SEMINAR: CYBER-PHYSICAL SYSTEM SECURITY WS24/25
PRE-COURSE MEETING 09.07.2024

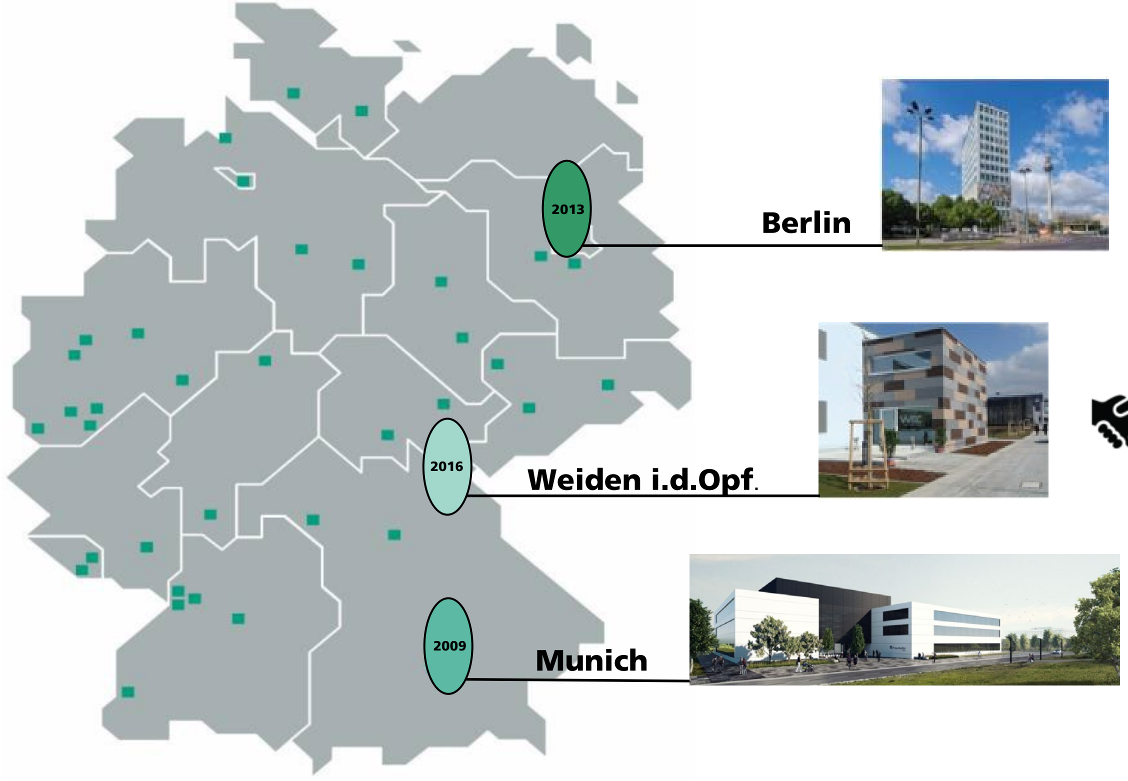
Sebastian Peters, Veronique Ehmes, Adrian Reuter, Nikolai Puch, Lukas Lautenschlager

SEMINAR: CYBER-PHYSICAL SYSTEM SECURITY
PRE-COURSE MEETING

- About Fraunhofer AISEC
- CPS, IT, and OT
- Course Objectives
- Previous knowledge
- Orga
- Process
- Deliverables & Grading
- Paper & Presentation
- Topics
- FAQ

FRAUNHOFER AISEC
KEY FACTS & FIGURES

- Cognitive Security Technologies
- Hardware Security
- Product Protection & Industrial Security
- Service & Application Security
- Secure Operating Systems
- Secure Systems Engineering
- Secure Infrastructure



