Guia docent
2301215 - ASIC - Disseny d'Asic per a Sistemes d'Alta Seguretat

Última modificació: 19/04/2024

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

Titulació: MÀSTER UNIVERSITARI EN ENGINYERIA DE SEMICONDUCTORS I DISSENY MICROELECTRÒNIC (Pla 2024). (Assignatura optativa).

Curs: 2024 **Crèdits ECTS:** 4.0 **Idiomes:** Anglès

PROFESSORAT

Professorat responsable: Consultar aquí / See here:
https://telecos.upc.edu/ca/curs-actual/coordinadors-i-professorat

Altres: Consultar aquí / See here:
https://telecos.upc.edu/ca/curs-actual/coordinadors-i-professorat

METODOLOGIES DOCENTS

El nombre total d'hores d'aquesta assignatura optativa és de 30, distribuïdes de la següent manera:

â□□Classes teòriques: 18 hores
â□□Laboratoris: 12 hores
â□□Presentació final: 1 hora

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

1.Comentar les vulnerabilitats de seguretat presents als circuits integrats (CI) estàndard.
2.Adquirir coneixements sobre els procediments d'anàlisi i avaluació de les debilitats de seguretat.
3.Entendre les tècniques especialitzades per mitigar les fuites de canals laterals en dissenys funcionals i infraestructures de proves.
4.Explorar detectors auxiliars que ajudin a minimitzar l'impacte dels atacs de canal lateral.
5.Conèixer les tècniques d'atac avançades que s'utilitzen actualment, especialment en els microprocessadors.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores aprenentatge autònom	70,0	70.00
Hores grup petit	12,0	12.00
Hores grup gran	18,0	18.00

Dedicació total: 100 h

CONTINGUTS

Bloc 1. Revisió històrica i antecedents de la criptografia moderna

Descripció:
1. Context històric.
En aquest capítol inicial, aprofundirem en els conceptes fonamentals de Seguretat i Confiança, oferint una perspectiva històrica que dilucida la seva evolució en l'àmbit de les tecnologies de la informació a diferents nivells d'abstracció. La discussió aprofundirà en l'arrel de la confiança i la seva connexió històrica amb la tecnologia integrada.
2. Introducció a les tècniques modernes de criptografia.
En aquest segon capítol, es discutiran les tècniques i primitives de seguretat prevalents emprades en criptografia, destacant la seva implementació final al nucli dels circuits integrats (CI).

Dedicació: 4h
Grup gran/Teoria: 4h

Bloc 2. Amenaces i debilitats existents en les implementacions de maquinari

Descripció:
3. Vulnerabilitats en implementacions de maquinari de circuits integrats.
En aquest capítol, es descriu una visió general completa de les diverses vulnerabilitats inherents als CI de productes de seguretat. Aquestes vulnerabilitats impregnen diverses etapes, que van des de la fase de disseny fins a la cadena de producció, la distribució final i el desplegament al camp. Després de la producció, sorgeix l'àmbit expansiu de la falsificació, que abasta un espectre de metodologies com les tècniques d'enginyeria inversa. A més, s'explora una sèrie de tècniques, amb l'objectiu d'extreure secrets interns de manera subrepticia sotmetent els IC a condicions operatives anormals i explorant meticulosament les emissions intrínseques, comunament denominades canals laterals.
4. Tècniques d'enginyeria inversa: invasives, semiinvasives i no invasives.
En el desplegament al camp, les bretxes de seguretat que afecten els CI s'executen mitjançant tècniques d'enginyeria inversa. Aquest esforç té com a objectiu exposar la informació interna a diversos nivells, que van des de la recuperació integral de tot el disseny fins a la identificació d'informació clau en enfocaments més específics. L'elecció de la tècnica d'enginyeria inversa, ja sigui invasiva, semiinvasiva o no invasiva, depèn dels recursos a disposició de l'adversari i de les contramesures implementades dins del xip. Aquest capítol aprofundeix en els complexos detalls d'aquests aspectes, proporcionant una exploració matisada de les metodologies emprades.
5. Atacs de canal lateral i falla.
Els adversaris amb recursos tècnics limitats aprofiten les emissions del canal lateral i els atacs de falla, dues metodologies rendibles que es poden augmentar amb equips d'alt rendiment per millorar la seva eficiència. Els circuits integrats produeixen una gran varietat d'emissions laterals durant el funcionament, comprometent així el principi fonamental de la caixa negra de qualsevol sistema de seguretat. Aquest capítol dilucida casos d'ús pràctics en què la metodologia es detalla sistemàticament. Per millorar l'èxit dels atacs més actius, s'utilitzen atacs de falla. Això implica operar intencionadament l'IC més enllà de les especificacions i supervisar el seu comportament anormal per identificar possibles bretxes de seguretat.

Dedicació: 5h
Grup gran/Teoria: 5h

Bloc 3. Estratègies per reforçar les primitives de seguretat a nivell de maquinari

