ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2019/2020

Máster en Ingeniería Informática (Plan 2018)

DATOS DE LA ASIGNATURA			
Nombre:			
Ataques y Seguridad Hardware			
Denominación en inglés:			
Hardware Attacks and Security			
Código:		**Carácter:**	
1180407		Obligatorio	
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, de Sistemas Informáticos y Automática	Ingeniería de Sistemas y Automática
Ingeniería Electrónica, de Sistemas Informáticos y Automática	Tecnología Electrónica
Curso:	**Cuatrimestre:**
1º - Primero	Primer cuatrimestre

DATOS DE LOS PROFESORES			
Nombre:	**E-Mail:**	**Teléfono:**	**Despacho:**
*Jiménez Naharro, Raúl	naharro@diesia.uhu.es	959 21 7660	ETP224/ETSI/Campus El Carmen

*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):

En esta asignatura se tratarán los siguientes contenidos. En primer lugar, se mostrará la diferencia existente entre ataques software y ataques hardware. A continuación, se verán diferentes tipos de clasificaciones de ataques hardware (como la que los divide en invasivos y no invasivos). Después de su tratamiento genérico, se pasa a la particularización de algunos de ellos, como pueden ser ingeniería inversa, ataques mediante inserción de fallos, clonación, etd. Una vez detectadas las posibles vulnerabilidades de nuestro sistema, se plantea la situación de defensa. En primer lugar, se trata la defensa de forma genérica, para después particularizar en algunos métodos como pueden ser módulos de encriptación hardware, métodos de autenticación, identificación de módulos, sensorización, etc. Del mismo modo también se considerarán los ataques y defensas a la comunicación entre sistemas, es decir, estudiando la comunicación en entornos hostiles.

1.2. Breve descripción (en inglés):

In this subject the following contents will be treated. First, the difference between software attacks and hardware attacks will be shown. Next, you will see different types of hardware attack classifications (such as the one that divides them into invasive and non-invasive). After its generic treatment, it goes on to the particularization of some of them, such as reverse engineering, attacks by inserting faults, cloning, etc. Once detected the possible vulnerabilities of our system, the defense situation arises. In the first place, the defense is treated in a generic way, to then particularize in some methods such as hardware encryption modules, authentication methods, identification of modules, sensorization, etc. In the same way, attacks and defenses to communication between systems will also be considered, that is, studying communication in hostile environments.

2. Situación de la asignatura

2.1. Contexto dentro de la titulación:

Esta asignatura se encuentra en el primer cuatrimestre del primer curso del Máster Oficial en Ingeniería Informática, dentro de la especialidad de "Ciberseguridad". Dicha asignatura trata de cubrir losconocimientos y competencias relativas a la seguridad de los sistemas informáticos desde un punto de vista hardware, temamuy importante en la utilización de estos sistemas. Al tratarse desde una perspectiva hardware, estas técnicas también sonaplicables a cualquier sistema electrónico en general.

2.2. Recomendaciones:

Sería aconsejable que el alumno tuviese un cierto conocimiento del lenguaje VHDL, ya adquirido en el Grado en Ingeniería Informática.

3. Objetivos (Expresados como resultados del aprendizaje):

El alumno, después de cursar esta asignatura, será capaz de:

- 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:

- **CETI4:** Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

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
- **CT1:** Gestionar adecuadamente la información adquirida expresando conocimientos avanzados y demostrando, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en el campo de estudio.
- **CT2:** Dominar el proyecto académico y profesional, habiendo desarrollado la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro su ámbito temático, en contextos interdisciplinares y, en su caso, con un alto componente de transferencia del conocimiento.
- **CT4:** Comprometerse con la ética y la responsabilidad social como ciudadano y como profesional, con objeto de saber actuar conforme a los principios de respeto a los derechos fundamentales y de igualdad entre hombres y mujeres y respeto y promoción de los Derechos Humanos, así como los de accesibilidad universal de las personas discapacitadas, de acuerdo con los principios de una cultura de paz, valores democráticos y sensibilización medioambiental.

