UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

GUÍA DOCENTE *CURSO: 2015/16*

14116 - PROTOCOLOS Y SERVICIOS

ASIGNATURA: *14116 - PROTOCOLOS Y SERVICIOS*
CENTRO: *Escuela de Ingeniería de Telecomunicación y Electrónica*
TITULACIÓN: *Ingeniero de Telecomunicación*
DEPARTAMENTO: *INGENIERÍA TELEMÁTICA*
ÁREA: *Ingeniería Telemática*
PLAN: *13 - Año 200* **ESPECIALIDAD:**
CURSO: *Quinto curso* **IMPARTIDA:** *Primer semestre* **TIPO:** *Troncal*
CRÉDITOS: *6* **TEÓRICOS:** *3* **PRÁCTICOS:** *3*

Información ECTS

Créditos ECTS: 6

Horas presenciales: 6 horas

Horas no presenciales: 120 horas

Idioma en que se imparte: Español

Descriptores B.O.E.

Planificación y gestión de redes y servicios. Normalización y política de telecomunicaciones. Codificación y cifrado de información.

Temario

PROGRAMA TEÓRICO:
Tema 1. Presentación de la asignatura (0.5 horas)
- 1.1. Proyecto docente.
- 1.3. Introducción los bloques temáticos
- 1.2. Herramientas utilizadas
- 1.3. Creación de grupos de trabajo

Tema 2. Gestión de red (0.5 horas)
- 2.1. Conceptos de gestión de red
- 2.2. ASN.1
- 2.3. SMI y MIB II
- 2.2. SNMP
- 2.4. CMIP y TMN

Tema 3: Seguridad de Red (1 hora)
- 2.1. Conceptos de seguridad
- 2.2. Algoritmos y protocolos
- 2.3. Seguridad en Internet

Tema 4: Política de Telecomunicaciones (1 hora)
3.1. Política de Telecomunicaciones en Europa
3.2. Proceso de la Liberalización de las Telecomunicaciones
3.3. Política de Telecomunicaciones en España

Requisitos Previos

Ninguno

Objetivos

1.Objetivos conceptuales:
1.1.Introducir conceptos, herramientas y procedimientos utilizados en la asignatura.
1.2.Conocer los conceptos básicos de la gestión de red.
1.3.Conocer y comprender diversas herramientas para gestionar la MIB.
1.4.Saber y conocer el protocolo de gestión de red SNMP.
1.5.Saber y comprender los aspectos matemáticos básicos asociados a la criptografía.
1.6.Conocer los principales algoritmos de cifrado por sustitución.
1.7.Saber y comprender los principales cifradores clásicos existentes.
1.8.Conocer y analizar el cifrado simétrico y asimétrico.
1.9.Conocer y comprender los aspectos principales de la firma digital y la gestión de claves.
1.10.Conocer la política de las telecomunicaciones en Europa.
1.11.Analizar el proceso de liberalización de las Telecomunicaciones en España.
1.12.Conocer la política de las telecomunicaciones en España.

2.Objetivos procedimentales:
2.1.Experimentar con las herramientas de laboratorio.
2.2.Manejar y elaborar diferentes configuraciones del servidor SNMP.
2.3.Utilizar aplicaciones gráficas para gestionar la MIB.
2.4.Ejecutar aplicaciones de consola para comunicación entre cliente y servidor SNMP.
2.5.Aplicar los conceptos matemáticos básicos asociados con la criptografía y manejar aplicaciones que permiten realizar estos cálculos.
2.6.Manejar los principales algoritmos de sustitución y ejecutar aplicaciones que permiten aplicar estos algoritmos.
2.7.Utilizar los principales cifradores clásicos y probar aplicaciones que los usan.
2.8.Manejar algoritmos de cifrado simétrico y asimétrico y ejecutar aplicaciones que permiten aplicar estos algoritmos.
2.9.Ejecutar aplicaciones que permiten la firma digital y la gestión de claves.
2.10.Aplicar las leyes de Telecomunicación a diferentes supuestos.

3.Objetivos actitudinales
3.1.Interesarse por los objetivos que se quieren cubrir.
3.2.Valorar la importancia de una buena gestión de red.
3.3.Apreciar que la seguridad es fundamental en la Sociedad de la Información.
3.4.Respectar el marco legal por el que se rigen las Telecomunicaciones.

Metodología

La disposición Transitoria Cuarta del Reglamento de Planificación Académica de la ULPGC establece que las asignaturas de los títulos no adaptados tendrán el segundo año de su extinción una carga docente del 10% de las horas contempladas en el plan de estudios para la realización de actividades de docencia y evaluación.

Puesto que el curso 2014-2015 es el segundo año de extinción de ésta asignatura de 3 créditos de teoría y 3 de prácticas, se impartirán 6 horas distribuidas como sigue:

a) 3 horas de tutoría presencial de la parte de teoría durante las cuales se facilitará a los alumnos el seguimiento secuencial de la asignatura resolviendo
dudas y proponiendo temas y ejercicios para la siguiente sesión.

b) 1 hora de tutoría presencial de la parte práctica durante las cuales se facilitará a los alumnos que lo deseen el seguimiento de la parte de laboratorio de la
asignatura.

c) 2 horas de evaluación.

Las tutorias presenciales tanto de la parte de teoría como de la parte práctica se llevarán a cabo en el Laboratorio de RDSI y Área Extensa. Se realizarán tres sesiones para cada parte (teoría y práctica). El horario y el lugar de las actividades se publicará durante la primera quincena del semestre en el campus virtual.

Criterios de Evaluación

La evaluación de la asignatura se realiza mediante exámenes en fechas de convocatorias oficiales.

Para la valoración de la parte teórica, se realizará un examen escrito que representará el 70% de la puntuación de la asignatura. Para la valoración de las prácticas, se realizará un examen práctico en el laboratorio que tendrá un peso del 30% en la nota final de la asignatura.

Descripción de las Prácticas

Las prácticas serán realizadas en el Laboratorio de Redes de Área Local, Extensa y RDSI del Departamento de Ingeniería Telemática.

Práctica 1: Gestión de Red con SNMP

1.1 Introducción a SNMP.
En esta práctica se pretende dar una visión general sobre la gestión de red con SNMP. Para ello, vamos a tomar el primer contacto con el entorno de trabajo y con el agente SNMP. En este último caso, veremos algunos aspectos básicos de su configuración así como la manera que tenemos para interactuar con él.

1.2 Cómo configurar y usar SNMP.
En esta práctica se pretende profundizar en la configuración del agente SNMP. También, profundizaremos en la manera que tenemos para interactuar con él incluyendo la posibilidad de modificar valores de la MIB.

1.3 Cliente y servidor SNMP.
En esta práctica se aplicar las opciones no vistan aún en la configuración del agente SNMP. También, profundizaremos en la manera que tenemos para interactuar con él desde otros ordenadores de la red.

1.4 Traps y MIB Browser.
En esta práctica vamos a configurar el agente SNMP para permitir el envío y recepción de traps (notificaciones).

Práctica 2: Seguridad en Redes

2.1 Fundamentos Teóricos de la criptografía
Esta práctica tiene como objetivo comprobar la entropía de los mensajes y de las claves, así como estudiar y comprobar el comportamiento característico del lenguaje y su redundancia, aspectos que permitirán el criptoanálisis de sistemas de cifra clásicos.

2.2 Cifradores por sustitución monográfica monoalfabeto
En esta práctica veremos los cifradores por sustitución monográmica monoalfabeto donde el cifrado se realiza mediante un algoritmo que hace corresponder una letra del texto en claro a una única letra del criptograma, es decir, cifra monogramas.

2.3 Cifra por sustitución polialfabética monográfica
En esta práctica utilizaremos los algoritmos de sustitución polialfabética que tienen por objeto producir una distribución plana de la frecuencia relativa de los caracteres en el criptograma. Para ello utilizan sustituciones múltiples de forma que en un texto largo se combinan las altas frecuencias de algunos caracteres con otros de menor frecuencia. La técnica anterior consiste en aplicar dos o más alfabetos de cifrado de forma que cada uno de ellos sirva para cifrar los caracteres del texto en claro, dependiendo de la posición
relativa de éstos en dicho texto.

