60929 - Advanced security and management

Información del Plan Docente

Academic Year	2016/17
Academic center	110 - Escuela de Ingeniería y Arquitectura
Degree	533 - Master's Degree in Telecommunications Engineering
ECTS	5.0
Course	1
Period	Second semester
Subject Type	Compulsory
Module	---

1.Basic info

1.1.Recommendations to take this course

1.2.Activities and key dates for the course

2.Initiation

2.1.Learning outcomes that define the subject

2.2.Introduction

3.Context and competences

3.1.Goals

3.2.Context and meaning of the subject in the degree

3.3.Competences

3.4.Importance of learning outcomes

4.Evaluation

5.Activities and resources

5.1.General methodological presentation

The teaching methodology is structured in two levels: theoretical classes where the main subject contents are presented and discussed, student participation is encouraged and also computer lab sessions

5.2.Learning activities

A01 Theoretical classes with the active involvement of the student (25 hours). The main course contents are presented.

A02 Problems and cases resolution (5 hours). This activity is intended to resolve example problems during the classes.

A03 Computer/lab sessions (20 hours). Different lab sessions are carried out. Notes for each computer/lab session where the different activities are planned will be available before the session.

A06 Tutorship. Students may solve any questions they might have about unclear contents of the course

A08 Assessment. The student will take an exam and several reports derived from the computer lab sessions and derived from the development of practical tasks will be evaluated

5.3.Program

The program offered to the students to cope with the learning results encompasses the following activities

Block 1. Advanced Security

1.1. Introduction
1.1.1 Computational complexity
1.1.2. The Game-playing Technique
1.2. Block Ciphers
1.3. Pseudorandom Functions
1.4. Symmetric Encryption
1.5. Hash Functions
1.6. Message Authentication Codes
1.7. Authenticated Encryption
1.8. Stream Ciphers and Pseudorandom Generators
1.9. Number Theoretic Primitives
1.10. Asymmetric Encryption
1.11. Digital Signatures
1.12. Key Distribution
1.13. Applications and Protocols

Block 2.Advanced Management - SNMPv3 secure management architecture

2.1 Architecture, security and management

2.2 Message processing and delivery

2.3 SNMPv3 applications

2.4 User-based security model

2.5 View-based Access Control model

60929 - Advanced security and management

Laboratory sessions

These sessions will be held in a computer network laboratory. It is divided in 10 sessions of 2 hours duration each. The students will defend the results obtained during each one of the practical units one finished.

5.4.Planning and scheduling

All the sessions will be defined by the EINA at the begining of the course

5.5.Bibliography and recomended 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
- 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