

SUBJECT TEACHING GUIDE

G1828 - System and Network Security and Assurance

Degree in Computer Systems Engineering

Academic year 2023-2024

| 1. IDENTIFYING DATA | | | |
|----------------------------------|---|------------------|--------------------|
| Degree | Degree in Computer Systems Engineering | Type and Year | Optional. Year 4 |
| Faculty | Faculty of Sciences | | |
| Discipline | Subject Area: Computer Engineering Mention in computer Engineering | | |
| Course unit title and code | G1828 - System and Network Security and Assurance | | |
| Number of ECTS credits allocated | 6 | Term | Semester based (2) |
| Web | | | |
| Language of instruction | English | Mode of delivery | Face-to-face |

| | |
|------------------|--|
| Department | DPTO. INGENIERÍA INFORMÁTICA Y ELECTRÓNICA |
| Name of lecturer | ESTEBAN STAFFORD FERNANDEZ |
| E-mail | esteban.stafford@gestion.unican.es |
| Office | Facultad de Ciencias. Planta: + 3. DESPACHO - COORDINACION NUEVO PLAN ESTUDIOS FAC. C (3017) |
| Other lecturers | |

| 3.1 LEARNING OUTCOMES |
|--|
| - Learn the procedures and mechanisms to protect the operating system. |
| - Get to know fundamental aspects of security in computation systems, by learning common attacks and vulnerabilities. |
| - Get to know fundamental aspects of security in computation systems, by learning common attacks and vulnerabilities. |
| - Learn the security requirements of computer systems and networks, and the mechanisms available to provide them, like cryptography, authentication, authorization, permissions, firewalls, etc. |
| - Be able to effectively communicate, orally and in writing, knowledge, techniques, results and ideas related to the content of the subject. |

4. OBJECTIVES

Society today is increasingly dependant on information technology. Therefore the consequences of the failure of the IT infrastructure can be disastrous. For this reason, IT Engineers must know how to ensure as best they can the systems they manage. To reach this goal, they have to put great care in the deployment and exploitation of these systems.

Throughout this subject, the students should achieve the following objectives:

- Learn the cryptographic tools commonly used in IT security. Symmetric and public key encryption and hash functions.
- Understand the mechanisms of authentication and authorization. Know how to assess their risks and be able to propose corrective methods.
- Understand and know how to evaluate the most common security risks of IT systems at an application level , as well as at system or network levels.
- Learn how to apply corrective means, to improve the security of IT systems, selecting protection, detection, contention and recovery measures.

6. COURSE ORGANIZATION

| CONTENTS | |
|----------|--|
| 1 | Part 1: General Concepts 1.1 Introduction 1.2 Cryptography basics 1.3 Authentication 1.4 Authorization |
| 2 | Part 2: Software Security 2.1 Malicious code 2.2 Denial of service 2.3 Stack overflow 2.4 Secure programming |
| 3 | Part 3: Network security 3.1 Intrusion detection 3.2 Intrusion prevention and firewalls |

7. ASSESSMENT METHODS AND CRITERIA

| Description | Type | Final Eval. | Reassessn | % |
|--|-----------------------|-------------|-----------|--------|
| Tests about the contents of the course. | Written exam | No | Yes | 80,00 |
| Evaluation of the lab assignments. | Laboratory evaluation | No | Yes | 20,00 |
| TOTAL | | | | 100,00 |
| Observations | | | | |
| Observations for part-time students | | | | |
| Part-time students will only have a final exam, corresponding to the 100% of the evaluation. | | | | |

8. BIBLIOGRAPHY AND TEACHING MATERIALS

BASIC

Computer Security: Principles and Practice, 2nd ed. W. Stallings, L Brown. Pearson Education Limited, 2011.

