

Identidad digital

Jordi Castellà-Roca
Antoni Felguera
Antoni Martínez-Ballesté
José María Palazón Romero
Agustí Solanas
Alexandre Viejo Galicia

PID_00184694

Material docente de la UOC

Jordi Castellà-Roca

Ingeniero técnico en Informática de Sistemas por la Universidad de Lleida. Ingeniero en Informática por la Universidad Rovira i Virgili. Doctor en Informática por la Universidad Autónoma de Barcelona. Sus ámbitos de investigación son la criptografía y la privacidad. Autor de más de cuarenta publicaciones, tanto nacionales como internacionales. Ha participado en más de 24 proyectos de investigación y transferencia, liderando nueve de ellos. Coautor de seis patentes (cinco en explotación), y socio fundador de tres empresas tecnológicas. Actualmente es profesor agregado de la Universidad Rovira i Virgili, y miembro de la Cátedra UNESCO de Privacidad de Datos.

Antoni Felguera

Ingeniero superior en Informática por la Universidad Politécnica de Cataluña (UPC), Executive MBA por EADA, CISSP y poseedor de diferentes másters de Arquitectura del software por ESI y Microsoft. Jefe del Área de Métodos y Sistemas del Institut Català de Tecnologia (ICT), director corporativo en tecnologías en empresas, del sector de la distribución deportiva en Andorra y de la educación superior en Barcelona, forma parte del Comité Directivo de esta última. En el 2007 se incorpora a la Fundación Barcelona Digital como director de Expansión, y en el 2008 pasa a ocupar la Dirección del Área de Investigación y Desarrollo en Seguridad.

Antoni Martínez-Ballesté

Ingeniero técnico en Informática de Sistemas e ingeniero en Informática por la Universidad Rovira i Virgili. Doctor en Ingeniería Telemática por la Universidad Politécnica de Cataluña. Experto en formación en TIC. Investiga en los ámbitos de privacidad y seguridad en las TIC. Autor de más de cuarenta publicaciones científicas. Profesor agregado de la Universidad Rovira i Virgili, y miembro de la Cátedra UNESCO de Privacidad de Datos. Consultor de la UOC y autor de materiales.

José María Palazón Romero**Agustí Solanas**

Ingeniero técnico en Informática de Sistemas por la Universidad Rovira i Virgili (2002). Ingeniero en Informática por la Universidad Rovira i Virgili (2004) (premio extraordinario – 1.º de la promoción). Doctor en Telemática por la Universidad Politécnica de Cataluña (2007) (sobresaliente cum laude). Sus líneas de investigación se centran en la seguridad y la privacidad así como en la inteligencia computacional. Autor de más de 70 publicaciones en revistas y congresos nacionales e internacionales. Ha participado en numerosos proyectos nacionales e internacionales y es miembro de diversas asociaciones científicas como ACM, SigmaXi y IEEE. Actualmente es profesor lector en el Departamento de Ingeniería Informática y Matemáticas de la Universidad Rovira i Virgili, y miembro de la Cátedra UNESCO de Privacidad de Datos.

Alexandre Viejo Galicia

Ingeniero en Informática en el 2005. Máster en Ingeniería informática y de la seguridad en el 2007. Máster en Administración de empresas y doctor en Ingeniería Informática en el 2008. Es autor de una decena de artículos científicos y sus ámbitos de investigación se centran en temas como la privacidad en los buscadores de información, la privacidad en las redes de vehículos y la seguridad en las redes de sensores. Actualmente es profesor lector del Departamento de Ingeniería Informática y Matemáticas de la Universidad Rovira i Virgili.

El encargo y la creación de este material docente los ha coordinado la profesora Helena Rifà Pous para el programa del Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones –MISTIC– (2011).



Primera edición: septiembre 2011

© Jordi Castellà-Roca, Antoni Felguera, Antoni Martínez-Ballesté, José María Palazón Romero, Agustí Solanas, Alexandre Viejo Galicia

Todos los derechos reservados

© de esta edición, FUOC, 2011

Av. Tibidabo, 39-43, 08035 Barcelona

Diseño: Manel Andreu

Realización editorial: Eureka Mèdia, SL

Depósito legal: B-365-2012



Los textos e imágenes publicados en esta obra están sujetos –excepto 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 la Universitat Oberta de Catalunya), no hagáis de ellos un uso comercial y ni obra derivada. La licencia completa se puede consultar en <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.es>

Introducción

La identidad se puede definir como el aspecto colectivo del conjunto de características mediante las cuales una cosa es reconocible o conocida. En este sentido, la identidad de una persona se entiende como aquello que hace que esta sea única como individuo respecto al resto.

El proceso de verificar la identidad de una persona recibe el nombre de *autenticación*, y su seguridad depende directamente de las características que se utilicen para ello. La importancia de la seguridad en la autenticación se debe a que esta se utiliza para dar acceso a un recurso o poder realizar determinada actividad. Si esta verificación falla, se podrá acceder al recurso por parte de individuos no autorizados, o estos podrán realizar acciones a las que no deberían tener acceso.

Estas acciones se han hecho, y siguen haciéndose de forma cotidiana en el mundo físico día tras día. En el caso del mundo digital, existen las mismas necesidades de proteger los recursos y las acciones que pueden hacer los usuarios. Es decir, es necesario disponer de una identidad en el mundo digital, a la que llamaremos "identidad digital", y de métodos de autenticación adecuados.

