ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2016/2017

Máster Oficial en Ingeniería Informática

DATOS DE LA ASIGNATURA			
Nombre:			
Ataques y Seguridad Hardware			
Denominación en inglés:			
Hardware Attacks and Security			
Código:		**Carácter:**	
1140220		Optativo	
Horas:			
	Totales	**Presenciales**	**No presenciales**
Trabajo estimado:	150	60	90
Créditos:			

	Grupos reducidos			
Grupos grandes	**Aula estándar**	**Laboratorio**	**Prácticas de campo**	**Aula de informática**
4.14	0	1.86	0	0

Departamentos:	**Áreas de Conocimiento:**
Ingeniería Electrónica, Sistemas Informáticos y Automática	Ingeniería de Sistemas y Automática
Ingeniería Electrónica, Sistemas Informáticos y Automática	Tecnología Electrónica
Curso:	**Cuatrimestre:**
2º - Segundo	Primer cuatrimestre

DATOS DE LOS PROFESORES			
Nombre:	**E-Mail:**	**Teléfono:**	**Despacho:**
*Jiménez Naharro, Raúl	naharro@uhu.es	959 21 7660	TUPB-13

*Profesor coordinador de la asignatura

Consultar los horarios de la asignatura

DATOS ESPECÍFICOS DE LA ASIGNATURA

1. Descripción de contenidos

1.1. Breve descripción (en castellano):

Diferencias entre ataques software y ataques hardware. Clasificación de ataques hardware: invasivos y no invasivos. Tipos de ataques hardware: ingenieríainversa, ataques mediante inserción de fallos, clonación, ¿ Módulos de encriptación hardware. Métodos de autenticación. Mecanismos de seguridad:identificación de módulos, sensorización, ¿ Comunicación en entornos hostiles.

1.2. Breve descripción (en inglés):

Differences between software and hardware attacks. Classification of hardware attacks: invasive and noon-invasive. Kind of hardware attacks: reverse engineering, fault injection attacks, cloning. Hardware modules of encryption. Authentication methods. Security: modules identification, sensoring. Communication in hostile environments.

2. Situación de la asignatura

2.1. Contexto dentro de la titulación:

La asignatura "Ataques y Seguridad Hardware" se encuentra enmarcada en el tercer cuatrimestre (por lo tanto, primer cuatrimestre del segundo curso) del Título de Máster en Ingeniería Informática. Dicha asignatura trata de cubrir los conocimientos y competencias relativas a la seguridad de los sistemas informáticos desde un punto de vista hardware, tema muy importante en la utilización de estos sistemas. Al tratarse desde una perspectiva hardware, estas técnicas también son aplicables a cualquier sistema electrónico en general.

2.2. Recomendaciones:

Sería aconsejable que el alumno tuviese un cierto conocimiento del lenguaje VHDL.

3. Objetivos (Expresados como resultados del aprendizaje):

La competencia aportada por esta asignatura se puede expresar como:
"Capacidad para diseñar y desarrollar mecanismos garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido"
Dicha competencia, expresada como resultados del aprendizaje, implicará que el alumno tendrá las competencias para:

- Distinguir entre una vulneración de la seguridad desde un punto de vista hardware y un punto de vista software.
- Identificar los principales tipos de ataques que un sistema puede sufrir, sin que esté involucrado el código software que es ejecutado (en su caso).Desarrollar las metodologías necesarias para ejecutar un ataque (pero no para capturar información privilegiada).
- Identificar los diferentes mecanismos de seguridad para hacer frente a los ataques.
- Desarrollar las metodologías necesarias para la inclusión de dichos mecanismos.

4. Competencias a adquirir por los estudiantes

4.1. Competencias específicas:

4.2. Competencias básicas, generales o transversales:

- **CB6:** Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
- **CB7:** Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
- **CB9:** Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
- **CB10:** Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo
- **CG1:** Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería informática
- **CG6:** Capacidad para la dirección general, dirección técnica y dirección de proyectos de investigación, desarrollo e innovación, en empresas y centros tecnológicos, en el ámbito de la Ingeniería Informática
- **CG8:** Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y mulitidisciplinares, siendo capaces de integrar estos conocimientos

5. Actividades Formativas y Metodologías Docentes

5.1. Actividades formativas:

- Sesiones de Teoría sobre los contenidos del Programa.
- Sesiones de Resolución de Problemas.
- Sesiones Prácticas en Laboratorios Especializados o en Aulas de Informática.
- Actividades Académicamente Dirigidas por el Profesorado: seminarios, conferencias, desarrollo de trabajos, debates, tutorías colectivas, actividades de evaluación y autoevaluación.

5.2. Metologías docentes:

- Clase Magistral Participativa.
- Desarrollo de Prácticas en Laboratorios Especializados o Aulas de Informática en grupos reducidos.
- Resolución de Problemas y Ejercicios Prácticos.
- Tutorías Individuales o Colectivas. Interacción directa profesorado-estudiantes.
- Planteamiento, Realización, Tutorización y Presentación de Trabajos.
- Evaluaciones y Exámenes.

