Programa Oficial de Asignatura

Seguridad en Redes y Criptografía

Ficha Técnica

Titulación:	Grado en Ingeniería Informática		
Plan BOE:	BOE número 98 de 24 de abril de 2013		
Asignatura:	Seguridad en Redes y Criptografía		
Módulo:	Redes Telemáticas y Sistemas Operativos		
Curso:	3º	**Créditos ECTS:**	6
Tipo de asignatura:	Obligatoria	**Tipo de formación:**	Teórica y Práctica

Presentación

La masiva utilización de las tecnologías de la información cuestiona la confianza y seguridad de los sistemas y productos informáticos en una sociedad que depende cada vez más de ellos.

Ante esta situación, se hace imprescindible emplear todo un conjunto de técnicas, heurísticas y tecnologías para garantizar la seguridad de los sistemas informáticos, así como para lograr la construcción de la confianza tanto en los sistemas de información como en las posibles interacciones de los mismos.

En esta asignatura se estudian los métodos y técnicas de criptografía y securización de redes y de sistemas informáticos. Dada su especial importancia en la sociedad de la información actual, se cubren en este módulo los conceptos, técnicas y algoritmos de la seguridad en las comunicaciones, y se estudian las principales amenazas software existentes, así como las formas de prevenir y recuperar los sistemas ante ellas.

Antes de matricular la asignatura, verifique los posibles requisitos que pueda tener dentro de su plan. Esta información la encontrará en la pestaña "Plan de estudios" del plan correspondiente.

Competencias y/o resultados del aprendizaje

- CE68. Conocer y evaluar las técnicas para proteger los sistemas informáticos y las redes frente a ataques y software malintencionado.

Contenidos Didácticos

1 Introducción a la seguridad de sistemas de información
  1.1 La arquitectura de seguridad OSI
  1.2 Ataques a la seguridad
  1.3 Servicios de seguridad
  1.4 Mecanismos de seguridad
  1.5 Un modelo de seguridad en redes
  1.6 Estándares de Internet y la Sociedad de Internet
2 Cifrado simétrico y confidencialidad de mensajes
  2.1 Principios del cifrado simétrico
  2.2 Algoritmos de cifrado simétrico
  2.3 Modos de operación del cifrado de bloques
  2.4 Ubicación de los dispositivos de cifrado
  2.5 Distribución de claves
3 Criptografía de clave pública y autentificación de mensajes
  3.1. Enfoques para la autentificación de mensajes

3.2. Funciones hash seguras y HMAC
3.3. Principios de criptografía de clave pública
3.4. Algoritmos de criptografía de clave pública
3.5. Firmas digitales
3.6. Gestión de claves
4 Aplicaciones de autentificación
4.1. Kerberos
4.2. Servicio de autentificación de X.509
4.3. Técnicas de cifrado Kerberos
5 Seguridad en el correo electrónico
5.1. PGP (Pretty Good Privacy)
5.2. S/MIME
6 Seguridad IP
6.1. Introducción a la seguridad IP
6.2. Arquitectura de seguridad IP
6.3. Cabecera de autentificación
6.4. Encapsulamiento de la carga útil de seguridad
6.5. Combinación de asociaciones de seguridad
6.6. Gestión de claves
6.7. Comunicación entre redes y protocolos de Internet
7 Seguridad de la web
7.1. Consideraciones sobre seguridad en la web
7.2. SSL (Secure Socket Layer) y TLS (Transport Layer Security)
7.3. SET (Secure Electronic Transaction)
8 Seguridad en la gestión de redes
8.1. Conceptos básicos de SNMP
8.2. Comunidades SNMPv1
8.3. SNMPv3
9 Software malicioso: ataques e intrusiones.
9.1 Intrusos
9.2 Detección de intrusos
9.3 Gestión de contraseñas
9.4 La falacia de la tasa base
9.5 Software dañino, virus y otras amenazas
9.6 Contramedidas a los virus
10 Técnicas de protección: cortafuegos, IDS, IPS.
10.1 Principios de diseño de cortafuegos
10.2 Sistemas de confianza
10.3 Sistemas IDS
10.4 Sistemas IPS

Contenidos Prácticos

Durante el desarrollo de la asignatura se realizarán las siguientes actividades prácticas:

- Resolución de cuestiones y ejercicios prácticos sobre seguridad en el framework COBIT (de ISACA) y el conjunto de buenas prácticas ITIL.
- Debate/coloquio sobre los informes de Auditorías Informáticas.
- Resolución de un caso práctico sobre la criptografía de clave simétrica.
- Resolución de un caso práctico sobre la criptografía de clave pública.
- Resolución de cuestiones teórico/prácticas sobre las funciones Hash.
- Debate/coloquio sobre la seguridad en Internet y en la Web.

- Resolución de un caso práctico sobre software malicioso y cómo evitar sus ataques.
- Debate/coloquio sobre los cortafuegos y los sistemas de detección y de prevención de intrusos.

Evaluación

El sistema de evaluación del aprendizaje de la UDIMA contempla la realización de diferentes tipos de actividades de evaluación y aprendizaje. El criterio de valoración establecido se detalla a continuación:

Actividades de aprendizaje	10%
Controles	10%
Actividades de Evaluación Continua (AEC)	20%
Examen final presencial	60%
TOTAL	**100%**

Bibliografía

- W. Stallings (2004). *Fundamentos de Seguridad en Redes, Aplicaciones y Estándares*. Pearson Prentice Hall