

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 UPGRADE, revista digital de CEPIS (Council of European Professional Informatics Societies) en lengua inglesa, y es miembro fundador de UPENET (UPGRADE European Network).

<<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, AIZ, ASTIC, RITSI e Hispalinux, junto a la que participa en Prolnova.

Consejo Editorial

Joan Balle, Montserrat, Rafael Fernández Calvo, Luis Fernández Sanz, Javier López Muñoz, Alberto Lobel Ballori, Gabriel Martí Fuentes, Josep Moias i Bertran, José Onofre Montes Adame, Olga Pallás Codina, Fernando Pira Gómez (Presidente del Consejo), Ramon Puigjaner Trepal, Miquel Sarries Griño, Adolfo Vázquez Rodríguez, Asunción Yturbe Herranz

Coordinación Editorial

Llorenç Pagés Casas <pages@ati.es>

Composición y autocorrección

Jorge Llácer Gil de Rameles

Traducciones

Grupo de Lengua e Informática de ATI <<http://www.ati.es/gt/lengua-informatica/>>

Administración

Tomás Brunete, María José Fernández, Enric Camarero, Felicidad López

Secciones Técnicas - Coordinadores

Acceso y recuperación de la información

José María Gómez Hidalgo (Opennet), <jmgomez@yahoo.es>

Manuel J. María López (Universidad de Huelva), <manuel.maria@diesta.uhu.es>

Administración Pública electrónica

Francisco López Crespo (MAE), <flc@ati.es>

Arquitecturas

Enrique F. Torres Moreno (Universidad de Zaragoza), <enrique.torres@unizar.es>

Jordi Tubella Morgadas (DAC-UPC), <jordit@ac.upc.es>

Análisis STIC

Marina Tourño Troitín, <marinatourno@marinatourno.com>

Manuel Palao García-Suelto (ASIA), <manuel@palao.com>

Base de y tecnologías

Isabel Hernando Collazos (Fac. Derecho de Donostia, UPV), <isabel.hernando@ehu.es>

Elena Davara Fernández de Marcos (Davara & Davara), <edavara@davara.com>

Escuela Universitaria de la Informática

Cristóbal Paraja Flores (DSIC-UPV), <cparajaf@si.upv.es>

J. Angel Velázquez Irujibe (DLSI-URJC), <angel.velazquez@urjc.es>

Entorno digital personal

Andrés Marín López (Univ. Carlos III), <amarin@it.uc3m.es>

Diego Gachet Páez (Universidad Europea de Madrid), <gachet@uem.es>

Estándares Web

Encarnación Quesada Ruiz (Pez de Babel) <equesada@pezdebabel.com>

José Carlos del Arco Prieto (TCP-Sistemas e Ingeniería), <jcarco@gmail.com>

Exestión del Conocimiento

Juan Baiget Solé (Cap Gemini Ernst & Young), <juan.baiget@ati.es>

Informática y Filosofía

José Angel Olivas Varela (Escuela Superior de Informática, UCLM) <joseangel.olivas@uclm.es>

Kerim Gherab Martin (Kherab University), <kgherab@gmail.com>

Informática Jurídica

Miguel Chover Sellés (Universitat Jaume I de Castellón), <chover@lsi.uji.es>

Roberto Vivó Hernández (Eurographics, sección española), <rvivo@dstc.upv.es>

Inteligencia del Software

Javier Dolado Cosin (DLSI-UPV), <dolado@si.ehu.es>

Luis Fernández Sanz (Universidad de Alcalá), <luis.fernandez@uah.es>

Inteligencia Artificial

Vicente Botti Navarro, Vicente Julián Inglada (DSIC-UPV) <vbotti_vinglada@dsic.upv.es>

Información Persona-Computador

Pedro M. Latore Andrés (Universidad de Zaragoza, AIPO) <platore@unizar.es>

Francisco I. Gutierrez Vela (Universidad de Granada, AIPO) <fgutier@ugr.es>

Lengua e Informática

M. del Carmen Ugarte García (IBM), <cuarte@ati.es>

Lenguajes Informáticos

Oscar Geromonte Fernández (Univ. Jaime I de Castellón), <belfern@lsi.uji.es>

Inmaculada Coma Tatay (Univ. de Valencia), <inmaculada.coma@uv.es>

Lingüística computacional

Xavier Gómez Guinovart (Univ. de Vigo), <xgg@uvigo.es>

Manuel Palomar (Univ. de Alicante), <mpalomar@dlsi.ua.es>

Mundo estudiantil y jóvenes profesionales

Federico G. Mon Trotti (RITSI) <gnu.fede@gmail.com>

Mikel Salazar Peña (Área de Jóvenes Profesionales, Junta de ATI Madrid), <mikelxbo_uni@yahoo.es>

Práctica Informática

Rafael Fernández Calvo (ATI), <rfcalvo@ati.es>

Miquel Sarries Griño (Ayto. de Barcelona), <msarries@ati.es>

Redes y servicios telemáticos

José Luis Marzo Lázaro (Univ. de Girona), <joseluis.marzo@udg.es>

Germán Santos Boada (UPC), <german@ac.upc.es>

Seguridad

Javier Arellano Bertollín (Univ. de Deusto), <jarellito@eside.deusto.es>

Javier López Muñoz (ETSI Informática-UMA), <jlm@cc.uma.es>

Sistemas de Tiempo Real

Alejandro Alonso Muñoz, Juan Antonio de la Puente Alfaro (DIT-UPM), <galtonso_puente@dit.upm.es>

