Guest Editors' Introduction: Special Section on Latest Developments for Security Management of Networks and Services

I. Introduction

AS THE backbone of communications amongst objects, humans, companies, and administrations, the Internet has become a great integration platform capable of efficiently interconnecting billions of entities, from RFID chips to data centers. This platform provides access to multiple hardware and virtualized resources (servers, networking, storage, applications, connected objects) coming from cloud computing and Internet-of-Things (IoT) infrastructures. From these resources that may be hosted and distributed amongst different providers and tenants, the building and operation of complex and value-added networked systems is enabled.

These networked systems are, however, subject to a large variety of security attacks, such as distributed denial-of-service (DDoS), man-in-the-middle (MITM), Web-injection and malicious software attacks, orchestrated in a more or less stealthy manner through the Internet. While they are gaining in sophistication and coordination (i.e., advanced persistent threats), these attacks may affect the fundamental security goals of confidentiality, integrity, availability and non-repudiation of resources. The accessibility, distribution, and increased complexity of networked systems make them particularly vulnerable targets. In that context, cybersecurity techniques offer new perspectives for protecting these networked systems, through the elaboration of intelligent and efficient management methods for detecting, analyzing and mitigating such attacks.

Given the strong interest in both industry and academia in this area, this second special issue on security management was opened to topics, including: network and service management for security, security of network and service management, security management architecture, protocols and APIs, secure and resilient design and deployment of networked systems, monitoring and detection of threats and attacks, artificial intelligence and data analytics, modeling for security management, and configuration and orchestration of security mechanisms.

Following the success of the TNSM Special Issue on Cybersecurity Techniques for Managing Networked Systems in 2020, this new 2021 Special Issue focuses on latest developments for security management of networks and services. The selected papers are addressing challenges that currently play a very important role in the security management of current and future network infrastructures, including advances in network monitoring, analytics and configuration.

II. Accepted Papers

This Special Issue welcomed submissions addressing the important challenges and presenting novel research and experimentation results on security management of networks and services. Survey papers that offer a perspective on related work and identify key challenges for future research have also been considered. Sixty-eight papers were submitted for this Special Issue. The submitted papers were thoroughly reviewed and, when needed some authors were given the time to update their papers and to address in detail the concerns raised by the reviewers. It was finally decided to accept sixteen papers for inclusion in this Special Issue.

From the selected papers in this Special Issue, the first ten papers deal with advanced methods for monitoring and detection using machine learning (Section III-A), while the six others are focused on configuration and mitigation techniques to counter attacks (Section III-B).

A. Advances in Monitoring and Detection

Efficient monitoring and detection methods are a key challenge for supporting the identification of threats and attacks at an early stage in network infrastructures. The papers in this category place a strong emphasis on machine learning (ML) techniques in different application domains, but also on techniques to address traffic encryption and anonymization.

In "A New Method for Flow-Based Network Intrusion Detection Using the Inverse Potts Model," C. Pontes *et al.* [item 2) in the Appendix] define a new algorithm, called Energy-based Flow Classifier (EFC), to support flow-based network intrusion detection using inverse Potts models. This algorithm is capable of accurately performing binary flow classification, and the experiments show that it is more adaptable to different data distributions than classical ML-based classifiers.

In "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," I. Siniosoglou *et al.* [item 3) in the Appendix] introduce an intrusion detection system, called MENSA, implementing a novel autoencoder-generative adversarial network (GAN) architecture for detecting anomalies and classifying cyber-attacks, by combining deep neural network techniques and

Digital Object Identifier 10.1109/TNSM.2021.3079189

taking into account the adversarial loss and the reconstruction difference.

In "Anomaly Detection for Insider Threats Using Unsupervised Ensembles," D. Le and N. Zincir-Heywood [item 4) in the Appendix] present an anomaly detection approach, where the focus is on employing unsupervised ML methods and different representations of data with temporal information for identifying signs of anomalous behaviours that may indicate insider threats. The purpose is to detect early signs of user behaviour changes flagged for further investigation, and potentially detect unknown attacks.

