Seguridad en redes

Joan Borrell Viader
Joaquín García Alfaro
Antoni Martínez Ballesté
Guillermo Navarro Arribas
Cristina Pérez Solà
Xavier Perramon Tornil
Helena Rifà Pous
Sergi Robles Martínez

PID_00191696

Material docente de la UOC

UOC
Universitat Oberta de Catalunya
www.uoc.edu

Joan Borrell Viader

Doctor en Informática (1996) por la Universidad Autónoma de Barcelona (UAB). Es profesor titular de esta universidad y director del Departamento de Ingeniería de la Información y de las Comunicaciones, donde combina investigación y docencia. Sus líneas actuales de investigación se centran en la seguridad en aplicaciones distribuidas tolerantes a retardos e interrupciones. Ha sido coautor de más de sesenta artículos y patentes, ha dirigido siete tesis doctorales y ha liderado varios proyectos de investigación. Es docente de asignaturas relacionadas con redes de ordenadores y su seguridad, y ha dirigido un centenar largo de proyectos de fin de grado.

Joaquín García Alfaro

Ingeniero de Informática por la Universidad Autónoma de Barcelona. Doctor en Informática por la UAB y por la Universidad de Rennes I (Francia). Es miembro de los grupos de investigación siguientes: KISON (UOC, profesor propio), SeNDA (UAB, colaborador posdoctoral), NRG (Carleton University, investigador posdoctoral) y SERES (Telecom Bretagne, ingeniero de investigación). Su ámbito de investigación gira en torno al estudio de las vulnerabilidades y las contramedidas que pueden mejorar la seguridad de los sistemas de información.

Helena Rifà Pous

Ingeniera de Telecomunicaciones y doctora por la Universidad Politécnica de Cataluña. Es profesora agregada de los Estudios de Informática, Multimedia y Telecomunicaciones de la UOC. Actualmente es la directora del máster interuniversitario de Seguridad TIC. Forma parte del grupo de investigación KISON. Sus líneas de investigación se centran en el campo de la seguridad en redes abiertas (p2p, *ad hoc*, radio cognitiva). En este campo ha publicado más de treinta artículos en revistas y congresos internacionales y ha dirigido más de cuarenta proyectos de fin de grado y de máster.

Sergi Robles Martínez

Doctor Ingeniero de Informática por la Universidad Autónoma de Barcelona (2002). Es profesor titular del Departamento de Ingeniería de la Información y de las Comunicaciones de la UAB, donde combina investigación y docencia. Sus líneas actuales de investigación se centran en la seguridad y las aplicaciones de las redes tolerantes a retardos y los agentes móviles. Ha publicado mucho en este campo y tiene experiencia en la dirección de proyectos de investigación. Es docente de asignaturas relacionadas con las redes de ordenadores y la seguridad computacional. Actualmente coordina el grupo de investigación SeNDA de la UAB y el grupo de innovación docente GIIDES Wiki de nuevas tecnologías aplicadas a la docencia.

Cristina Pérez Solà

Ingeniera de Informática por la Universidad Autónoma de Barcelona. Su investigación se centra en el estudio de los problemas de privacidad que surgen en las redes sociales en línea. Actualmente es consultora de los Estudios de Informática y Multimedia de la Universitat Oberta de Catalunya y técnica de apoyo a la investigación en la Universidad Autónoma de Barcelona.

Xavier Perramon Tornil

Doctor Ingeniero de Telecomunicación por la Universidad Politécnica de Cataluña. Actualmente trabaja en la protección de información multimedia. Es profesor del Departamento de Tecnologías de la Información y las Comunicaciones de la Universidad Pompeu Fabra.

Antoni Martínez Ballesté

Ingeniero de Informática por la Universidad Rovira i Virgili (2002) y doctor en Telemática por la Universidad Politécnica de Cataluña (2004). Profesor de la URV de los ámbitos de la telemática y la informática. Sus temas de investigación son la seguridad y la privacidad en las tecnologías de la información y las comunicaciones, a los que ha contribuido con más de cuarenta publicaciones. Es consultor de la UOC y autor de materiales.

Guillermo Navarro Arribas

Ingeniero de Informática y doctor por la Universidad Autónoma de Barcelona. En este momento es profesor lector en el Departamento de Ingeniería de la Información y de las Comunicaciones de la UAB y doctor vinculado al Instituto de Investigación en Inteligencia Artificial del CSIC. Su ámbito de investigación es la seguridad informática, y más concretamente la seguridad en redes, control de acceso y privacidad de datos. Es miembro de los grupos de investigación SeNDA de la UAB e IF-PAD (Informations Fusion for Privacy and Decision) del CSIC.

El encargo y la creación de este material docente los ha coordinado el profesor Jordi Herrera Joancomartí para el programa del Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones –MISTIC– (2012).