Freie Universität Berlin

Ostbayerische Technische Hochschule Amberg-Weiden

Technische Universität München

<210 employees

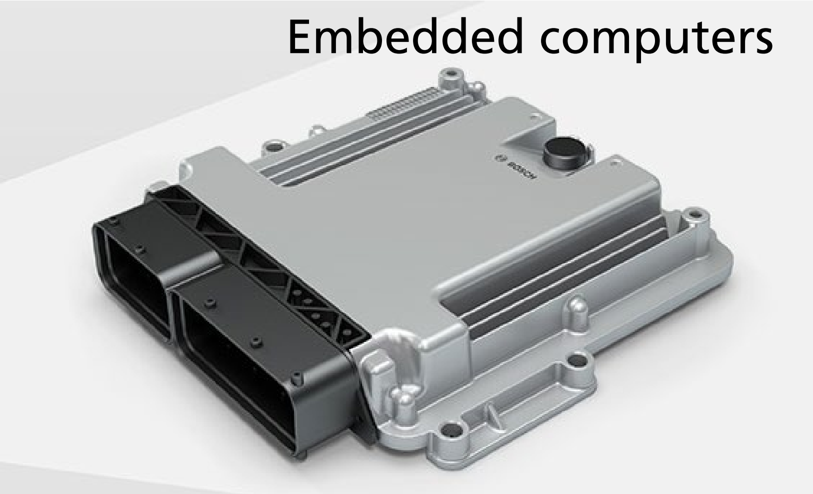
10 Hightech Security Labs

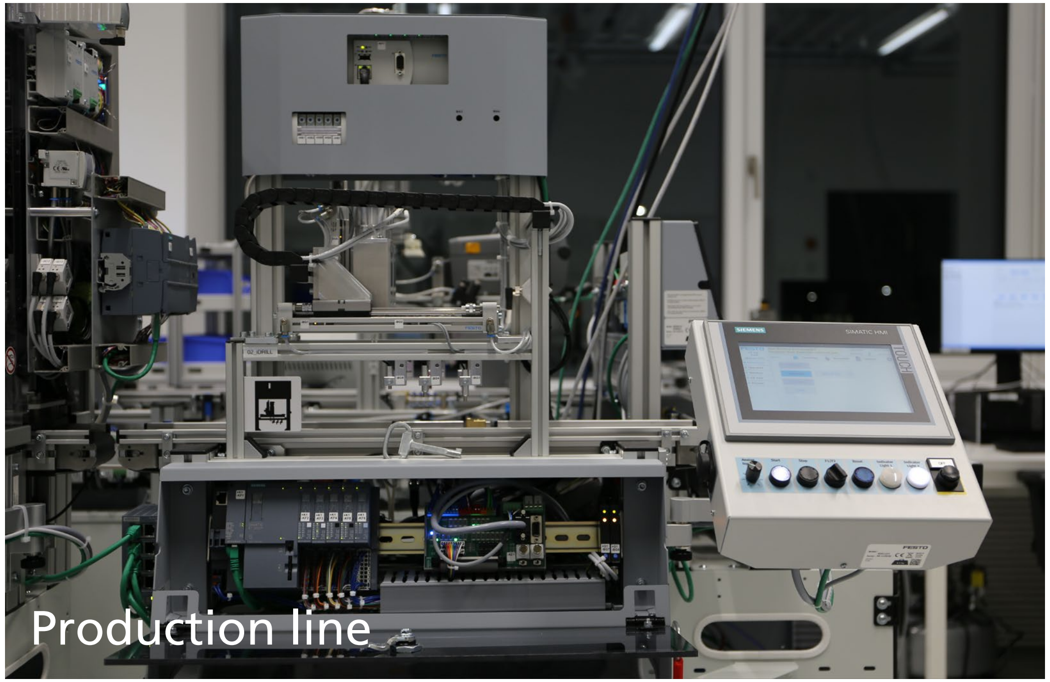
Funding €

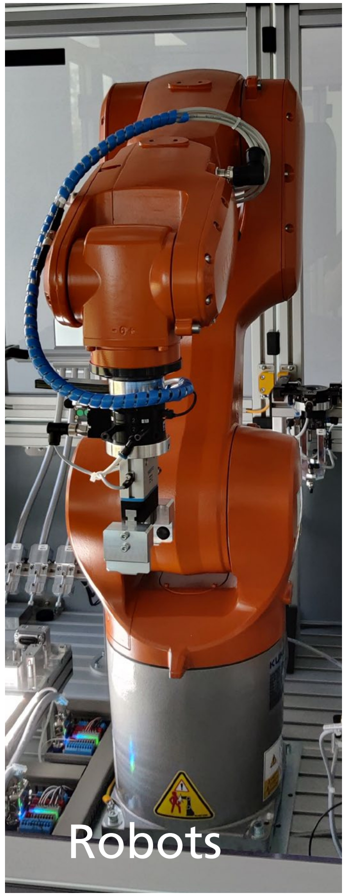
20% State directly

80% 3rd party research projects

What are CPS?


Embedded computers


Production line


Robots

Automotive

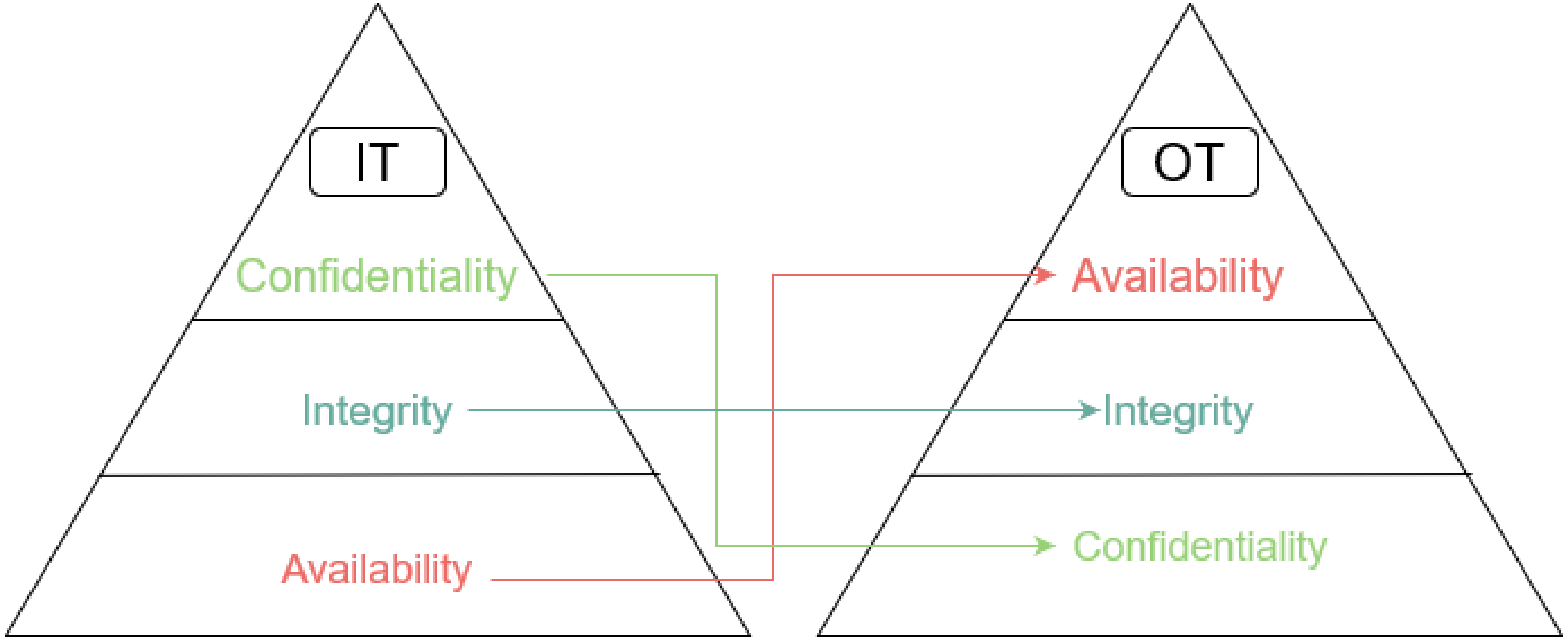
PLCs

IT vs OT differences

Security triad (CIA) upside down (AIC)

most important

least important



Course Objectives

- **Assessing** the state of the art regarding a specific topic in the context of CPS 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?

