Seminar course

Secure and Reliable Systems

(aka “secure-reliable-seminar”)

Preliminary meeting

https://dse.in.tum.de/

Dr. Redha Gouicem

Prof. Pramod Bhatotia

About us

Chair of Decentralized System Engineering

- Dr. Redha Gouicem
  - Postdoc
  - **Project:** Binary translation for weak memory architectures, virtualization
  - https://redha.gouicem.fr/

- Prof. Pramod Bhatotia
  - Professor
  - https://dse.in.tum.de/

Seminar info

https://github.com/**TUM-DSE/seminars/**

slack

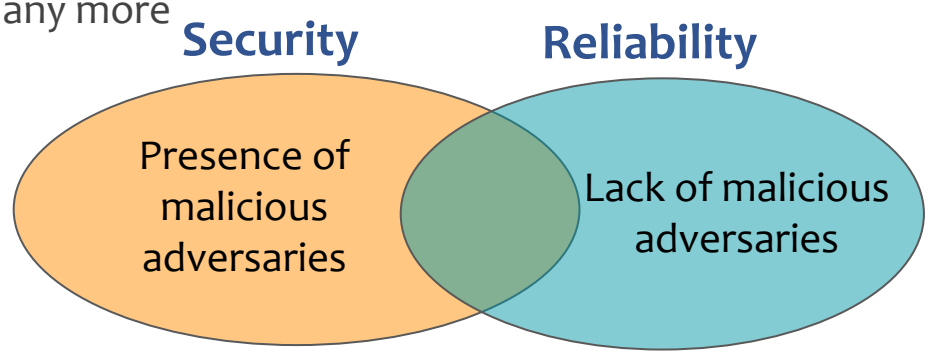
Communication:

Join us with TUM email address (@tum.de)
ls1-courses-tum.slack.com
#ws-22-secure-reliable-seminar

Context and motivation

Motivation

- Why security and reliability are important?
  - Sensitive data protection
  - Cyber-physical systems
  - National security
  - Economic cost
  - ..and many more



This course covers **mechanisms** to make systems **secure** and **reliable**

Concepts

- Security:
  - Ensuring goals (i.e. policies) in presence of malicious adversaries
  - Malicious adversaries:
    - e.g) Attacker reads user_x's password, and attempts to login with it.
  - Policies of security :
    - e.g) Only user_x can login to one's account
- Reliability:
  - Ability of a system to perform its required tasks under stated conditions for a specified period of time
  - Stated conditions:
    - Usually non-malicious adversaries
      - e.g) Missed communication of an emergency response device

High-level plans

- How to build secure systems
  - Set a goal (policy)
    - e.g.) Only user_x should be able to login
  - Set a threat model
    - Target adversaries you want to prevent and assume possible scenarios
    - E.g) Attackers can guess passwords, but cannot access to file server
  - Set a mechanism to prevent attackers' success
    - e.g) Adopt two-step verification for login
- How to build reliable systems
  - Get a goal (specification)
    - We already know a definition of what an error is
  - Set a mechanism to check deviation between an application and spec
- Note: a goal itself has nothing to do with mechanisms.

Intersection of security and reliability

- Aiming similar goals, so sharing mechanisms
  - Confidentiality
  - Integrity
  - Availability
- Ensuring one property helps one another
  - Many security vulnerabilities can be sanitized in the first place by ensuring reliability
  - A set of most exploited but addressable security vulnerabilities is small

Challenges in building secure/reliable systems

- Challenges in security
  - We don’t know what we are looking for
    - Assuming a threat model is best offer
  - Difficult to deploy a right mechanism at the right time
  - Attack mechanisms evolve
  - Policy may be irrelevant if the implementation has bugs.
- Challenges in reliability
  - What we are looking for is too broad
    - Entirety of the application (reliability bugs can be anywhere)
  - Many specifications are in a bad shape
    - Written in natural language, out-of-date
- Challenges in common
  - Reduce cost in both economic and performance aspects

Topics

Topics

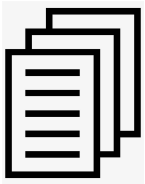
Security topics
Sanitizers (static/dynamic analysis, programming languages)
Formal verification, Symbolic execution
Threat models
Architectural support for system protection
Capabilities
Enclave
Software-based fault isolation (sandboxing)

Reliability topics
Sanitizers (static/dynamic methods, programming languages)
Formal verification, Symbolic execution
Fault models: Transient or permanent, Hardware or software faults
Fault injection: Fuzzing
Replication protocols
Testing: Concolic testing, Fuzzing

Format

Bird’s eyes view

Team
(2 students per team)



