Journal of Universal Computer Science, vol. 18, no. 6 (2012), 728-731
submitted: 20/2/12, accepted: 15/3/12, appeared: 28/3/12 © J.UCS

Security in Information Systems: New Challenges and Opportunities

J.UCS Special Issue

David G. Rosado
(GSyA Research Group, Department of Information Technologies and Systems
University of Castilla-La Mancha, Ciudad Real, Spain
David.GRosado@uclm.es)

Luis Enrique Sánchez
(Sicaman-NT, Departament of R+D, Ciudad Real, Spain
lesanchez@sicaman-nt.com)

Eduardo Fernández-Medina
(GSyA Research Group, Department of Information Technologies and Systems
University of Castilla-La Mancha, Ciudad Real, Spain
Eduardo.FdezMedina@uclm.es)

Jan Jürjens
(Technical University of Dortmund, Germany
jan.jurjens@cs.tu-dortmund.de)

Information Systems Security is one of the most pressing challenges facing all kinds of organizations today. 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, preventing intrusions, stopping secret information disclosure, etc. 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 of 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 that are faced by businesses and organizations that rely on all these systems, both hardware and software, therefore signify that it is crucial for information systems to be properly secured from the outset.

This Special Issue of the international Journal of Universal Computer Science includes papers received from a public Call for Papers and extended and improved versions of those papers that were selected from the best submissions of the

International Workshop on Security in Information Systems (WOSIS 2011). The aim of this workshop has been to serve as a forum for 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 eighth in a series, which began in Ciudad Real (Spain) in 2002, and has continued in Porto (Portugal), Paphos (Cyprus), Miami (USA), Funchal, Madeira (Portugal), Barcelona (Spain), Milan (Italy) and Beijing (China), respectively. The workshop has gained a considerable reputation as a result of this relatively long history, and it receives an annual average of almost fifty submissions, with an acceptance rate of approximately thirty five percent.

Our workshop has matured year by year, 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 28 members of 12 nationalities), and the invitation of exceptional speakers of great renown in this scientific area (Yvo Desmedt, Sushil Jajodia, Ernesto Damiani, Leonardo Chiariglione, Ruth Breu, Eduardo B. Fernández, and Sabrina De Capitani). Selections of the best papers of 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, Computer Standards and Interfaces and Journal of Universal Computer Science.

This special issue includes eight papers of interest within the wide spectrum of research into the area of information systems security. Three of them have been selected as the best papers presented in the workshop, and the rest of papers come from a public call. There is a predominance of theoretical papers, mainly focused on security engineering, but there is also an important sample of papers which contribute to the area of security software engineering. This fact reaffirms the importance of both research disciplines in the scientific community, and confirms the growth of the secure software engineering discipline as a clear integration of security engineering and software engineering. A brief introduction to each paper selected is presented in the following paragraphs.

The first paper, entitled “Success rate of remote code execution attacks – expert assessments and observations”, by Holms et al. describes a study on how cyber security experts assess the importance of three variables related to the probability of successful remote code execution attacks: (i) non-executable memory, (ii) access and (iii) exploits for High or Medium vulnerabilities as defined by the Common Vulnerability Scoring System. The authors present judgments made by 15 cyber security experts participating in an international cyber defense exercise. A methodology of the expert assessment study is defined where the respondents of the study, the cyber defense exercise, and the carried out questionnaire are described.

The second contribution, entitled “Combating Mobile Spam through Botnet Detection using Artificial Immune Systems”, by Vural and Venter studies the potential threat of Botnets based on mobile networks, and proposes the use of computational intelligence techniques to detect Botnets. The authors implement a software tool employing an artificial immune system that is installed on a mobile device and that detects spam SMSs being sent by malware or Botnets installed on the device. They explain how the prototype is used in a real-world situation to combat Botnet spam.

The third paper, “Qos-Security metrics based on ITIL and Cobit Standard for measurement Web service”, by Charuenporn and Intagosum is an approach for creating Qos-security metrics for measurement Web services based on IT practices guideline (ITIL and Cobit). The authors select two information system standards, COBIT and ITIL, as standards for the development of security metrics and presents security metrics in class diagram and explains security metrics based on both IT best practices. They develop a quality model and experiment with test set by vector method, to adapt the security of web service composition.

The fourth contribution, “A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment”, by Rebollo et al., describes a literature review in search of Information Security Governance frameworks that have been specifically designed for the Cloud Computing paradigm, and which take into account its particularities. The systematic literature review is followed by a data extraction process, in which the main characteristics of each Information Security Governance framework are highlighted in the light of different comparative criteria. These criteria have been defined to take into account the specific consideration of developing security governance in Cloud Computing environments.

The fifth contribution, entitled “Syntactic and Semantic Extension to Secure Tropos to Support Security Risk Management”, by Matulevicius et al. extends the Secure Tropos language, an agent-and goal-oriented security modelling language to support modelling of security risks. The authors suggest improvements of Secure Tropos semantics and syntax. On the syntax level they extend the concrete and abstract syntax of the language, so that it covers the security risk management domain. On the semantic level, they illustrate how language constructs need to be improved to address the three different levels of security risk management. The suggested improvements are illustrated with the aid of a running example.

The sixth contribution, “A Framework for the Comparison of Best Practice Recommendations and Legal Requirements for South African Banks”, by Botha and Loock, presents a framework which can be applied when determining and comparing information security best practice recommendations and information security legal requirements for online banking. The authors investigate whether the implementation of best practices are sufficient to comply with legal requirements and highlight the importance of applying such a framework in a comprehensive fashion to understand the legal requirements imposed and ensure that adequate controls are in place for achieving compliance.

The seventh paper, entitled “Countermeasures to Prevent Misbehaviour in VANETs”, by Molina-Gil et al., proposes a set of countermeasures to prevent selfish behaviour and malicious attacks, making use of node revocation through cooperation enforcement mechanisms and isolation of malicious nodes from the network. The authors introduce a mechanism to provide real and reliable information to those vehicles actively involved in the correct operation of the network. The scheme includes a decentralized revocation system of selfish and malicious nodes, using node cooperation and isolation of attackers, based on the use of reputation lists and rewarding mechanisms.

Finally, the eighth contribution, which is entitled “Adaptive Group Key Management Protocol for Wireless Communications”, by Gharout et al., offers a solution for group key management with a mobility support. The authors propose a decentralized architecture for group key management in mobile environments where the group is organized into clusters of areas, and areas of the same clusters use a common Traffic Encryption Key (TEK). They define a key distribution protocol which is highly scalable to dynamic groups and treats the nodes’ mobility with a null re-keying cost and keeps perfect backward and forward secrecies. This protocol is supported by simulation studies comparing to other protocols.

We would like to thank Professor Christian Gütl (Managing Editor) and Ms. Dana Kaiser (Assistant Editor) of the Journal of Universal Computer Science for their invaluable help and support, and for providing us with 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 not least, we would like to thank the authors for their contributions.

David G. Rosado
Luis Enrique Sánchez
Eduardo Fernández-Medina
Jan Jürjens

Ciudad Real, Spain and Dortmund, Germany, March 2012