Seguridad en dispositivos móviles

Curso Académico: (2019 / 2020) **Fecha de revisión: 22-04-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: FUENTES GARCIA ROMERO DE TEJADA, JOSE MARIA DE

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 4 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Criptografia y Seguridad Informática
Redes de Ordenadores
Ingeniería de la Seguridad

OBJETIVOS

Las características diferenciadoras de los dispositivos móviles: su tamaño (usualmente reducido y con importantes limitaciones en cuanto a energía y recursos computacionales) y el uso casi obligatorio de un canal inalámbrico de comunicaciones, hacen que gran parte de los mecanismos de seguridad tradicionales no les sean aplicables, y que otros (e.g. la seguridad física o técnicas poco exigentes de recursos) adquieran una especial relevancia.

En consecuencia, el objetivo de esta asignatura es que el alumno domine las herramientas técnicas específicas que son necesarias para garantizar la seguridad en un entorno de computación móvil.

Para lograr este objetivo, el alumno debe adquirir una serie de conocimientos, capacidades y actitudes. (PO: a, b, c, d, e, f, g, h, j, k)

Por lo que se refiere a los conocimientos, al finalizar el curso el estudiante será capaz de:
- Entender los riesgos de seguridad propios de un entorno móvil. (PO: b, e, j)
- Conocer las medidas de seguridad física aplicables a dispositivos móviles. (PO: b, e, j)
- Dominar las técnicas fundamentales de protección de la información almacenada en dispositivos móviles. (PO: a, b, c, e, f, j, k)
- Dominar los principales protocolos de seguridad existentes para comunicaciones móviles y su espectro de aplicación. (PO: a, e)

Por lo que atañe a las capacidades, el alumno será capaz de:
- Analizar las vulnerabilidades existentes en un entorno de computación móvil. (PO: b, e, j, k)
- Diseñar, en su caso, y aplicar los mecanismos de protección apropiados para garantizar el nivel de seguridad deseado. (PO: a, b, c, d, e, j, k)

En cuanto a las actitudes el alumno tras cursar la asignatura debería tener:
- Una actitud suspicaz respecto de la seguridad de los dispositivos móviles y las comunicaciones entre ellos. (PO: e, g, h, j)
- Una actitud indagadora para hallar nuevas vulnerabilidades y amenazas en los entornos abiertos en los que se mueven estos dispositivos. (PO: e, j, k)
- Una actitud analítica que le permita, a partir de las limitaciones propias del entorno y/o los dispositivos, identificar las soluciones aplicables. (PO: e, h, j, k)

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

El programa se divide en cinco grandes bloques:

1. Introducción a la seguridad de las redes inalámbricas
1.1. Medidas y mecanismos de seguridad en dispositivos móviles
1.2. Tipos de Redes en las comunicaciones inalámbricas.
1.3. Primitivas fundamentales en la provisión de servicios de seguridad de la información: confidencialidad, integridad, autenticación, no repudio, etc.
1.4. Objetivos de la seguridad en las comunicaciones inalámbricas.
1.5. Vulnerabilidades, riesgos, amenazas en las comunicaciones inalámbricas.

2. Medidas y Mecanismos de seguridad en los dispositivos móviles
2.1. Medidas técnicas de seguridad en los sistemas Android e iOS
2.1.1. Identificación
2.1.2. Autenticación
2.1.3. Control de acceso
2.1.4. Confidencialidad
2.1.5. No repudio
2.1.6. Trazabilidad
2.2. Mecanismos de seguridad en los sistemas Android e iOS
2.2.1. Aislamiento de procesos (Sandboxing)
2.2.2. Control de acceso basado en credenciales
2.2.3. Procedencia de las aplicaciones
2.2.4. Confidencialidad
2.2.5. Kill switch
2.2.6. Borrado remoto y localización
2.2.7. Copias de seguridad (Backups)
2.2.8. Actualizaciones

3. Seguridad en Redes de Area Local Inalámbrica (WLAN)
3.1. Fundamentos de la Seguridad de redes WLAN: Autenticación, Integridad, Manejo de Claves, Cifrado, Ataques
3.2. Wired Equivalent Privacy (WEP)
3.3. Wi-Fi Protected Access (WPA - WPA2)
3.4. Extensible Authentication Protocol (EAP)
3.4.1. Tecnología IEEE 802.1x
4. Seguridad en las comunicaciones móviles
4.1. GSM
4.2. GPRS - EDGE
4.3. UMTS, LTE
4.4. 5G
5. Seguridad de sistemas basados en dispositivos de identificación por radiofrecuencia (RFID) en las comunicaciones móviles
5.1. Mecanismos específicos para dispositivos de escasa potencia de cómputo
5.1.1. Autenticación
5.1.2. Confidencialidad
5.1.3. Cifrado

