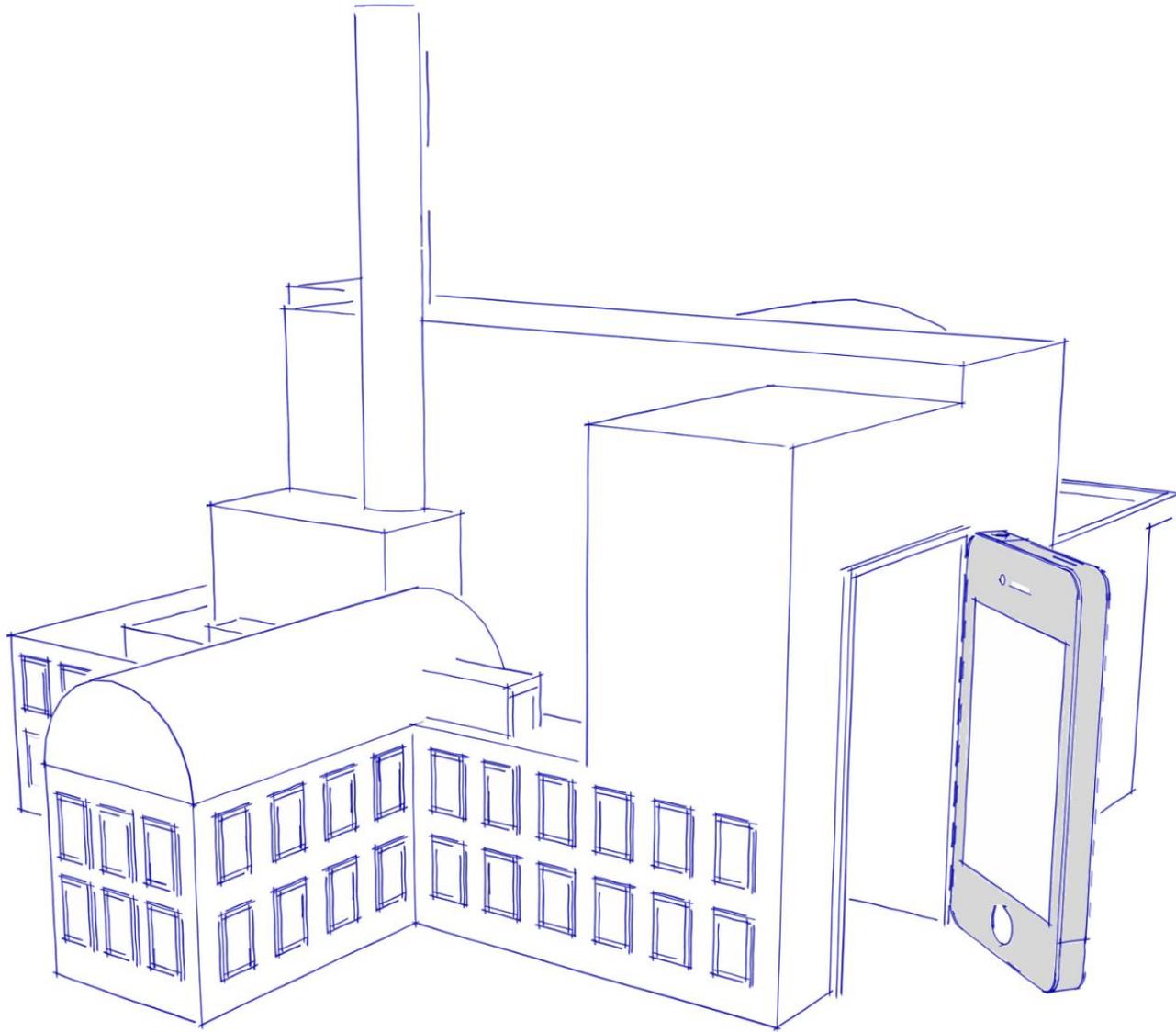




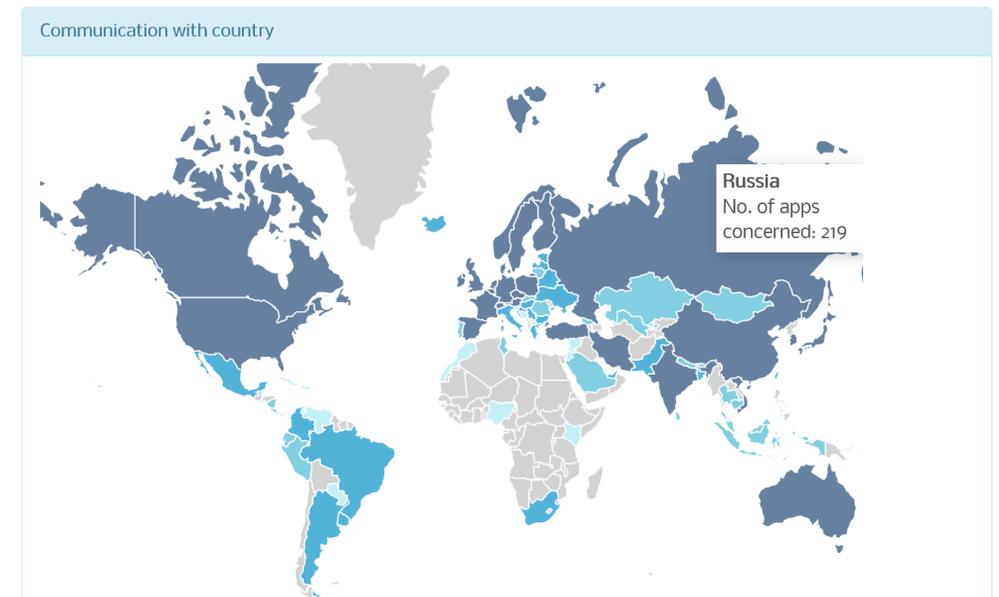
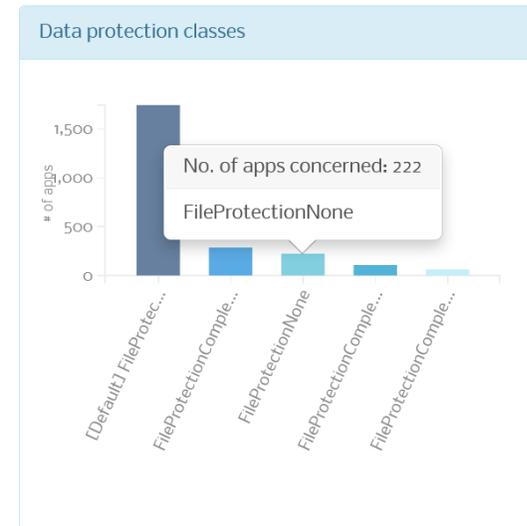
App-Sicherheit - Automatisierte Analyse für den Unternehmensschutz



Apps als **Einfallstor für Angriffe** auf Ihr Unternehmen

Apps im Unternehmenseinsatz

- Apps verarbeiten Unternehmensdaten
 - Daten durch Sandbox gegen andere Apps geschützt
 - Prüfung der Apps im App Store
 - Berechtigungen schützen Datenzugriffe
 - Weiterer Schutz abhängig von App-Programmierung
 - Speicherort
 - Verschlüsselung / Kryptographie
 - Datenschnittstellen
 - Nutzerschnittstellen
 - Kommunikation



