Academic Year/course: 2022/23

30390 - Network and Service Security

Syllabus Information

Academic Year: 2022/23
Subject: 30390 - Network and Service Security
Faculty / School: 110 - Escuela de Ingeniería y Arquitectura
Degree: 581 - Bachelor's Degree in Telecomunications Technology and Services Engineering
ECTS: 6.0
Year: 4
Semester: First semester
Subject Type: Optional
Module:

1. General information

1.1. Aims of the course

The course and its expected results respond to the following approaches and objectives:

The main objective of the course is to provide the student with a general perspective of the world of cybersecurity both in communication networks and in computer applications and services. Cybersecurity is one of the fundamental pillars for the operation of any ICT system and it is a booming area where a large number of qualified professionals are in demand. The approach is generalist, touching on the most relevant areas of current cybersecurity and going deeper into some of them so that the student can experience this exciting topic in detail. The course starts with the current cryptographic tools capable of offering the 3 basic pillars of security are presented: confidentiality, integrity and authenticity of origin. We continue with the characteristics of cybersecurity networks, services and applications and the tools that we have at our disposal to achieve them. In a third step, the most relevant dangers that communications services and systems face are exposed and how they can be faced, to finish, in a fourth step, putting all these pieces together in a common framework and thus being able to secure and control a system with a high degree of security (as we will see in the course, absolute security does not exist).

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

Goal 8. Decent work and economic growth

> Target 8.2 Achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive sectors

Goal 9: Build resilient infrastructure, promote sustainable industrialization and foster innovation

> Target 9.1 Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all
>
> Target 9.5 Enhance scientific research, upgrade the technological capabilities of industrial sectors in all countries, in particular developing countries, including, by 2030, encouraging innovation and substantially increasing the number of research and development workers per 1 million people and public and private research and development spending
>
> Target 9.C Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020

1.2. Context and importance of this course in the degree

The course of Security in Networks and Services is placed into the fourth year of the degree, more specifically in the autumn semester and has a workload of 6 ECTS. The subject is part of the subject called Design of telematic services that covers compulsory competences within the degree in Telecommunications Technology and Services Engineering in the specific technology of Telematics.

The learning results of this subject will complement the subjects of Transportation of Multimedia Services and Design and Evaluation of Networks that are part of the subject Network architecture and services, as well as Network Management and Electronic Commerce, which are part of the subject Design of Telematic Services, providing the student with the global vision he needs about security in telecommunication networks, a fundamental aspect for the correct operation of any network and system.

1.3. Recommendations to take this course

To follow this course, it is recommended that the student who wants to take it has previously taken the common basic subjects: Fundamentals of Networks, Interconnection of networks and Programming of networks and services.

For optimal use of the subject, the student is recommended to actively attend to class. 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

By studding the subject, the student will be more competent to:

Conceive, design and develop Engineering projects (C1)

Plan, budget, organize, direct and control tasks, people and resources (C2)

Combine general and specialized engineering knowledge to generate innovative and competitive proposals in professional activity (C3)

Ability to solve problems and make decisions with initiative, creativity and critical thinking (C4)

Communicate and transmit knowledge, abilities and skills in Spanish (C5)

Use the engineering techniques, skills and tools necessary to practice it (C6).

Information management, management and application of technical specifications and legislation necessary for the practice of Engineering (C9)

Learn continuously and develop autonomous learning strategies (C10)

Apply information and communication technologies in Engineering (C11)

Build, exploit and manage telecommunications networks, services, processes and applications, understood as systems for capturing, transporting, representing, processing, storing, managing and presenting multimedia information, from the point of view of telematic services (CT1)

Apply the techniques on which telematic networks, services and applications are based, such as management systems, signaling and switching, routing and routing, security (cryptographic protocols, tunneling, firewalls, charging, authentication and content protection mechanisms) , traffic engineering (graph theory, queuing theory and teletraffic) pricing and reliability and quality of service, both in fixed, mobile, personal, local or long distance environments, with different bandwidths, including telephony and data. (CT2)

Follow the technological progress of transmission, switching and process to improve telematic networks and services. (CT5)

Design architectures of networks and telematic services (CT6)

The programming of telematic, networked and distributed services and applications (CT7)

2.2. Learning goals

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

R1. It knows how to classify the different cryptographic operators by means of different metrics of complexity, security, effectiveness, efficiency, versatility, etc.

R2. Know the complexity of the computational problems that sustain these cryptographic operators.

R3. Knows how to characterize the basic cryptographic protocols: confidentiality, authenticity and integrity. It is capable of applying them to different distributed applications.