In "A Multi-Dimensional Deep Learning Framework for IoT Malware Classification and Family Attribution," M. Dib *et al.* [item 5) in the Appendix] define a novel multi-dimensional classification approach using Deep Learning (DL) architectures to combine the features extracted from strings- and image-based representations of the executable binaries towards accurate IoT malware classification and family attribution with a significantly improved accuracy.

In "DETONAR: Detection of Routing Attacks in RPL-Based IoT," A. Agiollo *et al.* [item 6) in the Appendix] design an intrusion detection system capable of dealing with multiple attacks while avoiding any RPL overhead. The proposed system is called DETONAR, standing for DETector of rOutiNg Attacks in RPL networks, and relies on a packet sniffing approach. DETONAR uses a combination of signature- and anomaly-based rules to identify any malicious behavior in the traffic.

In "In-Network Volumetric DDoS Victim Identification Using Programmable Commodity Switches," D. Ding *et al.* [item 7) in the Appendix] define an in-network DDoS victim identification strategy which has been implemented on a Tofino-based programmable switch using the domain-specific P4 language, proving that some limitations imposed by real hardware to safeguard processing speed can be overcome to implement relatively complex packet manipulations.

In "DNS Tunneling Detection by Cache-Property-Aware Features," N. Ishikura *et al.* [item 8) in the Appendix] propose a DNS tunneling detection method using cache-property-aware features. In particular, it relies on a specific feature to efficiently characterize DNS tunneling traffic and exploits a Long Short-Term Memory (LSTM)-based filter using this feature that achieves high detection rate of the DNS tunneling client while maintaining low misdetection rate.

In "FlowPic: A Generic Representation for Encrypted Traffic Classification and Applications Identification," T. Shapira and Y. Shavitt [item 9) in the Appendix] describe a novel approach for encrypted Internet traffic classification and application identification by transforming basic flow data into a picture, called a FlowPic, and then using known image classification deep learning techniques, such as CNNs, to identify the flow category (browsing, chat, video, etc.) and the application in use.

In "α-MON: Traffic Anonymizer for Passive Monitoring," T. Favale *et al.* [item 10) in the Appendix] introduce a flexible solution for privacy-preserving packet monitoring. It replicates input packet streams to different consumers, while anonymizing protocol fields according to flexible policies that cover all protocol layers. Beside classic anonymization mechanisms, it supports z-anonymization, a novel solution to obfuscate rare values that can be uniquely traced back to limited sets of users.

In "Edge Blockchain Assisted Lightweight Privacy-Preserving Data Aggregation for Smart Grid," W. Lu *et al.* [item 11) in the Appendix] define a blockchain-assisted lightweight privacy-preserving data aggregation schema for smart grids. It combines the homomorphic Paillier encryption and one-way hash chain techniques to ensure security performance, so that edge servers can reduce communication overheads by aggregating data from the same region and filter false data in advance.

B. Advances in Configuration and Mitigation

In security management, special attention should also be given to advanced configuration and mitigation techniques. In this section, the papers investigate the exploitation of novel methods to dynamically adapt to security threats and to benefit from network analytics to support the configuration of networked infrastructures.

In "Optimal Security Risk Management Mechanism for the 5G Cloudified Infrastructure," G. Carvalho *et al.* [item 12) in the Appendix] introduce an optimal security risk management mechanism based on a semi-Markov decision process framework to holistically minimize the risks of a Denial of Service (DoS) attack and Service Level Agreement (SLA) violations that might unfold at the 5G edge-cloud ecosystem.

In "A New Mutual Authentication and Key Agreement Protocol for Mobile Client - Server Environment," L. Tsobdjou *et al.* [item 13) in the Appendix] propose a mutual authentication protocol based on elliptic curve cryptography for mobile environments, intended to be lightweight as being designed for resource constrained mobile devices. They also introduce a formal and informal analysis of the security of the proposed protocol, by taking into account several security and performance properties.

