COURSE PROGRAM

Academic year: 2024/25

Identification and characteristics of the course				
Code	502299		ECTS credits	6
Course name (English)	*Network Security*			
Course name (Spanish)	Seguridad en Redes Telemáticas			
Degree programs	Bachelor Degree in Computer Science - Software Engineering			
Faculty / School	School of Technology			
Semester	7th	Type of Course	Optional	
Module	Optional Technology in Software Engineering			
Subject Matter	Network Technology/Architecture			
Lecture/s				
Name	Office		E-mail	Web page
Lorenzo M. Martínez Bravo	Nº 7, Computer Science Building		lorenzom@unex.es	Grupo GITACA
Subject Area	Telematics Engineering			
Department	Department of Computer and Telematic Systems Engineering			

Competencies

Basic Competencies (CB)

CB 1. That the students should have demonstrated that they have knowledge and understanding of concepts in the field of study that build based on of general secondary education and are at a level which, while supported by advanced texts, also include certain aspects that imply understanding of cutting-edge knowledge in the field of study.

CB 2. That the students should know how to apply their knowledge in a professional way to their work or vocation and have the competences that are usually demonstrated employing the preparation and defense of arguments and problem solving within their area of study.

CB 3. That the students should have the capacity to collect and interpret relevant data (within their area of study) to form judgements that include a reflection upon social, scientific, and ethical issues.

CB 4. That the students can transmit information, ideas, problems, and solutions to both specialized and non-specialized audiences.

CB 5. That the students should have developed those learning abilities necessary for future independent study.

Specific Competencies on Software Engineering (CIS)

CIS05 – Ability to identify, evaluate and manage associated potential risks that could appear.

Contents

Course outline

Information Security fundamentals. Security Policies. Security technologies. Network security.

Course syllabus

Unit 1: Network and Information security fundamentals.

Basic concepts about security. Security attacks. Security services. Security mechanisms. Network security models. Standards and norms. Security policies.

Laboratory: Analysis and Analysis and proposal of security policies. Basic information security tools

Unit 2: Introduction to Cryptography.

Basis of cryptography. Symmetric Block Encryption Algorithms. Random and Pseudorandom

Numbers. Streams Ciphers and RC4. Cipher Block Modes of Operation. **Laboratory:** • Private key encryption with JCA library.
Lecture 3: Public-Key Cryptography and Message Authentication Principles. Secure Hash Functions. Message Authentication Codes (MACs). Public-Key Principles and Algorithms. Digital Signatures. **Laboratory:** • Public key encryption ang signature with JCA library.
Unit 4: Key Distribution and User Authentication. Introduction. Symmetric Key Distribution. Kerberos. Public-Key Distribution. X509 Certificates. Public-Key Infrastructure. Federated Identity Management. **Laboratory:** Key management with JCA library. Personal X509 Public key certificates management.
Unit 5: Secure System Development and Management. Secure System Development Life Cycle. Management of secure systems. **Laboratory:** Analysis of secure development models.
Unit 6: Transport-Level Security. Web Security. SSL/TLS. HTTPS. SSH. **Laboratory:** Analysis of TLS/SSL secure connections.
Unit 7: Network Access Control. Wireless Network Security. Cloud Security. Network Access Control. EAP. IEE 802.1X. Wireless Security. Mobile Device Security. IEEE 802.11. 802.11i. Cloud Computing. Cloud Security. **Laboratory:** Wifi traffic analysis.
Unit 8: Secure Email. PGP. S/MIME. DKIM, … **Laboratory:** Email providers evaluation and assessment.
Unit 9: Network security tools. Firewalls, IDSs/IPSs, VPNs, Malware. **Laboratory:** Security tools use and configuration.

Educational Activities

Student workload (hours per lesson)		**Lectures**	**Practical Sessions**	**Monitoring activity**	**Homework**
Lesson	**Total**	**L**	**LAB**	**SGT**	**PS**
1	10,25	2	0	0,25	8
2	16,25	3	4	0,25	9
3	17,5	3	5	0,5	9
4	16,25	3	4	0,25	9
5	14,25	3	3	0,25	8
6	16,5	4	3	0,5	9
7	16,25	4	3	0,25	9
8	15,5	3	3	0,5	9
9	15,25	3	4	0,25	8
Assessment	12	2	1	0	9
Total	**150**	**30**	**30**	**3**	**87**

L: Lectures (85 students).
LAB: laboratory (15 students).
SGT: Scheduled Group Tutorials (Educational Monitoring, ECTS type tutorials).
SP: Personal Study, individual or group work and reading of bibliography.

