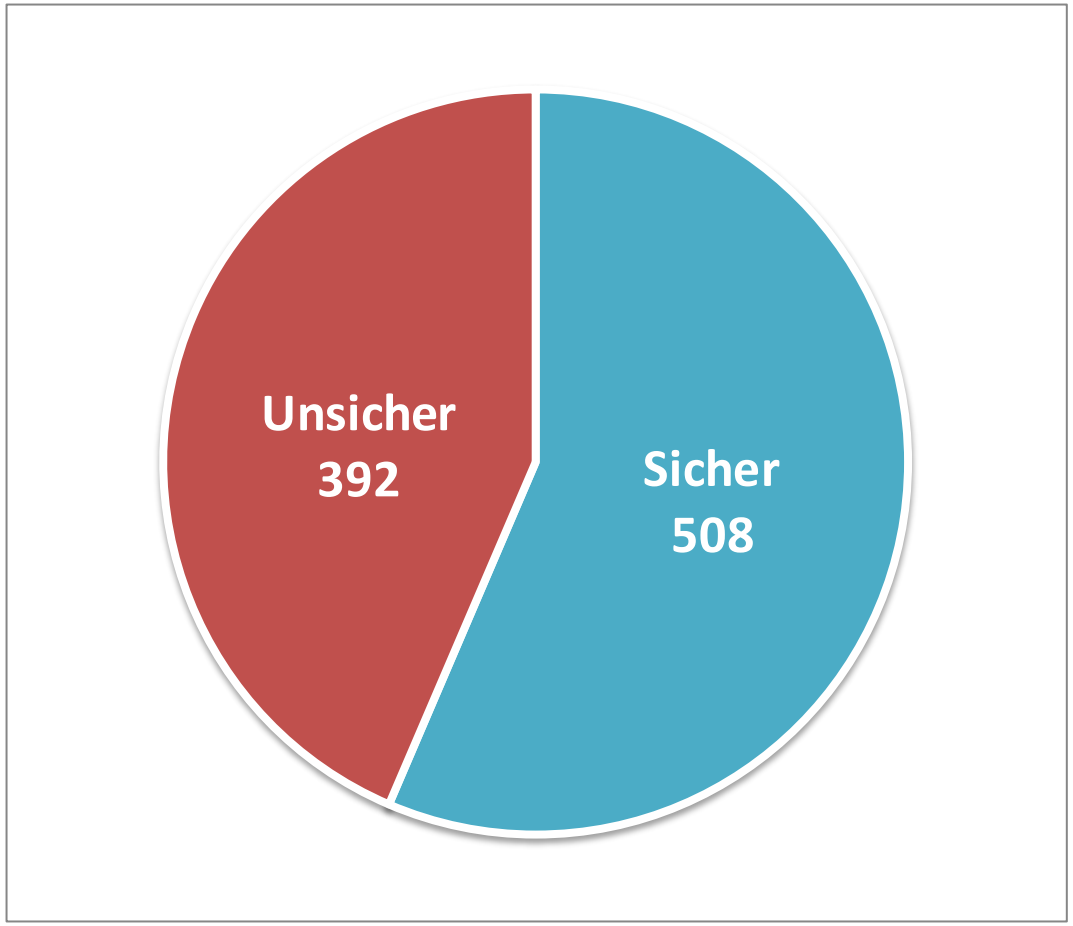
- Verlassen des Unternehmens über das Internet



Quelle: My Smartphone Knows What You Print: Exploring Smartphone-based Side-channel Attacks Against 3D Printer, *Chen Song, Feng Lin, Zhongije Ba, Kui Ren, Chi Zhou, Wenyao Xu (University at Buffalo, State University of New York),* ACM CCS 2016

Beispiel 2 – Unsichere Apps

900 exemplarisch getestete Apps (2012)



