

SEMINAR WINTER TERM 2025/2026: CYBER-PHYSICAL SYSTEMS SECURITY (CPSS)

PRE-COURSE MEETING 08.07.2025

Contents

- **Fraunhofer AISEC**
- **Seminar Schedule/Orga/Grading**
- **Seminar Topics Overview**
- **FAQ**

Fraunhofer AISEC

Facts & figures

- **Founded:** 2009
- **Employees:** approx. 250
- **Locations:** Garching near Munich (main location), Berlin, Weiden i.d. Oberpfalz
- **International:** Partner institute of Fraunhofer Singapore
- **University connections:**



Prof. Dr. Eckert und
Prof. Dr. Sigl



Prof. Dr. Margraf



Prof. Dr. Loebenberger

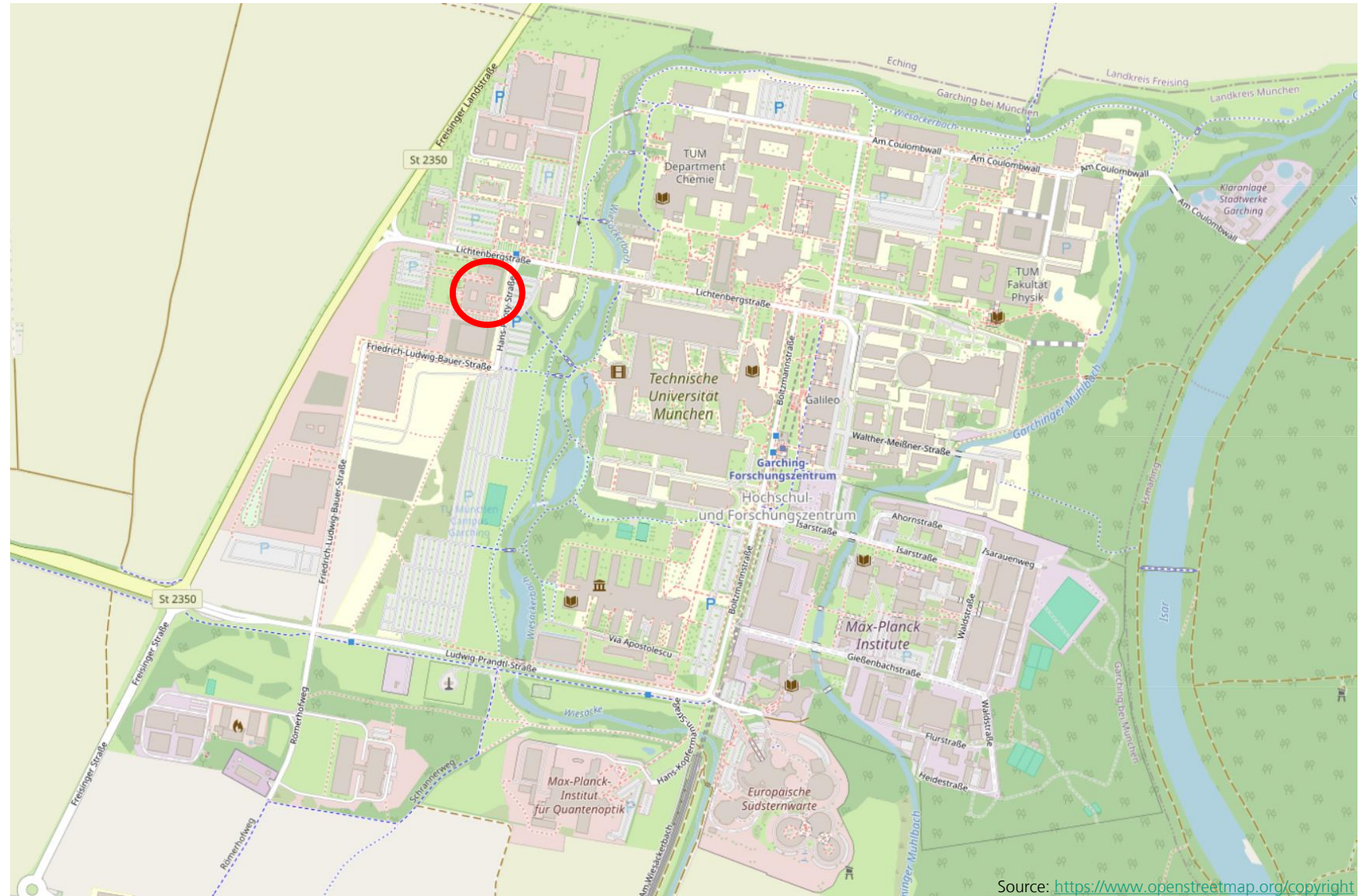


© Hans Georg Esch

Last updated: October 2024

Fraunhofer AISEC

Location



Fraunhofer AISEC

Areas of expertise



Service and Application Security

Cloud and container infrastructures,
distributed applications



Secure Operating Systems

Security of hardware-facing
software and operating systems



Product Protection and Industrial Security

Anti-counterfeiting, automotive security,
industrial security, IoT, smart building



Hardware Security

Trustworthy electronics and
secure embedded systems



Cognitive Security Technologies

Security for, with and through AI



Secure Infrastructure

Application of cryptographic methods,
secure network protocols



Secure Systems Engineering

Secure and user-friendly
digital systems

Security from Hardware to the Cloud

Course Objectives

Assessing the state of the art regarding a specific topic in the context of security

