SEGURIDAD DE SISTEMAS EN REDES

UC	HT	HP	HL	Modalidad	Código	Requisitos	Ult. Actualización
5	4	2		Optativa/ electiva	6022	Redes de Computadoras	Junio 2004

Fundamentación:
La seguridad de sistemas en redes constituye una temática vital y fundamental en el área de las telecomunicaciones y las redes. Su estudio y comprensión en la licenciatura es primordial en la formación de los estudiantes.

Objetivos:
- Conocer los fundamentos básicos de la Seguridad de redes y sistemas.
- Conocer las características básicas esenciales de la seguridad de los sistemas de información.
- Dominar los mecanismos de protección y seguridad de los sistemas de información.
- Aplicar y usar técnicas de detección y prevención de ataques a la seguridad de las redes.
- Estudiar la seguridad de las redes inalámbricas y sus debilidades.

Contenidos Temáticos

1. Fundamentos básicos de la Seguridad de redes.
   Introducción a la Seguridad: Seguridad de la Información, mecanismos de seguridad, servicios de seguridad y ataques o amenazas a la seguridad. Características de la Seguridad: Confidencialidad, Autenticación, Integridad, No repudiación, Control de Acceso, Disponibilidad. Arquitectura de seguridad en el modelo OSI y Modelo básico de Seguridad en redes.

2. Amenazas y Ataques.
   Ataques a la Seguridad: Definición. Categorías de Ataques: Interrupción, Intercepción, Modificación y Fabricación del mensaje. Ataques Pasivos: Definición, tipos. Ataque basado en contenido y en el análisis de tráfico Ataques activos: Definición, tipos. Impersonalización, retransmisión, modificación del mensaje, negación de servicio. Intrusos: Definición, clases de intrusos. Técnicas de Intrusión. Defensa contra la intrusión. Técnicas de Detección de Intrusos: registros de auditoría, estadísticas, basada en reglas. Virus: Definición, taxonomía. Estructura y funcionamiento del virus. Tipos de virus. Antivirus. Gusanos: Definición. Propagación. Contramedidas. Sistemas Confiables: Concepto. Control de Acceso a los datos. Reglas y propiedades de un sistema confiable. Seguridad de la red multinivel.

3. Criptología Convencional o simétrica.
   Criptografía, sistemas criptográficos o criptosistemas y Criptoanálisis. Modelo de Encriptación convencional o simétrico. Técnicas clásicas de encriptación: Técnicas de sustitución, transposición, rotación y esteganografía. Criptoanálisis: Criptoanálisis diferencial y criptoanálisis lineal. Distribución de las claves y generación de número aleatorios. Casos de Estudio de cifrado simétrico.

4. Criptología de clave pública o asimétrica.
   Introducción. Modelos de Criptosistemas de claves públicas. Requerimientos de los criptosistemas de claves públicas y aplicaciones. Criptoanálisis en sistemas de claves públicas. Distribución de las claves públicas y distribución de claves secretas de encriptación/cifrado convencional. Casos de Estudio de cifrado asimétrico o de clave pública.

5. Integridad, Autenticación y Firmas digitales.
   Requerimientos de la autenticación. Funciones de la Autenticación: encriptación del mensaje, Código de autenticación o verificación (MAC) y funciones "hash". Encriptación basada en esquemas simétricos y esquemas asimétricos para la autenticación. Requerimientos del Código de Autenticación de mensajes y caso de estudio. Funciones "hash": Definición. Requerimientos. Técnicas de encadenamiento de bloques. Casos de estudio. Firmas Digitales: Definición. Requerimientos. Firma digital directa. Firma digital arbitrada. Caso de

Estudio. Protocolos de autenticación: Autenticación mutua y autenticación en una sola dirección. Certificados digitales: Definición. Obtención/revocación del certificado. Procedimiento de autenticación con certificados digitales. Caso de estudio.

6. Seguridad en redes Inalámbricas y en IP.
   El problema de las redes inalámbricas. Detección del espectro de frecuencias. Seguridad en Redes 802.11x. El protocolo de Encriptación Inalámbrico (WEP). Vulnerabilidad y ataques en redes 802.11x. Seguridad en redes Bluetooth. Vulnerabilidades y ataques a redes Bluetooth. Seguridad en IP: Introducción. Arquitectura de la seguridad de IP. Cabeceras de autenticación y encapsulación de datos de seguridad.

Bibliografía:

- William Stallings. *Network and Internetwortk Security*.Prentice Hall. 2nd edition. 1999.
- Andrew Tanenbaum. *Computer Networks*. Prentice Hall. 4th Edition, 2002.
- William Stallings. *Criptography and Networtk Security*. Prentice Hall. 2nd edition. 1999.
- Randall K. Nichols. *Wireless Security: Models, Threats, and Solutions.* McGraw-Hill. 2001