Name of the course: Security of Autonomous Systems	Total credits: 2+2+1=5

IPM-AUTESASEG

Type: Optional

Total hours of per semester:

lecture: 26
practice: 26
consultation: 13

Other: project

Type of testing: exam

Other: project, tests

Semester: 1, 2, 3, 4th

Description

Introduction to security analysis methods, including threat modelling and attack modelling both for cyber attacks, e.g. attacks on software or communication and for physical (or field) attacks, e.g. manipulation of sensor data, GPS signals etc. in autonomous systems. Cryptographic primitives, mathematical background and scope. Use of appropriate cryptographic tools in protocols. Overview of most important protocols used in networking, especially in the automotive industry. Overview of existing standards and recommendations on safety and security of autonomous driving systems.

Literature

Compulsory

- Niels Ferguson, Bruce Schneier, Tadayashi Kohno: Cryptography Engineering: Design Principles and Practical Applications. Wiley Publishing, 2010. ISBN: 0470474246

- Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography. Chapman & Hall/Crc Cryptography and Network Security Series, 2007. ISBN: 1584885513

Recommended

- William Stallings: **Cryptography and Network Security Principles and Practices.** Prentice Hall, 4th Edition, 2005. ISBN: 0131873164

Competencies

Knowledge

- Up-to-date knowledge of security protocols in security-intensive software systems
- Solid understanding of the basic cryptographic methods used in software systems.
- Understanding the security aspects of autonomous systems.
- Familiarity with the most important glossary terms of security and cryptography.

Competencies

- Ability to formalize threats that could affect the security of a complex system.
- Ability to formalize security requirements of a system with associated threats, risks and

mitigation efforts.

- Ability to participate in the design of a complex system with security-aware attitude.
- Expertise in the design, development, operation and management tasks in the domain of complex software systems and database management systems.
- Skills for cooperation and team work, and ability to take leading role.
- Ability for written and oral communication in English, using the technical terms and expressions of computer science. Ability to argue, to prepare reports, to read, understand and exploit scientific and technical material (e.g. books and papers).
- Expertise in utilizing sources of technical information, their critical interpretation and evaluation, and the extraction of information relevant to the solution of a specific problem.
- Ability to perform supervised scientific research, and skills required for post-graduate studies.

Attitude

- Attends professional, technological development related to their qualification.
- Commitment to critical feedback and self-assessment.
- Commitment to lifelong learning and receptivity to new IT competencies.
- Adopts and coordinates the ethical principles of work, organizational culture and research.
- Shares professional knowledge, mediates professional results.
- Mediates and implements eco-conscious behavior and social responsibility, helping them with IT tools.
- Commitment to quality standards and its IT tools.
- Open to initiate collaboration with IT and other specialists.

Autonomy and responsibility

- Takes responsibility for his professional decisions taken during his professional activities.
- Takes responsibility for observing and enforcing deadlines.
- Takes responsibility for own and fellow workers' work.
- In the case of operational critical IT systems, he/she can be assigned responsibility for development and operation, according to his/her professional competencies.