R4. Know the basics of computer security.

R5. Know the basic tools for the analysis of vulnerabilities in communications networks as well as the techniques and / or tools to alleviate them.

R6. Learn about the protocols to secure the different levels of the TCP / IP architecture.

2.3. Importance of learning goals

We can classify the subject as useful for any itinerary of the degree. In addition, it is essential within the subject in which it is located, since a telematic service cannot be understood without a minimum layer of security. It is also of great interest within the other dominant subject in the itinerary, such as the Architecture of networks and services, to provide security to said networks.

3. Assessment (1st and 2nd call)

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

The student will be able to pass the subject through continuous evaluation, consisting of the completion and delivery of assignments, problems, practices and the completion of an evaluation test.

A. Problems represent 40% of the final grade.

B. Practices will represent 20% of the final grade.

C. The works will represent 20% of the final grade.

D. The evaluation test will represent 20% of the final grade.

To pass the subject by continuous assessment it is necessary that the grade of each of the parts (A, B, C, D) s is higher than 3 points out of 10, and that the average of all the parts is higher than 5.

The student who has not passed the subject by continuous assessment 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 EINA. The qualification of said test will be obtained as follows:

E1: Final exam (100%). Score from 0 to 10 points. It is a written test that can include both problem solving and theoretical and practical questions formulated in multiple-choice test mode (incorrect answers will penalize as 1 / (N-1), with N being the number of possible answers). Through this test, all the learning outcomes defined for the subject are evaluated.

To pass the subject a minimum score of 5 points out of 10 is required in E1.

4. Methodology, learning tasks, syllabus and resources

4.1. Methodological overview

The learning process that has been designed for this subject is based on the following:

The teaching-learning methodologies that will be carried out to achieve the proposed learning results are the following:

Participatory Lectures (30 hours). Presentation by the teacher of the main contents of the subject, combined with the participation of the students. This methodology, supported by individual student study, is designed to provide students with the theoretical foundations of the subject's content.

Laboratory sessions (30 hours). Students will carry out 2-hour practical sessions over 15 sessions.

Guided assignments (15 hours). This non-face-to-face activity will allow progress in all the proposed learning outcomes. The evolution of the work will be presented periodically to the teacher.

Tutoring. Schedule of personalized attention to the student in order to review and discuss the materials and topics presented in both theoretical and practical classes.

Evaluation (4 hours). Set of theoretical written tests - practical and presentation of reports or works used in the evaluation of the student's progress. Details can be found in the section corresponding to evaluation activities

4.2. Learning tasks

As has been described in the methodology, the activities are divided into lectures (30 hours) and laboratory practices (30 hours) in which students will be able to manage and develop security-related programs in which they will have to solve approaches to security scenarios. security applying the knowledge acquired in the master classes. In addition, supervised practical work is carried out (15 hours) where current cybersecurity issues will be addressed.

In a complementary way, the students have hours of tutoring in which they can consult any personal doubts that may have arisen.

4.3. Syllabus

The distribution in thematic units of the theory of the subject will be the following:

1. Introduction to cybersecurity
2. Practical cryptography
3. Security in Applications, Operating Systems and Endpoints
4. Redundant Systems
5. Botnets: SPAM + Fraud + DDoS
6. Malware
7. Security in the TCP / IP architecture
8. Security protocols and VPNs
9. Anonymity on the Internet: TOR + Proxy
10. Cyber ??intelligence: Shodan + Foca

Laboratory practices:

It will comprise 15 sessions of 2 hours each. At the beginning of each practice there will be an exposition of the theoretical foundations necessary to carry it out. The students will later present the results required for each of the practices.

1. External Security Audit
2. Setting up a VPN: openVPN tunnel

3. Implementing Perimeter Security: Firewalls

4. Detecting threats: Intrusion Detection Systems

5. Implementing a SIEM: Elasticsearch

4.4. Course planning and calendar

The course calendar, both for the contact hours and the laboratory sessions, will be defined by the center in the academic calendar of the corresponding course.

The course consists of a total of 6 ECTS credits. The activities are divided into theoretical classes and laboratory practices. Activities, problems, jobs, etc. Their objective is to facilitate the assimilation of theoretical concepts by complementing them with practical ones, so that the basic knowledge and skills related to the competencies provided in the subject are acquired.

The start and end dates of the course and the specific hours of the course, will be made public according to the schedules set by the EINA.

4.5. Bibliography and recommended resources

http://psfunizar10.unizar.es/br13/egAsignaturas.php?codigo=30390