Faculty of Information and Communication Technology/Department of Fundamentals of Computer Science

COURSE CARD

Name of the course in polish	:	**Systemy Wbudowane w Bezpieczeństwie Komputerowym**
Name of the course in english	:	**Embedded Security Systems**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	W04INA-SM4005G
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30		30		
The total number of hours of student workload (CNPS)	60		90		
Assesment	exam				
For a group of courses final course mark	X				
Number of ECTS credits	2		3		
including the number of points corresponding to the classes of practical (P)			3		
including the number of points corresponding occupations requiring direct contact (BK)	2		2		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

Fluency in programming, designing efficient algorithms, estimating computational complexity. Basic knowledge on computer systems architecture, operating systems and communication protocols and electronics.

COURSE OBJECTIVES

C1 presentation of architecture, limitations, functionalities and vulnerabilities of embedded systems in security area

C2 developing analysis skills of embedded systems, communication with them and conducting reverse engineering

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows design and architecture, programming and limits of embedded systems

W2 Knows communication standards used in embedded systems e.g. IrDA, UART, JTAG

W3 Knows basic principles and steps in embedded operating system analysis

W4 Knows specificity of embedded system vulnerabilities (side channel analysis, hardware-based trojans)

W5 Knows concept of SDR, programing GNU Radio and signal analysis

The student skills:

U1 Capability to conduct process of analysis of embedded system

U2 Capability to establish communication and conduct reverse engineering process of embedded system

U3 Capability to detect and exploit the vulnerabilities of embedded system

U4 Capability to design requirements for embedded system following security and privacy requirements

U5 Capability to program an Arduino microcontroller and communicate with peripherals

U6 Capability to utilize modules and protocols like IrDA, UART, SDR

The student's social competence:

K1 can design a system with respect to the expected social behaviour of its users

K2 can estimate the risk factor for a functioning system

K3 can create solutions oblivious to the end-user

K4 can estimate the potential of criminal activities

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to the embedded systems - reconnaissance	2h
Wy2	Hardware and software reverse engineering	6h
Wy3	Trusted Platform Module (TPM and Hardware Security Module (HSM)	2h
Wy4	Embedded systems vulnerabilities	2h
Wy5	Hardware-based trojans	2h
Wy6	Software Defined Radio (SDR)	2h
Wy7	GSM and SIM card	2h
Wy8	Automotive security	2h
Wy9	Physical Unclonable Functions (PUFs)	2h
Wy10	Side-channel attacks and analysis	4h
Wy11	Kleptography	2h
Wy12	Smart cards and modern ID documents	2h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	Assembling toolbox for working with embedded system	4h
Lab2	Establishing communication with embedded systems (e.g. UART)	4h
Lab3	Reverse engineering of selected embedded system	10h
Lab4	Remote analysis of embedded system vulnerabilities	6h
Lab5	Black-box embedded system analysis in a form of Arduino module	6h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Creating programming projects
5. Consultation
6. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W5, K1-K4	
F2	U1-U6, K1-K4	
P=%*F1+%*F2		

BASIC AND ADDITIONAL READING

1. Smart Card Handbook. Wolfgang Rankl, Wolfgang Effing, ISBN: 978-0-470-74367-6
2. Theoretical Aspects of Distributed Computing in Sensor Networks. Nikoletseas, Sotiris; Rolim, José, ISBN: 978-3-642-14848-4
3. Handbook of Sensor Networks. Yang Xiao, Hui Chen, Frank Haizhon Li, ISBN: 978-981-283-730-1
4. Embedded Systems Design with Platform FPGAs: Principles and Practices. Ronald Sass , Andrew G. Schmidt, ISBN:0123743338
5. Embedded Systems: A Contemporary Design Tool. James K. Peckol. ISBN: 0471721808
6. normative documents

SUPERVISOR OF COURSE

dr inż. Wojciech Wodo

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Systemy Wbudowane w Bezpieczeństwie Komputerowym
WITH LEARNING OUTCOMES IN THE FIELD OF ALGORITHMIC COMPUTER SCIENCE

Subject learning effect	Relating the subject effect to the learning outcomes defined for the field of study	Objectives of the course**	Program content**	Teaching tool number**
W1	K2_W01 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
W4	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
W5	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
U1	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U10 K2_U12	C2	Lab1-Lab5	3 4 5 6
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U10 K2_U12	C2	Lab1-Lab5	3 4 5 6
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U12	C2	Lab1-Lab5	3 4 5 6
U4	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U12 K2_U13	C2	Lab1-Lab5	3 4 5 6
U5	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U12 K2_U13	C2	Lab1-Lab5	3 4 5 6
U6	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U12 K2_U13	C2	Lab1-Lab5	3 4 5 6
K1	K2_K02 K2_K03 K2_K05 K2_K06 K2_K10 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab5	1 2 3 4 5 6
K2	K2_K02 K2_K07 K2_K08 K2_K09 K2_K10 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab5	1 2 3 4 5 6
K3	K2_K02 K2_K03 K2_K05 K2_K06 K2_K07 K2_K10 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab5	1 2 3 4 5 6
K4	K2_K03 K2_K05 K2_K07 K2_K09 K2_K10 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab5	1 2 3 4 5 6