Software Bills of Materials for Android

Kick-Off

Software Engineering Seminar

Thomas Sutter

2024

UNIVERSITÄT BERN

Zürcher Hochschule für Angewandte Wissenschaften

zh aw School of Engineering

Expectation

1. Develop a tool that can creating an accurate software bills of materials for Android apps

2. Evaluate the tool

3. Present your findings at the end of the semester in a 20 minutes talk (followed by 10 minutes Q&A)

4. Participate in the discussion, ask questions on colleagues' talks

Topic

Dynamic Analysis: Novel runtime library detection

- Build a detection method that is able to detect libraries during runtime
  - For example: “function traces”, “exceptions”, “memory”, or “logs”

Static Analysis: Develop and compare

- Students build their own fingerprinting method and compare it with existing tools
  - For example: “TLSH” or another similarity measurements

Procedere

1. Get Access to the data
2. Define research questions and read literature
   - Automated Third-Party Library Detection for Android Applications: Are We There Yet? https://dl.acm.org/doi/pdf/10.1145/3324884.3416582
   - A systematic assessment on Android third-party library detection tools https://ieeexplore.ieee.org/abstract/document/9551847/
   - Too Quiet in the Library: An Empirical Study of Security Updates in Android Apps' Native Code https://dl.acm.org/doi/pdf/10.1109/ICSE43902.2021.00122
3. Prototype Development
4. Prototype Evaluation
5. Presentation of Results

Getting access to a dataset

You can build your own testing data if you want.

- Otherwise use the Androzoo dataset: https://androzoo.uni.lu/
  - You need to write them an email and you will get an API-key

TODO

- Read Literature
- Define Research Questions
- Setup the testing and development environment
  - Android Studio
- Create a code repository on Github
  - Send me the link to your Github repository

- Next meeting date?