Course guide
300272 - NETAUTH - Network Security Authentication & Authorization

Last modified: 19/05/2025

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

Degree: MASTER'S DEGREE IN APPLIED TELECOMMUNICATIONS AND ENGINEERING MANAGEMENT (MASTEAM) (Syllabus 2015). (Optional subject).
MASTER'S DEGREE IN ADVANCED TELECOMMUNICATION TECHNOLOGIES (Syllabus 2019). (Optional subject).
ERASMUS MUNDUS MASTER IN COMMUNICATIONS ENGINEERING AND DATA SCIENCE (CODAS 1) (Syllabus 2024). (Optional subject).
ERASMUS MUNDUS MASTER IN COMMUNICATIONS ENGINEERING AND DATA SCIENCE (CODAS 2) (Syllabus 2024). (Compulsory subject).
MASTER'S DEGREE IN ARTIFICIAL INTELLIGENCE FOR CONNECTED INDUSTRIES (AI4CI) (Syllabus 2025). (Compulsory subject).

Academic year: 2025 **ECTS Credits:** 3.0 **Languages:** English

LECTURER

Coordinating lecturer: Hernandez Serrano, Juan Bautista

Others: Hernandez Serrano, Juan Bautista
León Abarca, Olga

PRIOR SKILLS

Basic knowledge of Linux OS.
Basic understanding of security-related topics; for instance: cryptography, security protocols, dynamic key management, CIA triad, etc.
Medium-average computer programming skills.

REQUIREMENTS

None

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Generical:
03 DIS. (ENG) Diseñar aplicaciones de alto valor añadido basadas en las Tecnologías de la Información y las Comunicaciones (TIC), aplicadas a cualquier ámbito de la sociedad.
06 RES. (ENG) Resolver problemas y mejorar procesos en cualquier ámbito social a partir de la aplicación de las TIC, integrando conocimientos de diversos ámbitos y aplicando ingeniería de alto nivel tecnológico.

Transversal:
05 TEQ. TEAMWORK. Being able to work as a team player, either as a member or as a leader. Contributing to projects pragmatically and responsibly, by reaching commitments in accordance to the resources that are available.
03 TLG. THIRD LANGUAGE. Learning a third language, preferably English, to a degree of oral and written fluency that fits in with the future needs of the graduates of each course.

Basic:
CB8. Students will be able to integrate knowledge and face the complexity of formulating judgments based on information that, while being incomplete or limited, includes reflections on social and ethical responsibilities linked to the application of their knowledge and opinions.
CB10. Students will acquire learning skills that allow them to continue studying in a way that will be largely self-directed or autonomous.

TEACHING METHODOLOGY

Theoretical classes encouraging the students to participate in the class discussion
Lab sessions that reinforce the contents learnt during the theoretical classes and put them into practice.

LEARNING OBJECTIVES OF THE SUBJECT

Upon finishing this course, students should be able to:
• Know and understand security threats and risks against the management of networks, with special focus on IP networks.
• Known the techniques to audit for vulnerabilities/attacks both networks and hosts.
• Know the techniques to prevent or counteract those security threats.

STUDY LOAD

Type	Hours	Percentage
Hours small group	3,0	4.00
Hours large group	12,0	16.00
Guided activities	12,0	16.00
Self study	48,0	64.00

Total learning time: 75 h

CONTENTS

Introduction to Security

Description:
An overview of network security basics (CIA, MACs, digital signatures, dynamic key management, etc.) and an introduction to virtualization of network scenarios.

Full-or-part-time: 14h 12m
Theory classes: 2h
Laboratory classes: 0h 36m
Guided activities: 4h
Self study : 7h 36m

Understanding Authentication

Description:
Authentication with one of multiple factors: something you know (passwords), something you have (tokens, keys), something you are (biometrics). Includes understanding authentication with secret keys, public keys, the need of nonces, password hashing, salted hashes, proper access control, and secure transmission of credentials.

Full-or-part-time: 16h 36m
Theory classes: 4h
Laboratory classes: 0h 36m
Guided activities: 2h
Self study : 10h

Access Authentication

Description:
Authentication protocols for network/resource access: PAP, CHAP, EAP with its methods

Full-or-part-time: 12h 36m
Theory classes: 2h
Laboratory classes: 0h 36m
Guided activities: 2h
Self study : 8h

Authentication, Authorization and Accounting (AAA)

Description:
Authentication, Authorization and Accounting (AAA): RADIUS, DIAMETER, federated cross-layer authentication, EDUROAM

Full-or-part-time: 12h 36m
Theory classes: 2h
Laboratory classes: 0h 36m
Guided activities: 2h
Self study : 8h

Web Authentication

Description:
TLS authentication, login forms, session control, Single Sign-On, delegated authentication (OAuth)

Full-or-part-time: 12h 36m
Theory classes: 2h
Laboratory classes: 0h 36m
Guided activities: 2h
Self study : 8h

GRADING SYSTEM

Defined in SIA (Infoweb of the course)