Journal of Information Assurance and Security 2 (2007) 153-154

Guest Editorial

Konrad Wrona and 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 second edition of the SIS took place on October 15-17, 2007 in Wisla, Poland. We are delighted to present in this special issue of JIAS a selection of 13 papers resulting from the workshop. The articles deal with a variety of problems such as intrusion detection, VoIP security, wireless sensor networks, enterprise security and risk analysis.

Service Oriented Architecture is the paradigm of choice for most of the modern enterprise applications. Menzel et al. propose in their paper "Access Control for Cross-Organizational Web Service Composition" a two-layered security architecture for a cross-organizational service composition. Security of routing protocols continues to be an important research topic in IT security. In "Steganographic Routing in Multi Agent System Environment" Szczypiorski et al. develop a new concept of proactive hidden routing. Two aticles, by Brzezinski and by Szabados et al. propose a more rigorous approach to evaluation of security. The first paper, "On Common Meta-Linguistic Aspects of Intrusion Detection and Testing", presents a taxonomy for capturing linguistic problems common to vulnerability testing and intrusion detection. The second one, "Model based code generation approach for fast-deployment wireless security applications" proposes an architecture and a corresponding model-based code generation scheme for applications of wireless sensor networks. The paper by Sorniotti et al., "Secure and Trusted in-network Data Processing in Wireless Sensor Networks" continues with the topic of wireless sensor networks (WSN) and present an comprehensive survey of current research trends in secure distributed data processing in WSN. One of the critical elements of security of almost every organization is nowadays the security management system. In "Integrated, Business-Oriented, Two-Stage Risk Analysis", Andrzej Bialas and Krzysztof Lisek presents the current state of the art in this area, focusing particularly risk analysis methods. When risks in enterprise systems are identified and quantified, it is important to deploy appropriate intrusion detection mechanisms. In "Anomaly Based Intrusion Detection Based on the Junction Tree Algorithm", Nikolova and Jecheva present a novel methodology for the attacks recognition. The contribution from Hirano et al., "Design and Implementation of a Portable ID Management Framewoek for a Secure Virtual Machine Monitor", is addressing importance of ID management in virtualized environments, which is a very timely issue as many Internet application providers and organizations are moving towards fully virtualized IT environments. Two other papers, by Ghafarian et al. "Securing Voice over Internet Protocol", and by Mazurczyk and Kotulski, "Adaptive VoIP with Audio Watermarking for Improved Call Quality and Security" analyze security risks and opportunities related to use of VoIP solutions, which quickly become one of the most important and frequently used applications of the Internet. Another point

Received September 17, 2007.

1554-1010 $03.50 © Dynamic Publishers, Inc.

of view on voice services is taken by Piotrowski and Gajewski in “Voice Spoofing as an Impersonation Attack and the Way of Protection”, where they discuss possibility of impersonating voice and propose appropriate countermeasures based on watermarking technology. Finally, “Dealing with Network Security in Academic Institutions – a Case Study” by Ivan Dolezal et al. presents a real-life experience of the authors with their efforts at a radical security improvement of the academic computer networks that they administer at a large university and a medium-sized research institute.

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.