- **Write a paper** about your findings
- **Give feedback** to (two of) your fellow students' papers (peer review)
- **Give a talk** in order to **discuss** your topic with your fellow students at the end of the semester

Previous Knowledge?

- no formal requirements
- ITsec knowledge necessary!



Orga

Communication

- TUM Moodle
- Video Calls via MS Teams
- E-mail – **always use "reply-all"** when writing or answering to us!
- Language of instruction and deliverables will be **English**

Individual work (no groups)

Registration in matching system (<http://docmatching.in.tum.de/>)

Motivational e-mail to security-seminar@aisec.fraunhofer.de

About, e.g., your relation to (IT-)security, your bachelor thesis, completed ITsec courses, your preferred topics from the seminar, which topic you like most, and why

Process (1/4)

08.07.2025 (today)

- Organizational information
- Overview on topics

31.07.2025

- Automated assignment of courses

Until 22.07.2025

- Registration via DocMatching: <http://docmatching.in.tum.de/>
- **Motivational email** to security-seminar@aisec.fraunhofer.de

Until 04.08.2025

- Please send us an *ordered* list of your 5 preferred topics via email (if not already done in your motivational email)

Process (2/4)

Until 06.08.2025

- Response from organizers with assigned topic
- Possibility to withdraw without penalty - non-attendance after this point is graded with 5.0

