SUBJECT TEACHING GUIDE

G1498 - Security in Communications Networks

Degree in Telecommunication Technologies Engineering

Academic year 2021-2022

1. IDENTIFYING DATA					
Degree	Degree in Telecommunication Technologies Engineering			Type and Year	Optional. Year 4
Faculty	School of Industrial Engineering and Telecommunications				
Discipline	Speciality Optional Subjects				
Course unit title and code	G1498 - Security in Communications Networks				
Number of ECTS credits allocated	6	Term	Semester based (2)		
Web	http://www.tlmat.unican.es				
Language of instruction	Spanish	English Friendly	No	Mode of delivery	Face-to-face

Department	DPTO. INGENIERIA DE COMUNICACIONES
Name of lecturer	JORGE LANZA CALDERON
E-mail	jorge.lanza@unican.es
Office	Edificio Ing. de Telecomunicación Prof. José Luis García García. Planta: - 2. DESPACHO JORGE LANZA (S227)
Other lecturers	LUIS SANCHEZ GONZALEZ PABLO SOTRES GARCIA

3.1 LEARNING OUTCOMES
- Understand the architecture of the security protocols used in Internet.
- The student will be able to design, specify and develop secure communication networks and services based on practical cases
- The student will be able to practically assess the operation of the different security solutions studied and which are their implications and technical requirements
- The student will be able to detect security threats and design the corresponding security countermeasures to provide a solution with the desired security policies

4. OBJECTIVES

Broaden the students' knowledge about current communication networks making emphasis on the security aspects that are applied depending on the requirements of each situation
Get the knowledge about necessary mechanisms to guarantee the fullfilment of the security policies defined in a given network or service, thus assuring the secure transport of information through them.
Get the knowledge about security recommendations and best practices.

6. COURSE ORGANIZATION

CONTENTS	
1	THEME I: INTRODUCTION TO NETWORK SECURITY. The concept of security. Terminology. Security policies. Threats and vulnerabilities.
2	THEME II: AUTHENTICATION AND KEY MANAGEMENT. Authentication services. Confidentiality, integrity and authentication criptographic algorithms. Digital certification. Public Key Infrastructure.
3	THEME III: SECURITY PROTOCOLS AND MECHANISMS. EAP, RADIUS, IPSec, TLS, PGP
4	THEME IV; ACCESS CONTROL. Access control, authorization and authentication. Architectures and configuration of firewalls.

7. ASSESSMENT METHODS AND CRITERIA

Description	Type	Final Eval.	Reassessn	%
Continuous Evaluation	Others	No	Yes	15,00
Practical sessions at laboratory	Laboratory evaluation	Yes	No	40,00
Final exam	Written exam	Yes	Yes	45,00
TOTAL				100,00

Observations

Practical sessions are mandatory.
Final mark is obtained as follows: FINAL_MARK = THEOR * 0.6 + PRAC * 0.4
where THEOR and PRAC are the theory and practice marks respectively
Theory mark is obtained from the Final Exam (EF) mark and the Continuous Evaluation (EC) mark as follows: TEOR = max{ 0.75 * EF + 0.25 * EC ; EF}
In any case, it is mandatory to get a mark above 4.0 in the final exam to pass the subject
Continuous Evaluation tests are meant to encourage the student to follow the subject on a day-by-day basis rather than at intervals fixed by the tests themselves. Hence, the marks for these tests and problems will only be available during the exams' review session after the Final Exam.
Evaluation would be carried out online in case required. The teacher could ask the students to present the exam answers during individual sessions.

Observations for part-time students

Practical sessions are mandatory.
Continuous Evaluation is not mandatory. Those students that do not attend classes regularly will have their final mark from the Final Exam and the mark from the practical sessions.

8. BIBLIOGRAPHY AND TEACHING MATERIALS
BASIC
W. Stallings, L. Brown, Computer Security: Principles and Practice, Prentice Hall, 2007
S. Northcutt et all, Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems, Sams, 2005