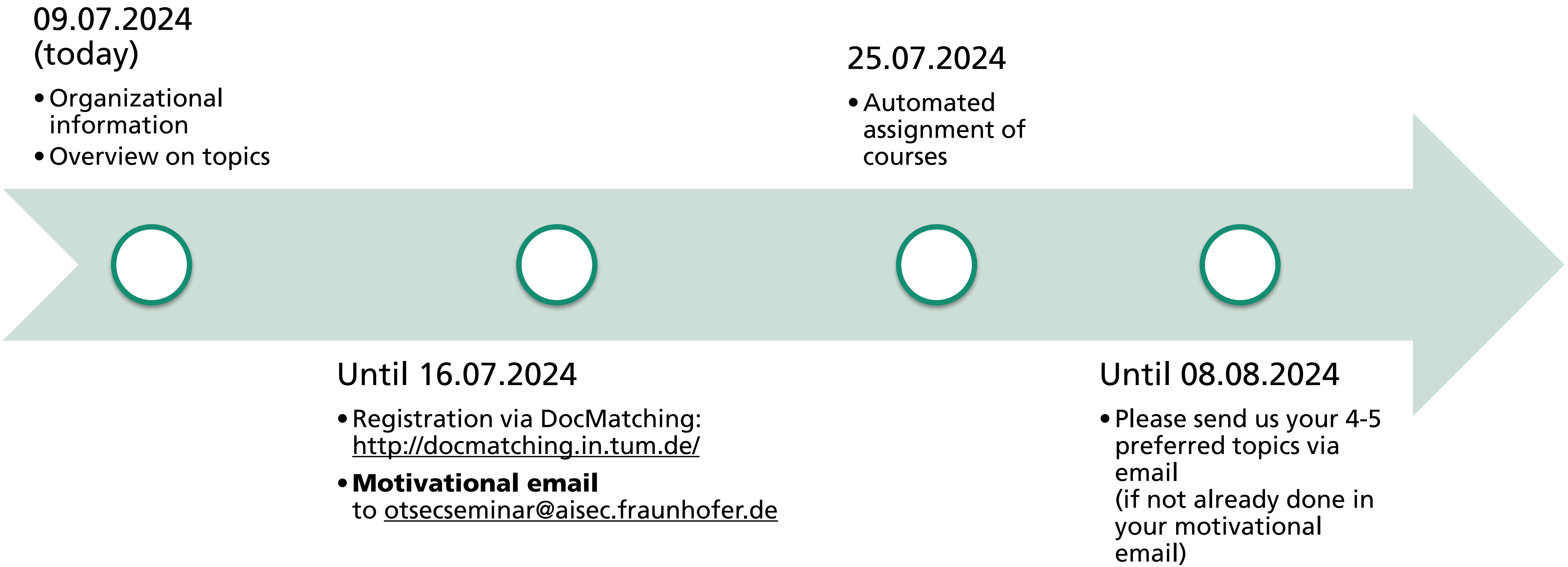
- no formal requirements
- ITsec knowledge necessary!

Spoofing
TLS
encryption
confidentiality
DoS
TCP
certificate
Phishing
Sniffing
SQL-Injection
symmetric-crypto
asymmetric-crypto
usability
TPM
integrity
SHA-3
vulnerability
Honeypot
UDP
DNS
intrusion-detection
security
IIoT
availability
Firewall
VPN
RFID
ECB
IoT
authentication
S/MIME
cryptographic-hash
HTTPS
HMAC
RSA
SMTP
Social-Engineering
PGP
AES

Orga

- Communication
  - TUM Moodle
  - Video Calls via MS Teams
  - E-mail – **always make sure to answer to all of us: Use our list otsecseminar@aisec.fraunhofer.de or use "reply-all". Avoid answering to only one!**
  - Language of instruction and deliverables will be **English**
- Individual work (no groups)
- **Registration** in matching system (http://docmatching.in.tum.de/)
- **Motivational email** to otsecseminar@aisec.fraunhofer.de (about, e.g., your relation to (IT-)security, your 4-5 preferred topics, which topic you like most, and why)

Process (1/4)



09.07.2024
(today)

- Organizational information
- Overview on topics

Until 16.07.2024

- Registration via DocMatching: http://docmatching.in.tum.de/
- **Motivational email** to otsecseminar@aisec.fraunhofer.de