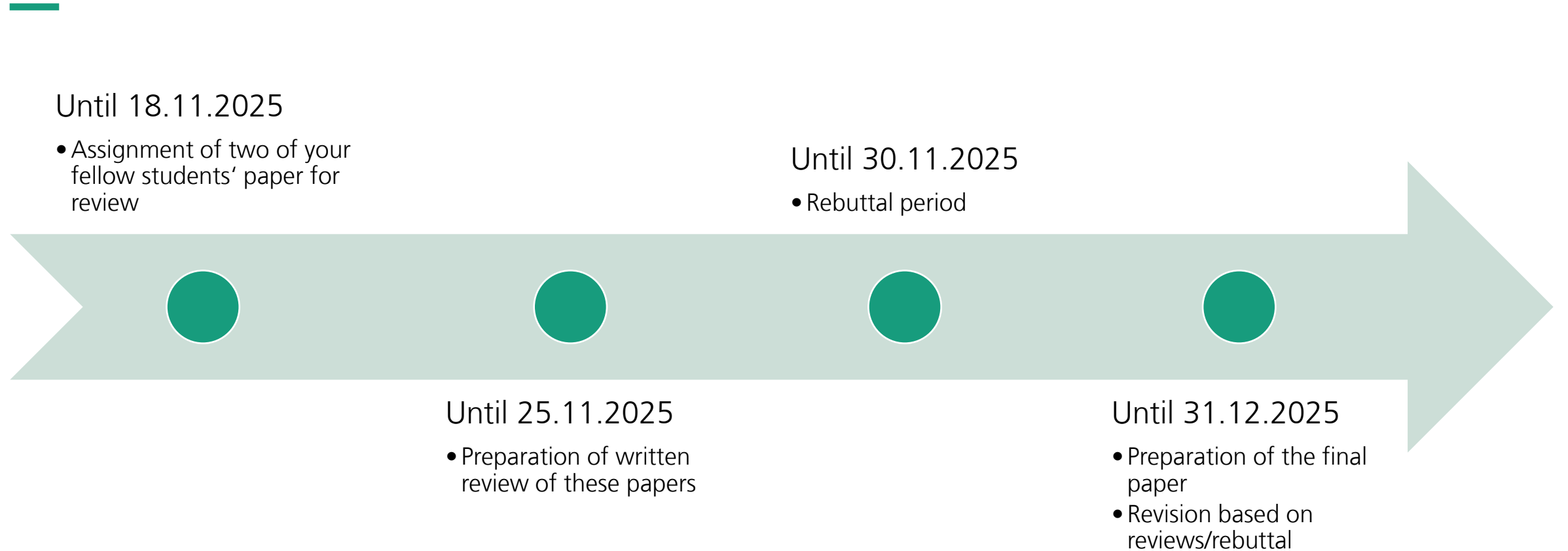
Until 16.11.2025

- Preparation of the draft version of the paper
- Submission of the draft is **obligatory!**

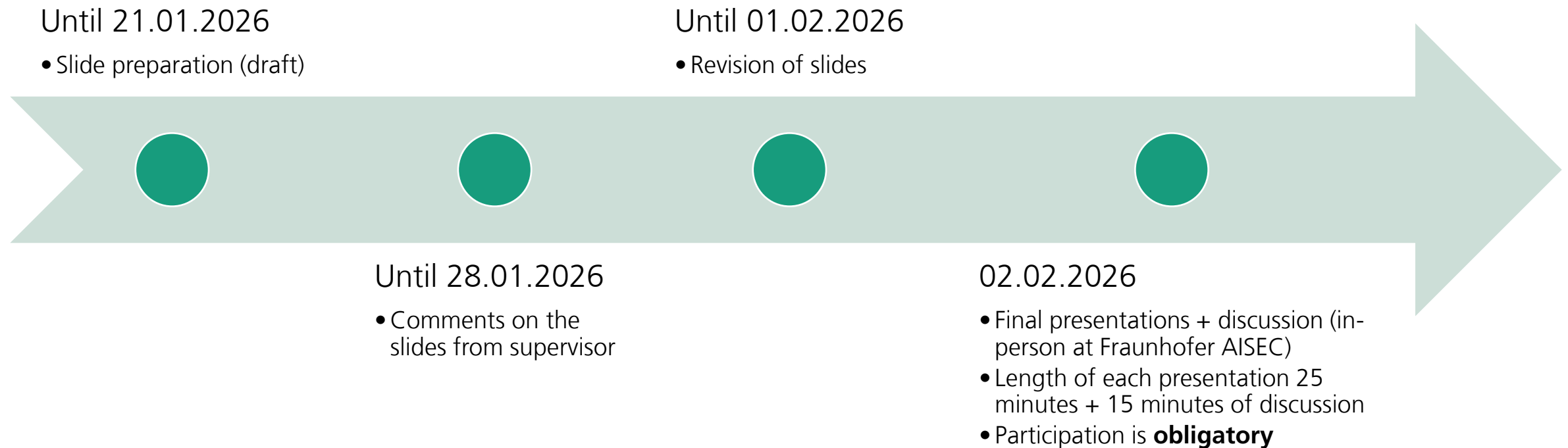
Until 30.09.2025

- Familiarize with literature
- Deep dive into your topic
- As soon as possible: Schedule a kickoff meeting with your supervisor – **obligatory!**

Process (3/4)



Process (4/4)



Deadlines for Obligatory Deliverables

	Due to	Grading
Schedule 1-to-1 Kick-Off Meeting with supervisors	30.09.2025	Obligatory
Submission of Draft Paper	16.11.2025	10%
Reviews	25.11.2025	5%
Rebuttal	30.11.2025	Obligatory
Submission of Final Paper	31.12.2025	50%
Presentation	02.02.2026	30%
Presentation Discussion	02.02.2026	5%
		Σ 100 %

-> Missing any deadline will have a major impact on your grade.

