Universidad Zaragoza

Academic Year/course: 2021/22

60962 - Advanced security

Syllabus Information

Academic Year: 2021/22
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

The main objective of the course is to offer the student an overview of the various existing methodologies and models for the generation of secure communications services. In addition to knowing the basic security tools (confidentiality, integrity and authenticity), we now need to acquire the ability to be able to design and evaluate the possibilities of more complex services (zero knowledge proofs, anonymous identification, online gambling, etc.) to have the basis for planning those may arise in a professional future. And all this, without losing sight of the services and networks that currently support them, to continue offering an optimal level of effectiveness and efficiency, and a suitable balance with the security levels required in each proposed service.

These approaches and objectives are aligned with some Sustainable Development Goals, SDG, of the 2030 Agenda (https://www.un.org/sustainabledevelopment/es/) and some specific targets, in such a way that the acquisition of the Learning outcomes of the subject provides training and competence to the student to contribute to their achievement:

- Goal 16: Promote just, peaceful and inclusive societies.
    - Target 16.5 Substantially reduce corruption and bribery in all their forms.
    - Target 16.6 Develop effective, accountable and transparent institutions at all levels.
    - Target 16.7 Ensure responsive, inclusive, participatory and representative decision-making at all levels.

1.2. Context and importance of this course in the degree

The Advanced Security subject is taught in the first year of the degree, more specifically in the second semester and has a workload of 6 ECTS. The subject is part of the knowledge fiel, Networks and Services within the Telecommunication Technologies module, which covers compulsory competences within the degree of the University Master's Degree in Telecommunication Engineering.

The learning results of this subject will complement the Heterogeneous Networks and New Generation Internet subjects that are part of the Networks and Services field, providing the student with the knowledge they need to plan secure services of telecommunication networks, that is a fundamental aspect for the correct design of any network.

1.3. Recommendations to take this course

In order to continue this subject normally, it is especially recommended that the student, apart from meeting the requirements for the master's degree, has a solid command of the application of security tools in communications and extensive knowledge of its fundamentals.

For optimal use of the subject, the student is recommended to actively attend class (both theory and exercise sessions). In the same way, the student is recommended to take advantage of and respect the teacher's tutoring schedules for the resolution of possible doubts about the subject and a correct follow-up of it.

2. Learning goals

2.1. Competences

CB6 Management of knowledge enough for providing a basis or opportunity to be original in the development and / or

application of ideas, often in a research context.

CB7 Students will know how to apply the acquired knowledge and their ability to solve problems in new or not environments within broader (or multidisciplinary) contexts related to their area of ??study.

CB8 Students will be able to integrate knowledge and face the complexity of formulating judgments based on information that, being incomplete or limited, include reflections on social and ethical responsibilities linked to the application of their knowledge and judgments.

CB9 Students will know how to communicate their conclusions - and the knowledge and ultimate reasons that support them - to specialized and non-specialized audiences in a clear and unambiguous way.

CB10 Students will possess the learning skills that they will continue feeding in a way that will be largely self-directed or autonomous.

CG1 Ability to project, calculate and design products, processes and facilities in all areas of telecommunications engineering.

CG4 Capacity for mathematical modeling, calculation and simulation in technology and engineering company centers, particularly in research, development and innovation tasks in all areas related to Telecommunication Engineering and related multidisciplinary fields.

CG7 Ability to start up, direct and manage electronic and telecommunications equipment manufacturing processes, with a guarantee of safety for people and goods, the final quality of the products and their approval.

CG11 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.

CG12 Possess skills for continuous, self-directed and autonomous learning.

CE4 Ability to design and size transport, broadcast and distribution networks for multimedia signals.

CE6 Ability to model, design, implement, manage, operate, administer and maintain networks, services and content.

CE7 Ability to carry out planning, decision making and packaging of networks, services and applications considering the quality of, direct and operating costs, the implementation plan, supervision, security procedures, scaling and maintenance, as well as manage and ensure quality in the development process.

CE8 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.

CE9 Ability to solve 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.

2.2. Learning goals

To pass this subject, the student must demonstrate the following results:

- Learn about a wide range of cryptographic operators and their efficiency and computational cost characteristics.
- He knows how to properly assess the different cryptographic operators that must be applied for the requirements that a communications scenario can show.
- You can distinguish between the security of an operator and the security of a protocol.
- It extracts, from the purposes of a service, what the security needs will be in its implementation.
- Based on different service requirements, he is able to identify the different security roles that will appear in his modeling.
- It recognizes the correctness in the design of safe services.
- Learn about different modeling tools that will help you establish a security metric.
- Know how to analyze the security level of a service.
- He knows the cryptographic protocols that apply to most security services and is able to adapt them to the needs of a particular implementation.
- It is capable of analyzing a security problem in communications, to later be able to offer design alternatives with the corresponding operators and obtain an optimal solution to the problem posed.

2.3. Importance of learning goals

We can label the subject as fundamental within the knowledge field where it is located, since the design, analysis and implementation of a telecommunications project cannot be understood without a methodology for evaluating security and the possibilities and scope of the services. The course allows the student to know and be able to design and evaluate the scope and security of a communications system and / or modify a previous system to provide it with new management and security capabilities.

3. Assessment (1st and 2nd call)

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

The student must demonstrate that he has achieved the expected learning results through the following evaluation activities

The student will have a global test in each of the calls established throughout the course. The dates and times of the tests will be determined by the School. The qualification of that test will be obtained as follows:

E1A: Exam of theoretical / practical content (50%). Score from 0 to 10 points. It is a written exam. Through this test the learning outcomes are evaluated. Consequently, the exam includes both theoretical questions and other ones that involve exercise solving, with concrete numerical results.

To pass the subject, a minimum score of 4 out of 10 is required in the Theoretical / Practical Content Exam.

E1B: Evaluation of laboratory practices and practical work (50%). Score from 0 to 10 points. There will be a practice whose delivery and subsequent defense in front of the teacher will suppose the grade of the same.

To pass the course, a minimum score of 4 out of 10 is required in the Laboratory Practice Assessment.

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