# ACM Transactions on Autonomous and Adaptive Systems (TAAS)

Special Issue on

# Adaptive Security Systems

http://www.acm.org/pubs/taas/

## Guest Editors

Dr. Yang Xiang
School of Management and Information Systems
Central Queensland University
Australia
Email: y.xiang@cqu.edu.au
Phone: +61-7-4923-2748
Fax: +61-7-4930-9729

Prof. Wanlei Zhou
School of Engineering and Information Technology
Deakin University
Australia
Email: wanlei@deakin.edu.au
Phone: +61-3-9251-7603
Fax: +61-3-9251-7604

## Important Dates

Submission deadline: 15 Mar 2009
Notification date: 15 Aug 2009
Camera-ready due: 15 Nov 2009
Expected publication: 2010 (tentative)

## Submission Guideline

Authors are invited to submit manuscripts reporting important developments (or advances) in the topics related to the special issue. The submitted papers must be written in English and describe original research not published nor currently under review by other journals or conferences. Parallel submissions will not be accepted. If an earlier version of the manuscript was published/accepted in conferences, authors should state so in the cover letter. The manuscript must be a substantial extension to the previously published/accepted work and a summary of changes and a copy of the previous conference paper must be submitted together with the submission to the special issue.

The manuscripts should be formatted according to the ACM TAAS guidelines available from the journal homepage (http://www.acm.org/pubs/taas) and submitted to the guest editors through email y.xiang@cqu.edu.au.

Guest editors will pre-screen submitted manuscripts for their suitability in the issue. Submissions passing the pre-screen process will go through a rigorous peer-review process according to the standards of TAAS. Submitting a paper implies the willingness of reviewing one paper submitted to the special issue.

## Call for Papers

Security and privacy have been the major concern when people design computer networks and systems. In recent years, there has been significant increase in network and system attacks, such as frauds, distributed denial of service, viruses, worms, spyware, and malware, etc, causing huge economical and social damage. While the attack tools have become more easy-to-use, sophisticated, and powerful, interest has greatly increased in the field of building more effective, intelligent, robust, autonomous and adaptive security systems. It is envisioned that the large-scale adaptive security system will be essential to provide comprehensive protection to networks and systems in the future. The aim of such an adaptive security system is to provide authentication, access control, availability, integrity, privacy, confidentiality, dependability and sustainability to networks and systems, with autonomous and adaptive capabilities. However, building such a system faces significant challenges. We expect the adaptive security system to be

- self-organizing and can deal with different attacks without central control, and through contextual interactions with the peer nodes;
- adaptive and broad-spectrum to both known and unknown attacks with high true positive detection rate and low false positive detection rate;
- able to counteract the distributed intelligent attack systems which have the learning capability; and
- collaborative and optimized to intelligently safeguard the networks and systems with low management and maintenance cost.

These challenges need to be addressed under joint efforts from different areas such as network security, computer communications, AI, autonomic computing, bio-inspired techniques for security, adaptive systems, and others.

## Topics

This special issue on Adaptive Security Systems in ACM TAAS focuses on autonomous and adaptive security system theories, technologies, and real-life applications. Original papers are solicited for this special issue. Suggested topics include, but are not limited to:

### Adaptive Security System Theories

- Adaptive security architectures, algorithms, and protocols
- Autonomic learning mechanisms in security systems
- Intelligent attack systems and mechanisms
- Interactions between autonomic nodes of security systems
- Modeling of adaptive attack and defense mechanisms
- Theories in adaptive security systems

### Adaptive Security System Technologies

- Adaptive security systems design
- Adaptive security systems implementation
- Adaptive intrusion detection/prevention systems
- Self-organizing identity management and authentication
- Adaptive defense against large-scale attacks
- Simulation and tools for adaptive security systems

### Adaptive Security System Applications

- Benchmark, analysis and evaluation of adaptive security systems
- Distributed autonomous access control and trust management
- Autonomous denial-of-service attacks and countermeasures
- Autonomous wireless security systems
- Autonomous secure mobile agents and middleware
- Adaptive defense against viruses, worms, and other malicious codes