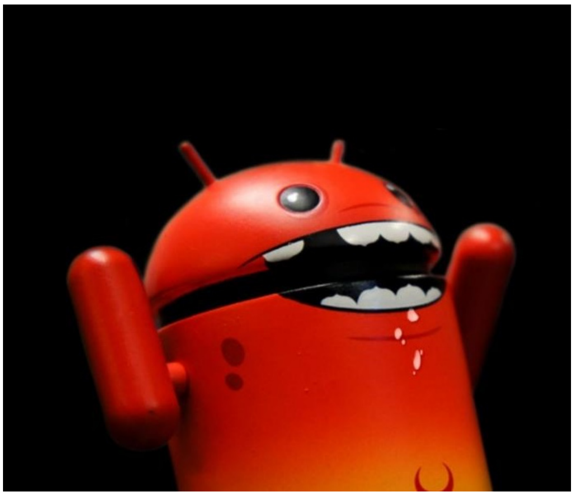
Prof. R. Wattenhofer

Malicious Data Leaks

In Android, apps ask for permissions to access private data, location, the Internet, etc. As a user you can only decide to generally allow or deny access to these resources. It is not clear what the app does with this data. A messaging app that has access to the contacts and the Internet could use the contacts to identify the conversation partner or it could send the entire list of contacts to its own server. By collaborating, apps could also try to circumvent the restrictions of the permission system, e.g., one app has only access to private data, the other access to the Internet.

We previously develped a system that is able to track private data within the app. The goal of this project is to find covert channels that can be used to leak sensitive data by a malicious app. Additionally, for each of these vulnerabilities, we want to come up with a detection mechanism. Such channels could be for example files, databases, audio, app collusion, and so on.



If that sounds like something you're interested in pursuing, don't hesitate to contact us so we can have a chat.

Requirements: Programming experience is an advantage. During your thesis, you will meet on a weekly basis with your advisors, to discuss progress and open questions.

Interested? Please contact us for more details!

Contacts

- Gino Brunner: brunnegi@ethz.ch, ETZ G63
- Simon Tanner: simtanner@ethz.ch, ETZ G97