Call for Papers

Journal of Defense Modeling and Simulation: Applications, Methodology, Technology (JDMS)

Special Issue: Cyber Risk and Vulnerability Estimation

Introduction

Recent strides in cyber operations, including description of the threat lifecycle, and component threat models, are currently limited only by the ability to estimate current system state, in terms of vulnerability and subsequent risk. The main objective of this special issue, therefore, is to lay down, a testable, repeatable, set of rules, policies, machine learning and artificial intelligence techniques that can be used to model and estimate cyber risk, vulnerabilities, and exploits in both current and designed systems. Recent improvements in learning models, deep learning, and big data analytics have the potential to capture the relationships among the security features and adversary activities to enhance cybersecurity defense and the estimation of vulnerabilities and exploits. Leveraging the cyber threat lifecycle, models for the special issue span from prevention to detection, through reconstitution, for a cyber-attack. Possible topics for authors to consider include:

- Modeling a cybersecurity environment with malware activities, adversary tactics, and anti-malware agents over any cybersecurity environment, including but not limited to networks, cyber-physical systems, connected vehicles, unmanned aerial systems.
- Leveraging adversarial machine learning, data analytics, deep learning, and tensorflow for enhancing cyber detection, malware defense, risk assessment, and agility maneuvers
- Modeling partial observability and temporal causality analysis of sensor measurements and observations for active cyber defense
- Development of trustworthy autonomous and collaborative agents for active cyber defense
- Device fingerprinting and physics to enhance security of cyber-physical systems
- Modeling and risk assessment of a cybersecurity environment with malware activities, online sensor measurements, and adversary tactics
- Modeling the risk and operational effectiveness of cyber security operation centers
- Leveraging machine learning and artificial intelligence technologies to enhance decision-making support and cyber defensive operations
- Develop proactive and reactive defense approaches to detecting exploits and protecting vulnerabilities over connected vehicles and cyber-physical systems

Papers submitted should not be concurrently under review at another conference, journal, or similar venue.

Instructions for Manuscript Preparation

For manuscript formatting and other guidelines, please visit the Author Guidelines for JDMS.

Note: Manuscripts must not have been previously published or be submitted for publication elsewhere. Each submitted manuscript must include title, names, authors’ affiliations, postal and
e-mail addresses, and a list of keywords. For multiple author submission, please identify the corresponding author.

**Due Dates**

Submission of papers September 30, 2018  
Expected date of publication Fall 2019

**Submissions for full paper review**

All manuscripts must be submitted electronically through the paper submission system to the [JDMS Manuscript Submission System](#). In the title page, author(s) must specifically mark that the paper is intended for this special issue as follows: "Submission for the Special Issue of JDMS: Cyber Risk and Vulnerability Estimation. Please follow the guidelines for submission on the Manuscript Central site.

**Final paper submissions**

Each final submission must be prepared based on the JDMS journal requirements (see the [Author Guidelines for JDMS](#) page).

**Guest Editors:**

Hasan Cam, ARL, US Army  
Sushil Jajodia, George Mason University  
Suresh K. Damodaran, MITRE  
Patrick McDaniel, Pennsylvania State University  
Hamed Okhravi, MIT Lincoln Laboratory

**For questions contact:**

Vicki Pate, Managing Editor  
Journal of Defense Modeling & Simulation  
[vmpate@scs.org](mailto:vmpate@scs.org)

Hasan Cam, Guest Editor  
[hasan.cam.civ@mail.mil](mailto:hasan.cam.civ@mail.mil)