Call for Papers

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

Special Issue: Model-Driven Paradigms for Integrated Approaches to Cyber Defense

Guest Editors

Dr. Alexander Kott, US Army Research Laboratory, Adelphi, Maryland, USA

Introduction

The growing military importance of cyber security is unquestionable. Increased use of commercial off the shelf (COTS) information technology and dependency on computerized information systems (CIS) for weapons, intelligence, communication, and logistics continues to increase vulnerability of military missions to cyber-attacks. Successful mission execution requires highly capable technologies that result in forces performing a broad range of defensive cyber operations for each step of an attacker's life cycle.

While many of these defensive cyber operations rely on essentially ad-hoc techniques, there is a growing realization, within the cyber community, that a comprehensive, systematic, principle-based, modeling and simulation approach is more likely to produce long-term, lasting, reusable approaches for defensive cyber operations. Such a paradigm is predicated on the creation and validation of mechanisms of modeling the organization whose mission is subject to assessment, the mission (or missions) itself, and the cyber-vulnerable systems that support the mission. The models are then used to simulate or otherwise portray the cyber-attacks and associate defensive phenomena and system operations, including the assessment of mission impact.

The main objective of this special issue is to offer the readers a broad yet integrated exploration of the field, while providing a publishing venue for researchers working toward a multi-purpose, integrated, system of cyber models, that guide a broad range of cyber security operations; examples include vulnerability analysis, intrusion prevention, intrusion detection, analysis, forensics, attribution, mission impact assessment and recovery.

Candidate model driven paradigms questions for cyber defense include - are there applications of the model-driven paradigm that are more likely to prove fruitful in near-term than others? What can be learned and adopted from the ongoing efforts, such as experiences in the European Union Panoptesec program that explores a model-based approach? What are ways to populate and validate models in an affordable fashion? Is the model-driven paradigm defeated by ever growing diversity and diffusion of IT infrastructures, such as Internet of Things? What commercial tools are emerging that can support the model-driven paradigm? Could these approaches be adapted for military-specific requirements?

Possible topics for authors to consider include:

- Theoretical foundations and formulations of the model-driven paradigm
- Relevance of game-theoretic and control-theoretic approaches
- Formal languages for model specification

- Assessment of barriers to successful use of the model-driven paradigm
- Potential techniques for using model-driven paradigms for cyber defense problem-solving at different phases of cyber operations (e.g., prior, during and after discovery of a cyber compromise)
- Analysis of known related approaches and methods
- Complexity and completeness of the models
- Feasibility of automated or semi-automated generation of models
- Modeling of the adversary
- Human factors in the models
- Calibration of the models
- Validation of the models
- Maintenance of the models
- Utility functions to be used in conjunction with models

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, 2016
Expected date of publication	Summer 2017

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: Model-Driven Paradigms for Integrated Approaches to Cyber Defense. 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:

- **Alexander Kott, PhD**
  Chief of Network Science Division, US Army Research Laboratory, Adelphi, Maryland, USA
- **Nazife Baykal, PhD**
  Professor, Director of Informatics Institute and Chair, Cyber Security Department, Middle East Technical University, Ankara, Turkey
- **Yilmaz Cankaya**
  Chief Researcher, TÜBITAK BILGEM Cyber Security Institute, Kocaeli, Turkey
- **Bob Madahar, PhD**
  Professor, Senior Fellow, DSTL, Porton, United Kingdom
- **Col. Nikolai Stoianov, PhD**
  Associate Professor, Defence Institute "Prof. Tsvetan Lazarova", Sofia, Bulgaria
- **Margaret Varga, PhD**
  Director at Seetru Ltd, visiting fellow at the University of Oxford. Bristol, United Kingdom

For questions contact:

Vicki Pate, Managing Editor
Journal of Defense Modeling & Simulation
vmpate@scs.org

Dr. Alexander Kott, Guest Editor
alexander.kott1.civ@mail.mil