# Information and Security Management

Code: 102757
ECTS Credits: 6

2024/2025

| Degree | Type | Year |
|---|---|---|
| 2502441 Computer Engineering | OB | 3 |
| 2502441 Computer Engineering | OT | 4 |

## Contact

Name: Guillermo Navarro Arribas

Email: guillermo.navarro@uab.cat

## Teaching groups languages

You can view this information at the end of this document.

## Prerequisites

There are no official requirements, but it is recommended to have basic knowledge of cryptography, computer networks and programming. This knowledge is achievable with previous courses of the degree: Networking, Information and Security, Information Technology Foundations, and Programming Methodology. It is the student respsibility to adquire these knowledge.

## Objectives and Contextualisation

The aim of this course is to provide students with a basic knowledge about the problem of information security and existing mechanisms for the protection of computer systems. Students will be able to develop a critical view of the security in computer systems. Furthermore students will be able to implement some aspects of the subject. Knowing how to perform certain attacks is an important step towards understanding the needs of system security, and to then apply appropriate protection techniques in each case.

## Competences

Computer Engineering

- Acquire thinking habits.
- Capacity to design, develop, evaluate and ensure the accessibility, ergonomics, usability and security of computer systems, services and applications, as well as of the information that they manage.
- Capacity to determine the requirements of information and communication systems in an organisation attending to security aspects and fulfilment of applicable standards and legislation.
- Conceive and develop centralised or distributed computer systems or architectures by integrating hardware, software and networks.
- Have the capacity to understand, apply and manage the guarantee and security of computer systems.
- Work in teams.

## Learning Outcomes

1. Collaborate in the design and follow-up of computer system security policies.
2. Design systems for protecting information: access control and integrity.
3. Determine security and confidentiality requirements, and identify the main types of attacks and threats.
4. Determine security requirements, applicable standards and legislation in the information and communication systems of an organisation.
5. Develop a mode of thought and critical reasoning.
6. Know and understand the technical possibilities of implanting security policies in distributed systems.
7. Know the principles of computer forensics and cybercrime treatment .
8. Understand security principles and apply them to the preparation and execution of action plans.
9. Work cooperatively.

## Content

Security Mechanisms

- Authentication
- Authorization and access control
- Public Key Infrastructure
- Software security
- Malware detection and Intrusion Detection
- Data Privacy

Security management and other aspects

- Vulnerability Management
- Threat modeling, pentesting
- Risk Management

In this course we see specific mechanisms for the design of information protection, access control and integrity. We also study an global overview of information security, vulnerability management, threat modeling, risk management, and we introduce disciplines such as computer forensic. Note that the order of topics may vary during the curse due to teaching planning.

## Activities and Methodology

| Title | Hours | ECTS | Learning Outcomes |
|---|---|---|---|
| Type: Directed | | | |
| Laboratory sessions | 12 | 0.48 | 1, 8, 7, 6, 5, 4, 3, 2, 9 |
| Practical (exercises) lectures | 12 | 0.48 | 1, 8, 7, 6, 5, 4, 3, 2, 9 |
| Theoretical lectures | 26 | 1.04 | 1, 8, 7, 6, 5, 4, 3, 2 |
| Type: Supervised | | | |
| Tutorized work | 18 | 0.72 | 1, 8, 7, 6, 5, 4, 3, 2 |
| Type: Autonomous | | | |
| Preparation and study of autonomous work (laboratories and exercises) | 45 | 1.8 | 1, 8, 7, 6, 5, 4, 3, 2, 9 |

| | | | |
|---|---|---|---|
| Study and preparation of assessments | 30 | 1.2 | 1, 8, 7, 6, 5, 4, 3, 2 |

The subject is developed in 50 hours of directed activities distributed in sessions for theory, problems and laboratory. The course is divided into a supervised part that will be held in classroom sessions (theory, problems and laboratory), and an unsupervised part that students will perform autonomously.

