Técnicas de ocultación de la información

Curso Académico: (2020 / 2021) **Fecha de revisión: 28-01-2021**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: CAMARA NUÑEZ, MARIA CARMEN

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 3 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Haber superado las materias de Matemáticas, Estadística e Informática del Módulo I (Formación básica) y la materia (asignatura) de Estadística (Investigación Operativa) del Módulo III (Fundamentos de ingeniería).

OBJETIVOS

Las competencias que se pretende que adquiera el estudiante son las siguientes:
- Identificar los objetivos de seguridad y las vulnerabilidades, amenazas y riesgos de un sistema de información dado en un entorno operacional definido. Analizar las posibles medidas de seguridad a emplear en el mismo.
- Evaluar los servicios de seguridad a implementar en un sistema dado y diseñar y aplicar los mecanismos y protocolos consiguientes.
- Evaluar para un sistema dado las herramientas existentes de cifrado y esteganográficas para protegerlo.
- Usar los sistemas de firma y certificación en un entorno concreto. Evaluar y aplicar los mecanismos de autenticación pertinentes para acceder a un sistema específico.
- Diseñar un plan de seguridad, desarrollando las distintas partes del mismo, evaluando su cumplimiento a lo largo del tiempo y corrigiendo sus desviaciones. Analizar y gestionar los riesgos de una instalación determinada.
- Elaborar un plan de recuperación integral de una instalación real. Realizar una auditoría de cumplimiento de los ficheros y sistemas conteniendo datos de carácter personal.
- Usar los instrumentos que permiten el control de los sistemas operativos, principalmente Windows y Linux.
- Manejar las principales técnicas de recopilación, identificación y análisis de sucesos, garantizando el aseguramiento de las pruebas y preservando la cadena de custodia de las mismas. Evaluar y manejar los sistemas de borrado seguro y de recuperación de datos.
- Implementar bases de datos sobre un sistema gestor. Evaluar y emplear las diferentes técnicas que integran la minería de datos: técnicas de análisis y extracción de modelos.

Para ello es preciso conseguir los resultados del aprendizaje que se resumen a continuación:
OBJETIVOS
El estudiante debe reconocer la importancia actual de las técnicas de ocultación de la información, en particular la criptografía y la esteganografía, así como las tecnologías que permiten su tratamiento, los puntos débiles de éstas y las amenazas que sufren. Con objeto de alcanzar estos objetivos, el alumno debe adquirir una serie de conocimientos, capacidades y actitudes que se detallan a continuación.

CONOCIMIENTOS
Al finalizar el curso el estudiante debe ser capaz de:
- Conocer los sistemas criptográficos y esteganográficos clásicos y los motivos de su inseguridad.
- Conocer los fundamentos matemáticos de la criptografía y la esteganografía modernas, así como de las técnicas para analizar su seguridad: criptoanálisis y estegoanálisis, respectivamente.
- Dominar los principales criptosistemas y los algoritmos de cifrado actuales más característicos.
- Conocer los sistemas de firma y verificación basados en clave pública
- Conocer los problemas asociados a la gestión de claves y sus diversas soluciones.

CAPACIDADES

Por lo que atañe a las capacidades, se pueden desglosar en específicas y genéricas (destrezas).

En cuanto a las capacidades específicas, el alumno será capaz de:

- Resolver problemas de la teoría de números en su aplicación a la criptografía. (P.O.: a)
- Reconocer las ventajas, inconvenientes y usos de los sistemas de clave secreta y pública. (P.O.: a, c)
- Firmar y verificar en distintos entornos, detectando posibles ataques (P.O.: a, c)
- Identificar métodos para ocultar información en distintos medios (P.O.: a, c)

En cuanto a las capacidades generales o destrezas, durante el curso se trabajarán:

- La capacidad para encontrar y seleccionar las informaciones relevantes para solucionar un problema concreto. (P.O.: a, b)
- La capacidad para aplicar conocimientos multidisciplinares a la resolución de un determinado problema. (P.O.: a, c, e, g)
- La capacidad para investigar un criptosistema o esteganosistema particular en un entorno concreto y hallar sus vulnerabilidades y amenazas. (P.O.: a, b)

En cuanto a las actitudes el alumno tras cursar el curso debería tener:

- Una actitud crítica respecto de la seguridad que ofrece un sistema de cifrado o de ocultación de información en particular, en un entorno dado y unos riesgos determinados. (P.O.: i)
- Una actitud recelosa respecto de la seguridad supuesta a los sistemas de ocultación de la información implementados en los sistemas. (P.O.: i)

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Conceptos de Seguridad de la Información
   1.1. Objetivos de la Seguridad de la Información
   1.2. Vulnerabilidades, Riesgos y Ataques
   1.3. Medidas y Mecanismos de Seguridad
   1.4. Criptología
   1.5. Canales Seguros

2. Fundamentos Matemáticos y de Teoría de la Información
   2.1. Sistemas de Numeración
   2.2. Operaciones Lógicas con Variables Binarias
   2.3. Teoría de la Información
   2.4. Aritmética Modular

3. Criptosistemas Clásicos
   3.1. Cifrado Monoalfabético
   3.2. Cifrado Polialfabético
   3.3. Cifrado Poligráfico
   3.4. Cifrado de Transposición
   3.5. Máquinas de Rotores

4. Criptosistemas Simétricos: Cifrado en Flujo
   4.1. Secreto Perfecto: Cifrador de Vernam (OTP)
   4.2. Generadores de Secuencias Pseudoaleatorias
   4.3. Generadores Lineales: LFSRs
   4.4. El Cifrador A5/1
   4.5. El Cifrador RC4

5. Criptosistemas Simétricos: Cifrado en Bloque
   5.1. Redes de Feistel
   5.2. Redes de Sustitución-Permutación
   5.3. El Cifrador AES
   5.4. Modos de Operación

6. Funciones Hash y MAC
   6.1. Funciones Hash Criptográficas
   6.2. Construcción Merkle-Daamgard
   6.3. Construcciones basadas en Cifradores de Bloque
   6.4. La Familia SHA
   6.5. Códigos de Autenticación de Mensajes (MAC)

7. Criptosistemas Asimétricos
7.1. Protocolo de Establecimiento de Claves Diffie-Hellman
7.2. Algoritmos Criptográficos Asimétricos y Firma Digital
7.3. RSA
7.4. Otros Criptosistemas Asimétricos

8. Esteganografía
8.1. Sistemas Esteganográficos Clásicos
8.2. Esteganografía Moderna
8.3. Esteganografía en Imágenes
8.4. Esteganografía en Otros Medios Digitales
8.5. Estegoanálisis

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

La metodología docente incluirá:

(1) Clases magistrales (2,5 ECTS). Los profesores presentarán un resumen de los conocimientos que los alumnos deben adquirir y se espera que el alumno participe activamente durante la clase. Para facilitar su desarrollo los alumnos recibirán el material básico de la asignatura (las notas de clase, las referencias a los textos bibliográficos básicos y el material complementario) en la herramienta web oportuna. Los alumnos leerán y estudiarán este material (trabajo del alumno). (P.O.: a, c, g, i)

(2) Problemas (2,5 ECTS). El alumno, guiado por el profesor durante las clases de problemas, resolverá ejercicios que le servirán para aplicar los conocimientos adquiridos. Los alumnos resolverán problemas adicionales fuera del tiempo de clase (trabajo del alumno). (P.O.: a, c, g, i)

(3) Prácticas (1,0 ECTS) en laboratorio / aula informática. El alumno aprenderá el uso de las principales herramientas criptográficas y esteganográficas. Se publicarán las instrucciones de las prácticas para que el alumno las realice. Se ofrecerán sesiones en las que el profesor dará soporte a los alumnos en la realización de las prácticas. Los alumnos completarán las tareas solicitadas en cada práctica fuera del tiempo de clase (trabajo del alumno). (P.O.: a, b, c, e, g, i)

Debido a la incertidumbre sobre el formato docente al que las circunstancias sanitarias nos avocarán durante el próximo curso, se prevé el inicio del mismo en la modalidad semipresencial, pudiendo derivar hacia la formación 100% presencial o 100% on-line según evolucione la propagación o el control sobre la pandemia y las normas higiénico-sanitarias que dicten las Autoridades del sector.

SISTEMA DE EVALUACIÓN

Peso porcentual del Examen Final:	55
Peso porcentual del resto de la evaluación:	45

El sistema de evaluación incluye la evaluación continua del trabajo del alumno (pruebas de evaluación de habilidades y conocimientos teórico-prácticos e informes de prácticas de laboratorio) y la evaluación final a través de un examen escrito en que se evaluará de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso. La evaluación de la asignatura se realizará de acuerdo con los siguientes criterios:

1. Exámenes escritos de teoría y problemas: 70% de la nota final
   1.1. Exámenes de evaluación continua: 15% de la nota final. Aproximadamente a mediados del cuatrimestre.
   1.2. Examen escrito final de teoría y problemas: 55% de la nota final. Para superar la asignatura el alumno debe obtener un mínimo de puntos en este examen.
2. Entrega de resultados de las prácticas en aulas informáticas: 30% de la nota final

En la convocatoria extraordinaria, el alumno elegirá entre:
a) Un examen final escrito por valor del 100% de la nota, compuesto de teoría, problemas y conocimientos adquiridos en las sesiones de laboratorio; o
b) Un examen final escrito por valor del 55% de la nota, compuesto de teoría y problemas. El restante 60% provendrá de la nota obtenida durante el curso en el examen de evaluación continua (15%) y las prácticas (30%)

BIBLIOGRAFÍA BÁSICA

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone Handbook of Applied Cryptography, CRC Press, 1996

- Juan Tapiador, Pedro Peris López Criptografía y Ocultación de la Información, Centro Universitario de la Guardia Civil, 2015

RECURSOS ELECTRÓNICOS BÁSICOS

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone . Handbook of Applied Cryptography: http://cacr.uwaterloo.ca/hac/