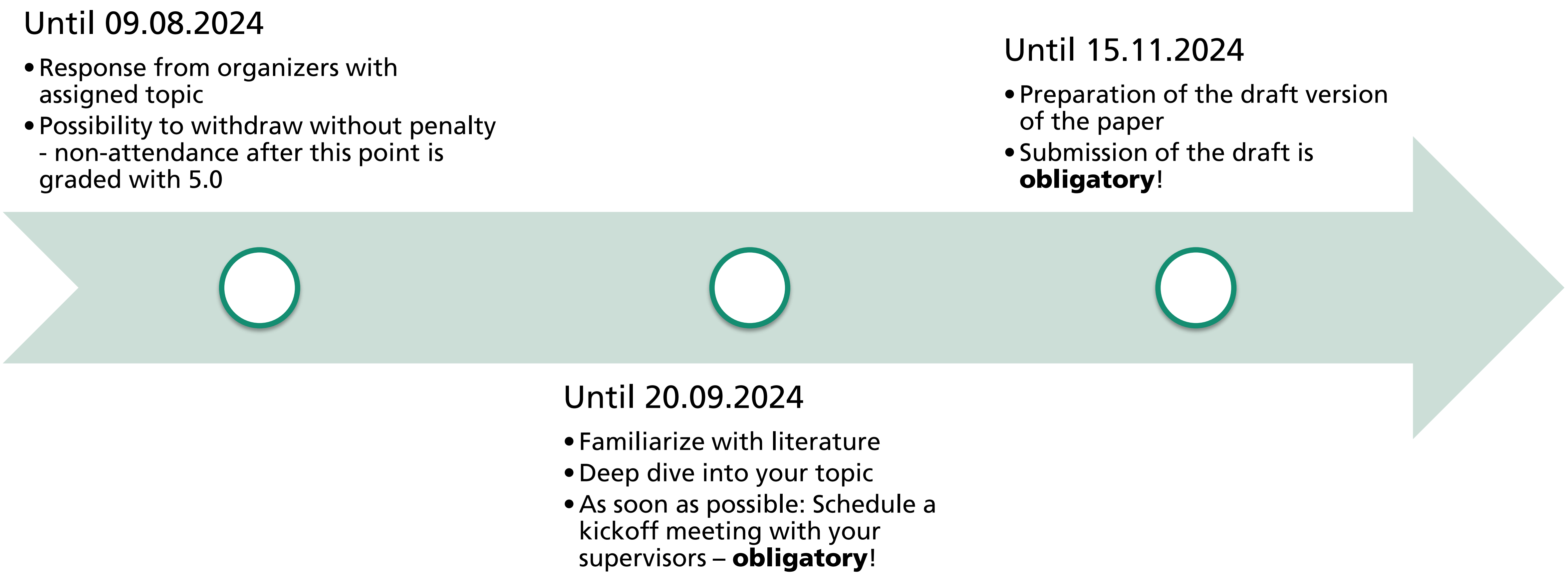
25.07.2024

- Automated assignment of courses

Until 08.08.2024

- Please send us your 4-5 preferred topics via email (if not already done in your motivational email)

Process (2/4)



Until 09.08.2024

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

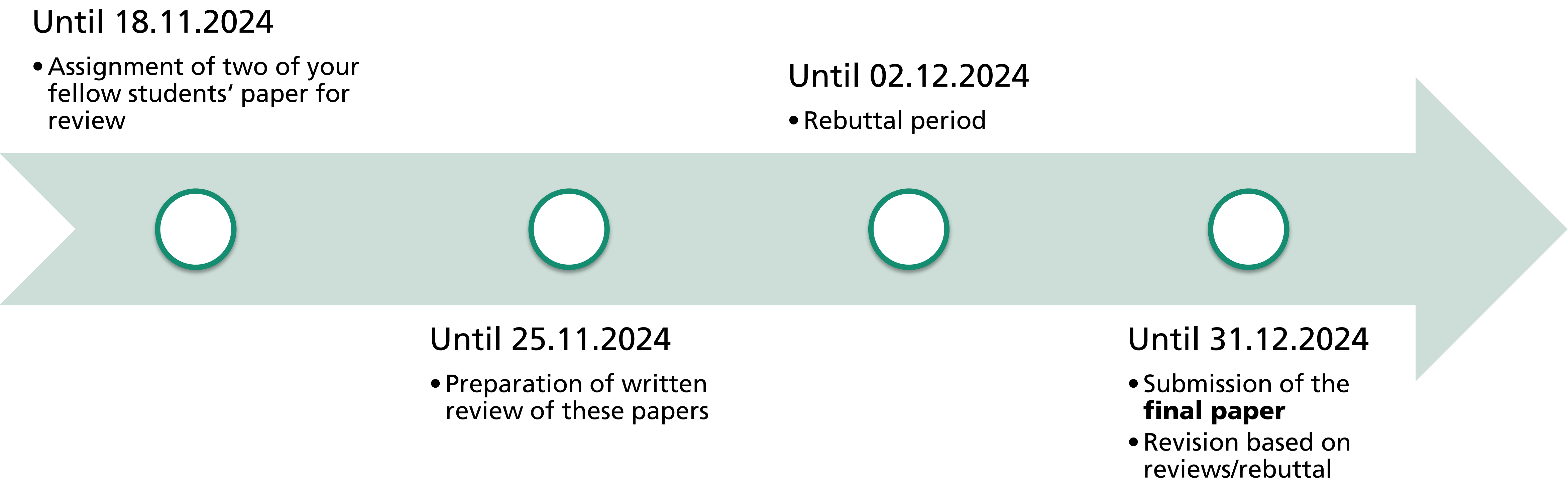
Until 20.09.2024

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

Until 15.11.2024

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

Process (3/4)



Until 18.11.2024

- Assignment of two of your fellow students‘ paper for review

Until 25.11.2024

- Preparation of written review of these papers

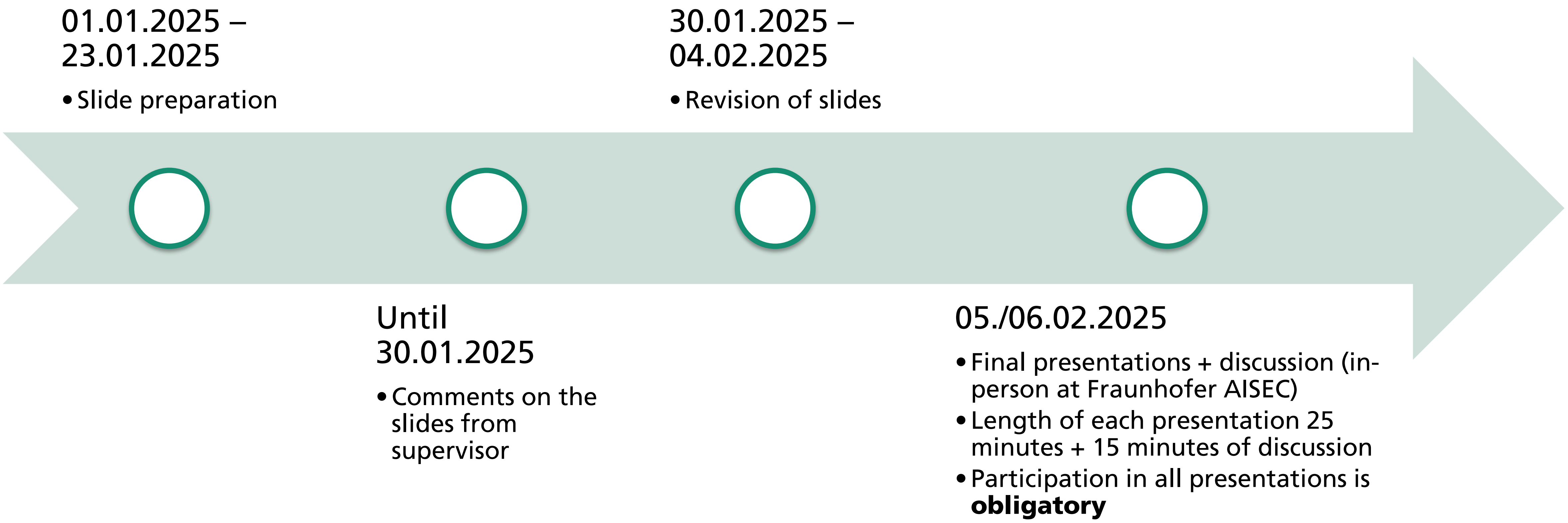
Until 02.12.2024

- Rebuttal period

Until 31.12.2024

- Submission of the **final paper**
- Revision based on reviews/rebuttal

Process (4/4)



