Universidad de Alcalá

TEACHING GUIDE

Security

Degree in
Telecommunications Technologies Engineering

Universidad de Alcalá

Academic Year 2020/2021

4th Year – 1st Semester

Approved by the School Board on June 24, 2020

TEACHING GUIDE

Course Name:	**Security**
Code:	**350039 (GITT)** **380002 (GIT)**
Degree in:	**Telecommunication Technologies Engineering (GITT)** **Telematics Engineering (GIT)**
Department and area:	**Automática** **Telematics Engineering**
Type:	**Optional (Specialized) (GITT)** **Compulsory (GIT)**
ECTS Credits:	**6**
Year and semester:	**4th Year - 1st Semester (GITT)** **3rd Year - 2nd Semester (GIT)**
Teachers:	Susel Fernández Melián
Tutoring schedule:	To be defined
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 Architectures I and Network Architectures II courses.

The course is structured in four parts:

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

2. SKILLS

Basic, Generic and Cross Curricular Skills.

This course contributes to acquire the following generic skills, which are defined in the Section 3 of the Annex to the Orden CIN/352/2009:

en_TR3 - Aptitude to solve problems with initiative, decision making, creativity, and to communicate and to transmit knowledge, skills and workmanship, comprising the ethical and professional responsibility of the activity of the Technical Engineer of Telecommunication.

en_TR6 - Ability to analyze and assess the social and environmental impact of technical solutions.

en_TR8 - Capacity of working in a multidisciplinary and multilingual team and of communicating, both in spoken and written language, knowledge, procedures, results and ideas related to telecommunications and electronics.

en_TRU4 - Autonomous learning skills.

Professional Skills

This course contributes to acquire the following professional skills, which are defined in the Section 5 of the Annex to the Orden CIN/352/2009:

en_CTE2 - Ability to apply the techniques on which telematic networks, services and applications

are based, such as management systems, signaling and switching, routing, security (cryptographic protocols, tunneling, firewalls, collection mechanisms, authentication and content protection), traffic engineering (graph theory, queuing theory and teletraffic) charging and reliability and quality of service, both in fixed, mobile, personal, local or long distance environments, with different bandwidths, including telephony and data.

en_CTE6 - Ability to design network architectures and telematic services.

Learning Outcomes

After succeeding in this course 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 system security 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. Asymmetric cryptography: RSA, ECC, hash functions, hmac.	16 hours (4 weeks)
Access control: authentication: passwords, Single Sing On (SSO), biometry. Authorization: access control lists (ACLs), multilevel models. Mechanisms: firewalls, intrusion detection systems (IDS).	12 hours (3 weeks)
Security protocols: authentication, mutual authentication, man-in-the-middle attacks. Security in the Internet protocols.	8 hours (2 weeks)
Systems security: vulnerabilities and threats, vulnerability analysis. Software security: privilege escalation, malware. Security in Web applications. Systems audit. Security in operating systems. Information forensics.	12 hours (3 weeks)

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

Classroom sessions	• Presentation and/or review of practical concepts. • Problem resolution. • Laboratory practices: aimed at consolidating the previously presented concepts, as well as to familiarize the student with the tools and methodologies to support the study of the subject and future professional performance (to improve the understanding of security concepts, intrusion detection, analysis of vulnerabilities, and implementation of security measures). • Oral presentations and other activities. • Group activities.
Tutoring (individual, for groups and via Web)	• Question discussion. • Support for autonomous learning
Autonomous work	• Reading. • Learning Activities: exercises, information search, data analysis.

5. ASSESSMENT: procedures, evaluation and grading criteria

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.

5.1. PROCEDURES

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 Alcalá, 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, students will undertake a continuous assessment process. This process includes lab assignments, activities in class, self-assessment quizzes, and two intermediate exams. In exceptional circumstances, adequately documented, a student might be assessed by a Single Final Exam.

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 skills 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 an 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 AND CRITERIA

The default grading tools correspond to continuous assessment via a series of follow-up assignments and a midterm exam, along with a 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 Exams (PEI):** The intermediate assessment exam will make up to a 30% of the student grade.
- **Overall Assessment Exam (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 attained at least 15% of their final grade 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.

Skills	Learning Outcome	Grading Criteria	Grading Tool	Contribution to the final mark
CTE2, CTE6, TR3, TR6, TR8, TRU4	RA1-RA6	CE1-CE13	E	30%
CTE2, CTE6	RA1,RA2	CE1-CE3, CE7	PEI	30%
CTE2, CTE6	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 theorical 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 preferrably be made in teams, with a contribution of 30% to the final mark.

Skills	Learning outcomes	Grading Criteria	Grading Tool	Contribution to the final mark
CTE2, CTE6	RA1-RA4	CE1-CE8, CE10, CE11	PEF	70%
CTE2, CTE6, TR3, TR6, TR8, TRU4	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 attained at least 15% of their final grade in the follow-up activities will not have to do the TA, getting the corresponding part of the grade from the follow-up activities.

Skills	Learning Outcomes	Grading Criteria	Grading tools	Contribution to the final mark
CTE2, CTE6, TR2, TR6, TR8, TRU4	RA1-RA4	CE1-CE11	E	0-30%
CTE2, CTE6	RA1-RA4	CE1-CE8, CE10, CE11	PEE	70%
CTE2, CTE6, TR3, TR8, TRU4	RA3-RA6	CE4-CE13	TA	30%

6. BIBLIOGRAPHY

6.1. Basic Bibliography

- Information Security: Principles and Practice (3ª 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 Modelling: Designing for Security. Wiley. 2014.

Disclosure Note

The University of Alcalá guarantees to its students that, if due to health requirements the competent authorities do not allow the total or partial attendance of the teaching activities, the teaching plans will achieve their objectives through a teaching-learning and evaluation methodology in online format, which will return to the face-to-face mode as soon as these impediments cease.