SEMINAR: CYBER-PHYSICAL SYSTEM SECURITY SS24
PRE-COURSE MEETING 06.02.2024

Sebastian Peters, Veronique Ehmes, Adrian Reuter, Nikolai Puch

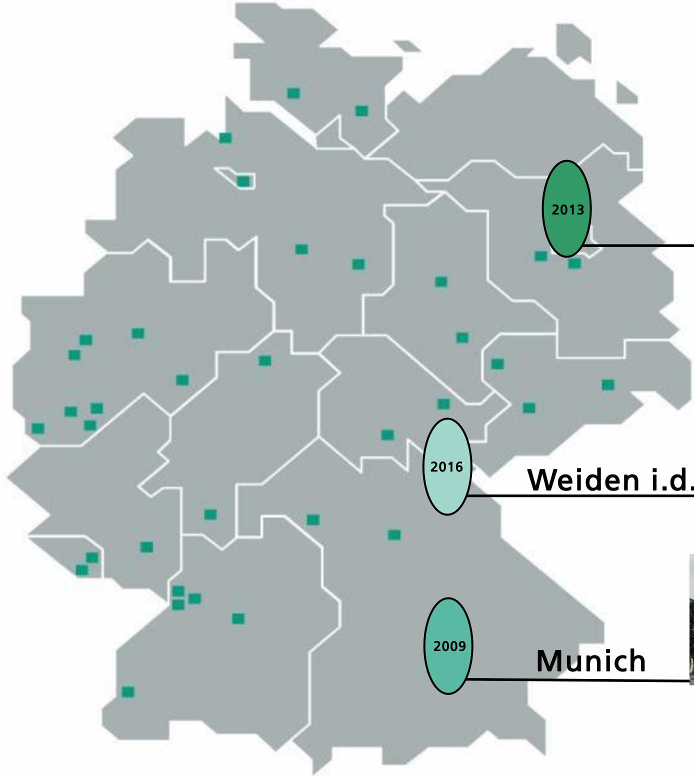
SEMINAR: CYBER-PHYSICAL SYSTEM SECURITY PRE-COURSE MEETING

- 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



Berlin

Freie Universität Berlin

Weiden i.d.Opf.

