CALL FOR PAPERS

Deadline Extended

ACM Transactions on Management Information Systems

Special Issue on Analytics for Cybersecurity and Privacy

Guest Editors:
Dr. Hsinchun Chen, Regents Professor, Management Information Systems, University of Arizona (hchen@eller.arizona.edu)
Dr. Murat Kantarcioglu, Professor, Computer Science, UT Dallas (muratk@utdallas.edu)
Dr. Sagar Samtani, Assistant Professor, Information Systems and Decision Sciences, University of South Florida (ssamtani@usf.edu)

Background:

The rapid proliferation of computing technologies has led to modern society's irreversible reliance on complex information systems (IS) to execute day-to-day operations. Unfortunately, these systems often contain numerous vulnerabilities that allow malicious hackers from across the globe to circumvent cybersecurity controls and manipulate them in a fashion not intended by the developer. These cyber-attacks result in hundreds of billions of dollars of loss and jeopardize the privacy of hundreds of millions of citizens. Increasingly sophisticated attack methods developed and used by cyber criminals and the growing role of outdated cyberinfrastructure and malicious insiders in several recent large-scale security breaches clearly indicate that traditional reactive approaches to information security and privacy can no longer keep up. Analytics is the key element in enhancing cyber resilience. To date, numerous social media analytics, stream data mining, social network analysis, and adversarial modeling, have been applied on terabytes of heterogeneous data ranging from the traditional internal server and application logs for vulnerability and risk assessment, to the emerging external adversarial hacker community (i.e., Dark Web) threats for proactive cyber threat intelligence (CTI). However, the highly dynamic threat landscape necessitates the development of novel analytics to quickly sift through large quantities of structured, unstructured, and semi-structured data to identify patterns, emerging threats, and key hackers. Ultimately, such advances can improve modern society's cybersecurity posture and protect the privacy of millions of people across the globe.

Scope and Topics of Interest:

This special issue seeks high quality papers related to emerging applications, techniques, and methodologies related to analytics for cybersecurity and privacy applications. Topics of interest include, but are not limited to:

- Dark Web Analytics for Proactive Cyber Threat Intelligence applications
- Open Source Intelligence (OSINT) and Social Media Intelligence (SOCINT) analytics for cybersecurity applications
- Adversarial machine learning for cybersecurity or privacy applications
- Phishing analytics (e.g., email, website, mobile, etc.)
- Security Intelligence Augmentation (e.g., human-in-the-loop systems)
- Big Data malware analysis (e.g., APT, static, dynamic, Hadoop/SPARK-based)
- IoT analysis (e.g., fingerprinting, anomaly detection, network telescopes, measurements etc.)
- Real-time analytics for threat detection (e.g., stream mining)
- Security data fusion (e.g., event correlation)
- Privacy analytics (e.g., pre-post GDPR analysis)
- Data anonymization techniques for privacy
- Privacy preserving data mining

All accepted manuscripts are expected to make a significant scientific contribution and present a rigorous evaluation of the Information Systems Outcomes focus on implementation in real world practices and analysis of real world practices to advance real world outcomes.

Submission Information:

For submission instructions and reviewing procedure, please refer to **https://tmis.acm.org/authors.cfm** and select the paper type for submission called "*Special Issue on Analytics for Cybersecurity and Privacy*." All papers will be reviewed by three external reviewers, plus at least one guest editor.

Editorial Timeline (*Extended*):

Submission Deadline: November 15, 2019
Notification to Authors (first round): February 15, 2020
Revision Deadline: April 30, 2020
Final Notification to Authors: August 1, 2020
Publication Date (tentative): December 2020

TMIS is indexed by the Emerging Sources Citation Index (ESCI) and other scientific databases, such as SCOPUS, INSPECT, and Ei Compendex (EI). For further information, please visit **tmis.acm.org.**

Association for Computing Machinery