Common Flaws in Protocolsecurity — SS 2022
Seminar

Ludwig Peuckert &
Maximilian von Tschirschnitz

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

January 31, 2022
What is this seminar about?

- **Design flaws** in communication protocols
- **Mitigations**, Fuzzing, Verification, Code Generation
- **Lessons learned**: Effect on later protocol generations
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

- Specific Attacks (e.g. Downgrade, Replay)
- Implementation Specific Bugs (e.g., Heartbleed, Ping of Death)
- Trust Establishment Design Principles (PKI, Web of Trust, TLS)
- Formal Verification for Protocols
- Automatic Code Generation/Validation from Specification
- Or: Provide us with your own topic proposal
Registration

- Registration using the matching system
- No letter of motivation
- approx. 16 slots
Time and Place

**When?** We pick the slot
① with the least collisions
② most comfortable for you

Talks at the **end** of the semester

**Where?**
Time and Place

**When?**  We pick the slot
① with the least collisions
② most comfortable for you

Talks at the **end** of the semester

**Where?** Seminartagungsstätte Frauenchiemsee

**Disclaimer:** Only if participants show interest!

Fallback: On-campus conference
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
peuckert@sec.in.tum.de,
tschirschnitz@sec.in.tum.de

https://www.sec.in.tum.de/i20/teaching/common-flaws-in-protocolsecurity