Cyber-security of networks and cyber-physical systems

Academic Year: (2021 / 2022) **Review date: 11/07/2020 02:10:36**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: LARRABEITI LOPEZ, DAVID

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 1

OBJECTIVES

BASIC COMPETENCES
CB6 Possess and understand knowledge that provides a basis or opportunity to be original in the development and / or application of ideas, often in a research context
CB7 That students know how to apply the knowledge acquired and their ability to solve problems in new or unfamiliar environments within broader (or multidisciplinary) contexts related to their area of study
CB10 That students have the learning skills that allow them to continue studying in a way that will be largely self-directed or autonomous

GENERAL COMPETENCES
CG4 Knowledge and understanding of the management principles applicable to productive and service environments.
CG5 Capacity for basic analysis of the requirements for information management and treatment of large volumes of data.

SPECIFIC COMPETENCES
CE9 Ability to identify computer security requirements in connected industry environments

LEARNING RESULTS
As a result of the learning the student will be able to:
- Configure secure transport protocols,
- Know the technologies to mitigate threats and protect data in networked systems.

DESCRIPTION OF CONTENTS: PROGRAMME

- Cryptography concepts: symetric key and public/private key encryption. Authentication.
- Secure end-to-end transport protocols
- Cybersecurity threats in CI4.0: malware types. Structure, components and infection vectors.
- Techniques and technologies for mitigating threats: attacks and countermeasurements. Firewalls, IDS and SIEMs.
- Data protection in networked systems: security in IP. IPsec. VPNs. Security in wireless communications.

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES OF THE SYLLABUS REFERRED TO MATTERS
AF1 Theory class
AF2 Practical classes
AF4 Laboratory session
AF5 Supervision sessions
AF6 Group work
AF7 Individual work by student
AF8 Mid-term and final exam

Code activity	Num Hours	Class Hours	% studiante
AF1	36	36	100
AF2	18	18	100
AF4	9	9	100
AF5	6	6	100
AF6	75	0	0
AF7	75	0	0
AF8	6	6	100
TOTAL MATTER	225	75	33%

TEACHING METHODOLOGIES RELATED TO MATTERS

MD1 Class presentations supported by computing and audiovisual media, where the main matter concepts are developed and the bibliography to complement the students' learning is provided

MD2 Critical lectures of texts recommended by the professor: articles, reports, manuals and research papers.

MD3 Solving of practical use cases, problems, etc posed by the teacher to individuals or groups.

MD4 Presentation and discussion in class, under the professor supervision of topics related to the matter, as well as several pracitcal use cases.

ASSESSMENT SYSTEM

% end-of-term-examination/test: 60

% of continuous assessment (assigments, laboratory, practicals…): 40

ASSESMENT OF THE SYLLABUS LINKED TO MATTERS

SE1 Class participation

SE2 Individual or group works

SE3 Final exam

Assessment Systems	minimal weight (%)	maximum weight (%)
SE1	0	20
SE2	20	40
SE3	40	60

BASIC BIBLIOGRAPHY

- Aditya Gupta The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things, Apress, 2019

- William Stallings Cryptography and Network Security: Principles and Practice. , Prentice Hall, 2013