SEMINAR: OPERATIONAL TECHNOLOGY SECURITY SS23
PRE-COURSE MEETING 07.02.2023

Michael Heinl, Sebastian Peters, Nikolai Puch, Veronique Ehmes

Fraunhofer AISEC

© Fraunhofer

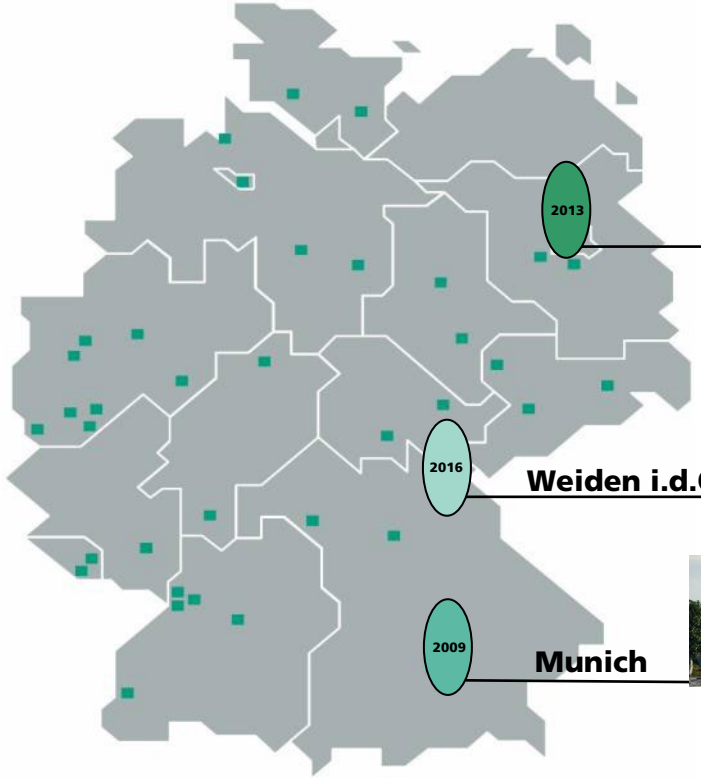
SEMINAR: OPERATIONAL TECHNOLOGY SECURITY PRE-COURSE MEETING

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

© Fraunhofer

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 €

© Fraunhofer

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

© Fraunhofer

Orga

- Online
  - TUM Moodle
  - Video Calls via MS Teams
- Up to 10 students
  - Individual work (no groups)
  - No qualification challenge, but
  - Higly recommended: **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!

© Fraunhofer

Deliverables

- Draft Paper and Final Paper
  - Systematization of Knowledge (SoK)
  - ~10 pages excl. list of references and appendices
  - IEEE conference proceedings template
  - Utilization of LaTeX (highly recommended)
- Kick-Off Meeting
- Reviews, Rebuttal
- Presentation
  - MS Powerpoint or similar
  - 25 minutes presentation, 15 minutes discussion
  - Submission of slides in advance

© Fraunhofer

Process (1/4)

- 07.02.2023 (today)
  - Organizational information
  - Overview on topics
- 09.02.2023 – 14.02.2023
  - Registration via DocMatching: http://docmatching.in.tum.de/
  - Motivational email to otsecseminar@aisec.fraunhofer.de
- 23.02.2023
  - Automated assignment of courses
- Until 05.03.2023
  - Please send us your three preferred topics via email

© Fraunhofer

Process (2/4)

- Until 10.03.2023
  - Response from organizers with assigned topic
  - Possibility to withdraw without penalty - non-attendance after this point is graded with 5.0
- 11.03.2023 – 23.04.2023
  - Familiarize with literature
  - Diving deep into your topic
  - As soon as possible: Schedule a kickoff meeting with your supervisors – **obligatory**!
- 24.04.2023 – 21.05.2023
  - Preparation of the draft version of the paper
  - Submission of the draft is **obligatory**!

