Identity and Privacy Management

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-Maria Torroglosa-García, Gabriel López-Millán, Antonio F. Gómez-Skarmeta, Joao Girao, and Mario Lischka, presents an identity management framework to provide advanced 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 Management 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-Rotaeche, Esther Palomar-González, Arturo Ribagorda-Garnacho and Benjamin Ramos-Alvarez, 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-
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 (IJS) 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 Soria-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>.

For the design of privacy-aware systems, the authors, Aggeliki Tsohou, Costas Lambrinoudakis, Spyros Kokolakis and Stefanos Gritzalis, draw up 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 Dèler-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 Puiggalí-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 Next-Generation Information and Communication Technologies", by Agusti 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-
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

Articles and Reports

Projects and Work Groups

Web sites