SEMINAR: OPERATIONAL TECHNOLOGY SECURITY
PRE-COURSE MEETING 02.02.2022

Michael Heinl, Sebastian Peters, Nikolai Puch

Fraunhofer AISEC

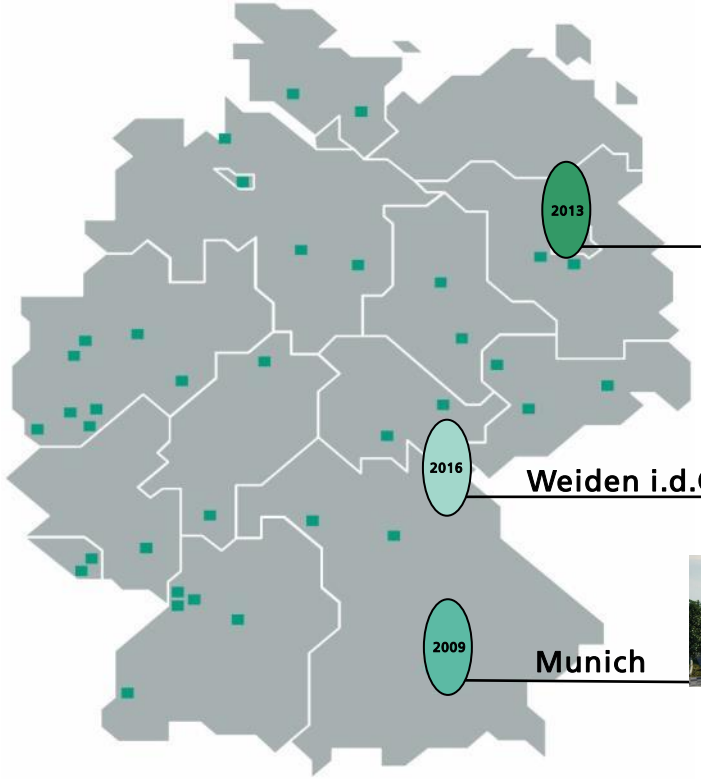
SEMINAR: OPERATIONAL TECHNOLOGY SECURITY PRE-COURSE MEETING

- About Fraunhofer AISEC
- Course Objectives
- Orga
- Deliverables
- Process
- Grading
- Possible Topics

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

<200 employees

10 Hightech Security Labs

Funding €

State directly

3rd party research projects

Fraunhofer AISEC

Course Objectives

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

Orga

- Online
  - Moodle
  - Video Calls
- Up to 10 students
  - Individual work (no groups)
  - No qualification challenge
  - Registration in matching system necessary (http://docmatching.in.tum.de/)
- Language of instruction and deliverables will be **English**

Deliverables

- Paper
  - Systematization of Knowledge (SoK)
  - IEEE conference proceedings template
  - ~10 pages excl. list of references and appendices
- Reviews/Rebuttal
  - Most likely via Moodle
- Presentation
  - 25 minutes presentation
  - 15 minutes discussion
  - Submission of slides in advance
- Utilization of LaTeX is encouraged wherever possible (paper!)

Process (1/4)

- 02.02.2022 (today)
  - Organizational information
  - Topic presentation
- 10.02.2022 – 15.02.2022
  - Registration via DocMatching (http://docmatching.in.tum.de/)
- 24.02.2022
  - Automated assignment of courses
- Until 03.03.2022
  - Please send us your three preferred topics via email
  - You may add a letter of motivation to emphasize your top choice

Process (2/4)

- Until 10.03.2022
  - Response from organizers with assigned topic
  - Alternatively: Possibility to withdraw without penalty
  - Non-attendance after this point is graded with 5.0
- 11.03.2022 – 29.04.2022
  - Familiarize with literature
  - Schedule kickoff meeting with your supervisor at Fraunhofer AISEC (as soon as possible)
- 29.04.2022 – 15.05.2022
  - Preparation of the draft version of the paper

Process (3/4)

