COURSE DESCRIPTION CARD - SYLLABUS

Course name
Data protection and cryptography [N2Inf1-ZTI>ODK]

Course

Field of study
Computing

Year/Semester
2/3

Area of study (specialization)
Advanced Internet Technologies

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
part-time

Requirements
compulsory

Number of hours

Lecture
16

Laboratory classes
18

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

4,00

Coordinators

dr inż. Maciej Miłostan
maciej.milostan@put.poznan.pl

Lecturers

Prerequisites

The student should have basic knowleadge about network technologies, internet applications, programming techniques and security.

Course objective

1. To familiarize students with the multi-aspect nature of the problem of ensuring the security of IT systems and maintaining the continuity of business processes. 2. Deepening students' knowledge in the field of practical application of cryptographic techniques, in particular in the field of public key infrastructure and asymmetric algorithms used in this infrastructure. Deepening knowledge of the practical use of symmetric algorithms. 3. To familiarize students with technologies used to ensure the continuity of business processes and security, i.e. methods of creating backup copies (including virtualized environments) and data recovery after failure, RAID arrays, deduplication mechanism. 4. Indication of the most common programming errors when creating applications, with particular emphasis on web applications. 5. Deepening knowledge in the field of computer network protection. 6. To familiarize students with the issue of responding to network incidents.

Course-related learning outcomes

Knowledge:
As a result of the conducted classes, the student:
1. Knows the basic methods, techniques and tools for ensuring an adequate level of data protection and examining IT security.
2. Deepens and systematizes the knowledge related to the software life cycle in the context of providing security mechanisms at various stages of IT system development, including the post-implementation phase.
3. Gets knowledge about development trends and new practices related to the protection of systems and applications, including protection against cybercriminal attacks.
4. Acquires detailed theoretical knowledge related to the practical use of cryptographic techniques and technical solutions for broadly understood data protection and ensuring business continuity.
5. Has in-depth and structured knowledge of threats related to electronic crime, understands the specificity of mission-critical systems.

Skills:
As a result of the conducted classes, the student:
1. Can apply analytical, simulation and experimental methods in the context of testing the security of systems.
2. Develops self-education skills through the independent implementation of laboratory tasks.
3. By creating reports on classes, the student deepens the ability to communicate in the native language and use English-speaking sources.
4. Can obtain information on the vulnerability of systems and applications, cyber threats and possible gaps in cryptographic algorithms from public databases, literature and other sources.
5. When analyzing problems in the field of data protection, he can apply a systemic approach and also take into account non-technical aspects, e.g. human or legal factor.
6. Can participate effectively in software inspection, especially in the necessary scope of examining software in terms of vulnerability to attacks.
7. Can assess the usefulness and the possibility of using new achievements (methods and tools) and new IT products.
8. Can formulate and test hypotheses related to engineering problems and simple research problems.
9. Can carry out a risk analysis related to the security aspects of the IT system architecture.

Social competences:
1. Student can properly define priorities for the implementation of a task set by himself or others. The element necessary to pass is the timely implementation of several practical assignments.
2. Student is aware of the responsibility for the decisions made - deficiencies in the implementation of tasks, untimely execution or attempts to plagiarize them affect the obtained marks.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Formative assessment
a) in the case of lectures, verification of the assumed learning outcomes is carried out by:
- answers to questions about the material discussed previously
b) in the case of laboratory exercises, verification of the assumed learning outcomes is carried out by:
- evaluation of reports prepared partly during the course and partly after their completion,
- assessment of laboratory exercises carried out by the student during the classes.
Summative assessment
a) in the case of lectures, verification of the assumed learning outcomes is carried out by:
- assessment of the knowledge and skills demonstrated in the written exam in the form of a test containing both questions with a choice of answers and problem questions. The final examination test will consist of min. 19 questions, the list of items will not be made available to students; only information about the scope of the exam will be made available. For a grade of 3.0, 70% of the maximum number of points must be scored. An oral examination is allowed.
b) in the case of laboratory exercises, verification of the assumed learning outcomes is carried out based on regular reports from the labs:
- the final grade is a weighted average from all the scores collected during the semester. It is required to pass at least 75% of blocks of laboratory exercises to get the promotion.
Activity during classes is rewarded with additional points, in particular for:

- a discussion of additional aspects of the issue,
- the effectiveness of applying the acquired knowledge while solving a given problem,
- remarks leading to the improvement of teaching materials or the teaching process.

Programme content

The course curriculum encompasses a range of topics including: the array of threats to business continuity, security of web applications (OWASP Top 10), fundamentals of cryptography (symmetric and asymmetric cryptography, OpenSSL), technical methods of data protection (such as RAID), recovery strategies, recognizing known vulnerabilities, and filtering network traffic.

