

Hands-on Training Software Development Tools Winter Semester 24/25

TuCan-No: 20-00-0673-pr

Course Type: 4SWS / 6 CPs

Workload: ~**180hours**

Prof. Dr.-Ing. Mira Mezini

Process

- **Today:** Send an e-mail with your three preferred topics and why you are the right person for these topics to: **leonid.glanz@tu-darmstadt.de**
- **Tomorrow:** Assignment of topics
- **Next:** Contact your supervisor to discuss details of your topic
- **During Practicum:** Bi-weekly meetings with supervisor in an agile process
 - Discuss the current state and the next steps
- **End of March:** Final submission of artifacts

Create Vulnerable Apps for iOS or Cross-Platform Frameworks

To develop privacy and security analyses, it is crucial to have test cases to find vulnerabilities or privacy violations.

Task: Develop an app with each framework for Android or iOS that contains vulnerabilities similar to violations of MASVS. Also document the vulnerabilities and violations.

Languages & Frameworks: Dart, C#, Typescript, Swift or other languages

Suitable for: 1 - 7 people

Contact: leonid.glanz@tu-darmstadt.de



Analyse Libraries of Frameworks

To enhance app analysis, it's crucial to identify libraries that are used for frameworks like Flutter, Xamarin, and others in cross-platform apps, and discern how these libraries are integrated into compiled Android or iOS app.

Task: Develop an approach that analyzes vulnerabilities and up-to-dateness of libraries from different frameworks such as Xamarin, Ionic, and others. Utilize existing tools for Flutter, React Native, Unity, and Qt to supplement this analysis.

Languages & Frameworks: Python  or  & 

Suitable for: 1 - 2 people

Contact: leonid.glanz@tu-darmstadt.de



Extend a Static Analysis Tool for OWASP MASVS Compliance

To ensure app security, it's vital to comply with standards like OWASP MASVS, which requires specific security controls.

Task: Extend a static analysis tool that automatically checks if Android apps meet OWASP MASVS security controls.

Languages & Frameworks: Scala



Suitable for: 1 - 2 people

Contact: leonid.glanz@tu-darmstadt.de



OPAL Natural Language Interface

The OPAL framework provides extensive functionality for statically analyzing JVM programs. Configuring OPAL for custom use cases requires domain knowledge, making it inaccessible to the common software engineer.

Task: Develop an LLM Agent to interface with the OPAL static analysis framework

Languages & Frameworks: Scala  , LLM prompting

Suitable for: 1 - 3 people

Contact: naeumann@cs.tu-darmstadt.de



Static analysis of .NET CIL Programs

C# and the .NET framework provide a widely used tech stack, with applications ranging from mobile apps to high-stakes enterprise backends. C# is compiled to CIL (Common Intermediate Language), which is comparable to Java Bytecode in functionality and level of abstraction.

Task: Explore and evaluate existing static analysis tools and libraries for CIL programs. Implement security-related static analyses.

Languages & Frameworks: C#, .NET, Static Analysis (Soot/OPAL/Compilers)

<https://github.com/icsharpcode/ILSpy>

<https://github.com/jbevain/cecil>

Suitable for: 1 - 3 people

Contact: naeumann@cs.tu-darmstadt.de



Positions & Theses

If you are interested in **HiWi Positions** or **Bachelor- or Master theses** contact:

leonid.glanz@tu-darmstadt.de