Journal of Universal Computer Science, vol. 25, no. 9 (2019), 1039-1042
submitted: 9/9/19, accepted: 20/9/19, appeared: 28/9/19

Recent Advances in Detection, Investigation and Mitigation of Cyber Crimes

J.UCS Special Issue

Artur Janicki, Wojciech Mazurczyk
(Institute of Telecommunications, Warsaw University of Technology, Poland
{a.janicki, w.mazurczyk}@tele.pw.edu.pl)

Xiangyang Luo
(Zhengzhou Information Science and Technology Institute, Zhengzhou, China
luoxy_ieu@sina.com)

Dengpan Ye
(Wuhan University, Wuhan, China
yedp2001@163.com)

Currently, societies are increasingly utilizing and becoming more and more dependant on open networks such as the Internet, where commercial activities, business transactions and government services are realized. This has caused the fast development of cyber threats and numerous information security issues which can be and are exploited by cyber criminals of which we have been informed by mass media practically every day. If this trend is going to continue the inability to provide trusted secure services in contemporary computer network technologies may have tremendous socio-economic impact on global enterprises as well as individuals.

Considering above, the research on cyber crimes detection, investigation and mitigation is of paramount importance. Especially that, the frequently occurring international frauds impose the necessity to conduct the investigation of facts spanning across multiple international borders. Moreover, such examination is often subject to different jurisdictions and legal systems. A good illustration of the above being the Internet, which has made it easier to perpetrate traditional crimes. It has acted as an alternate avenue for the criminals to conduct their activities, and launch attacks with relative anonymity. The increased complexity of the communications and the networking infrastructure is making investigation of the crimes difficult. Traces of illegal digital activities are often buried in large volumes of data, on various types of equipment (including Internet of Things devices) which are hard to analyze and inspect with the aim of detecting offences and collecting evidence. Nowadays, the digital crime scene functions like any other network, with dedicated administrators functioning as the first responders.

This poses new challenges for law enforcement policies and forces the computer societies to utilize digital forensics to combat the increasing number of cybercrimes. Forensic professionals must be fully prepared in order to be able to provide court admissible evidence. To make these goals achievable, forensic techniques should keep pace with new technologies.

That is why, the main aim of this J.UCS special issue was to present the latest, cutting-edge research in the field of detection and mitigation of cyber crimes and to present the development of tools and techniques, which assist the investigation process of potentially illegal cyber activity.

The special issue consists of eight articles. The first one, authored by Andrey Fedorchenko, Elena Doynikova and Igor Kotenko, entitled *Determination of System Weaknesses Based on the Analysis of Vulnerability Indexes and the Source Code of Exploits*, concerns the problem of automating the process of finding the system weaknesses to eliminate or mitigate them. The authors consider the techniques for analysis of vulnerability indexes and exploit source code and their subsequent classification. They proposed two techniques: one based solely on the analysis of publicly available vulnerability indexes, and the second one, based on the analysis of the exploit source code, for the exploits without associated vulnerabilities yet. The paper presents the experimental results for both techniques, showing satisfying classification scores, in particular for the first technique.

In the second article: *A Context-based Defense Model For Assessing Cyber Systems' Ability To Defend Against Known And Unknown Attack Scenarios*, the authors, Yosra Lakhdhar, Slim Rekhis and Noureddine Boudriga describe an enhanced cyber defense model to assess the effectiveness of the deployed security solutions to safeguard against various attack scenarios. They consider various contexts: the configuration of distributed security solutions, named observer agents, the type and location of reaction systems, and the type of data visible by the deployed solutions. In addition, the authors proposed a model which aims to generate known and unknown attack scenarios, based on formal descriptions of system variables and interactions between them.

Additionally, the authors developed the concept of observable executable scenario, which allows a step by step observation of how a given attack scenario is executed, how the observer agents react, if and how the attack occurrence is detected in a distributed system, and at which point it can be potentially stopped. The researchers ran several experiments using real case studies, such as the WannaCry attack, and positively assessed the performance of their method.

In the third article, the authors: Mohammed Al-Saleh and Hanan Hamdan in their publication entitled *Precise Performance Characterization of Antivirus on the File System Operations* discuss the problem of antivirus protection and their impact on the machine performance. Usually, a trade-off between security of antivirus protection and its usability is maintained, so that these two aspects are kept at a reasonable level. The authors focus on the crucial element on antivirus operation: the decision when a file should be scanned for the virus presence.

