Telecommun Syst
DOI 10.1007/s11235-009-9238-x

Guest editorial

Krzysztof Szczypiorski

The International Workshop on Secure Information Systems (SIS) is envisioned as a forum to promote the exchange of ideas and results addressing complex security issues that arise in modern information systems. We aim at bringing together a community of security researchers and practitioners working in such diverse areas as networking security, antivirus protection, intrusion detection, cryptography, security protocols, and others. We would like to promote an integrated view at the security of information systems.

As information systems evolve, becoming more complex and ubiquitous, issues relating to security, privacy and dependability become more critical. At the same time, the global and distributed character of modern computing—typically involving interconnected heterogeneous execution environments—introduces many new and challenging engineering and scientific problems. Providing protection against increasingly sophisticated attacks requires strengthening the interaction between different security communities, e.g. antivirus and networking. New technologies lead to the emergence of new threats and attack strategies, involving smart mobile devices, peer-to-peer networks, instant messaging, VoIP, mesh networks or even networked consumer devices, such as house appliances or cars. Furthermore, the increasing openness of the communications infrastructure results in novel threats and can jeopardize critical enterprise and public infrastructure, such as industrial automation and process control systems. Not only it is estimated that half of all Web applications and Internet storefronts still contain some security vulnerabilities, but secure commerce applications are also exposed to increasingly elaborate attacks, including spyware, phishing and other social engineering methods.

In order to develop a secure system, security has to be considered in all phases of the lifecycle and adequately addressed in all layers of the system. At the same time, good engineering has to take into account both scientific and economic aspects of every solution: the cost of security has to be carefully measured against its benefits—in particular the expected cost of mitigated risks. Most companies and individuals treat security measures in information system as a necessary, but often uncomfortable, overhead. The increasing penetration of computing in all domains of everyday life means that security of critical business systems is often managed and maintained by personnel who are not knowledgeable in the field. This highlights the importance of usability and ease of configuration of security mechanism and protocols.

The third edition of the SIS took place on October 20–22, 2008 in Wisla, Poland. We are delighted to present in this special issue a selection of 10 papers resulting from the workshop.

In “A New Worm Propagation Threat in BitTorrent: Modeling and Analysis” Sinan Hatahet, Abdelmadjid Bouabdallah and Yacine Challal identify the BitTorrent vulnerabilities including worms, analyze characteristics that accelerate and decelerate propagation of worms, and develop a mathematical model of their propagation. The paper by Ali Noorollahi Ravari, Jafar Haadi Jafarian, Morteza Amini and Rasool Jalili proposes a Generalized Temporal History Based Access Control (GTHBAC) model, aimed at integrating history-based constraints along with a generic access control model. The operators of GTHBAC are also compared with Linear Time Temporal Logic (LTL) operators to show the

K. Szczypiorski (✉)
Faculty of Electronics and Information Technology, Institute of Telecommunications, Warsaw University of Technology, 15/19 Nowowiejska Str., 00-665 Warszawa, Poland
e-mail: k.szczypiorski@tele.pw.edu.pl

Published online: 17 December 2009

expressive power of the model. Ali Ahmed and Ning Zhang in "Towards the Realisation of Context-Risk-Aware Access Control in Pervasive Computing" propose a novel Context-Risk-Aware Access Control (CRAAC) model for Ubiquitous Computing environments to allow access permissions to be adjusted dynamically in adaptation to the changes in the surrounding context. Elaine Hulitt and Rayford B. Vaughn, Jr. in "Information System Security Compliance to FISMA Standard: A Quantitative Measure" suggest the use of Pathfinder networks to generate a quantitative metric suitable to measure, manage, and track the status of information system compliance with FISMA. In "LACK—a VoIP Steganographic Method" Wojciech Mazurczyk and Józef Lubacz present a new steganographic method called LACK (Lost Audio PaCKets Steganography) which is intended mainly for VoIP. The method is presented in a broader context of network steganography and of VoIP steganography in particular. Nicholas M. Boers, Pawel Gburzynski, Ioanis Nikolaidis and Wlodek Olesinski in "Developing Wireless Sensor Network Applications in a Virtual Environment" describe "holistic" platform for developing wireless ad hoc sensor networks and focus on its most representative and essential virtualization component: the Virtual Underlay Emulation Engine. In "Conception Approach of Access Control in Heterogeneous Information Systems using UML" Aneta Poniszewska-Maranda proposes to use one common set of access control concepts to support the access control management in security of heterogeneous information systems. Tomasz Mrugalski and Jozef Wozniak perform analysis of IPv6 Handovers in IEEE 802.16 Environment. The authors modeled and tested all major elements of the WiMAX stack. In "Real-time Automated Risk Assessment in Protected Core Networking" Konrad Wrona and Geir Hallingstad propose use of Bayesian networks, known from operational risk assessment, for Protected Core Networking risk assessment and provide analytical and simulative evaluation of Real-time Automated Risk Assessment mechanisms. Finally, Xun Dong, John A. Clark, and Jeremy L. Jacob describe a novel approach for detecting phishing websites based on analysis of users' online behaviours.

We believe that this Special Issue will contribute to enhancing knowledge in many diverse areas of the ICT security. In addition, we also hope that the presented results will stimulate further research in the important areas of information and network security.

Krzysztof Szczypiorski holds M.Sc. (1997) and Ph.D. (2007) in telecommunications both with honours from Faculty of Electronics and Information Technology, Warsaw University of Technology (WUT). Assistant Professor at WUT. Founder and head of International Telecommunication Union Internet Training Centre (ITU-ITC) established in 2003. Research leader of Network Security Group at WUT (secgroup.pl). His research interests include: network security and steganography and wireless networks. He is the author or the co-author of over 110 publications including 65 papers, 2 patent applications, and 35 invited talks.