60929 - Advanced security and management

Información del Plan Docente

Academic Year	2017/18
Subject	60929 - Advanced security and management
Faculty / School	110 - Escuela de Ingeniería y Arquitectura
Degree	533 - Master's Degree in Telecommunications Engineering
ECTS	5.0
Year	1
Semester	Second semester
Subject Type	Compulsory
Module	---

1.General information

1.1.Introduction

1.2.Recommendations to take this course

1.3.Context and importance of this course in the degree

1.4.Activities and key dates

2.Learning goals

2.1.Learning goals

2.2.Importance of learning goals

3.Aims of the course and competences

3.1.Aims of the course

3.2.Competences

4.Assessment (1st and 2nd call)

4.1.Assessment tasks (description of tasks, marking system and assessment criteria)

5.Methodology, learning tasks, syllabus and resources

5.1.Methodological overview

The methodology followed in this course is oriented towards achievement of the learning objectives. A wide range of teaching and learning tasks are implemented, such as lectures where the main course contents are presented and discussed, computer lab sessions, and student participation.

5.2.Learning tasks

The course includes the following learning tasks:

- **A01 Lectures** (25 hours). The main theoretical contents are presented and student participation is encouraged.
- **A02 Practice session** (5 hours). Students solve example problems and cases during the classes.
- **A03 Computer lab sessions** (20 hours). 10 sessions of two hours each will be held in a computer network laboratory. Instructions for each computer/lab session where the different activities are planned will be available before the session. The students will present the results obtained during each one of the practical units once finished.
- **A05 Assignment** (10 hours). It helps acquire all proposed learning outcomes, especially those related to autonomous work skills and the ability to communicate oral and written conclusions.
- **A08 Assessment** (3 hours). A set of theoretical-practical written tests and reports or papers. Details can be found in the "Assessment" Section.

5.3.Syllabus

The course will address the following topics:

Section 1. Advanced Security

1. Introduction
    - 1.1 Computational complexity
    - 1.2. The Game-playing Technique
2. Block Ciphers
3. Pseudorandom Functions
4. Symmetric Encryption
5. Hash Functions
6. Message Authentication Codes
7. Authenticated Encryption
8. Stream Ciphers and Pseudorandom Generators
9. Number Theoretic Primitives
10. Asymmetric Encryption
11. Digital Signatures
12. Key Distribution
13. Applications and Protocols

Section 2. Advanced Management - SNMPv3 secure management architecture

1. Architecture, security and management
2. Message processing and delivery
3. SNMPv3 applications
4. User-based security model
5. View-based Access Control model

5.4.Course planning and calendar

Further information concerning the timetable, classroom, office hours, assessment dates and other details regarding this course, will be provided on the first day of class or please refer to the EINA website.

5.5.Bibliography and recommended resources

- Kurose, James F.. Computer networking : a top-down approach / James F. Kurose, Keith W. Ross ; international edition adapted by Bhojan Anand . - 4th ed. Boston : Pearson, cop. 2008
- Pastor Franco, José. Criptografía digital : fundamentos y aplicaciones / José Pastor Franco, Miguel Angel Sarasa López, José Luis Salazar Riaño . - 2a. ed. Zaragoza : Prensas Universitarias de Zaragoza, 2001

60929 - Advanced security and management

- Menezes, Alfred J.. Handbook of applied cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone . - [1st ed.] Boca Raton [etc.] : CRC, cop. 1997
- Goldreich, Oded. Foundations of Cryptography, Basic Tools / Oded Goldreich Cambridge University Press, 2001
- Goldreich, Oded. Foundations of Cryptography, Basic Applications / Oded Goldreich Cambridge University Press, 2004
- Goldreich, Oded. Computational Complexity / Oded Goldreich Cambridge University Press, 2008
- Katz, Jonathan. Introduction to Modern Cryptography / Jonathan Katz, Yehuda Lindell Chapman and Hall/CRC, 2008
- Subramanian, Mani. Network Management: Principles and Practices / Mani Subramanian. - 2nd ed. Prentice Hall, 2012