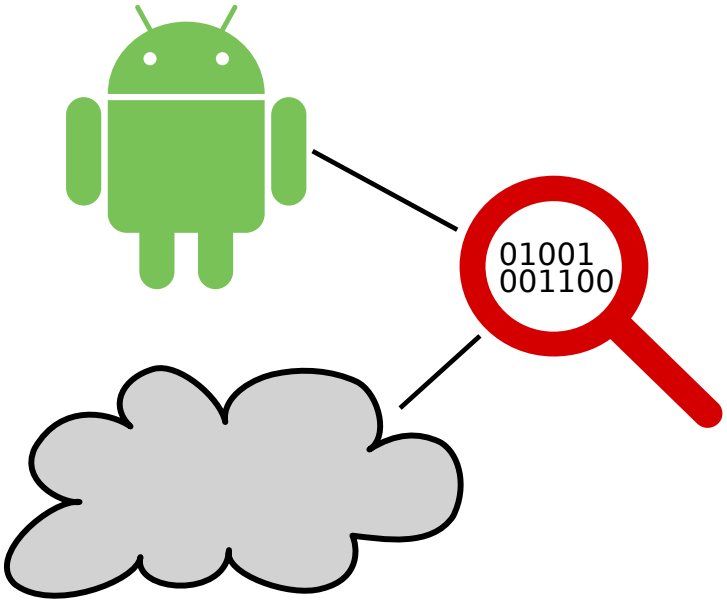
Bachelor Thesis

Analyzing Android Background Traffic

Smartphones are an indispensable companion in everyday live for almost all of us. They are used for privacy sensitive tasks like e-mail, instant messaging and navigation. The most widespread operating system (OS) for smartphones is Android. Depending on the permissions, the Android OS and installed applications have access to privacy sensitive data. While it is assumed that all outgoing traffic is encrypted, it is not guaranteed that this data is not misused or shared with a third party.



Tasks

In this thesis, the student should firstly review related work and assess which parts of Android have already been analyzed for possible privacy sensitive data leakage.

In a second step the outgoing network traffic of the OS should be analyzed with the help of a TLS proxy [1]. It should be assessed which type of data is sent to which server and it should be determined if this is in the best interest of the user from a privacy perspective. The following questions should be answered during this thesis:

- What sensitive information does the Android OS sent to which hosts?
- What sensitive information do the most common apps share with which hosts?
- Is TLS used for all outgoing communication?
- Is sensitive data encrypted additionally?

Required skills (or willing to learn)

- Networking basics
- Basic knowledge about TLS encryption
- Basic knowledge about the Android OS

Keywords

Network Security, Android, Data Privacy

[1] F. Erlacher, S. Woertz, and F. Dressler, "A TLS Interception Proxy with Real-Time Libpcap Export," in *41st IEEE Conference on Local Computer Networks (LCN 2016), Demo Session*, Dubai, UAE: IEEE, Nov. 2016.

Contact:
Felix Erlacher <erlacher@ccs-labs.org>
Website:
http://www.ccs-labs.org