Volume 30, Issue 6, August 2008

ISSN: 0920-5489

ELSEVIER

COMPUTER STANDARDS & INTERFACES

SPECIAL ISSUE

State of Standards in the Information Systems Security Area

Guest Editors: Eduardo Fernández-Medina and Mariemma I. Yagüe

The International Journal on the Development and Application of Standards for Computers, Software Quality, Data Communications, E-topics, Interfaces and Measurement

COMPUTER STANDARDS & INTERFACES (CS&I)

The International Journal on the Development and Application of Standards for Computers, Software Quality, Data Communications, Interfaces and Measurement

---

Aims and scope

The quality of software, well-defined interfaces (hardware and software), the process of digitalisation, and accepted standards in these fields are essential for building and exploiting complex computing, communication, multimedia and measuring systems. Standards can simplify the design and construction of individual hardware and software components and help to ensure satisfactory interworking.

COMPUTER STANDARDS & INTERFACES is an international journal dealing specifically with the topics below.

The journal:

- provides information about activities and progress on the definition of computer standards, software quality, interfaces and methods, at national, European and international levels
- publishes critical comments on standards and standards activities
- disseminates user's experiences and case studies in the application and exploitation of established or emerging standards, interfaces and methods
- offers a forum for discussion on actual projects, standards, interfaces and methods
- stimulates relevant research by providing a specialized refereed medium.

COMPUTER STANDARDS & INTERFACES is concerned with the specification, development and application of standards and with high-level publications of developments and methods in the following areas:

- ***Standards, Information Management, Formal Methods*** - Computers, Processors, Storage, Operating systems, Languages, Databases, Graphics, User interface, Multimedia, Information security, Office automation, Development of standards and instruments, Applications
- ***Software Quality, Software Process*** - Languages, Operating systems, Programming, Requirements specification, Design & implementation, Inspection & test, Maintenance, Product and process evaluation, Performance, Tools, Metrics, Embedded systems, Software in measurement and technical systems including real-time aspects, Development of International Standards in Software Engineering
- ***Distributed Systems, Open Systems, E-Topics*** - Digital interfaces, System and device buses, Fieldbuses, Data communication, Distributed computing, Protocols, Open systems interconnection, Local and wide area networks, Internet, Worldwide Web; Network security, Cryptology, E-services, E-business, E-commerce
- ***Data Acquisition*** - Analog-to-digital conversion, Specification, Modelling, Industrial electronics, Real-time systems, Laboratory automation, Automatic measurement, Process control, Electromagnetic compatibility
- ***Digital Instruments Standardization*** - Forum of EUPAS, European Project for ADC-based devices Standardisation (IMEKO TC-4 Working Group on A/D and D/A Converter Metrology), IEEE TC-10, IEC TC-42/WG8, IEC TC-85/WG16; Standardisation of specifications, modelling, testing, and analog and digital processing for digital instruments

The last issue of a volume includes an Author index and a Subject index.

CS&I also covers general topics concerning the standardization process, such as technical, political and commercial aspects of standards, their impact on the marketplace, cost/benefit analyses, legislative issues, and relationships among national and international standards bodies.

COMPUTER STANDARDS & INTERFACES
Volume 30/6

ELSEVIER

Amsterdam • Boston • Jena • London • New York • Oxford • Paris •
Philadelphia • San Diego • St. Louis

Printed in Printforce, Alphen a/d Rijn, The Netherlands

♾ The paper used in this publication meets the requirements of ANSI/NISO 239.48-1992 (Permanence of Paper)

COMPUTER STANDARDS & INTERFACES

Special Issue:

State of standards in the information systems security area

Guest Editors:

Eduardo Fernández-Medina
Mariemma I. Yagüe

Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 30 (2008) 339–340
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

Guest Editorial

State of standards in the information systems security area

The development and use of standards in information technologies, and in particular, in the area of security, have grown up in the last years. The main reason is the increasing need for interoperability due to the new scenarios (e.g. collaborative work, heterogeneous IT processes and systems) that have emerged on the Web.

As standards represent an important means of achieving interoperability on the WWW and the Web has become a new global platform, the scientific community focuses its attention on the different international standards bodies and organizations, such as the National Institute of Standards and Technology (NIST), the International Standard Organization (ISO), the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE), the International Telecommunication Union (standardization section — ITU-T), the Organization for the Advancement of Structured Information Standards (OASIS), the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), etc. Not only specifications from these organisms become standards but also recommendations from very representative consortiums, such as the Object Management Group (OMG) become de facto standards as well.

