SEMINAR: OT SECURITY
PRE-COURSE MEETING 29.01.2020

Alexander Giehl, Patrick Wagner, Michael Heinl

{alexander.giehl | patrick.wagner | michael.heinl}@aisec.fraunhofer.de

Fraunhofer
AISEC

About Fraunhofer AISEC

- Head: Prof. Dr. Claudia Eckert, Prof. Dr.-Ing. Georg Sigl
- Employees: > 120
- Research and Development:
  - Embedded Security, Smartcard & RFID Security
  - Product Protection & Industrial Security
  - Cloud & Service Security
  - Network Security
  - Automotive Security
  - Smart Grid & CPS
  - Security Evaluation
  - Security Engineering

Fraunhofer AISEC

General Information

- Type of course
  - Master Seminar
  - 5.0 ECTS
  - Module in „Distributed Systems, Networks and Security“
  - Course at Chair for IT Security, I20 (Prof. Eckert)
- Requirements
  - Knowledge of lecture „IT Sicherheit“

Process

- 29.01.2020 (today)
  - Organizational information
  - Topic presentation
- From 07.02.2020 to 12.02.2020
  - Registration via DocMatching (http://docmatching.in.tum.de/)
- 20.02.2020
  - Automated assignment of courses
- Until 02.03.2020
  - Please send us your three preferred topics via email
  - You may add a letter of motivation to emphasize your top choice
  - Alternatively: Possibility to withdraw without penalty
  - Non-attendance after this point is graded with 5.0

Process

- Until 11.03.2020
  - Response from organizers with assigned topic
- 11.03.2020 - 17.04.2020
  - Schedule kickoff meeting with the supervisor at Fraunhofer AISEC
- 11.03.2020 - 13.05.2020
  - Preparation of the (final) draft version of the written report
    - Language: English
    - Format: Latex (LNCS Style), 8-10 pages
  - Delivery of the draft written report until 9:00 at 13.05.2020

Process

- 13.05.2020 - 27.05.2020
  - Review of two written reports
    - Similar to the review process of a scientific conference
    - Using a given review form
    - Evaluation of two written reports
    - Delivery of the reviews until 9:00 at 27.05.2020
- 27.05.2020 - 17.06.2020
  - Preparation of the final written report
  - Revision on the basis of three reviews (two from students, one from the supervisor)
  - Delivery of the final written report until 9:00 at 17.06.2020

Process

- 17.06.2020 - 24.06.2020
  - Slide preparation
  - Delivery to the organizers until 9:00 at 24.06.2020
- Until 01.07.2020
  - Comments on the slides from the supervisor
- 01.07.2020 - 07.07.2020
  - Revision of slides (if necessary)
  - Delivery of final slides to the organizers until 9:00 at 07.07.2020
- 08.07.2020 + 09.07.2020
  - Oral presentations (at Fraunhofer AISEC, room *Claude E. Shannon*)
  - Both sessions are expected to begin at 10:00 and will end at 16:00
  - Length of each presentation 30 minutes + up to 15 minutes discussion

Process

- Any time
  - Questions to the supervisor via email
  - Face-to-face meetings (appointment via email)

Grading

- Final grade consists of:
  - Draft version of the written report (30%)
  - Reviews (15%)
  - Final version of the written report (20%)
  - Presentation (25%)
  - Discussion (10%)

Topics (Overview)

1. Differences and Challenges of IT/OT
2. Current State and Recent Developments of Security in OT
3. A Survey on Industrial Security Management Guidelines for SMEs
4. A Survey on Risk Analysis Methodologies Suitable for OT in SMEs
5. Industrial Security Maturity Model for SMEs
6. Intrusion Detection in OT Environments
7. Digital Forensics and Incident Response in OT Environments
8. The Role of OT in the Context of Critical Infrastructure Protection
9. Infiltration and Exfiltration Techniques for Air-Gapped OT Environments
10. Analysis of and Mitigation Strategies for Real World OT Security Incidents

Topics

1. Differences and Challenges of IT/OT
   - Comparatively introduce the basics of IT and OT
     - Where are they used?
     - What are their main objectives and challenges?
     - Which protocols are used?
   - Discuss the relationship of OT and other commonly used terms in the field such as ICS, SCADA, PLCs etc.
   - Describe how IT and OT are interconnected
     - Outline how they converged over time
     - What are the security implications of such a convergence?