5.3. Desarrollo y justificación:

La asignatura dispone de un total de 60 horas presenciales distribuidas en dos clases de 1.5 horas y una clase de 1 hora durante quince semanas. La distribución horaria en actividades formativas, junto a las metolodgías docentes se detallana a acontinuación.
Las sesiones teóricas dispondrán de un total de 24.9 horas dispuestas en 16 clases de 1.5 horas y una clase de 0.9 horas. En estas sesiones se impartirán los conocimientos necesarios para adquirir las competencias establecidas, utilizando una metodología docente de clase magistral participativa. Debido al carácter eminentemente práctico de la asignatura, se pondrá especial énfasis en el carácter participativo de la metodología.
Las sesiones de resolución de problemas dispondrán de un total de 10 horas dispuestas en 10 clases de 1 hora. En estas sesiones se propondrán y realizarán trabajos de índole docente sobre la temática de la asignatura, utilizando la metodología de resolución de problemas y ejercicios prácticos.
Las sesiones de prácticas en laboratorios especializados dispondrán de un total de 18.6 horas dispouestas en 12 clases de 1.5 horas y una clase de 0.6 horas. En estas sesiones se pasarán de los casos docentes a los casos reales sobre la temática de la asignatura. Para ello se utilizará la metodología docente de desarrollo de prácticas en laboratorios especializados.
Las actividades académicamente dirigidas por el profesorado dispondran de un total de 4.5 horas presenciales dispuestas en 1 clase de 1.5 horas y 3 clases de 1 hora. En estas sesiones, el profesor propondrá un conjunto de problemas específico a cada grupo de alumnos. Estas sesiones, junto con parte de la docencia no presencial, utilizará la metodología de planteamiento, realización, tutorización y presentación de trabajos; de tal forma que los grupos obtendrán una solución a sus problemas propuestos, expondiendo los resultados al resto de la clase. Dicha exposición acabará con un debate por parte de todos los alumnos.
Finalmente, las actividades de evaluación y autoevaluación dispondrán de un total de 2 horas dispuestas en dos clases de una hora. Dicha actividad hará uso de la metodología de evaluaciones y exámenes que se tratará en mayor detalle en el apartado de mecanismos de evaluación.
Ya fuera del ámbito presencial, se utilizará la metodología de tutorías individuales o colectivas para la resolución de dudas por parte del alumno. Cuando la duda sea planteada por un alumno, la tutoría será individual. Pero cuando la duda sea planteada por un grupo de alumno, la tutoría será colectiva buscando en este caso un espacio acorde al número de alumnos interesados.

6. Temario desarrollado:

****
BLOQUE TEMÁTICO: FUNDAMENTOS
Tema 1. Introducción a los Ataques y Seguridad Hardware
1. Introducción
2. Objetivos del ataque
3. Diferencia entre ataques software y hardware
4. Clasificación de hackers hardware

****
BLOQUE TEMÁTICO: MECANISMOS DE ATAQUE
Tema 2. Ataques Hardware
1. Introducción
2. Clasificación de ataques
3. Tipos de ataques

****
BLOQUE TEMÁTICO: MECANISMOS DE DEFENSA
Tema 3. Contramedidas
1. Introducción
2. Arquitecturas seguras
3. Tipos de contramedidas

****
BLOQUE TEMÁTICO: EJEMPLOS
Tema 4. Tarjetas inteligentes
1. Introducción
2. Arquitectura
3. Ataques y defensas conocidos

Tema 5. Aplicaciones
1. Introducción
2. Ataques y defensas en sistemas hardware
3. Ataques y defensas en sistemas software
4. Ataques y defensas en comunicaciones

7. Bibliografía

7.1. Bibliografía básica:

Fuente 1:
- Título: Security Engineering
- Autor: Ross Anderson
- Editorial: Wiley
- Año: 2008
- ISBN: 978-0-470-06852-6

Fuente 2:
- Título: Physical Security Devices for Computer Subsystems: A survey of Attacks and Defenses 2008
- Autor: Steve H. Weingart
- Editorial: ASEC Information Security Corporation
- Año: 2008

7.2. Bibliografía complementaria:

Fuente 1:
- Título: FPGA Prototyping by VHDL Examples
- Autor: Pong P. Chu
- Editorial: Wiley
- Año: 2008
- ISBN: 978-0-470-18531-5

8. Sistemas y criterios de evaluación.

8.1. Sistemas de evaluación:

- Examen de teoría/problemas
- Defensa de Prácticas
- Defensa de Trabajos e Informes Escritos

8.2. Criterios de evaluación y calificación:

Los mecanismos utilizados para obtener la calificación final del alumno son los siguientes:

- Examen de teoría/problemas: 25%
- Defensa de prácticas: 50%
- Defensa de trabajos e informes: 25%

9. Organización docente semanal orientativa:

Semanas	Grupos Grandes	Grupos Reducidos Aula Estándar	Grupos Reducidos Aula de Informática	Grupos Reducidos Laboratorio	Grupos Reducidos prácticas de campo	Pruebas y/o actividades evaluables	Contenido desarrollado
#1	3.4	0	0	0.6	0		Tema 1/Práctica 1
#2	4	0	0	0	0	Cuestionarios y lecciones	Tema 1
#3	4	0	0	0	0		Tema 2
#4	2.5	0	0	1.5	0		Tema 2/Práctica 1
#5	2.5	0	0	1.5	0		Tema 2/Práctica 1
#6	2.5	0	0	1.5	0		Tema 3/Práctica 1
#7	2.5	0	0	1.5	0		Tema 3/Práctica 1
#8	2.5	0	0	1.5	0		Tema 3/Práctica 2
#9	2.5	0	0	1.5	0		Tema 3/Práctica 2
#10	2.5	0	0	1.5	0		Tema 4/Práctica 2
#11	2.5	0	0	1.5	0		Tema 4/Práctica 2
#12	2.5	0	0	1.5	0		Tema 4/Práctica 3
#13	2.5	0	0	1.5	0		Tema 4/Práctica 3
#14	2.5	0	0	1.5	0		Tema 4/Práctica 3
#15	2.5	0	0	1.5	0		Tema 4/Práctica 3
	41.4	0	0	18.6	0		