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

La metodología docente incluirá:
(1) Clases magistrales, donde se presentarán los conocimientos que los alumnos deben adquirir. Para facilitar su desarrollo los alumnos recibirán las notas de clase y diversos documentos en la herramienta web oportuna y tendrán textos básicos de referencia que les permita completar y profundizar en aquellos temas en los cuales estén más interesados (P.O: a, e, j, k)
(2) Trabajo práctico con escenarios reales. Los alumnos deberán diseñar e implementar una solución que cumpla las especificaciones iniciales. (P.O: a, b, c, d, e, g, j, k)
(3) Análisis crítico de un artículo de investigación o tecnología relacionada con la seguridad. Memoria y, eventualmente, presentación oral por parte de los alumnos (P.O: a, d, f, g, h, i, j).

SISTEMA DE EVALUACIÓN

1. CONVOCATORIA ORDINARIA
1.1. EVALUACIÓN CONTINUA
La evaluación se basará en los siguientes criterios:
- Resolución de un caso práctico a lo largo del curso (obligatorio): 40% (P.O: a, b, c, d, e, f, g, j, k).
- Presentación de un trabajo teórico/práctico sobre un tema específico (obligatorio): 20% (P.O: a, d, f, g, h, i, j).
- Examen final (obligatorio): 40% (P.O: a, b, c, e, f, g, h, j).
Se podrá valorar la asistencia y participación activa en clase para obtener puntuación adicional.

Para aprobar la asignatura se deben satisfacer dos condiciones:
- Obtener en el examen final una calificación igual o superior a 4 puntos sobre 10.
- Lograr, como suma de todas las partes, al menos el 50% de la máxima puntuación posible.
1.2. EVALUACIÓN NO CONTINUA
Esta alternativa se aplica si no se entrega alguno de los trabajos planteados.
La evaluación se basará en los siguientes criterios:
- Examen final: 60% (P.O: a, b, c, e, f, g, h,i, j, k).
Dicho examen final incluirá pruebas específicas para comprobar el conocimiento que debe haberse

adquirido mediante la realización de los trabajos planteados.
Para aprobar la asignatura se debe satisfacer:
- Lograr al menos 5.0 puntos sobre 10.

CONVOCATORIA EXTRAORDINARIA
2.1. SI EL ESTUDIANTE SIGUIÓ EVALUACIÓN CONTINUA EN LA CONV. ORDINARIA
La evaluación se basará en los siguientes criterios:
- Se mantiene la nota obtenida en la evaluación continua en relación a los trabajos (60%)
- Examen final (obligatorio): 40% (P.O: a, b, c, e, f, g, h, j).

Para aprobar la asignatura se deben satisfacer dos condiciones:
- Obtener en el examen final una calificación igual o superior a 4 puntos sobre 10.
- Lograr, como suma de todas las partes, al menos el 50% de la máxima puntuación posible.

2.2. EVALUACIÓN NO CONTINUA
Esta alternativa se aplica si no se entregó alguno de los trabajos planteados.
La evaluación se basará en los siguientes criterios:
- Examen final: 100% (P.O: a, b, c, e, f, g, h,i, j, k).
Dicho examen final incluirá pruebas específicas para comprobar el conocimiento que debe haberse adquirido mediante la realización de los trabajos planteados.
Para aprobar la asignatura se debe satisfacer:
- Lograr al menos 5.0 puntos sobre 10.

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

BIBLIOGRAFÍA BÁSICA

- Frank Thornton, Chris Lanthem. RFID Security., Syngress (July 7, 2005).
- Matthew Gast 802.11 Wireless Networks The Definitive Guide. , O'Reilly, 2005
- Noureddine Boudriga. Security of Mobile Communications., Auerbach Publications., 2009
- Praphul Chandra Bulletproof wireless security, Newnes, 2005

BIBLIOGRAFÍA COMPLEMENTARIA

- Jeff Six Application Security for the Android Platform, O'Really Media, Inc, 2011
- Johnny Cache, Joshua Wright, Vincent Liu. Hacking wireless exposed: wireless security secrets and solutions., McGraw-Hill, 2010
- Pragati Ogal Rai Android Application Security Essentials, Packt Publishing, 2013