- 16./17.05.2022
  - Assignment of two of your fellow students' paper for review
- 18.05.2022 – 29.05.2022
  - Preparation of written review of these papers
- 30.05.2022 – 05.06.2022
  - Rebuttal period
- 06.06.2022 – 26.06.2022
  - Preparation of the final paper
    - Revision based on reviews/rebuttal

Process (4/4)

- 27.06.2022 – 03.07.2022
  - Slide preparation
- Until 10.07.2022
  - Comments on the slides from supervisor
- 11.07.2022 – 13.07.2022
  - Revision of slides (if necessary)
- 14./15.07.2022
  - Final presentations + discussion (most likely via video call)
  - Both sessions are expected to begin at 10am and will end at 3pm
  - Length of each presentation 25 minutes + 15 minutes of discussion

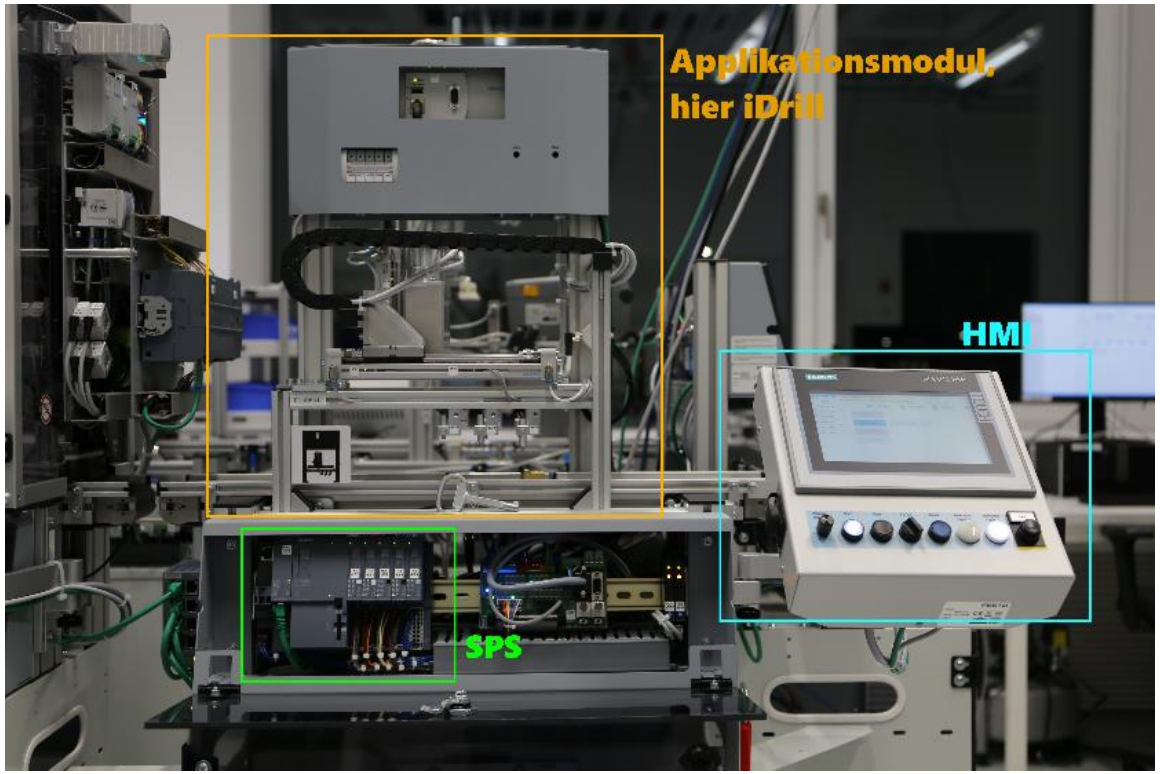
Grading

- **50 %** Final Paper
- **40 %** Presentation
- **5 %** Peer Reviews
- **5 %** Discussion Participation

Σ 100 % Total

Topics (Overview)

1. Secure Communication Protocols for OT
2. Trust Anchors in Industrial Environments
3. Post-Quantum Cryptography for OT
4. OT Device Fingerprinting
5. Secure and Usable Authentication for OT
6. OT Supply Chain Security
7. OT Ransomware
8. IDS/IPS for OT
9. Logging in OT Environments
10. Honeypots for OT



Topic 1: Secure Communication Protocols for OT

Possible questions to be answered:
What are the security aspects of OPC UA and MQTT? What are the weak points and how could they be exploited?