More specifically, the directed activities are:

- Theory sessions: where the teacher will provide information about the knowledge of the subject and strategies to acquire, expand and organize this knowledge. These sessions may include sessions given by professionals in the field of computer security in the form of seminars.
- Problems sessions: where students will work on problems or activities in group or individually (depending of the concrete activity). This work may consist of a part of supervised work and a part of autonomous work.
- Practical sessions in the laboratory: where topics related to those exposed in theory sessions will be dealt with in depth and at a practical level.

Throughout the course, the Moodle of the UAB Virtual Campus will be used as the main means of communication between teachers and students. This includes the publication of materials, publication of partial marks, discussion forum, ...

Annotation: Within the schedule set by the centre or degree programme, 15 minutes of one class will be reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

## Assessment

## Continous Assessment Activities

| Title | Weighting | Hours | ECTS | Learning Outcomes |
|---|---|---|---|---|
| Individual assessment | 45% | 3 | 0.12 | 1, 8, 7, 6, 5, 4, 3, 2 |
| Labs | 40% | 2 | 0.08 | 1, 8, 7, 6, 5, 4, 3, 2, 9 |
| Problems, exercises, and activities | 15% | 2 | 0.08 | 1, 8, 7, 6, 5, 4, 3, 2, 9 |

The evaluation activities are divided into individual and collective activities, both practical and theoretical. These activities will be carried out continuously throughout the course.

Final evaluation and grades:

Regarding the continuous evaluation that will be carried out during the course, it is planned to carry out:

- 2 partial tests of individual evaluation. The minimum grade required for each of the tests will be 4.5 out of 10.
- Evaluation of practices in the laboratory. The minimum grade required for each of the practices will be 4.5 out of 10.
- Evaluation of problems/activities (work done outside the classroom or in the corresponding class sessions). This part does not require a minimum grade.

In order to pass the subject, it is necessary that the evaluation of each one of the parts exceed the minimum required and that the total evaluation exceed 5 points.

In case of not passing the subject due to the fact that any of the evaluation activities does not reach the minimum required grade, the numerical grade of the file will be the lowest value between 4.5 and the weighted average of the grades.

The qualification of "*no evaluable*" will be awarded to students who do not participate in any of the evaluation activities.

Awarding a grade with honors (MH) is the decision of the faculty responsible for the subject. The UAB regulations indicate that the MH may only be awarded to students who have obtained a final grade equal to or greater than 9.00. Up to 5% MH of the total number of students enrolled can be awarded.

Recovery of continuous assessment notes:

There will be a final recovery exam that will allow students to recover the partial exams. Likewise, a final delivery will be allowed to recover those suspended labs (this additional delivery will entail a penalty in the final grade of the practice). The part of problems and activities that does not require a minimum grade cannot be recovered.

The student can take the recovery provided they have taken a set of activities that represent a minimum of two thirds of the total grade for the subject.

Partial validations for repeating students:

Initially, the possibility of validating parts of the subject is not considered, nor it is possible to carry out special tests for repeating students. Even so, this fact can be reconsidered at the beginning of the course, depending on the contents of each part.

Dates of evaluation activities:

The dates of continuous evaluation and delivery of work and practices will be published on the virtual campus and may be subject to changes in programming for reasons of adaptation to possible incidents. These changes will always be reported on the virtual campus, since it is understood that it is the usual mechanism for exchanging information between teachers and students.

Likewise, the evaluation mechanisms, methodology or general operation of the subject that have not been specified in this guide will be detailed with sufficient time in advance.

Grade Review Procedure

For each evaluation activity, a place, date and review time will be indicated in which the students will be able to review the activity with the teaching staff. In this context, claims may be made about the grade for the activity, which will be evaluated by the teaching staff responsible for the subject. If the student does not show up for this review, this activity will not be reviewed later.

