Guia docent
230989 - HSES - Seguretat en el Hardware de Sistemes Incrustats: Primitives, Debilitats i Contramesures

Última modificació: 11/04/2025

Unitat responsable: Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
Unitat que imparteix: 710 - EEL - Departament d'Enginyeria Electrònica.

Titulació: MÀSTER UNIVERSITARI EN CIBERSEGURETAT (Pla 2020). (Assignatura optativa).
MÀSTER UNIVERSITARI EN ENGINYERIA ELECTRÒNICA (Pla 2022). (Assignatura optativa).

Curs: 2025 **Crèdits ECTS:** 3.0 **Idiomes:** Anglès

PROFESSORAT

Professorat responsable: SALVADOR MANICH BOU

Altres:

METODOLOGIES DOCENTS

L'assignatura té assignada una càrrega lectiva de 3 crèdits ECTS, la qual cosa equival a una dedicació de l'estudiant de 75 hores. 24 d'aquestes corresponen a activitats presencials i 51 a hores de treball personal.
La part presencial comprèn les exposicions dels temes i la resolució i discussió d'exemples. El material de l'assignatura està disponible al campus digital.

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

Es una assignatura d'especialitat que te quatre objectius fonamentals:
1) Entendre com afecta la tecnologia electrònica en la integració de sistemes de seguretat.
2) Descobrir com s'aprofiten propietats intrínseques de la tecnologia per implementar primitives de seguretat.
3) Analizar les primitives de seguretat, les seves debilitats i les contramesures adequades.
4) Analitzar els mòduls criptogràfics i aritmètics bàsics, les seves debilitats i les contramesures.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup gran	24,0	32.00
Hores aprenentatge autònom	51,0	68.00

Dedicació total: 75 h

CONTINGUTS

MÒDUL I - Fonaments tecnològics per a la seguretat

Descripció:
- Tautologia d'atacs en sistemes de seguretat.
- Estils de lògica digital i dependències elèctriques.
- Fuites de dades causades per la tecnologia.
- Estratègies per reduir les dependències de fuga de dades.

Dedicació: 8h
Grup gran/Teoria: 8h

MÒDUL II - Primitives de seguretat. Debilitats i solucions.

Descripció:
- Generadors de nombres aleatoris veritables.
- Funcions físiques no clonables.
- Memòries segures.
- Atacs a l'operació normal de les primitives.
- Verificació i protecció de l'operació normal en les primitives.

Dedicació: 8h
Grup gran/Teoria: 8h

MÒDUL III - Criptomòduls i aritmètica. Debilitats i solucions.

Descripció:
- Implementacions criptogràfiques de clau secreta.
- Aritmètica per criptografia de clau pública.
- Disseny de maquinari per a funcions hash.
- Atacs d'anàlisi simple de potència.
- Atacs d'anàlisi diferencial de potència.
- Atacs d'anàlisi electromagnètic.
- Contramesures per SPA / DPA / EMA.

Dedicació: 8h
Grup gran/Teoria: 8h

SISTEMA DE QUALIFICACIÓ

L'avaluació de l'assignatura es farà d'acord amb tres puntuacions.
NPC - Nota de participació a classe.
NPT - Nota de presentació del treball.
NTF - Nota de l'informe final.
La qualificació a les actes serà el resultat d'aplicar l'equació següent, arrodonint al decimal més proper:
NA = 0,20 NPC + 0,4 NPT + 0,4 NTF
Constaran com a no presentats els alumnes que no hagin fet cap de les dues parts NPT i NTF.
El treball encomanat es podrà fer en grups de dues persones.

NORMES PER A LA REALITZACIÓ DE LES PROVES.

La presentació del treball (NPT) serà una exposició amb transparències d'una duràda màxima de 10 minuts.

BIBLIOGRAFIA

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