



## GENERAL INFORMATION

Data of the subject	
Subject name	Security in Communications Systems
Subject code	DTC-MIT-512
Mainprogram	
Involved programs	Máster Universitario en Ingeniería de Telecomunicación [Primer Curso] Grado en Administración y Dirección de Empresas y Máster Univ. en Ingeniería de Telecomunicación [Quinto Curso] Máster Universitario en Ingeniería de Telecomunicación y Máster en Ciberseguridad [Primer Curso] Máster Universitario en Ingeniería de Telecomunicación y Mást. Univ. en Administración de Empresas [Primer Curso] Máster Universitario en Ingeniería de Telecomunicación + Máster Big Data.Tecnología y Anal. Avanzada [Primer Curso]
Level	Postgrado Oficial Master
Quarter	Semestral
Credits	4,5 ECTS
Type	Obligatoria
Department	Department of Telematics and Computer Scienes
Coordinator	Rafael Palacios
Office hours	Contact Prof. by email

Teacher Information	
<b>Teacher</b>	
Name	Ángel Prado Montes
Department	Department of Telematics and Computer Scienes
EMail	aprado@comillas.edu
<b>Teacher</b>	
Name	Javier Jarauta Sánchez
Department	Department of Telematics and Computer Scienes
EMail	jarauta@comillas.edu

## DESCRIPTION OF THE SUBJECT

Contextualization of the subject
<b>Prerequisites</b>
Previous knowledge is required on network communications, web applications, and introduction to cryptography.
Some programming skills are required for lab practices and exercises in class.

## Course contents

Contents
<p>Chapter 1: Introduction and course overview</p> <p>Chapter 2: Browser and HTTP/HTTPS fundamentals</p> <p>Chapter 3: Security Architecture and Security Analysis Methodologies</p> <p>Chapter 4: Attacks against the applications layer, and defenses</p> <p>Chapter 5: Advanced Persistent Threats. Common web vulnerabilities, and pentesting</p> <p>Chapter 6: Attacks against SSL/HTTPS and defenses</p> <p>Chapter 7: More advanced side-channel attacks</p> <p>Chapter 8: Mobile devices security</p> <p>Chapter 9: Security Management Systems</p> <p>Chapter 10: Security monitoring and computer forensics</p> <p>Chapter 11: Policies and security governance (Recovery and Resiliency)</p> <p>Chapter 12: Information trust and regulatory compliance (certification and standards)</p> <p>Chapter 13: Conclusion, Guest lecture and/or open research discussion</p>

## EVALUATION AND CRITERIA

Evaluation activities	Evaluation criteria	Weight
Final Exam: 50% Tests: 20%	Knowledge of the subject Capability to apply suitable tools to solve problems	70
Labs evaluation	Knowledge of the subject Capability to apply suitable tools to solve problems	30

## Grading

### Exams 70%

- 50% Final exam
- 20% Tests

### Labs evaluation 30%

- 20% Lab reports
- 10% Active participation in class

---

### July Exam (retake)

- 80% Retake Exam

- 20% Labs

## BIBLIOGRAPHY AND RESOURCES

### Basic References

- John R. Vacca, Managing Information Security, Second Edition -<http://www.amazon.com/Managing-Information-Security-Second-Edition/dp/0124166881>
- Michal Zalewski ,The Tangled Web: A Guide to Securing Modern Web Applications<http://www.amazon.com/The-Tangled-Web-Securing-Applications/dp/1593273886>

In compliance with current regulations on the **protection of personal data**, we would like to inform you that you may consult the aspects related to privacy and data [that you have accepted on your registration form](#) by entering this website and clicking on "download"

<https://servicios.upcomillas.es/sedelectronica/inicio.aspx?csv=02E4557CAA66F4A81663AD10CED66792>