© Fraunhofer

Process (3/4)

- Until 23.05.2023
  - Assignment of two of your fellow students' paper for review
- 24.05.2023 – 04.06.2023
  - Preparation of written review of these papers
- 05.06.2022 – 11.06.2022
  - Rebuttal period
- 12.06.2022 – 02.07.2022
  - Preparation of the final paper
  - Revision based on reviews/rebuttal

© Fraunhofer

Process (4/4)

- 03.07.2023 – 09.07.2023
  - Slide preparation
- Until 14.07.2023
  - Comments on the slides from supervisor
- 15.07.2023 – 19.07.2023
  - Revision of slides
- 20./21.07.2023
  - 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**

© Fraunhofer

Grading

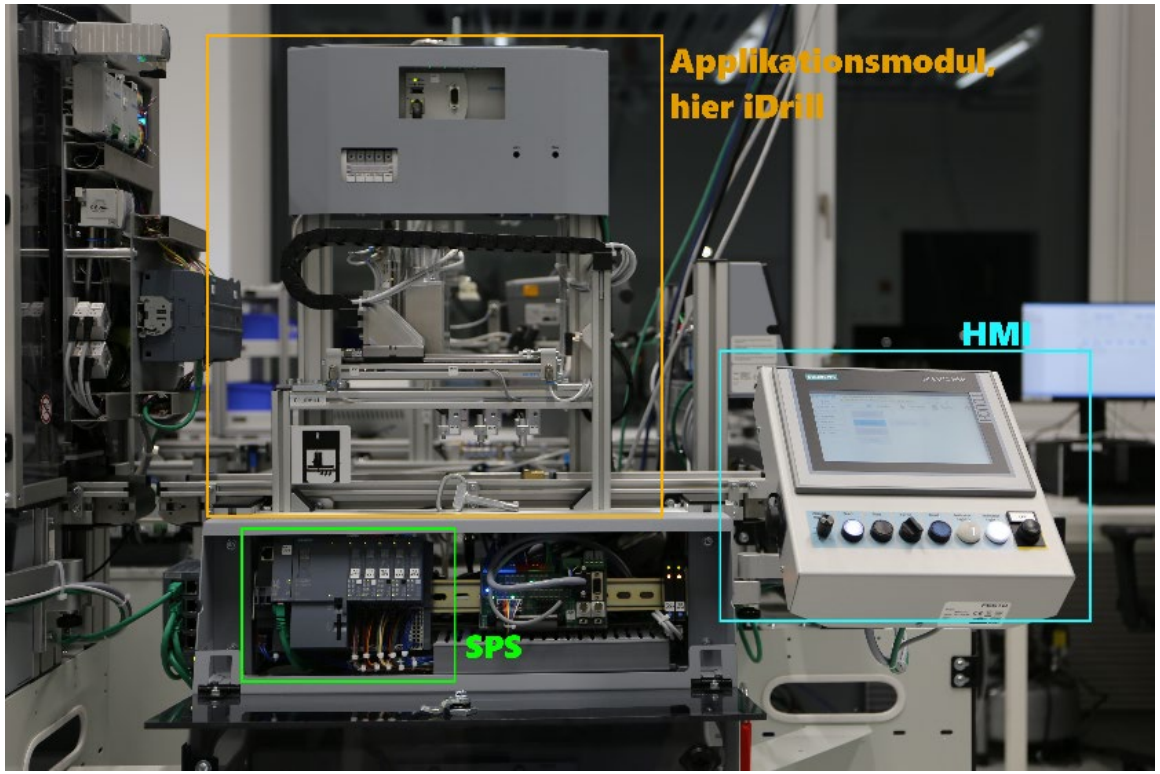
- **50 %** Final Paper
- **40 %** Presentation
- **5 %** Peer Reviews
- **5 %** Discussion Participation

Σ 100 % Total

© Fraunhofer

Topics (Overview)

1. Trust Anchors in OT
2. Remote Control for Safety-Critical OT
3. OT Authentication Usability
4. OT Logging
5. OT Datasets
6. Secure PLC Programming
7. OT Hardware-in-the-loop Testbeds for Security
8. Continuous authentication in OT
9. History of authentication in OT
10. Post-quantum cryptography for OT



© Fraunhofer

Topic 1: 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:

- Hardware Rooted Trust for Additive Manufacturing
  https://ieeexplore.ieee.org/abstract/document/8737928
- 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

© Fraunhofer

Topic 2: 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? What standards or recommendations are there for remote control and remote acknowledgement, especially to protect workers on machines?

