

**Security and Communication Networks (SCN), Wiley InterScience**  
**Special Issue on**  
**“Defending Against Insider Threats and Internal Data Leakage”**  
**<http://www.interscience.wiley.com/journal/security>**

**Overview**

The security analysis conducted by researchers in computer science and mathematics in the last decade has been working hard to prevent malicious attacks conducted by outside entities, such as hackers and intruders, or by extraneous malicious processes such as viruses, spywares, and all sort of malwares. However, security reports clearly reveal that an increasing number of threats come presently from insiders which, being legally authorized to have access to corporate resources, can exploit system vulnerabilities and data breaches to get access to systems and information. Actually, insiders can cause significant damages to enterprises, companies and even countries; they can threaten enterprises' reputation, weaken their national and international competitiveness, and compromise their overall business. Despite the fact that insiders' attacks happen less frequently than those conducted by outsiders, their consequences are definitely very severe, and recovering from an insider attacks is usually a daunting task. Therefore, countermeasures in terms of physical, managerial, and technical aspects are necessary to construct an integral security management system that can protect companies' major information assets and systems also from unauthorized and malicious attacks coming from inside.

This special issue collects scientific studies and works reporting on the most recent challenges and advances in security technologies and management systems about protecting an organization's information from corporate malicious activities. It aims to be the showcase for researchers that address the problems on how to prevent the leakage of organizations' information caused by insiders. The contributions to this special issue can conduct state-of-the-art surveys and case-analyses of practical significance, which, we wish, will support and foster further research and technology improvements related to this important subject.

Papers on practical as well as on theoretical topics are invited. Topics include (but are not limited to):

- Theoretical foundations and algorithms for addressing insider threats
- Insider threat assessment and modeling
- Security technologies to prevent, detect and avoid insider threats
- Validating the trustworthiness of staff
- Post-insider threat incident analysis
- Data breach modeling and mitigation techniques
- Authentication and identification
- Certification and authorization
- Database security
- Device control system

- Digital forensic system
- Digital right management system
- Fraud detection
- Network access control system
- Intrusion detection
- Keyboard information security
- Information security governance
- Information security management systems
- Risk assessment and management
- Log collection and analysis
- Trust management
- Socio-Technical Engineering Attack to Security and Privacy
- Secure information splitting and sharing algorithms
- Steganography and subliminal channels
- IT compliance (audit)
- Continuous auditing

### **Important Dates**

- Manuscript submission deadline: August 31, 2010
- Acceptance notification: October 31, 2010
- Camera-ready papers due: February 28, 2011
- Publication of special issue: Spring/Summer, 2011 (Tentative)

### **Submission Procedure**

Papers submitted to this special issue for possible publication must be original and must not be under consideration for publication in any other journals. Submissions of both in-depth research papers and review/application-oriented papers are encouraged. All submissions should be done in Wiley's manuscript central whose web link is: <http://mc.manuscriptcentral.com/scn>. For more detailed information on the submission requirements, please refer to the journal homepage at [www.interscience.wiley.com/journal/security](http://www.interscience.wiley.com/journal/security). When submitting the papers, the authors should make sure to choose the manuscript type as "Special Issue", enter the "Running Head" and the "Special Issue title" as "SCN-SI-23" and "Defending Against Insider Threats and Internal Data Leakage", respectively.

### **Guest Editors**

Dr. Elisa Bertino  
Purdue university, USA  
E-mail: [bertino@cs.purdue.edu](mailto:bertino@cs.purdue.edu)

Dr. Gabriele Lenzini  
SnT - Univ. of Luxembourg, Luxembourg  
E-mail: [gabriele.lenzini@uni.lu](mailto:gabriele.lenzini@uni.lu)

Dr. Marek R. Ogiela  
AGH University of Science & Technology, Poland  
E-mail: [mogiela@agh.edu.pl](mailto:mogiela@agh.edu.pl)

Dr. Ilsun You (Corresponding Editor)  
Korean Bible University, South Korea  
E-mail: ilsunu@gmail.com