Selected Topics of Protocol Security
WS 2023/24

Seminar

Maximilian von Tschirschnitz

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

July 4, 2023

What is this seminar about?

Familiarize innovative approaches to protocol design and change how we think about protocols.

- **Analysis** Application of different protocol analysis methods (Game Theory, Dependency Analysis, etc..)
- **Elaborate** On new approaches and new challenges
- **Mitigations** Verification, Code Generation

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 and thereby either:
   - Model, analyse or compare some existing protocol based on existing (underutilized) schemes
   - Compare different forms of modeling protocols
   - Elaborate on novel (cryptographic) approaches (e.g. Cryptographic Voting)
   - Elaborate on certain mitigations and their impact on protocol security
   - Create your own Systematization of Knowledge (SoK) paper
3. In all cases, you will put your work into context of exisiting literature
   - e.g at Usenix Security Symposium, S&P, ACM CCS, NDSS

Our Topics of Interest

- Modeling Protocols as Probabilistic I/O Automata
- Application of Game Theory on Wireless Sensor Networks
- SoK: Integrity Codes
- Survey on Threat/Attacker Models
- Cryptographic Voting in Ad Hoc Networks
- Homomorphic Time Lock Puzzles
- Zero Knowledge Proofs
- Automatic Code Generation/Validation from Specification
- (maybe) Protocols for Group Management
- (maybe) Specific Attacks (e.g. Downgrade, Replay)
- **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
- Your interests/skillset for that course
- Send **with subject** [STPS] to tschirschnitz@sec.in.tum.de

Time and Place

When? I pick the slot

① for Bi-Weekly Meetings during the Semester

① with the least collisions

② 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

① with the least collisions

② 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 us at
tschirschnitz@sec.in.tum.de