SEMINAR: SECURE SYSTEMS ENGINEERING

Introduction – October 20, 2016
OUTLINE

1. Basic Requirements
2. Preliminary Dates
3. Seminar Guidelines
4. Presentation of the Topics
Basic Requirements

- Completion of a seminar thesis in English
  - 20 pages written in LaTeX
  - We provided a template

- Design and run a presentation
  - Presentation is 30 min, to be held in a block seminar
  - 20 min for the contents
  - 10 min for discussion

- Reviews
  - Internal peer-review by students
  - also by supervisor
Preliminary Dates

- Thu, 20.10., 4:00 p.m.: Topic presentation
- Thu, 27.10., 11:00 a.m.: Seminar guidelines & introduction to scientific working

The following dates have their deadline 23:59 MEZ:

- Thu, 24.11.: Outline and literature references (student)
- Thu, 15.12.: Seminar thesis for review (student)
- Fr, 16.12.: Assignment of peer reviews (supervisors)
- Fr, 23.12.: Completed peer-review (student)
- Su, 15.01.: Presentation for supervisor feedback (student)
- Su, 22.01.: Supervisor feedback: presentation (supervisors)
- Su, 12.02.: Camera-ready version of thesis (student)
- Su, 26.02.: Supervisor feedback: thesis (supervisors)
- Su, 12.03.: Final hand-in of thesis (student)

Presentations (block seminar): 30.01.-03.02.2016
Seminar Guidelines

- Thursday, 27.10., 11:00 a.m. in ZM1.02-48
  - Presentation of seminar guidelines and rules
  - Introduction into scientific working
  - Participation is mandatory

- Topic Selection
  - Doodle poll
    - Choose exactly three topics
    - Each topic will be drawn from all applicants
  - Poll will be opened today at 6 p.m. and will be closed on Monday, October 24th at 4 p.m.
  - You will be informed via e-mail which topic you are assigned
    - Please confirm this mail until Tuesday, October 25th at 6 p.m.
OUTLINE

1. Basic Requirements
2. Preliminary Dates
3. Seminar Guidelines
4. Presentation of the Topics
Model-driven Security for Embedded Systems
Supervisor: Johannes Geismann

- When designing *safe and secure* embedded systems not only software but also hardware has to be considered.
- Model-driven approaches are used to assist designers and developers in early development steps.
- **SysML-Sec** is a method for this task.
- **Your task:**
  - Give a comprehensive overview.
  - Which threats / attacks are considered?
  - Which viewpoints are covered?
  - What are the assumptions/limitations made in this approach?
  - Compare to related approaches.

---

In Summary:

- Task: Compare two modelling languages in terms of their suitability for cryptography
- One student: Comparison based on papers
- Two students: Papers + Creating a model of subdomain in both languages

Supervisor: Stefan Krüger

stefan.krueger@upb.de

[Boucher et al., Introducing TVL, a Text-based Feature Modelling Language, VaMos 2010]
[Nadi et al., Variability Modeling of Cryptographic Components (Clafer Experience Report), VaMos 2016]
[Bak et al., Unifying Class and Feature Modelling, SoSyM 2014]
Architecture-based Intrusion Detection

David Schubert

- Code typically has flaws that can be exploited
- Finding all these flaws manually or by automated analyses is hard and expensive
- A second line of defense are runtime approaches that monitor the running system and aim at detecting intrusions (deviations from normal system behavior)
- These approaches are categorized by their information source

Literature:


Your Task:

1. Recap the approach by Yuan and Malek
2. Emphasize the (dis)advantages compared to classical host and network-based intrusion detection
Secure Isolation of Native Code for Java
Andreas Dann adann@mail.upb.de

General Risk: Java, Python, C#, JS, etc.

Real-Problem: Web-Server, Android, Plugins...

