

# Formal Methods in IT Security — SS 2023

Seminar

Ludwig Peuckert &  
Maximilian von Tschirschnitz

Lehrstuhl für Sicherheit in der Informatik / I20  
Prof. Dr. Claudia Eckert  
Technische Universität München

February 7, 2023

# What is this seminar about?

- ▶ **Formal Verification and Model Checking** in IT Security
- ▶ **Logic and Calculus** e.g. Logic for Authentication, Strand Spaces, BAN
- ▶ **Secure Code Generation**
- ▶ **Threat Modeling**

# Process

- ▶ Phase **I**: Select a **topic**
- ▶ Phase **II**: Find **literature**
- ▶ Phase **III**: Do your **reading / experiments / programming**
- ▶ Phase **IV**: **Writing** phase I
- ▶ Phase **V**: **Peer review**
- ▶ Phase **VI**: **Writing** phase II
- ▶ Phase **VII**: Final **talks**

Exact schedule will be published once list of participants is known.

# Phase I

1. We will provide you with a list of **our topics of interest**
2. You will **choose / propose** your own topic and either:
  - ▶ Work out the crucial design flaw
  - ▶ Elaborate on mitigations and impact on protocol security
  - ▶ Reproduce the results of an existing conference paper
  - ▶ Create your own Systematization of Knowledge (SoK) paper
3. In all cases, you will put your work into context of existing literature
  - ▶ e.g. at Usenix Security Symposium, S&P, ACM CCS, NDSS

# Our Topics of Interest

- ▶ Threat modeling approaches
- ▶ Verification tools like Tamarin, ProVerif
- ▶ Formal Verification for Protocols
- ▶ Automatic Code Generation/Validation from Specification
- ▶ **Or:** Provide us with your own topic proposal

# Registration

- ▶ Registration using the **matching system**
- ▶ Letter of motivation (approx. half page)
- ▶ Why are you particularly qualified for this seminar (preknowledge, projects)?
- ▶ What are your expectations to this Seminar ?
- ▶ Send letter to Ludwig using your university email before matching closes with Subject: "Motivation Letter - `YOURNAME`"
- ▶ Approx. **8** slots

# Time and Place

**When?** We pick the slot  
① With the least collisions

**Where?** Talks at the **end** of the semester





# Time and Place

**When?** We pick the slot  
① With the least collisions

**Where?** Talks at the **end** of the semester  
Seminartagungsstätte Frauenchiemsee  
**Disclaimer:** Only if participants interested + we have time!  
Fallback: On-campus conference

# Questions?

Contact us at  
peuckert@sec.in.tum.de,  
tschirschnitz@sec.in.tum.de