Universidad Zaragoza

Year : 2020/21

60962 - Advanced security

Syllabus Information

Academic Year: 2020/21
Subject: 60962 - Advanced security
Faculty / School: 110 - Escuela de Ingeniería y Arquitectura
Degree: 623 - Master's Degree in Telecommunications Engineering
ECTS: 6.0
Year: 1
Semester: Second semester
Subject Type: Compulsory
Module: ---

1.General information

1.1.Aims of the course

1.2.Context and importance of this course in the degree

1.3.Recommendations to take this course

2.Learning goals

2.1.Competences

2.2.Learning goals

2.3.Importance of learning goals

3.Assessment (1st and 2nd call)

3.1.Assessment tasks (description of tasks, marking system and assessment criteria)

4.Methodology, learning tasks, syllabus and resources

4.1.Methodological overview

The methodology followed in this course is oriented towards achievement of the learning objectives. A wide range of teaching and learning tasks are implemented, such as lectures where the main course contents are presented and discussed, computer lab sessions, and student participation.

Students are expected to participate actively in the class throughout the semester.

Classroom materials will be available via Moodle. These include a repository of the lecture notes used in class, the course syllabus, as well as other course-specific learning materials, including a discussion forum.

Further information regarding the course will be provided on the first day of class.

4.2.Learning tasks

The course includes the following learning tasks:

- A01 Lectures (30 hours). The main theoretical contents are presented and student participation is encouraged.
- A02 Practice session (10 hours). Students solve example problems and cases during the classes.
- A03 Computer lab sessions (20 hours). 10 sessions of two hours each will be held in a computer network laboratory. Instructions for each computer/lab session where the different activities are planned will be available before the session. The students will present the results obtained during each one of the practical units once finished.

- A08 Assessment (3 hours). A set of theoretical-practical written tests and reports or papers. Details can be found in the "Assessment" Section.

4.3.Syllabus

- Communication secure services introduction: Motivation and definition.
- Secure service design principles.
- Cryptographic functions for symmetric and asymmetric cryptography.
    - Pseudorandom functions.
    - Block ciphering.
    - Hash functions.
    - Authenticated encryption.
    - Public Key Cryptography.
- Analysis and management tools for secure services.
- Secure services:
    - Confidentiality.
    - Authentication
    - Integrity.
    - Key Distribution
    - Secret Sharing.
    - Blockchains.

4.4.Course planning and calendar

Further information concerning the timetable, classroom, office hours, assessment dates and other details regarding this course, will be provided on the first day of class or please refer to the EINA website.

4.5.Bibliography and recommended resources

http://biblos.unizar.es/br/br_citas.php?codigo=60962&year=2020