CALL FOR PAPERS

Special Issue of the International Journal on Network Management (IJNM) on
Measure, Detect and Mitigate –
Challenges and Trends in Network Security
Publication: September 2015

Scope of the Special Issue
Cybercrime has developed rapidly within the last decade and in particular the last years have seen an unprecedented amount of attacks. Despite increased national as well as international effort against cybercrime and the global financial crisis, cybercrime still has double-digit annual growth rates. On the one hand, more and more services and systems migrate to the Internet and cloud storage systems. On the other hand, the commercial success of the Internet and the possibilities to carry out attacks from a relatively safe distance attracts criminals and made e-Crime to a multi-billion dollar market. In addition, recent trends have highlighted that not only end-hosts are the target of attacks, but also the Internet infrastructure itself, with attacks aiming at impeding the functioning of e.g., the Domain Name System (DNS) or Internet backbones.

The dramatic trends in attack evolution call upon innovative solutions. Nowadays, detection and mitigation of network attacks are more than ever a must. However, current solutions need to evolve fast in order to cope with new attack scenarios. The goal of this Special Issue is twofold. We encourage, on the one hand, contributions characterizing and measuring emerging network threats; on the other hand we welcome submissions presenting cutting-edge detection and mitigation techniques effective against network attacks and insider activities in today and future small-to-enterprise sized networks and in backbones.

Contributions in the following areas are of specific interest, but are not limited to:

- Identification and Classification of Attacks
- Network Measurements to Understand Cyber-criminal Activities
- Network Attacks Characterization
- Multi-Layer Network Detection
- Inter-Domain and Cooperative Detection and Mitigation
- Detection in Encrypted Networks
- Supervised/Unsupervised Network Detection
- Alert and Event Correlation
- Visualization of Network Attacks and Alerts
- Interaction of Detection Systems and Exchange Formats
- Future Trends in Network Detection and Mitigation
- Mitigation of Large-Scale Distributed Attacks
- Novel Network Measurements and Data Analyses of Internet Malware

Submission Guidelines
Authors should submit their papers in PDF format only to http://mc.manuscriptcentral.com/nem
Paper submissions should not exceed 20 pages (double-space). Author instructions are available at
http://onlinelibrary.wiley.com/journal/10.1002/(ISSN)1099-1190/homepage/ForAuthors.html
and the respective LaTeX template can be found at
http://onlinelibrary.wiley.com/journal/10.1002/(ISSN)1099-1190/homepage/latex_class_file.htm

All submissions will be peer-reviewed. In case of acceptance, the final and camera-ready version has to take into account comments of reviewers and needs to follow the template's requirements.

Important Deadlines
Submission Deadline: December 1, 2014
Notification of Acceptance: March 1, 2015
Final Version: June 15, 2015
Publication: September 1, 2015
Submissions in PDF format only to
http://mc.manuscriptcentral.com/nem

Guest Editors
Gabi Dreo Rodosek - Universität der Bundeswehr Munich, Germany   gabi.dreo@unibw.de
Anna Sperotto - University of Twente, The Netherlands
a.sperotto@utwente.nl
Corinna Schmitt - University of Zurich, Switzerland
schmitt@ifi.uzh.ch
Rick Hofstede - University of Twente, The Netherlands
r.j.hofstede@utwente.nl
Alberto Dainotti - CAIDA, University of California, San Diego, USA   alberto@caida.org