Guest editorial: Special Issue on Novel Cyber-Security Paradigms for Software-defined and Virtualized Systems

ABSTRACT

The massive shift to “virtualization” paradigms has largely transformed the traditional computing models, by progressively eroding the typical strong link between applications and devices, hence requiring to rethink and reshape the structure and composition of services and infrastructures. On the one hand, the continuous disaggregation between the software and the hardware facilitates the migration of applications and services to different infrastructures. On the other hand, the growing “softwarization” trend allows the creation and disposal of even complex execution environments in a matter of minutes or seconds instead of days or weeks; this includes the provisioning of (virtual) computing and networking resources, the retrieval of software images, the processing of large data sets and the connection to an ever-growing Internet of Things.

The undergoing evolution has also fostered a groundbreaking transition in design and development patterns, from monolithic applications and closed silos to open and interconnected service meshes, which leverage cloud models, common interfaces, and orchestration paradigms. Pragmatic examples of such architectures in the networking domains are Network Functions Virtualization (NFV) and Software Defined Networking (SDN), which has not only brought more flexibility in network management, but has also opened new perspectives and opportunities in the realization of large, distributed, and pervasive cyber-physical systems. However, this has also determined an increase in the networks’ size and complexity, not to mention the security dependency on external software, services, data and infrastructures. The management of network devices has become more difficult than in the past, and the number of vulnerabilities that could be exploited in a cyberattack is nowadays bigger as well.

Unfortunately, cyber-security paradigms have not evolved at the same pace. As a matter of fact, the “security perimeter” model is still the predominant paradigm, but it cannot effectively address the many issues related to multi-tenancy, increased complexity, automated lifecycle management. Although cloud management and orchestration software is already mature for the market, many enterprises are reluctant to adopt such technologies due to security concerns, which still imply more traditional (and longer) processes. For instance, network services can today be designed as the composition of Virtual Network Functions (VNFs), including resource constraints, and then automatically deployed over self-provisioning virtualized infrastructures. VNFs can be rapidly turned on and set up, with respect to what a hardware device was used to require in the past. However, there are not as much fast security processes for checking software images, hardening an ever evolving topology, give visibility over functions running in external infrastructures.

A new breed of cyber-security paradigms and models are therefore necessary that could address the increased complexity and size of modern systems, not to mention the rapid escalation of advanced persistent threats and multi-vector attacks. Beyond more advanced techniques based on Machine Learning and other forms of Artificial Intelligence that could effectively cope the ever evolving threat landscape and attack patterns, it is also important to address the growing dynamicity of modern computing paradigms, self-provisioning models, service-oriented architectures, shared resources and software-defined infrastructures.

This special issue of Elsevier Computer Networks fostered new research work that took into consideration security challenges brought by the usage of public cloud, heterogeneous infrastructures and providers, and dynamic software deployment and orchestration mechanisms. The scope is not limited to a single topic, but covers several aspects that fall under the aforementioned evolutionary perspective.

To this end, after the two successful SecSoft workshops[1] that deal with these fields, we selected the best papers from these editions to invite the authors for submission of an extended paper for peer review and potential publication in this special issue.

Special issue overview

The review process resulted in the selection of 8 papers in the scope of this special issue. All submitted papers went through multiple review phases, with three international experts invited as reviewers for each. The accepted papers span three important areas of cyber-Security in software-defined and virtualized Systems: (i) Security of IoT systems; (ii) Malware detection in Virtualized environments and (iii) Cyber intelligence assistance in software-defined paradigms.

Security of IoT systems

The creation of cyber-physical systems requires the interconnection of smart devices and cloud applications through pervasive and capillary communication infrastructures. While there are already consolidated methodologies for securing the cloud and Internet communications, the weak posture of the Internet of Things is a major problem today, due to resource constraints and simplified usage models. In “On

ORCID(s):

[1] https://www.astrid-project.eu/secsoft/

the Suitability of Blockchain Platforms for IoT Applications: Architectures, Security, Privacy, and Performance," Brotsis *et al.*[1] provide a comprehensive and coherent review of the available blockchain solutions to determine their ability to meet the requirements and tackle the challenges of the IoT. Indeed, blockchain and distributed ledger technologies provide the means for creating truly trustless and secure solutions for IoT applications, but the risk is to introduce other defects, e.g. in terms of performance, making its adoption hard to achieve. The authors conclude that defenses provided by available platforms are not sufficient to thwart all the prominent attacks against blockchains, and only specific privacy aspects are considered by each mechanism.

In some domains, the IoT is simply created by connecting existing industrial systems to the Internet. The interconnection is facilitated by the usage of common protocols at the data link and network layer (i.e., Ethernet and IP), but this approach brings many cybersecurity risks because industrial applications have not been implemented having cybersecurity in mind. In "SPEAR SIEM: A Security Information and Event Management System for the Smart Grid," Radoglou-Grammatikis *et al.* [5] design and implement a Security Information and Event Management (SIEM) system, called SPEAR, capable of detecting, normalising and correlating events while specifically targeting cyberattacks and anomalies against a plethora of Smart Grid application-layer protocols.