Literature to start from:

- Open-Source OPC UA Security and Scalability
  https://ieeexplore.ieee.org/document/9212091
- Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments
  https://dl.acm.org/doi/abs/10.1145/3419394.3423666
- Securing smart maintenance services: Hardware-security and TLS for MQTT
  https://ieeexplore.ieee.org/abstract/document/7281913/
- Authorization mechanism for MQTT-based Internet of Things
  https://ieeexplore.ieee.org/document/7503802

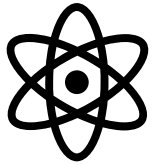
Topic 2: Trust Anchors in Industrial Environments

Possible questions to be answered:
What are the differences, similarities, and special aspects of trust anchors in OT? What are possible attack strategies? How can trust be established with minimal manual effort?

Literature to start from:

- Portable Trust Anchor for OPC UA Using Auto-Configuration
  https://ieeexplore.ieee.org/abstract/document/9211904
- Gateway for Industrial Cyber-Physical Systems with Hardware-based Trust Anchors
  https://rieke.link/IDC2019-GatewayICPS.pdf
- Hardware Rooted Trust for Additive Manufacturing
  https://ieeexplore.ieee.org/abstract/document/8737928
- Secure Device Identifiers and Device Enrollment in Industrial Control System
  https://ieeexplore.ieee.org/abstract/document/9118131

Topic 3: Post-quantum cryptography for OT



Possible questions to be answered:
How to integrate quantum-resistant primitives into IIoT devices? What about their performance, usability, and maturity? How does the PQC integration in OT differ from IT environments?

Literature to start from:

- Towards Post-Quantum Security for Cyber-Physical Systems: Integrating PQC into Industrial M2M Communication
  https://link.springer.com/chapter/10.1007/978-3-030-59013-0_15
- Hybrid OPC UA: Enabling Post-Quantum Security for the Industrial Internet of Things
  https://ieeexplore.ieee.org/abstract/document/9212112
- TPM-Based Post-Quantum Cryptography: A Case Study on Quantum-Resistant and Mutually Authenticated TLS for IoT Environments
  https://dl.acm.org/doi/abs/10.1145/3465481.3465747

Topic 4: OT Device Fingerprinting

Possible questions to be answered:
How to verify authenticity of responses from IoT devices by using their physical characteristics, e.g., sensor noise?

Literature to start from:

- Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems https://www.ndss-symposium.org/wp-content/uploads/2017/09/who-control-your-control-system-device-fingerprinting-cyber-physical-systems.pdf
- Hardware Identification via Sensor Fingerprinting in a Cyber Physical System https://ieeexplore.ieee.org/abstract/document/8004367
- Fingerprinting for Cyber-Physical System Security: Device Physics Matters Too https://ieeexplore.ieee.org/abstract/document/8490185

Topic 5: Secure and Usable Authentication for OT

Possible questions to be answered:
Which authentication procedures are best to be used in OT context? What about their performance, usability, robustness, and maturity?

Literature to start from:

- Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications https://ieeexplore.ieee.org/abstract/document/8675176
- Survey of Authentication and Authorization for the Internet of Things https://www.hindawi.com/journals/scn/2018/4351603/
- Survey on Delegated and Self-Contained Authorization Techniques in CPS and IoT https://ieeexplore.ieee.org/document/9467373

Topic 6: OT Supply Chain Security

Possible questions to be answered:
What are the cyber security flaws in current supply chains? How could they be mitigated? How might steganography be involved?

