Guest Editorial: Advances in Secure 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

Modern information systems are geographically distributed, parallel and network-based computing systems. The vulnerability of such computing systems greatly exceed the vulnerability of stand-alone computers. This is due, primarily, to the openness scale and heterogeneity of computer networks themselves. Accordingly, there are many ways to realize modern network attacks against distributed, parallel and network-based computing systems. The number of security threats and ways of their implementation is constantly growing. The main reasons here are the disadvantages of modern information technologies, as well as a steady increase in the complexity of software and hardware. The special issue has the goal to demonstrate the latest developments in the area of security. The issue focuses on problems related to authentication, privacy, vulnerability analysis and design of secure embedded devices for parallel, distributed and network-based systems. This special issue includes four papers that outline different aspects of security in parallel, distributed and network-based computing. These papers are selected from papers submitted to and presented in Special Session "Security in Parallel, Distributed and Network-Based Computing (SPDNS'16)" on the 24th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP'16), Heraklion, Crete, Greece, 17-19 February 2016.

The first paper [1], *Verifying Group Authentication Protocols by Scyther*, uses Scyther to analyze security properties of two group authentication protocols. The authors checked a subset of the security properties, which demonstrate that the group authentication protocols provide mutual authentication, implicit key authentication and they are secure against impersonation attack and passive adversaries.

The second paper [2], *Robust Decentralized Differentially Private Stochastic Gradient Descent*, presents an approach for performing private stochastic gradient descent (SGD) over an unreliable decentralized system, where every private data record is stored separately by an autonomous node. The authors introduced and simulated a protocol to implement a robust random walk in a dynamic network environment. The authors showed that the proposed SGD implementations can approximate the performance of their original noise-free variants in faulty decentralized environments.

The third paper [3], *Application Vulnerabilities in Risk Assessment and Management*, considers the suite Haruspex which supports the automation of risk assessment and management in complex infrastructures. The Haruspex can fulfill scenarios including an infrastructure and intelligent attackers. Each attacker realizes targeted attacks to get predefined sets of access rights or privileges. The suite uses a Monte Carlo method by running a set of experiments. The authors discuss the application of the suite in a NATO cyber defense exercise. The paper extends the infrastructure model to describe in more details the cascading effects of attacks and outlines the model to assess a critical infrastructure that supervises

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 7:2 (June 2016), pp. 1-2

and manages gas distribution.

Finally, in [4], *Design technique for secure embedded devices: application for creation of integrated cyber-physical security system*, presents a technique for design of secure embedded devices. The technique considers functional and non-functional characteristics of security components and device constraints, applying an optimization approach. The software tools realizing this technique were developed. The correctness of the technique was checked by its use in the development of the integrated cyber-physical security system.

We would like to express our sincere appreciation of the contributions made by all the authors and our deep gratitude to all 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 invaluable support throughout this special issue preparation.

Igor Kotenko
Guest Editor
June 2016

References

[1] H. Yang, V. Oleshchuk, and A. Prinz, "Verifying Group Authentication Protocols by Scyther," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 7, no. 2, pp. 3–19, June 2016.

[2] I. Hegedus, A. Berta, and M. Jelasity, "Robust Decentralized Differentially Private Stochastic Gradient Descent," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 7, no. 2, pp. 20–40, June 2016.

[3] F. Baiardi, F. Tonelli, and L. Isoni, "Application Vulnerabilities in Risk Assessment and Management," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 7, no. 2, pp. 41–59, June 2016.

[4] V. Desnitsky, D. Levshun, A. Chechulin, and I. Kotenko, "Design technique for secure embedded devices: application for creation of integrated cyber-phisical security system," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 7, no. 2, pp. 60–80, June 2016.

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 Government of the Russian Federation, Grant 074-U01.