Auszug Appicator Top 2000 Android Analyse, Oktober 2023

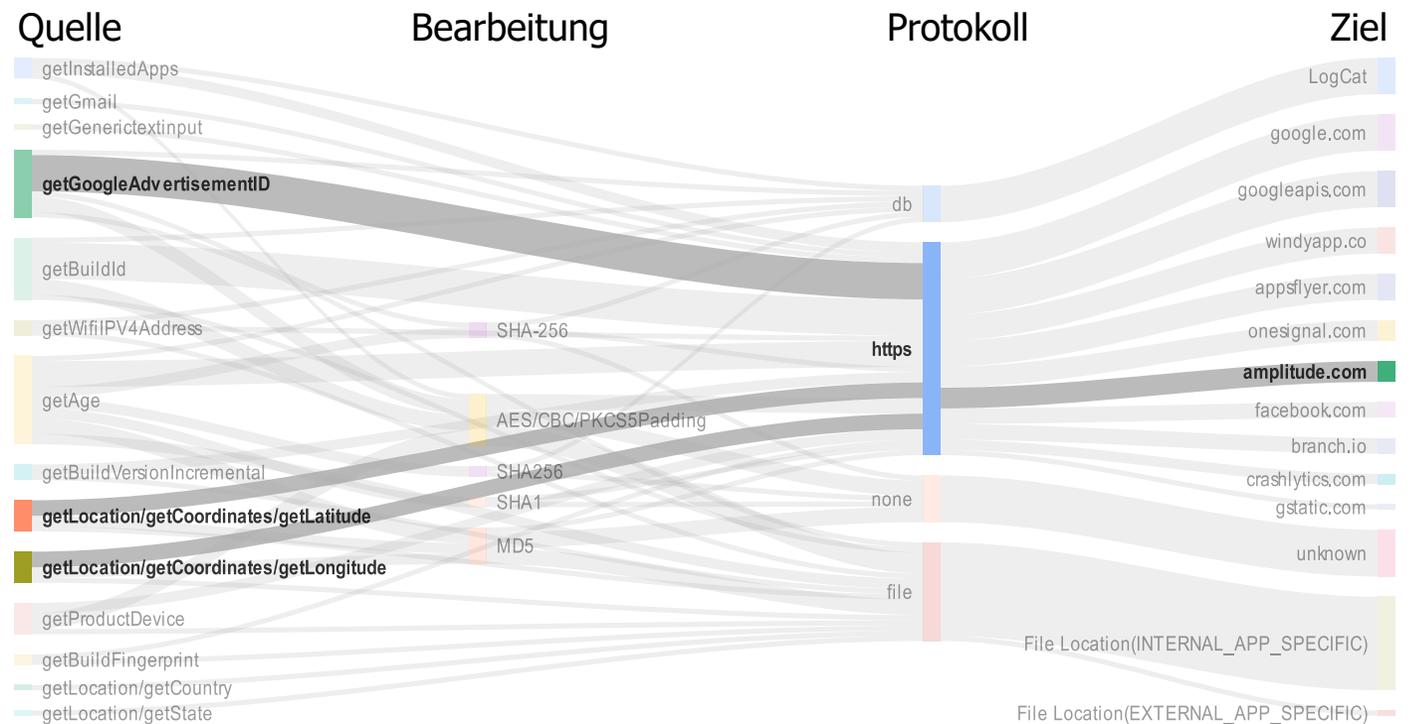
Datenflüsse zu Fremdanbietern

Beispiel: GPS-Daten

■ Berechtigungsnutzung

- Position für Wetter App OK
- App Bibliotheken nutzen Berechtigung
- Echtzeit Standort Tracking möglich