These standards and specifications are crucial in many areas related to security in information systems. First of all, standards are important for unifying security techniques in different aspects, such as security protocols, cryptography, access control, authentication, privacy, integrity, attack detection, availability, personal data protection, etc. Secondly, an organizational view of security is very relevant too. Therefore, standards also reach this approach through the definition of security management systems, security maturity models, risk management guidelines, and so on. Nevertheless, standards are intensively considered in software engineering processes for developing information systems, and these standards are constantly redefined and extended in order to incorporate security into the software development. In this sense, standards and specifications define software modeling techniques, requirement engineering techniques, architecture languages and specifications, pattern definitions, life cycles models, software development methodologies, metamodeling techniques, etc., and also many specific technologies, with specific security requirements, such as Web services, grid computing, mobile devices, etc.

This Special Issue of the International Journal of Computer Standards and Interfaces includes a selection of the most representative papers presented at the Fifth International Workshop on Security in Information Systems (WOSIS 2007), which was held in Funchal, Madeira — Portugal, June 12–13, 2007. This edition of the workshop has been specially oriented to standards for security in information systems, obtaining a representative sample of the existing papers dealing with security and where standards fulfill a relevant role.

Our workshop has matured year by year, and it is established as a forum for high quality research papers in the area of security in information systems. The most valuable assets of this workshop to be attractive for authors are a very exclusive set of program committee members, along with the invitation of exceptional speakers, highly relevant in this scientific area. Among them, we can mention, for example, Yvo Desmedt, Sushil Jajodia, Ernesto Damiani, Leonardo Chiariglione, and Ruth Breu. Additionally, selections of the best papers of past editions of the workshop have been published in international journals such as Information Systems Security, Journal of Research and Practice in Information Technology, and Internet Research.

In the following paragraphs, a brief introduction to each selected paper will be stated.

The first contribution by Soler et al., presents an extension to the CWM (Common Warehouse Metamodel) specification developed by the OMG (Object Management Group) with the aim of specifying security in data warehouse models at the PSM (Platform Independent Model) level of the Model Driven Architecture. In this paper, standards such as UML, CWM, MOF, QVT, MDA are intensively used in the area of software engineering, with the purpose of integrating security into the development of data warehouses.

The second contribution by Tafreschi et al., deals with a reputation system, which, on the one hand, facilitates trust building among business partners who interact in an ad hoc manner with each other, and on the other hand enables market participants to rate the business performance of their partners as well as the quality of the offered goods. In this proposal, many types of standards and specifications, such as HTTP, XML, SOAP and WSDL are directly and indirectly used for the definition of the system architecture.

The third paper by Mellado et al., states a security standard-based process for software product line development. The proposal is a contribution in the area of security requirements engineering for software product lines, but providing its integration

0920-5489/$ - see front matter
doi:10.1016/j.csi.2008.03.001

with the Common Criteria (ISO/IEC 15408), as well as with some of the most relevant standards related to security management, such as ISO/IEC 17799 and ISO/IEC 27001. This proposal also conforms to IEEE 830-1998, regarding software requirements specification.

The fourth manuscript by Agreiter et al., puts forward a framework that provides fair non-repudiation for Web services messages, since there is not any sophisticated standard specifying this requirement for this environment. However, the paper deals with several standards, specifications, and protocols, such as UML, XML, SOAP, SSL, WSS, TTP, XACML, etc.

The fifth contribution, by Damiani et al., specifies a general query rewriting technique to securely query XML, the standard for data interchange. The proposed model is described by a Deterministic Finite Automata and is able to rewrite unsafe queries into safe ones, avoiding the many backtrackings inherent to non-deterministic finite automata. The proposed technique is linear with the size and depth of the repository schema.

The sixth contribution, by Plößl and Federrath, deals with security requirements of vehicular ad hoc networks (VANET). Nodes (mainly vehicles) are expected to communicate by means of the North American DSRC standard that makes use of the IEEE 802.11p standard for wireless communication. Authors evaluate some requirements such as message integrity and non-repudiation as well as propose a security infrastructure meeting all requirements, specially designed to protect privacy of the VANET users and efficient in terms of computational needs and bandwidth overhead.