01.01.2025 – 23.01.2025

- Slide preparation

Until 30.01.2025

- Comments on the slides from supervisor

30.01.2025 – 04.02.2025

- Revision of slides

05./06.02.2025

- Final presentations + discussion (in-person at Fraunhofer AISEC)
- Length of each presentation 25 minutes + 15 minutes of discussion
- Participation in all presentations is **obligatory**

Deadlines for Obligatory Deliverables

	Due to	Grading
Schedule 1-to-1 Kick-Off Meeting with supervisors	20.09.2024	Obligatory
Submission of Draft Paper	15.11.2024	10%
Reviews	25.11.2024	5%
Rebuttal	02.12.2024	Obligatory
Submission of Final Paper	31.12.2024	50%
Presentation	05./06.02.2025	30%
Presentation Discussion	05./06.02.2025	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), e.g., via TUM ShareLaTeX
  - Note the *Scientific writing guide* in the Moodle course
- Presentation
  - MS Powerpoint or similar
  - 25 minutes presentation
  - 15 minutes discussion - moderated by you

Topics (Overview)

1. GNSS Authenticity
2. Industrial applicability of Messaging Layer Security (MLS)
3. Secure Bootstrapping in OT
4. Video Streaming Security
5. An Analysis of Dumb Password Policies and the Why
6. Authentication Method Obstacles
7. Light-weight authenticity schemes
8. Secure Logging in industrial applications
9. QUIC Security
10. Exploring NFV for Industrial Security Applications
11. Integrating security in the data plane - Using P4 for secure communication
12. Security metrics and empirical validation schemes
13. Early Works of Cryptographic Pairings
14. Federated Learning for IoT and IIoT
15. Peer-to-Peer Protocols
16. Mixnets vs Tor
17. Trust Value Scoring
18. (in)security of PROFINET in practice
19. Host-Intrusion Detection Systems
20. Steganography in 3D Printing
21. Continuous authentication in IIoT

Topic 1: GNSS Authenticity

Possible questions to be answered: What is the situation with NAVSTAR GPS, Galileo, GLONASS, BeiDou, IRNSS, QZSS in terms of spoofing security and authenticity? What methods are there to protect the integrity and authenticity of the messages? Did this lead to Galileo's OSNMA? Are there even better methods to protect authenticity?

Literature:

- Authenticating GNSS civilian signals: a survey - https://link.springer.com/article/10.1186/s43020-023-00094-6
- Authentication of Galileo GNSS Signal by Superimposed Signature with Artificial Noise - https://ieeexplore.ieee.org/abstract/document/8553467
- On Mixing Authenticated and Non-Authenticated Signals Against GNSS Spoofing - https://ieeexplore.ieee.org/abstract/document/10478578
- Galileo Authentication: A Programme and Policy Perspective - https://www.researchgate.net/publication/328139227_Galileo_Authentication_A_Programme_and_Policy_Perspective
- Galileo OSNMA Public Observation Phase: Signal Testing and Validation - https://ieeexplore.ieee.org/abstract/document/9729708
- Enhanced GNSS Authentication Based on the Joint CHIMERA/OSNMA Scheme - https://ieeexplore.ieee.org/abstract/document/9522141

Topic 2: Industrial applicability of Messaging Layer Security (MLS)

Possible questions to be answered: What industrial application scenarios exist for the new Messaging Layer Security (MLS) protocol? Could parts of the protocol be used to solve industrial problems? How about in decentralised scenarios?

Literature:

- The Messaging Layer Security (MLS) Protocol - https://datatracker.ietf.org/doc/rfc9420/
- TreeSync: Authenticated Group Management for Messaging Layer Security - https://eprint.iacr.org/2022/1732.pdf
- TreeKEM: Asynchronous Decentralized Key Management for Large Dynamic Groups - https://inria.hal.science/hal-02425247/file/treekem+%281%29.pdf
- Multi-Device Security Application for Unmanned Surface and Aerial Systems - https://www.mdpi.com/2504-446X/8/5/200
- Utilizing the Messaging Layer Security Protocol in a Lossy Communications Aerial Swarm (careful: only masters thesis) - https://apps.dtic.mil/sti/citations/trecms/AD1173274
- Use of Messaging Layer Security in a Military UAV Swarm (careful: only masters thesis) - https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3118795

Topic 3: Secure Bootstrapping in CPS

Possible questions to be answered: Which algorithms exist for secure bootstrapping? How do they compare in detail? Which features do they have in common, which ones does a protocol have exclusively, which ones should they have? What are their different target groups/applications? Are there solutions based on symmetric crypto (for usage on constrained devices)?

Literature:

- NIST Special Publication (SP) 1800-36, https://csrc.nist.gov/pubs/sp/1800/36/ipd
- ACME - https://datatracker.ietf.org/doc/html/rfc8555
- BRSKI-AE - https://datatracker.ietf.org/doc/draft-ietf-anima-brski-ae/
- BRSKI-PRM - https://datatracker.ietf.org/doc/draft-ietf-anima-brski-prm/
- Secure Bootstrapping for Internet of Things (Dissertation, parts of Chapter 2 interesting) - https://www.theses.fr/2022IPPAT023.pdf
- Secure IoT Bootstrapping: A Survey - https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-secure-bootstrapping-00
- cBRSKI - https://www.ietf.org/id/draft-ietf-anima-constrained-voucher-24.html

Topic 4: Video Streaming Security

Possible questions to be answered: Which security measures are in place to ensure confidentiality, integrity and/or authenticity of video streams? What do large movie streaming companies (e.g. Netflix) do, compared to video streaming in industrial applications? How can video data be saved with integrity protection?