Topics

2. Current State and Recent Developments of Security in OT
   - Provide on overview of security mechanisms integrated into protocols used in OT
   - Conduct an analysis of missing security mechanisms and how OT operators can realize them nevertheless (e.g. authentication)
   - Develop a reference architecture of a typical OT setup
     - The reference architecture should be based on one or more business cases/specific examples
     - Provide an evaluation of security-critical aspects in this reference architecture
     - Sketch possible improvements in regards to security to this architecture

Topics

3. A Survey on Industrial Security Management Guidelines for SMEs
   - Perform a literature review and address:
     - Challenges for SMEs concerning industrial security management
     - Suitability of existing industrial security management guidelines for SMEs
     - Gaps and future research directions

Topics

4. A Survey on Risk Analysis Methodologies Suitable for OT in SMEs
   - Perform a literature review and address:
     - Challenges for SMEs concerning risk analyses on OT
     - Suitability of existing risk analysis methodologies for OT in SMEs
     - Gaps and future research directions

Topics

5. Industrial Security Maturity Model for SMEs
   - Develop an industrial security maturity model for SMEs
     - Define industrial security maturity levels
     - Define focus areas and groups
     - Derive requirements for SMEs to reach those levels from existing standards and scientific literature

Topics

6. Intrusion Detection in OT Environments
   - Provide a short introduction of the different general types of intrusion detection systems (IDS) and how they work
   - What are the challenges of applying “traditional” IDS to OT?
   - Develop a specific scenario in which an attacker tries to compromise an OT environment
     - What could be possible entry points?
     - Which attack techniques could be used?
     - How could the attack be detected?
     - What could be done after an attack has been detected?

Topics

7. Digital Forensics and Incident Response in OT Environments
   - Provide a short introduction of the general principles of digital forensics and incident response
     - What are their underlying principles, methods, and procedures?
     - Describe the concept of attribution and its main challenges
   - What could be typical challenges forensic analysts and incident responders experience in OT environments?
   - Develop a specific scenario in which an attacker has successfully compromised an OT environment
     - How can methods of digital forensics and incident response help to detect the attack?
     - How to scope the extent and origin of the attack?
     - How can compromised systems be recovered?

Topics

8. The Role of OT in the Context of Critical Infrastructure Protection
   - Provide an introduction to critical infrastructures
     - What are critical infrastructures?
     - What are their specific security requirements?
     - Where are those requirements defined?
   - Describe the relation between OT and critical infrastructures
   - Outline two real-world attacks on critical infrastructures and their respective impact

Topics

9. Infiltration and Exfiltration Techniques for Air-Gapped OT Environments
   - Introduce the idea of air gapping
     - How does it work?
     - What are typical environments in which this method is used?
   - Describe techniques enabling external attackers to interact with systems despite an existing air gap (infiltration)
   - Describe techniques which allow to extract data from air-gapped systems (exfiltration)
   - Develop a specific scenario in which an attacker uses a specific infiltration technique to compromise an air-gapped system
     - How could data be exfiltrated subsequently?
     - What are possible mitigation techniques?

Topics

10. Analysis of and Mitigation Strategies for Real World OT Security Incidents
    - Provide a comparative overview of security-related real-world attacks on OT environments
        - Which types of attack techniques have been used?
        - Which attacker has the attack been attributed to?
        - What did they probably try to achieve with the attack?
            - Have they been successful or not?
            - Why did the attack fail or succeed?
        - What was the impact of the attack?
        - How did the OT operators react?
    - Discuss one of the attacks in detail (step-by-step from the attacker's point of view) and outline how it could have been mitigated

Contact

Alexander Giehl
Patrick Wagner
Michael Heinl

Fraunhofer AISEC
Lichtenbergstr. 11
85748 Garching (bei München)

E-Mail:
{alexander.giehl | patrick.wagner | michael.heinl}
@aisec.fraunhofer.de

Internet:
http://www.aisec.fraunhofer.de

Fraunhofer AISEC