In "Intrinsic Security and Self-Adaptive Cooperative Protection Enabling Cloud Native Network Slicing," W. Qiang *et al.* [item 14) in the Appendix] design an intrinsic cloud security approach as a unified paradigm to align cloud native technology with mimic defense and MTD (moving target defense). It makes full use of the new service features introduced by cloud native technology to implement a proactive defense mechanism of cloud native environments.

In "On the Flow of Software Security Advisories," L. Miranda *et al.* [item 15) in the Appendix] propose an analytical model to express the information flow through security advisories across multiple platforms. The model is based on a queueing network, where each platform corresponds to a queue which adds a delay in the information propagation and permits to collect temporal information about events associated with vulnerabilities from large-scale measurement campaigns.

In "From TTP to IoC: Advanced Persistent Graphs for Threat Hunting," A. Berady *et al.* [item 16) in the Appendix] define a formal model that dissects and abstracts the different

elements of an attack from both the attacker and defender perspectives. This model allows to compare the gap in knowledge and perceptions between the defender and the attacker, and to improve the quality of the threat hunting process by identifying false positives, adapting the logging policy and orienting investigations.

In "Blocklist Babel: On the Transparency and Dynamics of Open Source Blocklisting," A. Feal *et al.* [item 17) in the Appendix] perform an empirical analysis of the transparency and dynamics of the ecosystem of open blocklists providers. In particular, they look at the synergies between blocklists, observing a high overlap between specific providers, and finding that addition and removal of records is often propagated across those providers that have a high overlap.

ACKNOWLEDGMENT

The editors would like to thank explicitly all authors who submitted papers to this special issue and all reviewers for their valuable comments, useful suggestions, and timely submission of their reviews. Finally, we appreciate the support of the Editor-in-Chief, Filip De Turck.

RÉMI BADONNEL
University of Lorraine
LORIA-INRIA
54600 Villers-lès-Nancy, France

CAROL FUNG
Computer Science Department
Virginia Common Wealth University
Richmond, VA 23284 USA

SANDRA SCOTT-HAYWARD
School of Electronics
Queen's University Belfast
Belfast BT7 1NN, U.K.

QI LI
School of Computer Science and Engineering
Tsinghua University
Beijing 100084, China

JIE ZHANG
Interdisciplinary Graduate School
Nanyang Technological University
Singapore

CRISTIAN HESSELMAN
SIDN Lab
6825 MD Arnhem, The Netherlands
University of Twente
7522 NB Enschede, The Netherlands

