

STUDY MODULE DESCRIPTION FORM		
Name of the module/subject Information security in Internet		Code 1010335531010334336
Field of study Information Engineering	Profile of study (general academic, practical) (brak)	Year /Semester 2 / 3
Elective path/specialty Information Technologies	Subject offered in: Polish	Course (compulsory, elective) obligatory
Cycle of study: Second-cycle studies	Form of study (full-time, part-time) part-time	
No. of hours Lecture: 16 Classes: - Laboratory: 12 Project/seminars: -		No. of credits 5
Status of the course in the study program (Basic, major, other) (brak)		(university-wide, from another field) (brak)
Education areas and fields of science and art technical sciences		ECTS distribution (number and %) 5 100%
Responsible for subject / lecturer: dr inż. Tomasz Bilski email: tomasz.bilski@put.poznan.pl tel. 061 66 53 554 Faculty of Electrical Engineering ul. Piotrowo 3A 60-965 Poznań		
Prerequisites in terms of knowledge, skills and social competencies:		
1	Knowledge	Student has in-depth knowledge in the field of data security. He/she has in-depth knowledge of cryptography and basic in cryptanalysis.
2	Skills	Student can use advanced tools and information technologies.
3	Social competencies	Student understands the need to provide public information concerning the achievements in computer science and other aspects of business-computing engineer; he/she shall endeavour to provide information in a way understandable by presenting different points of view.
Assumptions and objectives of the course: Presentation of cryptographic protocols on the Internet.		
Study outcomes and reference to the educational results for a field of study		
Knowledge: 1. Student has knowledge concerning IT, their applications and related problems. - [K_W06] 2. Student has knowledge of the trends and the most important new developments in the field of computer science. - [K_W14]		
Skills: 1. Student can obtain information from literature, databases, and other sources; can integrate the information obtained, their interpretation and critical evaluation, and also draw conclusions and formulate and fully justify the feedback. - [K_U01] 2. Student is able to propose and justify improvements to existing solutions. - [K_U12]		
Social competencies: 1. Student is able to think and act in a way that is creative and enterprising - [K_K01]		
Assessment methods of study outcomes		
Written examination based on lecture. Laboratory: written test.		
Course description		

<p>Lecture</p> <p>Threats in networks, DoS attacks, security controls for networks, Standardization, TLS, IPsec (ESP, AH, ISAKMP, IKE), LDAP and OSCP, certification policy, cryptographic algorithms in access networks (GSM, UMTS, IEEE 802.11i).</p> <p>Course update 2017: IoT security, cloud security.</p> <p>Teaching methods:</p> <ul style="list-style-type: none"> - lecture with multimedia presentation, - additional topics available in Moodle course. <p>Laboratory</p> <p>SSL, TLS, S-HTTP protocols; Digital certificate; Public cryptographic system ? based on RSA, Communication security ? Secure Shell; Cryptographic algorithms in radio access networks</p>		
<p>Basic bibliography:</p> <p>1. Anderson R., Security Engineering, [online] http://www.cl.cam.ac.uk/~rja14/book.html</p>		
<p>Additional bibliography:</p> <p>1. Standards (ISO, IEEE)</p> <p>2. RFC</p>		
<p>Result of average student's workload</p>		
<p>Activity</p>	<p>Time (working hours)</p>	
1. Lecture	30	
2. Laboratory	15	
3. Preparation to the laboratory	15	
4. Realization of laboratory reports	10	
5. Preparation to tests	10	
6. Preparation to the examination	35	
7. Participation in the consultations and examination	10	
<p>Student's workload</p>		
<p>Source of workload</p>	<p>hours</p>	<p>ECTS</p>
Total workload	125	5
Contact hours	50	2
Practical activities	25	1