CCPE SPECIAL ISSUE ON *SECURING CYBERSPACE*

Submission: `http://mc.manuscriptcentral.com/cpe`
CFP: `http://www.tulip.org.au/research/cpe2014si`

Special Issue of *Concurrency and Computation: Practice and Experience* (CCPE)

1. *Scope and Objective*

Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources. Today, as the growth of Internet, *Cyberspace* represents a wide range of topics in Web X.0-related research.

Social media emerging in Cyberspace is now reshaping the way businesses manage their sales and marketing assets. Unlike traditional media such as the TV, radio or newspaper, the social media (e.g., FaceBook, YouTube, Twitter, TripAdvisor, VirtualTourist, Houzz, Sina Weibo, Tencent WeChat and many other Web 2.0 sites) is characterized by user contributions, sharing, decentralization and being free. Not only are they gaining phenomenal popularity as the Web becomes accessible via all sorts of devices, they also have a strong influence on a brand making it a force that many organizations can no longer ignore. Many of us would have sought online reviews before making a purchase decision or forming an opinion, so do the rest of the consumers.

Unlike traditional media and sites, social media rely on user-generated content. Unfortunately, many of the user-generated content may not be that genuine as expected. It has been found that *astroturfers* (online paid posters) have been hired by public relationship companies to post product comments on different online communities and social networks, without even consuming the services or products. While online paid posters can be used as an efficient e-marketing strategy, they can also act maliciously by spreading gossip or negative information about competitors. More specifically, a group of paid posters could operate with well-coordinated attacks, and generate a desired result of positive or negative opinions, to attract attention or trigger curiosity. This is known as "Cyber-gossips", which can mislead online users, and put the individuals or a business in a compromising position or at serious risk.

So powerful are these online opinions that businesses cannot ignore their impact: if businesses do not manage their online reputation properly, they risk damaging their brand and sales assets, and the battlefield to do so is clearly played out in the social media of Cyberspace.

Recent years have witnessed increasing research attention on spammer detection in social networks. This trend raises the need for launching the special issue on *Securing Cyberspace* in Social Networks. Of course, to realize above goal, we can not leave the help of applications and techniques for information security, which have been developed for more than twenty or so years.

This issue aims to increase potential collaborations and partnerships by bringing together academic researchers and industry practitioners from data mining, network security, digital forensics, behavioral and psychology sciences with the objectives to present updated research efforts and progresses on foundational and emerging topics, exchange new ideas and identify future research directions.

In addition to selected top quality papers accepted and presented in the *C^3-2014* (`http://C3.tulip.org.au`, mirror site: "`http://c3.niuteam.cc/2014`") and *ATIS-2014* (`http://atis2014.tulip.org.au`, mirror site: "`http://atis.niuteam.cc/2014`"), we welcome any original high-quality research papers in methods, theories, techniques and tools for advancing the *Securing Cyberspace*.

2. *Topics of Interest*

All submissions will be rigidly peer reviewed to guarantee the quality. This special issue will focus on but not limited to the following topics:

(1) Attacks against Implementations
  - Digital Forensics
  - Key Recovery

(2) Curbing Cyber-Crime
  - Blog spam detection
  - Botnets prevention
  - Click spam detection
  - Cloud Security
  - Cyber-Gossip Spread Models
  - Collusive crime/piracy detection
  - Collusive crime/piracy detection
  - Collaborative social recommendation
  - Datasets for cyber-gossips detection
  - Dynamic/hidden group presentation
  - Group and group behavior detection, tracking and recognition
  - Group interaction, collaboration, representation and profiling
  - Graph-based behavior/social modeling
  - Identity authentication
  - Poster spam detection

(3) Data Privacy
  - Privacy Protection
  - Privacy Preservation in Data Release
  - Smart device information leaks
  - Trusted and Trustworthy Computing

(4) Evaluation, standards and protocols
  - Domain name server security
  - Transport Layer Security
  - Risk Evaluation and Security Certification
  - Security Management

(5) Security Implementations
  - Access Control
  - Authentication and Authorization
  - Cryptography
  - Data and System Integrity
  - Database Security
  - Distributed Systems Security
  - Information Hiding and Watermarking
  - Intellectual Property Protection
  - Intellectual Property Protection
  - Key Management
  - Operating System Security
  - Sequential/Parallel/Distributed behavior modeling

(6) Tools and Methodologies
  - Evaluation of Security
  - Evaluation of Security Tools

(7) Vulnerabilities
  - Digital Forensics
  - Intrusion Detection
  - Malicious software

3. *Submission Guidelines*

All submitted papers must be clearly written in English and should not have been previously published nor be currently under consideration for publication elsewhere. Note that published papers and those currently under review by other journals are prohibited. Substantially revised (minimum 30% of new content) versions of papers published in conference proceedings can be submitted. In this case, the original paper should also be enclosed together with an extension summary. All manuscripts and any supplementary material should be submitted through `http://mc.manuscriptcentral.com/cpe`.

Authors must select "`Special Issue Submission`" when they are in the "`Editor Selection`" submission step, and select "`Special Issue Paper`" in the "`Manuscript Type`" step. Then it is very important to enter the special issue title "`Securing Cyberspace`" when reaching the "`Special Issue Information`" step. A guide for authors, templates and samples for submitting papers is available at: `http://www.cc-pe.net/journalinfo/authors.html#guidelines`.

4. *Important Dates*

Manuscript Due:	December 20th, 2014
Reviews Due:	February 20th, 2015
Submission of Revised Papers:	March 20th, 2015
Final Decisions:	March 31st, 2015

5. *Guest Editors*

- Dr Gang Li, Senior Lecturer, Director of TULIP Lab, School of IT, Deakin University, Australia. (Email: `gang.li@deakin.edu.au`)
- A/Professor Wenjia Niu, Institute of Information Engineering, Chinese Academy of Sciences, China. (Email: `niuwenjia@iie.ac.cn`)
- Professor Li Guo, Institute of Information Engineering, Chinese Academy of Sciences, China. (Email: `guoli@iie.ac.cn`)
- Professor Lynn Batten, Information Security Research Director, School of IT, Deakin University, Australia. (Email: `lynn.batten@deakin.edu.au`)
- A/Professor Yinlong Liu, Institute of Acoustics, Chinese Academy of Sciences, China. (Email: `liuyl@hpnl.ac.cn`)
- Professor Guoyong Cai, Director of Guangxi Key Lab of Trusted Software, School of Computer Science and Engineering, Guilin University of Electronic Technology, China. (Email: `ccgycai@guet.edu.cn`)