Guía docente
2301215 - ASIC - Diseño de Asic para Sistemas Altamente Seguros

Última modificación: 19/04/2024

Unidad responsable: Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona
Unidad que imparte: 710 - EEL - Departamento de Ingeniería Electrónica.

Titulación: MÁSTER UNIVERSITARIO EN INGENIERÍA DE SEMICONDUCTORES Y DISEÑO MICROELECTRÓNICO (Plan 2024). (Asignatura optativa).

Curso: 2024 **Créditos ECTS:** 4.0 **Idiomas:** Inglés

PROFESORADO

Profesorado responsable: Consultar aquí / See here:

Otros: Consultar aquí / See here:

METODOLOGÍAS DOCENTES

El número total de horas de esta asignatura optativa es de 30, distribuidas de la siguiente manera:

â□□Clases teóricas: 18 horas
â□□Laboratorios: 12 horas
â□□Presentación final: 1 hora

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

1.Discutir las vulnerabilidades de seguridad presentes en los circuitos integrados (CI) estándar.
2.Adquirir conocimientos sobre los procedimientos de análisis y evaluación de las debilidades de seguridad.
3.Comprender técnicas especializadas para mitigar fugas de canales laterales en diseños funcionales e infraestructura de prueba.
4.Explore detectores auxiliares que ayuden a minimizar el impacto de los ataques de canales laterales.
5.Obtener información sobre las técnicas de ataque avanzadas que se utilizan actualmente, particularmente dentro de los microprocesadores.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas aprendizaje autónomo	70,0	70.00
Horas grupo grande	18,0	18.00
Horas grupo pequeño	12,0	12.00

Dedicación total: 100 h

CONTENIDOS

Bloque 1. Reseña histórica y antecedentes de la criptografía moderna

Descripción:
1. Contexto histórico.
En este capítulo inicial, profundizaremos en los conceptos fundacionales de Seguridad y Confianza, ofreciendo una perspectiva histórica que dilucida su evolución dentro del ámbito de las tecnologías de la información a través de varios niveles de abstracción. La discusión profundizará en la raíz de la confianza y su conexión histórica con la Tecnología Integrada.
2. Introducción a las técnicas modernas de criptografía.
En este segundo capítulo, se discutirán las técnicas predominantes y las primitivas de seguridad empleadas en criptografía, destacando su implementación final en el núcleo de los circuitos integrados (CI).

Dedicación: 4h
Grupo grande/Teoría: 4h

Bloque 2. Amenazas y debilidades existentes en las implementaciones de hardware

Descripción:
3. Vulnerabilidades en implementaciones hardware de Circuitos Integrados.
En este capítulo, se describe una descripción general completa de las diversas vulnerabilidades inherentes a los circuitos integrados de productos de seguridad. Estas vulnerabilidades permean varias etapas, que van desde la fase de diseño hasta la cadena de producción, la distribución final y el despliegue en el campo. Después de la producción, surge el amplio ámbito de la falsificación, que abarca un espectro de metodologías como las técnicas de ingeniería inversa. Además, se explora una serie de técnicas con el objetivo de extraer subrepticiamente secretos internos sometiendo los circuitos integrados a condiciones operativas anormales y escaneando meticulosamente en busca de emisiones intrínsecas, comúnmente denominadas canales laterales.
4. Técnicas de ingeniería inversa: invasivas, semiinvasivas y no invasivas.
Tras su implementación en el campo, las violaciones de seguridad que afectan a los circuitos integrados se ejecutan mediante técnicas de ingeniería inversa. Estos esfuerzos tienen como objetivo exponer información interna en varios niveles, que van desde la recuperación integral de todo el diseño hasta la identificación de información clave en enfoques más específicos. La elección de la técnica de ingeniería inversa (ya sea invasiva, semiinvasiva o no invasiva) depende de los recursos a disposición del adversario y de las contramedidas implementadas dentro del chip. Este capítulo profundiza en los intrincados detalles de estos aspectos, proporcionando una exploración matizada de las metodologías empleadas.
5. Ataques de canal lateral y de falla.
Los adversarios que poseen recursos técnicos limitados aprovechan las emisiones de canales laterales y los ataques a fallas, dos metodologías rentables que pueden complementarse con equipos de alto rendimiento para mejorar su eficiencia. Los circuitos integrados producen una amplia gama de emisiones laterales durante el funcionamiento, comprometiendo así el principio fundamental de caja negra de cualquier sistema de seguridad. Este capítulo aclara casos de uso prácticos en los que la metodología se detalla sistemáticamente. Para mejorar el éxito de ataques más activos, se emplean ataques de falla. Esto implica operar intencionalmente el IC más allá de las especificaciones y monitorear su comportamiento anormal para identificar posibles violaciones de seguridad.