- Apps kommunizieren zum Teil ohne Wissen des Nutzers, andere kommunizieren unverschlüsselt
- Viele Apps fordern mehr Berechtigungen an als sie benötigen
- Wichtige vertrauliche Informationen können unbemerkt nach Außen gelangen
- Entwickler machen oft Fehler in der korrekten Programmierung sicherer Kommunikation

Quelle: https://blog.botfrei.de/2012/11/mediatest-digital-veroffentlicht-alarmierende-app-statistik/

BMBF Forschungsprogramm für IT-Sicherheit

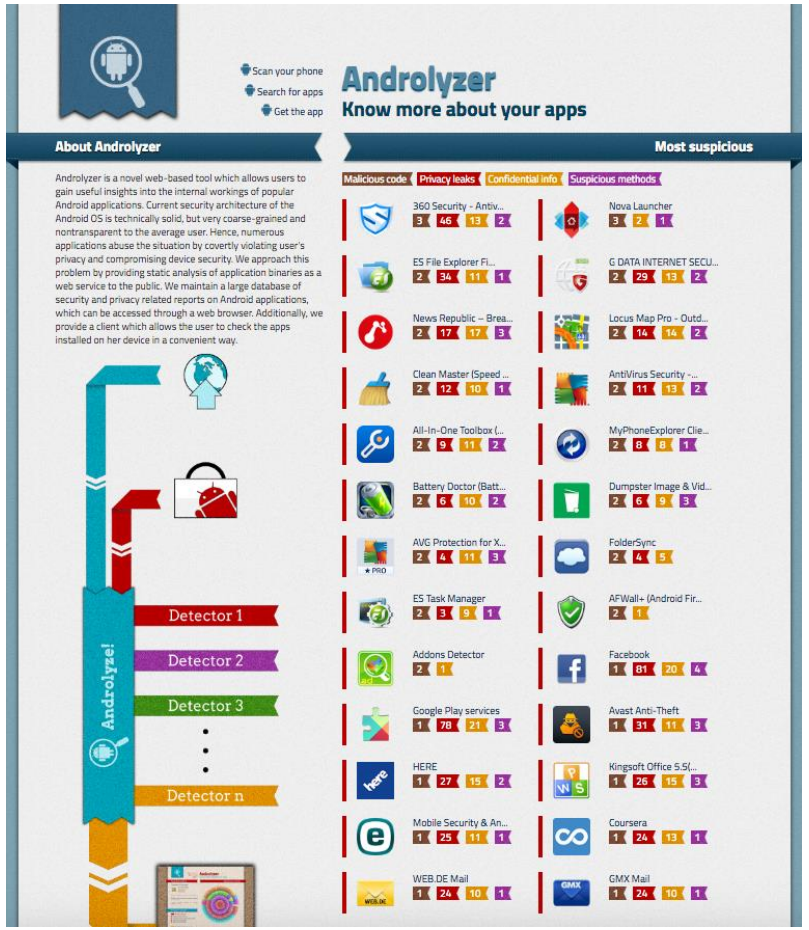
- Bekanntmachung: „Datenschutz: selbstbestimmt in der digitalen Welt“
- Fokus: Selbstdatenschutz, Privatsphäre

- Insgesamt 16 Projekte
  - 4 Projekte mit Beteiligung der TU-Berlin
  - 2 davon mit Beteiligung des DAI-Labors
- Themenschwerpunkte
  - Nachvollziehbarkeit verbessern
  - Risikobewertung ermöglichen
  - Alltagstaugliche Anonymisierung und Pseudonymisierung schaffen
  - Vertraulichkeit unterstützen

- http://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/datenschutz-selbstbestimmt-in-der-digitalen-welt