Software Libre

Jesús M. González Barahona (GSYC-URJC), <jgb@gsyc.es>

Israel Herráiz Tabernero (UCM), <herraiza@computer.org>

Tecnología de Objetos

Jesús García Molina (US-UM), <jmolina@um.es>

Gustavo Rossi (LUFIA-UNLP, Argentina), <gustavo@soi.info.unlp.edu.ar>

Tecnologías para la Educación

Juan Manuel Doderio Beardo (UC3M), <doderio@it.uc3m.es>

César Pablo Córcoles Briongo (UOC), <ccorcoles@uoc.edu>

Tecnologías y Empresa

Didac López Vilas (Universitat de Girona), <didac.lopez@ati.es>

Francisco Javier Cantais Sánchez (Indra Sistemas), <fjcantais@gmail.com>

Tendencias tecnológicas

Alonso Alvarez García (TID), <aad@tid.es>

Gabriel Martí Fuentes (Interbits), <gabi@atinet.es>

TIC y Turismo

Andrés Aguayo Maldonado, Antonio Guevara Plaza (Univ. de Málaga) <aguayo.guevara@lcc.uma.es>

UPGRADE

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
 Padilla 66, 3º dcha., 28006 Madrid
 Tfn. 914029391; fax. 913093685 <novatica@ati.es>

Composición, Edición y Redacción ATI Valencia
 Av. del Reino de Valencia 23, 46105 Valencia
 Tfn./fax 963330392 <secreval@ati.es>

Administración y Redacción ATI Cataluña
 Via Llatania 46, ppal. 1º, 08003 Barcelona
 Tfn. 934129235; fax. 934127113 <secrecat@ati.es>

Redacción ATI Aragón
 Lagasca 9, 3-B, 50006 Zaragoza
 Tfn./fax 976235161 <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
 Tfn. 914029391; fax. 913093685 <novatica@ati.es>

Impresión: Derra S.A., Juan de Austria 66, 08005 Barcelona

Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVACE

Partida: Identidad Indiferenciable - Concha Anas Pérez / © ATI

Diseño: Fernando Agresta / © ATI 2003

editorial

La protección de la privacidad personal en resumen

> 02

Confianza, elemento clave en el desarrollo de la Sociedad de la Información

> 02

Llorenç Pagés Casas

Noticias de IFIP

Nuevas Task Forces en IFIP

> 03

Ramón Puigjaner Trepal

monografía

Gestión de identidades y privacidad

(En colaboración con UPGRADE)

Editores invitados: *Javier López Muñoz, Miguel Soriano Ibáñez y Fabio Martinelli*

Presentación. Identifícate pero no reveles tu identidad

> 04

Javier López Muñoz, Miguel Soriano Ibáñez, Fabio Martinelli

Identidades digitales y tecnologías de gestión de identidad

> 06

Isaac Agudo Ruiz

SWIFT: Servicios avanzados para la gestión de identidad

> 12

Alejandro Pérez Méndez, Elena María Torroglosa García, Gabriel López Millán,

Antonio F. Gómez-Skarmeta, Joao Girao, Mario Lischka

Métodos y técnicas del atacante para ocultar su identidad en la Red

> 18

Guillermo Suarez de Tangil Rotaeché, Esther Palomar González,

Arturo Ribagorda Garnacho, Benjamín Ramos Álvarez

Privacidad... Protección a tres bandas

> 22

Gemma Déler Castro

¿Cómo medir la privacidad?

> 28

David Rebollo Monedero, Jordi Forné Muñoz

Gestión de la privacidad y el anonimato en el voto electrónico

> 33

Jordi Puiggalí Allepuz, Sandra Guasch Castelló

Identidad digital y privacidad en algunas TIC de nueva generación

> 38

Agustí Solanas, Josep Domingo-Ferrer, Jordi Castellà-Roca

Autenticación y privacidad en redes vehiculares

> 43

José María de Fuentes García-Romero de Tejada, Ana Isabel González-Tablas Ferreres,

Arturo Ribagorda Garnacho

secciones técnicas

Arquitecturas

En las nubes

> 49

Hannah Dee

Informática y Filosofía

La evaluación mediante el uso: reglas y prácticas

> 51

José Luis González Quirós

Lingüística Computacional

Un sistema de diálogo flexible para facilitar el uso de la Web

> 56

Marta Gatiús Vila, Meritxell González Bermúdez

Tecnología de Objetos

Propuestas para la captura de requisitos y el modelado de la interacción en el marco de MDA

> 61

Sergio España Cubillo, José Ignacio Panach Navarrete, Nathalie Aquino Salvioni,

Francisco Valverde Gromé, Oscar Pastor López

Referencias autorizadas

> 68

sociedad de la información

La Forja

Desarrollo del plugin

> 75

Israel Herráiz Tabernero

asuntos interiores

Coordinación Editorial / Programación de Novática / Socios Institucionales

> 77

Javier López Muñoz¹, Miguel Soriano Ibáñez², Fabio Martinelli³

¹Dpto. de Lenguajes y Ciencias de la Computación, Universidad de Málaga; ²Dpto. de Ingeniería Telemática, Universidad Politécnica de Cataluña; ³Istituto 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

Presentación. Identifícate pero no reveles tu identidad

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.

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 mé-

todos 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-

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 Management Systems" de **George Inman** y **David Chadwick**, "The Importance of Context Dependant Privacy Requirements and Perceptions to the Design of 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 **UPGRADE** 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. Kjøien.** *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 Shibolet 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/>>.