SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2015; **8**:1
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1180

EDITORIAL

Special issue on recent advances in network and information security—security and communication networks journal

Rapid advances in network and information security technologies are gradually making the dream of ubiquitous high-speed network access a reality. At the same time, however, such ubiquitous network access allows vandals and criminals to exploit vulnerabilities in networked systems on a widespread basis. This situation makes network and information security critical and challenging. In recent years, new topics and ideas in network and information security are flourishing, such as cloud computing, green radio, Internet of things, and heterogeneous networking. This special issue focuses on bringing in recent and novel research works on information and coding theory, network and information security, and designing best defenses and countermeasures to achieve more secure networks, protocols, systems, and applications.

The topics of this special issue interest include trust computing, secure communication techniques, malicious code analysis, and privacy-preserving systems.

After a very careful review of the many highly qualified submissions, the editorial committee accepted a total of eight papers in this special issue. Among these, one paper is related to trust computing, one relating to privacy-preserving system architecture, two relating to secure communication, one relating to encryption algorithms, and three relating to malicious code analysis.

The first paper is contributed by Li Tao and Hu Aiqun. They constructed an efficient trust chain model in system booting and running time to ensure security for mobile terminals.

Lei Jiang *et al.* in the second paper designed an efficient sparse matrix format and developed a regular expression matching architecture to accelerate regular expression matching on field-programmable gate arrays.

Xian Liu in the third paper derived the closed-form expressions of the probability of strictly positive secrecy capacity for two wireless communication systems.

The fourth paper is contributed by Jian Li *et al*. They proposed a quantum secure direct communication protocol by the use of a four-qubit cluster state to enhance the efficiency of eavesdropping detection.

Shengbao Wang *et al.* in the fifth paper presented an identity-based encryption scheme in multiple private key generator environments, which met chosen ciphertext security in a random oracle model.

Lejun Fan *et al.* in the sixth paper modeled the collaborative behaviors between different malicious functionality modules with Privacy Petri Net to analyze the behaviors of privacy theft malware.

The seventh paper is contributed by Buyun Qu *et al.* They empirically investigated the impact of network traffic morphing techniques on the actual traffic classification performance.

The last paper is contributed by Cui Xiang *et al.* They analyzed the essential property of a persistent bot behavior and proposed a new mitigation strategy to protect users.

On behalf of the editorial committee, we express our sincere thanks to all authors and reviewers for their grate contribution in this special issue. We are also very grateful to Professor Chen Hsiao Hwa, the editor-in-chief, and to the editorial staff for their excellent help and assistance. Without all of the contributions of these dedicated people, it would have been impossible to produce this special issue. We hope this special issue will inspire interested scholars to get involved in this promising and active research area.

Xueqi Cheng
Institute of Computing Technology, CAS
E-mail: cxq@ict.ac.cn

Jinhong Yuan
University of New South Wales
E-mail: j.yuan@unsw.edu.au

Ali Tajer
Princeton University
E-mail: tajer@princeton.edu

Aiqun Hu
Southeast University
E-mail: aqhu@seu.edu.cn

Wanlei Zhou
Deakin University
E-mail: wanlei.zhou@deakin.edu.au