

Concepts of Trust Establishment
WS 2024/25
Seminar

Maximilian von Tschirschnitz

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

July 11, 2024

What is this seminar about?

Grasping the concepts of Trust and how we can establish it (autonomously).

- ▶ What does the relation of Trust actually mean?
- ▶ What established/novel concepts of Trust Establishment are available ?
- ▶ For what action do we need which Trust / Trustless application ?

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

- ▶ Password Authenticated Key Agreement
- ▶ Zero Knowledge Proofs
- ▶ Formal (Computer Aided) Verification of Trust Establishment Protocols
- ▶ Onion Routing / Privacy Protecting Networks
- ▶ Device Finding Networks (Find My Device)
- ▶ Provenance and Dependency analysis in practical settings
- ▶ Proximity as Trust Factor
- ▶ Trustmanagement in Groups/Teams
- ▶ Game Theory applied to Ad Hoc networks
- ▶ **Or:** Provide me with your own topic proposal and I will consider it

Registration

- ▶ Registration using the **matching system**
- ▶ Letter of motivation gets preference
- ▶ 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
- ▶ Send **with subject** [CTE] 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`