

UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <<http://www.upgrade-cepis.org/>>

Publisher

UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <<http://www.cepis.org/>>) by **Novática** <<http://www.ati.es/novatica/>>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*, <<http://www.ati.es/>>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by **Novática**

UPGRADE was created in October 2000 by CEPIS and was first published by **Novática** and **INFORMATIK/INFORMATIQUE**, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <<http://www.svifsi.ch/>>)

UPGRADE is the anchor point for UPENET (UPGRADE European Network), the network of CEPIS member societies' publications, that currently includes the following ones:

- **InfoReview**, magazine from the Serbian CEPIS society JISA
- **Informatica**, journal from the Slovenian CEPIS society SDI
- **Informatik-Spektrum**, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- **ITNOW**, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- **Mondo Digitale**, digital journal from the Italian CEPIS society AICA
- **Novática**, journal from the Spanish CEPIS society ATI
- **OCG Journal**, journal from the Austrian CEPIS society OCG
- **Pliroforiki**, journal from the Cyprus CEPIS society CCS
- **Tölvumál**, journal from the Icelandic CEPIS society ISIP

Editorial Team

Chief Editor: Llorenç Pagés-Casas

Deputy Chief Editor: Rafael Fernández Calvo

Associate Editor: Fiona Fanning

Editorial Board

Prof. Vasile Baltac, CEPIS President

Prof. Wolfried Stucky, CEPIS Former President

Hans A. Frederik, CEPIS Vice President

Prof. Nello Scarabottolo, CEPIS Honorary Treasurer

Fernando Piera Gómez and Llorenç Pagés-Casas, ATI (Spain)

François Louis Nicolet, SI (Switzerland)

Roberto Carniel, ALSI – Tecnoteca (Italy)

UPENET Advisory Board

Dubravka Dukic (InfoReview, Serbia)

Matjaz Gams (Informatica, Slovenia)

Hermann Engesser (Informatik-Spektrum, Germany and Switzerland)

Brian Runciman (ITNOW, United Kingdom)

Franco Filippazzi (Mondo Digitale, Italy)

Llorenç Pagés-Casas (Novática, Spain)

Veith Risak (OCG Journal, Austria)

Panicos Masouras (Pliroforiki, Cyprus)

Thorvardur Kári Ólafsson (Tölvumál, Iceland)

Rafael Fernández Calvo (Coordination)

English Language Editors: Mike Andersson, David Cash, Arthur Cook, Tracey Darch, Laura Davies, Nick Dunn, Rodney Fennemore, Hilary Green, Roger Harris, Jim Holder, Pat Moody.

Cover page designed by Concha Arias-Pérez

"Indiscernible Identity" / © CEPIS 2010

Layout Design: François Louis Nicolet

Composition: Jorge Llácer-Gil de Ramales

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>

Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at

<<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>>

Copyright

© Novática 2010 (for the monograph)

© CEPIS 2010 (for the sections UPENET and CEPIS News)

All rights reserved under otherwise stated. Abstracting is permitted with credit to the source. For copying, reprint, or republication permission, contact the Editorial Team

The opinions expressed by the authors are their exclusive responsibility

ISSN 1684-5285

Monograph of next issue (April 2010)

**"Information Technology
in Tourism Industry"**

(The full schedule of UPGRADE is available at our website)

- 2 Editorial: Serbian Publication *InfoReview* joins UPENET, the Network of CEPIS Societies Journals and Magazines
- 2 From the Chief Editor's Desk
New Deputy Chief Editor of UPGRADE

Monograph: Identity and Privacy Management (published jointly with Novática*)

Guest Editors: *Javier Lopez-Muñoz, Miguel Soriano-Ibañez, and Fabio Martinelli*

- 3 Presentation: Identify Yourself but Don't Reveal Your Identity — *Javier Lopez-Muñoz, Miguel Soriano-Ibañez, and Fabio Martinelli*
- 6 Digital Identity and Identity Management Technologies — *Isaac Agudo-Ruiz*
- 13 SWIFT – Advanced Services for Identity Management — *Alejandro Pérez-Méndez, Elena-María Torroglosa-García, Gabriel López-Millán, Antonio F. Gómez-Skarmeta, Joao Girao, and Mario Lischka*
- 21 A Privacy Preserving Attribute Aggregation Model for Federated Identity Managements Systems — *George Inman and David Chadwick*
- 27 Anonymity in the Service of Attackers — *Guillermo Suarez de Tangil-Rotaèche, Esther Palomar-González, Arturo Ribagorda-Garnacho, and Benjamín Ramos-Álvarez*
- 32 The Importance of Context-Dependent Privacy Requirements and Perceptions to the Design of Privacy-Aware Systems — *Aggeliki Tsohou, Costas Lambrinouidakis, Spyros Kokolakis, and Stefanos Gritzalis*
- 38 Privacy... Three Agents Protection — *Gemma Déler-Castro*
- 44 Enforcing Private Policy via Security-by-Contract — *Gabriele Costa and Ilaria Matteucci*
- 53 How Do we Measure Privacy? — *David Rebollo-Monedero and Jordi Forné*
- 59 Privacy and Anonymity Management in Electronic Voting — *Jordi Puiggalí-Allepuz and Sandra Guasch-Castelló*
- 66 Digital Identity and Privacy in some New-Generation Information and Communication Technologies — *Agustí Solanas, Josep Domingo-Ferrer, and Jordi Castellà-Roca*
- 72 Authentication and Privacy in Vehicular Networks — *José-María de Fuentes García-Romero de Tejada, Ana-Isabel González-Tablas Ferreres, and Arturo Ribagorda-Garnacho*