APPENDIX

RELATED WORK

1) R. Badonnel, C. Fung, Q. Li, and S. Scott-Hayward, "Guest editors' introduction: Special issue on cybersecurity techniques for managing networked systems: Special section on cybersecurity techniques for managing networked systems," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 1, pp. 12–14, Mar. 2020.
2) C. Pontes, M. Souza, J. Gondim, M. Bishop, and M. Marotta, "A new method for flow-based network intrusion detection using the inverse potts model," *IEEE Trans. Netw. Service Manag.*, early access, Apr. 26, 2021, doi: 10.1109/TNSM.2021.3075503.
3) I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Trans. Netw. Service Manag.*, early access, May 7, 2021, doi: 10.1109/TNSM.2021.3078381.
4) C. Le and N. Zincir-Heywood, "Anomaly detection for insider threats using unsupervised ensembles," *IEEE Trans. Netw. Service Manag.*, early access, Apr. 8, 2021, doi: 10.1109/TNSM.2021.3071928.
5) M. Dib, S. Torabi, E. Bou-Harb, and C. Assi, "A multi-dimensional deep learning framework for IoT malware classification and family attribution," *IEEE Trans. Netw. Service Manag.*, early access, Apr. 23, 2021, doi: 10.1109/TNSM.2021.3075315.
6) Agiollo, M. Conti, P. Kaliyar, T. Lin, and L. Pajola, "DETONAR: Detection of routing attacks in RPL-based IoT," *IEEE Trans. Netw. Service Manag.*, early access, Apr. 26, 2021, doi: 10.1109/TNSM.2021.3075496.
7) Ding, M. Savi, F. Pederzolli, M. Campanella, and D. Siracusa, "In-network volumetric DDoS victim identification using programmable commodity switches," *IEEE Trans. Netw. Service Manag.*, early access, Apr. 15, 2021, doi: 10.1109/TNSM.2021.3073597.
8) N. Ishikura, D. Kondo, V. Vassiliades, I. Iordanov, and H. Tode, "DNS tunneling detection by cache-property-aware features," *IEEE Trans. Netw. Service Manag.*, early access, May 10, 2021, doi: 10.1109/TNSM.2021.3078428.
9) T. Shapira and Y. Shavitt, "FlowPic: A generic representation for encrypted traffic classification and applications identification," *IEEE Trans. Netw. Service Manag.*, early access, Apr. 6, 2021, doi: 10.1109/TNSM.2021.3071441.
10) T. Favale, M. Trevisan, I. Drago, and M. Mellia, "α-MON: Traffic anonymizer for passive monitoring," *IEEE Trans. Netw. Service Manag.*, early access, Feb. 9, 2021, doi: 10.1109/TNSM.2021.3057927.
11) W. Lu, Z. Ren, J. Xu, and S. Chen, "Edge blockchain assisted lightweight privacy-preserving data Aggregation for Smart Grid," *IEEE Trans. Netw. Service Manag.*, early access, Jan. 1, 2021, doi: 10.1109/TNSM.2020.3048822.
12) G. H. S. Carvalho, I. Woungang, A. Anpalagan, and I. Traore, "Optimal security risk management mechanism for the 5G cloudified infrastructure," *IEEE Trans. Netw. Service Manag.*, early access, Feb. 8, 2021, doi: 10.1109/TNSM.2021.3057761.
13) L. D. Tsobdjou, S. Pierre, and A. Quintero, "A new mutual authentication and key agreement protocol for mobile client–Server environment," *IEEE Trans. Netw. Service Manag.*, early access, Apr. 5, 2021, doi: 10.1109/TNSM.2021.3071087.
14) W. Qiang, W. Chunming, Y. Xincheng, and C. Qiumei, "Intrinsic security and self-adaptive cooperative protection enabling cloud native network slicing," *IEEE Trans. Netw. Service Manag.*, early access, Apr. 8, 2021, doi: 10.1109/TNSM.2021.3071774.
15) L. Miranda *et al.*, "On the flow of software security advisories," *IEEE Trans. Netw. Service Manag.*, early access, May 10, 2021, doi: 10.1109/TNSM.2021.3078727.
16) Berady, M. Jaume, V. Triem Tong, and G. Guette, "From TTP to IoC: Advanced persistent graphs for threat hunting," *IEEE Trans. Netw. Service Manag.*, early access, Feb. 3, 2021, doi: 10.1109/TNSM.2021.3056999.
17) Á. Feal *et al.*, "Blocklist babel: On the transparency and dynamics of open source blocklisting," *IEEE Trans. Netw. Service Manag.*, early access, Apr. 26, 2021, doi: 10.1109/TNSM.2021.3075552.

Rémi Badonnel is an Associate Professor of Computer Science with TELECOM Nancy, the Engineering School of Computer Science, University of Lorraine, France, where he is heading the Internet Systems and Security specialization. He is a Permanent Research Staff Member with the RESIST Team, LORIA—INRIA Nancy Grand Est, France. Previously, he worked on change management methods and algorithms for data centers with the IBM T. J. Watson Research Center, USA, and investigated autonomous smart systems with Oslo Metropolitan University, Norway. His research interests are mainly focused on network and service management, smart and autonomic environments, security and defense techniques, orchestration and chaining of services, cloud infrastructures, and Internet of Things. He has served as the TPC Co-Chair for the IFIP/IEEE International Symposium of Integrated Network Management (IM) in 2015, and for the IFIP/IEEE International Conference on Network and Service Management (CNSM) in 2019. He serves as the Chair of the IFIP TC6 Working Group 6.6 dedicated to the management of networks and distributed systems.