Literature to start from:

- A Lightweight Protocol for Secure Video Streaming - https://www.mdpi.com/1424-8220/18/5/1554
- Blockchain-based video forensics and integrity verification framework for wireless Internet-of-Things devices https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.143
- Cache-Enabled Physical Layer Security for Video Streaming in Backhaul-Limited Cellular Networks https://ieeexplore.ieee.org/abstract/document/8103927
- I know what you streamed last night: On the security and privacy of streaming https://www.researchgate.net/publication/323942067_I_know_what_you_streamed_last_night_On_the_security_and_privacy_of_streaming
- Steal This Movie: Automatically Bypassing DRM Protection in Streaming Media Services https://sefcom.asu.edu/publications/steal-this-movie-automatically-bypassing-drm-protection-usenix2013.pdf
- Beauty and the Burst: Remote Identification of Encrypted Video Streams https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/schuster

Topic 5: An Analysis of Dumb Password Policies and the Why

An analysis of the most common stupidities in password policies and the why! Actually, we all know what's best (if it has to be passwords at all): long random passwords + password manager. So why are there always (in the best case) strange policies? E.g. "no double letters" or "max. 12 characters".

Possible questions to be answered: What categories of stupid rules exist? Which are more/less commonly seen? Which are the most dangerous? What could drive responsibles to do this? Psychological effects?

Literature:

- Source for dumb password policies – non-scientific: https://dumbpasswordrules.com/sites/
- Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies - https://www.usenix.org/conference/soups2021/presentation/gerlitz
- Do Differences in Password Policies Prevent Password Reuse? - https://dl.acm.org/doi/abs/10.1145/3027063.3053100
- Password policies of most top websites fail to follow best practices - https://www.usenix.org/conference/soups2022/presentation/lee

Topic 6: Authentication Method Obstacles

Possible questions to be answered: What obstacles prevent the integration of authentication procedures? Which authentication methods are particularly affected? Can these obstacles be categorised and structured?

Literature:

- Computing and Authentication Practices in Global Oil and Gas Fields - https://arxiv.org/pdf/2108.02660.pdf
- Multifactor Authentication Protocol in a Mobile Environment - https://ieeexplore.ieee.org/abstract/document/8879478
- Why Aren’t We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication - https://www.usenix.org/system/files/sec24summer-prepub-618-lassak.pdf

Topic 7: Light-weight authenticity schemes in resource-constrained environments

Possible questions to be answered: Which types of light-weight authenticity schemes do exist (e.g. progressive, truncated, aggregated)? Which advantages and disadvantages do those schemes have? How is the security of those methods evaluated? Are there known attacks against existing light-weight authenticity schemes?

Literature:

- ProMACs: Progressive and Resynchronizing MACs for Continuous Efficient Authentication of Message Streams https://dl.acm.org/doi/pdf/10.1145/3372297.3423349
- BP-MAC: Fast Authentication for Short Messages - https://dl.acm.org/doi/abs/10.1145/3507657.3528554
- Take a Bite of the Reality Sandwich: Revisiting the Security of Progressive Message Authentication Codes - https://arxiv.org/abs/2103.08560
- Lightweight Authentication Methods in IoT: Survey: https://ieeexplore.ieee.org/document/9759798
- A Survey of Cryptographic Algorithms for Lightweight Authentication Schemes in the Internet of Things Environment: https://ieeexplore.ieee.org/document/9970015
- ISO/IEC 29192

Topic 8: Secure Logging in industrial applications

Possible questions to be answered: What solutions are there for secure logging in industrial applications? Which requirements are specific to industry/OT/IIoT? Which IT solutions can be used? What are their respective advantages and disadvantages? What would an ideal solution look like?

Literature:

- A Secure Event Logging System for Smart Homes - https://dl.acm.org/doi/abs/10.1145/3139937.3139945
- LogSafe: Secure and Scalable Data Logger for IoT Devices - https://ieeexplore.ieee.org/abstract/document/8366984
- Facilitate Security Event Monitoring and Logging of Operational Technology (OT) Legacy Systems - https://link.springer.com/chapter/10.1007/978-3-030-98741-1_38

Topic 9: QUIC Security

Possible questions to be answered: Which QUIC security recommendations, compared to the ones mentioned in the RFC exist? Are there attacks exploting weaknesses of the protocol? Are there known attacks on the protocol, which can be transferred into security considerations?

Literature to start from:

- A Quic(k) Security Overview: A Literature Research on Implemented Security Recommendations - https://arxiv.org/abs/2306.17568
- QUIC RFC - https://datatracker.ietf.org/doc/rfc9000/
- Revisiting QUIC attacks: a comprehensive review on QUIC security and a hands-on study - https://link.springer.com/article/10.1007/s10207-022-00630-6

Github:

- QUIC attacks: **https://github.com/efchatz/QUIC-attacks**

Topic 10: Exploring NFV for Industrial Security Applications

Possible questions to be answered: What is Network Function Virtualization and why is it of interest for security research? Which virtualized network functions are already implemented in the context of network security? Are there performance differences between virtualized and regular network functions? With focus on the industrial context are the existing VNFs already implemented and in use?

Literature to start from:

- IoT focused survey on security applications via NFV: https://ieeexplore.ieee.org/document/8424018
- Firewall, IDS implementation in the form of VNF: https://ieeexplore.ieee.org/document/9875076
- Automated Access control as VNF: https://ieeexplore.ieee.org/document/8264894

Topic 11: Integrating security in the data plane - Using P4 for secure communication

Possible questions to be answered: What is P4 and why is it of interest for security research? Which security controls are already realized using P4? Which security control groups are suitable for an implementation on the data plane? Are there missing security control groups, with special focus on the automotive or industrial sector, not realized using P4?

Literature to start from:

- P4 ICMPv6 DoS Protection: https://ieeexplore.ieee.org/document/9839137
- Dynamic firewall + dynamic port knocking in P4: https://ieeexplore.ieee.org/document/9937010
- Stateful firewall in P4: https://ieeexplore.ieee.org/document/9123046
- Authentication and Access control in P4: https://ieeexplore.ieee.org/document/9943765
- Survey P4 security applications: https://ieeexplore.ieee.org/document/10375491

Topic 12: Security metrics and empirical validation schemes

Possible questions to be answered: What are security metrics? Which security metrics do exist? What empirical methods are described to evaluate security metrics in systems? Are the empirical security metrics also applicable to the CPS environment? Which problems are showing by empirically evaluating the security of systems? Which problems do metrics impose onto the measured property?