Dedicación: 5h
Grupo grande/Teoría: 5h

Bloque 3. Estrategias para fortalecer las primitivas de seguridad a nivel de hardware

Descripción:
6. Enmascaramiento de silicona y medidas antifalsificación.
Los centros de fabricación subcontratados han aumentado la posibilidad de que se produzcan diversos tipos de fraude durante el proceso de producción. Los propietarios legítimos han respondido implementando técnicas antifraude que implican enmascarar diferentes partes del diseño. Este capítulo profundiza en la elucidación de varias de estas técnicas de enmascaramiento empleadas para protegerse contra actividades fraudulentas.
7. Puertas silenciosas, enmascaramiento lógico e implementaciones lógicas especiales.
Fortalecer la caja negra significa hacer que el CI funcione lo más silencioso posible. Esto significa que las emisiones laterales no deben estar correlacionadas con los datos que se están procesando. Cuando esto no es del todo posible viene al rescate el enmascaramiento lógico en el que se incorpora ruido a través de datos aleatorios con el objetivo de engañar al adversario. Existen diferentes tipos de implementaciones lógicas que explotan estas capacidades.
8. Asegurar la infraestructura de prueba.
La infraestructura de prueba es un componente indispensable de cada circuito integrado, especialmente en los sistemas digitales. Durante la fase de la cadena de diseño, la integración de la infraestructura de prueba suele estar automatizada y constituye uno de varios pasos en el proceso de diseño. Sin embargo, los procedimientos automatizados a menudo pasan por alto las amenazas a la seguridad, lo que convierte la infraestructura de prueba en una posible puerta trasera explotada por adversarios que buscan comprometer la seguridad. Durante la última década, ha surgido un aumento de recursos y soluciones para mejorar la seguridad de las infraestructuras de prueba. Este capítulo arroja luz sobre algunas de estas técnicas.
9. Primitivas por seguridad.
Los circuitos integrados son la base de la confianza en el ámbito de la seguridad. Las primitivas de seguridad representan implementaciones especializadas de funciones de seguridad diseñadas para ser a prueba de manipulaciones desde su propia base. Este capítulo presenta dos tipos distintos de primitivas de seguridad: funciones físicas no clonables (PUF) y generadores de números aleatorios verdaderos (TRNG). Aprovechando las propiedades físicas inherentes del silicio, estos primitivos oscurecen sus secretos, volviéndolos excepcionalmente resistentes y prácticamente inmunes a cualquier compromiso.

Dedicación: 6h
Grupo grande/Teoría: 6h

Bloque 4. Temas de investigación avanzada en diseño de circuitos integrados para seguridad

Descripción:
10. Implementaciones de seguridad para dispositivos perimetrales.
La computación basada en la nube es cada vez más omnipresente. Sin embargo, con la creciente concentración de poder en los centros de computación, hay una aceleración simultánea de la computación en los bordes de la nube. Los dispositivos perimetrales, al ser puntos terminales, son más susceptibles a violaciones de seguridad, principalmente debido a sus recursos limitados. Este capítulo aborda de manera integral varios aspectos de la computación de borde relacionados con la seguridad, incluida la generación de claves, así como estrategias para lograr seguridad de bajo consumo y bajo costo en implementaciones de hardware para estos dispositivos de borde dentro de las aplicaciones de IoT.
11. Técnicas avanzadas de ataque en grandes sistemas.
La seguridad es una consideración inherente en todas las facetas de los sistemas automatizados, desde el nivel de silicio hasta el nivel algorítmico. Este capítulo proporciona una descripción general integral, ofreciendo una perspectiva global que abarca estas diversas capas y aborda problemas fundamentales, incluidos los troyanos, los factores arquitectónicos que afectan los canales laterales, las preocupaciones generales sobre el malware y las amenazas más recientes y peligrosas, como Spectre y Meltdown.

Dedicación: 2h
Grupo grande/Teoría: 2h

Laboratorio 1

Descripción:
Introducción al diseño e implementación de un SBOX.

Dedicación: 2h
Grupo pequeño/Laboratorio: 2h

Laboratorio 2

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

Dedicación: 2h
Grupo pequeño/Laboratorio: 2h

Laboratorio 3

Descripción:
Lógica dinámica de precarga d'onada. Mejora de la biblioteca lógica dual con esta técnica de precarga. Mejora del SBOX y análisis del consumo eléctrico y detección de fuga de datos.

Dedicación: 2h
Grupo pequeño/Laboratorio: 2h

Laboratorio 4

Descripción:
Presentación del proyecto: objetivos, criterios de evaluación y organización del equipo de trabajo.

Dedicación: 2h
Grupo pequeño/Laboratorio: 2h

Laboratorio 5

Descripción:
Sesión de trabajo supervisada en proyecto.

Dedicación: 2h
Grupo pequeño/Laboratorio: 2h

Laboratorio 6

Descripción:
Sesión de trabajo supervisada en proyecto.

Dedicación: 2h
Grupo pequeño/Laboratorio: 2h

Presentación final

Descripción:
Presentación final del proyecto

Dedicación: 1h
Grupo grande/Teoría: 1h

SISTEMA DE CALIFICACIÓN

En el proceso de evaluación se tienen en cuenta tres actividades a la hora de calificar a los estudiantes:

â□□Gde (20%): Esto incluye pruebas y tareas, que se realizan en clase y se asignan como entregas.
â□□Grp (40%): Se refiere a la presentación del proyecto, donde los grupos de estudiantes muestran el logro de los objetivos establecidos.
â□□Gap (40%): Representa el examen final.

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

BIBLIOGRAFÍA

Básica:

- Bhunia, Swarup; Tehranipoor, Mark M. Hardware security : a hands-on learning approach [en línea]. 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 línea]. 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 línea]. 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 línea]. 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.