Scientific Research
Open Access

Intelligent Information Management

ISSN Online: 2160-5920

Special Issue on Cyber Security

Call for Papers

Cyber security affects the fabric and infrastructure of modern society. It encompasses the interplay between science, technology, and engineering practices to protect networks, computers, programs, and data, from attacks, damage, insider threat, or unauthorized access (e.g., intrusion) for criminal and nefarious purposes. Cyber security is first and foremost about all-encompassing recognition, in general, and intrusion detection, in particular, and it is adversarial in nature. It is crucial for both biological (e.g., immune system) and machine Oracle systems to recognize patterns as friend or foe and to respond to them appropriately. Recognition is continuous and multi-layered. It includes detection (e.g., intrusion detection system), categorization, continuous authentication and identification, and re-authentication.

This special issue aims to provide a platform both for academic researchers and industry partners to advance their latest new work, stimulate discussion on existing and emerging challenges in cyber security, and propose and evaluate feasible solutions which will advance research in the field. This special issue is particularly interested in papers aimed to enhance cyber security defenses against adaptive, malicious, persistent, and tactical offensive threats. The interface between machine learning and big data and multi-faceted protective and self-managing defensive shields are of particular interest. The ultimate goal for this special issue is to make community and readership aware of new trends in cyber security and to inform and guide future promising research.

In this special issue, we intend to invite front-line researchers and authors to submit original research and review articles on exploring **Cyber Security**. Potential topics include, but are not limited to:

- Active authentication
- Advanced persistent threats (APT)
- Adversarial learning
- Biometrics
- Cloud computing
- Cryptography
- Denial and deception
- Differential privacy
- Ecosystems
- Human factors
- Impersonation and spoofing

Scientific Research
Open Access

Intelligent Information Management

ISSN Online: 2160-5920

- Interoperability
- Malware, phishing, spam, and fraud detection
- Mobile platforms
- Moving target detection (MTD)
- Multi-modality and data fusion
- Performance evaluation and test beds

Authors should read over the journal's For Authors carefully before submission. Prospective authors should submit an electronic copy of their complete manuscript through the journal's Paper Submission System.

Please kindly specify the "**Special Issue**" under your manuscript title. The research field "**Special Issue - *Cyber Security***" should be selected during your submission.

All submissions will be screened by the Guest Editor to ensure an appropriate match to the theme of the special issue, but submissions not meeting this criterion can still be considered for including in a future regular issue of the Journal.

Special Issue Timetable:

Submission Deadline	September 2nd, 2015
Publication Date	November 2015

Guest Editor:
Prof. Harry Wechsler
George Mason University, USA

For further questions or inquiries, please contact Editorial Assistant at iim@scirp.org.