UPENET (UPGRADE European Network)

- 79 From **ITNOW** (BCS, United Kingdom)
ICT in Education
Enthusing Students — *Bella Daniels*
- 81 From **InfoReview** (JISA, Serbia)
Information Society
"Knowledge Society" is a European Educational Imperative that Should not Circumvent Serbia — *Marina Petrovic*

CEPIS NEWS

- 84 Selected CEPIS News — *Fiona Fanning*
- 86 Privacy-Consistent Banking Acquisition — *CEPIS Legal and Security Special Interest Network*

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <<http://www.ati.es/novatica/>>.

Presentation

Identify Yourself but Don't Reveal Your Identity

Javier Lopez-Muñoz, Miguel Soriano-Ibañez, and Fabio Martinelli

In recent years the number of Internet and Web applications and scenarios, and the number of users of all ages who make use of the new services that they provide, has been steadily growing. This growth has led to the field of digital identity management becoming one of the foremost challenges to be addressed by public administrations, enterprises and citizens.

In addition to this challenge, the provision of some guarantee regarding the privacy of individuals is a must for any scenarios involving digital identities. Finding solutions where both issues converge is no trivial task. This issue focuses precisely on this problem in a number of highly interesting papers.

The issue starts with the research work "*Digital Identity and Identity Management Technologies*", by **Isaac Agudo-Ruiz** which focuses on technologies for Web Services and the WS-Federation specification, together with related specifications. Although this technology is not as mature as SAML, the author shows how its modular design provides some advantages over SAML.

Next, the paper "*SWIFT – Advanced Services for Identity Management*", by **Alejandro Pérez-Méndez, Elena-María Torroglosa-García, Gabriel López-Millán, Antonio F. Gómez-Skarmeta, Joao Girao, and Mario Lischka**, presents an identity management framework to provide ad-

vanced services such as anonymity, authorization based on end-user attributes, and cross-layer SSO, designed to improve the usability and security of these systems by using virtual identities and preventing traceability by third-parties.

The third paper, "*A Privacy Preserving Attribute Aggregation Model for Federated Identity Managements Systems*", by **George Inman** and **David Chadwick**, addresses the fact that users are only able to use one or very few of their attributes to access a service, and provides a solution involving the aggregation of attributes from multiple IdPs before accessing a service. The authors describe some of the existing attribute aggregation models before introducing their own Linking Service model and its associated protocol mappings.

In the following article, "*Anonymity in the Service of Attackers*", by **Guillermo Suarez de Tangil-Rotaèche, Esther Palomar-González, Arturo Ribagorda-Garnacho** and **Benjamín Ramos-Álvarez**, traditional and state-of-the-art techniques used by the attackers in order to protect their identity are described. The authors also identify the need to provide anonymity to users of the Internet without creating new vulnerabilities that open the door to malicious intentions.

Also related to privacy, the article entitled "*The Impor-*



Skills Week

The Guest Editors

Javier Lopez-Muñoz is a Full Professor of the Computer Science Department at the *Universidad de Málaga*, Spain. He has managed various national and international projects in the area of Information and Communications Security, including projects from FP5, FP6 and FP7. He is the Co-Editor-in-Chief of *International Journal of Information Security (IJIS)* and the Spanish representative on the IFIP Technical Committee 11 on Security and Protection in Information Systems. He is also a member of the Editorial Board of, among others, the indexed journals *Computers & Security*, *Computer Networks*, *Wireless Communications and Mobile Computing*, *Computer Communications*, *Journal of Network and Computer Applications*, and *International Journal of Communication Systems*. He is a member of the Board of the Spanish society ATI (*Asociación de Técnicos de Informática*). <jlm@lcc.uma.es>.

Miguel Soriano-Ibañez received his Telecommunication Engineering degree and PhD from the *Universitat Politècnica de Catalunya (UPC)*, Barcelona, Spain, in 1992 and 1996, respectively. In 1992, he joined the Department of Applied Mathematics and Telematics of the UPC. Since 2007 he has been a lecturer at the UPC, where he teaches and coordinates undergraduate and graduate courses in Data Transmission, Cryptography and Network Security and E-commerce. Since

2007 he has been an associate researcher at CTTC (*Centre Tecnològic de Telecomunicació de Catalunya*). His current research interests include information and network security including information hiding for copyright protection. In the last 15 years he has participated in more than 30 national and international R&D projects, both publicly (CICYT, DURSI, European Commission or CIRIT) and privately funded, acting as the coordinator in 20 of them. He is the co-author of 3 books, 2 patents, more than 20 ISI-JCR papers and more than 100 conference papers in the field of information and network security. <soriano@entel.upc.es>.

