SEMINAR: AUTOMOTIVE SECURITY
INTRODUCTORY MEETING JAN 23. 2014

Dr. Christoph Krauß, Alexander Kiening, Alexander Giehl
{christoph.krauss | alexander.kiening | alexander.giehl}@aisec.fraunhofer.de
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
  - IT Early Warning
  - Smart Grid & CPS
  - Security Evaluation
General Information

- **Type of course**
  - Master Seminar
  - 2 SWS / 4,0 ECTS
  - Module in „Verteilte Systeme, Rechnernetze, Sicherheit“
  - Course at Chair for IT Security, I20 (Prof. Eckert)

- **Requirements**
  - Knowledge of lecture „IT Sicherheit“
Process

- 23.01.2014 (today)
  - Organizational information
  - Topic presentation
  - Process topic assignment
- until 21.02.2014
  - Application Email (cf. slide 10)
- 26.02.2014
  - Response from organizers
- Until 28.04.2014
  - Possibility to withdraw from the seminar
## Process

  - Kickoff meeting with the supervisor at Fraunhofer AISEC

- **26.02.2014 - 27.05.2014**
  - Preparation of the (final) draft version of the written report
    - Language: Englisch
    - Format: Latex (LNCS Style), 15-20 pages
  - Delivery of the draft written report until 9:00 at 28.05.2014
Process

28.05.2014 - 08.06.2014
- Review of two written reports
  - Similar to the review process of a scientific conference (Submission via easychair, Link will be posted on the seminar webpage)
  - Using a given review form
  - Evaluation of two written reports
  - Delivery of the reviews until 9:00 at 09.06.2014

09.06.2014 - 15.06.2014
- 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 16.06.2014
Process

- 16.06.2014 - 22.06.2014
  - Slide preparation
  - Delivery to the organizers until 9:00 at 23.06.2014
- 23.06.2014
  - Comments on the slides from the supervisor
- 25.06.2014
  - Revision of slides (if necessary)
- 26.06./27.06.2014
  - Oral presentations (room 01.06.011)
  - 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%)
Application / Topic Assignment

- EMail with the following information until 9:00 at 21.02.2014
  - Name and matriculation number
  - E-Mail
  - Program
  - Semester
  - Visited IT-Security lectures
  - Three preferred topics
  - Short motivation why you want to attend the seminar

- to christoph.krauss@aisec.fraunhofer.de and alexander.kieining@aisec.fraunhofer.de and alexander.giehl@aisec.fraunhofer.de
Topics (Overview)

- Secure Car2X Communication (Supervisor: TBD)
- Privacy-preserving C2X Communication (Supervisor: TBD)
- Secure Internal Vehicle Communication (Supervisor: TBD)
- Secure Operating Systems for Vehicles (Supervisor: TBD)
- Hardware-Security for Vehicles (Supervisor: TBD)
- Access Control Systems for Vehicles (Supervisor: TBD)
Secure Car2X Communication

Supervisor: TBD

- Vehicles communicate via different interfaces with other vehicles, Road Side Units (RSU), etc.

- Task
  - What applications result for Car2Car (C2C), Car2Infrastructure (C2I) communication?
  - Which technologies are applicable for this?
  - What threats except for privacy result from this?
  - What are the challenges for securing Car2X communication?
  - What are possible security solutions?
  - Results of IEEE 1609.2, C2C-CC, Network on Wheels project, simTD project, SeVeCom project etc.?
Movement profiles are easily generated due to communication with the outside world

Challenge: Ensuring the privacy and anonymity of the vehicle and the vehicle owner

Task

What threats in regard to privacy arise due to C2X communication?
Which mechanisms are employable?
How could possible security solutions look like?
What security problems arise?
Secure Internal Vehicle Communication

Supervisor: TBD

- Vehicles employ different bus technologies like CAN, FlexRay, Ethernet, LIN, MOST, etc.
- Possibilities for attacks on the internal network arise by opening up the vehicle’s network to the outside
- Task
  - What security problems exist within the employed bus technologies?
  - Which threats / attack vectors exist?
  - What countermeasures are applicable?
Increasing employment of standard software architectures and operating systems in vehicles (e.g., QNX, Android, AUTOSAR OS, Linux)

Task

- Which software architectures exist?
- What are their properties?
- Which IT security measures do they include?
- How secure are these measures?
Attacks often have full physical access (e.g., vehicle owner, workshop) and are able to execute offline attacks.

Tamper-proof hardware offers secure key storage, a secure execution environment, detection of falsified components, etc.

Task

- What are promising approaches for employment in vehicles (e.g., TPM, SHE-Module, EVITA-HSM, Freescale MPC56xx, PUFs)?
- What is achievable with tamper-proof hardware?
- What problems can be solved by it?
- How do concrete security solutions look like?
Access Control Systems for Vehicles

Supervisor: TBD

- Access control systems for vehicles: Radio remote control for opening doors, immobilizer

- Task
  - What challenges have to be met?
  - What problems need to be solved?
  - What approaches exist (keeloq, DST40, Hitag-2)?
  - What are the advantages?
  - What are the disadvantages?
Contact

Dr. Christoph Krauß
Alexander Kiening
Alexander Giehl

Fraunhofer AISEC
Parkring 4
85748 Garching (bei München)

E-Mail: christoph.krauss@aisec.fraunhofer.de
alexander.kiening@aisec.fraunhofer.de
alexander.giehl@aisec.fraunhofer.de

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