Formal Methods in IT Security — WS 2022/23

Seminar

Ludwig Peuckert &
Maximilian von Tschirschnitz

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

July 11, 2023

What is this seminar about?

Structural and **mathematical analysis** for improved security

- **Detect** design flaws (Fuzzing, Model Checking)
- **Develop** secure systems (Logic, Code Generation)
- **Proove** security (Verification)

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:
   - Apply a Formal Method
   - Develop a Formal Method
   - Reproduce the results of an exisiting conference paper
   - 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

- Fuzzing
- Formal Verification and Theorem Proovers
- Logic and Calculus (e.g. Logic for Authentication, Strand Spaces, BAN)
- Automatic Code Generation / Validation from Specification
- Threat Modeling
- **This year we will focus on Protocol Security**

Our Topics of Interest

- Fuzzing
- Formal Verification and Theorem Proovers
- Logic and Calculus (e.g. Logic for Authentication, Strand Spaces, BAN)
- Automatic Code Generation / Validation from Specification
- Threat Modeling
- **This year we will focus on Protocol Security**
- **Or:** Provide us with your own topic proposal

Registration

- Registration using the **matching system**
- Letter of motivation (approx. half page)
- What is your background (previous courses, etc.)?
- Why do you want to participate in this seminar?
- What are your expectations?
- In which topics are you interested?
- Send to `peuckert@sec.in.tum.de` before matching closes, subject "Motivation Letter – $YOURNAME"
- approx. **8** slots

Time and Place

When? Thursdays 14:00 - 16:00 roughly Bi-Weekly

① Some meetings will be canceled

② First meeting in the first lecture week

③ First task before first meeting

Talks at the **end** of the semester

Where?

Time and Place

When? Thursdays 14:00 - 16:00 roughly Bi-Weekly

① Some meetings will be canceled

② First meeting in the first lecture week

③ First task before first meeting

Talks at the **end** of the semester

Where? Seminartagungsstätte Frauenchiemsee

Disclaimer: Only if participants show interest!

Fallback: On-campus conference

Grading

	50 %	Final Paper (Content, Language, Scope, . . .)
	10 %	Practical application (depends on topic)
	mandatory, 0 %	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