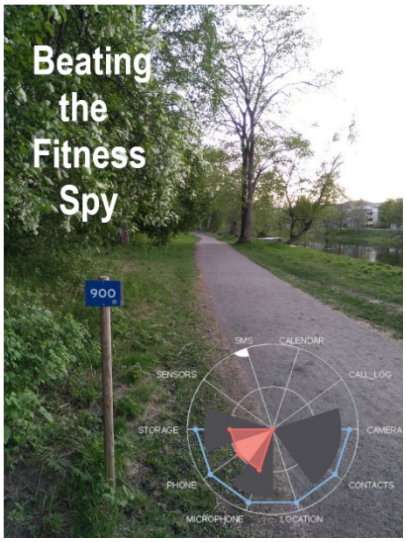
App: Privacy impact self-assessment

Supervisor: Assoc. Prof. Lothar Fritsch, with Nurul Momen.



The goal of this project is to design and implement a graphical user interface on Android devices for self-assessment of app privacy impact based on actual app use on Android phone.

The project team will develop an app that examines the list of installed apps on the phone. It then uses statistical information from the KAUDROID database [1,2,3,4] about the apps. This information is used to engage the app user into a graphical, interactive dialog about (a) the app's access to information, (b) potential impact on phone owner of this information being misused, and (c) the phone owner's preferred mode of restricted data sharing through partial consent [5].

Project elements:

The app shall present illustrative privacy risks caused by certain data sharing, bound to persona/context. This presentation shall be enriched with static statistics from measurements.

> The project group will develop a privacy threat matrix based on personas and contexts in a workshop with the supervisor. The risk sources: location tracing, contacts, phone and SMS logs, microphone, camera, device ID, person ID, network tracking

Examples for personas and contexts are:

- Personas: "Just a regular teenager", "Teenager with celebrity parents", "Rich person", "Politically exposed person", "Minority person", "Profiled job" (controls budget,...).
- contexts: time aspect (here and now, near future, medium future, long future)
- contexts: social circles (personal, family, acquiaintance, professional, public e.g. blogger)
- contexts: financial damage, reputation, stalking-kidnapping-mobbing-blackmail

The main focus of the project is the design and implementation of dynamic GUI elements for self-assessment, e.g. a group of parametrized sliders that graphically adjusts self-assessment dimensions.

After assessment: The app presents (hypothetical) options for partial consent, collects survey answers about which one would be most matching own situation within the chosen context/persona.

Possible models for parital consent:

- Time boundary, delete-after-transaction, try-before-buy (sandboxed for later decision...), ask me for permission for further processing, let me pay with money instead of personal data, ...

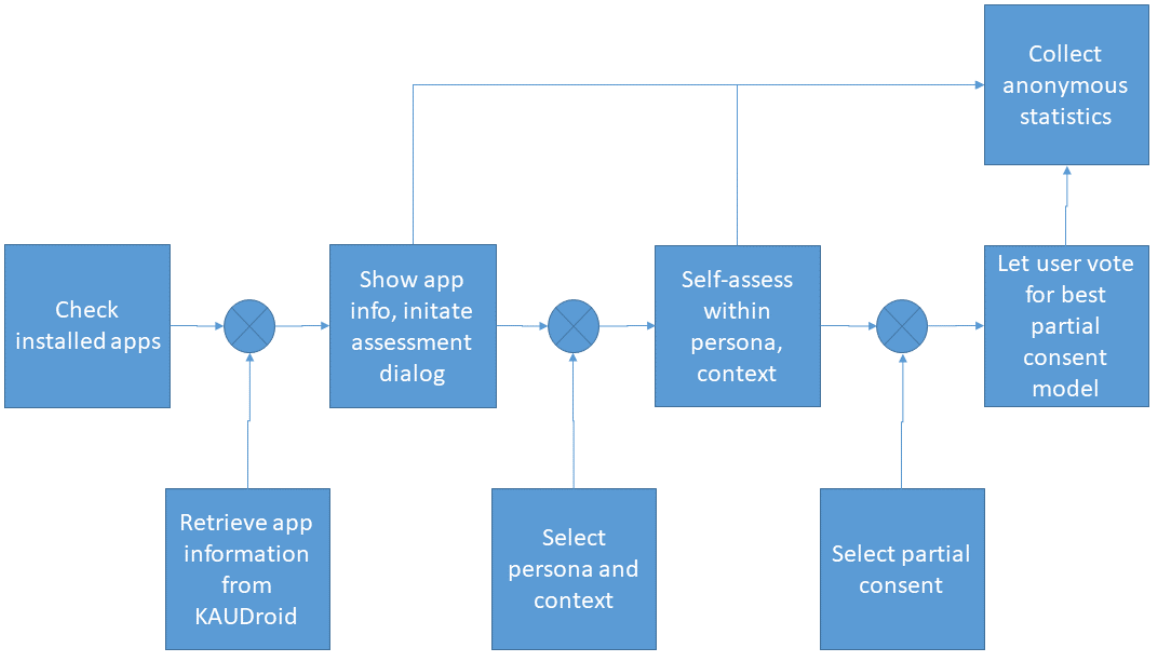
The app shall record self-assessments and choice of consent model for statistical analysis.

The project group will carry out the following activities:

- Read the background literature;
- Produce - together with advisor – a model of privacy threats, personas and contexts;

- Generate statistical profiles over app behavior from the KAUDroid database for popular apps;
- Design and implement experimental user interfaces for “sliding choices”;
- Implement the above into an interactive self-assessment app;
- Produce a complete project report.

A functional specification is shown in the following figure:



Background literature:

[1] Momen, N., 2018. Turning the Table Around: Monitoring App Behavior. In Sicherheit 2018, 25-27 April, Konstanz, Germany (pp. 279-284).

[2] Hatamian, M., Momen, N., Fritsch, L. and Rannenberg, K., 2019, June. A Multilateral Privacy Impact Analysis Method for Android Apps. In *Annual Privacy Forum* (pp. 87-106). Springer, Cham.7

[3] Carlsson, A., Pedersen, C., Persson, F. and Söderlund, G., 2018. KAUDroid: A tool that will spy on applications and how they spy on their users. Karlstads universitet. (DIVA, student reports)

[4] Sundberg, S., Blomqvist, A., & Bromander, A. (2019). KAUdroid-Project Report: Visualizing how Android apps utilize permissions. (DIVA, student reports)

[5] Fritsch, L., 2017, June. Partial commitment–“Try before you buy” and “Buyer’s remorse” for personal data in Big Data & Machine learning. In IFIP International Conference on Trust Management (pp. 3-11). Springer, Cham.

[6] J. Wachter, T. Grafenauer, S. Rass: Visual Risk Specification and Aggregation. SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, IARIA, 2017, pp. 93-98, ISBN: 978-1-61208-582-1, https://www.thinkmind.org/index.php?view=article&articleid=securware_2017_6_10_38009, accessed 19-Aug-2019