Universidad Zaragoza

Academic Year/course: 2024/25

61075 - Advanced security

Syllabus Information

Academic year: 2024/25
Subject: 61075 - Advanced security
Faculty / School: 110 - Escuela de Ingeniería y Arquitectura
Degree: 658 - Master in Telecommunications Engineering
ECTS: 6.0
Year: 1
Semester: Second semester
Subject type: Compulsory
Module:

1. General information

The main objective is to present an overview of some existing methodologies and models for the generation of secure communication services. In addition to knowing the basic security tools (confidentiality, integrity and authenticity), we now need to acquire the ability to design and evaluate more complex services (zero-knowledge proofs, anonymous identification, online gambling, etc.) to have the basis to plan those ones that may arise in a professional future. All of this, without losing support quality of the current services and networks, to continue offering an optimal level of effectiveness and efficiency, and an adequate balance with the security levels required in each proposed service.

2. Learning results

HA_01: Ability to project, compute and design products, processes and facilities in all areas of telecommunication engineering.

HA_04: Ability to carry out mathematical modeling, computation and simulation in technology centres and business engineering, focussing in research, development and innovation tasks in all areas related to Telecommunication Engineering and related multidisciplinary fields.

HA_07: Ability to launch, lead and manage manufacturing processes of electronic and telecommunication equipment, with guarantee of security for people and goods, the final quality of the products and their approval.

HA_13: Ability to design and size networks for transport, diffusion and distribution of multimedia signals.

HA_15: Ability to model, design, implement, manage, drive, produce and maintain networks, services and contents.

HA_16: Ability to carry out planning, decision making and packaging of networks, services and applications considering the quality of service, direct and operative costs, the deployment plan, supervision, security procedures, scaling and maintenance, as well as manage and ensure quality in the development process.

HA_17: Ability to understand and know how to apply the operation and organization of the Internet, new generation Internet technologies and protocols, component models, intermediary software and services.

HA_18: Ability to resolve the convergence, interoperability and design of heterogeneous networks with local, access and trunk networks, as well as the integration of telephony, data, television and interactive services.

CP_06: Permanent self-learning

CP_07: Ability to know how to communicate (orally and in writing) the conclusions - and the knowledge and ultimate reasons that support them - to specialized and non-specialized audiences in a clear and unambiguous way.

3. Syllabus

- Introduction to secure communications services: cause and definition.
- Principles of secure service design.
- Cryptographic operators: symmetric and asymmetric cryptography.
- Pseudo-random functions.
- Block encryption.
- Hash functions.
- Authenticated encryption.
- Public key cryptography.
- Tools for analysis and management of secure services.
- Secure services: confidentiality, authenticity, integrity, key distribution, secret sharing, blockchains, etc.

4. Academic activities

This course is English Language Friendly, which means that: the course syllabus is also available in English; the study and class materials are in English; the faculty is willing to conduct office hours in English; and students are allowed to take their assessments in English.

Master class (30 hours). It will be complemented with the student's previous individual study of bibliographic material and combined with their active participation.

Problem solving and case studies (10 hours). Solving of problems proposed by the teacher, with the possibility of exposition of the same by the students individually or in groups authorized by the teacher.

Laboratory practice (20 hours): students will have 2 hours of practical sessions each week.

Assessment (3 hours) Set of theoretical-practical written tests and presentation of reports or papers used in the evaluation of the student's progress.

5. Assessment system

The student must demonstrate achievement of the intended learning results through the following assessment activities.

The student will have a global test in each one of the calls established throughout the academic year. The dates and times of the tests will be determined by the School. The grade for this test will be obtained as follows:

E1A: theoretical/practical content exam (50%). 0 to 10 points. This is a written exam. This test assesses the learning results. Consequently, the exam includes both theoretical questions and questions involving problem solving, with concrete numerical results. A minimum grade of 4 out of 10 is required to pass the subject.

E1B: Assessment of laboratory practices and practical work (50%). 0 to 10 points. There will be a practice assignment whose delivery and subsequent defence in front of the teacher will provide the grade of the same. A minimum grade of 4 out of 10 is required to pass the subject.

Students will not pass the subject if they do not achieve a minimum grade of 5 out of 10 points in the average of both grades: (E1A + E1B)/2.

6. Sustainable Development Goals

16 - Peace, Justice and Strong Institutions