Guest Editorial: Security in Distributed and Network-Based Computing

Igor Kotenko[1, 2]
[1]*Laboratory of Computer Security Problems*
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS)
39, 14 Liniya, St. Petersburg, 199178, Russia
[2]*St. Petersburg National Research University of Information Technologies*
Mechanics and Optics, 49, Kronverkskiy prospekt, St. Petersburg, Russia
ivkote@comsec.spb.ru

Security should be a vitally important property of distributed and networked systems. While attack tools are becoming more powerful and easy-to-use, research and development of adaptive, active and intelligent security systems is required. Finding effective ways to protect networked and distributed systems and data is a very challenging research problem.

The special issue aims to provide the latest developments in the area of security systems. The issue focuses on problems related to confidentiality, integrity, availability, privacy, dependability and sustainability of distributed and networked systems.

This special issue includes five papers that outline different aspects of security in distributed and network-based computing. Most of them are selected from papers submitted to and presented in Special Session "Security in Parallel, Distributed and Network-Based Computing (SPDNS 2015)" on 23th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2015), Turku, Finland, 4-6 March 2015.

- The first paper [1], *Runtime Model Checking for SLA Compliance Monitoring and QoS Prediction*, proposes a quality of service prediction approach which combines runtime monitoring of the computer system with probabilistic model-checking on a parametric system model. This approach is validated by development of a prototype of the quality of service prediction framework, and experimenting with a smart grids case study.

- The second paper [2], *Security Compliance Tracking of Processes in Networked Cooperating Systems*, presents an approach for security compliance tracking of processes in networked cooperating systems, using predictive security analysis at runtime.

- In the third paper [3], *Integrated Repository of Security Information for Network Security Evaluation*, models and methods for integration of separate open databases of vulnerabilities, exploits, products into one common security repository are considered. The authors describe the repository implementation and analyze the results of experiments with the repository. This common security repository helps to improve the detection accuracy of network security vulnerabilities and weaknesses and evaluate different security metrics important for estimation of computer network security and generation of countermeasures.

- In [4], *Selecting Countermeasures for ICT Systems Before They are Attacked*, a model based approach to selects countermeasures is considered. It is based on multiple simulations of the behavior

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 6, number: 2, pp. 1-3

of a system which should be protected and the behavior of intelligent agents that implement sequences of attacks.

- Finally, the fifth paper [5], *Securing Mobile Devices: Malware Mitigation Methods*, is an overview of the defense methods proposed to mitigate mobile malware threats.

We would like to express our sincere appreciation of the valuable contributions made by all the authors and our deep gratitude to all anonymous reviewers who have carefully analyzed the assigned papers and contributed to improve their quality.

Our special thanks go to Prof. Ilsun You, Editor in Chief of the JoWUA for his tremendous support throughout this special issue preparation.

Igor Kotenko
Guest Editor
June 2015

References

[1] G. Cicotti, L. Coppolino, S. D'Antonio, and L. Romano, "Runtime Model Checking for SLA Compliance Monitoring and QoS Prediction," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 6, no. 2, pp. 4–20, June 2015.

[2] R. Rieke, M. Zhdanova, and J. Repp, "Security Compliance Tracking of Processes in Networked Cooperating Systems," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 6, no. 2, pp. 21–40, June 2015.

[3] A. Fedorchenko, I. Kotenko, and A. Chechulin, "Integrated Repository of Security Information for Network Security Evaluation," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 6, no. 2, pp. 41–57, June 2015.

[4] F. Baiardi, F. Tonelli, A. Bertolini, and R. Bertolotti, "Selecting Countermeasures for ICT Systems Before They are Attacked," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 6, no. 2, pp. 58–77, June 2015.

[5] A. Skovoroda and D. Gamayunov, "Securing Mobile Devices: Malware Mitigation Methods," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 6, no. 2, pp. 78–97, June 2015.

Author Biography

Igor Kotenko graduated with honors from St.Petersburg Academy of Space Engineering and St. Petersburg Signal Academy. He obtained the Ph.D. degree in 1990 and the National degree of Doctor of Engineering Science in 1999. He is Professor of computer science and Head of the Laboratory of Computer Security Problems of St. Petersburg Institute for Informatics and Automation. He is the author of more than 250 refereed publications, including 12 textbooks and monographs. Igor Kotenko has a high experience in the research on computer network security and participated in many projects on developing new security technologies. His current research is being supported by

the grants of the Russian Foundation of Basic Research (13-01-00843), the Program of fundamental research of the Department for Nanotechnologies and Informational Technologies of the Russian Academy of Sciences (contract #1.5), and by Government of the Russian Federation, Grant 074-U01.