Ostbayerische Technische Hochschule Amberg-Weiden

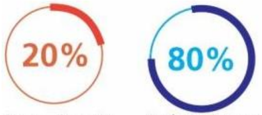
Munich

Technische Universität München

<210 employees

10 Hightech Security Labs

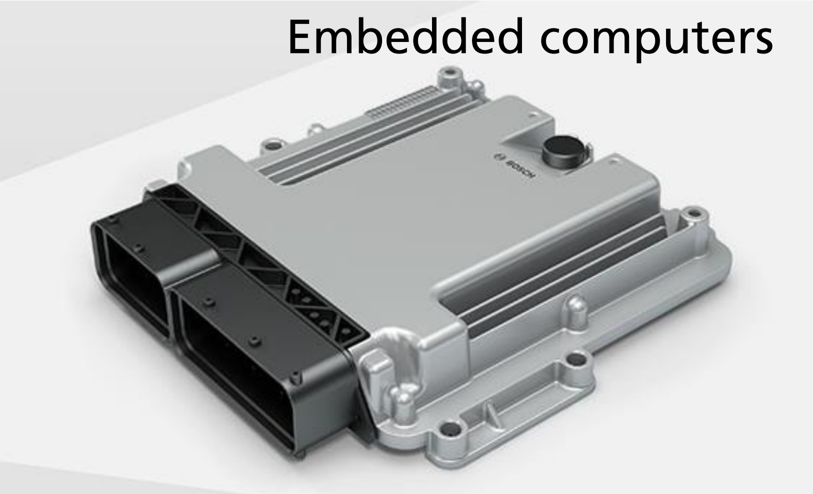
Funding €

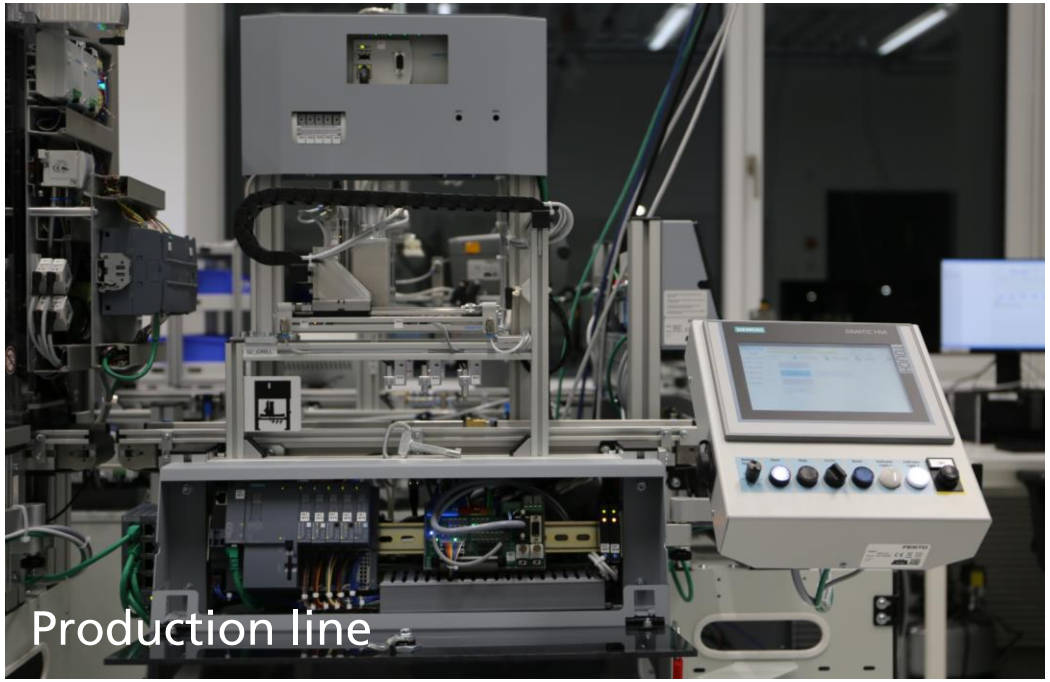


State directly

3rd party research projects

What are CPS?


Embedded computers


Production line

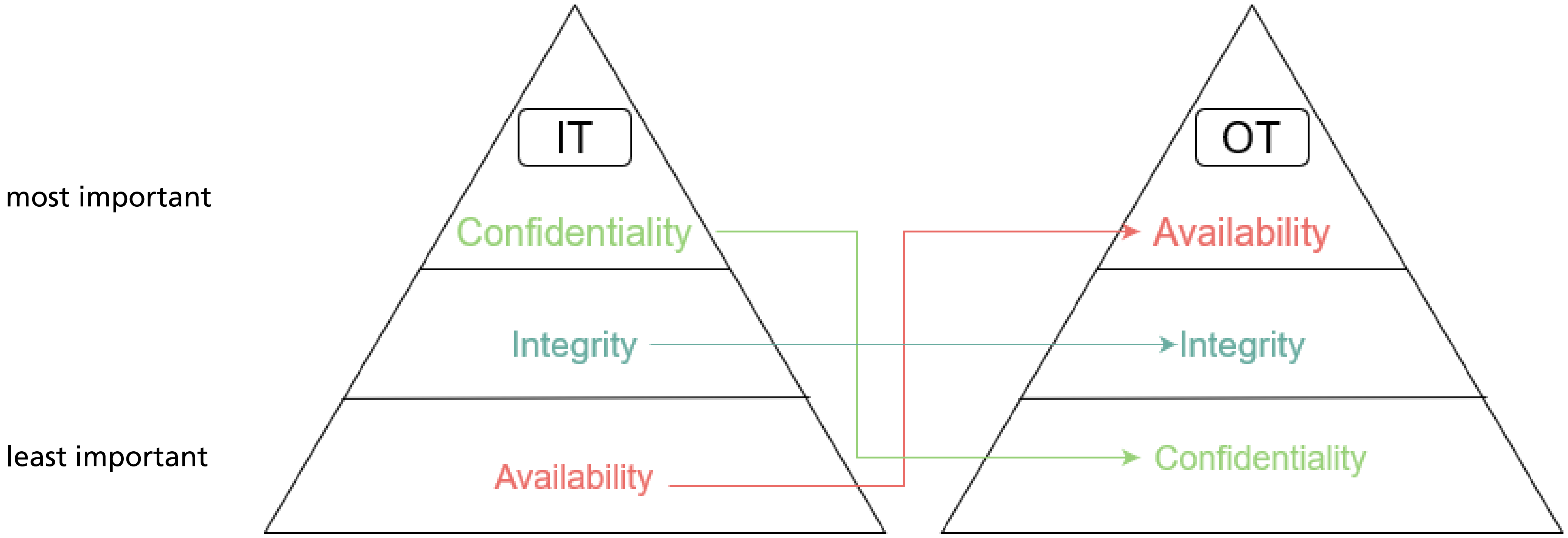
Robots

Automotive

PLCs

IT vs OT differences

Security triad (CIA) upside down (AIC)



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?

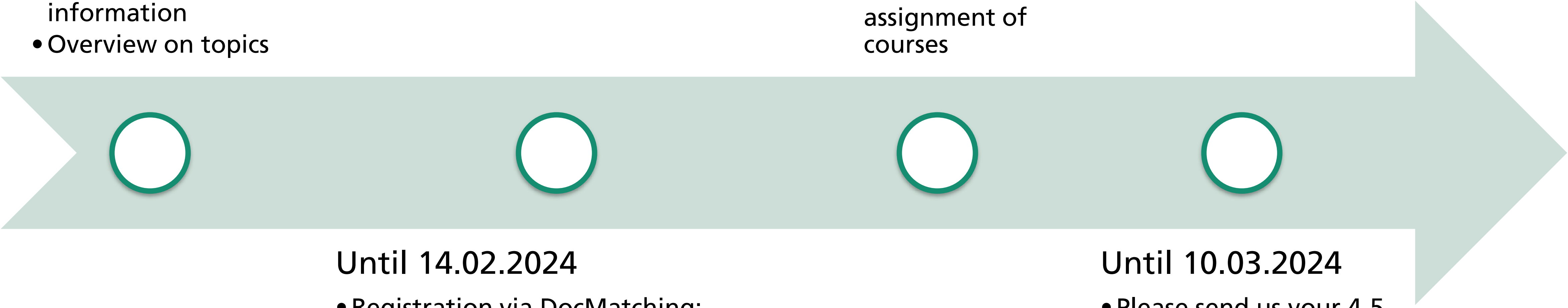
- no formal requirements
- ITsec knowledge necessary!