Course topics

Lectures:
The program of lectures covers the following topics.
Lecture 1-2: Introductory information on the course of the education process. Introducing students to the multifaceted nature of the problem of ensuring the security of information systems and maintaining the continuity of business processes. Discussion of security aspects in terms of technical, logistic, physical and data. Discussion of the spectrum of threats to the security of systems, services and applications, and the methods of addressing them in the context of defence in depth strategy. In particular, attacks on applications will be discussed during the lectures. The issue of denial of service attacks (DoS and DDoS) will also be addressed. Basic preventive measures addressing the threats discussed will be presented. The proposed measures take into account the multi-layered characteristics of the application environment. Besides, for a better understanding of the security assurance cycle, the economic aspect of this process and the cost of implementing security will be discussed.

Lecture 3-4: Overview of symmetric and asymmetric cryptographic systems. Cryptographic systems unconditionally and computationally secure. Cryptographic services. Euler function and the use of its properties in modular arithmetic. Modulo exponentiation algorithm. DES, 3DES and AES algorithm as examples of standard symmetric cyphers. RSA and ElGamal as examples of asymmetric algorithms. Finding prime numbers and number primality tests (sieve, Miller-Rabin test, AKS test). Hash functions. Selected applications of hash functions and asymmetric algorithms - incl. discussion of the electronic signature mechanism.

Lecture 5-6: Network security and disaster recovery. Application and types of firewalls. Network segmentation and a demilitarized zone. Access Personalization and IEEE802.1X protocol. Best practices for updating systems. Intrusion and anomaly detection systems. Backup, Archive, and Disaster Recovery.

Lecture 7-8: Researching the architecture of information systems in terms of possible attack vectors and the associated risk (STRIDE model, DREAD assessment). Proper responding to incidents in the light of applicable laws - selected aspects.

Laboratories:
Laboratory exercises are conducted in the form of eight two-hour classes in the computer laboratory. The first classes are partly intended to familiarize students with the rules of using the laboratory and completing tasks. The program of the laboratories is as follows: Lab 1. Attacks on the operating system with physical access to the target system. Packet filtering - stateful and stateless rules (iptables), simple network scanners and monitoring applications (nmap, tcpdump, iptraf, wireshark). Laboratory 2. Openssl and GnuPG libraries and public key infrastructure (PKI): obtaining certificates, signing and encrypting messages, integrating GnuPG with an e-mail client. Laboratory 3 and 4. OWASP WebGoat - attacks on Internet applications, practical exercises. Lab 5 and 6. Attacks on service servers - attempts to use vulnerable service servers in order to gain access to a non-updated system. An overview of the sources of information about vulnerabilities. Use of automated tools and databases of exploits for security testing (e.g. Metasploit, Nessus). Laboratory 7 and 8. Application layer filtration, next-generation firewall (NGN firewalls).
Some of the above-mentioned content is part of the student"s self-work.

Teaching methods

1. Lecture: multimedia presentation as needed, illustrated with additional examples given on the blackboard
2. Laboratory exercises: practical exercises at the computer carried out according to the given scenario, the

configuration of programs and scripts solving shared problems, discussion of applied solutions and programming structures

Bibliography

Basic
1. Official (ISC)2 (R) Guide to The CISSP (R) CBK (R) 5th edition, John Warsinske (editor), Wiley, 2019
2. Cryptography and Network Security: Principles and Practice (5th Edition), Stallings W, Prentice Hall, 2010 (lub Ochrona danych w sieci i intersieci - w teorii i praktyce, William Stallings, WNT, 1997)
3. Practical Cryptography, Niels Ferguson and Bruce Schneier, John Wiley&Sons, 2003 (lub Kryptografia w praktyce, Niels Ferguson and Bruce Schneier (Tłumaczenie: Tomasz Żmijewski), Helion, 2004)
4. Modelowanie zagrożeń, Frank Swiderski, Window Snyder, A.P.N. Promise, 2005
5. Bezpieczeństwo danych w systemach informatycznych, Stokłosa J., Bilski T., Pankowski T., Wydawnictwo Naukowe PWN, Warszawa - Poznań, 2001
6. Wykrywanie intruzów, Amoroso E, Wydawnictwo RM, Warszawa, 1999
Additional
1. Mastering Regular Expressions, Jeffrey E.F. Friedl, O"Reilly Media, 2006
2. Sed & Awk, Dougherty and Arnold Robbins, O"Reilly and Associates, 1997

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,00
Classes requiring direct contact with the teacher	36	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	64	2,50