Course guides

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 710 - EEL - Department of Electronic Engineering.
Degree: MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Optional subject).
Academic year: 2021 ECTS Credits: 3.0 Languages: English

LECTURER
Coordinating lecturer: Manich Bou, Salvador
Others: Manich Bou, Salvador
Rodríguez Montañes, Rosa
Arumi Delgado, Daniel
Álvaro Gómez Pau

TEACHING METHODOLOGY
The subject is assigned a teaching load of 3 ECTS credits, which is equivalent to a student dedication of 75 hours. 24 of these correspond to face-to-face activities and 51 to hours of personal work. The face-to-face part includes presentations of the topics and the resolution and discussion of examples. The material of the subject is available on the digital campus.

LEARNING OBJECTIVES OF THE SUBJECT
It is a specialty subject that has four fundamental objectives:
1) Understand how electronic technology affects the integration of security systems.
2) Discover how intrinsic properties of technology are harnessed to implement security primitives.
3) Analyze the security primitives, their weaknesses and the appropriate countermeasures.
4) Analyze the basic cryptographic and arithmetic modules, their weaknesses and countermeasures.

STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self study</td>
<td>51,0</td>
<td>68.00</td>
</tr>
<tr>
<td>Hours large group</td>
<td>24,0</td>
<td>32.00</td>
</tr>
</tbody>
</table>

Total learning time: 75 h
CONTENT

MODULE I - Technological Foundations for Security

Description:
- Tautology of attacks in security systems.
- Digital logic styles and electrical dependencies.
- Data leakages caused by technology.
- Strategies for reducing leakage data dependencies.

Full-or-part-time: 8h
Theory classes: 8h

MODULE II - Security Primitives. Weaknesses and Solutions

Description:
- True random number generators.
- Physical unclonable functions.
- Secure memories.
- Attacking primitive’s normal operation.
- Testing and protecting normal operation in primitives.

Full-or-part-time: 8h
Theory classes: 8h

MODULE III - Cryptomodules and Arithmetic. Weaknesses and Solutions

Description:
- Secret key crypto implementations.
- Arithmetic for public-key cryptography.
- Hardware design for hash functions.
- Simpler power analysis attacks.
- Differential power analysis attacks.
- Electromagnetic analysis attacks.
- Countermeasures against SPA/DPA/EMA.

Full-or-part-time: 8h
Theory classes: 8h

GRADING SYSTEM

The evaluation of the subject will be done according to three scores.
NPC - Class participation note.
NPT - Note of presentation of the work.
NTF - Final test note.
The qualification to the acts will be the result of applying the following equation, rounding to the nearest decimal:
NA = 0.20 NPC + 0.4 NPT + 0.4 NTF
Students who have not done either of the two parts NPT and NTF will be listed as not presented.
The assigned work can be done in groups of two people. The final test is an individual test.

EXAMINATION RULES.

The presentation of the work (NPT) will be an exhibition with transparencies of a maximum duration of 10 minutes. The final test (NTF) will be a multiple choice test, of 20 questions, to be answered in a maximum time of 2 hours.
BIBLIOGRAPHY

Basic: