Guest Editorial: Managing Insider Security Threats

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

At present, the most acute problem for any company is the leakage of information. It can occur for a number of independent reasons, but often the prerequisites lie in the employees themselves, and not external threats. Insiders pose a great threat to any organization and enterprise. According to opinions of security experts, about 80% of intrusions and attacks are performed either from within the controlled zone by the employees of the organization itself, or from outside with their knowledge or with direct participation. The special issue is aimed to demonstrate some of the latest developments in the area of managing insider security threats. The issue focuses on problems related to security and cryptography technologies to prevent, detect and predict insider threats. This special issue includes four papers that outline different aspects of the Insider Security. These papers are selected from papers originally presented at the 9th International Workshop on Managing Insider Security ?Threats (MIST'17) in conjunction with the ACM Conference on Computer and Communications Security (CCS), Dallas, TX, USA, October 30, 2017.

The first paper [1], *Stopping the Insider at the Gates: Protecting Organizational Assets Trough Graph Mining*, considers an approach to detect insider behaviors, which is based on the analysis of a bipartite graph of user and system interactions. The approach allows to learn regular community behavior using the interactions of users and system's components. The focus of the paper is on the malicious behaviors over time rather than identifying the static malicious nodes. The approach takes into account the evolution of the user and system interactions graph to identify topological properties that characterize the system's normal behavior. The monitored properties, which do not follow the norm of the regular pattern are assumed to indicate the presence of an anomalous event. Such an event may indicate a potential insider incident or an event that requires further investigation.

The second paper [2], *Subliminal Channels in High-Speed Signatures*, investigates high-speed signature schemes EdDSA and MQ (including QUARTZ, Gui-127, SFlash PFlash, MQQ-SIG and Rainbow) for the possibility from the side of insiders to establish subliminal channels. The authors describe how these channels can be applied in different scenarios and what methods can be used to prevent the subliminal communication. They presented different data leakage scenarios using subliminal channels. The paper concludes that almost all considered schemes yield subliminal channels that may lead to data exfiltration.

The third paper [3], *The Wolf Of SUTD (TWOS): A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition*, presents a dataset of insider threat behavior which is generated based

*Corresponding author: Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation (SPIIRAS), 39, 14-th Liniya, Saint-Petersburg, 199178, Russia, Tel: +7(812) 328-71-81, Web: `http://www.comsec.spb.ru/`

on a game of several users' teams. The dataset is named as the TWOS (Wolf Of Singapore University of Technology and Design), and it contains realistic labeled instances of insider threats. The game involved the participation of several users' teams imitating actions of both normal user behavior and malicious insider behavior for a period of five days. It includes 320 hours of active participation. Two types of malicious behaviors were investigated - masqueraders, performing illegal actions on behalf of a legitimate users, and traitors, i.e. legitimate users misusing privileges to perform malicious activities. The authors describe the methodology of the dataset generation, the experimental environment and the results of teams' competition. The activities were recorded from different sources, including mouse, keyboard, process and file-system monitor, network traffic, SMTP logs, etc. The paper illustrates the potential use of the TWOS dataset in different areas. Besides, several related datasets are analyzed.

Finally, in [4], *Achieving trustworthy Homomorphic Encryption by combining it with a Trusted Execution Environment*, considers an approach allowing for guarantee the integrity and correctness of the cloud database code and data. It suggests to combine Trusted Execution Environments (TEE) (e. g., Intel SGX) with Homomorphic Encryption (HE) schemes (e. g., Paillier cryptosystem). The authors demonstrate how to apply this approach in Multi Party Computations (MPC) schemes, and how to construct a voting system. This approach can be considered as an important mechanism for protection against different attackers, including insiders, having administrator privileges.

We would like to express my sincere appreciation of the papers written by all the authors and my deep thankfulness to all reviewers who have carefully analyzed these papers and contributed to improve their quality. My special gratitude goes to Prof. Ilsun You, Editor in Chief of the JoWUA, for his inestimable support throughout this special issue preparation.

Igor Kotenko
Guest Editor
March 2018

References

[1] P. Moriano, J. Pendleton, S. Rich, and L. J. Camp, "Stopping the Insider at the Gates: Protecting Organizational Assets Trough Graph Mining," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 9, no. 1, 2018.

[2] A. Hartl, R. Annessi, and T. Zseby, "Subliminal Channels in High-Speed Signatures," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 9, no. 1, 2018.

[3] A. Harilal, F. Toffalini, I. Homoliak, J. H. Castellanos, J. Guarnizo, S. Mondal, and M. Ochoa, "The Wolf Of SUTD (TWOS): A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 9, no. 1, 2018.

[4] N. Drucker and S. Gueron, "Achieving trustworthy Homomorphic Encryption by combining it with a Trusted Execution Environment," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 9, no. 1, 2018.

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 also a Co-Head of the International Laboratory ”Information security of cyber-physical systems”, ITMO University, St. Petersburg, Russia. He is the author of more than 350 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 grants of Russian Foundation for Basic Research (projects No. 16-29-09482 and 18-07-01488), by the budget (project No. AAAA-A16-116033110102-5), and by Government of the Russian Federation, Grant 074-U01.