novática
CEPIS UPGRADE Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software). ***Novática*** edita asimismo **UP**GRADE, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UP**ENET (**UP**GRADE *European* ***NET****work*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>
<http://www.upgrade-cepis.org/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2, ASTIC, RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Vía Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax.934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <http://www.ati.es/novatica/interes.html>, ATI Cataluña, ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Identidad indiscernible - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

Nº 202, noviembre-diciembre 2009, año XXXV

sumario

Monografía del próximo número: "*Informática y turismo*"

Presentación. Identifícate pero no reveles tu identidad

Javier López Muñoz[1], Miguel Soriano Ibáñez[2], Fabio Martinelli[3]

[1]Dpto. de Lenguajes y Ciencias de la Computación, Universidad de Málaga; [2]Dpto. de Ingeniería Telemática, Universidad Politécnica de Cataluña; [3]Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche - C.N.R. (Italia)

<jlm@lcc.uma.es>, <soriano@entel.upc.es>, <Fabio.Martinelli@iit.cnr.it>

Durante los últimos años, y a medida que han ido creciendo el número de aplicaciones y escenarios en Internet y la Web, así como el número de usuarios de todas las edades que hacen uso de los nuevos servicios que las anteriores proveen, el área de la administración de identidades digitales se ha convertido en uno de los principales retos a resolver para Administraciones, empresas, y ciudadanos.

A este reto hay que unir el hecho de que salvaguardar con unas mínimas garantías la privacidad de los individuos es una condición imprescindible para cualquiera de los escenarios en los que se lidie con las identidades digitales de los mismos. Encontrar soluciones que puedan hacer converger ambos aspectos no es trivial. Precisamente, esta monografía aborda esa problemática a través de una serie de artículos de sumo interés.

La monografía comienza con el trabajo "*Identidades digitales y tecnologías de gestión de identidad*", que se centra en tecnologías para servicios web y en la especificación WS-Federation, así como en sus especificaciones relacionadas. Aún no siendo ésta una familia de especificaciones tan madura como SAML (*Security Assertion Markup Language*), el autor argumenta los beneficios de su diseño modular y las ventajas que introduce respecto a SAML.

A continuación, el trabajo "*SWIFT - Servicios avanzados para la gestión de identidad*" presenta una infraestructura de gestión de identidad que permite a los usuarios acceder de modo anónimo a los servicios usando identidades virtuales y evita la trazabilidad de los usuarios por parte de terceras entidades.

En el artículo "*Métodos y técnicas del atacante para ocultar su identidad en la Red*", se describen tanto los primeros métodos como las técnicas más actuales empleadas por un atacante con el fin de proteger su identidad. Se señala, además, la necesidad de proporcionar anonimato a los usuarios de la red pero sin procurar nuevas vulnerabilidades que favorezcan a objetivos maliciosos.

Las leyes para la protección de la privacidad están en revisión para dar respuesta a los nuevos escenarios, y en el trabajo "*Privacidad... Protección a tres bandas*", la autora muestra que, en el marco actual, Administración y organizaciones son los dos agentes implicados en la protección del individuo, y argumenta que, dado el cambio de usos en la red, se hace necesario incluir un tercer agente, el mismo individuo, que asumiendo un rol más activo, haga efectiva la protección de la privacidad.

En el artículo "*¿Cómo medir la privacidad?*" se presentan distintas métricas utilizadas en privacidad, y se comparan usando conceptos de teoría de la información. Se revisa el estado del arte sobre métricas de privacidad en métodos con perturbación para el control estadístico de revelación. Aunque el artículo se enfoca en microagregación de datos, dichos métodos también son aplicables a una gran variedad de escenarios alternativos, tales como la ofuscación en servicios basados en la localización.

Por otro lado, en el artículo "*Gestión de la privacidad y el anonimato en el voto electrónico*" se pone de manifiesto cómo el requisito de privacidad entra en conflicto con la necesidad de saber que los votos han sido emitidos por votantes válidos, e introduce los mecanismos existentes para preservar la privacidad del votante en votaciones electrónicas sin comprometer la honestidad de la elección.

