Computer Standards & Interfaces 36 (2014) 687–688

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Editorial

# Security in information systems: Advances and new challenges

Information Systems Security is one of the most pressing challenges currently confronted by all kinds of organizations. Information systems undoubtedly play an important role in today's society and are increasingly at the heart of critical infrastructures. Although many companies have discovered how critical information is to the success of their business or operations, very few have managed to be effective in maintaining their information secure, avoiding unauthorized access, stopping intrusions, preventing the disclosure of secret information, etc. In any computer-related environment, it is possible to consider security as a non-functional requirement that maintains the overall system usable and reliable, and protects the information and information systems. There are various definitions of security, but all of them basically agree on the same components. Security in information systems considers the protection of information and the systems that manage it against a wide range of threats in order to ensure business continuity, minimize risks and maximize the return on investment and business opportunities. Security is, therefore, currently a widespread and growing concern that covers all areas of society: business, domestic, financial, government, and so on. In fact, the so-called information society is increasingly dependent on a wide range of software systems whose mission is critical, such as air traffic control systems, financial systems or public health systems. The potential losses confronted by the businesses and organizations that rely on all of these systems, be they hardware or software, therefore signify that it is crucial for information systems to be properly secured from the outset.

This Special Issue of the Computer Standards & Interfaces journal therefore includes papers received from the public call for papers and extended and improved versions of those papers that were selected from the best of the International Workshop on Security in Information Systems (WOSIS 2012). It aims to serve as a forum in which to unite academics, researchers, practitioners and students in the field of security engineering and security software engineering, by presenting new developments and lesson learned from real world cases, and to promote the exchange of ideas, discussion and development in these areas.

This edition is the ninth in a series which began in Ciudad Real (Spain) in 2002, and which has continued, in chronological order, in Porto (Portugal), Paphos (Cyprus), Miami (USA), Funchal, Madeira (Portugal), Barcelona (Spain), Milan (Italy), Beijing (China) and Wroclaw (Poland). The workshop has gained a considerable reputation as a result of its relatively long history, and receives an annual average of almost fifty submissions, with an acceptance rate of approximately thirty five percent.

Our workshop has matured throughout the years of its existence, and is now established as a forum for high quality research papers in the area of security in information systems. The most valuable assets of this workshop, which make it attractive to authors, are both the highly exclusive set of program committee members (comprising 44 members of 14 nationalities), and the invitations extended to exceptional speakers of great renown in this scientific area (Yvo Desmedt, Sushil Jajodia, Ernesto Damiani, Leonardo Chiariglione, Ruth Breu, Eduardo B. Fernández, Sabrina De Capitani and Christos Kalloniatis). Selections of the best papers from past editions of the workshop have, moreover, been published in international journals such as Information Systems Security, Journal of Research and Practice in Information Technology, Internet Research, Journal of Universal Computer Science and Computer Standards and Interfaces.

This special issue includes nine papers of interest within the wide spectrum of research into the area of Information Systems Security. Four of them have been selected as the best papers to be presented in the workshop, and the remaining papers are from the public call. There is a predominance of theoretical papers, which is principally focused on security engineering, security patterns, security policy, trust, authentication, privacy and security requirements, but there is also an important sample of papers which contributes to the area of software engineering security. This reaffirms the importance of both research disciplines in the scientific community, and confirms the growth in the secure software engineering discipline as a clear integration of security engineering and software engineering. A brief introduction to each of the papers selected is presented in the following paragraphs.

The first contribution, "End-to-End Policy Based Encryption Techniques for Multi-Party Data Management", by M. Beiter et al., proposes a method that can be applied in order to improve the privacy of sensitive information in cloud applications. The method is a user-centric data control and involves machine-readable policies that are attached to data in order to define allowed usage and obligations, and to travel among multiple parties.

The second paper, entitled "Mutual Authentication in Self-Organized VANETs", by C. Caballero-Gil et al., is focused on vehicular networks and defines a self-organized method of authentication for VANETs in which each node can choose its public key certificates and certifies public keys from other nodes. This method can be used for several applications, such as those for traffic conditions, and can be applied using existing devices (such as smartphones).

