Ruhr Master School
of Applied Sciences

Dieses Wahlpflichtmodul ist ein Angebot der:

Fachhochschule Dortmund
University of Applied Sciences and Arts

Master Digital Transformation

Digital Systems 2

daniel.vonfalkenhayn@fh-dortmund.de

Prof. Dr. Ingo Kunold
kunold@fh-dortmund.de

Digital Systems 2 (MOD2-03)

Code Number	Workload	Credits	Semester	Frequency	Duration
48080/81	180 h	6	2	summer semester	1 Semester

	Course Title	Contact hours	Self-Study	Planned Group Size
1	Digital Systems 2	4 SWS / 60 h	120 h	25 students

2 Course Description

The module is expanding student competence to understand, analyze, develop, set up and evaluate digital systems based on the latest scientific state of the art. This involves mainly the topics security in cyber-physical systems (CPS) and operating systems. During the module, students will develop a security concept for the IoT devices from Digital Systems 1. Furthermore, they will structure an application with real-time requirements according to the operator controller module (OCM) and select an appropriate operating system for the device. Recent topics from research projects (e.g. smart grid, eMobility) complement the course with the aim to stimulate discussion of scientific results.

3 Course Structure

1. Introduction to internet security for CPS
2. Architectures for trusted platforms
3. Secure communication
4. Intrusion detection and advanced methods in CPS
5. Authentication, data protection and privacy and IoT systems
6. Introduction to the Operator-Controller-Module
7. Real-time processing
8. Operating systems (OS) and databases for embedded systems
9. Case study of a state-of-the-art application, e.g. smart grids

4 Application Focus

Project IoT System: students will the security system for the IoT system from the previous semester. Furthermore, they will implement an application with real-time aspects based on a selected operating system. The respective case study will be taken from a recent R&D project or an industry case. The result will be a demonstrator system.

Trainings: students attend a training for CPS security tools from Institute for Internet Security.

5 Scientific Focus

Students will do a scientific evaluation of the security issues in a specific domain (e.g. eMobility charging systems) based on recent scientific literature.

6 Parameters

- ECTS: 6
- Hours of study in total: 180
- Weekly hours per semester: 4

	– Contact hours: 60 – Self-Study hours: 120 • Course characteristics: compulsory • Course frequency: every year – summer semester • Maximal capacity: 25 students • Course admittance prerequisites: none • Skills trained in this course: theoretical knowledge, practical skills and scientific competences • Assessment of the course: Theoretical knowledge: Written Exam at the end of the course (50%) and Practical Skills: Individual programming task (50%): implementation of an IoT security system in device, communication and cloud level (e.g. based on Eclipse IoT stack) => demonstration of the result • Teaching staff: Prof. Dr. Ingo Kunold, staff from IKT institute, guest lecturers from joint research projects
7	**Learning outcomes** 7.1 Knowledge • Knows relevant theoretical foundations of internet security • Knows relevant architectures for trusted platforms • Knows relevant secure communication protocols • Know the theoretical background of the operator controller module (OCM) • Know methodical background of real time system design • Is aware of critical limitations of CPS security and real-time OS 7.2 Skills • Can develop a secure IoT system • Can implement real-time OS into IoT systems • Can apply state of the art tools for CPS security • Can select embedded OS according to system requirements 7.3 Competence – attitude • Can discuss CPS security issues with experts • Can lead cross domain design for IoT systems based on OCM • Understands the connections between cloud security and IoT security
8	**Teaching and training methods** • Theoretical knowledge: e-learning modules on IoT security and operating systems, tool tutorials • Practical Skills: Projects, Labs & Exercises, continuation of the small project with an IoT device, OSGi software architectures, Cloud systems and microservice architectures • Scientific Competences: own research on IoT security issues and, Semantic Web Technologies
9	**Course mapping** Input for: MOD-E09 - Smart Home & Smart Building & Smart City MOD-E10 - Edge Computing Input from: MOD1-03 – Digital Systems 1

10	**References**

10 References

<u>Basics & Practitioner</u>

Toby Segaran, Colin Evans, Jamie Taylor, Programming the Semantic Web, August 2009

Bob DuCharme, Learning SQARQL, 2nd Edition, Juli 2013

Herbert Schildt, Java: The Complete Reference, Eleventh Edition, December 2018

W3C, „Web of Things (WoT) Thing Description," 16 May 2019. [Online]. Available: https://www.w3.org/TR/wot-thing-description/.

W3C, „Web of Things (WoT) Security and Privacy Guidelines" 6 November 2019. [Online]. Available: https://www.w3.org/TR/wot-security/.

ETSI, „TS 103 264 V2.1.1 SAREF version 2 Technical Specification," [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103200_103299/103264/02.01.01_60/ts_103264v020101p.pdf.

OSGi Alliance Specifications, May 2017, [online] Available: https://www.osgi.org/developer/specifications/.

W3C, „RDF1.1 primer," [Online]. Available: https://www.w3.org/TR/rdf11-primer/.

Schema.org, „IoT Schema," [Online]. Available: http://iotschema.org/.

<u>Research (Examples for selected papers)</u>

S. Emerson, Y. Choi, D. Hwang, K. Kim and K. Kim, "An OAuth based authentication mechanism for IoT networks, "2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2015, pp. 1072-1074.

A. Prasetio, S. R. Akbar, B. Priyambadha, "Implementation of semantic system in the smart home lights device based on agent", IEEE 2017 International Conference on Sustainable Information Engineering and Technology (SIET), Nov. 2017

Y.-H. Son, K. C. Lee, "Cloud of things based on linked data", IEEE 2018 International Conference on Information Networking (ICOIN), April 2018

I. Kunold, H. Wöhrle, M. Kuller, N. Karaoglan, F. Kohlmorgen, J. Bauer, „Semantic Interoperability in Cyber-Physical Systems", The 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 18-21 September, 2019, Metz, France