Spoofing
TLS
encryption
confidentiality
DoS
TCP
certificate
Phishing
Sniffing
TPM
integrity
SQL-Injection
symmetric-crypto
asymmetric-crypto
usability
SHA-3
UDP
Honeypot
vulnerability
DNS
intrusion-detection
availability
security
IIoT
Firewall
IoT
VPN
RFID
ECB
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 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 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)



06.02.2024 (today)

- Organizational information
- Overview on topics

Until 14.02.2024

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

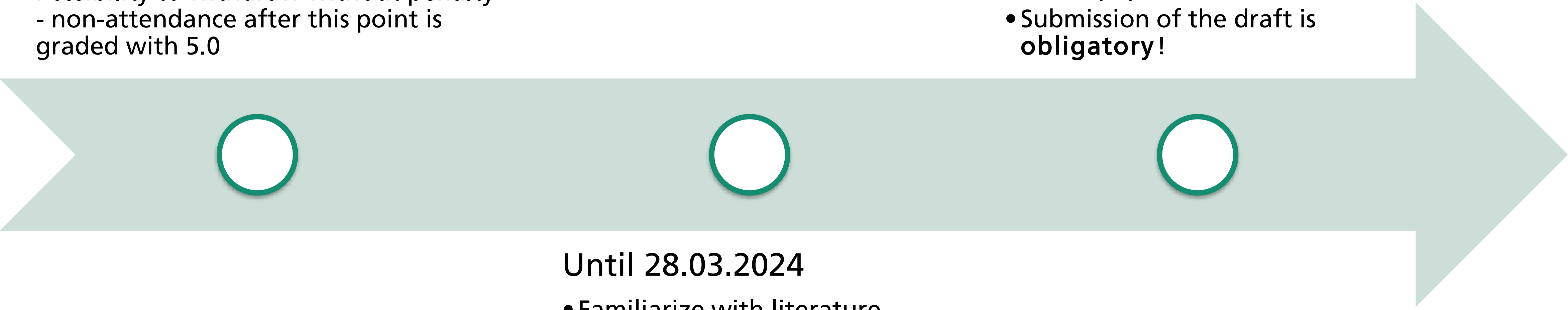
29.02.2024

- Automated assignment of courses

Until 10.03.2024

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

Process (2/4)



Until 13.03.2024

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

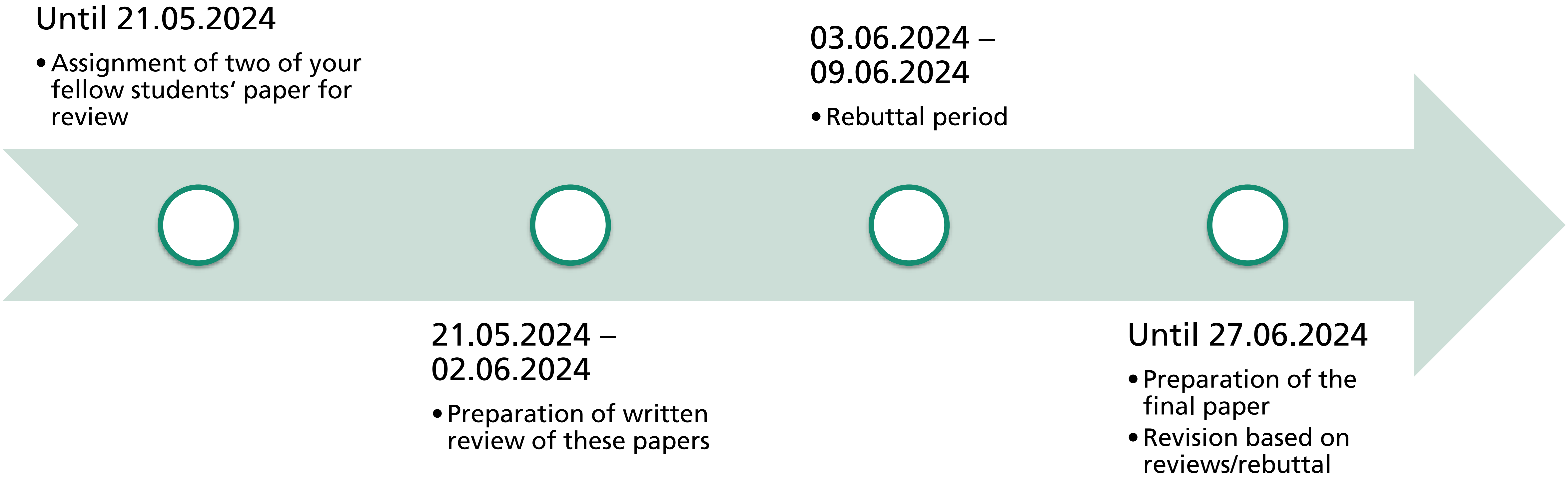
Until 28.03.2024

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

Until 19.05.2024

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

Process (3/4)



Until 21.05.2024

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

21.05.2024 – 02.06.2024

- Preparation of written review of these papers

03.06.2024 – 09.06.2024

- Rebuttal period

Until 27.06.2024

- Preparation of the final paper
- Revision based on reviews/rebuttal

Process (4/4)

