Course guide
230152 - CSI - Information Security and Coding

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

Degree: BACHELOR’S DEGREE IN TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES ENGINEERING (Syllabus 2015). (Optional subject).
            BACHELOR’S DEGREE IN ELECTRONIC ENGINEERING AND TELECOMMUNICATION (Syllabus 2018). (Optional subject).

Academic year: 2022  ECTS Credits: 6.0  Languages: Spanish

LECTURER

Coordinating lecturer: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Others: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat idioma

TEACHING METHODOLOGY

- Lectures
- Application lectures
- Teamwork
- Individual work
- Presentations
- Written exams

LEARNING OBJECTIVES OF THE SUBJECT

- Learning general concepts of information security and privacy.
- Knowing the main mechanisms of authentication and key management.
- Deepening the knowledge of the main security protocols used on the Internet.
- Introducing the main data anonymization algorithms and the associated privacy guarantees
- Introducing the main privacy guarantees defined by different application scenarios.
- Understanding the challenges and mechanisms of privacy in personalized information systems
- Introducing anonymous communication systems

STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours large group</td>
<td>52,0</td>
<td>34.67</td>
</tr>
<tr>
<td>Self study</td>
<td>98,0</td>
<td>65.33</td>
</tr>
</tbody>
</table>

Total learning time: 150 h
## CONTENTS

### 1. Network security fundamentals

**Description:**
Security services and mechanisms. Symmetric cryptography and public-key cryptography; digital signature; Perimeter security.

**Full-or-part-time:** 18h  
Theory classes: 8h  
Self study: 10h

### 2. Authentication and Key Management

**Description:**
Authentication protocols and mechanisms; Key management protocols; Public Key infrastructures (PKI); Trust models.

**Full-or-part-time:** 24h  
Theory classes: 8h  
Self study: 16h

### 3. Internet Security Protocols

**Description:**
IP Security and Virtual Private Networks; Email security; Web security

**Full-or-part-time:** 24h  
Theory classes: 8h  
Self study: 16h

### 4. Introduction to data privacy

**Description:**
Motivation. Definition of basic concepts. Attackers and trusted parties. Privacy metrics.

**Full-or-part-time:** 12h  
Theory classes: 4h  
Self study: 8h

### 5. Data anonymization algorithms

**Description:**
Statistical disclosure control. Data microaggregation algorithms. Measuring the commitment to privacy-utility.

**Full-or-part-time:** 36h  
Theory classes: 12h  
Self study: 24h
6. Privacy in personalised information systems

Description:

Full-or-part-time: 12h
Theory classes: 4h
Self study : 8h

7. Anonymous communication systems.

Description:
content engTraffic analysis. Anonymous communications systems: TOR, Crowds, Mix Networks.lish

Full-or-part-time: 12h
Theory classes: 4h
Self study : 8h

8. Differential privacy

Description:
Syntactic vs. semantic privacy. Differential privacy in interactive databases.

Full-or-part-time: 12h
Theory classes: 4h
Self study : 8h

GRADING SYSTEM

The grade will be obtained from the continuous assessment, including active participation in class, as well as tests, oral presentations and class projects. If the student do not pass the continuous assessment, she/he can attend to a final exam.

BIBLIOGRAPHY

Basic:

Complementary: