Fundamentos de seguridad en comunicaciones

Curso Académico: (2022 / 2023) **Fecha de revisión: 20-06-2022**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: MUÑOZ ORGANERO, MARIO

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 4 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Para cursar esta materia es necesario poseer conceptos de redes y protocolos de comunicaciones. En particular se recomienda haber superado las asignaturas de:

- Redes y servicios de comunicaciones

- Aplicaciones Telemáticas

También se necesitan conocimientos básicos de probabilidad y de estructuras algebraicas por lo que se recomiendan conocimientos de:

- Estadística

OBJETIVOS

Resumen: Conocer, saber analizar y diseñar y saber aplicar a la resolución de problemas concretos, las principales técnicas criptográficas, así como sus aplicaciones a sistemas de seguridad en redes y servicios telemáticos. El alumno debe familiarizarse con las técnicas de cifrado simétrico y asimétrico, funciones hash, checksums criptográficos, firmas y certificados digitales, protocolos de autentificación y las aplicaciones combinadas de los mismos.

Detalle en cuanto a conocimientos:
- Conocer el entorno genérico del criptosistema junto con los diferentes agentes que lo conforman.
- Conocer la evolución de los diferentes mecanismos de seguridad clásicos como sustento de los mecanismos de seguridad modernos.
- Conocer las técnicas de cifrado convencional (cifrado simétrico) así como el estándar de cifrado actual (AES) y el estándar anterior (DES).
- Conocer los principales modos de operación usados en el cifrado simétrico.
- Conocer las bases matemáticas de los principales mecanismos de cifrado de clave pública. Conocer en profundidad el algoritmo RSA.
- Conocer las diferentes técnicas de hash y su utilización conjunta con los algoritmos de clave pública para crear firmas digitales y certificados digitales (PKI).
- Conocer las diferentes técnicas de distribución de claves de sesión, tanto basadas en clave pública como basadas en clave secreta.
- Conocer la utilización conjunta de los diferentes mecanismos estudiando diferentes protocolos de seguridad (IPSec, SSL, etc.)

Detalle en cuanto a análisis, diseño y resolución de problemas:
- Capacidad de utilizar la definición de criptosistema como marco de comparación de los diferentes mecanismos de seguridad para analizar sistemas y redes de comunicaiones.
- Capacidad de utilizar los criterios adquiridos para evaluar la seguridad de un determinado protocolo.
- Capacidad de análisis y de saber elegir con criterio el algoritmo de seguridad más adecuado en cada circunstancia y en función de unos determinados requisitos.
- Saber definir un protocolo de seguridad para la resolución de un determinado escenario y proporicionando unos servicios de seguridad.
- Saber utilizar herramientas de seguridad que permitan aplicar los diferentes mecanismos estudiados.
- Ser capaz de resolver en pareja una serie de retos criptográficos como la ruptura de

contraseñas, determinar a partir de mensajes cifrados cómo se han cifrado y ciertos parámetros de los algoritmos asi como generar certificados y firmar digitalmente información.
- Ser capaz de entender las recomendaciones sobre estándares criptográficos.
- Capacidades básicas de criptoanalizar sistemas

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Este es un curso básico de introducción a la seguridad en las comunicaciones en el que se estudian las tecnologías básicas que permiten proporcionar diferentes servicios de seguridad a la información que se transmite.

El programa se divide en cuatro partes:

1. Introducción a la seguridad.
1.1. Qué es la seguridad.
1.2 Mecanismos de seguridad.
1.3 Servicios de seguridad.
1.4 Teoría de la Información

2. Criptografía simétrica
2.1 Algoritmos de cifrado clásicos.
2.2 Algoritmos de cifrado simétrico.
2.3 DES. TDES. AES.
2.4 Modos de operación.
2.5 Mecanismos de distribución de claves.

3. Criptografía asimétrica
3.1 Algoritmos de cifrado asimétrico.
3.2 Firmas digitales.
3.3 Certificados digitales (identidad y atributos).

4. Aplicaciones
4.1 IPsec (seguridad a nivel de red)
4.2 SSL/TLS (seguridad sobre TCP)

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

La actividades formativas incluyen:

- Clases magistrales, clases de problemas y de resolución de dudas en grupos reducidos, presentaciones de los alumnos, tutorías individuales y trabajo personal del alumno, incluyendo estudio, pruebas y exámenes; orientados a la adquisición de conocimientos teóricos.
- Prácticas de laboratorio y clases de problemas en grupos reducidos, tutorías individuales y trabajo personal del alumno, incluyendo estudio, pruebas y exámenes; orientados a la adquisición de habilidades prácticas relacionadas con el programa de cada materia.

SISTEMA DE EVALUACIÓN

El sistema de evaluación se ha mejorado para poner en valor todo el esfuerzo realizado por parte del alumno.

El sistema de evaluación incluye la evaluación continua del trabajo del alumno (trabajos, informes de prácticas de laboratorio, participación en clase y pruebas de evaluación de habilidades y conocimientos teórico-prácticos) y la evaluación final a través de un examen escrito final en que se evaluará de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso.

En concreto:

- Evaluación continua (45%):
+ Entrega de 4 laboratorios realizados en parejas sobre los diferentes aspectos de la asignatura (30%)
+ 2 pruebas de evaluación continua (15%) que facilitarán el estudio de los contenidos parciales de la asignatura y pretenden motivar la realización de los ejercicios de clase

- Examen final (55%)

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

BIBLIOGRAFÍA BÁSICA

- A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone Handbook of Applied Cryptography, CRC Press, August 2001
- Mike Speciner; Radia Perlman; Charlie Kaufman Network Security: Private Communication in a Public World, Prentice Hall, 2002
- William Stallings Cryptography and network security . Principles and Practice, Pearson Education M.U.A., 2014

BIBLIOGRAFÍA COMPLEMENTARIA

- MCNAB, CHRIS SEGURIDAD DE REDES. SEGUNDA EDICIÓN, ANAYA MULTIMEDIA, 2008

RECURSOS ELECTRÓNICOS BÁSICOS

- Jorge Ramió . Libro Electrónico de Seguridad Informática y Criptografía: http://www.criptored.upm.es/guiateoria/gt_m001a.htm