Until 04.07.2024

- Slide preparation

Until 11.07.2024

- Comments on the slides from supervisor

12.07.2024 – 17.07.2024

- Revision of slides

15./16.07.2024

- 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	28.03.2024	Obligatory
Submission of Draft Paper	19.05.2024	10%
Reviews	02.06.2024	5%
Rebuttal	09.06.2024	Obligatory
Submission of Final Paper	27.06.2024	50%
Presentation	15./16.07.2024	30%
Presentation Discussion	15./16.07.2024	5%
		Σ 100 %

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

Paper writing and presentation

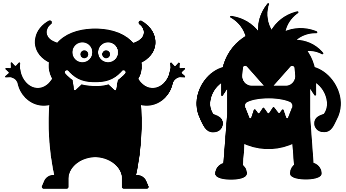
- Paper
  - Systematization of Knowledge (SoK)
  - ~10 pages excl. list of references and appendices
  - IEEE conference proceedings template
  - Utilization of LaTeX (highly recommended)
  - Note the *Scientific writing guide* in the Moodle course
- Presentation
  - MS Powerpoint or similar
  - 25 minutes presentation
  - 15 minutes discussion - moderated by you

Topics (Overview)

1. FrankenCert Lives
2. Deniable Authentication in Cyber-Physical Systems
3. Security of C-ITS and Vehicular Ad-Hoc Networks
4. History of authentication in Cyber-Physical Systems
5. Security of Electronic Data Interchange (EDI)
6. Intrusion Detection Systems for CPS
7. Anomaly Detection for CPS
8. Cyber-Physical-System-Environments and Usability for Authentication
9. Video Streaming Security
10. a) Vulnerability databases and Open-Source Software (OSS) ecosystems

    b) Security Advisories and their role in vulnerability information and software ecosystems
11. Forensic of autonomous vehicles
12. Automotive Authentication
13. Selection of Privacy-Enhancing Technologies
14. Continuous Authentication in IoT and IIoT
15. Attribute based encryption of data in a P2P networks
16. Federated Learning for CPS
17. Authentication Token Security Perception
18. Secure PLC Programming
19. Secure Bootstrapping
20. Objectives, concepts and development status of the Asset Administration Shell (AAS)

Topic 1: Frankencert lives

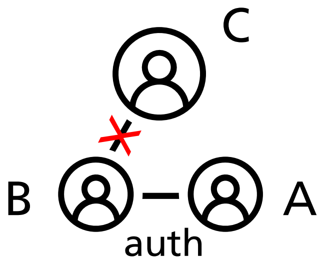


Possible questions to be answered: What are Frankencerts, Mucerts, Transcerts, etc? Which approaches were carried out over the years? How do the concepts differ? To which extend are cyber-physical systems affected?

Literature to start from:

- Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations - https://www.cs.utexas.edu/~shmat/shmat_oak14.pdf
- Guided differential testing of certificate validation in SSL/TLS implementations - https://dl.acm.org/doi/abs/10.1145/2786805.2786835
- Guided, Deep Testing of X.509 Certificate Validation via Coverage Transfer Graphs - https://ieeexplore.ieee.org/abstract/document/9240633
- Coverage-directed Differential Testing of X.509 Certificate Validation in SSL/TLS Implementations - https://dl.acm.org/doi/full/10.1145/3510416

Topic 2: Deniable Authentication in Cyber-Physical Systems



Possible questions to be answered: What is Deniable Authentication? How do the various concepts differ? What use cases arise in CPS?

Literature to start from:

- Efficient deniable authentication and its application in location-based services - https://www.sciencedirect.com/science/article/abs/pii/S0045790622002336
- A practical and communication-efficient deniable authentication with source-hiding and its application on Wi-Fi privacy - https://www.sciencedirect.com/science/article/abs/pii/S0020025519311958
- Weak and Strong Deniable Authenticated Encryption: On their Relationship and Applications - https://ieeexplore.ieee.org/abstract/document/8514181?casa_token=b8_eVz6XFMAAAAA:1dA8_cdr-F4heQifUlIS_lfKw5EQBPfssZ5FfclbSokCdN_sadLJ1YPtwfRws54Hskhjo8d7gx7XSA

Topic 3: Security of C-ITS and Vehicular Ad-Hoc Networks

Possible questions to be answered:

What types of Vehicular Networks exist? Focus on European variants (C-ITS and 802.11p). What are potential attacks on VANETs? Which Countermeasures are / could be utilized against the different types of attacks

Literature to start from:

- Wireless Threats Against V2X Communication
  https://doi.org/10.1109/QRS60937.2023.00058
- BSI, Kooperative Intelligente Verkehrssysteme (C-ITS)
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Automotive/Kooperative_Intelligente_Verkehrssysteme/Kooperative_Intelligente_Verkehrssysteme.html
- Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey (Section VIII Vehicular Networks)
  https://doi.org/10.1109/COMST.2022.3159185

Topic 4: History of Authentication in Cyber-Physical Systems

Possible questions to be answered:

How has authentication in CPS developed over the years? Which methods have been added? Which ones are not pursued any further? How have recommendations changed over the years (length of passwords, regular changing of passwords, use of MFA, use of EC, ...)? Which standard works have been published by relevant organisations (BSI, IEC, NIST, etc.) or researchers and had an impact?