Ethical commitment:

Without prejudice to other disciplinary measures deemed appropriate, and in accordance with current academic regulations, irregularities committed by a student that may lead to a grade variation in an any activity will be graded zero (0). The evaluation activities qualified in this way and by this procedure will not be recoverable. If it is necessary to pass any of these evaluation activities to pass the subject, this subject will be directly suspended, with no opportunity to recover it in the same course. These irregularities include, among others:

- the total or partial copy of a practice, report, or any other evaluation activity;
- to let copy;
- to present a group work not carried out entirely by the members of the group (applied to all members, not only to those who have not worked);
- unauthorized use of AI (e.g. Copilot, ChatGPT or equivalent) to solve exercises, labs and/or any other

activity;
- to submit as your own, materials prepared by a third party, even if they are translations or adaptations, and generally works with non-original and exclusive elements of the student;
- to have communication devices (such as mobile phones, smart watches, camera pens, etc.) accessible during individual theoretical-practical assessment tests (exams);
- to talk with classmates during individual theoretical-practical evaluation tests (exams);
- to copy or try to copy from other students during the theoretical and practical evaluation tests (exams);
- the use or attempt to use writings related to the subject during the theoretical-practical evaluation tests (exams), when these have not been explicitly allowed.

The numerical mark of the file will be the lower value between 3.0 and the weighted average of the marks in case the student has committed irregularities in an act of evaluation (and, therefore, it will not be possible to pass by compensation). In future editions of this course, students who have committed irregularities in an evaluation act will not have any of the evaluation activities carried out validated.

In summary: copying, allowing copying or plagiarism (or the attempt to) in any of the evaluation activities is equivalent to a FAIL, non-compensable and without validation of parts of the subject in subsequent courses.

Single evaluation

The single evaluation of the subject will consist of the following evaluation activities:

- Individual exam: specific individual exam for students with single evaluation on the content of the subject, 50% of the final grade.
- Practices: delivery and validation of the practices that will be proposed specifically for single assessment students, 50% of the final grade.

The same recovery system will be applied as in the case of continuous evaluation but with respect to single evaluation activities. The review of the final grade follows the same procedure as for the continuous assessment.

## Bibliography

Main bibliography:


- Paul C. van Oorschot (2021) Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin, Second Edition. https://people.scs.carleton.ca/~paulv/toolsjewels.html


Complementary:


- Mark Stamp (2022) Information Security: principles and practice, Third Edition. Wiley. https://bibcercador.uab.cat/permalink/34CSUC_UAB/avjcib/alma991010618636406709
- Adam Shostack (2014) Threat Modeling. Designing for security. John Wiley & Sons. https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010486872806709
- Xabiel García Pañeda, David Melendi Palacio (2008) La peritación informática, un enfoque práctico, Colegio Oficial de Ingenieros en Informática Principado de Asturias. https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991007440409706709
- Vicenç Torra (2022) Guide to data privacy : models, technologies, solutions. Springer. https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010721333006709
- Wenliang Du (2021) Computer Security. A Hands-on Approach. Third Edition. https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010604568906709
- Matt Bishop (2019) Computer Security: Art and Science, Second Edition. Addison-Wesley. https://bibcercador.uab.cat/permalink/34CSUC_UAB/avjcib/alma991010604569006709

- Dieter Gollmann (2011) Computer Security, 3rd Edition. John Wiley & Sons. https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991004205279706709
- Michael Sikorski, Andrew Honig (2012) Practical Malware Analysis. The hands-on guide to dissecting malicious software. No Starch Press. https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010489658406709


## Software

Given the multidisciplinary nature of this subject, we will use different tools and programming languages depending on the specific activity to be carried out, both for the labs and for the activities and exercises. We might use programming languages such as Python, or C, and different applications and system tools.

## Language list

| Name | Group | Language | Semester | Turn |
|---|---|---|---|---|
| (PAUL) Classroom practices | 451 | Catalan/Spanish | second semester | morning-mixed |
| (PAUL) Classroom practices | 452 | Catalan/Spanish | second semester | morning-mixed |
| (PLAB) Practical laboratories | 451 | Catalan | second semester | morning-mixed |
| (PLAB) Practical laboratories | 452 | Catalan | second semester | morning-mixed |
| (PLAB) Practical laboratories | 453 | Catalan | second semester | morning-mixed |
| (PLAB) Practical laboratories | 454 | Catalan | second semester | morning-mixed |
| (PLAB) Practical laboratories | 455 | Catalan | second semester | morning-mixed |
| (TE) Theory | 450 | Catalan/Spanish | second semester | morning-mixed |