Literature to start from:

- Quantitative Security Metrics: Unattainable Holy Grail or a Vital Breakthrough within Our Reach? https://ieeexplore.ieee.org/document/6798561/citations?tabFilter=papers#citations
- A Survey on Systems Security Metrics: https://dl.acm.org/doi/10.1145/3005714

Topic 13: Early Works of Cryptographic Pairings and their Application

Possible questions to be answered: What are cryptographic pairings? How are they defined? When were pairings introduced, and how did they evolve to lead to today’s application scenarios? What are groups with bilinear maps? How are they used for anonymous credential systems (zero-knowledge proofs), group signatures, and encryption (attribute-based encryption, somewhat homomorphic encryption)?

Literature to start from:

- Miller 1986: Short Programs for functions on Curves - https://crypto.stanford.edu/miller/miller.pdf
- A. Menezes 1993: Reducing elliptic curve logarithms to logarithms in a finite field - https://ieeexplore.ieee.org/document/259647
- A. Joux 2000: A One Round Protocol for Tripartite Diffie-Hellman - https://link.springer.com/chapter/10.1007/10722028_23
- Sakai, Ohgishi, Kasahara 2000: Provably secure non-interactive key distribution based on pairings - https://www.sciencedirect.com/science/article/pii/S0166218X05002337
- Boneh, Frankllin 2001: Identity-Based Encryption from the Weil Pairing - https://dl.acm.org/doi/10.5555/646766.704155
- Berlin, Heidelberg 2004: Signature Schemes and Anonymous Credentials from Bilinear Maps - http://link.springer.com/10.1007/978-3-540-28628-8_4

Topic 14: Federated Learning for IoT and IIoT

Possible questions to be answered: What is federated learning (FL)? Which problems can FL models solve? How can federated learning be used to secure the confidentiality of sensor data? How mature is federated learning and the respective Federated Optimization algorithms? Is it possible to reconstruct confidential information from models trained with Federated Learning?

Literature to start from:

- Federated Learning Based Privacy Ensured Sensor Communication in IoT Networks: A Taxonomy, Threats and Attacks - https://ieeexplore.ieee.org/document/10107624
- Federated Learning-Based Privacy-Preserving Data Aggregation Scheme for IIoT -https://ieeexplore.ieee.org/document/9968228
- A Review of Privacy-Preserving Federated Learning, Deep Learning, and Machine Learning IIoT and IoTs Solutions - https://ieeexplore.ieee.org/document/10270935
- Federated Learning for Internet of Things: Recent Advances, Taxonomy, and Open Challenges - https://ieeexplore.ieee.org/document/9460016
- Survey on federated learning threats: Concepts, taxonomy on attacks and defences, experimental study and challenges - https://arxiv.org/abs/2201.08135
- A survey on security and privacy of federated learning - https://www.sciencedirect.com/science/article/abs/pii/S0167739X20329848
- How To Backdoor Federated Learning - https://proceedings.mlr.press/v108/

Topic 15: P2P Protocols: libp2p and devp2p based networks

Possible questions to be answered: How are Peer-to-peer (P2P) networks designed? What is the underlying technique of decentralized P2P protocols like IPFS, PubSub, and GossipSub? How do they function? What are future use cases like privacy preserving networks and anonymized networks?

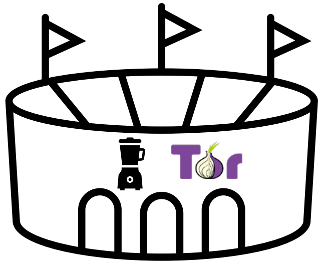
Literature to start from:

- Crawling the IPFS Network - https://ieeexplore.ieee.org/document/9142764
- S/Kademlia: A practicable approach towards secure key-based routing - https://ieeexplore.ieee.org/document/4447808
- Design and evaluation of ipfs: A storage layer for the decentralizedweb - https://dl-acm-org.eaccess.tum.edu/doi/10.1145/3544216.3544232
- Decentralized Hole Punching - https://ieeexplore-ieee-org.eaccess.tum.edu/document/9951368
- Pubsub: An efficient publish/subscribe system - https://ieeexplore-ieee-org.eaccess.tum.edu/document/6782663
- Privacy-Preserving Spam-Protected Gossip-Based Routing - https://ieeexplore-ieee-org.eaccess.tum.edu/document/9912176

Some non-scientific material for your lunch break:

- https://www.youtube.com/watch?v=BUc4xta7Mfk
- https://www.youtube.com/watch?v=oIMZP7sfFtM

Topic 16: Mixnets vs Tor: Which is the better anonymity network?

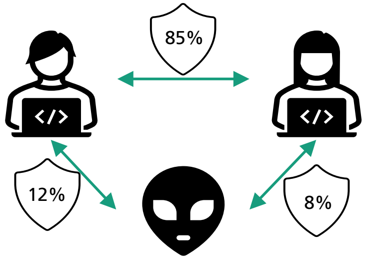


Possible questions to be answered: What are Mixnets? What is Tor? How were they created, and who invented them? How do they hide metadata for private communication? What are the known strengths, weaknesses, and attacks of both networks? What does current research say about them, and what is the level of anonymity they grant?

Literature to start from:

- Low-Cost Traffic Analysis of Tor - 10.1109/SP.2005.12
- How Secure Are The Main Real-World Mix Networks - 10.1145/3579856.3595785
- Untraceable electronic mail, return addresses, and digital pseudonyms - https://dl.acm.org/doi/10.1145/358549.358563
- The Loopix Anonymity System - https://arxiv.org/abs/1703.00536
- Two Cents for Strong Anonymity: The Anonymous Post-office Protocol - https://link.springer.com/chapter/10.1007/978-3-030-02641-7_18
- Generalising Mixes - https://link.springer.com/chapter/10.1007/978-3-540-40956-4_2
- A Systematic Survey On Security in Anonymity Networks: Vulnerabilities, Attacks, Defenses, and Formalization - https://ieeexplore.ieee.org/document/10380756
- Sphinx: A Compact and Provably Secure Mix Format - https://ieeexplore.ieee.org/document/5207650
- Stadium: A Distributed Metadata-Private Messaging System - https://dl-acm-org.eaccess.tum.edu/doi/10.1145/3132747.3132783

Topic 17: Trust Value Scoring between Peers



Possible questions to be answered: How are trust and reputation defined? What approaches are used to derive a computational trust score from parameters like the quality and quantity of data, like cyber threat intelligence data a peer distributes, as well as the connectedness and reputation of a peer in a network? How can anonymity still be achieved in an environment where trust is paramount?