Literature to start from:

- Information Hiding in Industrial Control Systems: An OPC UA based Supply Chain Attack and its Detection
  https://dl.acm.org/doi/abs/10.1145/3369412.3395068
- Understanding Security Requirements for Industrial Control System Supply Chains
  https://ieeexplore.ieee.org/abstract/document/8823698
- A novel approach for analyzing the nuclear supply chain cyber-attack surface
  https://www.researchgate.net/publication/345433537_A_novel_approach_for_analyzing_the_nuclear_supply_chain_cyber-attack_surface

Topic 7: OT Ransomware

Possible questions to be answered:
How does OT ransomware differ from other ransomware? What are possible mitigation strategies? Who's behind OT ransomware? What simulation environments/ransomware frameworks exist? How much does OT ransomware rely on (/is adopted to) specific OT environments?

Literature to start from:

- Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things https://ieeexplore.ieee.org/document/8703829
- All Your PLCs Belong to Me: ICS Ransomware Is Realistic https://ieeexplore.ieee.org/abstract/document/9343036
- The Ransomware Threat to Energy-Delivery Systems https://ieeexplore.ieee.org/abstract/document/9383178

Topic 8: IDS/IPS for OT

Possible questions to be answered:
How do IDS/IPS work in OT environments? How effective are they? What are the in comparison with IT? Does Machine Learning provide an advantage over simpler (traffic-)rule-sets? How do prevention strategies work?

Literature to start from:

- Detection of Unauthorized IoT Devices Using Machine Learning Techniques
  https://arxiv.org/abs/1709.04647
- Network Anomaly Detection: A Machine Learning Perspective
  https://www.researchgate.net/publication/307936101_Network_Anomaly_Detection_A_Machine_Learning_Perspective
- A three-tiered intrusion detection system for industrial control systems
  https://academic.oup.com/cybersecurity/article/7/1/tyab006/6153960
- Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning
  http://arxiv.org/pdf/1709.05342v2
- Intrusion Detection for Cyber-Physical Attacks in Cyber-Manufacturing System (DISS)
  https://surface.syr.edu/etd/1078/
- Attack Scenarios in Industrial Environments and How to Detect Them
  https://www.jstor.org/stable/27033629

Topic 9: Protocol for Logging in OT environments

Possible questions to be answered:
What logging solutions and protocols exist for OT environments? How secure are they? Do they need any special precautions? How important is logging? What solutions exist for aggregating data from different event sources?

Literature to start from:

- Secure Logging in Operational Instrumentation and Control Systems
  https://opus4.kobv.de/opus4-fau/frontdoor/index/index/docId/12613
- Fear and Logging in the Internet of Things
  https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_01A-2_Wang_paper.pdf
- Anomaly detection for industrial control systems using process mining
  https://www.sciencedirect.com/science/article/pii/S0167404818306795

Topic 10: OT Honeypots

Possible questions to be answered:
What are honeypots used for in the OT environment? Can they protect critical infrastructure? How are they integrated and set-up? What results do they produce?

Literature to start from:

- Don’t get Stung, Cover your ICS in Honey: How do Honeypots fit within Industrial Control System Security https://doi.org/10.1016/j.cose.2021.102598
- Angriffserkennung für industrielle Netzwerke innerhalb des Projektes IUNO https://arxiv.org/abs/1709.09455
- A Mixed-Interaction Critical Infrastructure Honeypot https://www.cesar-conference.org/wp-content/uploads/2020/11/CESAR2020_090_M-O-PAHL_a_mixed-interaction_critical_infrastructure_honeypot_v2.pdf
- World Wide ICS Honeypots: A Study into the Deployment of Conpot Honeypots https://eprints.lancs.ac.uk/id/eprint/161485/

Thanks for your attention. Open questions?

Michael Heinl, Sebastian Peters, Nikolai Puch
Department Product Protection & Industrial Security
Fraunhofer Institute for Applied and Integrated Security AISEC

{michael.heinl | sebastian.peters | nikolai.puch}@aisec.fraunhofer.de

Address: Fraunhofer AISEC
Lichtenbergstr. 11
85748 Garching
Germany
Internet: www.aisec.fraunhofer.de

Fraunhofer AISEC