The seventh contribution, by Canfora and Visaggio, refers to privacy preservation in highly dynamic, untrustworthy and scalable contexts, implementing the paradigm of front end trust filter. Therefore, the proposed solution makes the assumption that a privacy policy can be expressed at least at three different levels of detail, so-called layers, in other words, the statement of the policy, the strategies for realizing such policy and the implementation, which applies the strategy at the level of applications and database. This three-layered structure confers a high degree of flexibility.

The eighth contribution, by Zych, et al., studies the key management problem of the data-centric protection model, where data is cryptographically protected and allowed to be outsourced or even freely float on the network. Namely, when data is encrypted, the access control policies have to be taken into account so that control regulating what users are allowed to access to what data is maintained. Authors propose an efficient method that eliminates, as compared to broadcast encryption methods, the need for multiple copies of data keys and reduces to a single key the storage required per user. The solution is based on the Diffie–Hellman Key Exchange protocol, standardized by the RSA Laboratories as the Diffie–Hellman Key Agreement Standard.

The ninth contribution, by Sánchez, et al., is focused on the authorization problem. It shows how the eduroam user federation for an inter-NREN network roaming service based on AAA servers and the IEEE 802.1X standard can take advantage of the use of authorization services with the objective of offering a more grained network access control process. For that purpose, this work presents how eduroam can be extended with the NAS-SAML infrastructure and eduGAIN. The first is a network access control approach based on the AAA architecture and authorization attributes and the SAML and XACML standards. Secondly, the main goal of eduGAIN is to build an interoperable authentication and authorization infrastructure to interconnect different existing federations.

The tenth paper by Prandini and Ramilli proposes a communication scheme for remote system administration aimed at overcoming some intrinsic security issues of the traditional client–server models. While the subject of system administration has not been the subject of a comprehensive standardization activity, this proposal provides a viable alternative to de facto standards in the area of remote access such as SSH (RFC4250–4254), IPSec (RFC4301–4303 and related ones). Furthermore, it is related to the general problem of authentication and access control as defined in ISO/IEC 10181-2/3. The proposed system is based on human-oriented meeting places such as IRC (RFC2810–2813), but future extensions can foresee the design of more structured distributed meeting places, for instance, those in accordance with the CORBA Security Service definition.

This Special Issue does not try to cover all applications of security standards in information systems, since it would be impossible. However, we hope to offer a good sample of papers to show how important the use and development of standards for information technologies, and particularly to security are.

We would like to gratefully acknowledge the hard work and kindness of all members of our international program committee when performing their timely, complete and professional reviews. We would like to thank Sabrina De Capitani di Vimercati (Italy), Ernesto Damiani (Italy), Csilla Farkas (USA), Eduardo B. Fernández (USA), Steven Furnell (UK), Christian Geuer-Pollmann (Germany), Paolo Giorgini (Italy), Ehud Gudes (Israel), Carlos Gutiérrez (Spain), Haralambos Mouratidis (England), Jan Jürjens (Germany), Stamatis Karnouskos (Germany), Antonio Maña (Spain), Martin Olivier (South Africa), Brajendra Panda (USA), Günther Pernul (Germany), Mario Piattini (Spain), Joachim Posegga (Germany), Indrajit Ray (USA), Indrakshi Ray (USA), Damian Sauveron (France), Ambrosio Toval (Spain), Rodolfo Villarroel (Chile), and Duminda Wijesekera (USA).

Finally, we would like to thank Computer Standards & Interfaces and Elsevier, and particularly Professor Bhavani Thuraisingham for giving us the opportunity to publish this Special Issue.

Eduardo Fernández-Medina
ALARCOS Research Group,
Information Systems and Technologies Department,
University of Castilla-La Mancha, Paseo de la Universidad 4,
13071 Ciudad Real, Spain
Corresponding author.
E-mail address: Eduardo.FdezMedina@uclm.es.

Mariemma I. Yagüe
GISUM Research Group, Department of Computer Science
Málaga University Campus Universitario de Teatinos,
s/n 29071 Málaga, Spain
E-mail address: mariemma@lcc.uma.es.

