Seguridad en Sistemas y Comunicaciones Móviles

Curso Académico: (2018 / 2019) **Fecha de revisión: 06-11-2017**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: SEDANO JARILLO, FCO JAVIER

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

OBJETIVOS

Al finalizar la asignatura, los alumnos 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.

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. Introducción a los estándares de telefonía móvil activos
1.1. Protección de datos
1.2. Esquema interno del operador
1.3. Seguridad en redes de datos móviles y posicionamiento

2. Seguridad en comunicaciones inalámbricas
2.1. Seguridad en comunicaciones de bajo alcance
2.2. VoIP

3. Ataques conocidos a redes de telefonía/datos móviles
3.1. Ataques a tarjetas y replicación de tarjetas
3.2. Ataques al canal radio

4. Sistemas operativos móviles
4.1. Protección de los recursos
4.2. Protección contra ingeniería social

5. Seguridad en smartphones
5.1. Sistemas de gestión de dispositivos móviles
5.2. Aplicaciones maliciosas y desarrollo seguro

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

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

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 (40%)

2.2. Trabajo guiado del laboratorio y participación (20%)

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%) y 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