The large availability of personal and sensitive devices, like smartphones, make them popular targets for attacks. In "RansomCare: Data-Centric Detection and Mitigation Against Smartphone Crypto-Ransomware," Faghihi and Zulkernine [3] present a data-centric detection and mitigation method against smartphone crypto-ransomware. Their work detects and neutralizes crypto-ransomware by employing dynamic and lightweight static analysis, based on user's data and data entropy; it also recovers user's lost files while preserving data privacy.

Malware detection in Virtualized environments

Looking for novel forms of malware and zero-day attacks is always challenging, because existing rules and signatures do not work. This task is also resource-consuming and difficult to apply in multi-tenancy systems (like the cloud), so the detection often focus on the identification of communications with remote control centers. The usage of steganography techniques is gaining momentum to elude such detection. Machine Learning (ML) is emerging today as a powerful mechanism to detect anomalies. This works quite well in traditional environments, where the topology, configuration and traffic patterns are relatively static, but it does not fit the dynamic nature of virtualized services. In "Unsupervised Packet-Based Anomaly Detection in Virtual Networks," Spiekermann and Keller [6] investigate the impact of virtual networks on the detection capabilities of machine learning algorithms for malware detection. In particular, they identify changes in virtual overlay and underlay networks that may point to anomalies, like malware, and evaluate forensic machine learning with datasets created in such conditions. In "Kernel-level Tracing for Detecting Stegomalware and Covert Channels in Linux Environments," Caviglione *et al.* [2] use simple eBPF programs to create custom statistics about the usage of the Flow Label field in the IPv6 header. The target is to detect anomalies while avoiding to keep track of each single flow, an approach which is not easily scalable on large Internet links.

Cyber intelligence assistance in software-defined paradigms

All modern network management paradigms (i.e., SDN, NFV, SFC) leverage software-defined paradigms that allow to create and change network services at run-time. This brings several opportunities for integrating cyber-defense with network control and management. In "An SDN-based Intrusion Detection System using SVM with Selective Logging for IP Traceback," Hadem *et al.* [4] analyze packet features extracted by OpenFlow switches with Support Vector Machines (SVM) at the controller to detect anomalous traffic and network intrusions. Besides dropping malicious traffic, selective logging of suspicious packets/flows is done at the controller, with relevant saving in terms of the overall memory resources, and IP traceback provides the ability to track the actual source of the packets in the eventuality of an attack. In "Citadel: Cyber Threat Intelligence Assisted Defense System for Software-Defined Networks," Yurekten and Demirci [7] present Citadel, a novel system architecture that retrieves CTI data, evaluates it considering the network topology, assets, and current defense policies, and selects and applies one or more network-level automated defense solutions. Their work leverages a new data model for effective sharing of Cyber-Threat Intelligence (CTI) data to automate network-level courses of action against cyber-attacks, by orchestrating network-level defense services and virtual network functions. Their implementation covers four defense services that can be used against various attack models.

Despite the availability of flexible and sophisticated authentication and authorization mechanisms at the application layer, security controls in the network are still largely based on source addresses, which are likely to be spoofed. In "An SDN-based Intrusion Detection System using SVM with Selective Logging for IP Traceback," Zhou *et al.* [8] consider existing limitations for source address validation implementation in Software-Defined Networks (SDN), which creates bindings between the IP address of a node and a property of the host's network attachment, but incurs performance cost in the controller. Their implementation reduces resource consumption by improving existing mechanisms with a fine-grained two-level structure for flexible matching of flow entry, a priority-based validation mechanism, and a state partition and transition module to optimize network performance under anomaly conditions.

Acknowledgment

We sincerely thank the authors for contributing their papers and the reviewers for their thorough assessment and

their work to improve the quality and presentation of each paper. We are very grateful to Editor-in-Chiefs Tommaso Melodia and Antonio Iera for their continuous support throughout the process and to Jacqueline Zhu, Chang Liu and Cmohammed Samiullah for their help with the administrative tasks associated with this special issue.

References

[1] Brotsis, S., Limniotis, K., Bendiab, G., Kolokotronis, N., Shiaeles, S., 2021. On the suitability of blockchain platforms for iot applications: Architectures, security, privacy, and performance. Computer Networks 191, 108005. URL: https://www.sciencedirect.com/science/article/pii/S1389128621001225, doi:https://doi.org/10.1016/j.comnet.2021.108005.

[2] Caviglione, L., Mazurczyk, W., Repetto, M., Schaffhauser, A., Zuppelli, M., 2021. Kernel-level tracing for detecting stegomalware and covert channels in linux environments. Computer Networks , 108010URL: https://www.sciencedirect.com/science/article/pii/S1389128621001249, doi:https://doi.org/10.1016/j.comnet.2021.108010.