Paper writing and presentation

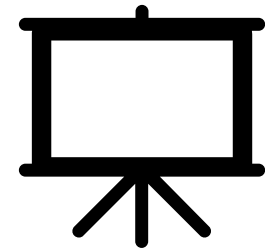
Paper

- Systematization of Knowledge (SoK)
- ~10 pages excl. list of references and appendices
- IEEE conference proceedings template
- Utilization of LaTeX (highly recommended)
- Note the *Scientific writing guide* in the Moodle course

Presentation

- MS Powerpoint or similar
- 25 minutes presentation
- 15 minutes discussion - moderated by you

L^AT_EX



Cyber Physical Systems Security (CPSS)

Topic 1: Industrial Bootstrapping using the WiFi Device Provisioning Protocol (DPP)

Possible questions to be answered: What is DPP? Which security features does it offer? What are the relevant requirements for Device Onboarding/Enrollment in industrial applications? To what extent does DPP fulfill them?

Literature to start from:

- Security analysis of the Wi-Fi Easy Connect - <https://link.springer.com/article/10.1007/s10207-025-00988-3>
- WIFI Easy Connect Specification - <https://www.wi-fi.org/wi-fi-download/35330>
- Leveraging BRSKI to Protect the Hardware Supply Chain of Operational Technology: Opportunities and Challenges - <https://dl.acm.org/doi/10.1145/3672608.3707707> [requirements]

Topic 2: DHCP Authenticity – A lost cause?

Possible questions to be answered: Which methods are around to ensure authentic DHCP communication? Are they in use? What hinders the deployment? How would authenticity be ensured with today's methods? → Possibility for your own proposal.

Literature to start from:

- DHCPAuth — A DHCP message authentication module - <https://ieeexplore.ieee.org/abstract/document/7208238>
- RFC 3118 Authentication for DHCP Messages - <https://www.rfc-editor.org/info/rfc3118> (very old)
- DHCP Authentication Using Certificates - https://link.springer.com/chapter/10.1007/1-4020-8143-X_30

Topic 3: Password Strength Estimators

Possible questions to be answered: Which different approaches exist to measure, display, and communicate the strength of passwords? What do they have in common, and which aspects are different? What is the latest state of research in that field (apart from transitioning to Passkeys and MFA)?

The possibility for a small evaluation/testbed exists - going a bit beyond a pure SoK paper.

Literature to start from:

- On the Accuracy of Password Strength Meters - <https://dl.acm.org/doi/abs/10.1145/3243734.3243769>
- From Very Weak to Very Strong: Analyzing Password-Strength Meters - <https://spectrum.library.concordia.ca/id/eprint/978105/>
- An Explainable Online Password Strength Estimator - https://link.springer.com/chapter/10.1007/978-3-030-88418-5_14

Topic 4: AI Agent Authenticity

Possible questions to be answered: What are (personal) AI agents expected to look like? How would they communicate? How could the authenticity of that communication be ensured?

Motivation: <https://www.youtube.com/watch?v=EtNagNezo8w>

Literature to start from:

- A Novel Zero-Trust Identity Framework for Agentic AI: Decentralized Authentication and Fine-Grained Access Control - <https://arxiv.org/pdf/2505.19301>
- Holistic Authentication Framework for Virtual Agents; UK Banking Industry - https://link.springer.com/chapter/10.1007/978-3-030-87166-6_10
- Privacy for agentic AI - <https://www.schneier.com/blog/archives/2025/05/privacy-for-agentic-ai.html> [informative, non-scientific]

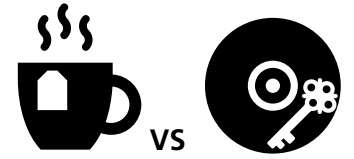
Topic 5: Secure use of AI in Machine Safety

Possible questions to be answered: What is machine safety, and how is it traditionally ensured? In which scenarios can AI support machine safety, and in which is it a risk factor? What are the requirements to use AI in machine safety?

Literature to start from:

- EU Machinery Directive - Old: <https://eur-lex.europa.eu/eli/dir/2006/42/2019-07-26> vs New: <https://eur-lex.europa.eu/eli/reg/2023/1230/oj/eng>
- AI safety for everyone - <https://www.nature.com/articles/s42256-025-01020-y>
- Artificial intelligence in Industry 4.0: Implications for occupational safety and health - <https://www.econstor.eu/bitstream/10419/300311/1/1895160103.pdf>
- Test Criteria Catalogue for AI Systems in Finance - https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Kriterienkatalog_KI-Systeme_Finanzsektor_250603.html

Topic 6: Trusted Execution Environments (TEEs) vs. Disc Encryption



Possible questions to be answered: What is the more-suitable storage protection solution or Secure Execution Environment (SEE) for data at rest/in use/in transit on edge devices? Are TEEs or Disc Encryption more lightweight? What has the greater maturity/use ? Which solution provides better security guarantees? Any known attacks?