The third paper, "Secure Tropos Framework for Software Product Lines Requirements Engineering", by D. Mellado et al., investigates the definition of security requirements for software product lines. In this work, the authors consider a goal-driven technique, Secure Tropos, and extend it to specify security requirements by considering the specific characteristics of SPLs in order to develop a framework called SecureTropos-SPL.

The fourth contribution, entitled "Securing Business Processes using Security Risk-oriented Patterns", by N. Ahmed and R. Matulevicius, is

0920-5489/$ – see front matter 
http://dx.doi.org/10.1016/j.csi.2013.12.003

also focused on considering security aspects in the early stages of information systems development. The authors propose a method with which to model business processes within security aspects. This goal is achieved by defining security risk-oriented patterns using the BPMN notation.

The fifth paper, entitled "An Extensible Pattern-based Library and Taxonomy of Security Threats for Distributed Systems", by A.V. Uznov and E.B. Fernandez, studies the incorporation of security features during the development of a distributed system which requires a sound analysis of potential attacks or threats in various contexts, a process that is often termed as "threat modeling". The authors combine the values of threat libraries and taxonomies and propose an extensible, two-level "pattern-based taxonomy" for distributed systems, in addition to proposing a simple and effective method with which to construct pattern-based threat taxonomies for more specific system types and/or technology contexts by specializing one or more threat patterns.

The sixth contribution, "Enterprise Security Pattern: A Model-Driven Architecture Instance", by S. Moral-García et al., presents various instances of the solution models for the Secure SaaS enterprise security pattern in an attempt to discover the risks that an organization would incur if each of the instances was to be deployed. This new pattern is defined to provide an instance of model-driven architecture, which offers a solution to recurring problems related to Information Systems Security.

The seventh paper, entitled "Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts", by C. Kalloniatis et al., discusses a number of security and privacy properties that are applicable to the cloud, and it provides a clear linkage between those properties and relevant security and privacy threats. The authors also provide set of requirements for any development methodology that supports analysis and design of security and privacy in the cloud.

The eighth contribution, "Specifying Model Changes with UMLchange to Support Security Verification of Potential Evolution", by S. Wenzel et al., presents a proposal for modeling changes in UML models. They are focused on checking that the security properties specified in models are preserved in the different evolutions of the original model. The authors of this paper define their own notation for representing changes (UMLchange), and use UMLsec to represent security constraints. They also present a tool and evaluate their proposal with professionals from a real enterprise.

Finally, the ninth contribution, "Building Trust from Context Similarity Measures", by C. Fernandez-Gago et al., has the objective of establishing trust in computational settings by following a similar approach to that adopted by users in social settings. These authors are interested in discovering which users are similar to a given one in a specific context in an online community. This similarity between users is followed to define a function with which to derive trust. This similarity network is then used as a basis to define a trust model that also allows trust to be established along a path of entities.

We would like to thank Professor Barbara Carminati (Editor-in-Chief), Snigdha Satapathy and Prince Ebenezer (Journal Managers) from the Computer Standard and Interfaces Journal for their invaluable help and support, and for giving us the opportunity to edit this special issue. We are also extremely grateful for the hard work and kindness of all the members of our international program committee when performing their timely, complete and professional reviews. Last, but by no means least, we would like to thank the authors for their contributions.

Carlos Blanco*
*GSyA Research Group, Institute of Information Technologies and Systems, University of Cantabria, Santander, Spain*
*Corresponding author at: GSyA Research Group, Institute of Information Technologies and Systems, University of Cantabria. Faculty of Sciences Dep. of Mathematics, Statistics and Computer Science Av de los Castros s/n. 39071. Santander, Spain.
*E-mail address:* Carlos.Blanco@unican.es.

David G. Rosado
*GSyA Research Group, Institute of Information Technologies and Systems, University of Castilla-La Mancha, Ciudad Real, Spain*
*E-mail address:* David.GRosado@uclm.es.

Luis Enrique Sánchez
*Sicaman-NT, Departament of R + D, Spain*
*E-mail address:* lesanchez@sicaman-nt.com.

Jan Jürjens
*Technical University of Dortmund, Germany*
*E-mail address:* jan.jurjens@cs.tu-dortmund.de.