SEMINAR: OPERATIONAL TECHNOLOGY SECURITY WS 22/23
PRE-COURSE MEETING 08.07.2022

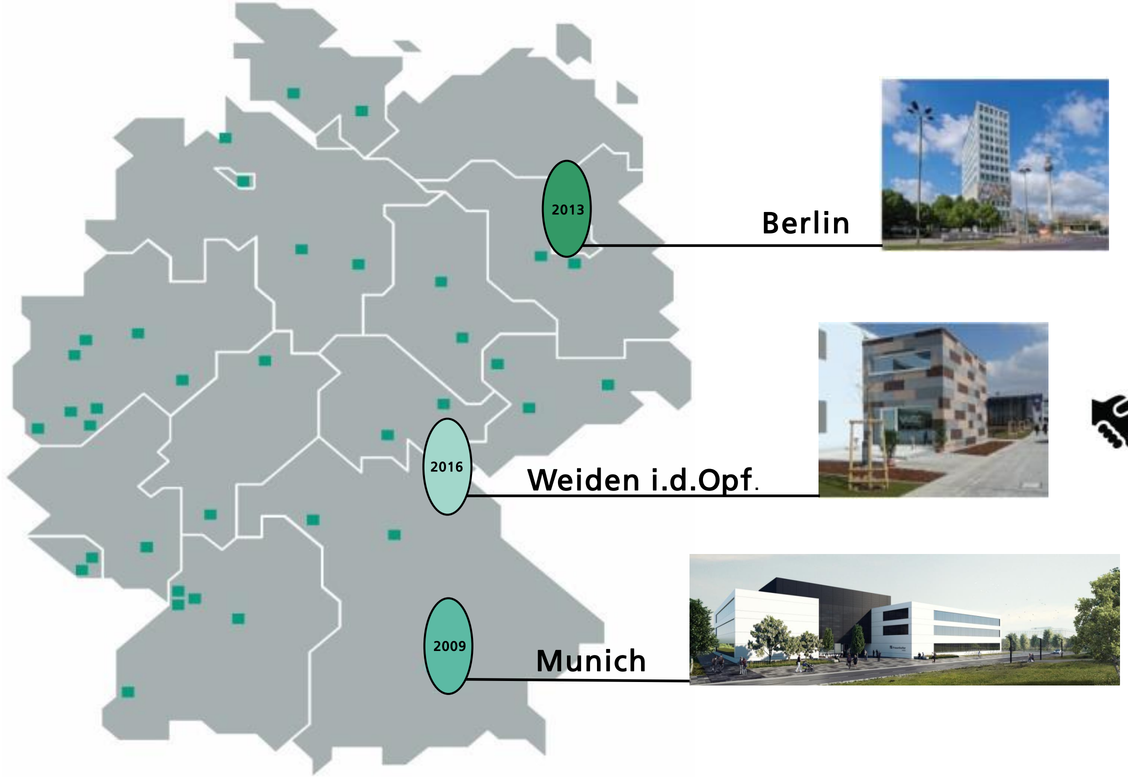
Michael Heinl, Sebastian Peters, Nikolai Puch

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

<210 employees

10 Hightech Security Labs

Funding €

20% State directly

80% 3rd party research projects

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
  - TUM Moodle
  - Video Calls via MS Teams
- Up to 10 students
  - Individual work (no groups)
  - No qualification challenge
  - Optional: Motivational email to otsecseminar@aisec.fraunhofer.de
    (your name, which topic you like most, and why)
  - Necessary: Registration in matching system (http://docmatching.in.tum.de/)
- Language of instruction and deliverables will be **English**
- Communication via email – **always use "reply-all"** when writing or answering to us!

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)

- 08.07.2022 (today)
  - Organizational information
  - Topic presentation
- 22.07.2022 – 27.07.2022
  - Registration via DocMatching (http://docmatching.in.tum.de/)
  - Optional: Motivational email
- 05.08.2022
  - Automated assignment of courses
- Until 14.08.2022
  - 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 19.08.2022
  - Response from organizers with assigned topic
  - Alternatively: Possibility to withdraw without penalty
  - Non-attendance after this point is graded with 5.0
- 20.08.2022 – 11.09.2022
  - Familiarize with literature
  - Schedule kickoff meeting with your supervisor at Fraunhofer AISEC (as soon as possible)
- 12.09.2022 – 06.11.2022
  - Preparation of the draft version of the paper