Easy Literature (non-scientific):

- Current TEE landscape: <https://next.redhat.com/2019/12/02/current-trusted-execution-environment-landscape/>
- Comparison of Prominent Trusted Execution Environments - <https://elib.uni-stuttgart.de/bitstreams/b01e43e2-bd8b-4d9e-8c2b-bfd75b1f83a8/download>

Literature to start from:

- DITES: A Lightweight and Flexible Dual-Core Isolated Trusted Execution SoC Based on RISC-V - <https://pmc.ncbi.nlm.nih.gov/articles/PMC9416496/>
- A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories - <https://www.mdpi.com/2073-431X/14/2/61>
- Lightweight and High-Performance Data Protection for Edge Network Security - <https://onlinelibrary.wiley.com/doi/10.1155/2022/8458314>
- TEE-PA: TEE Is a Cornerstone for Remote Provenance Auditing on Edge Devices With Semi-TCB - <https://ieeexplore.ieee.org/document/10436677>
- IloTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices - <https://ieeexplore.ieee.org/document/7839870>
- Exploiting Unprotected I/O Operations in AMD's Secure Encrypted Virtualization - https://www.usenix.org/system/files/sec19-li-mengyuan_0.pdf

Topic 7: Remote Attestation for OT

Possible questions to be answered: Which state-of-the-art algorithms and protocols for Remote Attestation (RA) exist nowadays? What are unique constraints and requirements for applying RA in OT environments? How compatible are existing algorithms with OT? Which algorithms fit best in OT? How much adoption is RA showing in OT environments already?

Literature to start from:

- Device attestation: Past, present, and future - <https://doi.org/10.23919/DATE.2018.8342055>
- Remote Attestation: A Literature Review - <http://arxiv.org/abs/2105.02466>
- Introducing Remote Attestation and Hardware-based Cryptography to OPC UA - <https://doi.org/10.1109/ETFA.2017.8247591>
- Remote attestation for low-end embedded devices: the prover's perspective - <https://doi.org/10.1145/2897937.2898083>
- A Taxonomy and Review of Remote Attestation Schemes in Embedded Systems - <https://doi.org/10.1109/ACCESS.2021.3119220>
- Cybersecurity Challenges in Large Industrial IoT Systems - <https://ieeexplore.ieee.org/document/8869162>
- Secure Remote Attestation - <https://eprint.iacr.org/2018/031.pdf>
- Principles of remote attestation - <https://doi.org/10.1007/s10207-011-0124-7>
- A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects - <https://www.sciencedirect.com/science/article/abs/pii/S0167404821003229>

FAQ

FAQ

Do I need to answer all the „possible questions“?

No. They are just an orientational starting point.

Do I need to include all the listed publications in my SoK paper?

No. Not even a single one, if you find better/more interesting/more fitting ones on your topic.

Many listed publications = lots of work?

No. Just lots of hints ;-)

Are the listed publications to be considered conclusively?

No. You are expected to find and read a lot more!

Do I need to read each publication completely?

No. Learn quick-reading to quickly sort out less interesting publications.

How can I access publication xyz or specification abc?

Check the university library tools. University VPN. Main authors webpage.

How to find scientific literature?

Attend a course on scientific writing! References of the listed papers. Google Scholar, ResearchRabbit, and ConnectedPapers

FAQ cont.

Does the 1-to-1 kickoff meeting have to take place until 30.09.2025?

No. The meeting only has to be organized within this period but can take place after the 30.09.2025

Do I have to participate in all presentations?

Yes. To facilitate the discussion, participation is mandatory, and your discussion will be graded. In seminars with many participants, we usually make only one day obligatory.

When should I start working on the seminar?

Right after your topic is assigned to you!

How close to the final paper should my draft paper be?

Content-wise we expect about 2/3 of your final paper

In general, it should be as close as possible – that way you can make the most from the reviewer's feedback and are more relaxed in June/July.

Will the slides be available after the meeting?

Yes! We will upload them to the [chair's website](#) and/or in the TUMonline course description

Is this seminar lots of work?

It depends! For example, on how well you can structure and write. We set high expectations, as all topics come from our own research areas.

Contact

Sebastian N. Peters

Veronique Ehmes

Adrian Reuter

Andy Ludwig

security-seminar@aisec.fraunhofer.de