Mobile Networks and Applications (2020) 25:234–235
https://doi.org/10.1007/s11036-019-01439-9

Editorial: Advanced Techniques for Memory Forensics Analysis

Andrea Lanzi[1]

Published online: 17 December 2019

Editorial:

The scope of digital forensics is expanding, and as we continuously explore mechanisms of hacking into devices to pull evidence, as well as find traces of evidence of complex hacks, it has become apparent that different cybersecurity communities have to start working together. Emerging technologies bring with them new avenues for cyber attacks, and this requires new strategies for cyber defense. Moreover, the increased complexity of communication and networking infrastructure has made the investigation of cybercrime more difficult. Clues of illegal activities are often buried in large volumes of data that needs to be sifted through in order to detect crimes and collect evidence. The field of digital forensics and cybercrime investigation has become very important for law enforcement, national security, and information assurance. In this special issue we will present three very high quality papers that work in such a direction.

The first article “Scoring system for cyber exercises based on graph distance” proposes a novel approach for the evaluation of the performance achieved by trainees involved in cyber security exercises realized through modern cyber ranges. Main contributions include: the definition of a distributed monitoring architecture for gathering relevant information about trainees activities; a novel algorithm for modeling the trainee activities in the form of a directed graph; a novel ranking algorithm that evaluates the correctness of a trainee solution based on the distance between its graph and the graph representing the optimal solution to the exercise.

In the second article titled “Disk Cluster Allocation Behavior in Windows and NTFS” The authors have studied the NTFS allocation algorithm and its behavior empirically for forensic purpose (e.g., timestamp verification). Their results show that files written as one large block are allocated areas of decreasing size when the files are fragmented. The decrease in size is generally applicable not only within files, but also between them. Hence a file having smaller fragments than another file is written after the file having larger fragments. They also found that a file written as a stream gets the opposite allocation behavior, i.e. its fragments are increasing in size as the file is written. The first allocated unit of a stream written file is always very small and hence easy to identify. The results of the experiment are of importance to the digital forensics field and will help improve the efficiency of for example file carving and timestamp verification.

In the last article with the title “A Market in Dream: The Rapid Development of Anonymous Cybercrime” the authors have conducted a comprehensive measurement and analysis on the Dream market, an anonymous online market that uses cryptocurrency as transaction currency. They first collect data between October 30th 2018 and March 1st 2019. Then they use decision tree-based approach to classify goods. Following they analyze the category of goods sold in the market, the shipping place of vendors. By analyzing more than 1,970,303 items, they find that the products sold in Dream Market are mainly drugs and digital goods. The authors estimate the total sales of all vendors, and find that an average monthly income is $14 million during the measurement period, which means that the market commission income is more than $560,000 per month. Based on these data, they use transaction cost theory to analyze the transaction attributes of illegal transactions, which shows that anonymous online market can reduce transaction cost of illegal transactions.

Acknowledgements The guest editors are thankful to our reviewers for their effort in reviewing the manuscripts.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

✉ Andrea Lanzi
andrea.lanzi@unimi.it

[1] Computer Science Department, Università degli Studi di Milano, Via Celoria 18, Milano 20135, MI, Italy

Andrea Lanzi is currently an Assistant Professor at Universita` degli studi di Milano at Computer Science Department, Italy where he’s leading a security Lab, called LaSER (systems and network security lab). From 2009 to 2013 He has been a Senior Research at Eurecom Graduate School in the S3 lab, located in Sophia Antipolis on the French riviera where He has been part of the iSeclab group. From 2007 to 2009 He has been Ph.D visiting scholar in Georgia Tech University US, in the GTISC Security Lab led by the Prof. Wenke Lee. He is interested in several aspects of Cyber Security. In particular, his main area of research deals with Host Intrusion Detection Systems (HIDS), memory errors exploitation, reverse engineering, malware and forensic analysis. In recent years He has mainly studied the application of emulation/virtualization and compiler techniques for malware analysis and detection in Android context. In addition He has been working on analyzing large-scale security malware datasets to investigate the behavior of current cyber threats.