Advanced Security Analysis
WS 2025

Seminar

Maximilian von Tschirschnitz

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

July 9, 2025

What is this seminar about?

- How can machines interact securily ?
- How can we establish Trust between multiple parties ?
- How can we collaborate trustless ?
- Investigating issues, advanced and interesting cases of Secure Protocol Design and its verification.
- How can we assure correctness of these protocols ?
- Security Proofs and Proving Frameworks, Security Models.
- Code Generation
- Differential Privacy

What is expected?

- Curiosity and motivation to actually learn something new.
- Regular in-person attendance to our meetings.
- Endurance and ability to time manage.

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. I will provide you with a list of starting points for topics that are of interest for this seminar
2. You will **choose / propose** your topic by skimming and deep diving
3. 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

- Secure Code Generation from Specification
- Formal Security Models and Proving Strategies.
- Formal (Computer Aided) Verification of interesting Protocols
- Secure Multi Party Computation
- Provenance and Dependency Analysis in Practical Settings
- Privacy Protecting Networks
- Privacy Protecting Shared Storage and Computation
- Quantum Information Theory for Trust Establishment
- Proximity as Trust Factor
- Trustmanagement in Groups/Teams
- Game Theory
- Or: Provide me with your own topic proposal and I will consider it

Registration

- Registration using the **matching system**
- Letter of motivation required (no generated content)
- Email **one paragraph** why you want to do this seminar
- If you have a project/topic idea on your own, suggest it here
- Your interests/skillset for that course and progress of studies
- Send **with subject** [ASA] to tschirschnitz@sec.in.tum.de

Time and Place

When? I pick the slot
① for Bi-Weekly Meetings during the Semester
② with the least collisions
③ Physical attendance mandatory!

Talks at the **end** of the semester

Time and Place

When? I pick the slot

① for Bi-Weekly Meetings during the Semester

② with the least collisions

③ Physical attendance mandatory!

Talks at the **end** of the semester

Grading

	40 %	Final Paper (Content, Style, Language, Scope, ...)
	10 %	Practical application (depends on topic)
	10 %	Review
	30 %	Presentation (Content, Style, Timeliness, ...)
	10 %	Discussion
Σ	100 %	Total

Questions?

Contact me at
`tschirschnitz@sec.in.tum.de`