Solution: SFI, Process,…

Java Application

3rd Party Library

Security Risk: Malicious/Buggy

Outside of Language Security

Approaches:
- Robusta, Siefers J. et al., 2010 DOI: 10.1145/1866307.1866331
- JVM-Portable Sandboxing, Sun, M., 2012 DOI: 10.1007/978-3-642-33167-1_48
- JNICodejail, Hassanshai B., 2013 DOI: 10.1145/2500828.2500848

Your Task: Compare Approaches
- What is the concept?
- What threats are mitigated?
- What are drawbacks?
- Your Conclusion?
Static Analysis using LLVM

Supervisor: Philipp Schubert (Philipp.Schubert@upb.de)

- Static analyses can be used for automated bug detection and code optimization
- Static analysis builds on compiler infrastructure and vice versa
- Your task
  - Familiarize yourself with the powerful compiler technology LLVM (C/C++ based)
  - Give an overview on LLVMs capabilities
  - What is the concept? What are the benefits? What are the drawbacks?
  - What are the characteristics of the used IR?
  - Compare the LLVM project to related approaches
  - Two students: comprehensive comparison with Graal & Truffle project
- Learning outcomes
  - Understand basic concepts of compiler technology & static analysis
  - Gain deeper understanding of how programming languages are processed

Graal & Truffle Compiler Technology

Supervisor: Philipp Schubert (Philipp.Schubert@upb.de)

- Static analyses can be used for automated bug detection and code optimization
- Several compiler projects exist (specific advantages / disadvantages)
- Your task
  - Familiarize yourself with the Graal & Truffle project (Java based)
  - What is the concept of Graal & Truffle?
  - What are the benefits? What are the drawbacks?
  - What are the characteristics of the used IR?
  - Compare the Graal project to related approaches
  - Two students: comprehensive comparison with the LLVM project
- Learning outcomes
  - Understand basic concepts of compiler technology & static analysis
  - Gain deeper understanding of how programming languages work

https://github.com/graalvm/graal-core/blob/master/docs/Publications.md
Security Risks in Android’s Inter-App Communication

Supervisor: Goran Piskachev

- Android Apps can exchange messages to make a re-use of some functionalities provided by components in other applications.
- For example, a review app for restaurants can ask the map application to display the location of the restaurant.
- **Problem:** The Android passing message system which enables the Inter-App communication may be attacked if it is used incorrectly. The messages can be sniffed, modified, or stolen.
- **Approach:** Analysis of Android applications and automatic detection of known vulnerabilities related to the Inter-App communication.
- **Your task:**
  - Give an overview and classification of attacks to the Inter-App communication.
  - Evaluate at least two analysis tools using your classification.

**Literature:**

Surveying Requirements Specification Approaches for Information Flow Security
Supervisor: Christopher Gerking

- Secure Information Flow of Cyber-Physical Systems (CPS) is critical
- Problem: How to specify Information Flow Requirements?

Literature
Relaxing Information Flow Restrictions by means of Information Declassification

Supervisor: Christopher Gerking

- Classical Noninterference Policy too strict in Practice
- Problem: How to relax Information Flow Restrictions?
- **Your Task:** study the Theory of Noninterference, give an Overview of existing Approaches for Declassification, demonstrate Advantages and Shortcomings in the context of CPS

**Literature**

A Survey of Static Code Analysis techniques for PLC Programs

Supervisor: Faezeh Ghassemi

- Static code analysis (SCA) is analyzing the code without executing it

- There are plenty of SCA tools and techniques for languages like Java and C

- Not many tools/approaches for **PLC programming languages**

Your task

- Make a survey of existing static analysis tools and methods for PLC programming languages and explain their capabilities as well as advantages and disadvantages

Literature


faezeh.ghassemi@iem.fraunhofer.de
SECURE TROPOS – Integrating Security and Systems Engineering
Supervisor: Thorsten Koch

■ Problem

Security is a crucial issue for information systems. However, in Software Engineering security is mainly considered as non-function requirements after the definition of the systems. This approach often leads to problems, which translate to security vulnerabilities.

■ Approach

The methodology Secure Tropos is proposed to model and analyze security requirements alongside functional requirements. It provides a requirements analysis process that drives system designers from the acquisition of requirements up to their verification to consider security during the whole development process.

■ Your Task

■ Describe the methodology Secure Tropos

■ Especially focus on the possibilities to analyze the specified security requirements

Literature


[http://www.troposproject.org/node/301]
Topic Selection

- Doodle poll
  - Choose exactly three topics
  - Each topic will be drawn from all applicants
  - Poll will be opened today at 6 p.m. and will be closed on Monday, October 24th at 4 p.m.

- Write a mail if you would like to work in a “group”
  - Names of both students
  - Topic number
  - Important: Both students have to mark this topic in the doodle poll!

- You will be informed via e-mail which topic you are assigned
  - Please confirm this mail until Tuesday, October 25th at 6 p.m.