

## Management of Security and Security for Management Systems

Carlos Becker Westphall · Peter Mueller

Published online: 12 June 2010  
© Springer Science+Business Media, LLC 2010

Political and military events, coupled with the accelerating frequency of cyber attacks on network/IT systems and technical revelations of management protocol insecurities, underscore the substantial risks associated with network, systems and applications management. Through management systems, rogue elements can perpetrate targeted as well as system-wide fraud, theft of services, and disruption of capabilities and management data. Worse yet, due to the extended, pervasive reach of management systems, rogues can get a stranglehold on the IT and networking resources of an enterprise, entire industry sectors, even national critical infrastructures or governments.

Consequently, interest in the security aspects of management systems has skyrocketed. Security is an essential feature, not an after-thought, of an information enterprise. The commercial sector is pursuing double-digit growth rates for IT and network security spending. Corporations embracing e-business strategies that involve integration of systems and resources with business partners want assurances that their internal resources will not be compromised by vulnerable management systems, internal or external. Corporations and governments remain at risk for cyber attack on mission-critical management components. Legislation is making security an R&D priority.

This special issue of Journal of Network and Systems Management focuses on topics associated with both the management of security in telecommunications, network, and systems environments, and the security for management systems in such environments.

---

C. B. Westphall (✉)  
Federal University of Santa Catarina, Florianópolis, Brazil  
e-mail: westphal@inf.ufsc.br

P. Mueller  
IBM Zurich Research Laboratory, Rüschlikon, Switzerland  
e-mail: pmu@zurich.ibm.com

For this special JNSM issue we received 69 high quality submissions, each of which was reviewed by at least two reviewers. Following is a brief description of the accepted papers.

The first paper is written by Dijiang Huang and Vinayak Kandiah (Arizona State University) and is entitled “Low-latency Mix using Split and Merge Operations”. The paper proposes mix network schemes that are more robust against attacks, using traffic redistribution techniques. Traffic redistribution involves changing the number and size of messages in the network by splitting and merging the messages at network nodes and using variable size messages to confuse the attacker. The security of the proposed techniques are evaluated against traffic analysis attacks.

The second paper is written by Mohammad GhasemiGol, Reza Monsefi, and Hadi Sadoghi-Yazdi (Ferdowsi University of Mashhad) and is entitled “Intrusion Detection by Ellipsoid Boundary”. The paper presents a novel approach to describe the normal behavior of computer networks based on Support Vector Data Description (SVDD). In the proposed method the authors find a minimal hyper-ellipse around the normal objects in the input space. Hyper-ellipse can be expanded in high-dimensional space or used as a preprocessing in the SVDD method to obtain better results for Intrusion Detection Systems.

The third paper is written by Stefan Rass, Angelika Wiegele, and Peter Schartner (Alpen-Adria University Klagenfurt) and is entitled “Building a Quantum Network: How to Optimize Security and Expenses”. The paper discusses methods of designing quantum key distribution networks with provable end-to-end security at provably optimized efforts. The authors formulate two optimization problems, along with investigations of computational difficulty: First, what is the minimal cost for a desired security? Second, how much security is achievable under given (budget-) constraints? Both problems permit applications of commercial optimization software, so allow taking a step towards an economic implementation of a globally spanning quantum key distribution network.

The fourth paper is written by Michael Rossberg, Guenter Schaefer, and Thorsten Strufe (Technische Universität Ilmenau) and is entitled “Distributed Automatic Configuration of Complex IPsec-Infrastructures”. The paper presents a fully automated approach for the distributed configuration of IPsec domains, utilizing peer-to-peer technology. The authors’ approach scales well with respect to the number of managed IPsec gateways, reacts robustly to network failures, and supports the configuration of nested networks with private address spaces. The authors analyze the security requirements and further desirable properties of IPsec policy negotiation, and show that the distribution of security policy configuration does not impair security of transmitted user data in the resulting VPN.

The fifth paper is written by Angelo Rossi, Samuel Pierre, and Suresh Krishnan (École Polytechnique de Montréal) and is entitled “An efficient and secure self-healing scheme for LKH”. The paper presents two self-healing recovery schemes based on the dual directional hash chains for the logical key hierarchy rekeying protocol. This enables a member that has missed up to “m” consecutive key updates to recover the missing decryption keys without asking the group controller key server for retransmission. Conducted simulations show considerable improvements

in the ratio of decrypted messages and in the rekey message overhead in high packet loss environments.

The guest editors greatly thank all the authors who submitted their papers to this special issue and all the reviewers whose diligent work was crucial for the realization of this special issue. We also would like to thank the help of Dr. Manu Malek (Editor-in-Chief of the JNSM) and Anitha Sankar (Springer—Journals Editorial Office).

## References

- Hale, J., Brusil, P.J.: Secur(e/ity) management: two sides of the same coin. *J. Netw. Syst. Manage.* **12**(1), 1–8 (2004)
- Pras, A., Schönwälder, J., Stiller, B.: Peer-to-peer technologies in network and service management. *J. Netw. Syst. Manage.* **15**(3), 285–288 (2007)
- Magedanz, T., Madeira, E., Bellavista, P.: Management challenges and solutions for IP multimedia subsystems. *J. Netw. Syst. Manage.* **16**(1), 11–13 (2008)
- Westphall, C.B., Brunner, M., Nogueira, J.M., Ulema, M.: Pervasive management for ubiquitous networks and services—report on NOMS 2008. *J. Netw. Syst. Manage.* **16**(3), 317–321 (2008)

## Author Biographies

**Carlos Becker Westphall** is a full professor in the Department of Informatics and Statistics at the Federal University of Santa Catarina, Brazil, where he is the leader of the Networks and Management Laboratory. His research interests include network management, security, and grid and cloud computing. Westphall received his DSc in computer science at the Paul Sabatier University, France.

**Peter Mueller** joined the IBM Zurich Research Laboratory as e research staff member in 1988. He is vice chair of the IEEE Communications and Information Systems Security Technical Committee. His research expertise covers broad areas on security of human-machine interfaces, distributed computing systems architecture, communications and interconnects technology, and modeling.