SUBJECT TEACHING GUIDE

327 - Systems, virtualization and safety

Master's Degree in computing engineering

Academic year 2023-2024

1. IDENTIFYING DATA					
Degree	Master's Degree in computing engineering			Type and Year	Compulsory. Year 1
Faculty	Faculty of Sciences				
Discipline	COMPUTER ENGINEERING				
Course unit title and code	327 - Systems, virtualization and safety				
Number of ECTS credits allocated	6	Term		Semester based (1)	
Web					
Language of instruction	Spanish	English Friendly	No	Mode of delivery	Face-to-face

Department	DPTO. INGENIERÍA INFORMÁTICA Y ELECTRÓNICA
Name of lecturer	VALENTIN PUENTE VARONA
E-mail	vpuente@unican.es
Office	Facultad de Ciencias. Planta: + 1. DESPACHO (1103)
Other lecturers	

3.1 LEARNING OUTCOMES
- - Be able to evaluate and improve the performance of computer systems based on system level virtualization
- - Being able to deploy virtualization based computer systems
- - Being able to move IaaS infrastructure support
- - To know the hardware elements aimed at improving the security of computer systems.

4. OBJECTIVES

The course is focused on providing students with the fundamental tools for the understanding and management of virtualization at the system level, as a key element for the deployment of cloud computing. The main approaches, from the hardware perspective to enhance the security of these environments will be introduced.

6. COURSE ORGANIZATION

CONTENTS	
1	Introduction
2	Operating Systems. Direct limited execution model, CPU virtualization and memory virtualization. I/O and persistence.
3	Introduction to Virtualization. Virtualization without architectural support: Popek Goldberg's Theorem.
4	Hardware support for CPU and memory virtualization: x86 case
5	Input-output virtualization
6	Basic concepts of security, secure processors and root-of-trust.
7	Processor and Memory Protection. Side channel attacks and current hardware limitations.
8	Review of scientific papers
9	Final exam

7. ASSESSMENT METHODS AND CRITERIA

Description	Type	Final Eval.	Reassessn	%
Review of Scientific Papers	Others	No	Yes	50,00
Final Evaluation	Written exam	Yes	Yes	50,00
TOTAL				100,00

Observations

If the quota of 'Matrículas de honor' of the course is completed
in ordinary evaluation, students in the September call can't opt for one of them'

Observations for part-time students

Students enrolled part-time by the same method of assessment shall be governed students enrolled full-time.

8. BIBLIOGRAPHY AND TEACHING MATERIALS

BASIC

E. Bugnion, J. Nieh, and D. Tsafrir, “Hardware and Software Support for Virtualization,” Synth. Lect. Comput. Archit., vol. 12, no. 1, pp. 1–206, Feb. 2017.

J. Szefer, “Principles of secure processor architecture design,” Synth. Lect. Comput. Archit., vol. 13, no. 3, pp. 1–173, 2018.

Operating Systems: Three Easy Pieces
Remzi H. Arpaci-Dusseau and Andrea C. Arpaci-Dusseau
Arpaci-Dusseau Books
March, 2018