Androlyzer als Webservice

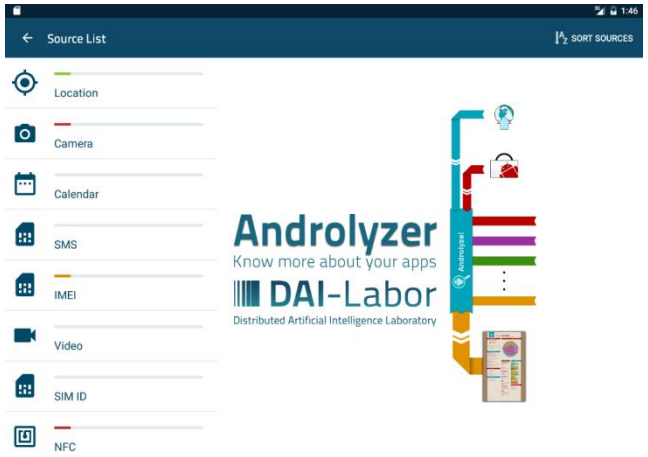
- Client-seitige statische Analyse von Android-Applikationen
  - Untersuchung von Quellcode
- Untersuchung von Privatsphärenlecks
  - Erkennung von Sicherheitsverstößen durch Datenflussanalyse
- Signaturanalyse
- Gewonnene Erkenntnisse werden als App und Webservice bereitgestellt
- Gibt dem Benutzer Einblicke in die Interna von Apps

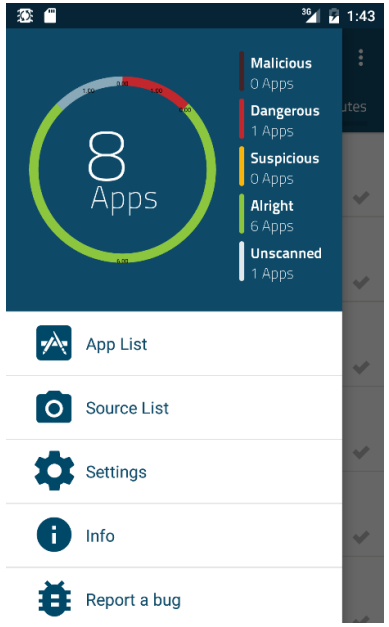


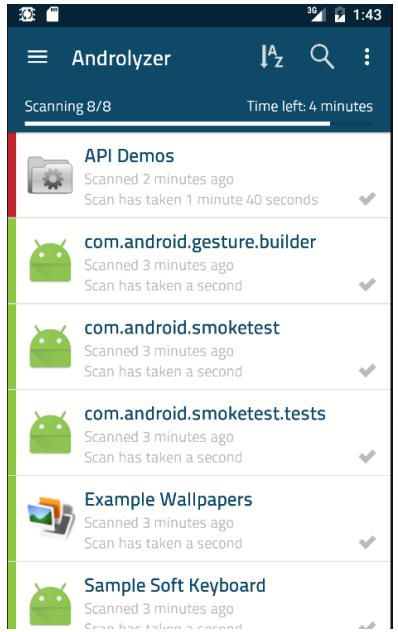
https://www.androlyzer.com

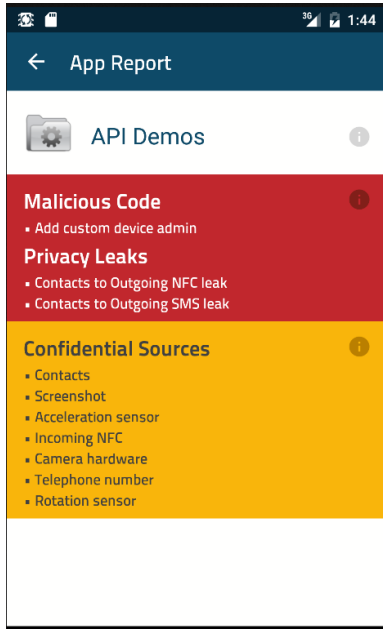
Androlyzer als mobile Applikation

- Analysierte Apps mit Bedrohlichkeitslevel gekennzeichnet
  - Ampelfarben-System
- App ist verfügbar auf Goolge Play Store
  - Android 4.0 und höher









AndProtect – Kontrolle von Datenflüssen

- AndProtect – Selbstdatenschutz durch statische und dynamische Analyse zur Validierung von Android-Apps
  - App-interne Verarbeitungsschritte sind für Nutzer nicht nachvollziehbar
  - Welche App verwendet private Daten und wie werden diese weitergeleitet?
  - Wie können Nachvollziehbarkeit und Risikobewertung verbessert werden?

