6 June 2017 Study · Mobile Security · Web & Cloud

Traffic Analysis of Mobile Applications

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/traffic-analysis-of-mobile-applications/

As a supporting measure for the inspection of mobile applications, the data sent and received to/from the Internet has always been of interest. If data was transferred in plain text, intuitive conclusions could be drawn about their use in the context of a mobile application. Due to the fact that more and more network traffic is encrypted (HTTPS / TLS), the meaningfulness of captured data packets becomes limited and, consequently, allows only little conclusions to be drawn about the actually transmitted content.

In the course of this project, solutions were sought in order to derive an understanding of the behaviour of mobile applications from their data transmissions using current scientific methods. Based on existing approaches to analyse network traffic, it was determined whether it would be possible to identify mobile applications in a targeted way, even if encryption prevented access to the actually transmitted content. By focusing on the metadata of transmissions, an approach was sought to distinguish applications from each other individually.

A practical implementation of the proposed analysis concept has been applied to a recorded data set. This test scenario has shown that mobile applications can be classified with a reliability of 83.3% based on their network traffic – regardless of whether communication occurred in an encrypted or unencrypted manner.