Course guide
230989 - HSES - Hardware Security in Embedded Systems. Primitives, Weaknesses and Countermeasures

Last modified: 14/06/2023

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).
MASTER'S DEGREE IN ELECTRONIC ENGINEERING (Syllabus 2022). (Optional subject).

Academic year: 2023 **ECTS Credits:** 3.0 **Languages:** English

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

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

Type	Hours	Percentage
Self study	51,0	68.00
Hours large group	24,0	32.00

Total learning time: 75 h

CONTENTS

MODULE I - Technological Foundations for Security

Description:
- Tautology of attacks in security systems.
- Digital logic styles and electrical dependecies.
- Data leakages cause 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.
- Coutermeasures 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 score.
NPT - Score of the presentation.
NTF - Final report score.
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 slides of a maximum duration of 10 minutes.

BIBLIOGRAPHY

Basic:
- Koç, Çetin Kaya. Cryptographic engineering [on line]. Boston, MA: Springer US, 2009 [Consultation: 16/06/2021]. Available on: http://dx.doi.org/10.1007/978-0-387-71817-0. ISBN 9780387718170.
- Verbauwhede, Ingrid M.R. Secure integrated circuits and systems [on line]. Boston, MA: Springer US, 2010 [Consultation: 16/06/2021]. Available on: http://dx.doi.org/10.1007/978-0-387-71829-3. ISBN 9780387718293.
- Joye, Marc; Tunstall, Michael. Fault analysis in cryptography [on line]. Berlin: Springer, 2012 [Consultation: 19/10/2021]. Available on: https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=994274. ISBN 9781283627221.
- Bhunia, Swarup; Tehranipoor, Mark M. Hardware security: a hands-on learning approach [on line]. Cambridge: Elsevier, [2019] [Consultation: 18/03/2024]. Available on: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=5754491. ISBN 9780128124789.