Seguretat en Xarxes de Computadors

Jordi Herrera Joancomartí (Coordinador)

6 crèdits
XP03/05070/02091

www.uoc.edu

Jordi Herrera Joancomartí

Llicenciat en Matemàtiques per la Universitat Autònoma de Barcelona i Doctor per la Universitat Politècnica de Catalunya. El seu àmbit de recerca és la seguretat de la informació i més concretament la protecció del copyright electrònic i la seguretat en entorns sense fils. És autor de diversos articles nacionals i internacionals i investigador principal de projectes de recerca nacionals i internacionals en l'àmbit de la seguretat. Actualment és professor dels Estudis d'Informàtica i Multimèdia de la Universitat Oberta de Catalunya.

Joaquín García Alfaro

Enginyer tècnic en Informàtica de Gestió i Enginyer en Informàtica per la Universitat Autònoma de Barcelona. El seu àmbit de recerca és la seguretat en xarxes de computadors i més concretament la criptogràfia i la detecció d'atacs i intrusions en xarxes TCP/IP. Actualment està realitzant els seus estudis de doctorat al grup CCD de la UAB, a on també col·labora com a personal de suport a la recerca i com a docent de la assignatura de Xarxes de Computadors I de la enginyeria informàtica.

Xavier Perramón Tornil

Doctor Enginyer de Telecomunicació per la Universitat Politècnica de Catalunya. Actualment treballa en el disseny i estandardització de sistemes de documentació multimèdia. 'Es professor del Departament d'Arquitectura de Computadors adscrit a l'Escola Universitària Politècnica del Baix Llobregat.

Primera edició: febrer 2004

Av. Tibidabo, 39 - 43, 08035 Barcelona
Disseny: Manel Andreu
Material realitzat per Eurecamedia, SL
ISBN: 84-9788-061-7
Dipòsit legal: B-1013-2004

Introducció

En aquesta assignatura es presenta la problemàtica de la seguretat en les xarxes de computadors, i més en concret en les xarxes TCP/IP.

L'estructuració d'aquesta assignatura segueix el següent model. En primer lloc, es presenta la problemàtica de la seguretat en les xarxes TCP/IP. Cal destacar que aquesta assignatura se centra en la problemàtica de la seguretat en les xarxes i per tant alguns temes de seguretat que fan referència a coses més específiques dels propis sistemes informàtics només les veurem de passada com a conseqüència de la problemàtica de la seguretat en les xarxes.

Un com haguem vist quins són els eventuals problemes de seguretat en aquest tipus de xarxes, ens centrarem en els mecanismes de prevenció que existeixen de cara a intentar minimitzar la realització dels atacs descrits en el primer mòdul. Veurem que fonamentalment, les tècniques de prevenció es basen en el filtrat d'informació.

Posteriorment farem èmfasi en les tècniques específiques de protecció que hi ha. En particular, introduïrem les nocions bàsiques de criptografia que ens permetran entendre el funcionament de diferents mecanismes i aplicacions que permeten protegir-se en front dels atacs. En concret farem èmfasi en els mecanismes d'autentificació existents i la fiabilitat que ens donen els diferent tipus, veurem quins mecanismes de protecció hi ha a nivell de xarxa i a nivell de transport i veurem com podem crear xarxes privades virtuals. D'altra banda, també veurem com funcionen algunes aplicacions segures com ara el protocol SSH o estàndards de correu electrònic segur.

Finalment, i assumint que no tots els sistemes de prevenció i protecció de les xarxes TCP/IP són infal·libles, estudiarem els diferents mecanismes de detecció d'intrusos que existeixen i quines són les seves arquitectures i funcionalitats.

Objectius

Globalment, els objectius bàsics que s'han d'assolir són els següents:

1. Entendre els diferents tipus de vulnerabilitats que presenten les xarxes TCP/IP.
2. Veure quines tècniques de prevenció hi ha contra els atacs més freqüents.
3. Assolir uns coneixements bàsics del funcionament de les eines criptogràfiques més utilitzades.
4. Conèixer els sistemes d'autentificació més importants tot identificant-ne les seves característiques.
5. Veure diferents propostes existents per a oferir seguretat tant a nivell de xarxa, de transport o d'aplicació.
6. Conèixer els diferents sistemes de detecció d'intrusos.

Continguts

Mòdul didàctic 1
Atacs contra les xarxes TCP/IP

1. Seguretat en xarxes TCP/IP
2. Activitats prèvies a la realització d'un atac
3. Escoltadors de xarxa
4. Fragmentació IP
5. Atacs de denegació de servei
6. Deficiències de programació

Mòdul didàctic 2
Mecanismes de prevenció

1. Sistemes Tallafocs
2. Construcció de sistemes tallafocs
3. Zones desmilitaritzades
4. Característiques addicionals dels sistemes tallafocs

Mòdul didàctic 3
Mecanismes de protecció

1. Conceptes bàsics de criptografia
2. Sistemes d'autentificació
3. Protecció del nivell de xarxa: IPsec
4. Protecció del nivell de transport: SSL/TLS
5. Xarxes privades virtuals

Mòdul didàctic 4
Aplicacions segures

1. El protocol SSH

2. Correu electrònic segur

Mòdul didàctic 5
Sistemes per a la detecció d'atacs i intrusions

1. Necessitat de mecanismes addicionals a la prevenció i protecció

2. Sistemes de detecció d'intrusos

3. Escàners de vulnerabilitats

4. Sistemes de decepció

5. Prevenció d'intrusions

6. Detecció d'atacs distribuïts

Bibliografia

1. William R. Cheswick, Steven M. Bellovin and Aviel D. Rubin. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker.* (5a. edició): Addison-Wesley Professional Computing.

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

3. J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (2001). *Handbook of Applied Cryptography.* (5a. edició): CRC Press.