COURSE DATA

DATA SUBJECT

Code: 34896
Name: Computer security
Cycle: Undergraduate Studies
ECTS Credits: 6
Academic year: 2025-26

STUDY (S)

Degree	Center	Acad. year	Period
1403 - Degree in Telematics Engineering	Escola Tècnica Superior d'Enginyeria	3	Sin determinar, Second quarter

SUBJECT-MATTER

Degree	Subject-matter	Character
1403 - Degree in Telematics Engineering	Management of systems	COMPULSORY

COORDINATION

SORIANO GARCIA FRANCISCO R

SUMMARY

Computer Security is an essential component of a computer system. Security requirements can change very quickly. On the one hand, computing dependence for daily life tasks is rapidly increasing. This brings increasing demands and expectations that indeed include security aspects, such as privacy or security in commercial transactions. On the other hand, new technologies are constantly emerging. Although these allow the construction of more sophisticated security mechanisms, they also permit the realization of more sophisticated attacks.

In this context, the subject ¿Computer Security¿ attempts to provide an overview of the essential security elements in a computer system. The contents focus on fundamental principles, and aims at teaching the student to be able to decide on and apply the most appropriate tools and techniques to accomplish the security requirements of a computer system.

The course relies on previous contents introduced in the subjects of networking, operating systems, databases and programming. These are extended with other contents related to computer security, such as security policies, vulnerability assessment, intrusion detection or forensic analysis.

"Information Security " is taught in the second semester of the third year, as part of the module "Computer Systems Administration".

PREVIOUS KNOWLEDGE

RELATIONSHIP TO OTHER SUBJECTS OF THE SAME DEGREE

There are no specified enrollment restrictions with other subjects of the curriculum.

OTHER REQUIREMENTS

It is recommended that the student has completed the following subjects: Computer Science, Advanced Computer Science, Operating Systems and Computer Network Architecture. Among them, the last two are particularly relevant. They address some security-related concepts that are extended in this course

COMPETENCES / LEARNING OUTCOMES

-

E1 - Ability to construct, exploit and manage telecommunication networks, services , processes and applications, understood as systems for the acquisition, transport, representation, processing, storage, management and presentation of multimedia information, from the perspective of telematics services.

E2 - Ability to apply the techniques under the telematic networks, services and applications, such as management systems, signaling and switching, routing, security (cryptographic protocols, tunneling, firewall, collecting mechanisms, authenticating and protecting contents), traffic engineering (graph theory, queuing theory and teletraffic) pricing and reliability and quality of service, in fixed, mobile, personal, local or long distance environments, with different bandwidths, and including telephony and data.

E3 - Ability to construct, operate and manage telematic services using analytical tools for planning, dimensioning and analysis.

G4 - Ability to solve problems with initiative, decision-making and creativity, and to communicate and transmit knowledge, abilities and skills, understanding the ethical and professional responsibility of the activity of a telecommunications technical engineer.

R1 - Ability for self-learning of new knowledge and techniques appropriate for the conception, development and exploitation of telecommunications systems and services.

DESCRIPTION OF CONTENTS

1. Introduction

Security concept
What do we want to protect and why? Security Policy
What do we protect against? Risks and vulnerabilities
The security process
Regulations (ethics, law and standards, ISACA, ISO 27000, IS2)

2. Cryptography

Symmetric cryptography
Public key cryptography
Hashes
Communication and secure storage
Integrity
Digital signature
Public Key Management
Authentication and session key interchange
Privacity
Lab

3. Host based security

Validation and authentication
Access Control
Secure programming
Server and client security
Lab

4. Perimeter Security

Firewall concept
Packet filtering
Proxies
Firewall design
Integration of VPN
Lab

5. Intrusion Detection and Response

Host Intrusion Detection Systems (HIDS)

Network Intrusion Detection Systems (NIDS)
Honeypots and Honeynets
Forensic Analysis
Lab

6. Audit and Ethical Hacking

Introduction to the audit process
The penetration test and types
Phases of an attack / pentest
Tools for ethical hacking

WORKLOAD

PRESENCIAL ACTIVITIES

Activity	Hours
Theory	30,00
Laboratory	20,00
Classroom practices	10,00
Total hours	**60,00**

NON PRESENCIAL ACTIVITIES

Activity	Hours
Attendance at other activities	0,00
Individual or group project	10,00
Independent study and work	30,00
Preparation of lessons	30,00
Preparation for assessment activities	20,00
Resolution of case studies	0,00
Total hours	**90,00**

TEACHING METHODOLOGY

Activities will be conducted according to the following distribution:

- Theoretical activities. During theory lectures, the key and most complex aspects will be explained in detail. Student participation will be promoted (E-2).
- Practical activities. They complement the theoretical activities. These include the following: exercise-based lectures, discussion sessions, labs and scheduled tutorials. During the practical activities, students will apply the foundations of computer security to solve a range of practical challenging problems (G-4, E-2).
- Student¿s individual work. This includes the realization (outside the classroom) of monographs, literature research, questions, problems, and the preparation of classes and exams (study). These are done individually and attempt to promote autonomous learning. (G-4, R-1, E-2).

- Team-Work in small groups. Team work done in small groups (2-4) outside the classroom. This type of activity attempts to develop team work skills (G-4, R-1, E-2).

EVALUATION

First call

The subject may be evaluated in two ways. In the first scheme, both in-class quizzes and the final quiz have a weight in the final mark. In the second scheme, in-class quizzes do not compute. The final grade will be the greater of the grades obtained by using the two schemes.

In the first call the course grade will be composed of the following:

Evaluation of theory and problems (TP).

