

Identitat digital

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

PID_00184693

Material docent de la UOC

Jordi Castellà-Roca

Enginyer tècnic d'Informàtica de Sistemes per la Universitat de Lleida. Enginyer d'Informàtica per la Universitat Rovira i Virgili. Doctor en Informàtica per la Universitat Autònoma de Barcelona. Els seus àmbits de recerca són la criptografia i la privadesa. Autor de més de quaranta publicacions, tant nacionals com internacionals. Ha participat en més de 24 projectes de recerca i transferència, dels quals ha liderat nou. Coautor de sis patents (cinc en explotació) i soci fundador de tres empreses tecnològiques. Actualment, professor agregat de la Universitat Rovira i Virgili, i membre de la Càtedra Unesco de Privadesa de Dades.

Antoni Felguera

Enginyer superior d'Informàtica per la Universitat Politècnica de Catalunya, *executive MBA* per EADA, CISSP i posseïdor de diferents màsters d'Arquitectura del programari per ES1 i Microsoft. Cap de l'Àrea de Mètriques i Sistemes de l'Institut Català de Tecnologia (ICT), director corporatiu de tecnologies en empreses del sector de la distribució esportiva a Andorra i de l'educació superior a Barcelona, ha format part del Comitè Directiu d'aquesta última. El 2007 s'incorpora a la Fundació Barcelona Digital com a director d'expansió, i el 2008 passa a ocupar la direcció de l'Àrea de Recerca i Desenvolupament en Seguretat.

Antoni Martínez-Ballesté

Enginyer tècnic d'Informàtica de Sistemes i enginyer d'Informàtica per la Universitat Rovira i Virgili. Doctor en Enginyeria Telemàtica per la Universitat Politècnica de Catalunya. Expert en formació en TIC. Investiga en els àmbits de privadesa i seguretat en les TIC. Autor de més de quaranta publicacions científiques. Professor agregat de la Universitat Rovira i Virgili, i membre de la Càtedra Unesco de Privadesa de Dades. Consultor de la UOC i autor de materials.

José María Palazón Romero**Agustí Solanas**

Enginyer tècnic d'Informàtica de Sistemes per la Universitat Rovira i Virgili (2002). Enginyer d'Informàtica per la Universitat Rovira i Virgili (2004) (premi extraordinari - 1r. de la promoció). Doctor en Telemàtica per la Universitat Politècnica de Catalunya (2007) (excel·lent *cum laude*). Les seves línies de recerca se centren en la seguretat i la privadesa i també en la intel·ligència computacional. Autor de més de 70 publicacions en revistes i congressos nacionals i internacionals. Ha participat en nombrosos projectes nacionals i internacionals i és membre de diverses associacions científiques com ACM, SigmaXi i IEEE. Actualment, professor lector al Departament d'Enginyeria Informàtica i Matemàtiques de la Universitat Rovira i Virgili, i membre de la Càtedra Unesco de Privadesa de Dades.

Alexandre Viejo Galicia

Enginyer d'Informàtica el 2005. Màster en Enginyeria informàtica i de la seguretat el 2007. Màster en Administració d'empreses i doctor en Enginyeria Informàtica el 2008. Autor d'una desena d'articles científics, els seus àmbits de recerca se centren en temes com la privadesa en els cercadors d'informació, la privadesa a les xarxes de vehicles i la seguretat a les xarxes de sensors. Actualment, professor lector del Departament d'Enginyeria Informàtica i Matemàtiques de la Universitat Rovira i Virgili.

L'encàrrec i la creació d'aquest material docent han estat coordinats per la professora: Helena Rifà Pous per al programa del Màster Interuniversitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions –MISTIC– (2011)



Primera edició: setembre 2011

© Jordi Castellà-Roca, Antoni Felguera, Antoni Martínez-Ballesté, José María Palazón Romero, Agustí

Solanas, Alexandre Viejo Galicia

Tots els drets reservats

© d'aquesta edició, FUOC, 2011

Av. Tibidabo, 39-43, 08035 Barcelona

Disseny: Manel Andreu

Realització editorial: Eureca Media, SL

Dipòsit legal: B-364-2012



Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>

Introducció

La identitat es pot definir com l'aspecte col·lectiu del conjunt de característiques mitjançant les quals una cosa és recognoscible o coneguda. En aquest sentit, la identitat d'una persona s'entén com allò que fa que aquesta sigui única com a individu respecte a la resta.

El procés de verificar la identitat d'una persona rep el nom d'*autenticació*, i la seva seguretat depèn directament de les característiques que s'utilitzin per a això. La importància de la seguretat en l'autenticació es deu al fet que s'utilitza per a donar accés a un recurs o per a poder fer una activitat determinada. Si aquesta verificació falla, individus no autoritzats podran accedir al recurs, o bé podran fer accions a les quals no haurien de tenir accés.

