Course guide
300049 - SX - Network Security

Last modified: 01/06/2023

Unit in charge: Castelldefels School of Telecommunications and Aerospace Engineering
Teaching unit: 744 - ENTEL - Department of Network Engineering.

Degree: BACHELOR'S DEGREE IN NETWORK ENGINEERING (Syllabus 2009). (Compulsory subject).

Academic year: 2023 **ECTS Credits:** 4.0 **Languages:** Catalan, Spanish, English

LECTURER

Coordinating lecturer: Definit a la infoweb de l'assignatura.

Others:

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
1. CE 22 TEL. Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones de telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y telegráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos. (CIN/352/2009, BOE 20.2.2009.)

Generical:
7. PROJECT MANAGEMENT - Level 2: Define the objectives of a well-defined, narrow scope, and plan development, identifying resources, tasks, shared responsibilities and integration. Use appropriate tools to support project management.

Transversal:
2. EFFICIENT ORAL AND WRITTEN COMMUNICATION - Level 1. Planning oral communication, answering questions properly and writing straightforward texts that are spelt correctly and are grammatically coherent.
3. EFFICIENT ORAL AND WRITTEN COMMUNICATION - Level 2. Using strategies for preparing and giving oral presentations. Writing texts and documents whose content is coherent, well structured and free of spelling and grammatical errors.
4. EFFICIENT ORAL AND WRITTEN COMMUNICATION - Level 3. Communicating clearly and efficiently in oral and written presentations. Adapting to audiences and communication aims by using suitable strategies and means.
5. EFFICIENT ORAL AND WRITTEN COMMUNICATION. Communicating verbally and in writing about learning outcomes, thought-building and decision-making. Taking part in debates about issues related to the own field of specialization.
6. ENTREPRENEURSHIP AND INNOVATION - Level 3. Using knowledge and strategic skills to set up and manage projects. Applying systemic solutions to complex problems. Devising and managing innovation in organizations.

TEACHING METHODOLOGY

LEARNING OBJECTIVES OF THE SUBJECT

After passing the Network Security course, the student should be able to:
- Understand what network security is and be able to identify potential attacks and countermeasures.
- Identify and understand cryptographic algorithms used to provide security to networks.
- Define the different methods of confidentiality, integrity, authentication, freshness and management of cryptographic material.
- Know firewalls and intrusion detection systems
- Use different security protocols for secure data exchange on the Internet: IP security, virtual private networks, security mechanisms for email, www security or secure payment systems.

STUDY LOAD

Type	Hours	Percentage
Guided activities	16,0	16.00
Self study	56,0	56.00
Hours medium group	4,0	4.00
Hours large group	24,0	24.00

Total learning time: 100 h

CONTENTS

(ENG) 1. INTRODUCCIÓ A LA SEGURETAT EN XARXA

Description:
Conceptos fundamentales. La seguridad en red engloba: ataques de seguridad, mecanismos de seguridad y servicios de seguridad. A partir del conocimiento de estos tres bloques, se plantea un modelo de seguridad en red que debe estar presente durante toda la asignatura.
Los mecanismos y servicios de seguridad se basan en gran medida en herramientas que garanticen confidencialidad, integridad, autenticación, autorización, AAA, no repudio y anonimato.

Full-or-part-time: 4h 15m
Theory classes: 2h
Practical classes: 0h 15m
Self study : 2h

(ENG) 2. EINES DE SEGURETAT DE LA INFORMACIÓ

Description:
Aritmética modular y criptografía clásica
Criptografía simétrica moderna
- Cifrado de flujo/bloque
- Modos de funcionamiento cifradores de bloque (ECB, OFB, CBC, CTR, CBC-MAC, CCM, etc.)
Criptografía asimétrica y PKI
- Intro: funciones asimétricas/unidireccionales y criptografía asimétrica
- RSA
Necesidad de autenticar:
- PKI: certificados digitales, firma electrónica
- Secreto compartido: Message Authentication Codes (MAC)
Gestión y acuerdo de claves

Full-or-part-time: 33h 45m
Theory classes: 10h 30m
Practical classes: 1h 15m
Self study : 22h

3. Overview of security threats & countermeasures

Description:
content english

Full-or-part-time: 11h 15m
Theory classes: 2h
Practical classes: 0h 15m
Guided activities: 2h
Self study : 7h

4. Internet Security Protocols

Description:
Applied security, link-layer security (e.g. WEP, WPA), network-layer security (IPSec), transport-security (SSL/TLS, SSH).

Full-or-part-time: 50h 45m
Theory classes: 9h 30m
Practical classes: 2h 15m
Guided activities: 14h
Self study : 25h

ACTIVITIES

AD1. Network virtualization, link-layer MITM atacks, virtual private networks with IPSec

Description:
[content]

Full-or-part-time: 16h
Theory classes: 2h
Guided activities: 7h
Self study: 7h

AD2. Certification Authorities, SSL/TLS and SSH

Description:
[content]

Full-or-part-time: 17h
Theory classes: 2h
Guided activities: 7h
Self study: 8h

AD3. OPEN ACTIVITY

Description:
[content]

Full-or-part-time: 8h
Guided activities: 2h
Self study: 6h

(ENG) PLANIFICACIÓ D'EXÀMENS (RESOLUCIÓ DE PROBLEMES)

Full-or-part-time: 8h
Theory classes: 4h
Self study: 4h

Mid-term exam

Full-or-part-time: 4h 30m
Theory classes: 1h 30m
Self study: 3h

Final exam

Full-or-part-time: 4h 30m
Theory classes: 1h 30m
Self study: 3h

GRADING SYSTEM