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 achive 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.

- *W. Mazurczyk and K. Szczypiorski are with the Institute of Telecommunications, Warsaw University of Technology, Nowowiejska Str. 15/19, 00-665, Warsaw, Poland. E-mail: {wmazurczyk, ksz}@tele.pw.edu.pl.*
- *T. Holt is with the School of Criminal Justice, Michigan State University, East Lansing, MI 48824. E-mail: holtt@msu.edu.*

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 Timing" by Pradhumna 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 Off-line 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

Wojciech Mazurczyk received the MSc, PhD (with honors), and DSc (habilitation) degrees in 2004, 2009, and 2014, respectively, all in telecommunications from the Warsaw University of Technology (WUT), Poland, where he is currently an associate professor. He is the author of more than 80 scientific papers, one patent application, and more than 30 invited talks on information security and telecommunications. He is the head in Bio-inspired Security Research Group (http://bsrg.tele.pw.edu.pl/) at the Institute of Telecommunications, WUT. His research interests include bioinspired cybersecurity and networking, information hiding and network security. He is the author or the coauthor of about 100 papers and many invited talks. He is also a TPC member of a number of refereed conferences, including IEEE INFOCOM, IEEE GLOBECOM, IEEE ICC, and ACSAC. He also serves as the reviewer for a number of major refereed international magazines and journals. From 2013, he is an associate technical editor for the *IEEE Communications Magazine*, *IEEE Comsoc*. He is a senior member of IEEE.

Thomas J. Holt received the MS and PhD degrees in 2003 and 2005, respectively, all from the University of Missouri-Saint Louis. He is an associate professor in the School of Criminal Justice at Michigan State University, and is the editor of the *Journal of Qualitative Criminal Justice and Criminology*. He has published over 40 peer-reviewed aritlces in major journals in criminology, sociology, and major IEEE conferences, as well as authoring or co-authoring multiple books, including *Cybercrime and Digital Forensics: An Introduction* (Routledge, 2015), *Cybercrime in Progress* (Routledge, 2016), and *Policing Cybercrime and Cyberterror* (CAP, 2015). His research interests include cybercrime markets, testing theories of cybercrime offending, and the law enforcement response to cybercrime at the state, local, and federal level.

Krzysztof Szczypiorski received the PhD (doctorate) and DSc (habilitation) degrees in 2007 and 2012, respectively, all in telecommunications from the Warsaw University of Technology (WUT). He also finished his postgraduate studies in psychology of motivation in 2013 from the University of Social Sciences and Humanities (SWPS), Warsaw, Poland. He graduated from Hass School of Business, University of California, Berkeley, in 2013. He is a professor of telecommunications at Warsaw University of Technology, Poland. He is the head and co-founder of Cybersecurity Division at the Institute of Telecommunications, WUT. He is a research leader of Network Security Group at WUT. His research interests include theory of observing change, network security, digital forensics, open-source intelligence, and wireless and ad-hoc communications. He is the author or the co-author of 150+ papers and 50+ invited talks. He is the inventor of two patents (one of them is pending). He is a senior member of the IEEE.