Literature to start from:

- A Survey on the Security in Cyber Physical System with Multi-Factor Authentication https://ieeexplore.ieee.org/abstract/document/9370515
- Multi-Factor Authentication in Cyber Physical System: A State of Art Survey https://ieeexplore.ieee.org/abstract/document/8701960
- Empirical Study of PLC Authentication Protocols in Industrial Control Systems https://ieeexplore.ieee.org/abstract/document/9474296
- [idea for analogous methodology] Two decades of SCADA exploitation: A brief history https://ieeexplore.ieee.org/document/8270432

Relevant standards:

BSI ICS-Security-Kompendium (2013) and later/related recommendations

NIST Guide to Industrial Control Systems (ICS) Security (Rev1, Rev2, Rev3)

ISA/IEC 62443 Industrial communication networks – Network and system security (revs from 2009-2020)

Topic 5: Security of Electronic Data Interchange (EDI)

Possible questions to be answered: Which standardized means of electronic business data exchange exist? How do large companies securely exchange transaction information (order notices & acknowledgements, shipment & delivery notices, invoices, payment confirmations etc.) in an automized and scalable manner? How secure are information exchanged via EDI(FACT), ASC X12, ebXML, ODETTE, RosettaNet or comparable solutions?

Literature to start from:

- Standardization of business-to-business electronic exchanges
  https://ieeexplore.ieee.org/abstract/document/4629329
- A Modern Review of EDI: Representation, Protocols and Security Considerations
  https://ieeexplore.ieee.org/abstract/document/8988546
- Business-to-Business E-Commerce Framework
  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=876291
- Security of E-Procurement Transactions in Supply Chain Reengineering
  https://spectrum.library.concordia.ca/id/eprint/977921/1/23142-91217-1-PB.pdf

Topic 6: Intrusion Detection Systems for Cyber Physical Systems

Possible questions to be answered:

What is an Intrusion Detection System (IDS)? What are ways to enhance IDS to sufficiently protect IoT environments? What are future recommendations and guidance related to cybersecurity issues for IDS in the IoT environment? What is the difference between anomaly detection and IDS?

Literature to start from:

- A Comprehensive Analyses of Intrusion Detection System for IoT Environment - https://doi.org/10.3745/JIPS.03.0144
- A three-tiered intrusion detection system for industrial control systems – https://doi.org/10.1093/cybsec/tyab006
- An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things - https://ieeexplore.ieee.org/document/8470090
- Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks – https://dl.acm.org/doi/10.1145/3264888.3264896
- Cyber-Physical Architecture for Automated Responses (CyPhAAR) Using SDN in Adversarial OT Environments – https://ieeexplore.ieee.org/document/9241285

Topic 7: Anomaly Detection for Cyber Physical Systems

Possible questions to be answered:
What is Anomaly Detection and how is it used to secure the OT environment? What are open research topics, like privacy preserving anomaly detection? What are the most common used techniques for Anomaly detection and what makes it a good/bad approach e.g., Machine Learning with Autoencoders? On which different data types can Anomaly Detection be implemented (Side Channel, Network, …)

Literature to start from:

- WADAC: Privacy-Preserving Anomaly Detection and Attack Classification on Wireless Traffic - https://doi.org/10.1145/3212480.3212495
- Anomaly Detection: A Survey - http://doi.acm.org/10.1145/1541880.1541882
- Distributed Anomaly Detection of Single Mote Attacks in RPL Networks - http://doi.org/10.5220/0007836003780385
- High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks - https://doi.org/10.1145/3264888.3264890
- Deep Learning for Anomaly Detection: A Review - https://arxiv.org/abs/2007.02500
- A Comprehensive Survey on Graph Anomaly Detection with Deep Learning - https://arxiv.org/abs/2106.07178

Topic 8: Cyber-Physical-System-Environments and Authentication Usability

Possible questions to be answered: What CPS environments exist, in which authentication factors can be used? How can these environments be classified/characterized? What subtle differences are relevant for authentication? Which assumptions are made about environments in authentication usability studies? What is the environments influence on authentication usability? Try to capture the niche of ‘environments’.

Literature to start from:

- 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
- Human Factors and Information Security: Individual, Culture and Security Environment - https://apps.dtic.mil/sti/pdfs/ADA535944.pdf
- NIST Special Publication 1500-201 Framework for Cyber-Physical Systems: Volume 1, Overview - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

Topic 9: 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 10a: Vulnerability databases and Open-Source Software (OSS) ecosystems

Possible questions to be answered: How can Open-Source Software components be related to public vulnerability information? (What are CVEs and CPEs? What is the initial goal CPEs are trying to achieve? What are the weaknesses of the current concept? How can it be improved in the future?)