Process (3/4)

- Until 11.11.2022
  - Assignment of two of your fellow students' paper for review
- 12.11.2022 – 27.11.2022
  - Preparation of written review of these papers
- 28.11.2022 – 04.12.2022
  - Rebuttal period
- 05.12.2022 – 31.12.2022
  - Preparation of the final paper
    - Revision based on reviews/rebuttal

Process (4/4)

- 01.01.2023 – 15.01.2023
  - Slide preparation
- Until 20.01.2023
  - Comments on the slides from supervisor
- 21.01.2023 – 29.01.2023
  - Revision of slides (if necessary)
- 02./03.02.2023
  - 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
  - Participation is obligatory!

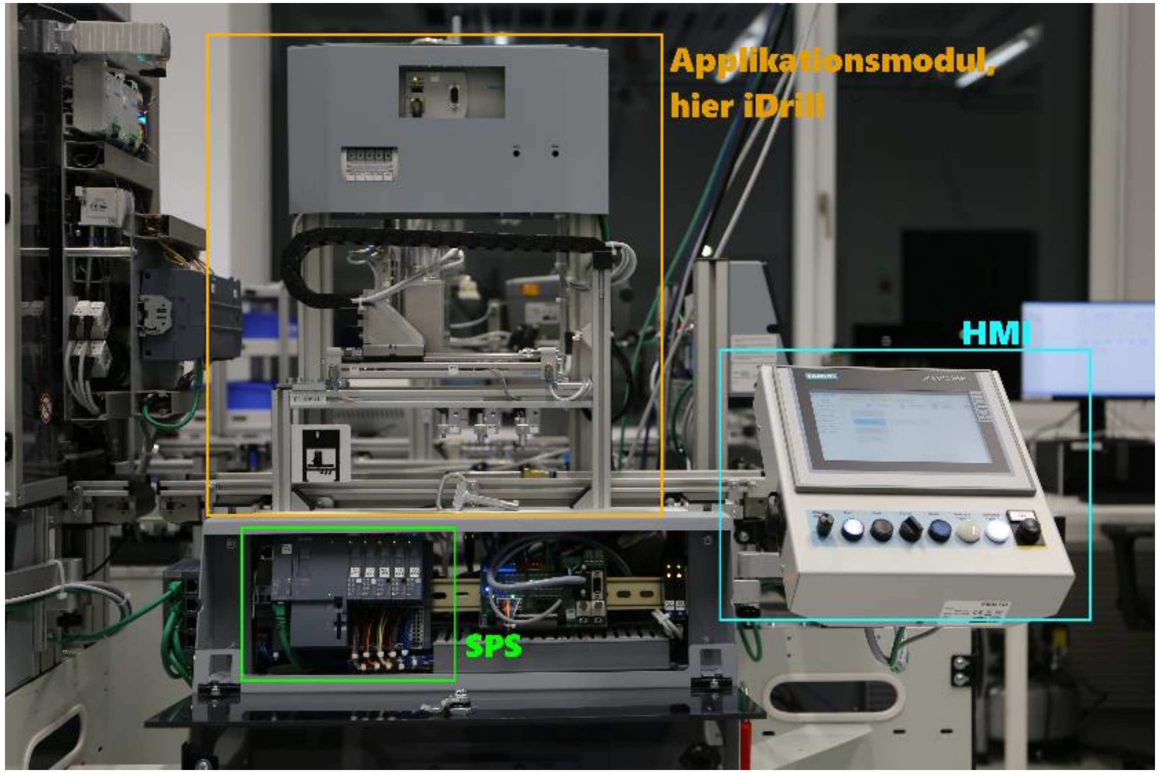
Grading

- 45 % Final Paper
- 35 % Presentation
- 10 % Paper draft
- 5 % Peer Reviews
- 5 % Discussion Participation

Σ 100 % Total

Topics (Overview)

1. PKI in OT
2. Trust Anchors in OT
3. OT PQC
4. OT Remote Safety
5. OT Authentication Usability
6. OT Logging
7. OT IDS/IPS
8. Secure Communication Protocols - OPC UA/MQTT
9. OT Datasets
10. Secure PLC Programming
11. OT Hardware-in-the-loop Testbeds for Security



Topic 1: PKI in OT

Possible questions to be answered:
How do Public Key Infrastructures work in OT environments? What are challenges and attack vectors?