En el trabajo "*Identidad digital y privacidad en algunas TIC de nueva generación*" se describen los riesgos que entraña el uso de distintos servicios TIC como buscadores Internet, re-

Editores invitados

Javier López Muñoz es catedrático del Dpto. de Lenguajes y Ciencias de la Computación de la Universidad de Málaga, al que se incorporó en 1994. Ha dirigido diferentes proyectos nacionales y europeos en el área de Seguridad de la Información y de las Comunicaciones, incluyendo proyectos de los Programas Marco FP5, FP6 y FP7. Es co-editor jefe del *International Journal of Information Security* (IJIS), y representante español, en nombre de ATI, del IFIP *Technical Committee 11 on Security and Protection in Information Systems*. Además, es miembro de los consejos editoriales de, entre otras, las revistas con índice de impacto *Computers & Security*, *Computer Networks*, *Wireless Communications and Mobile Computing, Computer Communications*, *Journal of Network and Computer Applications*, y *International Journal of Communication Systems*.

Miguel Soriano Ibáñez obtuvo el grado de Doctor Ingeniero de Telecomunicaciones por la Universidad Politécnica de Cataluña (UPC), Barcelona, España, en 1996. Su actividad investigadora se inició en 1992 en el Departamento de Matemática Aplicada y Telemática de dicha universidad. Desde 2007 es catedrático de universidad en el Departamento de Ingeniería Telemática de la UPC, donde imparte y coordina los cursos de pregrado y de postgrado en Transmisión de Datos, Criptografía y Seguridad de la red y Comercio Electrónico. Por otra parte, también desde 2007, es investigador adscrito al CTTC (*Centre Tecnològic de Telecomunicacions de Catalunya*). Sus intereses de investigación actuales incluyen la información y la seguridad de red, incluyendo la protección de los derechos de autor. En los últimos 15 años ha participado en más de 30 proyectos de I+D nacionales e internacionales, con financiación pública (CICYT, DURSI, la Comisión Europea o CIRIT) o privada, siendo coordinador en 20 de ellos. Es co-autor de 3 libros, 2 patentes, más de 20 artículos en revistas JCR y más de 100 ponencias en congresos en el ámbito de la seguridad de la información.

Fabio Martinelli es investigador senior del *Istituto di Informatica e Telematica* del *Consiglio Nazionale delle Ricerche* (IIT-CNR) donde lidera el grupo de seguridad de la información. Es co-autor de más de un centenar de artículos internacionales de revistas y conferencias de relevancia. Sus principales temas de interés están relacionados con la seguridad y privacidad en sistemas distribuidos y móviles así como con los fundamentos de la seguridad y confianza. Fundó y dirigió (2005-2009) el grupo de trabajo "*Security and Trust Management* (STM)" del *European Research Consortium in Informatics and Mathematics* (ERCIM). También es miembro del grupo de trabajo 11.11 de la IFIP sobre Trust Management. Normalmente, lidera proyectos de investigación en el área de seguridad de la información y las comunicaciones, y está o ha estado implicado en los siguientes proyectos FP6-FP7: ARTIST2, BIONETS, CONNECT, CONSEQUENCE, GRIDtrust, S3MS, y SENSORIA.

des vehiculares, y servicios basados en localización para la privacidad de los usuarios. Asimismo, se describen las posibles contramedidas en estos tres ámbitos.

Finalmente, el trabajo "*Autenticación y privacidad en redes vehiculares*" se argumenta que a través de una red vehicular se puede efectuar un seguimiento electrónico del camino seguido por un vehículo y, por lo tanto, puede comprometerse la privacidad de sus ocupantes. Precisamente este artículo presenta los principales mecanismos que se han propuesto para implementar un compromiso entre identificación y privacidad.

