Faculty of Fundamental Problems of Technology
COURSE CARD

Name in polish	:	**Bezpieczeństwo Systemów II**
Name in english	:	**System Security II**
Field of study	:	Computer Science
Specialty (if applicable)	:	
Undergraduate degree and form of	:	masters, stationary
Type of course	:	compulsory
Course code	:	E2_BI05
Group rate	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	15	15		
The total number of hours of student workload (CNPS)	30	30	30		
Assesment	exam				
For a group of courses final course mark	X				
Number of ECTS credits	1	1	1		
including the number of points corresponding to the classes of practical (P)		1	1		
including the number of points corresponding occupations requiring direct contact (BK)	1	1	1		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS
Passed 'Security I' course.

COURSE OBJECTIVES

C1 Introduction to the formal analysis of security of information systems. Discussion of security models, types of attacks, adversaries and scenarios. Presentation of theorem proving techniques in the field of security.

C2 Provide the skills to: a) analyze the correctness of security protocols, b) prove security properties of selected systems for different models of adversaries.

C3 Design and prototype selected cryptosystems.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows mathematical models of access control and risk analysis

W2 Knows adversary models and attack scenarios

W3 Knows techniques for security proofs

The student skills:

U1 Specify security requirements for given systems in chosen models

U2 Analyse and evaluate security of given systems in chosen models

U3 Synthesize new systems from secure building blocks

The student's social competence:

K1 Describe and analyse computer security problems in chosen theoretical models.

K2 Understand and can argue for the need of theoretical analysis of computer security.

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to formal models of computer system security.	1h
Wy2	Adversary models and attack scenarios.	1h
Wy3	Formal models of cryptosystems and protocols security.	1h
Wy4	Proving security via reduction techniques.	1h
Wy5	Secure Identification.	5h
Wy6	Security digital Signatures.	5h
Wy7	Authenticated Key Establishment.	5h
Wy8	Secure schemes on untrusted devices.	5h
Wy9	Sequence of games with the adversary.	5h
Wy10	The framework of Universal Composability.	1h
Type of classes - exercises		
Ćw1	Models.	1h
Ćw2	Proving security via reduction techniques.	8h
Ćw3	Proving security via sequence of games.	5h
Ćw4	Proving security in the UC Framework	1h
Type of classes - laboratory		
Lab1	Implementing a prototype of a chosen security protocol.	15h

Applied learning tools

1. Traditional lecture

2. Solving tasks and problems

3. Creating programming projects

4. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS		
Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W3, K1-K2	
F2	U1-U3, K1-K2	
F3	U1-U3, K1-K2	
P=%*F1+%*F2+%*F3		

BASIC AND ADDITIONAL READING
1. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols, Mihir Bellare and Phillip Rogaway 2. The Random Oracle Methodology Revisited, Ran Canetti, Oded Goldreich and Shai Halevi. 3. Abstract models of computation in cryptography, Ueli Maurer. 4. Universally Composable Security: A New Paradigm for Cryptographic Protocols, R. Canetti.

SUPERVISOR OF COURSE
dr inż. Łukasz Krzywiecki

RELATIONSHIP MATRIX EFFECTS OF EDUCATION FOR THE COURSE
System Security II
WITH EFFECTS OF EDUCATION ON THE DIRECTION OF COMPUTER SCIENCE

Course training effect	Reference to the effect of the learning outcomes defined for the field of study and specialization (if applicable)	Objectives of the course**	The contents of the course**	Number of teaching tools**
W1	K2_W01 K2_W02 K2_W04_B	C1	Wy1-Wy10	1 4
W2	K2_W01 K2_W02 K2_W04_B	C1	Wy1-Wy10	1 4
W3	K2_W01 K2_W02 K2_W04_B	C1	Wy1-Wy10	1 4
U1	K2_U01_B K2_U02 K2_U09_B K2_U12_B K2_U13 K2_U14	C2 C3	Ćw1-Ćw4 Lab1-Lab1	2 3 4
U2	K2_U01_B K2_U02 K2_U04 K2_U08_B K2_U09_B K2_U10 K2_U11 K2_U12_B K2_U13 K2_U14 K2_U15	C2 C3	Ćw1-Ćw4 Lab1-Lab1	2 3 4
U3	K2_U01_B K2_U02 K2_U04 K2_U09_B K2_U10 K2_U11 K2_U13 K2_U14	C2 C3	Ćw1-Ćw4 Lab1-Lab1	2 3 4
K1	K2_K01_B K2_K04 K2_K14_B K2_K15 K2_K16	C1 C2 C3	Wy1-Wy10 Ćw1-Ćw4 Lab1-Lab1	1 2 3 4
K2	K2_K01_B K2_K04 K2_K13 K2_K14_B K2_K15 K2_K16	C1 C2 C3	Wy1-Wy10 Ćw1-Ćw4 Lab1-Lab1	1 2 3 4