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.
- 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 tiene asignada un total de seis créditos, o lo que es lo mismo, un total de 60 horas. Además la asignatura tiene un grado de presencialidad del 50%, por lo que la presencialidad del alumno en el aula es igual a 30 horas. Para ello, la asignatura tiene reservadas dos horas semanales durante un cuatrimestre completo, distribuidas en un única sesión de dos horas. Según la ficha de la memoria de verificación, se tendrán un total de 12 horas para clases de teoría (distribuidas en seis sesiones de 2 horas), 12 horas para prácticas de laboratorio (distribuidas en seis sesiones de 2 horas), 4 horas para actividades académicamente dirigidas y 2 horas para actividades de evaluación.
Las sesiones de teoría serán utilizadas para recalcar al alumno los contenidos más importantes y de más difícil asimilación de su aprendizaje autónomo (que será importante debido al grado de presencialidad del Título). Las metodologías básicas utilizadas en estas sesiones serán la clase magistral participativa y la resolución de problemas. También se utilizará la metodología de visualización y escuchas de vídeos seleccionados, para dotar al alumno de diferentes versiones y problemáticas del contenido estudiado. Con el fin de hacer las clases lo más dinámicas posibles, el carácter participativo será remarcado en ambas metodologías. La principal función de la clase magistral participativa será la adquisición y asimilación de conocimientos, mientras que en el caso de las sesiones de problemas, será la aplicación de dichos conocimientos a casos prácticos.
Adicionalmente, un selecto grupos de problemas serán realizados en grupos y expuestos al resto de la clase utilizando una metodología de planteamiento, realización, tutorización y presentación de trabajos. Estas acciones utilizarán una metodología de actividades académicamente dirigidas y actividades de evaluación.
Finalmente, las sesiones prácticas de laboratorio tendrán el mismo objetivo que las sesiones de problemas. La diferencia entre ambas metodologías será la tipología y la conclusión de las actividades. Mientras que en las sesiones de problemas se utilizarán principalmente situaciones académicas que permitan explotar los conocimientos en la mayor medida de lo posible; en el caso de las sesiones prácticas se utilizarán situaciones cuasi-reales llegando a implementaciones físicas de la solución. La metodología utilizada en estas sesiones será el desarrollo de prácticas en laboratorios especializados o aulas de informática en grupos reducidos.
La distribución anterior podrá ser modificada en función del discurrir de la asignatura, incluyendo seminarios y conferencias. Esta alteración podrá ser realizada porque todas las sesiones se llevarán a cabo en el mismo aula, con capacidad informática y de placas de desarrollo.
Ya fuera del carácter presencial, y debido al grado de presencialidad, se utilizarán un cierta variedad de metodologías docentes en el aprendizaje autónomo. Entre dichas metodologías caben destacar las siguientes: metodología de tutorías individuales o colectivas, utilizada para la resolución de dudas que puedan plantear los propios alumnos; cuando se precise por imposibilidad de desplazamiento, también se utilizarán tutorías en línea; también se utilizará la metodología de trabajo colaborativo y metodologías basadas en la acción, principalmente en la resolución de problemas y trabajos.
Finalmente, la calificación será determinada por la metodología de evaluaciones y exámenes. Esta metodología será explicada en mayor detalle en el apartado de mecanismos de evaluación.

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:

CRITERIOS PARA LA OBTENCIÓN DE LA MENCIÓN DE "MATRÍCULA DE HONOR".
La mención de "Matrícula de Honor" podrá ser otorgada a aquellos alumnos que han superado una calificación del 95% en cada uno de los criterios de evaluación (examen de teoría/problemas, defensa de prácticas y defensa de trabajos e informes escritos).
En el caso de que haya que desempatar porque existan más alumnos que uedan optar a la mención de "Matrícula de Honor" que posibles menciones, las menciones serán otorgadas a los alumnos que obtengan una mayor puntuación en el examen de teoría/problemas, y si todavía hay empate, los que obtengan una mayor puntuación en la defensa de prácticas; y si todavía hay empate, los que obtengan una mayor puntuación en la defensa de trabajos e informes escritos.
SISTEMA DE EVALUACIÓN CONTINUA. Los sistemas de evaluación utilizados estarán ponderados de la siguiente forma:

