Seminar Common Flaws in Protocol Security

Session 1

Maximilian von Tschirschnitz, Ludwig Peuckert
I20

Winterterm 2022
18. Oct 2022

Timeline

Phase	Description	Creates Deliverable	Due Date
P	Choose a topic	Citation graph	18.10.2022
I	Deep dive & Concept	Identify research questions	25.10.2022
II	Refine concept	A well structured idea for your paper	08.11.2022
III	Writing	Paper draft (review version)	13.12.2022
IV	Reviewing & writing	Your reviews	20.12.2022
VI	Presentation deadline	Presentation ready	30.01.2023
–	End of Lecture Period	Paper camera ready	11.02.2023

Goal of this Course

We want you to develop your skills as a member of the scientific community:

- Surveying skills (Related Work).
- Ability to conceptualize abstract concepts for yourself.
- Ability to adjust such concepts.
- Ability to present your thoughts to others in clarity.

⇒ **Show us that you posses those skills, by presenting a representative work!**

For Example

Some paper types that would be perfectly suited as demonstrator of your amazing research skills:

- Simplified representation of existing knowledge (simplify for the next reader).
- Reproduction of an experiment and interpretation of results.
- Creative combinations of existing techniques.
- Systemization of Knowledge and discussion.

Your paper does not need to present groundbreaking innovation!
(ofc cool if it does)

Orga

- Meeting (about) every 2 weeks in presence. **The TUM calendar counts!**
- Regularly: Complete provided exercises, and receive feedback from us and others.
- We will have at least one round of personal meetings with us and each of you. (When?)
- Issues?

Help with Literature

Technische Universität München

- https://scholar.google.com
- https://semanticscholar.org
- https://dblp.uni-trier.de
- https://arxiv.org
- Get around paywalls using https://login.eaccess.ub.tum.de/login or bookmarklet:

```
javascript:void(location.href='https://eaccess.ub.tum.de/login?url='+location.href)
```

- Researchers' homepages can be valuable! (source code, raw data, instructions, technical information, ...)

Buddy System

“Hey... you wanna be buddys ?”

Next Exercise

Identify points of interests for your paper concept

For this we ask you to execute the following iterative process.

1. Go through your catalog of papers (Make notes!) and ask yourself questions like

(a) What are remaining research questions, what was hard to understand? **What annoyed you?** Provide context to your answers!

(b) Have those results been reproduced? If not, why not ?

(c) Which works or results should be compared with each other ? What would such a discussion yield?

(d) Why was an attack possible ? Is there an underlying systematic problem? What was affected? What can be done now ?

2. Try to resolve those questions (e.g.)

(a) Are there better explanations in other papers ? Has future work already been addressed ?

(b) Are there already reproductions of this aspect ? If so, do you agree with the methodology ?

(c) What comparisons where drawn in other works on this topic?

(d) How did the community react to this attack ? Are there follow up-publications?

3. Repeat on the new material until you are left with a large collection of unresolved questions.

Next Exercise

Be ready to present those possible research questions to the course.

The End (for today)

Technische Universität München

Questions?