Guest Editors’ Introduction: Special Issue on Cyber Crime

Wojciech Mazurczyk, Senior Member, IEEE, Thomas Holt, and Krzysztof Szczypiorski, Senior Member, IEEE

Cyber crimes reflect the evolution of criminal practices that have adapted to the world of information and communication technologies. Cybercriminality has become a curse of the modern world with the potential to affect every one nationally and/or internationally. Individuals, companies, governments and institutions may become victims as well as (involuntary) helpers of cyber criminals. The inability to provide effective cyber-security can potentially have a tremendous socio-economic impact on global enterprises as well as individuals.

In this IEEE Transactions on Dependable and Secure Computing (TDSC) special issue on Cyber Crime, we wanted to bring together the research accomplishments provided by researchers from academia and industry to present the latest research results in the field of cyber crime. In response to the call for papers, after rigorous review and careful revision, the following 12 papers were included in this special issue.

The first paper “Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service” by Shams Zawoad, Amit Kumar Dutta, and Ragib Hasan contains an analysis of the threats on cloud users’ activity logs considering the collusion between cloud users, providers, and investigators. Based on the presented threat model, the authors propose Secure-Logging-as-a-Service (called SecLaaS), which preserves various logs generated for the activity of virtual machines running in clouds and ensures the confidentiality and integrity of such logs.

The second paper “Assessing the Effectiveness of Moving Target Defenses using Security Models” by Jin B. Hong and Dong Seong Kim targets incorporation of Moving Target Defense techniques with a security model, called a Hierarchical Attack Representation Model, to provide a formal framework and to achieve the efficient and scalable method for analyzing the security.

The third paper “Data Lineage in Malicious Environments” by Michael Backes, Niklas Grimm, and Aniket Kate presents a new generic data lineage framework called LIME for data flow across multiple entities. The authors developed and analyzed a novel accountable data transfer protocol between two entities within a malicious environment by building upon oblivious transfer, robust watermarking, and signature primitives.

The fourth paper “Malware Detection in Cloud Computing Infrastructures” by Michael R. Watson, Noor-ul-hassan Shirazi, Angelos K. Marnerides, Andreas Mauthe and David Hutchison targets cloud anomaly detection approach, comprising dedicated detection components of the proposed cloud resilience architecture. The authors exhibit the applicability of novelty detection under the one-class Support Vector Machine (SVM) formulation at the hypervisor level, through the utilisation of features gathered at the system and network levels of a cloud node.

The fifth paper “Hacking is not random: a case-control study of webserver-compromise risk” by Marie Vasek, John Wadleigh, and Tyler Moore describes an interesting case-control study to identify risk factors that are associated with higher rates of webserver compromise. The authors inspect a random sample of around 200,000(!) webservers and automatically identify attributes hypothesized to affect the susceptibility to compromise, notably content management system and webserver type.

The sixth paper “Leveraging Strategic Detection Techniques for Smart Home Pricing Cyberattacks” by Yang Liu, Shiyan Hu, and Tsung-Yi Ho targets vulnerability of the electricity pricing model in the smart home system and considers two closely related pricing cyberattacks which manipulate the guideline electricity prices received at smart meters. As a result of this research the authors propose long-term detection techniques for such attacks.

The seventh paper “An Empirical Study of HTTP-based Financial Botnets” by Aditya K. Sood, Sherali Zeadally, and Richard J. Enbody contains an empirical study of the components, features and operations of some of the most widely deployed HTTP-based financial botnets (such as Zeus, SpyEye, ICE 1X, Citadel, Carberp, Tinba, Bugat and Shylock). The study provides critical insights into the design of these botnets and should help the security community to generate intelligence and develop more robust security solutions to defend against cyber attacks by these botnets.

The eighth paper “Industrial Control System Network Intrusion Detection by Telemetry Analysis” by Stanislav Ponomarev, and Travis Atkison contains an approach to detect the intrusions into network attached Industrial Control Systems by measuring and verifying data that is transmitted through the network but is not inherently the data used by the transmission protocol—network telemetry. Using simulated programmable logic controllers, depending on scenario the developed intrusion detection system was able to achieve almost 99.5 percent accuracy.

For information on obtaining reprints of this article, please send e-mail to: reprints.org, and reference the Digital Object Identifier below.

Digital Object Identifier no. 10.1109/TDSC.2015.2502407
The ninth paper “Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance” by Markus Riek, Rainer Boehme, and Tyler Moore presents a parsimonious model that builds on technology acceptance research and insights from criminology to identify factors that reduce Internet users’ intention to use online services. Using a structural equation modeling analysis of a representative pan-European sample the authors confirm the negative impact of perceived risk of cybercrime on the use of all three online service categories and support the role of cybercrime experience as an antecedent of perceived risk of cybercrime.

The 10th paper “Support Vector Machine-based Framework for Detection of Covert Timings” by Pradhunna L. Shrestha, Michael Hempel, Fahimeh Rezaei, and Hamid Sharif contains a proposal of the SVM-based framework for reliable detection of covert communications. This framework utilizes the fingerprints derived from the traffic under investigation to classify the traffic as covert or overt. The authors show that the machine-learning framework is able to blindly detect covert channels, even when the covert message size is reduced.

The 11th paper “Achieving Flatness: Selecting the Honeywords from Existing User Passwords” by Imran Erguler targets the security of the honeyword (decou password) systems and presents some remarks to highlight possible weak points of these systems. The author suggests an alternative approach that selects the honeywords from existing user passwords in the system in order to provide realistic honeywords—a perfectly flat honeyword generation method—and also to reduce storage cost of the honeyword scheme.

The 12th paper “FRoDO: Fraud Resilient Device for Offline micro-payments” by Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, and Matteo Signorini describes FRoDO, a secure off-line micro-payment solution that is resilient to point of sales data breaches. The proposed solution improves over up to date approaches in terms of flexibility and security. In this paper the architecture, components, and protocols of the proposed system are provided as well as an analysis of its effectiveness and viability.

In closing, the authors would like to thank all of the authors who have submitted their research to this special issue. They are also grateful for the many experts in this field who have participated in the review process and provided helpful suggestions to the authors for improving their work. They hope you enjoy the papers.

Wojciech Mazurczyk
Thomas Holt
Krzysztof Szczypiorski

Guest Editors

For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.