Journal of Universal Computer Science, vol. 15, no. 15 (2009), 2912-2915
submitted: 25/8/09, accepted: 30/8/09, appeared: 1/9/09

Security in Information Systems: New Advances and Tendencies

J.UCS Special Issue

Eduardo Fernández-Medina
(Dept. Information Technologies and Systems, University of Castilla-La Mancha, Ciudad Real Spain
eduardo.fdezmedina@uclm.es)

Alfonso Rodríguez
(Dept. Computer Science and Information Technologies, University of Bio Bio, Chillán, Chile
alfonso@ubiobio.cl)

Information Systems Security is one of the most pressing challenges currently facing all kinds of organizations. However, ensuring security and quality in both information and the systems which manage information is a complex goal necessitating the combination of two wide research disciplines which are usually separate: security engineering and security software engineering. The first discipline has a long history, and has usually focused on providing advances in security models, protocols, and techniques, but it remains in a constant state of development. Security software engineering, however, has emerged relatively recently, but is swiftly maturing and is focused on the integration of security into software engineering techniques, models and processes, in order to develop more secure information systems.

This Special Issue of the international Journal of Universal Computer Science therefore includes the extended and improved versions of those papers that were selected from the best of the International Workshop on Security in Information Systems (WOSIS 2009), and 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 seventh 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) and Milan (Italy), 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 25 members of 11 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, and Computer Standards and Interfaces.

This special issue includes eight papers of interest within the wide spectrum of research into the area of information systems security. 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 "SeAAS – A Reference Architecture for Security Services in SOA", by Hafner et al. introduces the idea of considering Security as a Service, discussing the limitations of endpoint security. The authors then present SeAAs, a reference security architecture, which realizes Security as a Service, and which is able to cope with the complex security requirements imposed by use cases from industries that need to deal with security-critical processes considering multiple security domains. This architecture complements the SECTET framework, developed by these authors, which specializes Model Driven Software Engineering towards information security, and attempts to integrate security aspects at the early stages of the software development.

The second contribution, entitled "Information Theoretically Secure Encryption with Almost Free Authentication", by Alomair and Poovendran deals with the problem of authenticated encryption. The authors present an information theoretically secure direction for the construction of secure channels, by proposing a method through which to achieve unconditionally secure authentication with half the amount of key material required by traditional unconditionally secure message authentication codes. The authors then extend their method in order to achieve unconditionally secure authentication with almost free key material, thus obtaining a method with which to unconditionally authenticate arbitrarily long messages with much shorter keys. The authors formally demonstrate the usefulness of their proposal.

The third paper, "ModelSec: A Generative Architecture for Model-Driven Security", by Sánchez et al. is an approach for generating code which implements security requirements, through a Model Driven Security approach. The proposed architecture is composed of two transformation steps. In the first step, the authors propose obtaining a security platform dependent model from three models, which express the security constraints, the design decisions and the information needed on the target platform. In the second step, the security software artefacts are derived from the security platform dependent model. The authors have also considered a security metamodel which has been used to define a Domain Specific Language for security requirements management.

The fourth contribution, "Graph-Based Approach to the Edit Distance Cryptanalysis of Irregularly Clocked Linear Feedback Shift Registers", by Caballero-

Gil et al. proposes a new approach towards a known-plaintext cryptanalysis of Linear Feedback Shift Registers based stream ciphers. This new approach is a divide-and-conquer attack which is based on a combination of graph-based techniques with edit distance concepts, and which offers a new heuristic optimization that avoids the evaluation of an important number of initial states through the identification of the most promising branches of the search graph, producing a lower computational complexity. The proposed method also has the advantage of obtaining results from the attack which are completely deterministic.

The fifth contribution, entitled "A User Controlled Approach for Securing Sensitive Information in Directory Services", by Claycomb and Shin deals with the problem of protecting sensitive user information in directory services. The proposal is composed of two solutions for protecting directory services information from insider attack, the first being a centralized approach which utilizes a customized virtual directory server, and the second being a distributed approach which uses an existing key management infrastructure and a new component called Personal Virtual Directory Service, which moves the protection components to a local service on the client machine. The paper also offers rich explanations about the low impact of the proposal with regard to the existing users, client applications, and directory services, and also implementation details and security analysis.

The sixth contribution, "Optimizations for Risk-Aware Secure Supply Chain Master Planning", by Schröpfer et al. presents an approach for centralized planning using secure computation, the Secure Supply Chain Master Planning. The authors improve the traditional supply chain master planning through secure computation in order to protect the confidentiality of the input values, and they suggest three approaches for modifying the linear programming algorithm. These improvements produce more effective results, as can be observed in the experimental study presented at the end of the paper.

The seventh paper, entitled "Managing Security and its Maturity in Small and Medium-Sized Enterprises", by Sánchez et al., presents a detailed overview of their methodology for developing, implementing and maintaining Information Security Management Systems (ISMS), which is explicitly adapted to the characteristics of Small and Medium-Size Enterprises. The methodology is composed of three main sub-processes. The first of these has the goal of building reusable security management schemas, which are necessary structures for the construction of ISMS, and which are applicable to a set of enterprises from one particular activity sector. The second is in charge of instancing the correct schema to a particular enterprise, therefore generating its ISMS. Finally, the last sub-process deals with the maintenance of the ISMS, ensuring that the level of security for the enterprise is correctly maintained.

Finally, the eighth contribution, which is entitled "A System for Managing Security Knowledge using Case Based Reasoning and Misuse Cases", by Vissagio and de Rosa, offers a practical strategy for capturing, sharing and reusing software security knowledge from software development enterprises. The approach suggests obtaining knowledge represented by misuse cases in the context of case based reasoning in order to implement knowledge management processes. The process is composed of three phases (knowledge creation, retention and usage), and its applicability is presented through several case studies.

We would like to thank Professor Hermann Maurer (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.

Eduardo Fernández-Medina
Alfonso Rodríguez
Ciudad Real, Spain and Chillan, Chile, August 2009