Literature to start from:

- HSE and Cyber Security in Remote Work
  https://ieeexplore.ieee.org/abstract/document/9478249
- 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

© Fraunhofer

Topic 3: OT Authentication Usability

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

© Fraunhofer

Topic 4: OT Logging

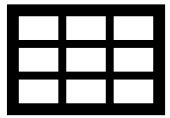
Possible questions to be answered:
What logging solutions and protocols exist for OT environments? How secure are they? Do they need any special precautions? How important is logging? What solutions exist for aggregating data from different event sources? What would an ideal OT logging protocol look like? How important is a common time source and how can synchronous time be established?

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

© Fraunhofer

Topic 5: OT Datasets



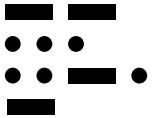
Possible questions to be answered:
Which OT datasets exist? What are useful aspects of them, especially with regard to machine learning? What requirements can be derived for an optimal OT dataset?

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/

© Fraunhofer

Topic 6: 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
- Empirical Study of PLC Authentication Protocols in ICS - https://ieeexplore.ieee.org/abstract/document/9474296
- Walking under the ladder logic: PLC-VBS: a PLC control logic vulnerability scanning tool https://www.sciencedirect.com/science/article/pii/S0167404823000263
- Top 20 Secure PLC Coding Practices - https://plc-security.com/content/Top_20_Secure_PLC_Coding_Practices_V1.0.pdf

© Fraunhofer

Topic 7: OT Hardware-in-the-loop Testbeds for Security

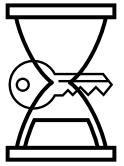
Possible questions to be answered:
Which approaches for hardware-in-the-loop testbeds in the context of OT security exist? What are their main purposes? Which kind of OT components can be tested employing these testbeds? What are their key differences?

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
- A Hardware-in-the-Loop Water Distribution Testbed Dataset for Cyber-Physical Security Testing https://ieeexplore.ieee.org/abstract/document/9526562
- Hardware-in-the-Loop CPS Security Architecture for DER Monitoring and Control Applications https://ieeexplore.ieee.org/abstract/document/9042578
- Enabling multi-layer cyber-security assessment of Industrial Control Systems through Hardware-In-The-Loop testbeds https://ieeexplore.ieee.org/document/7428063
- Hardware-in-the-Loop Testbed for Cyber-Physical Security of Photovoltaic Farms https://ieeexplore.ieee.org/abstract/document/9494258

© Fraunhofer

Topic 8: Continuous authentication in OT



Possible questions to be answered:
Which approaches exist, to bring continuous authentication to OT? What would be the advantages? Which variants of continuous authentication are best suited? What about the performance, usability, robustness, and maturity? Which influence does the OT environment have?

Literature to start from:

- Advanced Device Authentication: Bringing Multi-Factor Authentication and Continuous Authentication to the Internet of Things http://personales.upv.es/thinkmind/dl/conferences/cyber/cyber_2016/cyber_2016_4_20_80029.pdf
- On the Applicability of Users' Operation-action Characteristics for the Continuous Authentication in IIoT Scenarios - https://ieeexplore.ieee.org/abstract/document/9353805
- Passive User Authentication Utilizing Two-Dimensional Features for IIoT Systems https://ieeexplore.ieee.org/abstract/document/9971753
- Towards a Lightweight Continuous Authentication Protocol for Device-to-Device Communication https://ieeexplore.ieee.org/abstract/document/9343112

© Fraunhofer

Topic 9: History of Authentication in OT

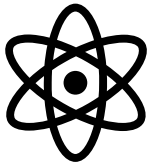
Possible questions to be answered:
How has authentication in OT developed over the years? Which methods have been added? Which ones are not pursued any further? How have recommendations changed over the years (length of passwords, regular changing of passwords, use of MFA, use of EC, ...)? Which standard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

Literature to start from:

- BSI ICS-Security-Kompendium (2013) and later/related recommendations, Link
- NIST Guide to Industrial Control Systems (ICS) Security (Rev1 2013, Rev2 2015)
- ISA/IEC 62443 *Industrial communication networks – Network and system security (revs from 2009-2020),* Link
- 'Why Johnny can't encrypt' – series of papers
- Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications https://ieeexplore.ieee.org/abstract/document/8675176
- Empirical Study of PLC Authentication Protocols in Industrial Control Systems https://ieeexplore.ieee.org/abstract/document/9474296

© Fraunhofer

Topic 10: 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

© Fraunhofer

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

Fraunhofer AISEC

© Fraunhofer