:OMPUTER STANDARDS & INTERFACES
'he International Journal on the Development and Application of Standards for Computers, Software)uality, Data Communications, E-topics, Interfaces and Measurement

'ublication information

:omputer Standards & Interfaces (ISSN 0920-5489). For 2008 volume 30 (6 issues) is scheduled for ublication. Subscription prices are available upon request from the Publisher or from the Regional ales Office nearest you or from this journal's website (http://www.elsevier.com/locate/csi). Further iformation is available on this journal and other Elsevier products through Elsevier's website: ittp://www.elsevier.com). Subscriptions are accepted on a prepaid basis only and are entered on a alendar year basis. Issues are sent by standard mail (surface within Europe, air delivery outside urope). Priority rates are available upon request. Claims for missing issues should be made within six onths of the date of dispatch.

rders, claims, and product enquiries

ease contact the Customer Service Department at the Regional Sales Office nearest you:
rlando: Elsevier, Customer Service Department, 6277 Sea Harbor Drive, Orlando, FL 32887-4800, SA; phone: (+1) (877) 8397126 [toll free number for US customers], or (+1) (407) 3454020 [customers itside US]; fax: (+1) (407) 3631354; or (+1) (407) 3639661; e-mail: usjcs@elsevier.com or spcs@elsevier.com
nsterdam: Elsevier, Customer Service Department, PO Box 211, 1000 AE Amsterdam, The etherlands; Tel.: +31-20- 4853757; Fax: +31 20 4853432; E-mail: jp.info@elsevier.com
kyo: Elsevier, Customer Service Department, 9-15 Higashi-Azabu 1-chome, Minato-ku, Tokyo 106-)44, Japan; Tel.: +81- 3-55615033; Fax: +81-3-55615047; E-mail: jp.info@elsevier.com
ngapore: Elsevier, Customer Service Department, 3 Killiney Road, #08-01 Winsland House I, ngapore 239519; Tel.: +65-6349 0222; Fax: +65-6733 1510; E-mail: asiainfo@elsevier.com.sg
o de Janeiro: Elsevier, Rua Sete de Setembro 111/16 Andar, 20050-002 Centro, Rio de Janeiro - I, Brazil; Tel.: +55-21-509-5340; Fax: +55-21-507-1991; E-mail: elsevier@campus.com.br [Note (Latin nerica): for orders, claims and help desk information, please contact the Regional Sales Office in New rk as listed above]

lvertising information

vertising orders and enquiries can be sent to: **USA, Canada and South America:** Mr Tino DeCarlo, e Advertising Department, Elsevier Inc., 360 Park Avenue South, New York, NY 10010-1710, USA; .: +1-212-6333815; Fax: +1-212-6333820; E-mail: t.decarlo@elsevier.com. **Europe and ROW:** mmercial Sales Department, Elsevier Ltd., The Boulevard, Langford Lane, Kidlington, Oxford OX5 B, UK; Tel.: +44-1865-843016; Fax: +44-1865-843976; E-mail: media@elsevier.com. **Japan:** The vertising Department, Elsevier K.K., 9-15 Higashi-Azabu 1-chome, Minato-ku, Tokyo 106-0044,)an; Tel.: +81-3-55615033; Fax: +81-3-55615047.

thor enquiries. For enquiries relating to the submission of articles (including electronic submission ere available) please visit this journals homepage at http://www.elsevier.com/locate.csi. You can track :epted articles at http://www.elsevier.com/trackarticle and setup e-mail alerts to inform you of when an cle's status has changed. Also accessible from here is information on copyright, frequently asked :stions and more.

glish language help service: Authors who require information about language editing and copy-ting services pre- and post-submission please visit http://www.elsevier.com/locate/languagepolishing :ontact authorsupport@elsevier.com for more information. Please note Elsevier neither endorses nor :s any responsibility for any products, goods or services offered by outside vendors through our service ı any advertising. For more information please refer to our Terms & Conditions http://www.elsevier.com/ nsandconditions.

A mailing notice: *Computer Standards and Interfaces* (ISSN 0920-5489) is published bi-monthly Elsevier (P.O. Box 211, 1000 AE Amsterdam, The Netherlands). Annual subscription price in the USA $1,108 (valid in North, Central and South America), including air speed delivery. Periodical postage d at Rahway NJ and additional mailing offices.
A POSTMASTER: Send change of address to: *Computer Standards and Interfaces*, Elsevier, 6277 ı Harbor Drive, Orlando, FL 32887-4800.
FREIGHT AND MAILING in USA by Mercury International Limited, 365, Blair Road, Avenel,)7001.

ELSEVIER

Volume 30, Issue 6, August 2008

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

CONTENTS

Abstracted/indexed in: INSPEC, Pascal, Ei Compendex, UnCover, SCISEARCH, Social SciSearch, Inside Conferences, Information Science & Technology Abstracts. Also covered in the abstract and citation database SCOPUS®. Full text available on ScienceDirect®.

0920-5489(200808)30:6;1-F