Literature to start from:

- A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources - https://dl.acm.org/doi/10.1145/3339252.3342112
- A topological potential weighted community-based recommendation trust model for P2P networks - http://link.springer.com/10.1007/s12083-014-0288-9
- Trust and Reliance in Multi-Agent Systems: A Preliminary Report - https://www.researchgate.net/publication/2269307
- Survey on Computational Trust and Reputation Models - https://dl.acm.org/doi/10.1145/3236008
- Trust and Quality Computation for Cyber Threat Intelligence Sharing Platforms - https://doi.org/10.1109/CSR51186.2021.9527975
- A Novel Trust Taxonomy for Shared Cyber Threat Intelligence - https://doi.org/10.1155/2018/9634507
- Anonymity vs. Trust in Cyber-Security Collaboration - https://doi.org/10.1145/2808128.2808134
- A survey of attack and defense techniques for reputation systems - https://doi.org/10.1145/1592451.1592452

Topic 18: (In)Security of PROFINET in Practice

Possible questions to be answered: How do the protocols of the PROFINET family differ (RT, IRT, over TSN, PROFIsafe, PROFINET IO, …)? Are there any practical attacks on the different PROFINET protocols? Are there reasonable countermeasures and are they relevant in practice?

Literature to start from:

- https://www.profibus.com/technologies/profinet
- https://profinetuniversity.com/
- Exploring Security in PROFINET IO
  https://doi.org/10.1109/COMPSAC.2009.61
- Exploring Network Security in PROFIsafe
  https://doi.org/10.1007/978-3-642-04468-7
- A Fully-Blind False Data Injection on PROFINET I/O Systems
  https://doi.org/10.1109/ISIE45552.2021.9576496
- PI White Paper: Security Extensions for PROFINET
  https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet

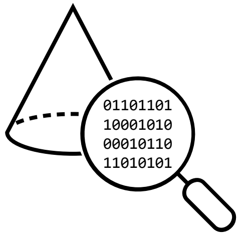
Topic 19: Host-based Intrusion Detection Systems

Possible questions to be answered: What is a Host Intrusion Detection System? Which different types of host intrusion detection systems do exist? In the case of the anomaly-based method, which data is used to train the model? Which different types of attacks are already labeled for supervised learning? What kinds of ML models are used to detect attacks in hosts? What existing models exist for supervised, semi-supervised, and unsupervised learning?

Literature to start from:

- Survey for HIDS: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10439152
- Using Syscalls to detect intrusions in hosts https://ieeexplore.ieee.org/document/7824846
- Ensemble method https://ieeexplore.ieee.org/document/10435091
- A dataset generator for next generation system call host intrusion detection systems: https://ieeexplore.ieee.org/document/8170835
- Survey of intrusion detection systems: techniques, datasets and challenges: https://doi.org/10.1186/s42400-019-0038-7

Topic 20: Steganography in 3D Printing



Possible questions to be answered: What are the different goals/purposes of steganography in 3D Printing? How does steganography work in 3D Printing? What countermeasures exist against unwanted steganography attacks?

Literature to start from:

- Crypto-Steganographic Validity for Additive Manufacturing (3D Printing) Design Files
  https://doi.org/10.1007/978-3-031-22390-7_3
- What Did You Add to My Additive Manufacturing Data?: Steganographic Attacks on 3D Printing Files
  https://doi.org/10.1145/3471621.3471843
- Information Hiding Using 3D-Printing Technology - https://doi.org/10.1109/IDAACS.2019.8924352
- Stop Stealing My Data: Sanitizing Stego Channels in 3D Printing Design Files
  https://doi.org/10.48550/arXiv.2404.05106

Topic 21: Continuous authentication in IIoT

Possible questions to be answered: How can continuous authentication be applied to IIoT scenarios? How do scenarios / solutions / utilized technologies differ? What are pros and cons?

Literature to start from:

- Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective https://doi.org/10.1109/JIOT.2020.3004077
- RFID-assisted Continuous User Authentication for IoT-based Smart Farming https://doi.org/10.1109/RFID-TA.2019.8892140
- On the Applicability of Users' Operation-action Characteristics for the Continuous Authentication in IIoT Scenarios https://doi.org/10.1109/NaNA51271.2020.00029
- Passive User Authentication Utilizing Behavioral Biometrics for IIoT Systems https://doi.org/10.1109/JIOT.2021.3138454
- On the Applicability of Multi-Characteristics for the Continuous Authentication in IIoT Scenarios https://doi.org/10.1109/NaNA53684.2021.00041
- Access Control in Critical Infrastructure Control Rooms using Continuous Authentication and Face Recognition (Masters Thesis) - http://hdl.handle.net/11250/2502564

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 20.09.2024?
  - *No. The meeting only has to be organized within this period but can take place after the 20.09.2024*
- Do I have to participate in all presentations?
  - Yes. To facilitate the discussion participation is mandatory and your discussion will be graded.
- 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?
  - As close as possible – that way you can make the most from the reviewer's feedback and are more relaxed in December.
- Will the slides be available after the meeting?
  - Yes! We will upload them to the chair's website: https://www.sec.in.tum.de/i20/teaching

Thanks for your attention. Open questions?

Sebastian N. Peters, Veronique Ehmes, Adrian Reuter, Nikolai Puch, and Lukas Lautenschlager

Department Product Protection & Industrial Security

Fraunhofer Institute for Applied and Integrated Security AISEC

otsecseminar@aisec.fraunhofer.de

Address: Fraunhofer AISEC
Lichtenbergstr. 11
85748 Garching
Germany

Internet: www.aisec.fraunhofer.de

Fraunhofer
AISEC