SEMINAR: SECURITY IN AUTOMOTIVE AND INDUSTRIE 4.0

INTRODUCTORY MEETING 01.02.2018

Alexander Kiening, Alexander Giehl

{alexander.kiening | alexander.giehl}@aisec.fraunhofer.de

Fraunhofer

AISEC

About Fraunhofer AISEC

- Head: Prof. Dr. Claudia Eckert, Prof. Georg Sigl
- Employees: 70
- Research and Development:
  - Embedded Security, Smartcard & RFID Security
  - Product Protection
  - Cloud & Service Security
  - Network Security
  - Automotive Security
  - Smart Grid & CPS
  - Security Evaluation
  - Security Engineering

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

- 01.02.2018 (today)
  - Organizational information
  - Topic presentation and assignment of preferred topics
- From 09.02.2018 to 14.02.2018
  - Registration via DocMatching (http://docmatching.in.tum.de/)
- 21.02.2018
  - Automated assignment of courses
- Until 23.02.2018
  - Possibility to withdraw from the seminar
  - Not attendance after this point is graded with 5.0
- Until 15.03.2018
  - Response from organizers with assigned topic

Process

- 15.03.2018 - 26.04.2018
  - Kickoff meeting with the supervisor at Fraunhofer AISEC
- 15.03.2018 - 30.05.2018
  - Preparation of the (final) draft version of the written report
    - Language: English
    - Format: Latex (LNCS Style), 15-20 pages
  - Delivery of the draft written report until 9:00 at 30.05.2018

Process

- 30.05.2018 - 08.06.2018
  - 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 08.06.2018
- 09.06.2018 - 18.06.2018
  - 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 18.06.2018

Process

- 18.06.2018 - 22.06.2018
  - Slide preparation
  - Delivery to the organizers until 9:00 at 22.06.2018
- Until 25.06.2018
  - Comments on the slides from the supervisor
- 26.06.2018 - 05.07.2018
  - Revision of slides (if necessary)
  - Delivery of final slides to the organizers until 9:00 at 05.07.2018
- 06.07.2018
  - Oral presentations (room 01.08.033)
  - Length (25 minutes + 5 minutes discussion)
  - Additional details will be given later

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. Security incidents in automotive
2. Security incidents in industry
3. Security protocols and the OSI stack
4. Security in Industrial Ethernet protocols
5. Comparison of hardware security modules
6. Secure multicast communication
7. Automotive operating systems
8. Security in internal industrial networks
9. Security in external industrial networks
10. [Student topics]

Topics

1. Security incidents in automotive
    - Provide on overview of security-related attacks on automotive components
        - Which types of attacks have been executed?
        - Which approach did the individual attackers take?
        - What did they 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 OEMs react?
    - Give two detailed discussions of individual attacks
        - Provide a possible security solution to prevent this attacks in the future

Topics

2. Security incidents in industry
   - Provide on overview of security-related attacks on industrial facilities/components
     - Which types of attacks have been executed?
     - Which approach did the individual attackers take?
     - What did they 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 plant/factory operators react?
   - Give two detailed discussions of individual attacks
     - Provide a possible security solution to prevent this attacks in the future

Topics (Overview)

3. Security protocols and the OSI stack
   - Introduction to security protocols
     - TLS
     - MACsec
     - IPsec
     - other relevant protocols?
   - Provide a comparison of advantages/disadvantages across OSI stack layers
     - Focus on security and security-related features
   - Give an evaluation of security protocols in regard to their usage in embedded systems
     - Focus on the automotive and/or industrial domain

Topics (Overview)

4. Security in Industrial Ethernet protocols
   - Provide an introduction to Industrial Ethernet protocols
     - Powerlink
     - Profinet
     - Ethercat
     - etc.
   - Compare the advantages/disadvantages of the researched protocols
   - Discuss the relevance of the protocols in industrial use cases
     - Possible application areas, market share, etc.
   - Perform an evaluation of security in these Industrial Ethernet protocols
   - Sketch possible improvements in regards to security

Topics (Overview)

5. Comparison of hardware security modules
   - Provide an overview of different HSMs
     - Different standards and implementations
       - Trusted Platform Module (TPM), and many more
   - Compare the features of the researched HSMs
   - Develop or use an existing taxonomy for HSMs
   - Provide an evaluation towards the usage of the researched HSMs in regard to their application in automotive and industrial use cases
     - Are there any automotive/industrial components deployed with HSMs?
     - What are the possible use cases for HSMs?
     - etc.

Topics (Overview)

6. Secure multicast communication
   - Introduce the problem of secure multicast communication
   - Provide an overview of possible techniques for secure multicast communication
     - Are there any reference implementations or real world use cases available?
   - Sketch use cases in respect to automotive and industrial settings for secure multicast
   - Evaluate the researched secure multicast techniques towards their application in automotive and industrial settings

Topics (Overview)

7. Automotive operating systems
   - Provide an overview on automotive operating systems and their security related features
     - QNX
     - AUTOSAR Classic and Adaptive Platforms
     - and other relevant OSs
   - Perform an evaluation of the researched OSs in regards to their security features
   - Sketch possible attacks on these OSs and provide an outline for improvements

Topics (Overview)

8. Security in internal industrial networks
   - Provide an overview on the industrial communication stack
     - “Automation pyramid” (ERP, MES, SCADA, SPS, I/O layers)
   - Develop a reference architecture of a typical automation setup within a factory
     - 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 (Overview)

9. Security in external industrial networks
   - Provide an overview on business cases facilitating interconnection along the value chain
   - Develop a reference architecture of a typical automation setup within a factory
     - The reference architecture should be based on one or more business cases and should provide specific examples
   - Sketch how to implement a secure connection of factories with each other
   - Evaluate possible approaches towards the protection value they provide and towards their feasibility in respect to the provided business cases/examples

Topics (Overview)

10. [Student topics]
    - Possibility to provide your own suggestions for topics
    - The suggested topics need to
        - be focused on security
        - in the domains automotive or automation/manufacturing
            - or related areas in which case a motivation needs to be provided why this area is chosen
        - and cannot be solely literature research
    - Topics suggestions via email prior to registration via DocMatching
        - If you suggested topic has not been approved by the supervisors, no claim on this topic is provided by us

Contact

Alexander Kiening
Alexander Giehl

Fraunhofer AISEC
Parkring 4
85748 Garching (bei München)

E-Mail: alexander.kiening@aisec.fraunhofer.de
alexander.giehl@aisec.fraunhofer.de
Internet: http://www.aisec.fraunhofer.de