- Examen de teoría/problemas: 10% (se evaluarán las competencias CG1, CB6, CB7, CB9, CT1, CETI4). Dicho examen será un examen tipo test.
- Defensa de Prácticas: 40% (se evaluarán las competencias CG1, CG6, CG8, CB7, CB9, CT1, CT2, CT4, CETI4). La defensa de los prácticas será realizada mediante una exposición oral de las soluciones utilizadas el mismo día del examen.
- Defensa de Trabajos e Informes Escritos: 30% (se evaluarán las competencias CG1, CG6, CG8, CB7, CB9, CT1, CT2, CT4, CETI4). La defensa de los trabajos e informes escritos serán realizada mediante un informe escrito.
- Pruebas de evaluación mediante plataformas de enseñanza virtual: 10% (se evaluarán las competencias CG1, CG8, CB6, CB7, CB10, CT1, CT4, CETI4)
- Participación en las actividades propuestas: 10% (se evaluarán las competencias CG1, CG8, CB6, CB7, CB10, CT1, CT4, CETI4)

En el seguimiento individual del estudiante se valorará tanto las pruebas de evaluación mediante plataformas de enseñanza virtual como la participación en las actividades propuestas.
Este sistema se podrá aplicar a las convocatorias I y II siempre y cuando la realización de trabajos (40% para las prácticas y 30% para los trabajos) y el seguimiento individual del estudiante (10% para las pruebas en plataformas de enseñanza virtual y 10% para la participación) hayan sido realizados durante el curso correspondiente a la convocatoria en cuestión.Este sistema se podrá aplicar a la convocatoria III siempre y cuando la realización de trabajos (40% para las prácticas y 30% para los trabajos) y el seguimiento individual del estudiante (10% para las pruebas en plataformas de enseñanza virtual y 10% para la participación) hayan sido realizados durante el curso anterior a la convocatoria en cuestión.
SISTEMA DE EVALUACIÓN ÚNICA. Los sistemas de evaluación utilizados estarán ponderados de la siguiente forma:

- Examen de teoría/problemas: 10% (se evaluarán las competencias CG1, CB6, CB7, CB9, CT1, CETI4). Dicho examen será un examen tipo test.
- Defensa de Prácticas: 40% (se evaluarán las competencias CG1, CG6, CG8, CB7, CB9, CT1, CT2, CT4, CETI4). La realización de esta actividad será realizada a través de una prueba en el laboratorio.
- Defensa de Trabajos e Informes Escritos: 30% (se evaluarán las competencias CG1, CG6, CG8, CB7, CB9, CT1, CT2, CT4, CETI4). La realización de esta actividad será realizada a través de preguntas específicas durante el examen.
- Pruebas de evaluación mediante plataformas de enseñanza virtual: 10% (se evaluarán las competencias CG1, CG8, CB6, CB7, CB10, CT1, CT4, CETI4). La realización de esta actividad será realizada a través de preguntas específicas durante el examen.
- Participación en las actividades propuestas: 10% (se evaluarán las competencias CG1, CG8, CB6, CB7, CB10, CT1, CT4, CETI4). La realización de esta actividad será realizada a través de preguntas específicas durante el examen.

Como se indica en la normativa de evaluación de la Universidad de Huelva, aquellos alumnos que deseen utilizar el sistemade evaluación único deberán solicitarlo (vía email de la UHU) al docente de la asignatura en las dos primeras semanas declase. Según la solicitud, este sistema de evaluación podrá ser utilizado en las convocatorias I, II y III. Adicionalmente, este será el único sistema de evaluación válido para la convocatoria extraordinaria para lo cual no hará falta solicitud.

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	0.4	0	0	0.6	0		Tema I
#2	2	0	0	0	0		Tema I
#3	3	0	0	0	0	Cuestionarios y Lecciones	Tema I
#4	3	0	0	0	0		Tema II
#5	3	0	0	0	0		Tema II
#6	3	0	0	0	0	Cuestionarios y Lecciones	Tema II
#7	3	0	0	2	0		Tema III
#8	3	0	0	2	0		Tema III
#9	3	0	0	2	0	Cuestionarios y Lecciones	Tema III
#10	3	0	0	2	0		Tema IV
#11	3	0	0	2	0		Tema IV
#12	3	0	0	2	0	Cuestionarios y Lecciones	Tema IV
#13	3	0	0	2	0		Tema V
#14	3	0	0	2	0		Tema V
#15	3	0	0	2	0	Cuestionarios y Lecciones	Tema V
	41.4	0	0	18.6	0		