UAB
Universitat Autònoma de Barcelona

Information and Security Management

2026/2027

Code: 102757
Credits: 6

Degree programme	Type	Course
Computer Engineering	OB	3
Computer Engineering	OP	4

Contact lecturer

Name : Guillermo Navarro Arribas

Email : guillermo.navarro@uab.cat

Teaching staff

Carlos Garrigues Olivella

Group languages

You can consult this information at the end of the 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.

Objectives

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.

Learning outcomes

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

9. Work cooperatively.

Contents

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

Learning activities and methodology

Title	Hours	ECTS	Learning outcomes
Theoretical lectures	26	1.04	1, 2, 3, 4, 5, 6, 7, 8
Preparation and study of autonomous work (laboratories and exercises)	45	1.8	1, 2, 3, 4, 5, 6, 7, 8, 9
Study and preparation of assessments	30	1.2	1, 2, 3, 4, 5, 6, 7, 8
Laboratory sessions	12	0.48	1, 2, 3, 4, 5, 6, 7, 8, 9
Tutorized work	18	0.72	1, 2, 3, 4, 5, 6, 7, 8
Practical (exercises) lectures	12	0.48	1, 2, 3, 4, 5, 6, 7, 8, 9

The subject is developed over 50 hours of guided activities divided into theory, problem-solving, and laboratory sessions. The approach to the subject will emphasize supervised work on specific aspects of the course. This work is divided into a supervised part carried out during class sessions, and an unsupervised part that students will complete autonomously.

More specifically, the guided activities are:

- Theory and problem-solving sessions: the teaching staff will provide information on the subject's knowledge and on strategies to acquire, expand, and organize this knowledge. Active student participation will be encouraged, and learning will be monitored through individual or group activities.
- Laboratory practice sessions: where topics related to those presented in the theory sessions will be covered in depth and at a practical level.

Throughout the course, the Moodle classroom of the UAB Virtual Campus will be used as the main means of communication between teaching staff and students.

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

Continuous assessment activities

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

Final assessment and grading:

For the continuous assessment carried out during the course, the following is planned:

- 2 individual midterm exams. The minimum required grade for each exam is 4.5 out of 10.
- Laboratory practical assessment. The minimum required grade for each practical is 4.5 out of 10.
- Assessment of problems/activities. This part does not require a minimum grade.

To pass the course, the assessment of each part must exceed the required minimum, and the overall assessment must exceed 5 points. If a student fails the course because one of the assessment activities does not reach the minimum required grade, the numerical grade on their transcript will be the lower of 4.5 or the weighted average of the grades.

The grade "not assessable" will be given to students who do not participate in any of the assessment activities.

For each assessment activity, a location, date, and time for review will be indicated, during which students may review the activity with the teaching staff. In this context, complaints about the grade of the activity may be submitted, which will be evaluated by the teaching staff responsible for the course. If a student does not attend this review, the activity will not be reviewed afterward.

Awarding of honors (Matrícula de Honor): honors may only be awarded to students who have obtained a final grade equal to or higher than 9.00. Up to 5% of enrolled students may receive honors.

Resit/recovery of continuous assessment grades:

- A final resit exam will be held, allowing the midterm exams to be resat separately.
- Likewise, failed practicals may be resubmitted (this additional submission will incur a penalty on the final grade for the practical).
- The assessment of problems/activities cannot be resat, but students may choose (at the start of the course) to be assessed on this part through an additional activities test held on the same day as the knowledge-validation resit exam.

Partial credit transfer for repeating students: Initially, there is no plan to allow credit transfer for parts of the course, nor special tests for repeating students. However, this may be reconsidered at the start of the course depending on the content of each part.

Activity schedule: Dates for continuous assessment and submission of assignments and practicals will be published on the virtual campus and may be subject to scheduling changes to accommodate possible incidents. Any such changes will always be announced on the virtual campus, as this is understood to be the standard channel of communication between teaching staff and students. Likewise, assessment mechanisms, methodology, or general operation of the course not specified in this guide will be detailed with sufficient advance notice.

Ethical commitment: Without prejudice to other disciplinary measures deemed appropriate, and in accordance with current academic regulations, irregularities committed by a student that could lead to a change in the grade of an assessable activity will be graded with a zero (0). Assessment activities graded in this way through this procedure cannot be resat. If passing any of these assessment activities is required to pass the course, the course will be failed outright, with no opportunity to resit it in the same academic year. These irregularities include, among others:

- copying, in whole or in part, a practical, report, or any other assessment activity;
- allowing someone to copy from you;
- submitting group work not carried out entirely by the group members (this applies to all members, not only those who did not contribute);
- unauthorized use of AI (e.g., Copilot, ChatGPT, or equivalents) to solve exercises, practicals, and/or any other assessable activity;
- presenting as one's own material produced by a third party, even if translated or adapted, and in general submitting work with elements that are not original and exclusive to the student;
- having communication devices (such as mobile phones, smartwatches, camera pens, etc.) accessible during assessment activities;
- talking to classmates during assessment activities;
- copying or attempting to copy from other students during assessment activities;
- using or attempting to use subject-related written materials during assessment activities when these have not been explicitly authorized.

The numerical grade on the transcript will be the lower of 3.0 or the weighted average of the grades if the student has committed irregularities in an assessment activity (and, therefore, a passing grade through compensation will not be possible). In future editions of this course, students who have committed irregularities in an assessment activity will not be granted credit transfer for any assessment activities already completed. In summary: copying, allowing copying, or plagiarizing (or attempting to do so) in any assessment activity results in a FAIL, non-compensable, with no credit transfer for parts of the course in subsequent years.

For this course, the use of artificial intelligence (AI) technologies is permitted exclusively for support tasks, such as bibliographic or information searches, text correction, or translations. Students must clearly identify which parts have been generated using this technology, specify the tools used, and include a critical reflection on how these have influenced the process and final result of the activity. Lack of transparency regarding AI use in assessable activities will be considered a breach of academic integrity and may result in a partial or total penalty on the activity's grade, or more severe sanctions in serious cases.

Single assessment (Avaluació única): The single assessment option for the course will consist of the following assessment activities:

- Individual exam: individual exam on the course content, 75% of the final grade.
- Labs: submission and examination of the practicals specifically proposed for students under the single assessment option, 50% of the final grade.
- The same resit system used for continuous assessment will apply, but with respect to the single assessment activities. The review of the final grade follows the same procedure as for 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.

Course groups and languages

The information provided is provisional until November 30. After this date, you will be able to consult the language of each group through this link. To access the information, you will need to enter the course CODE

Type of teaching	Group	Language	Semester	Shift
(TE) Theory	450	Catalan/Spanish	second semester	morning-mixed
(PAUL) Classroom practices	451	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	451	Catalan/Spanish	second semester	morning-mixed
(PAUL) Classroom practices	452	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	452	Catalan/Spanish	second semester	morning-mixed
(PAUL) Classroom practices	453	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	453	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	454	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	455	Catalan/Spanish	second semester	morning-mixed