Fabio Martinelli is a Senior Researcher at IIT-CNR, Italy, where he leads the information security group. He is the co-author of more than one hundred papers on international journals and conference/workshop proceedings. His main research interests centre on security and privacy in distributed and mobile systems and foundations of security and trust. He founded and chaired (2005-2009) the WG on security and trust management (STM) of the European Research Consortium in Informatics and Mathematics (ERCIM). He is also a member of the IFIP WG on trust management 11.11 (as academia/research liaison coordinator). He regularly manages R&D projects on information and communication security and he has played various roles in the following FP6-FP7 projects: ARTIST2, BIONETS, CONNECT, CONSEQUENCE, GRIDtrust, S3MS, SENSORIA. <Fabio.Martinelli@iit.cnr.it>.

tance of Context-Dependent Privacy Requirements and Perceptions to the Design of Privacy-Aware Systems", by **Aggeliki Tsohou**, **Costas Lambrinoudakis**, **Spyros Kokolakis** and **Stefanos Gritzalis**, draws upon security management tasks in order to highlight the gaps that need to be explored regarding privacy management, so as to be able to justifiably select the privacy enhancing technologies that meet a system's privacy requirements.

Laws for privacy protection to meet the requirements of new scenarios are currently under discussion, and in the paper "*Privacy: Three-way Agents*", where **Gemma Déler-Castro** describes how, in the present framework, public administrations and organizations are the two agents involved in protecting the individual. However, the author also argues that, because of changes in the use of networks, a third agent, the individual, needs to play a more active role in effective privacy protection.

In their paper "*Enforcing Private Policy via Security-by-Contract*", the authors, **Gabriele Costa** and **Ilaria Matteucci**, adopt the Security-by-Contract approach to ensure that the application implementing the communication interface is always safe; i.e., it satisfies the security policies set by its components. The authors also present an extension of the Security-by-Contract for dealing with trust. Trust management is useful when one of the involved actors is considered to be potentially untrusted and the others want to measure its trust level.

In the research work "*How Do we Measure Privacy?*", **David Rebollo-Monedero** and **Jordi Forné** present the state-of-the-art on privacy metrics in perturbative methods for

statistical disclosure control and compare recent criteria for privacy based on information-theoretic concepts. While the focus of these metrics is on data microaggregation, these methods also address a wide variety of alternative applications such as obfuscation in location-based services.

The paper "*Privacy and Anonymity Management in Electronic Voting*", by **Jordi Puiggali-Allepuz** and **Sandra Guasch-Castelló**, emphasizes the trade-off between privacy and verifying the eligibility of voters to ensure election integrity. The authors introduce security mechanisms and techniques to preserve voter privacy without compromising election integrity.

The article "*Digital Identity and Privacy in some New-Generation Information and Communication Technologies*", by **Agustí Solanas**, **Josep Domingo-Ferrer** and **Jordi Castellà-Roca**, describes the threats related to the identity of ICT users, and summarizes the countermeasures that can be applied in three especially important areas: Internet search engines, vehicular networks, and location-based services.

Finally, in the paper "*Authentication and Privacy in Vehicular Networks*", **José-María de Fuentes García-Romero de Tejada**, **Ana-Isabel González-Tablas Ferreres** and **Arturo Ribagorda-Garnacho** argue that data interchange in vehicular network could lead to tracking, and so user privacy may be compromised. The article presents the most widely accepted mechanisms used to achieve an optimal identification-privacy trade-off in systems aimed at achieving a better road safety.

As usual we have included at the end of this presenta-

tion a number of references (books, websites, articles, reports and projects) for those **UPGRADE** readers who may wish to gain a deeper knowledge of the subject matter covered in this monograph, that we hope will be of interest for non-specialized readers too.

To close this presentation, we want to express our sincerest gratitude to the authors for their valuable papers and to editorial teams of **UPGRADE** and **Novática** for the opportunity given to us of publishing this monograph.

Useful References on "Identity and Privacy Management"

These links and references, together with the ones available in each of the papers of this issue, may help the reader to go further into the knowledge of the matter covered by this monograph.

Books

- G. Williamson, D. Yip, I. Shari, 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. Lambrinouidakis, 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.

Articles and Reports

- R. Morgan, S. Cantor, S. Carmody, W. Hoehn, K. Klingenstein. "Federated Security: The Shibboleth Approach". Educause Quarterly. Volume 27, Number 4, 2004.
- Inteco/APD (Spanish Institute of Communications Technologies/Spanish Data Protection Agency). "Study on

the Privacy of Personal Data and on the Security of Information in Social Networks". Feb. 2009. <<http://www.inteco.es/file/vuiNP2GNuMjfCgs9ZBYoAQ>>.

- 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, January 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.

Projects and Work Groups

- European Project PRIME (Privacy and Identity Management for Europe). <<https://www.prime-project.eu/>>.
- European Project PrimeLife (Bringing sustainable privacy and identity management to future networks and services). <<http://www.primelife.eu/>>.
- European Project 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/>>.

Web sites

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