Research paper

Understand

Research ideas

1 presentation

1 short report

Peer-reviewing

Overview

Phase I

Kick-off

Phase II: Understand & explore

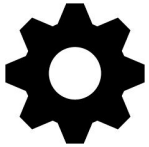
Understand

Presentation

Phase III: Research

Design

Implement (Bonus)



Phase IV: Report & review

Report

Peer-review

Phase I: Kick-off meeting

Format and motivation
(all participants meeting)

Team formation
(2 students per team)

Paper selection
(Most referenced papers, or big impact)

The first week

NOTE

1. A list of papers will be provided for FCFS bidding
2. Paper presentation guidelines will be provided for the next phase

Phase II: Understand & explore

Understand the paper(s)

Focus

1. **Understand** the paper and related work
2. Also **explore** a "laundry list" of research ideas/directions

Paper presentation

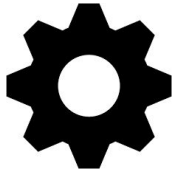
Focus

1. Explain the work/related work (**"why?"** and **"how?"**)
2. Explain and discuss all possible research directions
3. Pick a research direction

Phase III: Research

Research work

Focus:
Indepth research work to nail-down the problem and detailed approach to solve it!



Research prototype

Bonus:
(Optional)
"Build the system to solve it!" and show us the working idea and associated results

Phase IV: Report & review

Report

Focus

Prepare a single “short & sweet” report summarizing

(a) Paper

(b) Research work

Peer-review

Focus

Give constructive (positive and critical) feedback for

(a) Paper summary

(b) Research work

END.

Overall timeline

Phase I

Kick-off

Phase II: Understand & explore

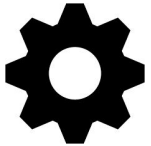
Understand

Presentation

Phase III: Research

Design

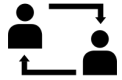
Implement (optional)



Phase IV: Report & review

Report

Peer-review



Milestone #1: Team formation & paper selection

Milestone #2: Paper presentations

Milestone #3: Research work complete

Milestone #4: Report submission

Milestone #5: Peer-reviewing

1 week

3 weeks

2 weeks

3 weeks

1 week

2 weeks

Meeting

Meeting

Organization

- Format
  - Team-based seminar course (2 students per team)
- Communication
  - Slack for announcements and information sharing
  - Hotcrp for report submission and peer-reviewing
- Meetings (**in-person, attendance is compulsory**)
  - **Meeting #1:** Kick-off
  - **Meeting #2:** Paper presentation

Learning goals

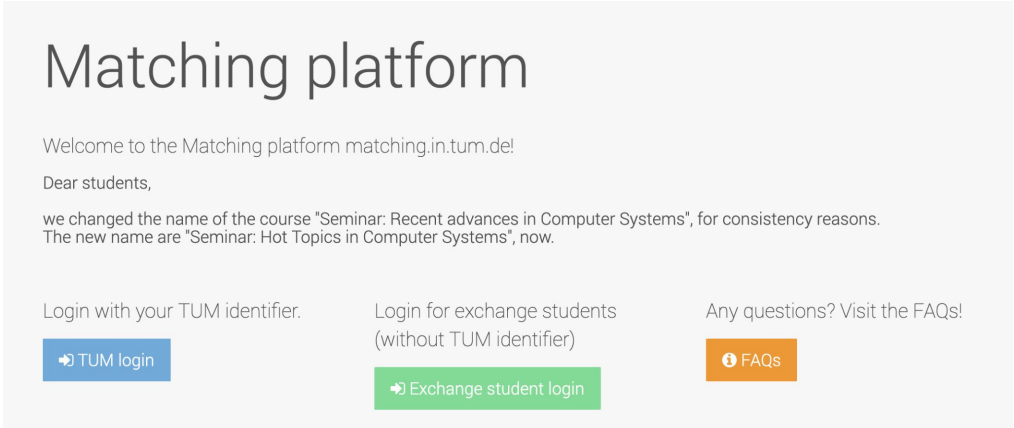
- Explore advanced and seminal research topics
- Promote critical and creative thinking
- Constructive feedback and peer-reviewing
- Presentation and writing skills

Code of conduct

- University plagiarism policy
  - https://www.in.tum.de/en/current-students/administrative-matters/student-code-of-conduct/

- Decorum
  - Promote freedom of thoughts and open exchange of ideas
  - Cultivate dignity, understanding and mutual respect, and embrace diversity
  - Racism and bullying will not be tolerated

Interested?



Sign up on the TUM matching platform

Contact

- Dr. Redha Gouicem
  - https://redha.gouicem.fr/

- **All seminar-related info:** https://github.com/TUM-DSE/seminars

Communication:
Join us with TUM email address (@tum.de)
Workspace: ls1-courses-tum.slack.com
#ws-22-secure-reliable-seminar