
Curso Académico: (2024 / 2025)**Fecha de revisión: 25-04-2024**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática**Coordinador/a: DIAZ SANCHEZ, DANIEL****Tipo: Optativa Créditos ECTS : 3.0****Curso : 1 Cuatrimestre : 2**

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Identificación y Autenticación
Protección de Datos

OBJETIVOS

Al finalizar la asignatura, el alumnado deben adquirir las siguientes competencias generales y específicas:

- Ser capaces de aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en sistemas móviles dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- 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.
- Analizar los riesgos de la introducción de dispositivos personales en un entorno profesional. Conocer y aplicar las medidas para controlar dichos riesgos y amenazas.
- Ser capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
- Ser capaces de 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.
- Ser capaces de elaborar concisa, clara y razonadamente reportes técnicos que contengan un modelo de riesgos y amenazas dado un escenario específico donde intervienen sistemas, terminales y/o comunicaciones móviles.
- Ser capaces de aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto.
- Poseer habilidades de auto-aprendizaje que les permitan continuar estudiando.

RESULTADOS DE APRENDIZAJE

Esta asignatura contribuye a los siguientes resultados de aprendizaje:

Diseñar estrategias de sensorización para distintos elementos de un sistema en red y analizar los eventos observados en un ataque concreto para distinguir cuáles son de interés.

Dado un sistema con unos requisitos de seguridad establecidos, proponer mecanismos y protocolos necesarios para proporcionar algunos de los servicios básicos de seguridad: autenticación, autorización, privacidad y control de acceso. Dar una medida de su eficacia y limitaciones.

Explicar la problemática de seguridad asociada a los dispositivos móviles personales en un entorno

profesional dado y aplicar las técnicas estudiadas a la ingeniería de sistemas seguros.

Evaluar la arquitectura de seguridad de un sistema vulnerable dado y proponer mejoras.

Conocer los principios de desarrollo y mantenimiento de sistemas seguros, incluyendo el desarrollo y adquisición de componentes software, durante todo su ciclo de vida

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Esta asignatura profundiza en aspectos de seguridad y mecanismos de protección contra ataques relacionados con sistemas y protocolos de comunicaciones de redes inalámbricas, tanto de alcance local como extendido, y dispositivos móviles. El programa de la asignatura es el siguiente:

1. Comunicaciones celulares
 - 1.1. Introducción a las comunicaciones celulares
 - 1.2. Seguridad en comunicaciones celulares
 - 1.3. Ataques conocidos a comunicaciones celulares
2. Comunicaciones inalámbricas
 - 2.1. Bluetooth
 - 2.2. Wireless LAN
3. Seguridad en convergencia VoLTE
4. Seguridad en plataformas móviles
 - 4.1. Diseño de seguridad en plataformas móviles
 - 4.2. Mobile Device Management (MDM)
 - 4.3. Malware para móviles y desarrollo de aplicaciones

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS

Clase teórica
Clases prácticas
Clases teórico prácticas
Prácticas de laboratorio
Tutorías
Trabajo en grupo

La metodología docente constará de las siguientes actividades formativas y tutorías:

- Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía complementaria al aprendizaje de los alumnos.
- Análisis y síntesis de lecturas recomendadas (p.ej., artículos de prensa, informes técnicos, artículos científicos, etc.) por parte de los profesores de la asignatura para afianzar y profundizar conceptos.
- Realización de prácticas: resolución de problemas, discusión de casos de estudio, prácticas en laboratorios informáticos con herramientas útiles para la simulación y despliegue de ataques y desarrollo de aplicaciones móviles.
- Elaboración y presentación de trabajos, tanto individuales como en grupo, por parte de los alumnos.
- Tutorías personalizadas de acuerdo con el horario fijado entre los profesores y los alumnos.

SISTEMA DE EVALUACIÓN

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

Para aprobar la asignatura SERÁ NECESARIO PRESENTARSE A TODAS LAS PRUEBAS de la evaluación continua; en alguna de las partes podría requerirse nota mínima. No concurrir a alguna de las pruebas supondrá la obtención de NO PRESENTADO en la calificación.

Peso porcentual del Examen Final: 40

Peso porcentual del resto de la evaluación: 60

El sistema de evaluación se basa en la realización de un examen escrito final, trabajos individuales y en grupo y la participación durante el curso. Concretamente, la evaluación continua de la asignatura se desglosa en:

1. Examen Final (40%)

2. Trabajos y participación (60%):

2.1. Realización de un trabajo, en grupo, sobre ataques en sistemas y comunicaciones móviles, incluyendo la preparación, presentación y defensa técnica del mismo (30%)

2.2. Trabajo guiado del laboratorio y participación (30%)

De forma similar se evaluará la asignatura en la convocatoria extraordinaria:

a) Si no se ha seguido el proceso de evaluación continua, se realizará un examen escrito (50% or 100%) y, a criterio del profesor se entregará un trabajo individual sobre ataques a sistemas móviles (50%).

b) En caso de haber seguido el proceso de evaluación continua, se realizará la parte de la evaluación continua no superada.

BIBLIOGRAFÍA BÁSICA

- Boudriga, Noureddine Security of Mobile Communications, Auerbach, 2010
- D. Forsberg, G. Horn, W.D. Moeller, V. Niemi LTE Security, John Wiley & Sons, 2012
- Dwivedi, Himanshu. Mobile application security., McGraw-Hill., 2010
- Neil Bergman; Mike Stanfield; Jason Rouse; Joel Scambray; Sarath Geethakumar; Swapnil Deshmukh; Scott Matsumoto; John Steven; Mike Price. Hacking Exposed Mobile Security Secrets & Solutions., McGraw-Hill., 2013

BIBLIOGRAFÍA COMPLEMENTARIA

- Lee Barken. How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN., Prentice Hall., 2003.
- Ollie Whitehouse; Shaun Colley; Tyrone Erasmus; Dominic Chell. The Mobile Application Hacker's Handbook., Chell. John Wiley & Sons., 2015