INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT
Int. J. Network Mgmt 2015; **25**:261–262
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/nem.1905

Editorial

Special issue on measure, detect and mitigate–challenges and trends in network security

A. Sperotto,[1,*,†] R. Hofstede,[1] A. Dainotti,[2] C. Schmitt[3] and G. Dreo Rodosek[4]

[1] *University of Twente, Enschede, The Netherlands*
[2] *Center for Applied Internet Data Analysis, UCSD, San Diego, SD, USA*
[3] *University of Zurich, Zurich, Switzerland*
[4] *Universität der Bundeswehr München, Munich, Germany*

Cybercrime has developed rapidly during the last decade, and recent years in particular have seen an unprecedented number of cyber attacks. Despite increased national and international efforts against cybercrime, cybercrime still has double-digit annual growth rates. As the number of services and systems connected to the Internet and migrating to cloud infrastructures increases, the ability to carry out attacks from a seemingly safe distance attracts more criminals and has made e-Crime a multi-billion dollar market. Furthermore, recent trends highlight that attacks target not only end hosts but also the Internet infrastructure itself, with attacks aiming at impeding the functioning of the domain name system and Internet backbones, for example.

Network security is also gaining enormous political attention in times of mass surveillance, advanced persistent threats, and data leakages. Security is not just about detecting external perpetrators and protecting Internet users against them anymore. Companies and government agencies are called to responsibility when it comes to publicly reporting data breaches against their infrastructures. For example, European governments have just approved new data protection regulations that force parties to report data breaches to both governments and those who may be potentially affected.

In this context, it becomes evident the importance of the steps we highlighted in this Special Issue: *measure, detect, and mitigate*. The dramatic trends in attack evolution call upon constant innovative solutions in each of these areas as well as in their synergistic combination. The goal of this Special Issue is twofold: we present contributions characterizing and measuring emerging network threats, as well as cutting-edge detection and mitigation techniques that are effective against network attacks and insider activities in today's and future small-to-enterprise-sized networks and network backbones.

A total of 14 papers was received for this Special Issue, for which we wish to thank all the authors. Three papers were considered, at an early stage, as out of scope and therefore did not go through the full review process. Of the 11 remaining papers, one was accepted after the first review round, five were rejected, and five underwent a second revision. In both review rounds, the papers received three reviews on average. In total, 33 reviewers participated in the review process, and based on their reviews, a final number of six papers were selected for publication.

The papers featured in this Special Issue show how network security research is gaining increasing attention in both academia and industry. Monitoring in large networks, for example, university networks and Internet service provider access and backbone networks, plays a major role for gathering a better understanding of malicious activities in today's networks. Bartos *et al.* investigate the use

*Correspondence to: Anna Sperotto, Design and Analysis of Communication Systems Group, University of Twente, Enschede, The Netherlands.
†E-mail: a.sperotto@utwente.nl

of novel flow sampling techniques for reducing the amount of monitoring data without impacting the performance of attack detection systems. Casas *et al.* study the use of unsupervised cluster and correlation analysis for attack detection in Internet service providers. The work of Zhang *et al.* focuses on classification of malicious and benign HTTP traffic by means of context-free grammars. Dedicated networks such as the Internet-of-Things and industrial control systems are by now also subject to attacks and need therefore targeted security solutions. Mayzaud *et al.* present mitigation strategies against topological inconsistency attacks in so-called low-power lossy networks. The work of Baiardi *et al.* emphasizes the need of selecting appropriate countermeasures for industrial control systems. Also, because of the sharp rise of encrypted traffic on the Internet, we generally see an increased interest for security in encrypted environments. The work of Velan *et al.* surveys existing methods for encrypted traffic analysis. Finally, it is worth noting that most of the papers in this Special Issue utilize some form of network flows (Velan *et al.*, Bartos *et al.*, Zhang *et al.*, and Casas *et al.*), confirming the interest for aggregated network information in the networking and security community.

The guest editors of this Special Issue wish to acknowledge the excellent work that has been performed by the reviewers, who have spent a considerable amount of their time providing high-quality reviews. We would also like to extend our thanks to the editorial board of the *International Journal of Network Management*, in particular to James Hong and Filip De Turck, for the great opportunity and their support in editing this Special Issue. Last but not least, we thank the Editorial Team of Wiley, for the support offered to the authors.

The work on this Special Issue was partly funded by FLAMINGO, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

DOI: 10.1002/nem