Nota del Editor de Novática

Por razones de espacio no se han incluido en esta monografía de ***Novática*** los siguientes artículos: "*A Privacy Preserving Attribute Aggregation Model for Federated Identity Managements Systems*" de ***George Inman*** y ***David Chadwick***, "*The Importance of Context Dependant Privacy Requirements and Perceptions to the Design ïf Privacy Aware Systems*" de ***Aggeliki Tsohou***, ***Costas Lambrinoudakis***, ***Spyros Kokolakis*** y ***Stefanos Gritzalis***, y "*Enforcing Private Policy via Security-by-Contract*" de ***Gabriele Costa*** y ***Ilaria Matteucci***. Estos artículos han sido publicados en el número 1/2010 de **UP**GRADE en inglés <http://www.upgrade-cepis.org/>, y aparecerán en próximos números de ***Novática*** en castellano.

Referencias útiles sobre "Gestión de identidades y privacidad"

Las referencias que se citan a continuación, junto con las proporcionadas en cada uno de los artículos, tienen como objetivo ayudar a los lectores a profundizar en los temas tratados en esta monografía permitiendo contrastar ideas y obtener información actualizada.

Libros

■ **G. Williamson, D. Yip, I. Sharoni, K. Spaulding.** *Identity Management: A Primer.* Mc Press, 2009. ISBN-10: 158347093X.

■ **D. Birch.** *Digital Identity Management.* Ashgate Publishing, 2007. ISBN-10: 0566086794.

■ **D. Todorov.** *Mechanics of User Identification and Authentication: Fundamentals of Identity Management.* Auerbach Publications, 2007. ISBN-10: 1420052195.

■ **Geir M. Køien.** *Entity Authentication and Personal Privacy in Future Cellular Systems.* River Publishers, 2009. ISBN 978-87-92329-32-5.

■ **Acquisti, S. Gritzalis, C. Lambrinoudakis, S. di Vimercati (Editors).** *Privacy: Theory, Technologies, and Practices.* Auerbach Publications, 2007. ISBN-10: 1420052179.

■ **W. Diffie, S. Landau.** *Privacy on the Line: The Politics of Wiretapping and Encryption.* The MIT Press, 2007. ISBN-10: 0262042401.

Artículos e informes

■ **R. Morgan, S. Cantor, S. Carmody, W. Hoehn, K. Klingenstein.** "Federated Security: The Shibboleth Approach". *Educause Quarterly. Volume 27, Number 4*, 2004.

■ **INTECO.** "*Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*". <http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes Estudios_e_Informes_1/est_red_sociales_es>.

■ **T. El Maliki, J.M. Seigneur.** "A Survey of User-centric Identity Management Technologies", *International Conference on Emerging Security Information, Systems, and Technologies, 2007*, pp. 12–17.

■ **I. Antón, J. B. Earp, J. D. Young.** "How Internet Users' Privacy Concerns Have Evolved since 2002". *IEEE Security & Privacy*, pp. 21-27, enero 2010.

■ **F. H. Cate.** "Security, Privacy, and the Role of Law". *IEEE Security and Privacy, September/October 2009* (vol. 7 no. 5), pp. 60-63.

Proyectos y grupos de trabajo

■ **Proyecto Europeo PRIME** – "Privacy and Identity Management for Europe" <https://www.prime-project.eu/>.

■ **Proyecto Europeo PrimeLife** – "Bringing sustainable privacy and identity management to future networks and services" <http://www.primelife.eu/>.

■ **Proyecto Europeo PICOS** – "Privacy and Identity Management for Community Services". <http://www.picos-project.eu/>.

■ **IFIP Technical Committee 11** on *Security and Privacy Protection in Information Processing Systems.* <http://www.ifiptc11.org/>.

Sitios web

EPIC. Electronic Privacy Information Center, <http://epic.org/privacy/>.

The Privacy Center. <http://theprivacyplace.org/>.