Vulnerabilities, threats and computer security protocols

Academic Year: (2022 / 2023) **Review date: 17-04-2023**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: CAMARA NUÑEZ, MARIA CARMEN

Type: Compulsory ECTS Credits : 6.0

Year : 3 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

- Mathematics
- Statistics and Information Module II (Basic Training) and the material (subject) of Statistics (Operations Research) Module III (Fundamentals of Engineering)
- Information hiding techniques

OBJECTIVES

- Identify security objectives and vulnerabilities, threats and risks of a given information system in a defined operational environment. Analyze the possible security measures to be used.
- Evaluate the security services to be implemented in a given system and design and implement mechanisms and subsequent protocols.
- Evaluate and implement appropriate authentication mechanisms to access a specific system.
- Use the signature and certification systems in a particular environment.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Introduction to networks and distributed systems.
2. Status of security systems and products.
3. Analysis and classification of attacks.
4. Measures, services and security mechanisms.
5. Digital Signature. Certification authorities. Public key infrastructures.
6. Systems and multifactor authentication based on public key infrastructure.
7. Security protocols.

LEARNING ACTIVITIES AND METHODOLOGY

The training activities include:
1st. Lectures, individual or group tutorials, personal work and student presentations, including theoretical and practical tests and examinations. To facilitate their development students receive class notes in the appropriate web tool and have basic reference texts that allow them to complete and deepen the most important or more fundamental issues.
2nd. Practice in computer rooms in small groups, individual tutorials and personal work, including tests and examinations. All it aimed at the acquisition of practical skills related to the program for each subject.

Due to the uncertainty about the teaching format to which the health circumstances will lead us during the next course, it is expected to start in the semi-attendance mode and may lead to training 100% classroom or 100% online depending on the evolution of the spread or control of the pandemic and the health and hygiene standards dictated by the authorities of the sector.

ASSESSMENT SYSTEM

The grading system includes continuous assessment of the student's work (tests assessing skils, theoretical, and practical concepts, and also laboratory tasks) and a final assessment through a written exam that will assess the concepts, skills, and abilities acquired throughout the module.

Grading will be done according to the following criteria:

1. Written exams containing both theory and problems: 70% of the final mark, consisting of:
   1.1. Continuous assessment exam: 15% of the final mark. This will take place approximately by mid-term.

1.2. Final written exam: 55% of the final mark. To pass the module, the student must get a minimum grade of 4 in this exam.
2. Hand-in practicals done during the lab sessions: 30% of the final mark, consisting of:

In the extraordinary exam, the student will choose between:
a) A final written exam accounting for 100% of the final grade. This exam consists of theory, problems, and practical material covered in the lab sessions; or
b) A final written exam accounting for 60% of the final grade. This exam consists of theory and problems. The remaining 45% comes from the grade obtained during the term in the continuous assessment exam (10%) and lab sessions (30%).

% end-of-term-examination:	60
% of continuous assessment (assigments, laboratory, practicals…):	40

BASIC BIBLIOGRAPHY

- Anderson, Ross Security Engineering: A guide to Building Dependable Distributed Sistems (2nd edition), Wiley, 2008
- Kaufman, Charlie, et al. Network Security: Private Communication in a Public World. Second Edition., Prentice Hall, 2002
- Pfleeger, Charles et al Security in Computing (4ª edition), Prentice Hall, 2007
- Stallings, William Cryptography and Network Security: Principles and Practice, Prentice Hall, 2013
- Vacca, John R. (editor) Computer and Information Security Handbook, Elsevier (The Morgan Kaufmann Series in Computer Security), 2009

ADDITIONAL BIBLIOGRAPHY

- Bishop, Matt Computer Security: Art & Science. (cap 12), Addison-Wesley, 2015
- Kurose, James F. Ross, Keith W. Redes de Computadoras, un enfoque descendente, Pearson, 2017

BASIC ELECTRONIC RESOURCES

- ENISA . ENISA: http://www.enisa.europa.eu/publications
- INTECO . INTECO: <a href=" http://www.inteco.es/Seguridad/Observatorio" type="Reference"
- INTYPEDIA . INTYPEDIA: http://www.intypedia.com/
- NIST . NIST: http://csrc.nist.gov/publications/PubsSPs.html