Universidad de Alcalá

TEACHING GUIDE

Security

Degree in
Information System Engineering (GISI)
Computer Engineering (GIC)
Computer Science Engineering (GII)

Universidad de Alcalá

Academic Year 2023/2024

4th Year - 2nd Semester (GISI+GIC+GII)

Approved by the School Board on June 12th, 2023

TEACHING GUIDE

Course Name:	**Security**
Code:	**780036 (GISI+GIC+GII)**
Degree in:	**Information System Engineering (GISI)** **Computer Engineering (GIC)** **Computer Science Engineering (GII)**
Department and area:	**Automática** **Telematics Engineering**
Type:	**Optional (Generic) (GISI+GIC+GII)**
ECTS Credits:	**6.0**
Year and semester:	**4th Year - 2nd Semester (GISI+GIC+GII)**
Teachers:	Susel Fernández Melián
Tutoring schedule:	Consultar al comienzo de la asignatura
Language:	Spanish/English Friendly

1. COURSE SUMMARY

Information stored in computers and exchanged between them through communication networks may have great value for people, organizations and companies. Since it is available through a communications network such as the Internet, it can be accessible to a large number of people, among which there will be some with malicious intent. This means that the information is subject to a large number of threats and therefore increases the risk of being lost, modified or eavesdropped without authorization, in acts that we know today as cybercrime or human failures, equipment breakdowns or accidents. For these reasons, information security is a fundamental aspect of today's society, and the necessary capabilities to analyze the level of information security and take appropriate protection measures have a high demand in the business world.

This course delves into the technical aspects related to information security, once students have acquired the basic knowledge that supports the technology that allows generating, exchanging and storing information, in the Network Architecture I and Network Architecture II courses.

The course is structured in four parts:

1. Information Security, where the cryptographic procedures that allow processing the information itself to hide it or have guarantees that it has not been generated or modified without authorization are analyzed.
2. Access control, where the main mechanisms that exist to prevent access to information by unauthorized parties and mechanisms to detect attempts of unauthorized access are studied.
3. Security protocols: where the main global security solutions that are used to protect information in different classic environments are analyzed, usually a composition of mechanisms seen in parts 1 and 2.
4. System Security, where the main attacks that can occur against the systems that have and process information are analyzed, such as personal computers, smartphones or servers and the different applications that run on them, focusing in the methodologies to assess the level of security of these systems through an audit process.

2. SKILLS

Basic, Generic and Cross Curricular Skills.

This course contributes to acquire the following basic, generic and cross curricular skills:

en_CG3 - Ability to design, develop, evaluate and ensure accessibility, ergonomics, usability and security of computer systems, services and applications, as well as the information they manage.

en_CG9 - Ability to solve problems with initiative, decision making, autonomy and creativity. Ability to know how to communicate and transmit the knowledge, skills and abilities of the profession of Computer Engineering Engineer.

en_CG10 - Knowledge to perform measurements, calculations, assessments, appraisals, appraisals, studies, reports, task planning and other similar computer work, in accordance with the knowledge acquired as set out in section 5, annex 2, of BOE resolution -A-2009-12977.

en_CG11 - Ability to analyze and assess the social and environmental impact of technical solutions, including the ethical and professional responsibility of the activity of the Technical Computer Engineer.

en_CB1 - That students have demonstrated to possess and understand knowledge in an area of study that is based on general secondary education, and is usually found at a level that, although supported by advanced textbooks, also includes some aspects that involve knowledge from the

forefront of their field of study.

en_CB2 - That the students know how to apply their knowledge to their work or vocation in a professional manner and possess the competencies that are usually demonstrated through the elaboration and defense of arguments and the resolution of problems within their area of study.

en_CB3 - That students have the ability to gather and interpret relevant data (usually within their area of study) to make judgments that include a reflection on relevant social, scientific or ethical issues.

en_CB4 - That students can transmit information, ideas, problems and solutions to both a specialized and non-specialized public.

en_CB5 - That the students have developed those learning skills necessary to undertake further studies with a high degree of autonomy.

en_TRU1 - Capacity of analysis and synthesis.

en_TRU2 - Oral and written competencies.

en_TRU3 - Ability to manage information.

en_TRU4 - Autonomous learning skills.

en_TRU5 - Team work.

Specific Skills

This course contributes to acquire the following specific skills:

en_CIC6 - Ability to understand, implement and manage the guarantee and security of computer systems.

en_CSI2 - Ability to determine the requirements of information and communication systems of an organization considering aspects of security and compliance with regulations and legislation.

en_CSI5 - Ability to understand and apply the principles of risk assessment and apply them correctly in the development and implementation of action plans.

Learning Outcomes

After succeeding in this subject the students will be able to:

RA1. Use cryptographic mechanisms to manage information security risks, evaluating the implications of using the different available mechanisms.