Teaching Methodologies

- Theory and practice lessons at classroom. Lectures to develop subject fundamentals.
- Theory and practice lessons at classroom. Brief activities, individually or in a group, to allow the students apply the explained concepts and solve the proposed problems. Stimulation of student's participation.
- Practical lessons in the laboratory. Practical activities, lectures with guidelines, seminaries to solve problems, etc. in groups under the advice of a lecturer. In order to achieve the proposed objectives, additional activities can be added before or after practical lessons. Activities related to project development, hypothetical scenarios, technical reports, etc. will be proposed.
- Monitoring activities, both individually or in a small group. A follow-up for students monitoring will be done by means of training and orientation activities. These activities will be mainly used to monitor the proposed assignments, to discuss different alternatives and to evaluate the proposed objectives.
- Activities, assignments, study, both individually and in a group. Those activities carried out autonomously by the student will be oriented to acquire basic knowledge within the scope of computer science, and on projects and assignments development.

Learning outcomes

After finishing the specific module, the student:

- Controls concepts related to information security and computer security
- Knows main basis of information security as well as concepts like Threat, Risk and Privacy.
- Knows how to use mechanisms to grant security for computer stored information and transmitted information.
- Understands system security basis and how to apply these techniques for advanced security of operative systems and the Internet.
- Knows computer systems and information security fundamentals.
- Master concepts related with system security policies.
- Knows methodologies, techniques, and tools for system security.

Assessment systems

According to the Evaluation Regulations of the official bachelor's and master's degrees of the University of Extremadura, the course can be evaluated following a continuous evaluation system or with a global final test.
According to these regulations, the student must choose the evaluation system that he or she prefers by following the indicated procedure that will be made available to the student (Course Virtual Campus, in the first weeks of the semester). By default, it is understood that the student chooses continuous assessment.
The evaluation of the course is composed of two main blocks: Theory and Laboratory.

Theory Block
In this block, special mention will be made to the acquisition of competences and the achievement of learning results, from a more theoretical and conceptual point of view. For this, the following evaluation mechanisms will be used:

Theoretical activities
Throughout the semester, a series of activities will be proposed to be carried out individually or in groups. These activities will be carried out within class hours and/or out of the class time.
The activities can be of different types: search and analysis of information about cases, analysis of technical documents, resolution of problems, analysis of tools, etc. These activities encourage work and will receive feedback from the teacher.

Written tests
There will be several written tests (on paper and/or virtual campus) with theory questions, exercises and problems about the fundamental concepts and their application. The tests are distributed throughout the semester, covering the different topics.

Laboratory block
Several laboratory's activities related to the contents explained in the laboratory classes will be carried out, delivered, and evaluated. In addition, it is contemplated the possibility of taking a final evaluation test of such laboratory's activities, to verify the correct acquisition of the worked knowledge and skills.

Evaluation criteria
As already indicated, the course can be passed according to two different assessment systems: Continuous Assessment or Global Final Assessment.

Continuous evaluation procedure
To pass the course, all the minimum requirements of all the two blocks must be passed: Theory and Laboratory.

Theory Block:
As already indicated, this block has two components:
Theoretical activities:
This block will be evaluated and passed by carrying out the proposed activities. Your grade will be calculated as the weighted average of all activities. There is no minimum grade requirement in this section. Some activities will be recoverable, while others will not. This block will be the 30% of the theory block grade.
Written tests:
There will be several written tests, which will be evaluated. The grade in this section will be the weighted average of all the tests. It is mandatory to obtain a minimum average grade of 5; Failed tests could be compensated, as long as a minimum grade of 4 is obtained in such tests. This block will be the 70% of the theory grade.

Laboratory Block:
This block will be evaluated and passed by carrying out the laboratory proposed activities. The grade will be calculated as the weighted average of all proposed activities. You must obtain a minimum grade of 5 in all the activities in this block. These activities will be recoverable.

The theory mark represents 70% of the course mark, while the laboratory mark represents the remaining 30%.
In case of passing only one of the two parts, theory or Laboratory, such part will be saved for the remaining current academic year, therefore, the student will only have to recover and pass the other part. Specific instructions will be given on how to recover the failed part.

Global final assessment
It will consist of a final exam that will include a theory part and a Laboratory part, covering all the course worked on contents. To pass the course, a minimum grade of 5 must be obtained in both parts. The final mark will be calculated in the same way as in the CE, that is, 70% theory and 30% Laboratory.

Bibliography (basic and complementary)

- *Effective Cybersecurity. A guide to using best practices and standards*. William Stallings, Ed. Addison-Wesley, 2019.
- *Network Security Essentials. Applications and Standards*, William Stallings, Ed. Pearson, 6ª Ed., 2017.
- *Seguridad en Redes*, Chris McNab, Ed. Anaya-Multimedia, 2ª edición, 2008.

Bibliography in UEx library

Other resources and complementary educational materials

Resources: subject's virtual room, available at the Campus Virtual of the University of Extremadura (https://campusvirtual.unex.es).