UNIVERSITY OF MITROVICA "ISA BOLETINI"

Course Curriculum Model (Syllabus)		
Faculty:	FACULTY OF MECHANICAL AND COMPUTER ENGINEERING	
Department:	Informatics Engineering	
Level:	Bachelor	
Code of the course:	112-CSE	
Course:	Data security	
Course Status:	E	(mandatory)
Semester:	I	(summer)
Number of hours per week:	2+2	
ECTS:	4	
Time / location:	According to schedule /UMIB	
Year of studies:	I	
Lecturer:	Prof. Ass. Dr. Arianit Maraj	
Assistant:		
Contact details:	Lecturer	Assistant
Email:	arianit.maraj@umib.net	
Telefon:	044 425 159	

Content	This course contains the main concepts of data security. Specifically, it contains details relating to the security of the operating system, including; Stages of software development cycle, protection in Operating Systems, etc. Then, an important focus of this course is network security, with particular emphasis on the main threats to networks. Also, other important topics it contains are worth mentioning, such as: cryptography and the role of cryptography for Internet security, data security and privacy on the Internet, security at the DB level, and even physical security.
Purpose	The main purpose of this course is to explain to students the basic concepts, definitions and best practices of data security and Information Technology Systems in general. The course begins with definitions of data and information, databases as well as basic concepts of data security. The data attacks and the way of protection from these attacks will be elaborated. Cryptography and data encryption forms also play an important role. Forms of data protection are explored in databases, software applications, computer network, servers and web servers, e-mail, etc.

<table>
<tr><td>Accessibility</td><td colspan="2">At the end of this course the student will be able to:
1. Know and understand the basic notions of Data Security
2. Know and understand the terms of cryptography and the basic meanings of symmetric and asymmetric cryptography
3. Understand encryption algorithms and their types
4. Know the application of cryptography for data protection
5. Know computer-level security concepts
6. Know the security concepts of servers
7. Know the concepts of security at the level of computer networks
8. Know Internet security and Internet technologies
9. Know the security risks
10. Recognize security applications (software)
11. Know issues of data protection planning and storage</td></tr>
<tr><td rowspan="15">Program</td><td>weeks</td><td>Lecture</td></tr>
<tr><td>First week:</td><td>Presentation and discussion of the syllabus</td></tr>
<tr><td>Second week:</td><td>Concepts of data security and information technology systems</td></tr>
<tr><td>Third week:</td><td>Methods of safety risks</td></tr>
<tr><td>Fourth week:</td><td>Operating system security I</td></tr>
<tr><td>Fifth week:</td><td>Operating system security II</td></tr>
<tr><td>Sixth week:</td><td>Network security</td></tr>
<tr><td>Seventh week:</td><td>Server security</td></tr>
<tr><td>Eighth week:</td><td>First test</td></tr>
<tr><td>Ninth week:</td><td>Cryptography applications for internet security</td></tr>
<tr><td>Tenth week:</td><td>Cryptography applications in VPN and wireless networks</td></tr>
<tr><td>Eleventh week:</td><td>Internet security and privacy</td></tr>
<tr><td>Twelfth week:</td><td>Database software computers and networks</td></tr>
<tr><td>Thirteenth week:</td><td>Recovery from destruction and data storage strategies</td></tr>
<tr><td>Fourteenth week:</td><td>Physical security</td></tr>
<tr><td>Fifteenth week :</td><td><u>Second test</u></td></tr>
</table>

<table>
<tr><td>Literature</td><td>Principal literature:

Security in Computing, Fifth Edition, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies. Copyright 2015, Pearson Education

Stallings, W., Brown, L., Bauer, M.D. and Bhattacharjee, A.K., 2012. Computer security: principles and practice (pp. 978-0). Upper Saddle River, NJ, USA: Pearson Education.

Recommended Literature:

1. Cryptography and Network Security, Principles and Practice, 5th Edition, William Stallings, Pearson Education, 2011.
2. Principles of Computer Security: CompTIA Security+™ and Beyond, Lab Manual, Second Edition,Vincent Nestler, Wm. Arthur Conklin,Gregory White,Matthew Hirsch
3. Network Security Fundamentals, Eric Cole, Ronald L. Krutz, James W. Conley, Brian Reisman, Mitch Ruebush, and Dieter Gollmann
4. Computer Security Fundamentals, Chuck Easttom, 2012 by Pearson</td></tr>
<tr><td>Teaching methodology</td><td>Lecture, Tutorials, Assignments, Lab Experiments, Lab Report and presentation.</td></tr>
<tr><td></td><td>
<table>
<tr><th colspan="4">Contribution to student workload (which should correspond to student learning outcomes - 1 ECTS credit = 25 hours)</th></tr>
<tr><th>Activity</th><th>Hours</th><th>Days/weeks</th><th>Total</th></tr>
<tr><td>Lectures</td><td>2</td><td>15</td><td>30</td></tr>
<tr><td>Exercise sessions (with TA)</td><td>2</td><td>15</td><td>30</td></tr>
<tr><td>Practical work</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Office hours</td><td>0.5</td><td>10</td><td>5</td></tr>
<tr><td>Fieldwork</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Midterms, seminars</td><td>1</td><td>3</td><td>3</td></tr>
<tr><td>Homework</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Self-study</td><td>2</td><td>10</td><td>20</td></tr>
<tr><td>Final exam preparation</td><td>2</td><td>3</td><td>6</td></tr>
<tr><td>Time spent in exams</td><td>2</td><td>3</td><td>6</td></tr>
<tr><td>Projects, presentations, etc</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Total</td><td></td><td></td><td>100</td></tr>
</table>
</td></tr>
</table>

Evaluation

Teaching methodology:
(according to the Statute and Regulation for studies of UMIB)

Tests / Colloquia	60%
Practical test during exercises	10%
Seminary work	-
Interpretation and presentation of artistic creativity and other works	-
Assignments and other courses during the semester	10 %
Professional activities	-
Others (specify) -	-
Final exam	20%

Academic policies

The Professor sets the criteria for regular attendance at lectures and exercises and the rules of ethics such as keeping calm in class, turning off cell phones, entering the hall on time, etc.

The students are expected to behave in correct and professional manner. They can cooperate and discuss papers and projects among themselves, but the submitted papers and projects need to be unique and individual. Each student will be graded individually, based on evaluation methods. No copying between students or the presentation of solutions received from unauthorized books or other online resources will be tolerated. Eventual cases of violation of academic conduct and norms will be reported to the management of the Faculty.

The achieved performance will be evaluated according to the following table:

Points	Grade
50 - 59.9	6
60 - 69.9	7
70 - 79.9	8
80 - 89.9	9
90 – 100	10

Mitrovica

08.01.2021

Course provider:

Prof. Ass. Dr. Arianit Maraj

(Signature)