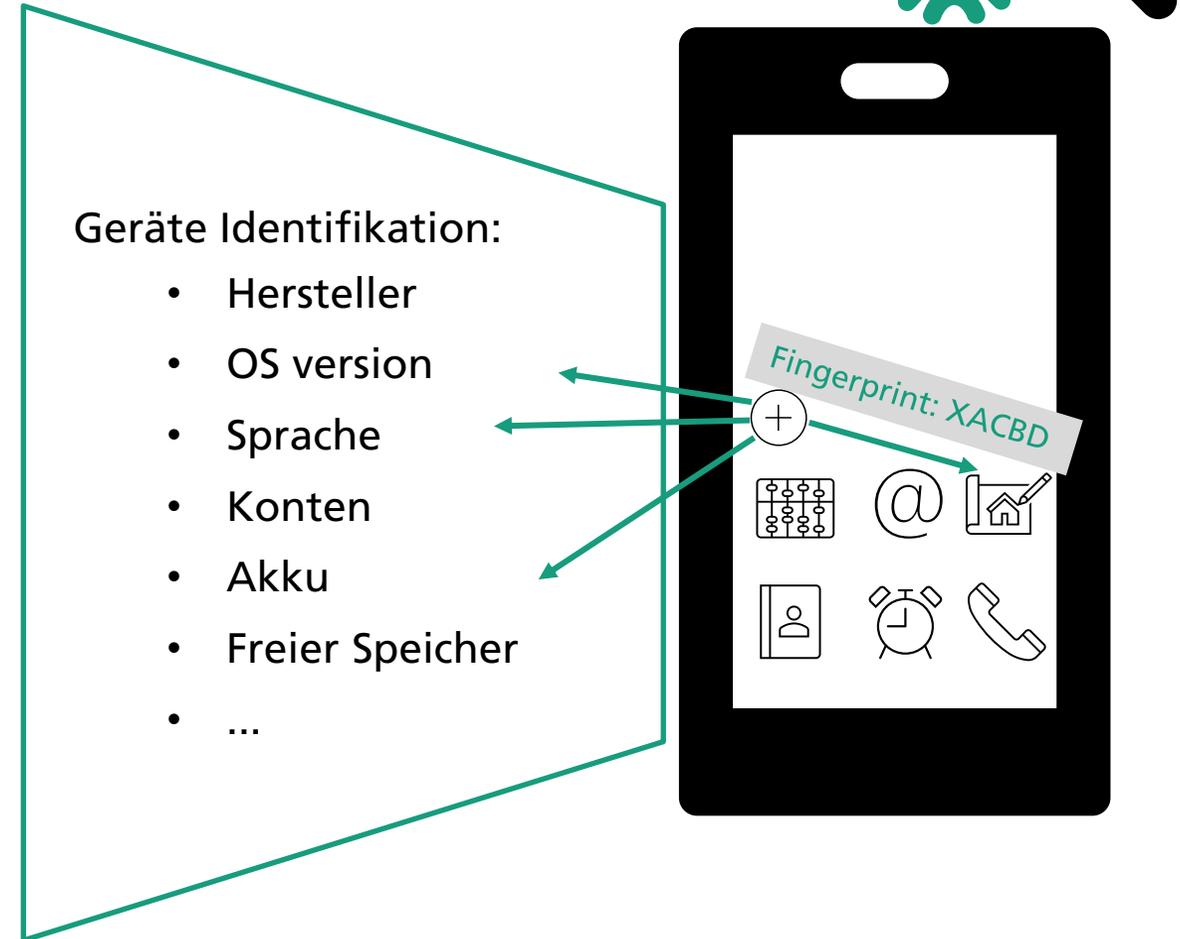
Wetter App



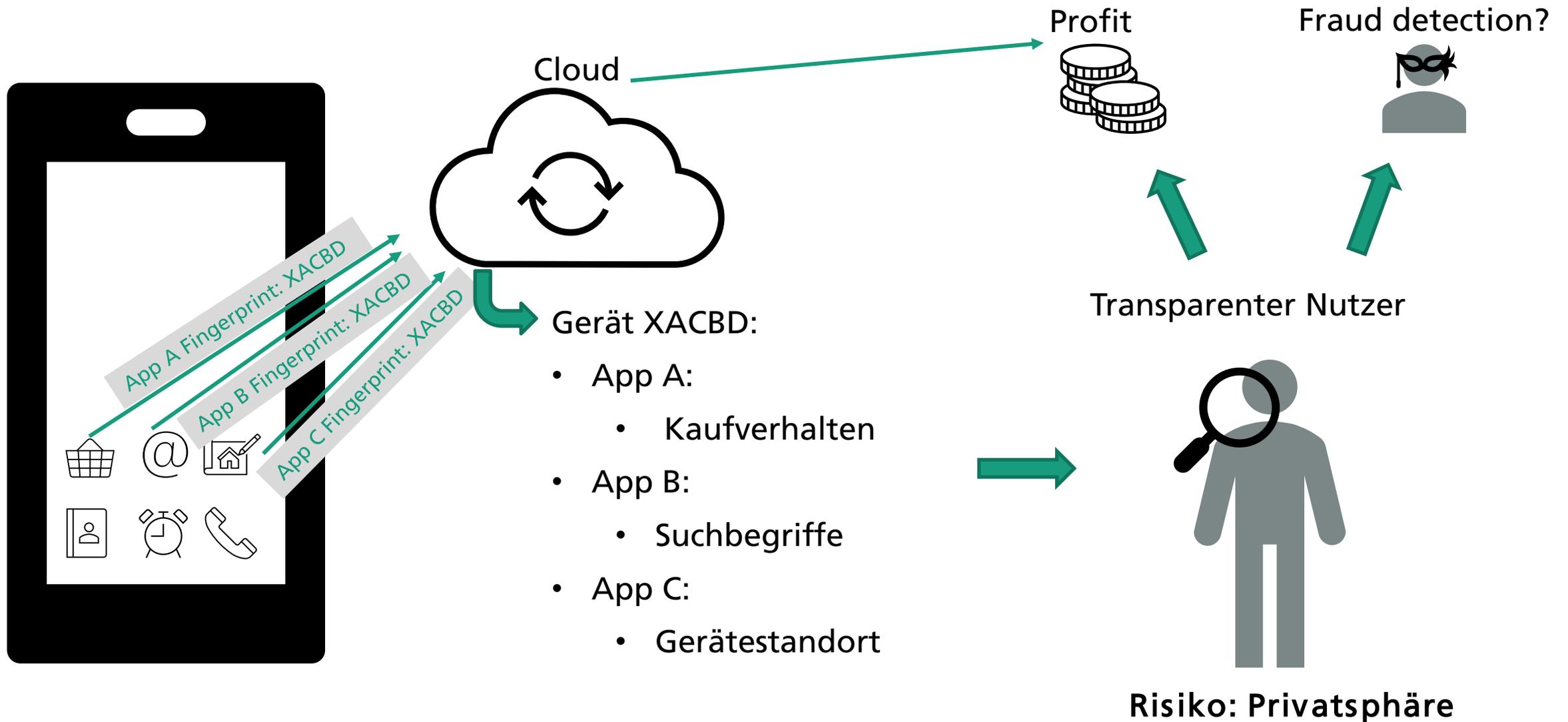
Auszug dynamische Datenflussanalyse: PANDERAM BMBF Projekt

