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

<210 employees

10 HighTech Security Labs

Funding

© Fraunhofer
What are CPS?

- Robots
- Autonomous vehicles
- Production line
- PLCs
- Embedded computers
IT vs OT differences

Security triad (CIA) upside down (AIC)

Most important

Confidentiality

Integrity

Availability

Least important

Availability

Integrity

Confidentiality
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!
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/](http://docmatching.in.tum.de/))

**Motivational email** to otsecseminar@aisec.fraunhofer.de (about, e.g., your relation to (IT-)security, your 3-4 preferred topics, which topic you like most, and why)
06.02.2024 (today)
- Organizational information
- Overview on topics

23.02.2024
- Automated assignment of courses

Until 14.02.2024
- Registration via DocMatching: http://docmatching.in.tum.de/
- Motivational email to otsecseminar@aisec.fraunhofer.de

Until 03.03.2024
- Please send us your 3-4 preferred topics via email (if not already done in your motivational email)
Process (2/4)

Until 06.03.2024
• 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**!
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

- **12.01.2024 – 17.02.2024**
  - Revision of slides

- **Until 11.07.2024**
  - Comments on the slides from supervisor

- **15./16.07.2024**
  - Final presentations + discussion (in-person at Fraunhofer AISEC)
  - Length of each presentation 25 minutes + 15 minutes of discussion
  - Participation is **obligatory**
# Deadlines for Obligatory Deliverables

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Due to</th>
<th>Grading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-to-1 Kick-Off Meeting with supervisors</td>
<td>28.03.2024</td>
<td>-</td>
</tr>
<tr>
<td>Submission of Draft Paper</td>
<td>19.05.2024</td>
<td>10%</td>
</tr>
<tr>
<td>Reviews</td>
<td>02.06.2024</td>
<td>5%</td>
</tr>
<tr>
<td>Rebuttal</td>
<td>09.06.2024</td>
<td>-</td>
</tr>
<tr>
<td>Submission of Final Paper</td>
<td>27.06.2024</td>
<td>50%</td>
</tr>
<tr>
<td>Presentation</td>
<td>15./16.07.2024</td>
<td>30%</td>
</tr>
<tr>
<td>Presentation Discussion</td>
<td>15./16.07.2024</td>
<td>5%</td>
</tr>
</tbody>
</table>

Σ 100 %
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
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. Vulnerability databases and Open-Source Software (OSS) 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
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:

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:


- Weak and Strong Deniable Authenticated Encryption: On their Relationship and Applications - [https://ieeexplore.ieee.org/abstract/document/8514181?casa_token=b8_eVz6XFMAAAAA:1dA8_cdr-F4heQifUIIS_IfKw5EQBPfssZ5FclbSokCdN_sadLJ1YPtwfRws54Hskhjo8d7gx7XSA](https://ieeexplore.ieee.org/abstract/document/8514181?casa_token=b8_eVz6XFMAAAAA:1dA8_cdr-F4heQifUIIS_IfKw5EQBPfssZ5FclbSokCdN_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
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
- Multi-Factor Authentication in Cyber Physical System: A State of Art Survey
- Empirical Study of PLC Authentication Protocols in Industrial Control Systems
- [idea for analogous methodology] Two decades of SCADA exploitation: A brief history

Relevant standards:
- BSI ICS-Security-Kompendium (2013) and later/related recommendations
- ISA/IEC 62443 Industrial communication networks – Network and system security (revs from 2009-2020)
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 automated 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
- A Modern Review of EDI: Representation, Protocols and Security Considerations
- 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
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
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:
- 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
Possible questions to be answered: What CPS environments exist, in which authentication factors can/could be used? How can these environments be classified/characterized? What subtle differences are relevant for authentication? What is their influence on Authentication Usability? Try to catch the niche of ‘environments’.

Literature to start from:

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:
- Beauty and the Burst: Remote Identification of Encrypted Video Streams https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/schuster
Topic 10: 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 CCVE exploits from across the internet https://cvexploits.io/

Scientific Sources to start from:
- The (un)reliability of NVD vulnerable versions data: an empirical experiment on Google Chrome vulnerabilities - https://dl.acm.org/doi/10.1145/2484313.2484377
**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_roadAhead_automotive_digital_forensics](https://media.ccc.de/v/37c3-11935-unlocking_the_roadAhead_automotive_digital_forensics)

**Literature to start from:**
- 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](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](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://tches.iacr.org/index.php/TCHES/article/view/9063 - My other car is your car: compromising the Tesla Model X keyless entry system (2021)
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
- 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
**Possible questions to be answered:** Which approaches exist, to implement continuous authentication in IIoT? What would be 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](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](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](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](https://doi.org/10.1145/3432206)
Topic 15: Attribute based encryption and zero knowledge proofs in Peer-to-Peer networks

Possible questions to be answered: What is attribute based encryption (ABE)? What are zero knowledge proofs (ZKP)? How can attribute-based encryption and zero-knowledge proofs contribute to safeguarding the confidentiality of resources exchanged within a public peer-to-peer network, while also ensuring privacy for both data providers and users? Is it feasible to achieve this without utilizing blockchain technology?

Literature to start from:
- Blockchain-Based Fair Payment for ABE with Outsourced Decryption - https://link.springer.com.eaccess.tum.edu/article/10.1007/s12083-022-01406-4
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-Preserving Data Aggregation Scheme for IIoT - https://ieeexplore.ieee.org/document/9968228
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://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://link.springer.com/chapter/10.1007/978-3-031-43033-6_5 - Authentication of IT Professionals in the Wild – A Survey (2023)
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
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