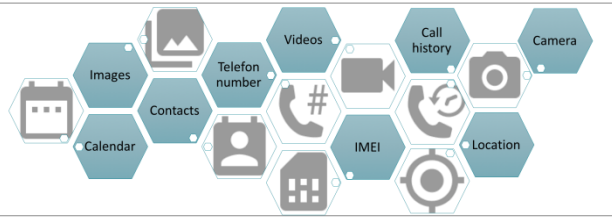
- Ziele:
  - Nachvollziehbarkeit von Datenverarbeitungsvorgängen
    - Wie und auf welche privaten Daten eine App zugreift
    - Auf welche Art und Weise die Daten das Gerät verlassen
  - Risikobewertung
    - Fundierte Aussagen über Datenschutzrisiken
    - Untersucht konkrete Datenflüsse und bewertet deren Auswirkungen

- Durch einer Studie zu Privatsphärenbedenken sowie den orchestrierten Einsatz von statischer und dynamischer Analyseverfahren soll eine qualifizierte Aussage über datenschutzrelevante Informationsflüsse getroffen werden

AndProtect

Privatsphäre

- Identifizierung von Datenarten im mobilen Nutzungskontext
- Studie zur Bewertung der Zweckmäßigkeit von Datenarten



Statische Analyse

- Aufdeckung des App-Verhaltens
- Untersuchung von Datenflüssen auf handelsüblichen Android-Geräten
- Identifizierung von sensiblen Datenquellen und -Senken innerhalb App und Suchen nach einer realisierbaren Verbindung

Androlyzer
Know more about your apps
DAI-Labor
Distributed Artificial Intelligence Laboratory

www.androlyzer.com

Dynamische Analyse

- Liefert Informationen über tatsächliches Ablaufverhalten
- Teile der App werden kontrolliert ausgeführt, um Zugriffe auf private Daten zuverlässig zu erkennen