Geräte Fingerprinting durch Apps

- Eindeutige Identifikation über Geräteeigenschaften
- Bekannt für Webseiten
 - Nutzer Identifizierung und Tracking

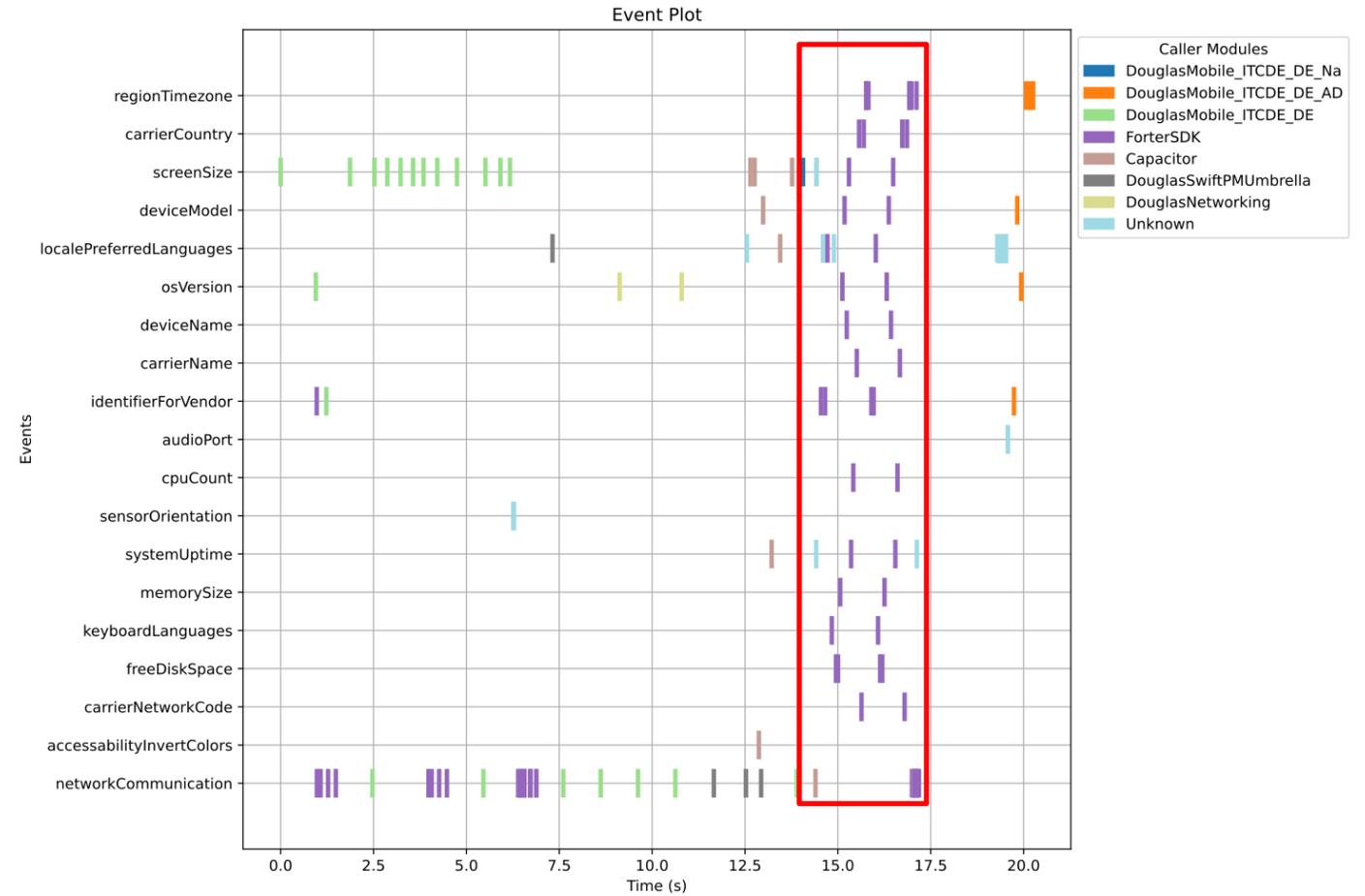


Geräte Fingerprinting durch Apps: Risiken



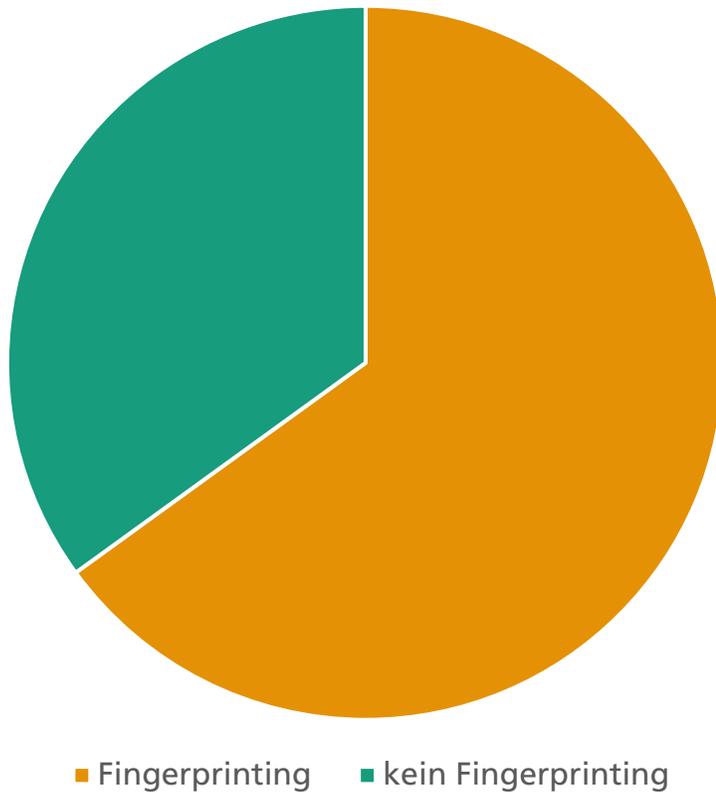
Geräte Fingerprinting erkennen

- Viele gesammelte Eigenschaften
- Kurzer Zeitraum
- Netzwerkkommunikation

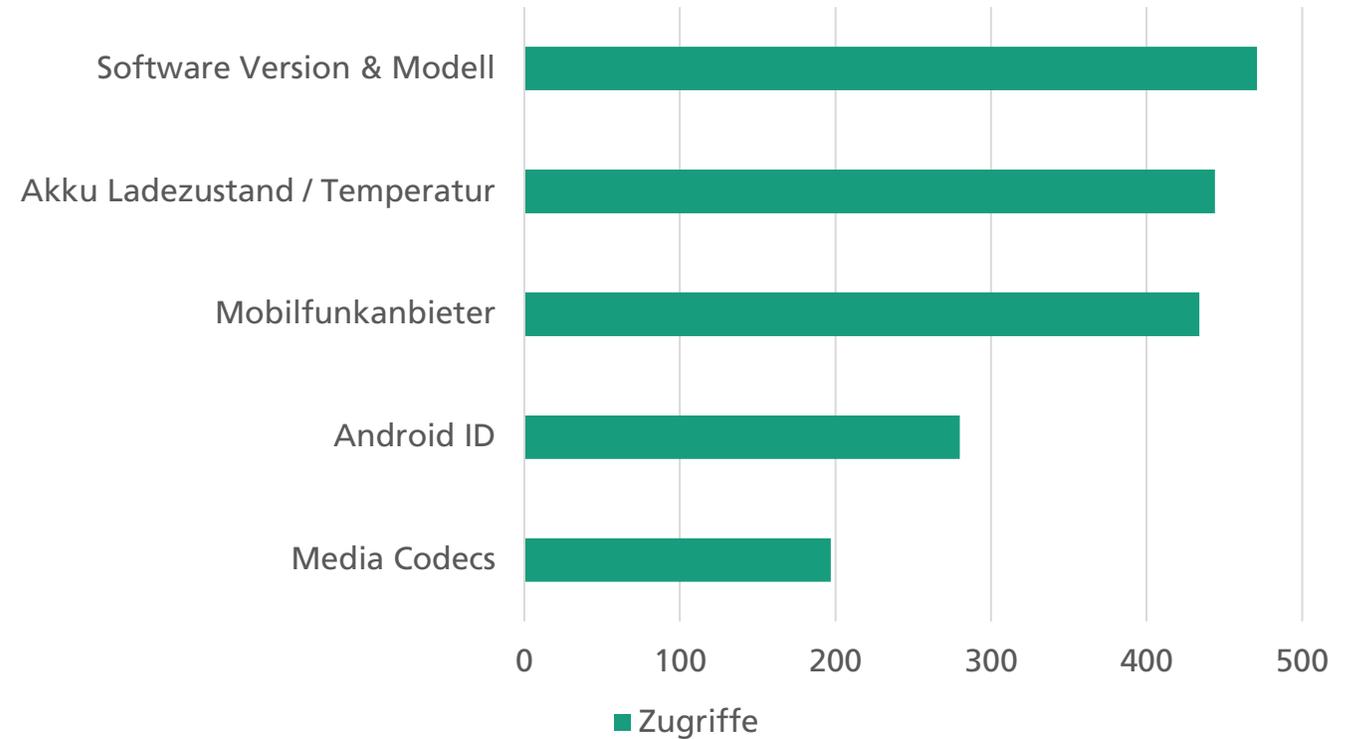


Geräte Fingerprinting Statistiken

Top 1000 Apps Google Play



Zugriffe



Freigabe- und Prüfkonzept für Apps notwendig

Name	Insecure PDF-Viewer
App Type	File Viewer
Platform	iOS
Internal Name	com.company.insecure.pdf
Version	12.1.3
Vendor	Example Inc.
Appstore URL	https://itunes.apple.com/de/app/insecurepdf/id1231231237?mt=8&uo=4
SHA 256	F1A1 45FF 9180 8A86 1B04 D224 3277 7F54 1BFB 29CA 4868 D116E4A6 8619 173F 2297


