# Secure Architecture

**Academic Year: ( 2023 / 2024 )** **Review date: 02-05-2023**

**Department assigned to the subject: Telematic Engineering Department**

**Coordinating teacher: PEREZ MARTINEZ, ALFONSO DE JESUS**

**Type: Electives ECTS Credits : 3.0**

**Year : 1 Semester : 2**

## REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Students should work comfortable in Unix environments and have knowledge on Public Key Infrastructure (PKI), Data Protection subject.

## OBJECTIVES

After the course, the students will be able to:

- Analyze the architecture of an information system from a security point of view.

- Design information systems architectures that fulfil a set of specified security requirements.

- Apply appropriate security services, mechanisms and security protocols that minimize risks and provide resistance to attacks, mainly DDoS.

- Know procedures and principles to handle classified information.

- Apply acquired knowledge to solve problems under novel or almost novel situations or within broader (multidisciplinar) contexts related with cyber security.

- Discuss in a public audience about their acquired knowledge, and the conclusions from the work. Students will be able to give their foundational and most convincing reasons to a specialized and non specialized audience in a clear way, without ambiguities.

-Continue studying in a autonomous or self-directed way

LEARNING OUTCOMES
This course contributes to the following learning outcomes:

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.

Evaluate the security architecture of a given vulnerable system and propose improvements.

To design and evaluate appropriate measures for the identification and authentication of users and management of identities and associated authorizations.

## DESCRIPTION OF CONTENTS: PROGRAMME

This course presents and elaborates aspects related to the design of secure architectures that minimize security risks and provide resistance to attacks. The course also covers the principles, procedures and systems for handling classified information, as well as elements of physical security.

The course program is organized as follows:

1. Secure Architectures
1.1. Motivation and Practical Cases
1.2. Security Design Principles
1.3. Security in Cloud Computing and Cloud Native Applications

2. Authorization
2.1. Traditional Access Control Models: DAC, MAC and RBAC
2.2. Curent Access Control Models: ABAC
2.3. Identity & Access Control Architecture (IAM) and Languages: XACML/SAML.

3. Attack Tolerance
3.1. DoS Overview
3.2. Protection against DDoS
3.3. Back-up systems

4. Multilevel and Multilateral Security Systems
4.1. Information Classification
4.2. Principles and Procedures for handling classified Information
4.3. MLS Systems. Examples and practical considerations

5. Physical Security
5.1. Security against emanations. TEMPEST
5.2. Intrusion resistant Hardware

## LEARNING ACTIVITIES AND METHODOLOGY

Learning activities:

Theoretical lectures
Practical lectures
Mixed theoretical and practical lectures
Laboratory practices
Tutoring sessions
Teamwork
Individual work by the student

The teaching methodology consists of:

- Lectures given by the professor using audiovisual elements to develop the main concepts and to provide additional references for further learning.

- Complementary activities to broaden and consolidate the acquired knowledge. Such activities are of different nature: problems, discussion of practical cases, and/or exercises using the computers in order to test tools that are useful for the deployment of secure architectures.

- Elaboration and oral presentation of technical works by the students.

## ASSESSMENT SYSTEM

The evaluation system consists of:

1) Technical work and participation (60%):

1.1) Students must elaborate a work in the context of Secure Architectures, including documentation, oral presentation and defense: 40% (of the final mark).

1.2) Students must deploy infrastructure for secure remote management and for identity management and authorization: 20% (of the final mark).

2) Final Exam (40%)

The participation in-class will be take into account: problems, demo deployment, discussions, etc.

In case of not passing the course, students will have to repeat the failed parts and the evaluation will be conducted following the scheme 40% exam, 60% technical work/participation.

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

## BASIC BIBLIOGRAPHY

- Bhavani Thuraisingham Developing and Securing the Cloud, Auerbach Publications, 2013
- Dieter Gollmann. Computer Security., John Wiley & Sons., 2011
- Liz Rice, Michael Hausenblas Kubernetes Security, O'Reilly Media, Inc, 2018
- Sam Bishop. Computer Security: Art and Science., Addison- Wesley Professional., 2003
- Sam Newman. Building Microservices., O'Reilly Media, Inc., 2015

## ADDITIONAL BIBLIOGRAPHY

- Fran Ramírez, Elías Grande y Rafael Troncoso. Docker: SecDevOps., 0xWord., 2018
- Guy Podjarny Cloud Native Application Security, O'Reilly Media, Inc., June 2021
- Stephane Jourdan, Pierre Pomes. Infrastructure as Code (IAC) Cookbook., PACKT., 2017
- William Stallings and Lawrie Brown. Computer Security: principles and practice., Pearson Education., 2008