Vulnerability Databases to be considered:

- NIST NVD (National Vulnerability Database) https://nvd.nist.gov/vuln/search
- Google ecosystem: A distributed vulnerability database for Open Source https://osv.dev/
- GitHub Security Advisory https://github.com/advisories/
- CVExploits Search: Your comprehensive database for CVE exploits from across the internet https://cvexploits.io/

Scientific Sources to start from:

- Software Vulnerability Analysis Using CPE and CVE - https://arxiv.org/abs/1705.05347
- CPE and CVE based Technique for Software Security Risk Assessment - https://ieeexplore.ieee.org/document/9660968
- Detecting "0-Day" Vulnerability: An Empirical Study of Secret Security Patch in OSS - https://ieeexplore.ieee.org/document/8809499
- Security Risk Visualization for Open-Source Software based on Vulnerabilities, Repositories, and Dependencies - https://ieeexplore.ieee.org/document/10406153
- The (un)reliability of NVD vulnerable versions data: an empirical experiment on Google Chrome vulnerabilities - https://dl.acm.org/doi/10.1145/2484313.2484377
- CVEfixes: automated collection of vulnerabilities and their fixes from open-source software: https://dl.acm.org/doi/10.1145/3475960.3475985

Topic 10b: Security Advisories and their role in vulnerability information and software ecosystems

Possible questions to be answered: What are Security Advisories? What problems are they trying to solve? How are Security Advisories related to Common Vulnerabilities and Exposures (CVEs)? What is the purpose of the Common Security Advisory Framework (CSAF) in this context? How can information extracted from Security Advisories help to map CVEs to Software Products?

Online Sources to be considered:

- GitHub Security Advisory https://github.com/advisories/
- Oasis Tools https://oasis-open.github.io/csaf-documentation/tools.html

Scientific Sources to start from:

- Development of a GraphQL-based API for querying security advisories for Common Security Advisory Framework (CSAF) - https://www.fernuni-hagen.de/pv/docs/wiegel-abschlussarbeit.pdf
- Development of an API to request security advisories for CSAF 2.0 - https://opus.hs-offenburg.de/files/6011/CSAF_API_development_v1.pdf
- Generating ICS vulnerability playbooks with open standards - https://link.springer.com/article/10.1007/s10207-023-00760-5
- A Method and Platform for Security Advisory Dissemination Leveraging Web3 Technologies - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10411464
- Semi-automated information extraction from unstructured threat advisories - https://dl.acm.org/doi/10.1145/3021460.3021482
- Backstabber’s knife collection: A review of open source software supply chain attacks - https://dl.acm.org/doi/10.1007/978-3-030-52683-2_2

Topic 11: Forensic of autonomous vehicles

Possible questions to be answered: Where is data stored within a car? How is the integrity of black box data ensured during storage and transmission? How can data collection in autonomous systems be structured to facilitate subsequent forensic investigations, ensuring that either no sensitive data is stored, or the privacy protection of sensitive data while maintaining access to sufficient information?

Video as entry point:

- https://media.ccc.de/v/37c3-11935-unlocking_the_road_ahead_automotive_digital_forensics

Literature to start from:

- Towards an AI-Based After-Collision Forensic Analysis Protocol for Autonomous Vehicles - https://ieeexplore-ieee-org.eaccess.tum.edu/document/9283838
- Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects - https://www.mdpi.com/2227-7080/11/5/117
- A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection - https://ieeexplore.ieee.org/document/9815132
- Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art - https://doi-org.eaccess.tum.edu/10.1109/ACCESS.2022.3213843
- Enabling Digital Forensics Readiness for Internet of Vehicles - https://doi.org/10.1016/j.trpro.2021.01.040

Topic 12: Automotive Authentication

Possible questions to be answered: What options were/are there for authenticating yourself to a vehicle? Compare various manufacturers, both access and engine start. Which algorithms were broken or contradicted basic security principles, where could the journey still go? What about PKES concepts or similar?

Literature to start from:

- https://arxiv.org/abs/2003.13251 - Hold the Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft (2003)
- https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia - Lock It and Still Lose It - on the (In)Security of Automotive Remote Keyless Entry Systems (2016)
- https://link.springer.com/article/10.1007/s41635-022-00126-8 - PAKAMAC: A PUF-based Keyless Automotive Entry System with Mutual Authentication (2022)
- https://arxiv.org/abs/2210.11923 - RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems (2022)
- https://tches.iacr.org/index.php/TCHES/article/view/9063 - My other car is your car: compromising the Tesla Model X keyless entry system (2021)
- https://documentserver.uhasselt.be/handle/1942/29311 - Security analysis and exploitations of keyless entry systems in cars (2019)
- https://ieeexplore.ieee.org/abstract/document/8710105 - On the Security of Remote Key Less Entry for Vehicles (2019)
- https://ieeexplore.ieee.org/abstract/document/9730437 - Automotive Security and Theft Prevention Systems: State of The Art (2021)
- https://www.illmatics.com/remote%20attack%20surfaces.pdf - A Survey of Remote Automotive Attack Surfaces (2014)
- https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces - Comprehensive Exp. Analyses of Automotive Attack Surfaces (2011)
- https://illmatics.com/Remote%20Car%20Hacking.pdf - Remote Exploitation of an Unaltered Passenger Vehicle (2015)
- https://ieeexplore.ieee.org/abstract/document/9039557 - Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges (2020)

Topic 13: Selection of Privacy-Enhancing Technologies (PETs) for Cyber Physical Systems

Possible questions to be answered: What are Privacy Enhancing Technologies (PETs)? Which PETs are suitable for real-world deployment in practical use cases? How are PETs chosen to align with the demands of Cyber Physical System environments? How can the appropriate PETs be identified to address the pertinent protection goals and requirements?

