SOFTWARE TECHNOLOGY GROUP

Advanced Hands-on Training

Software Development Tools
Summer Semester 23

TuCan-No: 20-00-0673-pr
Course Type: 4SWS / 6CPs
Workload: **~180hours**

Prof. Dr.-Ing. Mira Mezini

Process

- **Today:** Send an e-mail with your three preferred topics and your knowledge about the topics to: **leonid.glanz@tu-darmstadt.de**
- **Tomorrow:** Assignment of topics
- **Next:** Contact your supervisor to discuss details of your topic
- **During Hands-on Training:** Bi-weekly meetings with supervisor in an agile process
    - Discuss the current state and the next steps
- **End of September:** Final submission of artifacts

Android Analysis: Not Reinvent the Wheel but Just Change the Tires

Many different tools are currently used for the security analysis of Android apps. These tools provide useful results, but these results are not combined in one report.

- **Task:** Extract & categorize results from different analysis tools.
- **Languages & Frameworks:** One of the languages we support & docker
- **Suitable for:** 1 - * people
- **Contact:** florian.breitfelder@tu-darmstadt.de

Android Analysis: Analyze the Analysers

Many different tools use Pattern matching to identify Vulnerabilities in Java source code. We also want to use these Patterns for Java bytecode.

- **Task:** Write a detector that parses regex expressions & categorizes them by the need analysis.
- **Languages & Frameworks:** One of the languages we support & docker
- **Suitable for:** 1 - 3 people
- **Contact:** florian.breitfelder@tu-darmstadt.de

Library Detection & Dependencies

Often libraries depend on others and are thus integrated together in an app. However, the connection between the libraries can no longer be traced afterwards and not all library versions are known in the app.

- **Task:** Build a gradle script that download dependencies from Maven Central and other source. Additionally, extract library information from apps.
- **Languages & Frameworks: JAVA &** Scala
- **Suitable for:** 1 - 2 people
- **Contact:** florian.breitfelder@tu-darmstadt.de

Library Binary Compilation & Detection

Binary libraries are integrated in different apps. However, libraries and their versions cannot be identified after they are compiled into an app.

- **Task:** Build a crawler that downloads the code of binary libraries and compile them with different options to create multiple signatures for the library version.
- **Languages & Frameworks:** One of the languages we support.
- **Suitable for:** 1 - 2 people
- **Contact:** florian.breitfelder@tu-darmstadt.de

Matching & Extending Missing Code

Many code snippets are not usable, because of missing code pieces.

- **Task:** Extract knowledge from a manually analyzed project to train a machine learning model that creates stubs for missing code pieces.
- **Languages & Frameworks:** Any machine learning model & docker
- **Suitable for:** 1 - 2 people
- **Contact:** leonid.glanz@tu-darmstadt.de

Cross-Language Call Detectors

Modern software is multilingual, especially when created with frameworks. To analyze multilingual software, cross-language calls must be detected.

Task: Write cross-language call detectors in our static analysis framework OPAL

- **Languages & Frameworks:** Scala, OPAL, JavaScript, Java, (C/C++)
- **Suitable for:** 1 - 3 people
- **Contact:** roth@cs.tu-darmstadt.de

Support for Machine Learning of Texts

Currently, text classification is a very popular tasks but needs a pre-labeled data set to enable classifications for new categories.

- **Task:** Develop a GUI that shows text and let users label specific parts which can be fed to a machine learning model as an advanced feature.
- **Languages & Frameworks:** Any language we support & docker
- **Suitable for:** 1 - 2 people
- **Contact:** leonid.glanz@tu-darmstadt.de

Flexible analyses for OPAL data structures

Our static analysis framework OPAL uses many pre-computed, static data structures, e.g., class hierarchy or a collection of all field accesses. Turning these into proper, modular analysis will open up many future possibilities, e.g., incremental analyses, better reflection support, or multi-lingual analysis.

Task: Take one or two data structures and turn them into proper analyses.

- **Languages & Frameworks:** Scala, OPAL
- **Suitable for:** 1 - 3 people
- **Contact:** helm@cs.tu-darmstadt.de

Positions & Theses

If you are interested in **HiWi Positions** or **Bachelor- or Master theses** contact: leonid.glanz@tu-darmstadt.de