Primera edición: septiembre 2012
© Joan Borrell Viader, Joaquín García Alfaro, Antoni Martínez Ballesté, Guillermo Navarro Arribas, Cristina Pérez Solà, Xavier Perramon Tornil, Helena Rifà Pous, Sergi Robles Martínez
Todos los derechos reservados
© de esta edición, FUOC, 2012
Av. Tibidabo, 39-43, 08035 Barcelona
Diseño: Manel Andreu
Realización editorial: Eureca Media, SL
Depósito legal: B-25.301-2012

Los textos e imágenes publicados en esta obra están sujetos –salvo que se indique lo contrario– a una licencia de Reconocimiento-NoComercial-SinObraDerivada (BY-NC-ND) v.3.0 España de Creative Commons. Podéis copiarlos, distribuirlos y transmitirlos públicamente siempre que citéis el autor y la fuente (FUOC. Fundació per a la Universitat Oberta de Catalunya), no hagáis un uso comercial de ellos y no hagáis obra derivada. La licencia completa se puede consultar en http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.es.

Objetivos

Los objetivos que alcanzaréis con el estudio de los materiales de esta asignatura son los siguientes:

1. Conocer qué es un sistema cortafuegos, cuál es su funcionamiento y cómo se puede utilizar para dotar de seguridad a una red informática.
2. Comprender las diferencias técnicas que se pueden utilizar para detectar intrusos en un sistema informático y saber cómo se pueden implementar.
3. Entender los problemas de seguridad y los ataques a redes WLAN y conocer los mecanismos que permiten minimizarlos.
4. Identificar los problemas de seguridad que surgen en entornos de redes inalámbricas de alcance personal (WPAN) y ver los diferentes mecanismos de seguridad que proporcionan diferentes tecnologías (RFID, Bluetooth y ZigBee).
5. Conocer cómo afectan diferentes ataques a las propiedades de confidencialidad de la información y autenticidad de los servicios de voz sobre IP y de mensajería instantánea.
6. Entender los problemas de seguridad y algunas posibles soluciones de las redes emergentes, especialmente redes *ad hoc*, de sensores y redes tolerantes a retardos.

Contenidos

Módulo 1
Sistemas de cortafuegos
Guillermo Navarro Arribas
1. Sistemas de cortafuegos
2. Tipos de cortafuegos
3. Arquitecturas de cortafuegos
4. Mecanismos y reglas de filtrado
5. Más allá del filtrado de paquetes

Módulo 2
Sistemas de detección de intrusos en red
Joaquín García Alfaro
1. Detección de intrusos en red
2. Detección de intrusos en red con Snort
3. Gestión de eventos, alertas e incidentes

Módulo 3
Seguridad en redes WLAN
Xavier Perramon Tornil
1. Conceptos básicos de redes Wi-Fi
2. Métodos de autenticación de las estaciones Wi-Fi
3. Protección de tramas con WEP
4. Vulnerabilidades del protocolo WEP
5. Soluciones a las vulnerabilidades WEP

Módulo 4
Seguridad en redes inalámbricas de alcance personal
Cristina Pérez Solà
1. RFID
2. Bluetooth
3. ZigBee
4. Comparativa y discusión de la seguridad

Módulo 5
Seguridad en servicios de voz sobre IP y mensajería instantánea
Antoni Martínez Ballesté
1. Servicios de comunicación síncrona
2. Denegación y degradación del servicio
3. Problemas de seguridad en la comunicación
4. Herramientas para comunicaciones seguras

Módulo 6

Redes emergentes. MANET, WSN, DTN

Helena Rifà Pous, Sergi Robles Martínez y Joan Borrell Viader

1. Redes emergentes
2. Redes *ad hoc*
3. Redes de sensores
4. Protocolos tolerantes a retardos e interrupciones
5. Problemas de seguridad en protocolos DTN

Bibliografía

Baronti, P.; Pillai, P.; Chook, V.; Chessa, S.; Gotta, A.; Hu, Y. (2007). *Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards*. Ámsterdam: Elsevier Science Publishers B. V.

Cayirci, E.; Rong, C. (2009). *Security in Wireless Ad Hoc and Sensor Networks*. John Wiley & Sons.

Cheswick, W. R.; Bellovin, S. M.; Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker* (2.ª ed). Addison-Wesley Professional Computing.

Endler, D. y otros (2006). *Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions*. McGraw-Hill Professional Publishing.

Farrell, S.; Cahill, V. (2006). *Delay- and Disruption-Tolerant Networking*. Norwood (MA, EUA): Artech House, Inc.

Ma, Jianfeng; Ma, Zhuo; Wang, Changguang (2009). *Security Access in Wireless Local Area Networks: From Architecture and Protocols to Realization*. Springer-Verlag Berlin.

Proctor, P. E. (2001). *The practical intrusion detection handbook*. Prentice-Hall.