Universitat Autònoma de Barcelona

2020/2021

Information and Security Management

Code: 102757
ECTS Credits: 6

Degree	Type	Year	Semester
2502441 Computer Engineering	OB	3	2
2502441 Computer Engineering	OT	4	2

The proposed teaching and assessment methodology that appear in the guide may be subject to changes as a result of the restrictions to face-to-face class attendance imposed by the health authorities.

Contact

Name: Guillermo Navarro Arribas
Email: Guillermo.Navarro@uab.cat

Use of Languages

Principal working language: catalan (cat)
Some groups entirely in English: No
Some groups entirely in Catalan: Yes
Some groups entirely in Spanish: No

Teachers

Jordi Casas Roma

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
- Computer forensic
- Social Engineering

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.

Methodology

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, ...

Activities

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

Assessment

The overall assessment of the subject will be based on the follow-up of the students during the course. It is divided mainly into two blocks:

- Individual assessment: with concrete evidences on the content of the subject and evaluation of the supervised work individually. Although there may be a part of practical assessment, it is mostly theoretical work.
- Collective evaluation: consists mainly of the evaluation of the supervised work, both theoretical and practical.

As you can see, the evaluation activities are divided into individual and collective test or assessments, both practical and theoretical. Individual tests will be carried out throughout the course on a continuous basis. However, a final test is expected to allow the partial evaluation of the individual test to be recovered.

Final evaluation:

During the continuous evaluation of the course, there will be:

- 2 partial individual tests. The minimum mark required for each of the tests is 4.5 out of 10.
- Evaluation of laboratory sessions. The minimum grade required for each of the practices is 4.5 out of 10.
- Evaluation of supervised work (work done outside the classroom) and problems or activities in problem sessions. This part does not require a minimum mark.

To be able to pass the subject, the evaluation of each one of the parts must exceed the minimum required in each case and that the total evaluation has to exceed 5 points over 10.

If you do not pass the subject due to the fact that some of the evaluation

activities do not reach the minimum grade required, the numerical final mark will be the lowest value between 4.5 and the weighted average of the marks.

The "non-assessed" qualification will be awarded to students who do not participate in any of the assessment activities.

The qualification of "with honors" will be awarded to students with a mark equal to or greater than 9 by order of the best final grade.

Recovery of marks from the continuous assessment:

A final test will be carried out that will allow the recovery of partial tests. There will also be also a final opportunity to recover the
laboratory practices (which will carry a penalty on the mark). The part of problems and / or activities that do not require a minimum mark can not be recovered.

Keeping partial marks for repeating students:

Repeating students will not keep the partial marks from previous years in the current course. However this fact can be reconsidered at the beginning of the course depending on the availability of resources and specific content of the assessed parts.

Dates for assessment activities:

The dates for test, assessments, work and practices deliveries will be published on the virtual campus and may be subject to change. All this changes will be always informed in the virtual campus, which is understood as the usual mechanism for exchanging information between teachers and students.

Likewise, the assessment mechanism, text, methodology or general operation of the course, that have not been specified in this guide will be detailed in advance.

For each assessment activity, a place, date and time of revision will be indicated in which the student will be able to review the activity with the teacher. In this context, claims can be made about the activity mark, which will be evaluated by the responsible teacher for the subject. If the student does not submit to this review, this activity will not be reviewed later.

Ethical Commitment:

Notwithstanding other disciplinary measures deemed appropriate, and in accordance with the academic regulations in force, the irregularities committed by a student who can lead to a variation of the qualification will be qualified with zero (0). The assessment activities qualified in this way and by this procedure will not be recoverable. If you need to pass any of these assessment activities to pass the subject, this subject will be failed
directly, without 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;
- present a group work not done entirely by the members of the group;
- present as 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;
- have communication devices (such as mobile phones, smartphones, smartwatches, etc.) accessible during theoretical-practical assessment tests.

In these cases the final mark of the subject will be the lowest value between 3.0 and the weighted average of the marks (and therefore it will not be

possible to pass the course by compensation).

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

Bibliography

In an orientative way the following bibliography is given:

- Mark Stamp (2011) Information Security: principles and practice, 2n Edition. John Wiley & Sons.
- Adam Shostack (2014) Threat Modeling. Designing for security. John Wiley & Sons.
- Xabiel García Pañeda, David Melendi Palacio (2008) La peritación informática, un enfoque práctico, Colegio Oficial de Ingenieros en Informática Principado de Asturias.
- Vicenç Torra (2017) Data Privacy: Foundations, New Developments and the Big Data Challenge. Springer.
- Peter Szor (2005) The Art of Computer Virus Research and Defense. Adisson-Wesley.
- Wenliang Du (2017) Computer Security. A Hands-on Approach
- Matt Bishop (2002) Computer Security: Art and Science, Addison-Wesley.
- Dieter Gollmann (2011) Computer Security, 3rd Edition. John Wiley & Sons