Literature to start from:

- A taxonomy for privacy enhancing technologies - https://doi.org/10.1016/j.cose.2015.05.002
- Application-Oriented Selection of Privacy Enhancing Technologies - https://arxiv.org/abs/2206.07329
- Technical privacy metrics: a systematic survey - https://dl.acm.org/doi/10.1145/3168389
- Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey - https://doi-org.eaccess.tum.edu/10.1016/j.jnca.2020.102807
- A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements - https://link-springer-com.eaccess.tum.edu/article/10.1007/s00766-010-0115-7

Topic 14: Continuous Authentication in IIoT

Possible questions to be answered: Which approaches exist to implement continuous authentication in IIoT? What are the advantages of passive authentication vs. traditional active approaches? Which variants (behavior, biometrics, …) of continuous authentication are best suited? What about the performance, usability, robustness, and maturity? Which influence does the (I)IoT environment have?

Literature to start from:

- 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
- Not Quite Yourself Today: Behaviour-Based Continuous Authentication in IoT Environments
https://doi.org/10.1145/3432206

Topic 15a: Attribute based encryption and zero knowledge proofs in Peer-to-Peer networks for anonymous identities

Possible questions to be answered: What is attribute based encryption (ABE)? What are zero knowledge proofs (ZKP)? How can a privacy-preserving identity management be established trough anonymous credentials and selective disclosure? How can attribute-based encryption and zero-knowledge proofs contribute to ensure privacy for both data providers and users? Is it feasible to achieve this without utilizing blockchain technology?

Literature to start from:

- Decentralized Identities for Self-sovereign End-users (DISSENS) - https://dl.gi.de/handle/20.500.12116/36501
- reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption - https://ieeexplore.ieee.org/document/8456003
- Toward a Post-Quantum Zero-Knowledge Verifiable Credential System for Self-Sovereign Identity - https://eprint.iacr.org/2022/1297
- Signature Schemes and Anonymous Credentials from Bilinear Maps - https://link.springer.com/chapter/10.1007/978-3-540-28628-8_4
- Authentication, Authorization, and Selective Disclosure for IoT data sharing using Verifiable Credentials and Zero-Knowledge Proofs - https://arxiv.org/abs/2209.00586
- A decentralized strongly secure attribute-based encryption and authentication scheme for distributed Internet of Mobile Things - https://www.sciencedirect.com/science/article/abs/pii/S1389128621004722
- An improved attribute-based encryption technique towards the data security in cloud computing - https://onlinelibrary-wiley-com.eaccess.tum.edu/doi/10.1002/cpe.4364
- Secure and Fine-Grained Flow Control for Subscription-Based Data Services in Cloud-Edge Computing - https://ieeexplore-ieee-org.eaccess.tum.edu/document/9873982

Topic 15b: Cyber Threat Intelligence sharing and zero knowledge proofs in Peer-to-Peer networks

Possible questions to be answered: What is Cyber Threat Intelligence (CTI) sharing? What are zero knowledge proofs (ZKP)? How can trust be established for Cyber Threat Intelligence sources? How can the quality of the source be determined, and which source should be trusted? How can zero-knowledge proofs contribute to safeguarding the confidentiality of resources exchanged within a decentralized network?

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
- Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus - https://www.hindawi.com/journals/scn/2023/3303122/
- TradeChain: Decoupling Traceability and Identity in Blockchain enabled Supply Chains - https://ieeexplore-ieee-org.eaccess.tum.edu/document/9724455
- A topological potential weighted community-based recommendation trust model for P2P network - https://link.springer.com/article/10.1007/s12083-014-0288-9
- Authentication, Authorization, and Selective Disclosure for IoT data sharing using Verifiable Credentials and Zero-Knowledge Proofs - https://arxiv.org/abs/2209.00586
- Survey on Computational Trust and Reputation Models - https://dl.acm.org/doi/10.1145/3236008

Topic 17: Authentication Token Security Perception

Possible questions to be answered: How is the security of authentication tokens perceived? Are there different test groups with different perceptions? By which range do the perceptions differ? Which authentication tokens have been extensively researched with regard to perception and which have not?

Literature to start from:

- https://dl.acm.org/doi/full/10.1145/3503514 - “Nah, it’s just annoying!” A Deep Dive into User Perceptions of Two-Factor Authentication (2022)
- https://www.sciencedirect.com/science/article/abs/pii/S1071581919301119 - The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes (2020)
- https://www.sciencedirect.com/science/article/abs/pii/S0167404808000941 - User perceptions of security, convenience and usability for ebanking authentication tokens (2008)
- https://www.sciencedirect.com/science/article/abs/pii/S0167404822000025 - Usable and secure? User perception of four authentication methods for mobile banking (2022)
- https://dl.acm.org/doi/abs/10.1145/3282894.3282923 - Open Sesame!: User Perception of Physical, Biometric, and Behavioural Authentication Concepts to Open Doors (2018)
- https://dl.acm.org/doi/abs/10.1145/3173574.3174030 - “It's not actually that horrible”: Exploring Adoption of Two-Factor Authentication at a University (2018)
- https://link.springer.com/chapter/10.1007/978-3-030-31500-9_7 - User Perceptions of Security and Usability of Mobile-Based Single Password Authentication and Two-Factor Authentication (2019)
- https://arxiv.org/abs/1908.05901 - Evaluating User Perception of Multi-Factor Authentication: A Systematic Review (2019)
- https://dl.acm.org/doi/abs/10.1145/3427228.3427243 - More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication (2020)
- https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.124 - Assessment of privacy and security perception of biometric technology case study of Kaduna state tertiary academic institutions (2020)
- https://link.springer.com/chapter/10.1007/978-3-031-43033-6_5 - Authentication of IT Professionals in the Wild – A Survey (2023)
- https://ieeexplore.ieee.org/abstract/document/8802493 - Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication (2019)
- https://www.usenix.org/conference/soups2021/presentation/owens - User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators (2021)
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4177411 - Building An Authentication Infrastructure — Designing a Two Factor Authentication Hardware Token with Form Factor that Encourages Engagement (2022)
- https://tspace.library.utoronto.ca/handle/1807/89824 - User Perceptions of Security Risks in Multiple Authentications (2018)
- https://link.springer.com/chapter/10.1007/978-3-662-58387-6_9 - Why Johnny Doesn’t Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key (2018)

