Editorial

Shui Yu

School of Information Technology,
Deakin University,
Burwood, VIC 3125, Australia
Email: syu@deakin.edu.au

Biographical notes: Shui Yu received the B.Eng. and M.Eng. degrees from University of Electronic Science and Technology of China, Chengdu, China, in 1993 and 1999, respectively, and the Ph.D. degree from Deakin University, Victoria, Australia, in 2004. He is currently a Senior Lecturer with the School of Information Technology, Deakin University, Victoria, Australia. His research interests include network security, networking theory, and mathematical modelling. He is a Senior Member of IEEE and a Member of AAAS.

We are very pleased to present this Special Issue on Network Forensics, Security and Privacy to readers. There are 6 papers in this Special Issue, and some were published in the first International Workshop of Network Forensics, Security and Privacy, which was a joint workshop of the 32nd International Conference of Distributed Computing Systems, Macau, China, 18–21 June 2012. All the workshop papers were asked to conduct an essential extension, and reviewed again before they were accepted. One paper was an invited paper, which went through rigorous review process as well.

Network security and privacy are continuous challenges for researchers. We have witnessed ever-increasing new attack strategies, such as from brute force DDoS attacks to low-rate DDoS attacks, from IP fluxing to domain fluxing for botnets. When a new detection method is employed, attackers will develop another strategy to convict it. When a vulnerable package is patched, attackers try hard to find another vulnerable point to continue their attacks. The battle between defenders and attackers is an endless loop.

Network forensics is an emerging topic for network security communities. Unfortunately, we cannot apply the traditional forensic techniques directly. There are many challenges in this brand new field. For example, is a given image in the cyberspace a genuine one? how to identify anomaly information from the tremendous network traffic, especially when cyber criminals try their best to disguise their traces, and even mimic legitimate behaviour to fly under the radar. Another challenge is how to trace back to the people who commit network attacks, the current trace back methods can only reach zombies, rather than the human master head. Another great challenge is the constraints of network forensic techniques from the perspective of law enforcement. Many advanced forensic techniques are not necessarily feasible in practice because of possible contamination in terms of computer crime laws.

The papers of this Special Issue covers different aspects of current hot topics of security community, from cyber security to privacy protection, from industry based research to theoretical analysis.

Acknowledgements

We would like to take this opportunity to express our appreciation to all authors who submitted their work to this Special Issue. Moreover, we also appreciate the hard work of Dr Xinwen Fu and all anonymous reviewers who have done a wonderful job to raise up the quality of this Special Issue. Without their diligent work, the success of this Special Issue is simply not possible. We would also like to thank the Editor-in-Chief of *International Journal of Security and Networks* (*IJSN*), Professor Yang Xiao, for his strong support to give me such a great opportunity to edit this Special Issue. It is always a great pleasure to work with him. Finally, we hope this Special Issue is informative and helpful to readers.