Literature to start from:

- Mixed Certificate Chains for the Transition to Post-Quantum Authentication in TLS 1.3
  https://eprint.iacr.org/2021/1447.pdf
- 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
- Secure Device Identifiers and Device Enrollment in Industrial Control System
  https://ieeexplore.ieee.org/abstract/document/9118131

Topic 2: Trust Anchors in OT

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 a minimum of manual effort?

Literature to start from:

- 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
- 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

Topic 3: Post-quantum cryptography for OT

Possible questions to be answered:

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

Literature to start from:

- 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
- 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

Topic 4: Remote Control for Safety-Critical OT

Possible questions to be answered:
What are security aspects and concepts for remote control of safety-critical OT applications? What are the interactions between safety and security in the OT context?

Literature to start from:

- Safety of Unmanned Ships
  https://aaltodoc.aalto.fi/handle/123456789/28061
- Dam-Safety
  https://www.jstage.jst.go.jp/article/jdr/16/4/16_607/_article/-char/ja/
- Federated Remote Labs
  https://link.springer.com/chapter/10.1007/978-3-030-52575-0_2

Topic 5: Secure and Usable Authentication for OT

Possible questions to be answered:
Which authentication procedures are best to be used in an OT context? Which authentication procedures cannot be used with regard to OT and why? What about their performance, usability, robustness, and maturity? Which influence does the OT environment have?

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: 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? What would an ideal OT logging protocol look like?

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 7: IDS/IPS for OT

Possible questions to be answered:

How do IDS/IPS work in OT environments? How effective are they 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 8: Secure Communication Protocols - OPC UA/MQTT

Possible questions to be answered:
What are the security aspects and concepts of OPC UA and MQTT? What are the weak points and how could they be exploited? How can secure communication be scaled up in OT?

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 9: OT Datasets

Possible questions to be answered:
Which OT datasets exist? What are useful aspects of them, especially with regard to machine learning? What requirements can be derived for an optimal OT dataset?

Literature to start from:

- Datasets are not Enough: Challenges in Labeling Network Traffic
  https://www.sciencedirect.com/science/article/pii/S0167404822002048
- Dataset of anomalies and malicious acts in a cyber-physical subsystem
  https://www.sciencedirect.com/science/article/pii/S2352340917303402
- A Survey on Industrial Control System Testbeds and Datasets for Security Research
  https://ieeexplore.ieee.org/abstract/document/9471765
- Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions
  https://ieeexplore.ieee.org/abstract/document/9646172
- SWaT Dataset
  https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/

Topic 10: Secure PLC Programming

Possible questions to be answered:
How to securely develop programs for OT devices? What are similarities and differences to IT development? How do development techniques differ?

Literature to start from:

- Software security: Application-level vulnerabilities in SCADA systems
  https://ieeexplore.ieee.org/abstract/document/6009603
- Programmable logic controllers based systems (PLC-BS): vulnerabilities and threats
  https://link.springer.com/article/10.1007/s42452-019-0860-2
- Awareness of Secure Coding Guidelines in the Industry - A First Data Analysis
  https://ieeexplore.ieee.org/abstract/document/9343011
- Employing secure coding practices into industrial applications: a case study
  https://link.springer.com/article/10.1007/s10664-014-9341-9
- Top 20 Secure PLC Coding Practices
  https://plc-security.com/content/Top_20_Secure_PLC_Coding_Practices_V1.0.pdf

Topic 11: OT Hardware-in-the-loop Testbeds for Security

Possible questions to be answered:
Which approaches for hardware-in-the-loop testbeds in the context of OT security exist? What are their main purposes? Which kind of OT components can be tested employing these testbeds? What are their key differences?

Literature to start from:

- Evaluating the Effects of Cyber-Attacks on Cyber Physical Systems using a Hardware-in-the-Loop Simulation Testbed
  https://ieeexplore.ieee.org/abstract/document/8088669
- Enabling multi-layer cyber-security assessment of Industrial Control Systems through Hardware-In-The-Loop testbeds
  https://ieeexplore.ieee.org/abstract/document/7428063

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

otsecseminar@aisec.fraunhofer.de

Address: Fraunhofer AISEC
Lichtenbergstr. 11
85748 Garching
Germany

Internet: www.aisec.fraunhofer.de