SYLLABUS

Name: ***IoT Security (InfAAu-IOT>SM1IOTS19)***
Name in Polish:
Name in English: ***IoT Security***

Information on course:

Course offered by department: Faculty of Automatic Control, Electronics and Computer Science
Course for department: Silesian University of Technology

Default type of course examination report:

EGZ

Language:

English

Course homepage:

https://platforma2.polsl.pl/rau2/course/view.php?id=969

Short description:

The objective of the course is to deliver to the students the latest and up-to-date knowledge on the internet of thinks security including risks, threats, attacks, and defensive activities. That includes theoretical and practical approaches.
• theoretical approach to the information security
• advanced aspects of the security during data transmission
• legal aspects of information security
• the impact of the security of the Internet of Things systems on the personal security
• analysis of the security of the Internet of Things systems

Description:

Lectures:

The aim of the course is to familiarize students with the current situation and the state of security of Internet of Things systems, to present attack vectors, classification of threats in terms of type and level, to present examples of cyber attacks on IoT systems and the resulting consequences for the entire system, to present the concept of security by design and preparation cybersecurity solutions at the system design stage, assessment of communication protocols in terms of vulnerability, the introduction of communication security elements and basic principles and methodology of encryption, familiarization with the holistic approach to cybersecurity in IoT systems designed to protect all key elements of such systems: users, devices and data.
Paying attention to the comprehensive security, creating and securing IoT systems.
Lecture supported by a multimedia presentation. Film materials available on the remote education platform.

Laboratories:
A set of tasks to be solved regarding creation of the secure IoT systems, hacking of the communication and systems (ethical).

Prerequisites:
Algorithmics, basics of networking, programming in C++, embedded systems, Arduio framework understanding.
Familiarity with basic development frameworks and tools, such as PlatformIO, Arduino IDE, Visual Studio Code is necessary.

ECTS: 4
Total: 100h (contact 50h / self study 50h)
Lecture 30h
Labs 15h
Other 5h
Self-study: self-paced learning via PZE, report writing, literature and documentation study

Bibliography:

[0] Piotr Czekalski, et al., "Advanced IoT Systems", preprint, https://iot-open.eu/advanced-iot-systems-coursebook/
[1] Ammar Rayes, Samer Salam, “The Things in IoT: Sensors and Actuators”, https://link.springer.com/chapter/10.1007/978-3-319-44860-2_3
[2] IEEE, “Towards a definition of the Internet of Things (IoT)”.
[3] McKinsey&Company, “The Internet of Things”, http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things
[4] ITU-T Y.2060, “Overview of the Internet of things”, https://www.itu.int/rec/T-REC-Y.2060-201206-I
[5] European Commission, “Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination”, https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination
[6] EPRS, Ron Davies, “Industry4.0”, http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf
[7] Tara Salman, “Networking Protocols and Standards for Internet of Things”, https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot.pdf
[8] ISO/IEC, “ISO/IEC CD 30141:20160910(E) - Internet of Things Reference Architecture (IoT RA)”, https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf
[9] https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/
[10] https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/
[11] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures
[12] https://www.enisa.europa.eu/publications/good-practices-recommendations
[13] https://www.enisa.europa.eu/publications/ics-scada-dependencies
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-atool-for-structuring-threat-information
[15] https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf
[16] https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices

Learning outcomes:

The student understands the theoretical foundations of security in IoT systems, including authentication, encryption, and access control mechanisms, and can explain how they relate to general principles of computer security. K2A_W03 (exam, labwork grade/report grade)

The student has in-depth knowledge of IoT-specific security threats (e.g. device spoofing, firmware attacks, side-channel attacks) and is familiar with advanced protection mechanisms tailored for resource-constrained IoT devices and networks. K2A_W06 (exam, labwork grade/report grade)

The student understands the legal and regulatory aspects of data privacy, cybersecurity policies.
K2A_W12 (exam)

The student can identify and critically discuss ethical and societal challenges related to IoT security, including surveillance, data ownership, digital inequality, and the balance between usability and privacy. K2A_W15 (exam)

The student is able to evaluate the security architecture of existing IoT solutions, identify vulnerabilities, and propose feasible improvements or redesigns, taking into account technical constraints and real-world applicability. K2A_U12 (exam, labwork grade/report grade)

Assessment methods and assessment criteria:

Lecture: Written exam, required 60% of the correct answers, to pass. Lectures are not compulsory.

Laboratories: The credit is obtained on the basis of graded reports from each of the laboratory exercises.
Attendance at laboratory classes is compulsory. Labwork is evaluated based on the work done and the report. Students need to ensure that the report for every laboratory taken has been accepted.

Positive grade requires passing of the on-line quizzes (PZE) for module M4 IoT Security.

Final grade is then calculated based on the weighted average of the exam (E) and laboratory work (L):

final grade = E*0.4 + L*0.6

The syllabus is valid from academic year 2025/2026 and its content cannot be changed during the semester.

Course credits in various terms:

Informatics, full-time master degree studies 3 sem. (InfAAu-SM3)

Type of credits	Number	First term	Last term
European Credit Transfer System (ECTS)	4	2020/2021-Z	