Software libre

Jordi Herrera Joancomartí (coord.)
Joaquín Garciía Alfaro
Xavier Perramón Tornil

XP06/M2107/01768

Aspectos avanzados de seguridad en redes

UOC
www.uoc.edu

Jordi Herrera Joancomartí

Coordinador

Licenciado en Matemáticas por la Universidad Autònoma de Barcelona y doctor por la Universitat Politècnica de Catalunya. Su ámbito de investigación es la seguridad de la información y, más concretamente, la protección del copyright electrónico y la seguridad en entornos inalámbricos. Es autor de varios artículos nacionales e internacionales e investigador principal de proyectos de investigación nacionales e internacionales en el ámbito de la seguridad. Actualmente es profesor de los Estudis d'Informàtica y Multimèdia de la Universitat Oberta de Catalunya.

Xavier Perramón Tornil

Autor

Doctor ingeniero de Telecomunicaciones por la Universitat Politècnica de Catalunya. Actualmente trabaja en el diseño y estandarización de sistemas de documentación multimedia. Es profesor del Departamento de Arquitectura de Computadores adscrito a la Escola Universitària Politècnica del Baix Llobregat.

Joaquín García Alfaro

Autor

Ingeniero técnico en Informètica de Gestión e ingeniero en Informática por la Universitat Autònoma de Barcelona (UAB). Su ámbito de investigación es la seguridad en redes de computadores y, más concretamente, la criptografia y la detección de ataques e intrusiones en redes TCP/IP. Actualmente está realizando estudios de doctorado en el grupo CCD de la UAB, donde también colabora como personal de apoyo a la investigación y como docente de la asignatura de Redes de computadores I de la Ingeniería Informática.

Segunda edición: febrero 2007

Av. Tibidabo, 39-43, 08035 Barcelona
Material realizado por Eureca Media, SL

Depósito legal: B-4.642-2007

Agradecimientos

Los autores agradecen a la Fundación para la Universitat Oberta de Catalunya (http://www.uoc.edu) la financiación de la primera edición de esta obra, enmarcada en el Máster Internacional en Software Libre ofrecido por la citada institución.

Introducción

En esta asignatura se presenta la problemática de la seguridad en las redes de computadores y, más concretamente, en las redes TCP/IP.

La estructuración sigue el siguiente modelo. En primer lugar, se presenta la problemática de la seguridad en las redes TCP/IP. Cabe destacar que esta asignatura se centra en la problemática de la seguridad en las redes y, por lo tanto algunos temas de seguridad que hacen referencia a procesos más específicos de los propios sistemas informáticos sólo los estudiaremos sumariamente como consecuencia de la problemática de la seguridad en las redes.

Una vez hayamos visto cuáles son los eventuales problemas de seguridad en este tipo de redes, nos centraremos en los mecanismos de prevención que existen para a intentar minimizar la realización de los ataques descritos en el primer módulo. Veremos que, fundamentalmente, las técnicas de prevención se basan en el filtraje de información.

Posteriormente pondremos énfasis en las técnicas específicas de protección existentes. En particular, introduciremos las nociones básicas de criptografía que nos permitirán entender el funcionamiento de distintos mecanismos y aplicaciones que permiten protegerse frente los ataques. En concreto nos centraremos en los mecanismos de autentificación y en la fiabilidad que nos proporcionan los diferentes tipos, veremos qué mecanismos de protección existen a nivel de red y a nivel de transporte y veremos cómo podemos crear redes privadas virtuales. Por otro lado, también veremos cómo funcionan algunas aplicaciones seguras, como el protocolo SSH o estándares de correo electrónico seguro.

Finalmente, y partiendo de la base que no todos los sistemas de prevención y protección de las redes TCP/IP son infalibles, estudiaremos los diferentes mecanismos de detección de intrusos que existen y cuáles son sus arquitecturas y funcionalidades.

Objetivos

Globalmente, los objetivos básicos que se deben alcanzar son los siguientes:

1. Entender los distintos tipos de vulnerabilidades que presentan las redes TCP/IP.

2. Ver qué técnicas de prevención existen contra los ataques más frecuentes.

3. Alcanzar unos conocimientos básicos del funcionamiento de las herramientas criptográficas más utilizadas.

4. Conocer los sistemas de autentificación más importantes, identificando sus características.

5. Ver diferentes propuestas existentes para ofrecer seguridad tanto a nivel de red, de transporte o de aplicación.

6. Conocer los diferentes sistemas de detección de intrusos.

Contenidos

Módulo didáctico 4
Aplicaciones seguras

1. El protocolo SSH

2. Correo electrónico seguro

Módulo didáctico 5
Mecanismos para la detección de ataques e intrusiones

1. Necessidad de mecanismos adicionales en la prevención y protección

2. Sistemas de detección de intrusos

3. Escáners de vulnerabilidades

4. Sistemas de decepción

5. Prevención de intrusos

6. Detección de ataques distribuidos

Apéndice
GNU Free Documentation License

Bibliografía

1. Cheswick, W.R.; Bellovin, S.M.; Rubin, A.D. . (2003). *Firewalls and Internet Security: Repelling the Wily Hacker.* (5^a ed.): Addison-Wesley Professional Computing.

2. Oppliger, R. (2000). *Security technologies for the Word Wide Web.* 1^a ed.: Artech House.

3. Menezes, J.; van Oorschot, P.C.; Vanstone, S.A. (2001). *Handbook of Applied Cryptography.* (5^a ed.): CRC Press.