Cyber-security of networks and cyber-physical systems

Academic Year: (2024 / 2025) **Review date: 17-09-2024**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: LARRABEITI LOPEZ, DAVID

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 1

OBJECTIVES

- Learning of basic principles of cyber-security of connected digital systems.
- Learning of fundamentals of symmetric and asymmetric cryptography
- Learning of the main threats and protection tools
- Knowledge of protection architectures in connected industry environments
- Hands-on knowledge of security configuration with TLS, WiFi and firewalls.

DESCRIPTION OF CONTENTS: PROGRAMME

- the cybersecurity problem of CI4.0
- Cryptography concepts: definitions, security services, symmetric key and public/private key encryption. Authentication. Hashing.
- Secure end-to-end transport protocols
- Cybersecurity threats in CI4.0: malware types. Structure, components and attack vectors.
- Techniques and technologies for mitigating threats: attacks and counter-measurements. 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

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:	60
% of continuous assessment (assigments, laboratory, practicals…):	40

ASSESMENT OF THE SYLLABUS LINKED TO THE MATTER
SE1 Class participation

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

SE2 Individual or group works
SE3 Final exam

The concrete distribution of weights in this subject is: SE1 0%, SE2 40%, SE3 60%.

A minimum score of 3 over 10 is required in the exam to compute the average and pass the course.

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

ADDITIONAL BIBLIOGRAPHY

- Ian Neil CompTIA Security+ SY0-701 Certification Guide - Third Edition, Packt Publishing, O'Reilly, 2024