Aquestes accions s'han fet, i es continuen fent, de manera quotidiana al món físic dia rere dia. En el cas del món digital, hi ha les mateixes necessitats de protegir els recursos i les accions que poden fer els usuaris. És a dir, cal disposar d'una identitat al món digital, que anomenarem *identitat digital*, i de mètodes d'autenticació adequats.

El pas següent a l'autenticació pot ser el control de l'accés als recursos, o les accions que es poden fer. Aquest control normalment es basa en rols. Cada usuari té un rol assignat i pot dur a terme unes accions o unes altres en funció d'aquest rol.

L'explosió dels serveis disponibles ha ocasionat que els usuaris disposin de més d'una identitat digital, i que els proveïdors d'aquests serveis les hagin de gestionar. Aquesta gestió es torna més complexa quan diferents serveis es combinen entre si, o els usuaris d'un sistema han d'accedir a un altre amb una única identitat. La col·laboració entre els serveis és vital per a un millor aprofitament dels recursos.

Una característica important del món digital són les traces que deixen els usuaris cada vegada que accedeixen a un servei o fan una acció. Aquestes traces es poden vincular amb la identitat digital esmentada. En alguns casos les traces poden desvetllar informació confidencial de l'usuari mateix. Per aquest motiu és important preservar la privadesa dels usuaris tant com sigui possible.

En aquesta assignatura es presenten les principals tècniques per a identificar els usuaris en el món digital, fer-ne una autenticació segura, i dur a terme un control d'accés. A continuació es descriuen les tecnologies i les aplicacions que permeten fer una autenticació i autorització en entorns multiusua-

ri, els serveis de directori, l'autenticació única per a accedir als serveis, i la federació d'identitats. Finalment, es destaca la importància de la privadesa, i s'introdueixen les principals tècniques per a garantir-la.

Amb la finalitat de facilitar l'assoliment dels objectius d'aquesta assignatura, es combinen els continguts teòrics amb els pràctics. Es pretén que els estudiants adquireixin un coneixement suficient de les principals aplicacions i tecnologies.

Objectius

Aquesta assignatura conté els materials didàctics necessaris perquè l'estudiant adquireixi els objectius següents:

1. Comprendre què és l'autenticació de la identitat.
2. Conèixer les tècniques i els conceptes relacionats amb l'autenticació d'usuaris.
3. Conèixer les fases i les polítiques del control d'accés, i el funcionament dels principals tipus de control d'accés.
4. Assimilar les tecnologies que permeten fer una autenticació i una autorització en aplicacions multiusuari.
5. Comprendre el concepte i la utilitat d'un servei de directori, i el concepte d'*espai de noms*.
6. Conèixer les principals implantacions de serveis de directori.
7. Adquirir el concepte de *federació d'identitats*, els termes associats i la seva relació amb els diferents elements de la gestió de la identitat i l'accés.
8. Conèixer els mètodes i les tecnologies que permeten fer la federació d'identitats.
9. Entendre què és l'empremta digital d'un usuari, què conté, i com es crea.
10. Entendre el funcionament de les tècniques disponibles per a preservar la privadesa dels usuaris.

Continguts

Mòdul didàctic 1

Identificació, autenticació i control d'accés

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

1. Tècniques d'identificació i autenticació
2. Cicle de vida de la identitat digital
3. Control d'accés

Mòdul didàctic 2

Autenticació i autorització en aplicacions multiusuari

José María Palazón Romero

1. Autenticació i autorització en Java
2. Autenticació i autorització en PHP
3. Autorització i autenticació en aplicacions .NET

Mòdul didàctic 3

Serveis de directori

Antoni Martínez-Ballesté

1. Concepte i ús dels directoris
2. Disseny del directori
3. Implementacions de servei de directori

Mòdul didàctic 4

Single sign-on i federació d'identitats

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

1. La federació d'identitats
2. Estàndards
3. Tecnologia per a la gestió d'identitats federades

Mòdul didàctic 5

Privadesa

Alexandre Viejo Galicia i Jordi Castellà-Roca

1. L'empremta digital
2. Perfils d'usuari
3. Definició i polítiques de privadesa
4. Tècniques per a proporcionar privadesa

Bibliografia

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

Desmond, R. i altres (2008). *Active Directory: Designing, Deploying and Running Active Directory*. Sebastopol (Califòrnia): O'Reilly.

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

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

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

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

Stallings, W. (2008). *Computer security: principles and practice*. Upper Saddle River, (Nova 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 (Califòrnia): O'Reilly Media. ISBN 978-0596008789.