Blacklisted

4 Risks

✘ Violations of default policy

- Detected risks are not compliant to security policy requirements for apps managing files.
- Enterprise documents maybe at risk in a lost device scenario.
- Enterprise documents maybe at risk during communication processes with external entities.

⚠ App risks for enterprise usage

- Possible flaw: Use of insecure methods to secure communication with SSL/TLS. Common source for flawed communication protection that are vulnerable to man-in-the-middle attacks.
- Possible flaw: Unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Data Protection: App disables iOS default data protection at least in one case and can handle office files, which poses a potential risk as the storage of corporate data is protected lesser than needed for sufficiently targeting the lost device scenario.
- Advertisement/Tracking: App uses more than 5 advertisement and tracking providers.

- App-Sicherheit: Wichtig für alle Unternehmen
- Sicherheitsqualität Beurteilung:
 - Audit
 - Code-Analyse
- Durch Automatisierung viele App Analysen
- Zyklische Wiederholung der Tests ermöglichen
- Sicherheitskonzept: Reaktiv oder Proaktiv
 - Analyse Inventar + Blacklisting
 - Analyse Interner App-Store + Freigabekonzept

Automatisierte App-Sicherheitsanalyse mit Appicaptor

- Ihr Weg zu Appicaptor
 - Appicaptor auf der it-sa 2023: Fraunhofer-Gesellschaft (Stand 311 in Halle 6)
 - Individuelle Live Demo für Sie und Ihre Kollegen (auf der Messe oder im Nachgang)
 - Testen Sie den Appicaptor-Dienst einen Monat kostenlos

- Kontaktieren Sie uns
 - E-Mail: appicaptor@sit.fraunhofer.de
 - Webseite: www.appicaptor.de