2.4 Cifradores clásicos
En esta práctica veremos otro método clásico utilizado para cifrar mensajes: la transposición o permutación de caracteres. Esto consiste en reordenar los caracteres del texto. El resultado de tal acción es la de difuminar la información del texto en claro y provocar, por tanto, la difusión propuesta por Shannon para la protección de la misma.

2.5 Cifrado asimétrico por bloques y asimétrico
Este tipo de cifradores utiliza una única clave que debe guardarse en secreto ya que en ella reside la seguridad de los mismos. Por esta razón se les denomina también simétricos puesto que usan la misma clave para cifrar en emisión y descifrar en recepción. Los cifradores de exponenciación que usan el problema matemático de la factorización de números grandes basan su seguridad en que, para el propietario del par de claves asimétricas es fácil deducir la clave privada de la clave pública.

2.6 Funciones resumen y gestión de claves
Las funciones hash, tienen su principal aplicación en los sistemas de cifra actuales generalmente bajo dos términos: como parte principal de algoritmos de autenticación o como funciones resumen para reducir el tamaño de un bloque de texto en claro a un valor constante de sólo unas centenas de bits y con ello permitir la firma digital.

Bibliografía

[1 Básico] Computer networks /
Andrew S. Tanenbaum.
Prentice Hall,, Englewood Cliffs (New Jersey) : (2003) - (4th. ed.)
0130384887

[2 Básico] Applied cryptography: protocols,algorithms and source code in C.
Schneier, Bruce
John Wiley & Sons,, Chichester : (1996) - (2nd. ed.)
0471117099

[3 Básico] Política de Telecomunicaciones en la Unión Europea.

Ministerio de Obras Públicas, Transportes y Medio Ambiente,, Madrid : (1995)
844980146X

[4 Recomendado] Handbook of applied cryptography /

Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.
CRC,, Boca Ratón [etc.] : (1996)
0-8493-8523-7

[5 Recomendado] Protocolos criptográficos y seguridad en redes /

Jaime Gutiérrez, Juan Tena, (eds).
Servicio de Publicaciones de la Universidad de Cantabria,, Santander : (2003)
84-8102-345-0

[6 Recomendado] Normalización y política de las telecomunicaciones /

José Andrés
Vázquez Travieso ; Gustavo Rodríguez Rodríguez, dir.
Escuela Universitaria de Ingeniería
Técnica de Telecomunicación,, Las Palmas de Gran Canaria : (2000)

[7 Recomendado] Gestión de red, SNMP /

José María Quinteiro González ; Gustavo Rodríguez Rodríguez.
Universidad de Las Palmas de Gran Canaria,, Las Palmas de Gran Canaria : (1997)

[8 Recomendado] SNMP, SNMPv2, and CMIP: the practical guide to network management standards /

William Stallings.
Addison-Wesley,, Reading, Mass. : (1993)
0201633310

Equipo Docente

JUAN DOMINGO SANDOVAL GONZÁLEZ *(COORDINADOR)*
Categoría: TITULAR DE UNIVERSIDAD
Departamento: INGENIERÍA TELEMÁTICA
Teléfono: 928451235 **Correo Electrónico:** juandomingo.sandoval@ulpgc.es

Resumen en Inglés

DESCRIPTOR:
Network Management. Applied Criptography. Telcommunications Policies.

GOALS
- Study Network Management.
- Apply Criptography Algorithm.
- Analyze Telcommunications Policies in Europe Specially Spanish Policies.

METHODOLOGY
- The instructor presents in class the main concepts
- The instructor proposes exercises that help the students to understand the concepts presented in class
- In the laboratory the students will program complementary exercies
- The electronic documents containing complementary material will be available in the Campus

Virtual server of the ULPGC.