SEGURIDAD EN LA INTERNET

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

Fundamentación:

La explosión de la Internet en los últimos años ha sido vertiginosa. Sin embargo, este crecimiento incontrolado ha favorecido el incremento en los riesgos de seguridad, el aumento de las amenazas y ataques a los sistemas y servicios que operan en la Internet. El estudio y comprensión de la seguridad de la Internet es primordial en la formación del estudiante de la licenciatura en Computación.

Objetivos:

- Conocer los fundamentos básicos de la Seguridad para los servicios de la Internet.
- Familiarizar al estudiante con los problemas de seguridad de la Internet.
- Identificar los riesgos que afectan la comunicación, al cliente y al servidor en la Internet.
- Entender y establecer las medidas de seguridad apropiadas para proteger la privacidad del usuario y la integridad de su computador.
- Identificar las amenazas y ataques a los sistemas cliente, al transporte y a al servidor en la Internet.

Contenidos Temáticos

1. Fundamentos básicos de la Seguridad en la Internet.
   Introducción a la Internet como red de redes: surgimiento, historia. Autoridades administrativas de la Internet. Arquitectura de la Internet: Sistemas autónomos y dominios. Administración distribuida. Servicios básicos de la Internet: el sistema de correo electrónico. El servicio web. El sistema de nombre de dominios. El servicio de transferencia de archivos. Otros servicios de la Internet. La seguridad de la Internet: problemas básicos de la seguridad de la Internet y sus servicios.
2. Seguridad en la Web.
   Arquitectura de la Web segura: El Servidor web. El cliente web. Cliente/servidor seguro. Protocolo web seguro. Seguridad en el tráfico de la red: seguridad en el nivel de la red y el protocolo IP seguro. Seguridad en el transporte. Seguridad en nivel de aplicación. Seguridad y autenticación de aplicaciones web multi-capas: seguridad y autenticación en el cliente. Seguridad y autenticación en la capa web. Seguridad y autenticación en la capa del negocio. Seguridad y autenticación en la capa de servicios. Roles, usuarios y grupos. Mecanismos de propagación de la identidad de seguridad entre capas. Casos de estudio de arquitectura de aplicaciones multi-capas seguras. Transacciones seguras en la web. Infraestructura de claves públicas: consideraciones de diseño. Emisión de Certificados digitales. Arquitectura e implantación de la infraestructura de clave publica. Casos de Estudio de seguridad en la Web.
3. Seguridad en el Correo electrónico.
   Arquitectura del Sistema de correo electrónico. Protocolos de correo entrante. Protocolos de correo saliente. Casos de estudio de protocolos. Correo electrónico seguro: Seguridad basada

en el transporte. Seguridad sobre el mensaje. Autenticación del correo electrónico: autenticación del usuario para el correo entrante. Autenticación en el correo saliente. Casos de estudio de autenticación. Casos de Estudio de correo electrónico seguro basado en el mensaje o nivel de aplicación.

4. Seguridad en el Transporte.
   Protocolos de transporte y sesión seguros. Arquitectura del protocolo de sesión seguro. Arquitectura del protocolo de transporte seguro. Autenticación del cliente y el servidor en el transporte. Caso de estudio: protocolos de aplicación sobre transporte seguro.
5. Amenazas y Ataques a la seguridad en la Internet.
   Amenazas y ataques a los Sistemas de Correo electrónico. Ataques a la aplicación cliente de correo. Ataques al servidor de correo. Amenazas a la seguridad en la Web: amenazas a la integridad, confidencialidad, autenticación y negación de servicio en la Web. Consecuencias y contramedidas. Ataques al sistema cliente: ataques a la sesión del cliente. Robo de sesión.
   Ataques al sistema de transporte: ataques a la capa se sesión segura. Ataques al protocolo de transporte seguro. Ataques al sistema de nombres de dominios. Suplantación del servidor DNS. Otros ataques al DNS.

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.
- Garfinkel S., Spafford G., *Web Security & Commerce.* O'Reilly & Associates. 1997
- Eric Rescorla. *SSL and TLS: Designing and Building Secure Systems.* Addison-Wesley. 2000
- Sun Microsystems. *J2EE Tutorial*. http://java.sun.com/j2ee/1.4/docs/tutorial/doc/index.html