Editorial

Khaled Salah*

Department of Information and Computer Science,
King Fahd University of Petroleum and Minerals,
P.O. Box 475, Dhahran 31261, Saudi Arabia
E-mail: salah@kfupm.edu.sa
*Corresponding author

Mohammed Sqalli

Department of Computer Engineering,
King Fahd University of Petroleum and Minerals,
P.O. Box 1447, Dhahran 31261, Saudi Arabia
E-mail: sqalli@kfupm.edu.sa

Mohamed Gouda

Department of Computer Sciences,
The University of Texas at Austin,
1 University Station (C0500),
Austin, Texas 78712-0233, USA
E-mail: gouda@cs.utexas.edu

Biographical notes: Khaled Salah is an Associate Professor of Computer Science. He received his BS in Computer Engineering with a minor in Computer Science from Iowa State University, USA, in 1990, MS in Computer Systems Engineering from Illinois Institute of Technology, USA, in 1994, and PhD in Computer Science from the same institution in 2000. He joined King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, in September 2000. He is currently with the Department of Information and Computer Science, teaching graduate and undergraduate courses in the areas of computer and network security, computer networks, and performance evaluation.

Mohammed H. Sqalli is an Assistant Professor in the Department of Computer Engineering at King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia. He obtained his PhD in Engineering – Systems Design (2002) and Master's in Computer Science (1996), both from the University of New Hampshire, USA. He is a recipient of a Fulbright Scholarship for the period of 1994–1998. He is also an IEEE member. His research interests include: network design and management, network security, traffic engineering, and iterative heuristics. He has over 25 publications in related areas.

Mohamed G. Gouda received his BSc in Engineering and in Mathematics from Cairo University, MA in Mathematics from York University, and Master's and PhD degrees in Computer Science from the University of Waterloo. He was with the Honeywell Corporate Technology Center at Minneapolis from 1977 to 1980. In 1980, he joined The University of Texas at Austin, where he currently holds the Mike A. Myers Centennial professorship in computer sciences. He has many awards and IEEE publications in the area of computer security and networks.

Over the past few years, attacks targeting private and global networks have become more easy-to-use, stealthier, more powerful, armed with advanced and sophisticated techniques to bypass, subvert and even target modern state-of-the-art security defence appliances and mechanisms as those of firewalls, intrusion detection/prevention systems, and antivirus software. The research and technical community in the field of IT security has recognised the utmost need for devising and designing more effective, intelligent, adaptive and active defence systems and mechanisms.

In this special issue on 'Recent advances in network security attacks and defences', we seek to bring together an exemplary set of research and technical works in this field, representing useful and fore-frontier research in modern security attacks and defences related to computer networks. We loosely organise eight selected papers into three sets: firewall security, countermeasures against botnets and

DDoS attacks in P2P networks, and networking monitoring and ARP spoofing.

The first set of three papers addresses security and performance challenges related to network firewalls. In the first paper, 'Analysis of firewall policy rules using traffic mining techniques', Abedin et al. show how to significantly enhance the effectiveness of a firewall filtering operations and ensure the correct implementation of firewall rules and policies. To accomplish this, the authors employ offline traffic mining techniques on only log files that are generated by the network firewalls. Using analysis and experimentation, the authors demonstrate that such techniques are highly accurate and effective. In the paper, 'Discovering last-matching rules in popular open-source and commercial firewalls', Salah et al. identify a potential probing mechanism that can be exploited by outside attackers to remotely discover last-matching rules of a firewall. If these rules get discovered by an attacker, the attacker can effectively be used to launch a low-rate DoS attack that can bring the firewall to its knees. The authors evaluate the resiliency of five of the most widely deployed network firewalls, of which three are open-source and two are commercial. The third paper is titled, 'Evaluation of gatekeeper proxies for firewall traversal in secure videoconferencing systems', in which Calyam et al. evaluated and studied possible techniques and best practices to prevent attackers from exploiting videoconferencing ports set by the firewall policy to pass video traffic. Attackers can possibly use these same open ports to bypass network firewall policy and penetrate inside internal networks.

The second set of two papers deals with mitigating the presence of botnets and DDoS attacks in peer-to-peer networks. In 'Detecting and blocking P2P botnets through contact tracing chains', Huang et al. propose a framework for detecting and blocking P2P botnets. The framework is based on tracing contact behaviours among peers to identify those peers that exhibit suspicious or abnormal symptoms. Using simulation, the authors show that their framework can be highly effective in quickly detecting and blocking the propagation of P2P botnets. In 'Request diversion: a novel mechanism to counter P2P-based DDoS attacks', Al-Duwairi and Mustafa propose a scheme to counter DDoS attacks originating from P2P networks. Their scheme is based on diverting users' requests destined to malicious sites to different fake sites. The authors demonstrated by simulation that their request-diversion scheme can reduce the attack request rate drastically.

The last set of three papers presents effective monitoring and marking techniques that deal with identifying unwanted traffic and tracing back the origin of packets, as well as evaluating effective solutions for ARP spoofing. In 'Real-time behaviour profiling for network monitoring', Xu et al. present novel network profiling and monitoring algorithms to identify suspicious events and sudden traffic surges as those of DoS attacks and worm outbreaks. In addition, the authors propose blocking strategies to reduce unwanted traffic. In 'A hybrid scheme using packet marking and logging of IP traceback', Malliga and Tamilarasi study and evaluate a novel hybrid approach based on marking and logging of IP packets in order to traceback the origin and path of a single packet. Using mathematical analysis and simulation, the authors show that their approach outperforms other existing approaches in terms of accuracy and effectiveness. In 'On investigating ARP spoofing security solutions', Trabelsi and El-Hajj evaluate, using several practical experiments, the existing solutions to counter ARP spoofing attacks. The authors conclude that these solutions have a limited success, and then they propose an optimal algorithm. The authors show that their proposed algorithm is more effective and require minimal overhead.

In presenting these diverse set of research efforts in the area of computer network security, we hope to provide more possible directions in future research related to network attacks and defences and to excite future research explorations in this intriguing, challenging and never-ending field, where ensuring security is a moving target. It is also our hope that the selected set of papers has shown to you, the readers, the depth of the challenges we face, and the existence of many open research issues.

We express our thanks to the authors who submitted papers and to the reviewers for their diligent and timely efforts and insightful comments on the quality and appropriateness of the submitted papers. It has been a pleasure to put together this issue on this very timely topic and we hope you enjoy it.