
Hands-on Training

# Software Development Tools

# Summer Semester 24

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 September:** Final submission of artifacts

# Privacy Analysis in iOS Apps

Building on our tool for assessing the privacy declaration of Android apps, we need to extend this capability to iOS. This task involves using the Ghidra tool (https://ghidra-sre.org/) to develop a script that can extract specific information from iOS apps.

**Task:** Develop a script using Ghidra that can analyze iOS apps to extract and assess their privacy declarations. The script should be capable of identifying and parsing key privacy-related data.

**Languages & Frameworks:** Python  & Ghidra  & 


**Suitable for:** 1 person

**Contact:** leonid.glanz@tu-darmstadt.de

# Extract User Input Data from Cross-Platform Frameworks

To enhance user privacy and security assessments, it is crucial to understand what user data is collected and how it's handled by apps built with frameworks like Flutter, Xamarin, React Native and Unity.

**Task:** Develop a tool that extracts information about all user input fields and data collection mechanisms in Android apps. This includes checking if an app contains advertising libraries or other data-gathering features.

**Languages & Frameworks:** Python or Java or Kotlin & docker

**Suitable for:** 1 - 4 people

**Contact:** leonid.glanz@tu-darmstadt.de

Unity Xamarin React Flutter

# Identify Xamarin & Ionic Versions in Apps

To enhance security analysis for Xamarin and Ionic it is needed to accurately detect and identify the framework versions (Ionic or Xamarin) used in Android APKs and iOS IPAs.

**Task:** Compile and analyze sample apps using Ionic and Xamarin. Develop a tool that evaluates APK or IPA files to confirm the framework used and ascertain its version.

**Languages & Frameworks:** Python  or 

& 


**Suitable for:** 1 - 2 people

**Contact:** leonid.glanz@tu-darmstadt.de

Xamarin

IONIC

# Find Accompanying Libraries with Frameworks

To enhance app analysis, it's crucial to identify not just the versions of frameworks like Flutter, Xamarin, and others in cross-platform apps, but also to discern which binaries are integral to these frameworks.

**Task:** Develop filters to detect and categorize binaries associated with 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

# Automatic Compilation of GitHub Repositories

Efficiently compiling code from GitHub repositories requires an automated system to minimize manual setup and errors.

**Task:** Design and implement an automated compilation system. This system should initiate a virtual machine with Ubuntu, install necessary dependencies, and compile the GitHub repository to produce SO files.

**Languages & Frameworks:** Python or BASH & docker

**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

# Analyze and Identify Libraries in iOS Apps

To enhance security and compliance, it's essential to accurately identify and analyze libraries integrated into iOS apps, including their versions and the methods they use.

**Task:** Implement an iOS app with various libraries, then use Ghidra to develop scripts that can identify library code within the app.

**Languages & Frameworks:** Python  & Ghidra  & 

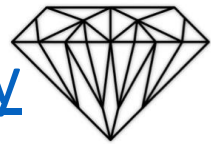

**Suitable for:** 1- 2 people

**Contact:** leonid.glanz@tu-darmstadt.de

# Relational Numerical Analysis in Sturdy

Sturdy is a static analysis framework implemented in Scala. We are currently implement relational numerical analyses in Sturdy to more precisely analyze WebAssembly programs.

**Task:** Extend our analysis to consider numeric overflows and numeric exceptions.

**Languages & Frameworks:** Scala  Sturdy  Apron

**Suitable for:** 1 - 2 people

**Contact:** sven.keidel@tu-darmstadt.de

# Positions & Theses

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