Data Protection

Academic Year: (2023 / 2024) **Review date: 19-01-2023**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: LOPEZ GARCIA, SERGIO

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 1

OBJECTIVES

SKILLS AND LEARNING RESULTS
In relation to the skills, during the course the following will work:

- Knowledge and understanding that provide a basis or opportunity for originality in developing and / or applying ideas, often in a research context.
- Students can communicate their conclusions and knowledge to specialist and non-specialist audiences clearly and unambiguously.
- Students must possess the learning skills that enable them to continue studying.
- Develop concise, clear and reasoned documents, plans and projects working in the field of cybersecurity.
- Apply the services, mechanisms and security protocols appropriate in a particular case.
- Design and evaluation of systems, security architectures and networks.
- Know and apply encryption mechanisms and relevant steganography to protect data residing on a system or in transit through a network.

Regarding learning outcomes, to overcome this subject students will be able to:
- Given a system with security requirements established to propose mechanisms and protocols required to provide some basic security services: authentication, authorization, privacy and access control. Give a measure of their effectiveness and limitations.
- To design and evaluate appropriate measures for the identification and authentication of users and management of identities and associated authorizations.

DESCRIPTION OF CONTENTS: PROGRAMME

PROGRAM

This course covers the various aspects of data protection, especially focusing on the services of confidentiality, integrity and authenticity of information exchanged or stored. The course addresses these issues from a very practical standpoint, by conducting a case study over the development of consistent application of current data protection.

The course syllabus is divided into four parts:

* Part I: introduction.
  - Presentation of the course: agenda, legislation, practical description of the case study.
  - Introduction to the data protection: definitions, dimensions of information security.
  - Types of encryption systems (symmetric / asymmetric)

* Part II: symmetric encryption
  - Block and stream ciphers.
  - Encryption algorithms: DES, modes of operation, 2DES, 3DES, AES.
  - Management of cryptographic keys.

* Part III: asymmetric encryption
  - RSA, Diffie-Hellman ECC.

* Part IV: authentication and digital signature
  - Authentication and one-way functions: cryptographic hash functions, Message Authentication Code (MAC).
  - Digital Signature. Standards.
  - Digital certificates and public key infrastructure (PKI) (digital certificates ITU-T X.509v3, trust Authorities (CA) and public key infrastructure (PKI), electronic signature legislation..

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES
Theoretical lectures
Practical lectures
Laboratory practices
Tutoring sessions

The teaching methodology will include:
- Teacher exhibitions in classroom, with support of computer and audiovisual media, in which the main concepts of the subject are developed and the literature is provided to aid student learning.
- Critical reading recommended by the teacher of texts related to the subject: newspaper articles, reports, manuals and / or academic articles, either for further discussion in class, either to expand and consolidate the knowledge of the subject.
- Resolution of case studies, problems, etc. posed by the teacher individually or in groups.
- Presentation and discussion in class under teacher moderation issues related to the content of matter, as well as case studies.

ASSESSMENT SYSTEM

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

EVALUATION CRITERIA

The grade for the course consists of the following blocks:

- Practical case study (continuous evaluation): 60%.
- Final exam: 40%.

To pass the course is necessary to obtain at least 50 points in the sum of the two blocks (without a minimum of points necessary in any of the same).

According to the rules of continuous assessment established by the University in the ordinary call students who have not followed the continuous assessment a final examination with a value of 60% of the course will be allowed. In the extraordinary session, the student has the right to be qualified through a final exam worth 100% of the subject.

BASIC BIBLIOGRAPHY

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone Handbook of applied cryptography, http://www.cacr.math.uwaterloo.ca/hac/, 2001

- C. Kaufman, R. Perlman, M. Speciner, E. Cliffs. Network security : private communication in a public world , Prentice Hall, 1995

- Stallings, William Cryptography and network security. Principles and Practice. Sixth Edition, Prentice Hall, 2014