[3] Faghihi, F., Zulkernine, M., 2021. Ransomcare: Data-centric detection and mitigation against smartphone crypto-ransomware. Computer Networks 191, 108011. URL: https://www.sciencedirect.com/science/article/pii/S1389128621001250, doi:https://doi.org/10.1016/j.comnet.2021.108011.

[4] Hadem, P., Saikia, D.K., Moulik, S., 2021. An sdn-based intrusion detection system using svm with selective logging for ip traceback. Computer Networks , 108015URL: https://www.sciencedirect.com/science/article/pii/S1389128621001274, doi:https://doi.org/10.1016/j.comnet.2021.108015.

[5] Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, I., Sesis, A., Vakakis, N., Tzovaras, D., Kafetzakis, E., Giannoulakis, I., Tzifas, M., Giannakoulias, A., Angelopoulos, M., Ramos, F., 2021. Spear siem: A security information and event management system for the smart grid. Computer Networks , 108008URL: https://www.sciencedirect.com/science/article/pii/S1389128621001237, doi:https://doi.org/10.1016/j.comnet.2021.108008.

[6] Spiekermann, D., Keller, J., 2021. Unsupervised packet-based anomaly detection in virtual networks. Computer Networks , 108017URL: https://www.sciencedirect.com/science/article/pii/S1389128621001286, doi:https://doi.org/10.1016/j.comnet.2021.108017.

[7] Yurekten, O., Demirci, M., 2021. Citadel: Cyber threat intelligence assisted defense system for software-defined networks. Computer Networks , 108013URL: https://www.sciencedirect.com/science/article/pii/S1389128621001262, doi:https://doi.org/10.1016/j.comnet.2021.108013.

[8] Zhou, Q., Yu, J., Li, D., 2021. A dynamic and lightweight framework to secure source addresses in the sdn-based networks. Computer Networks , 108075URL: https://www.sciencedirect.com/science/article/pii/S1389128621001663, doi:https://doi.org/10.1016/j.comnet.2021.108075.

Fulvio Valenza received the M.Sc. (summa cum laude) and Ph.D. (summa cum laude) degrees in computer engineering from the Politecnico di Torino, Turin, Italy, in 2013 and 2017, respectively. From January 2017 to September 2018, Fulvio was a Research Fellow at CNR-IEIIT, in which now he is a Research Associate. He is currently a PostDoc Research Fellow at the Politecnico di Torino, where he is with the Computer Network Group (NetGroup), in the Department of Control and Computer Engineering. He teaching many courses in computer networks and network security and he has been also involved in different EU projects. His main research interests are in the areas of cybersecurity and network management, with a special focus on the analysis and refinement of Network Security and Access Control Policy. He also works in modelling of Network Security Functions (NSF) and security management and orchestration in virtualized networks.

Matteo Repetto received the Ph.D. degree in Electronics and Computer Science in 2004 from the University of Genoa. From 2004 to 2009 he was a postdoc at University of Genoa. From 2010 to 2019 he was a Research Associate at CNIT. In 2019 he joined the Institute for Applied Mathematics and Information Technologies (IMATI), CNR. He has been teaching many courses in telecommunication networks and network security. He has been involved in several research national and international projects on quality of service, mobility in data networks, energy efficiency, cloud computing, and network function virtualization. He is currently the scientific and technical coordinator of the ASTRID and GUARD projects, which investigate new security paradigms for cloud services. He has co- authored over 60 scientific publications in international journals and conference proceedings. His current research interests include pervasive communications and mobility management, energy-efficient networking, software-defined networking and network function virtualization, cloud/fog/edge computing and network security.

Stavros Shiaeles received the B.Eng./M.Eng. degree in electrical and computer engineering and the Ph.D. degree in cybersecurity from the Democritus University of Thrace, Greece, in 2007 and 2013, respectively. He is currently a Senior Lecturer with the School of Computing and a member of the Cyber Security Research Group, University of Portsmouth. He holds an EC-Council Certified Ethical Hacker (CEH) Certificate, an EC-Council Advance Penetration Testing (CAST611) Certificate, an ISACA Cobit 5 Foundation Certificate, and a Cyberoam Certified Network and Security Professional (CCNSP) Certificate. He is an EC-Council Accredited Instructor and delivers training to professionals in U.K. and EU on cybersecurity. He has published more than 30 articles in international scientific journals, conferences, and books and has participated in EU-funded and national research and development projects. His research interests span the broad areas of cybersecurity, open-source intelligence, trust, blockchain, digital forensics, and machine learning applied in cybersecurity context. He is actively involved with professional bodies in U.K., Greece, and Cyprus and a Fellow of BCS and the Higher Education Academy. He has been a TPC member and a regular reviewer for a number of international journals and conferences.

Guest Editors:

Fulvio Valenza, Politecnico di Torino, Italy, fulvio.valenza@polito.it
Matteo Repetto, CNR-IMATI, Italy, matteo.repetto@cnr.it
Stavros Shiaeles, University of Portsmouth, UK, stavros.shiaeles@port.ac.uk