RA2. Choose and deploy security mechanisms (controls) for prevention, detection and reaction over network devices and services, including firewalls, intrusion detection systems and security policies.

RA3. Assess the security risks in a given information system, according to the inventory of system assets and the threats and vulnerabilities that affect them.

RA4. Build security solutions feasible for specific scenarios, using different cryptography mechanisms and security applications.

RA5. Collect evidence on security incidents of systems, search for information about them and perform the analysis and subsequent communication of conclusions as part of a research team.

RA6. Work as a team in a collaborative way to solve problems related to network and systemsecurity and effectively communicate their knowledge, procedures, results and ideas, in both oral and written form.

3. CONTENTS

Contents Blocks	Total number of hours
Information security. Introduction; symmetric cryptography: DES, 3DES, AES; symmetric cryptography: RSA, ECC, hash functions, hmac.	20 hours
Access control. Authentication: passwords, Single Sing On (SSO), biometry; uthorization: access control lists (ACLs), multilevel models; Mechanisms: firewalls, intrusion detection systems (IDS).	20 hours
Security protocols: authentication, mutual authentication, man-in-the-middle attacks; security in the Internet protocols.	8 hours
Systems security: vulnerabilities and threats, vulnerability analysis; software security: privilege escalation, malware; security in Web applications; systems audit.	8 hours

4. TEACHING - LEARNING METHODOLOGIES. FORMATIVE ACTIVITIES.

4.1. Credits Distribution

Number of on-site hours:	58 hours (56 hours on-site +2 exams hours)
Number of hours of student work:	92
Total hours	150

4.2. Methodological strategies, teaching materials and resources

The teaching strategy of the course is divided into 3 sections: classroom learning, learning in small groups and finally the working sessions in the laboratory.

Classroom sessions:

Working sessions in the classroom, in large groups, will consist of lectures where the main concepts of the theory of circuits will be presented. The aim is to introduce students to the theoretical foundations of circuit analysis in a guided and reflective way. The understanding of these concepts will culminate with the use of them in both the laboratory and the problem solving sessions in small groups.

Teaching materials will be essential to create reflective learning environments, where students and teachers can undertake a critical analysis that allows the student to autonomously relate concepts.

The order of presentation of the contents will evolve from the simple to the complex, in order to avoid a high degree of abstraction that might cause a student lack of interest in the course. In any case, it is very convenient, during the working sessions in the classroom, to establish linkages with other subjects in the curriculum, and to provide possible experience on the contents, which will help to attract students' attention and will encourage their interest in the subject.

5. ASSESSMENT: procedures, evaluation and grading criteria

5.1. PROCEDURES

The evaluation must be inspired by the criteria of continuous evaluation (Learning Assesment Guidelines, LAG, art 3). However, in compliance with the regulations of the University of Alcalá, an alternative process of final evaluation is made available to the student in accordance with the Learning Assesment Guidelines as indicated in Article 10, students will have a period of fifteen days from the start of the course to request in writing to the Director of the Polytechnic School their intention to take the non-continuous evaluation model adducing the reasons that they deem convenient. The evaluation of the learning process of all students who do not apply for it or are denied it will be done, by default, according to the continuous assessment model. The student has two calls to pass the subject, one ordinary and one extraordinary.

Preferably, students will be offered a continuous assessment model that has characteristics of formative assessment in a way that serves as feedback in the teaching-learning process.

The evaluation must be inspired by the criteria of continuous evaluation (Regulations for the Regulation of Teaching Learning Processes, NRPEA, art 3). However, in compliance with the regulations of the University of Alcala, an alternative process of final evaluation is made available to the student in accordance with the Regulations for the Evaluation of Apprenticeships (approved by the Governing Council on March 24, 2011 and modified in the Board of Directors). Government of May 5, 2016) as indicated in Article 10, students will have a period of fifteen days from the start of the course to request in writing to the Director of the Polytechnic School their intention to take the non-continuous evaluation model adducing the reasons that they deem convenient. The evaluation of the learning process of all students who do not apply for it or are denied it will be done, by default, according to the continuous assessment model. The student has two calls to pass the subject, one ordinary and one extraordinary.

Ordinary Call

In the ordinary call, there are two possible ways for evaluation: Continuous Assessment (EC) and Final Assessment (EF).

Extraordinary Call

The Extraordinary Call will have a similar exam format to the one used for the Final Exam assessment in the Ordinary Call.

5.2. EVALUATION

EVALUATION CRITERIA

The assessment criteria measure the level in which the competences have been acquired by the student. For that purpose, the following are defined::

CE1. The student knows the different cryptographic mechanisms seen in the course.

CE2. The student is able to select, given a specific scenario with its information security risks, the most suitable cryptographic mechanism to fulfil a set of confidentiality, integrity and availability requirements.