This part will account for 70% of the final grade. The student will need to obtain a minimum of 4.5 points out of 10 to be able to pass the module. Otherwise the module will be failed. The mark for this part will depend on student participation and three quizzes taken along the course. These are detailed below:

The Continuous Evaluation (EC) component is based on the student¿s participation and involvement in the teaching-learning process. Both regular attendance and in-class activities are considered. This part is not recoverable. (G-4, R-1, E-2)

Quizzes. These consist of two in-class quizzes which will be conducted in the first half of the semester (called T1) and during the second half of the semester (T2), and one final quiz that will conducted outside school hours during the exam period (called T3). (G-4, E-2)

Each of these tests will address all of the subject content taught until the quiz date.

TP is calculated as follows:

TP = 0.15 * EC + 0.15 * T1 + 0,25 * T2 + 0.45 * T3

Evaluation of the laboratory activities (L), which depends on the achievement of objectives in the laboratory sessions. (G-4, E-2)

Labs are carried out in pairs. Laboratory grade accounts for 30% of the final grade. As with TP, it will be necessary to obtain a minimum of 4.5 points out of 10 to be able to pass the module. Otherwise the module will be failed. All lab sessions will have the same weight on the final grade.

Were some student unable to attend a session, lab work should be submitted to the lab instructor before the laboratory session is held. Delivery shall be in person, during tutorial hours. The student should be prepared to answer questions about the work and to re-do parts of it in real-time (with minor changes). This type of delivery will be penalized by subtracting 20% of the grade obtained.

The algorithm used to compute the final grade is given below:

If TP is minor than 4.5 or L is minor than 4.5 final_grade = Minimum (TP, L)

In another case:

final_grade = 0.70 * TP + 0.30 * L

In the case of not having passed the subject following the continuous assessment (or in the case that the mark calculated in this second way is more favourable for the student), the the mark calculated in this second way would be more favourable for the student), the T3 will be the final exam of the subject and TP will be calculated in the following way:

TP = 0.15 * EC + 0.85 * T3

The final mark will be calculated in the same way as for continuous assessment.

Second Call

In the second call, the course will be assessed in the same way as in the first call, with the following exceptions.

a.- There will be a deadline for the delivery of labs with the same conditions as in the first call (logically they will not be carried out in the laboratory), except that the penalty will be 30% and that the delivery must be done before the exam of the second call.

b.- The exam of the second round will replace the T3 test.

c.- In the EC part, the student's mark will be maintained.

Advance Call

To apply for an advance call, students must have previously taken the course and have obtained the minimum mark required in assessing the practical laboratory activities (L). In this way, it is attempted to reconcile the right of students to an advance call with the subject's teaching methodology and evaluation criteria.

In any case, the evaluation system will be governed by what is established in the Evaluation and Qualification Regulations of the Universitat de València for degrees and masters (**ACGUV 108/2017**).

Copying or plagiarism of any activity that is part of the evaluation will result in the impossibility of passing the course, and the student will then be subject to the appropriate disciplinary procedures indicated in the ACTION PROTOCOL FOR FRAUDULENT PRACTICES AT THE UNIVERSITY OF VALENCIA (ACGUV 123/2020).

REFERENCES

Main:

- Pfleeger, Charles P., et al. Security in Computing. Sixth edition., Addison Wesley Professional,

2024
- Kizza, Joseph Migga. Guide to Computer Network Security. 6th ed. 2024., Springer International Publishing, 2024, https://doi.org/10.1007/978-3-031-47549-8

Secondary:

- Vacca, John R., editor. Computer and Information Security Handbook. Volume 1. Fourth edition., Morgan Kaufmann, 2025
- Pfleeger, Charles P., and Shari Lawrence Pfleeger. Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach. 1st edition, Prentice Hall, 2012
- Tanenbaum, Andrew S., and David J. Wetherall. Computer Networks. 5th ed., Pearson, 2014.
- Schneier, Bruce. Applied Cryptography¿: Protocols, Algorithms, and Source Code in C. 20th anniversary edition., Wiley, 2015.
- Zwicky, Elizabeth D., et al. Building Internet Firewalls. 2nd ed., O¿Reilly, 2000.
- Northcutt, Stephen. Inside Network Perimeter Security. 2nd ed., Sams, 2005.
- Khan, Umer. Cisco PIX Firewalls: Configure / Manage / Troubleshoot. 1st ed., Elsevier Science & Technology Books, 2005, https://doi.org/10.1016/B978-1-59749-004-7.X5000-6.
- Sammons, John. The Basics of Digital Forensics¿: The Primer for Getting Started in Digital Forensics. Second edition., Syngress, 2015.
- Nikkel, Bruce. Practical Linux Forensics. No Starch Press, 2021
- Carrier, Brian. File System Forensic Analysis. Addison-Wesley, 2005
- Farmer, Dan, and Wietse Venema. Forensic Discovery. Addison-Wesley, 2004.
- Shiva V. N. Parasram. Digital Forensics with Kali Linux - Second Edition. Packt Publishing, 2020.
- Cannon, David, et al. CISA¿: Certified Information Systems Auditor Study Guide. 4th ed., Sybex, a Wiley brand, 2016.
- Engebretson, Patrick. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Second edition, Elsevier Science, 2013.
- Graham, Daniel. Ethical Hacking. No Starch Press, 2021.
- Sheikh, Ahmed. Certified Ethical Hacker (CEH) Preparation Guide¿: Lesson-Based Review of Ethical Hacking and Penetration Testing. 1st ed., Apress, 2021, https://doi.org/10.1007/978-1-4842-7258-9.
- Velu, Vijay Kumar. Mastering Kali Linux for Advanced Penetration Testing¿: Become a Cybersecurity Ethical Hacking Expert Using Metasploit, Nmap, Wireshark, and Burp Suite. Fourth edition., Packt Publishing, Limited, 2022.