



Prof. R. Wattenhofer

Android Private Data Leak Detection

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.

The goal of this project is to automate the execution of apps in order to automatically detect data leaks. Finally, some popular apps can be evaluated to see what data those apps access and what the apps then do with the data. In a previous project, a system to dynamically analyze the usage of private data has been created. This system can be used and possibly improved. We already have some ideas on how to approach this, and it will involve working with the Android Open Source Project (AOSP).

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

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

