
Editorial

Khalil Drira

LAAS-CNRS,
Université de Toulouse,
7, Av. Colonel Roche,
31077 Toulouse Cedex 04, France
E-mail: khalil@laas.fr

Ahmed Hadj Kacem

ReDCAD Laboratory, FSEG Sfax,
Route de l'Aéroport Sfax,
B.P. 1088, 3018 Sfax, Tunisia
E-mail: ahmed.hadjkacem@fsegs.rnu.tn

Biographical notes: Khalil Drira is a CNRS Researcher. His research interests include formal design, implementation and provisioning of distributed communicating systems and co-operative networked services. His research activity addresses different topics in this field focusing on model-based analysis and design of correctness properties including adaptability and reconfiguration. He has been involved in several R&D projects. He is an author of more than 150 regular and invited papers in international conferences and journals. He is initiator of several different national and international projects and collaborations. He served on or chaired different international and national conferences. He is a member of the editorial board of a number of international journals.

Ahmed Hadj Kacem received his MS in Computer Science and his PhD in Computer Science from UPS, University Paul Sabatier Toulouse-III, respectively in 1991 and 1995. He joined the University of Sfax (Tunisia) as an Assistant Professor in 1997, then as a Professor in 2007. Since 2008, he is the Head of the Computer Science Department at the Faculty of Economics and Management of Sfax. He participated in the initiation of many graduate courses. He is a member of the ReDCAD Research Unit (<http://www.redcad.org>). His current research areas include formal design of multi-agent systems and adaptive software architectures for distributed systems.

1 Introduction

Internet, as a wired or wireless technology and as a worldwide communication infrastructure and the related web-based applications, constitutes the main foundation of the current and the future communication systems and their applications. Internet has become essential for a large number of activities including critical activities using remote monitoring and communicating device control. Such communication systems are

currently used in different industrial and economic activities including e-health, remote surveillance and emergency and rescue activities. Defining and specifying security properties and analysing risks for such systems is an important research activity. It requires the association of different results varying from design, specification, verification and implementation of security management policies to handle intrusion and attacks in communication networks. Different approaches and techniques, emerging from recent research works devoted to this issue, have been presented in the 2008 International Conference on Risks and Security of Internet and Systems (CRISIS'2008).

This issue presents seven papers selected from CRISIS'2008 and addressing different problems related to security management. Security in communication networks is addressed by the first two papers: the paper of Elhdhili et al. and the paper of Mostafa et al., which address, respectively, wireless networks and IP networks. The problem of intrusion detection for web applications and communication networks is addressed by the third and the fourth papers: the paper of Hiet et al. and the paper of Cuppens-Boulahia et al. The last three papers address the access control problem using and extending standard or specific models and formal specifications: the paper of Bertolissi and Fernández, the paper of Loulou et al. and the paper of Kallel et al.

2 Content of the issue

The paper of Elhdhili et al. deals with malicious nodes in wireless networks. The authors propose a Reputation based Clustering Algorithm (REAC) that takes into consideration the trust level of a node in the metric used for clusterhead election. Simulation results show that the algorithm, associated with a reputation system, can converge to a state where all clusterheads are trustworthy and clusters are stable.

The paper of Mostafa et al. presents a new security protocol for IP networks and provides a detailed specification of the protocol operation. The protocol is also intended to ensure implicitly QoS in IP networks. It alleviates packet overhead as well as processing compared with same purpose protocols.

The paper of Hiet et al. proposes a solution to the problem of intrusion detection for web applications based on a combination of policy-based intrusion detection and information flow control and monitoring at the OS-level. An implementation of the proposed solution is achieved and experimental results are presented.

The paper of Cuppens-Boulahia et al. proposes a novel approach for handling network intrusions and attacks. The approach covers different refinement steps from attacks detection and categorisation to effective policies instantiation to stop the attacks. The approach presented is based on an ontology, in which the alert and the policy information models are combined to help in the instantiation of the policies.

The paper of Bertolissi and Fernández presents an algebraic-functional framework for specifying distributed access control systems. The framework is based on lambda-calculus and term rewriting for specifying access control policies. The authors define a system, called Distributed-DEBAC, a variation of the DEBAC model where user's access rights vary depending on the history of events linked to the user. The resulting system is able to evaluate access requests in a distributed context making use of higher-order functions.

The paper of Loulou et al. defines a security framework dealing with static and dynamic aspects of security policies for mobile agent systems. The paper introduces a

precise specification of access control policies. It provides formal verification framework security specification verification and a practical framework for security policies enforcement.

The paper of Kallel et al. is devoted to access control using AOP. The authors formally specify the RBAC model policies using *TemporalZ* and extend it to deal with delegation characteristics. They generate an aspect-based enforcement layer in the ALPHA language from the formal specification.

Acknowledgements

The guest editors of this special issue would like to thank the IJICS Editor-in-Chief, Professor Dr. Eldon Y. Li, for his valuable suggestions and all the authors who have submitted to this special issue. Special thanks go to all the reviewers for their thorough comments that helped in enhancing the quality of the papers.