AndProtect

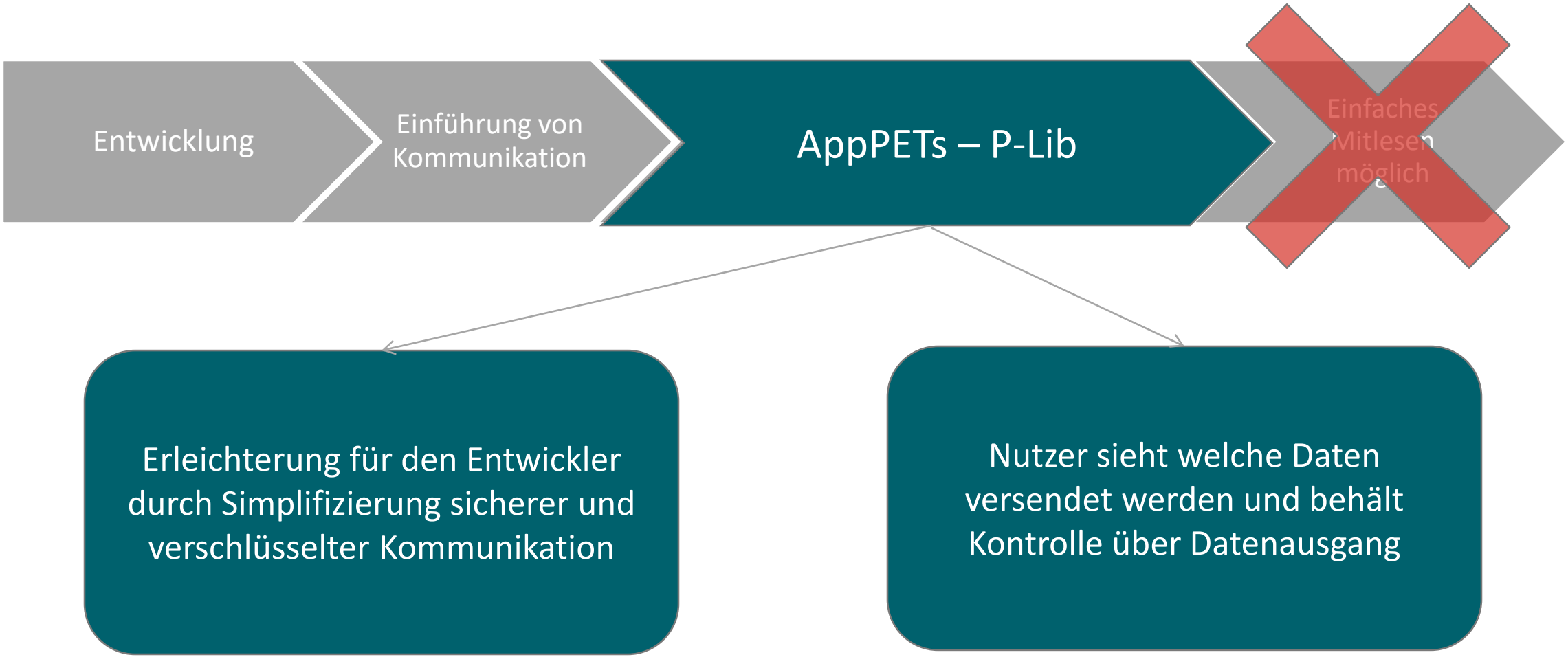
AndProtect: Partner

AppPETs - App Privacy Enhancing Technologies

- Bibliothek für iOS und Android
- Unterstützt Entwicklern bei der Erstellung datenschutzfreundlicher Apps
- Verschlüsselt und anonymisiert Kommunikation für erhöhten Datenschutz
- Verfügt über diverse Sicherheitsverfahren und regelt private Datenflüsse
- Apps die diese Bibliothek verwenden, bekommen nach einer Verifizierung ein Zertifikat, woran der Nutzer erkennen kann, ob er Kontrolle über seine Daten behalten kann.

- **Ziele**:
  - **Nachvollziehbarkeit verbessern**
    - Nutzer sieht wann welche Daten versendet werden
  - **Risikobewertung ermöglichen**
    - Nutzer kann den Versand der Daten zustimmen oder verweigern
  - **Alltagstaugliche Anonymisierung und Pseudonymisierung schaffen**
    - Daten werden verschlüsselt versendet und persistiert
  - **Vertraulichkeit unterstützen**
    - Alle Apps die AppPETs verwenden werden untersucht und erhalten ein Zertifikat an dem sich der Nutzer orientieren kann

AppPETs


Entwicklung
Einführung von Kommunikation
AppPETs – P-Lib
Einfaches Mitlesen möglich
Erleichterung für den Entwickler durch Simplifizierung sicherer und verschlüsselter Kommunikation
Nutzer sieht welche Daten versendet werden und behält Kontrolle über Datenausgang

AppPETs: Partner

DAI-Labor
Distributed Artificial Intelligence Laboratory

berlin

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Westfälische Wilhelms-Universität Münster

