Analysing “zero-touch” privacy violations on iOS

Proposal for a “Projektarbeit” · Benjamin Altpeter (b.altpeter@tu-bs.de)

Motivation

Previous research has shown that automated data collection in the background is common in Android apps. A large portion of apps transmits telemetry data about device details (model, settings, battery status, etc.), sensor data, events (which pages are opened and buttons are clicked), or even the geolocation and which data is entered in the app. Often, this data is sent to third-party companies and linked to the device’s *Android Advertising ID* that allows those companies to track users across multiple apps.

These practices are troubling from a data protection standpoint, especially since the *General Data Protection Regulation* (GDPR) that mandates strict legal guidelines for such data collection went into force in 2018. According to the GDPR, any processing of personal data (meaning any data that can somehow be linked to a natural person, including pseudonymously) needs to have one of six possible legal bases (Art. 6(1) GDPR). According to the supervisory authorities, which are responsible for enforcing the GDPR in the EU, usually informed consent is the only applicable legal basis for tracking [1].

Additionally, tracking companies are often based in the US. This is also problematic since the European Court of Justice’s *Schrems II* ruling from July 2020, which invalidated the *Privacy Shield* adequacy decision that such transfer were usually based on [2].

On iOS, on the other hand, research into privacy violations by apps, is scarce and outdated. A 2011 study explored using static analysis on app binaries to detect privacy leaks [3] and a 2015 study crawled app store pages of health apps [4]. Further, a 2014 report presented a dynamic analysis of apps on physical hardware [5].

Meanwhile, in late 2020, Apple started requiring self-labeling of the affected categories of data that apps handle through so-called *privacy labels* [6], sparking controversy and comparisons between similar apps by different companies [7], [8], [9].

Goal

The project will give an up-to-date insight into how common tracking is in iOS apps. In particular, tracking without any user interaction, and thus without consent, will be analysed.

To this end, a large number of popular iOS will be collected and automatically analysed to record the network traffic happening in the background.

The results of this analysis will then be compared to the existing results for Android.

Research tasks

- Investigate whether emulation is viable on iOS or whether a physical device will be necessary.
- Develop a method for automatically installing and starting apps on the chosen platform.
- Record (encrypted) network traffic by apps using a custom root CA and circumvent certificate pinning.
- Identify categories of transmitted data and recipients in the collected data.
- Give an assessment of the legality of the observed data transfers.
- Compare the results with Android.