10-11

GUÍA DE ESTUDIO DE LDI

SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACION

CÓDIGO 01555173

10-11

SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACION

CÓDIGO 01555173

ÍNDICE

OBJETIVOS

El objetivo esencial de la asignatura es adquirir los conocimientos asociados a todos los aspectos del problema de la seguridad en redes de ordenadores, oriéntandolos a la consecución de la creación de una política de seguridad informática y, en particular, de las redes de una organización. En ese sentido, se analizan los problemas de seguridad física y lógica asociados con los componentes hardware (cableado, repetidores, encaminadores, etc.) así como software (sistemas operativos, aplicaciones y protocolos). Se estudian los distintos tipos de ataques por la red, haciendo una taxonomía lo más exhaustiva posible, así como los distintos tipos de defensas posibles. Se estudian las distintas herramientas de defensa habituales como cortafuegos, analizadores de vulnerabilidades, sistemas de detección de intrusiones, analizadores de protocolos y otros. Se hace especial énfasis en las aplicaciones de la criptografía al problema de la seguridad informática, empezando por una aproximación básica, siguiendo con la clasificación de los distintos tipos de algoritmos criptográficos, su aplicación en protocolos y aplicaciones de uso habitual (y experimental) hoy en dia, y finalizando con una discusión de cómo todo lo anteriormente expuesto se está utilizando para construir lo que llamamos redes privadas virtuales. Finalmente, se hace una descripción del estado actual del comercio electrónico, en relación con la seguridad informática, y sus posibilidades en el futuro muy cercano.

CONTENIDOS

La numeración de los temas hacen referencia al libro, de bibliografía básica, de DIAZ ORUETA G. y otros: *Seguridad en las comunicaciones y en la información,* Ed. UNED, 2004, 1º edición.

Unidad Didáctica 1

TEMA 1. Descripción del problema de la seguridad en las comunicaciones y en la información. Tipos de ataques.

TEMA 2. Seguridad en los elementos físicos existentes en una red: canales de comunicación, cableado, repetidores, conmutadores, encaminadores, servidores, etc.

TEMA 3. Seguridad en los elementos software existentes en una red: sistemas operativos, aplicaciones, protocolos de red IP (e IPv6).

TEMA 4. Métodos de ataque a equipos y redes.Taxonomía de los ataques.

TEMA 5. Defensas básicas ante ataques.

TEMA 6. La política de seguridad como la respuesta razonable a los problemas de seguridad en las comunicaciones y en la información.

Unidad Didáctica 2

TEMA 7. Introducción a los métodos no criptográficos en la implantación de la política de seguridad.

TEMA 8. Los cortafuegos (firewalls) y sus aplicaciones como elemento básico de una política de seguridad de redes.

TEMA 9. Tecnologías de última generación en cortafuegos.

TEMA 10. Herramientas de análisis de vulnerabilidades para la auditoría de seguridad en las comunicaciones.

TEMA 11. Herramientas de detección de intrusiones para la monitorización de la seguridad en las comunicaciones.

TEMA 12. Diseño seguro de redes. Conceptos de alta disponibilidad y diseños redundantes.

Unidad Didáctica 3

TEMA 13. Introducción a la Criptografía como herramienta de obtención de una mayor seguridad en las comunicaciones.

TEMA 14. Métodos criptográficos: sistemas de clave privada, sistemas de clave pública y sistemas de una sola via (*one-way* hash).

TEMA 15. Certificación, autenticación e integridad de la información. Firma digital. Protección de datos.

TEMA 16. Protocolos criptográficos: S.S.L., P.G.P., IPSec, PKI, etc.

TEMA 17. Redes Privadas Virtuales. Túneles IP.

TEMA 18. El comercio electrónico. Seguridad en las transacciones comerciales.

EQUIPO DOCENTE

Nombre y Apellidos	MANUEL ALONSO CASTRO GIL
Correo Electrónico	mcastro@ieec.uned.es
Teléfono	91398-6476
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

Nombre y Apellidos	CLARA MARIA PEREZ MOLINA
Correo Electrónico	clarapm@ieec.uned.es
Teléfono	91398-7746
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

Nombre y Apellidos	GABRIEL DIAZ ORUETA
Correo Electrónico	gdiaz@ieec.uned.es
Teléfono	91398-8255
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

Nombre y Apellidos	ELIO SAN CRISTOBAL RUIZ
Correo Electrónico	elio@ieec.uned.es
Teléfono	91398-9381
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

Nombre y Apellidos	SERGIO MARTIN GUTIERREZ
Correo Electrónico	smartin@ieec.uned.es
Teléfono	91398-7623
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

BIBLIOGRAFÍA BÁSICA

ISBN(13):9788436249750
Título:SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN (1ª)
Autor/es:Castro Gil, Manuel Alonso ; Díaz Orueta, Gabriel ; Peire Arroba, Juan ; Mur Pérez, Francisco ;
Editorial:U.N.E.D.

DÍAZ ORUETA, G., MUR PÉREZ, F., SANCRISTÓBAL, E., CASTRO, M. y PEIRE, J., *Seguridad en las comunicaciones y en la información*, Ed. UNED, 2004, 1º edición.

BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13):9788420541105
Título:COMUNICACIONES Y REDES DE COMPUTADORES (7ª)
Autor/es:Stallings, William ;
Editorial:PRENTICE-HALL

ISBN(13):9788478972449
Título:REDES DE ALTA VELOCIDAD (1ª)
Autor/es:Piattini Velthuis, Mario G. ; García Tomas, Jesús ; Ferrando Girón, Santiago ;
Editorial:RA-MA

ISBN(13):9789702601623
Título:REDES DE COMPUTADORAS
Autor/es:Tanenbaum, Andrew S. ;
Editorial:PEARSON-PRENTICE HALL

Bibliografía general recomendada:

COMER, D., *Redes Globales de información con Internet y TCP/IP, vol. 1: Principios básicos, protocolos y arquitectura*, 3º edición, Ed. Prentice-Hall, 1996.
FEIT, S., *TCP/IP Arquitectura, protocolos e implementación, además de IPv6 y seguridad de IP*, Ed. McGraw-Hill, 1998.
CASTRO, M. y COLMENAR, A., *Sistemas básicos de comunicaciones*, Ed. RA-MA, 1999.
MARIÑO, P., *Las Comunicaciones en la Empresa: Normas, redes y servicios*, 2º edición, Ed. RA-MA, 2003.
STALLINGS, W., *Comunicaciones y redes de computadoras*,6º edición, Ed. Alhambra-Longman, 2000.
GARCÍA, J., FERRANDO, S. y PIATTINI, M. *Redes de alta velocidad*. Ed. Ra-Ma, 1997.
GARCÍA, J., FERRANDO, S. y PIATTINI, M. *Redes para proceso distribuido, 2.ª edición. Ed. Ra-Ma, 2001.*
TANENBAUM, A. S. Redes de computadoras, 3.ª edición. Ed. Prentice-Hall, 1997.

Unidad didáctica 1:

KAEO, M., Designing Network Security, Ed. Cisco Press, 1999.SCHNEIER, B., Secrets and lies, Ed. Wiley, 2000.GARFINKEL, S. y SPAFFORD, G., Practical UNIX and Internet Security

,

Ed. O'Reilly, 1999.

DENNING, D., Information warfare and security, Ed. Addison Wesley,1999.DIFFIE, W. y LANDAU, S., Privacy on the line, MIT Press, 1999.STOLL, C., The cuckoo's egg, Pan Books, 1990.LITTMAN, J., The fugitive. Online with Kevin Mitnick, Ed.LittleBrown,

1997.MITNICK, K., The art of deception, 2003.

Unidad didáctica 2:

SIYAN, K. y HARE, C., Firewalls y la seguridad en Internet, Ed. McGraw-Hill, 1996.
CHAPMAN, D. B. y ZWICKY, E. D., Construya Firewalls para Internet, Ed. Prentice Hall, 1997.
CHESWICK, W. y BELLOVIN, S., Firewalls and Internet Security, Ed. Addison-Wesley, 1994.
LITTLEJOHN SHINDER, D., Prevención y detección de delitos informáticos, Ed. Anaya Multimedia, 2003.

Unidad didáctica 3:

SINGH, S., Los códigos secretos, Ed. Debate, 2000.KAHN, D., The codebreakers, 2º edición, Ed. Scribner, 1996.SCHNEIER, B., Applied Cryptography, 2º edición, Ed. Wiley, 1996.GARFINKEL, S., PGP: encryption for everyone, Ed. O'Reilly, 1995.KOSIUR, D., Building and managing Virtual Private Networks, Ed. Wiley,

1998.SCOTT, C., WOLFE, P., ERWIN, M. y ORAM, A., Virtual Private Networks, 2.ª edición, Ed. O'Reilly, 1999.

SISTEMA DE EVALUACIÓN

1. PRUEBAS DE EVALUACIÓN A DISTANCIA

En el presente curso no hay previstas.

2. TRABAJOS PRÁCTICOS

No está prevista ningún tipo de prácticas

3. PRUEBAS PRESENCIALES

La prueba constará de 20 preguntas tipo test con un valor de 0,5 puntos cada una. Las preguntas mal contestadas restan 0,25 puntos cada una. Las preguntas sin contestar no puntuan. La duración máxima de la prueba será de dos horas.

HORARIO DE ATENCIÓN AL ESTUDIANTE

Será los martes lectivos, de 16 a 20 h. Edificio de la Escuela Técnica Superior de Ingenieros Industriales de la UNED.

D. Gabriel Díaz Orueta

Tel.: 91 398 82 55

D. Sergio Martín Gutiérrez

Tel.: 91 398 79 23

D. Manuel Castro Gil

Tel.: 91 398 64 76

También se pueden dirigir las consultas a la dirección de correo electrónico: gdiaz@ieec.uned.es.

OTROS MEDIOS DE APOYO

Está prevista, al menos, una emisión radiofónica relacionada con esta asignatura. Consulte la Guía de Medios Audiovisuales para una información más detallada sobre calendario y contenidos de las emisiones.

Cualquier novedad que pudiera producirse durante el curso, así como otros materiales para el estudio de la asignatura, quedarán reflejadas en la página web de la misma:
http://www.ieec.uned.es/
(véase actividad docente y busque la asignatura)

RECOMENDACIONES INICIALES PARA LA ASIGNATURA

Para un seguimiento correcto de esta asignatura, el alumno debe tener unos claros conceptos de comunicaciones. Se asume que se conocen bien las estructuras básicas de la arquitectura OSI, así como que se tiene conceptos claros del conjunto de protocolos TCP/IP, de su estructura y de su funcionamiento.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.