El siguiente paso a la autenticación puede ser el control del acceso a los recursos, o las acciones que se pueden realizar. Este control normalmente se basa en roles. Cada usuario tiene un rol asignado y puede realizar unas acciones u otras en función de este.

La explosión de los servicios disponibles ha ocasionado que los usuarios dispongan de más de una "identidad digital", y que los proveedores de estos servicios deban gestionarlas. Esta gestión se vuelve más compleja cuando diferentes servicios se combinan entre sí, o los usuarios de un sistema deben acceder a otro sistema con una única identidad. La colaboración entre los servicios es vital para un mejor aprovechamiento de los recursos.

Una característica importante del mundo digital son las trazas que dejan los usuarios cada vez que acceden a un servicio o realizan una acción. Estas trazas se pueden vincular con la mencionada "identidad digital". En algunos casos estas pueden desvelar información confidencial del propio usuario. Por este motivo es importante preservar la privacidad de los usuarios tanto como sea posible.

En esta asignatura se presentan las principales técnicas para identificar a los usuarios en el mundo digital, realizar una autenticación segura, y llevar a cabo un control de acceso. A continuación se describen las tecnologías y aplicaciones que permiten realizar una autenticación y autorización en entornos mul-

usuario, los servicios de directorio, la autenticación única para acceder a los servicios, y la federación de identidades. Finalmente, se destaca la importancia de la privacidad, y se introducen las principales técnicas para garantizarla.

Con el fin de facilitar la consecución de los objetivos de esta asignatura, se combinan los contenidos teóricos con los prácticos. Se pretende que los estudiantes adquieran un conocimiento suficiente de las principales aplicaciones y tecnologías.

Objetivos

Esta asignatura contiene los materiales didácticos necesarios para que el estudiante adquiera los objetivos siguientes:

1. Comprender qué es la autenticación de la identidad.
2. Conocer las técnicas y conceptos relacionados con la autenticación de usuarios.
3. Conocer las fases y políticas del control de acceso, y el funcionamiento de los principales tipos de control de acceso.
4. Asimilar las tecnologías que permiten hacer una autenticación y autorización en aplicaciones multiusuario.
5. Comprender el concepto y la utilidad de un servicio de directorio, y el concepto de espacio de nombres.
6. Conocer las principales implantaciones de servicios de directorio.
7. Adquirir el concepto de Federación de Identidades, los términos asociados y su relación con los diferentes elementos de la gestión de la identidad y acceso.
8. Conocer los métodos y tecnologías que permiten realizar la Federación de Identidades.
9. Entender qué es la huella digital de un usuario, qué contiene, y cómo se crea.
10. Entender el funcionamiento de las técnicas disponibles para preservar la privacidad de los usuarios.

Contenidos

Módulo didáctico 1

Identificación, autenticación y control de acceso

Antoni Martínez-Ballesté, Agustí Solanas y Jordi Castellà-Roca

1. Técnicas de identificación y autenticación
2. Ciclo de vida de la identidad digital
3. Control de acceso

Módulo didáctico 2

Autenticación y autorización en aplicaciones multiusuario

José María Palazón Romero

1. Autenticación y autorización en Java
2. Autenticación y Autorización en PHP
3. Autorización y autenticación en aplicaciones .NET

Módulo didáctico 3

Servicios de directorio

Antoni Martínez-Ballesté y Jordi Castellà-Roca

1. Concepto y uso de los directorios
2. Diseño del directorio
3. Implementaciones de servicio de directorio

Módulo didáctico 4

Single sign-on y federación de identidades

José María Palazón Romero, Antoni Felguera y Jordi Castellà-Roca

1. La federación de identidades
2. Estándares
3. Tecnología para la gestión de identidades federadas

Módulo didáctico 5

Privacidad

Alexandre Viejo Galicia y Jordi Castellà-Roca

1. La huella digital
2. Perfiles de usuario
3. Definición y políticas de privacidad
4. Técnicas para proporcionar privacidad

Bibliografía

Arkills, B. (2003). *LDAP Directories Explained: An Introduction and Analysis*. Boston (Massachusetts): Addison-Wesley Professional. ISBN 978-0201787924

Desmond, R. y otros (2008). *Active Directory: Designing, Deploying and Running Active Directory*. Sebastopol (California): O'Reilly.

Gollmann, D. (2005). *Computer Security* (2.^a ed.). Chichester (West Sussex): John Wiley & Sons.

Harris, S. (2008). *All in one CISSP Exam Guide*. Nueva York: McGraw Hill.

Herrera Joancomartí, J. (2006). *Aspectos avanzados de seguridad en redes*. Barcelona: Editorial UOC.

Raya, J. L. y otros (2008). *Aprenda Microsoft Windows Server 2008*. Madrid: Ra-Ma.

Stallings, W. (2008). *Computer security: principles and practice*. Upper Saddle River, (Nueva Jersey): Pearson/Prentice Hall.

Todorov, D. (2007). *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. Boca Raton (Florida): Auerbach Publications. ISBN 978-1420052190

Williamson, G.; Yip, D.; Sharoni, I.; Spaulding, K. (2009). *Identity Management: A Primer*. Lewisville (Texas): McPress Online. ISBN 978-1583470930

Windley, P. J. (2005). *Digital Identity*. Sebastopol (California): O'Reilly Media. ISBN 978-0596008789