CE3. The student is able to assess, given a specific cryptography scenario, the potential vulnerabilities that might appear.

CE4. The student knows the most common vulnerabilities and threats regarding network and system security.

CE5. The student is able to perform an asset inventory on an information system.

CE6. The student is able to assess the security risks of an information system, according to the system asset inventory and the vulnerabilities and threats affecting it.

CE7. The student knows the different security mechanisms that may be used to protect an information system, including firewalls, intrusion detection systems and security policies.

CE8. The student is able to apply the different security mechanisms for prevention, detection and reaction on network services and devices.

CE9. The student is able to work in a team to analyze information systems, to design security solutions, and to investigate security incidents.

CE10. The student is able to make decisions in an autonomous and proactive way, and to justify those decisions.

CE11. The student is able to generate, given a specific scenario regarding information system security risks, an acceptable security solution using different cryptographic mechanisms and security applications.

CE12. The student is able to work collaboratively in a team to solve problems regarding system and network security.

CE13. The student is able to communicate effectively knowledge, procedures, results and ideas within the context of the course, both in oral and written form.

GRADING TOOLS

The default grading tools correspond to continuous assessment via a series of follow-up assignments and a midterm exam, along with an overall exam at the end of the semester.

- **Follow-up assignments (E)**: Following up student's work allows the professor to know the performance of the student regarding the different assignments. In addition, it helps students to know whether they are reaching the goals established throughout the course. Among the follow-up activities there will be: problem solving activities, quizzes and small assignments. These activities may be designed to do in class, in the lab, or at home. Follow-up activities make up to a 30% of the student grade.
- **Intermediate Assessment (PEI)**: The intermediate assessment exam will make up to a 30% of the student grade.
- **Final assessment (PEF)**: The overall assessment exam has a 40% weight in the student grade, and has a double purpose: assess the ability of the student to integrate the course contents and review the learning of these concepts. Taking this into account, if students have passed the average mark in the follow-up activities, the overall assessment exam will allow to improve the grade if the result obtained is higher than the average grade of the continuous assessment.

GRADING CRITERIA

In the **ordinary call-continuous assessment** the relationship between the competences, learning outcomes, criteria and evaluation instruments is as follows.

Skill	Learning Outcomes	Evaluation criteria	Grading Tool	Contribution to the final mark
CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CB1-CB5, TRU1-TRU5	RA1-RA6	CE1-CE13	E	30%
CIC6, CSI2	RA1, RA2	CE1-CE3, CE7	PEI	30%
CIC6, CSI2, CSI5	RA1-RA4	CE1-CE8, CE10, CE11	PEF	40%

Students to which the Dean has granted final assessment, according to the UAH regulations, will have to do a final assessment exam (PEF) including theoretical questions and exercises, with a contribution of 70% to the final mark. In addition, they will have to deliver a Course Assignment (TA), which will preferably be made in teams, with a contribution of 30% to the final mark.In the **ordinary call-final assessment** exam, the relationship between the competences, learning outcomes, criteria and evaluation instruments is as follows.

Skill	Learning Outcomes	Evaluation criteria	Grading Tool	Contribution to the final mark
CIC6, CSI2, CSI5	RA1-RA4	CE1-CE8,CE10,CE11	PEF	70%
CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CB1-CB5, TRU1-TRU5	RA3-RA6	CE4-CE13	TA	30%

The extraordinary call will have an extraordinary assessment exam (PEE) including theorical questions and exercises, with a contribution of 70% to the final mark. In addition, students will have to deliver a Course Assignment (TA), which will preferably be made in teams, with a contribution of 30% to the final mark. Students who have followed the continuous assessment in the ordinary call and have passed the average mark in the follow-up activities will not have to do the TA, getting the corresponding part of the mark from the follow-up activities. In the **extraordinary call**, the relationship between the competences, learning outcomes, criteria and evaluation instruments is as follows:

Skill	Learning Outcomes	Evaluation criteria	Grading Tool	Contribution to the final mark
CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CB1-CB5, TRU1-TRU5	RA1-RA6	CE1-CE13	E/TA	30%
CIC6, CSI2, CSI5	RA1-RA4	CE1-CE8, CE10, CE11	PEE	70%

6. BIBLIOGRAPHY

6.1. Basic Bibliography

- Information Security: Principles and Practice (2ª Ed.) M. Stamp Wiley, 2011
- Hacking Exposed 7: Network security secrets & solutions. Mc Graw-Hill, 2012

6.2. Additional Bibliography

- Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017.
- Threat Modeling: Designing for Security. Wiley. 2014.

Disclosure Note

During the evaluation tests, the guidelines set out in the Regulations establishing the Rules of Coexistence of the University of Alcalá must be followed, as well as the possible implications of the irregularities committed during said tests, including the consequences for committing academic fraud according to the Regulation of Disciplinary Regime of the Students of the University of Alcalá.