Topic 18: Secure PLC Programming

Possible questions to be answered: How does the way differ in which way PLCs are programmed from IT devices? What are security best practices for programming PLCs? Are there secure coding standards for PLCs? What kind of vulnerabilities may arise in PLCs and how can they be detected?

Literature to start from:

- Software security: Application-level vulnerabilities in SCADA systems
  https://doi.org/10.1109/IRI.2011.6009603
- Programmable logic controllers based systems (PLC-BS): vulnerabilities and threats
  https://doi-org.eaccess.tum.edu/10.1007/s42452-019-0860-2
- Employing secure coding practices into industrial applications: a case study
  https://doi-org.eaccess.tum.edu/10.1007/s10664-014-9341-9
- Walking under the ladder logic: PLC-VBS: a PLC control logic vulnerability scanning tool
  https://doi.org/10.1016/j.cose.2023.103116
- [non-scientific] Top 20 Secure PLC Coding Practices
  https://plc-security.com/
- Security of Programmable Logic Controllers and Related Systems: Today and Tomorrow
  https://doi.org/10.1109/OJIES.2023.3335976

Topic 19: Secure Bootstrapping

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?

Literature to start from:

- Secure IoT Bootstrapping: A Survey - https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-secure-bootstrapping-00
- Terminology and processes for initial security setup of IoT devices - https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-security-setup-iot-devices
- On the Security of IIoT Deployments: An Investigation of Secure Provisioning Solutions for OPC UA - https://ieeexplore.ieee.org/document/9478911
- Secure Bootstrapping for Internet of Things (Dissertation, parts of Chapter 2 interesting) - https://www.theses.fr/2022IPPAT023.pdf

- Protocol specifications:
  - BRSKI/EST - https://datatracker.ietf.org/doc/rfc8995/ and https://datatracker.ietf.org/doc/html/rfc7030, possibly also BRSKI-AE, BRSKI-ACE, BRSKI-PRM
  - SZTP - https://datatracker.ietf.org/doc/rfc8572/
  - FIDO automatic onboarding - https://fidoalliance.org/intro-to-fido-device-onboard/
  - OMA LwM2M - https://technical.openmobilealliance.org/index.html
  - Wi-Fi Alliance Device Provisioning Protocol (DPP) - https://www.wi-fi.org/downloads-public/Device_Provisioning_Protocol_Specification_v1.1_1.pdf/35330
  - Extensible Authentication Protocol-Nimble Out-of-Band (EAP-NOOB) - https://datatracker.ietf.org/doc/html/rfc9140

Topic 20: Objectives, Concepts and Development Status of the Asset Administration Shell (AAS)

Possible questions to be answered: What are the objectives, use cases and target groups of the AAS? What are the central concepts and design principles of the AAS? How does the AAS map or integrate asset supply chains? Does the AAS facilitate or provide a mechanism for secure bootstrapping / provisioning of assets? What is the current state of development (conception and implementation)? Are there alternative approaches to the AAS?

Literature to start from:

- Publications by the official Industrie 4.0 website: https://www.plattform-i40.de/SiteGlobals/IP/Forms/Listen/Downloads/EN/Downloads_Formular.html?cl2Categories_Typ_name=veroeffentlichung
  - Structure of the Administration Shell - Trilateral perspectives from France, Italy and Germany.
  - IIoT Value Chain Security – Chain of Trust for Organizations and Products.
  - Details of the Asset Administration Shell. Part 1 - The exchange of information between partners in the value chain of Industrie 4.0.
  - and many more…
- Product lifecycle management with the asset administration shell. https://www.mdpi.com/2073-431X/10/7/84/pdf
- The asset administration shell as enabler for predictive maintenance: a review. https://link.springer.com/article/10.1007/s10845-023-02236-8
- Open-Source Implementations of the Reactive Asset Administration Shell: A Survey. https://www.mdpi.com/1424-8220/23/11/5229
- Diskussionspapier – Interoperabilität mit der Verwaltungsschale, OPC UA und AutomationML. https://www.automationml.org/wp-content/uploads/2023/04/Diskussionspapier-Zielbild-und-Handlungsempfehlungen-fuer-industrielle-Interoperabilitaet-5.3.pdf

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 & Co. ResearchRabbit and ConnectedPapers*

FAQ cont.

- Does the 1-to-1 kickoff meeting have to take place until 28.03.2024?
  - *No. The meeting only has to be organized within this period but can take place after the 28.03.2024*
- Do I have to participate in all presentations?
  - Yes. To facilitate the discussion participation is mandatory and your discussion will be graded.

Thanks for your attention. Open questions?

Veronique Ehmes, Sebastian Peters, Adrian Reuter, Nikolai Puch
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