Carol Fung received the Ph.D. degree in computer science from the University of Waterloo, Canada. She is an Associate Professor with the Computer Science Department, Virginia Commonwealth University. Her research area is network management and cyber security, including trust management, resource allocation, game theory, Bayesian inference theory, and crowdsourcing. Her research has applications in SDN/NFV networks, 5G networks, cyber security, and smartphone systems. She has published more than 100 peer-reviewed papers. She was the recipient of the IEEE/IFIP IM Young Professional Award, the University of Waterloo Alumni Gold Medal, and best paper awards three times in IM/NOMS. She also received numerous prestigious awards and scholarships, including the Google Anita Borg Scholarship, the NSERC Postdoctoral Fellowship, the David Cheriton Scholarship, the NSERC Postgraduate Scholarship, and the President's Graduate Scholarship in UoW. She serves on multiple journal editorial boards and was the General Co-Chair of 2019 IFIP/IEEE International Symposium on Integrated Network Management.

Sandra Scott-Hayward received the Ph.D. degree from Queen's University Belfast (QUB). She is a Lecturer (Assistant Professor) with the School of Electronics, Electrical Engineering and Computer Science, and a member of the Centre for Secure Information Technologies, QUB. She has published a series of IEEE/ACM papers on security designs and solutions for softwarized networks based on her research on the development of network security architectures and security functions for emerging networks. She began her career in industry and became a Chartered Engineer in 2006 having worked as a Systems Engineer and an Engineering Group Leader with Airbus. She received the Outstanding Technical Contributor and Outstanding Leadership awards from the Open Networking Foundation in 2015 and 2016, respectively, having been elected and serving as the Vice-Chair of the ONF Security Working Group from 2015 to 2017. Amongst many other service memberships, she was the TPC Co-Chair for IEEE NFV-SDN 2020 and is an Associate Editor of IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT. She is the Director of the QUB Academic Centre of Excellence in Cyber Security Education, one of the first universities to be awarded this recognition by the U.K. National Cyber Security Centre.

Qi Li received the Ph.D. degree from Tsinghua University, where he is currently an Associate Professor with the Institute for Network Sciences and Cyberspace. He has worked with ETH Zürich, the University of Texas at San Antonio, and The Chinese University of Hong Kong. He heads the Internet and Cloud Security Group with a group of graduate students working on different topics in security. His research interests are in network and system security, particularly in Internet security, mobile security, and big data security. He is the co-recipient of several best paper awards, including awards from SecureComm 2017, IEEE ICPADS 2018, and IEEE DSC 2019. He is currently an Editorial Board Member of IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING and *ACM Digital Threats: Research and Practice*, and has served on the organization or program committees of various premier conferences.

Jie Zhang received the Ph.D. degree with the Cheriton School of Computer Science, University of Waterloo, Canada. He is currently an Associate Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research is in the general area of artificial intelligence and focuses on trust modeling and preference modeling for various emerging application domains, e.g., e-commerce, VANET, IoT, and collaborative systems. His papers have been published by top AI conferences, such as NeurIPS, AAAI, and IJCAI and top networking and security journals, such as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT. He was the recipient of the Alumni Gold Medal at the 2009 Convocation Ceremony. The Gold Medal is awarded once a year to honor the top Ph.D. graduate from the University of Waterloo. He has won several best paper awards at the conferences, such as IM, CNSM, and IFIPTM. He is also active in serving research communities. He is serving as the Senior Editor for the *Electronic Commerce Research and Applications* and an Associate Editor for IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT. He also served as the general chair and the PC chair for several international conferences.

Cristian Hesselman received the M.Sc. and Ph.D. degrees in computer science from the University of Twente, The Netherlands, in 1996 and 2005, respectively. He directs SIDN Labs, the research arm of the operator of the Netherlands' national top-level domain, .nl. His work focuses on advancing the Internet and future networks to support the higher degrees of trust and autonomy that modern digital societies need, for instance, through the design and evaluation of transparent and controllable networks and through large-scale infrastructure measurements. He is also a part-time Associate Professor with the University of Twente and a member of the Security and Stability Advisory Committee at ICANN.