Descripció:
6. Mascareta de silici i mesures contra la falsificació.
Els centres de fabricació subcontractats han augmentat el potencial de diversos tipus de frau durant el procés de producció. Els propietaris legítims han respost implementant tècniques antifrau que impliquen emmascarar diferents parts del disseny. Aquest capítol aprofundeix en l'elucidació de diverses tècniques d'emmascarament utilitzades per protegir-se d'activitats fraudulentes.
7. Portes silencioses, emmascarament lògic i implementacions lògiques especials.
Enfortir la caixa negra significa fer que l'IC funcioni el més silenciós possible. Això vol dir que les emissions laterals no estan correlacionades amb les dades que s'estan processant. Quan això no és del tot possible l'emmascarament lògic arriba al rescat en el qual s'incorpora soroll a través de dades aleatòries amb l'objectiu d'enganyar l'adversari. Existeixen diferents tipus d'implementacions lògiques que exploten aquestes capacitats.
8. Assegurar la infraestructura de proves.
La infraestructura de prova és un component indispensable de cada IC, especialment en sistemes digitals. Durant la fase de la cadena de disseny, la integració de la infraestructura de prova normalment s'automatitza i constitueix un dels diversos passos del procés de disseny. Tanmateix, els procediments automatitzats sovint passen per alt les amenaces de seguretat, convertint la infraestructura de prova en una porta posterior potencial explotada pels adversaris que busquen comprometre la seguretat. Durant l'última dècada, ha sorgit un augment de recursos i solucions per millorar la seguretat de les infraestructures de prova. Aquest capítol aclareix algunes d'aquestes tècniques.
9. Primitives per a la seguretat.
Els CI són la base de la confiança en el domini de la seguretat. Les primitives de seguretat representen implementacions especialitzades de funcions de seguretat dissenyades per ser a prova de manipulacions des de la seva pròpia base. Aquest capítol presenta dos tipus diferents de primitives de seguretat: Funcions físiques no clonables (PUF) i Generadors de nombres aleatoris veritables (TRNG). Aprofitant les propietats físiques inherents del silici, aquests primitius enfosquien els seus secrets, fent-los excepcionalment resistents i pràcticament impermeables al compromís.

Dedicació: 6h
Grup gran/Teoria: 6h

Bloc 4. Temes de recerca avançada en disseny de CI per a la seguretat

Descripció:
10. Implementacions de seguretat per a dispositius Edge.
La computació basada en núvol és cada cop més omnipresent. No obstant això, amb l'augment de la concentració de potència als centres de càlcul, hi ha una acceleració concurrent de càlcul a les vores del núvol. Els dispositius Edge, en ser els punts terminals, són més susceptibles a les infraccions de seguretat, principalment a causa dels seus recursos limitats. Aquest capítol aborda de manera exhaustiva diversos aspectes de la informàtica perifèrica en relació amb la seguretat, inclosa la generació de claus, així com estratègies per aconseguir una seguretat de baix consum i de baix cost en les implementacions de maquinari per a aquests dispositius de punta dins d'aplicacions IoT.
11. Tècniques d'atac avançades en grans sistemes.
La seguretat és una consideració inherent a totes les facetes dels sistemes automatitzats, des del silici fins al nivell algorítmic. Aquest capítol ofereix una visió general completa, oferint una perspectiva global que abasta aquestes diverses capes i aborda qüestions fonamentals, com ara els troians, els factors arquitectònics que afecten els canals secundaris, els problemes generals de programari maliciós i les amenaces més recents i perilloses, com ara Spectre i Meltdown.

Dedicació: 2h
Grup gran/Teoria: 2h

Laboratori 1

Descripció:
Introducció al disseny i implementació d'un SBOX.

Dedicació: 2h
Grup petit/Laboratori: 2h

Laboratori 2

Descripció:
Biblioteca lógica de doble carril. Implementación y librería y rediseño del SBOX.

Dedicació: 2h
Grup petit/Laboratori: 2h

Laboratori 3

Descripció:
Lògica dinàmica de precàrrega d'onada. Millora de la biblioteca lògica dual amb aquesta tècnica de precàrrega. Millora de la SBOX i anàlisi del consum d'energia i detecció de fuites de dades.

Dedicació: 2h
Grup petit/Laboratori: 2h

Laboratori 4

Descripció:
Presentació del projecte: objectius, criteris d'avaluació i organització de l'equip de treball.

Dedicació: 2h
Grup petit/Laboratori: 2h

Laboratori 5

Descripció:
Sessió de treball supervisada sobre projecte.

Dedicació: 2h
Grup petit/Laboratori: 2h

Laboratori 6

Descripció:
Sessió de treball supervisada sobre projecte.

Dedicació: 2h
Grup petit/Laboratori: 2h

Presentació final

Descripció:
Presentació final del projecte

Dedicació: 1h
Grup gran/Teoria: 1h

SISTEMA DE QUALIFICACIÓ

En el procés d'avaluació es tenen en compte tres activitats a l'hora de qualificar els alumnes:

â□□Gde (20%): Inclou proves i treballs de classe, que es realitzen a classe i s'assignen com a deures.
â□□Grp (40%): Fa referència a la presentació del projecte, on els grups d'estudiants mostren l'assoliment dels objectius marcats.
â□□Gap (40%): representa l'examen final.

La nota final, denominada Gadhsy, es calcula mitjançant la fórmula: Gadhsy = 0,2 Gde + 0,4 Grp + 0,4 Gap

BIBLIOGRAFIA

Bàsica:
- 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 9780128124772.
- Goubin,Louis; Matsui, Mitsuru. Cryptographic Hardware and Embedded Systems [en línia]. 1. [Berlin ; New York]: Springer-Verlag Heidelberg, [2006] [Consulta: 18/03/2024]. Disponible a: https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/11894063. ISBN 1611-3349.
- Tehranipoor, Mark; Guin, Ujjwal; Forte, Domenic. Counterfeit integrated circuits [en línia]. Cham: Springer, 2015 [Consulta: 18/03/2024]. Disponible a: https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/978-3-319-11824-6. ISBN 9783319118246.
- Thomas, Donald E.; Moorby, Philip R. The Verilog hardware description language [en línia]. 5th ed. New York: Kluwer, 2002 [Consulta: 18/03/2024]. Disponible a: https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/b116662. ISBN 9780306476662.