Requirements Eng (2011) 16:1–2
DOI 10.1007/s00766-011-0117-0

EDITORIAL

Digital privacy: theory, policies and technologies

Annie I. Anton · Travis D. Breaux · Stefanos Gritzalis · John Mylopoulos

Published online: 3 February 2011
© Springer-Verlag London Limited 2011

1 Digital privacy: theory, policies and technologies

Information and communication technologies (ICT) continue to evolve at a remarkably high pace. As a result, more individuals use ICT at work and at home, carrying out routine daily tasks such as on-line shopping, banking and social interaction. Unfortunately, increased use of ICT has resulted in increased risk that individuals' privacy rights will be violated. These risks to privacy include violations of user anonymity during sensitive transactions, unauthorized disclosures of personal data, misuse of personal data for unauthorized purposes, misrepresentation of personal character and more.

To comply with privacy laws, regulations and policies, we need to develop techniques for identifying, documenting and testing privacy requirements that are feasible and efficient to implement. Moreover, developers need to update their software processes to ensure that privacy is not an afterthought whereby privacy measures become an add-on or employed in an ad hoc or arbitrary fashion. Finally, organizations that manage personal information must integrate privacy-enabled technologies and processes into their business practices to comply with emerging legislation.

This special issue of the Springer's *Requirements Engineering* journal aims at providing researchers and professionals with insights into the state-of-the-art in Digital Privacy from the views of Theory, Policies and Technologies.

2 The content of this special issue

The papers presented in this special issue contribute to the aforementioned research directions. The four papers presented in this special issue have been selected following a thorough review process of 16 submissions that responded to the Call for Papers which was distributed. Each of the papers was reviewed by at least three reviewers, with a range from three to five reviewers, in two review stages.

In their paper entitled '*A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements*', M. Deng, K. Wuyts, R. Scandariato, B. Preneel and W. Joosen provide a framework to model privacy threats in software-based systems, which includes a systematic methodology to model privacy-specific threats. The methodology instructs the analyst on what issues should be investigated and where in the model those issues

A. I. Anton
College of Engineering, Computer Science Department,
North Carolina State University, Raleigh, NC, USA
e-mail: anton@csc.ncsu.edu
URL: http://www4.ncsu.edu/~aianton/

T. D. Breaux
Institute for Software Research, Carnegie Mellon University,
Pittsburg, PA, USA
e-mail: breaux@cs.cmu.edu
URL: http://www.cs.cmu.edu/~breaux/

S. Gritzalis (✉)
Laboratory of Information and Communication Systems
Security, Department of Information and Communication
Systems Engineering, University of the Aegean,
83200 Karlovassi, Samos, Greece
e-mail: sgritz@aegean.gr
URL: http://www.icsd.aegean.gr/sgritz

J. Mylopoulos
Department of Computer Science,
University of Toronto, Toronto, ON, Canada
e-mail: jm@cs.toronto.edu
URL: http://www.cs.toronto.edu/~jm/

could emerge. This is achieved by (1) defining a list of privacy threat types and (2) providing the mappings between threat types and the elements in the system model. Additionally, the paper provides an extensive catalogue of privacy-specific threat tree patterns that can be used to detail the threat analysis outlined above. Finally, this work provides the means to map the existing privacy-enhancing technologies to the identified privacy threats.

J. D. Young in her paper entitled '*Commitment Analysis to Operationalize Software Requirements from Privacy Policies*' presents a methodology for obtaining requirements from privacy policies based on a theory of commitments, privileges and rights, which was developed through a grounded theory approach. This methodology was developed from a case study in which software requirements were derived from 17 healthcare privacy policies. The contribution of the paper is significant for users, organizations and system analysts. Users need to understand privacy policies in order to know how their personal information is being collected, stored, used and protected. Organizations need to ensure that the commitments they express in their privacy policies reflect their actual business practices, especially in the United States where the Federal Trade Commission regulates fair business practices. Requirements engineers need to understand the privacy policies to know the privacy practices with which the software must comply and to ensure that the commitments expressed in these privacy policies are incorporated into the software requirements. Among the findings, this research concludes that legal-based approaches do not provide sufficient coverage of privacy requirements because privacy policies focus primarily on procedural practices rather than on legal practices.

The paper by E. Kosta, C. Kalloniatis, L. Mitrou and E. Kavakli, '*The 'Panopticon' of Search Engines: The Response of the European Data Protection Framework*', examines the applicability of the European data protection legislation to non-EU-based search engine providers and studies the main privacy issues with regard to search engines, such as the character of search logs, their anonymization and their retention period. The increasing importance of search engines for the location of desired information on the Internet usually leads to considerable inroads into the privacy of users. The authors present the current debate in Europe regarding whether search engine providers that are established outside the European Union are covered by the European data protection framework and the obligations it imposes on entities that process personal data and present Ixquick, a privacy-friendly meta-search engine as an alternative to privacy intrusive existing practices of search engines.

In their paper '*A Methodology for Security Assurance Driven Development*', J. L. Vivas, I. Agudo and J. Lopez introduce an assurance methodology that integrates assurance case creation with system development. The methodology has been developed in order to provide trust and privacy assurance to the evolving European project PICOS Privacy and Identity Management for Community Services. This research project focused on mobile communities and community-supporting services, with special emphasis on aspects such as privacy, trust, and identity management. The leading force behind the approach is the ambition to develop a methodology for building and maintaining security cases throughout the system development life cycle in a typical system engineering effort, when much of the information relevant for assurance is produced and feedback can be provided to system developers. The paper also presents the first results of the application of the methodology to the development of the PICOS platform.

Acknowledgments We would like to thank a number of people that contributed to the preparation of this special issue. First, we would like to thank Professor P. Loucopoulos and Professor W. Robinson, *Requirements Engineering* Editors-in-Chief, for giving us the opportunity to prepare this special issue. In addition, we would like to thank numerous reviewers for their professional effort to select the articles to reflect the essence of this special issue and all authors for their contributions and for undertaking two-cycle revision of their manuscripts.