Vulnerabilities, threats and computer security protocols

Academic Year: (2023 / 2024) **Review date: 28/04/2023 15:52:00**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: DE PABLO LOBO, FELIX

Type: Compulsory ECTS Credits : 6.0

Year : 4 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. intrinsic vulnerabilities and extrinsic.
3. Analysis and classification of attacks. Assessment of its consequences.
4. Measures, services and security mechanisms. They prevent risks.
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.

ASSESSMENT SYSTEM

% end-of-term-examination/test:	55
% of continuous assessment (assigments, laboratory, practicals…):	45

1. Ordinary sitting - continuous assessment

Student lab assessment, by means of deliverable(s) or exam(s) as defined by the instructor: 30%
partial theory exam: 15% (contents addressed herein may also appear in the final exam).
Final evaluation through a written exam that will assess knowledge globally,

% end-of-term-examination/test:	55
% of continuous assessment (assigments, laboratory, practicals…):	45

skills and abilities acquired during the course: 55%

To consider continuous assessment grades (lab + partial) grades, it will be necessary to obtain at least 40% of the maximum score in the final evaluation. All assignments have to be handed in -- otherwise non-continuous assessment applies.

2. Ordinary sitting - non-continuous assessment
Final exam (100% of final mark)
- The maximum grade will be 6.0 marks
The exam contains specific parts to assess the competences related to lab assignments.

3. Extraordinary sitting
In the extraordinary sitting, the following rules apply:

a. If the student followed the continuous assessment method, the exam will have the same relative weight as in the ordinary sitting. The mark of the continuous evaluation is kept.
b. Otherwise, students will have an exam counting for 100% of the final mark, which will include additional questions related to the lab assignments. The type of assignments make them unsuitable to be delivered again in this sitting.
c. Even if the student did follow the continuous assessment, he/she has the right to be assessed considering only the mark from the final exam if it is more favourable to him/her.

BASIC BIBLIOGRAPHY

- Anderson, Ross Security Engineering: A guide to Building Dependable Distributed Sistems (2nd edition), Wiley, 2008

- Christof Paar, Jan Pelzl Understanding cryptography: a textbook for students and practitioners, Springer Science & Business Media, 2009

- Pfleeger, Charles et al Security in Computing (4ª edition), Prentice Hall, 2007

- 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