This is why, using the Microsoft's minifilter driver technology, the researchers tried to get as closely as possible to antivirus components, measuring the impact of the antivirus software on the main file system operations: CREATE, READ, WRITE and CLEANUP. Using testing environment, the authors compared five commonly used commercial antiviruses in terms of the speed of the before mentioned operations and referenced them to the case when no antivirus was used. The authors found that most overhead is related to the CREATE operation. Detailed results of their experiments are enclosed in the paper.

The next paper, entitled *Mobile Agents for Detecting Network Attacks Using Timing Covert Channels*, authored by Jędrzej Bieniasz, Monika Stępkowska, Artur Janicki and Krzysztof Szczypiorski, deals with network security and hidden channels using timing steganography. This technique uses time relationships between packets to convey hidden messages. The authors propose an efficient method of detecting such hidden channels, based on the Change Observation Theory, using two types of agents: the base agents, which are installed on fixed nodes, and flying ones, which are able to move between nodes. The agents monitor timing parameters of the packets, using a modified version of histograms and machine learning methods.

The authors present results of their experiments using various machine learning algorithms, showing that they were able to reach an area under the ROC curve (AUC) above 0.85 for the evaluation data. They present a proof-of-concept for an attack detection method that combines the classifier, the proposed anomaly metric and the mobile agents. The authors suggest that their multi-agent intrusion detection method can be also used for a wider group of other IT systems.

The problem of steganography and its detection is also discussed by Hui Tian, Meilun Huang, Chin-Chen Chang, Yongfeng Huang, Jing Lu and Yongqian Du in their article *Steganalysis of Adaptive Multi-Rate Speech Using Statistical Characteristics of Pitch Delay.* The authors present a steganalysis method for detecting adaptive-codebook based steganography in adaptive multi-rate (AMR) speech streams. They propose a new feature set, which has much lower dimensionality (only 14) than the other steganalysis methods. These features are derived from the pitch delay parameter, used in speech coding.

The authors describe a steganalysis scheme for AMR speech streams based on support vector machines. The researchers present their evaluation results, comparing their method with other ones, e.g., the Ren's one, for various embedding rates. The authors show that their method is both more accurate and less computationally demanding than the other competing methods.

The next article, authored by Mingying Huang, Ming Xu, Tong Qiao, Ting Wu and Ning Zheng, entitled *Designing Statistical Model-based Discriminator* *for Identifying Computer-generated Graphics from Natural Images*, concerns the vital problem of detecting manipulated (i.e. fake) photos. The authors propose using two different denoising filters and analysis of the residual noise of an inspected image. Next, to differentiate real and computer-generated images the authors use hypothesis testing theory and employ the likelihood ratio test (LRT), defining all the nuisance parameters. Next, a generalized likelihood ratio test (GLRT) is applied.

The authors ran multiple experiments on real and simulated data and described their results. They showed that their method is highly efficient and resistant against some post-processing techniques, such as compression or resizing.

Two last articles in our special issue are devoted to forensic methods. Ziad Al-Sharif, Mohammed Al-Saleh, Yaser Jararweh, Luay Alawneh and Ahmed S. Shatnawi in their paper *The Effects of Platforms and Languages on the Memory Footprint of the Executable Program: A Memory Forensic Approach* focus on the problem of identifying the software used in a cybercrime. One of the methods to achieve that is to analyze the content of the RAM memory – the so called memory footprint, which contains information about the current state of the system and the processes running. The authors analyze various factors, which can influence the memory footprint: the programming language used, the host platform and the encoding scheme.

The presented results display that all these factors heavily affect the memory footprint. The authors show very interesting results, for example, proving that a program written in Java is easier traceable than written in C++ or C#. They also discuss differences of RAM footprints among Linux, Windows and Mac OS.

François Bouchaud, Gilles Grimaud, Thomas Vantroys and Pierrick Buret in their paper *Digital Investigations of IoT Devices in the Criminal Scene* address newly emerging possibilities of using IoT devices in forensics. They argue that the traditional digital forensic methods often do not fit well the IoT environment, due to the heterogeneity of IoT devices, the lack of standards and complex architecture. The authors propose a methodology for identifying and classifying connected objects in search of the best forensic evidence. The described techniques involve, among others, frequency mapping and radio localization techniques. The authors describe a use case, in which wellness data from a sleep sensor can be used to analyze the sequence of events in the criminal context.

In summary, we would like to sincerely thank all the authors and the reviewers for their contributions and efforts invested to prepare these publications. We hope that all eight articles will be found interesting and valuable for cybersecurity researchers and all other interested readers.