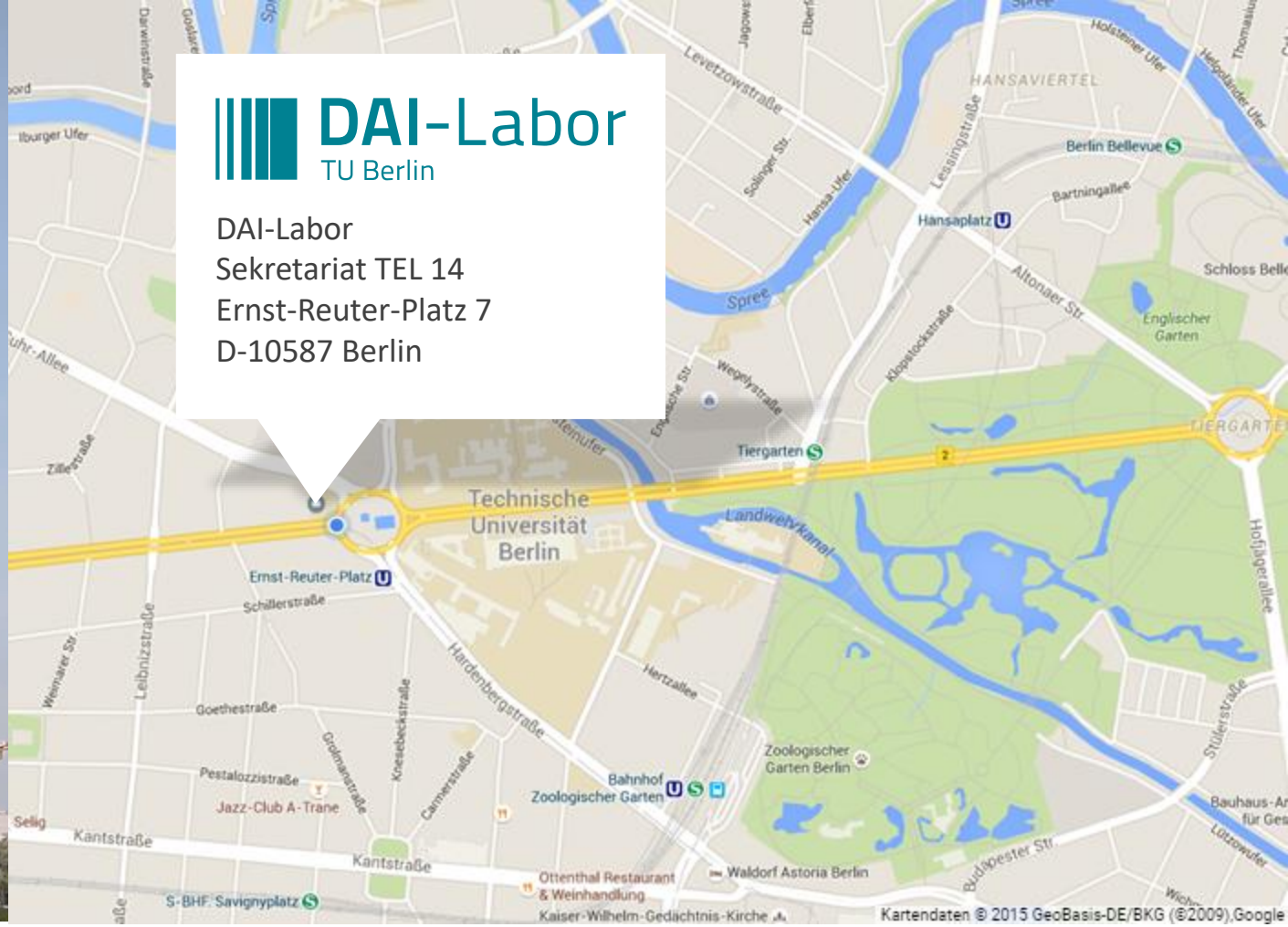
ULD

mediaTest digital

praemandatum
Sicherheit durch Wissen

JonDos

- Assoziierte Partner: Deutsche Post AG, NESO Security Labs GmbH, Zeta Project GmbH, Digitalcourage e.V., Flff e.V., Verbraucherzentrale Hamburg
- Entwicklerbeirat: Appdream AG, xinfo Wieland Sacher GmbH, Team-Drive Systems GmbH, socialbit GmbH, creative workline GmbH



Get In Touch

sahin.albayrak@dai-labor.de

Prof. Dr. Dr. h.c. Sahin Albayrak

+49 30 - 314 74000