Security and Communication Networks

Special Issue on

Analytical Models and Decision Making in Adaptive Security

CALL FOR PAPERS

Adaptive security is a decision-making approach for protecting systems infrastructure and data by detecting threats and malicious behaviors over time and taking the most secure and efficient actions to safeguard the underlying computer systems. The basic capability of such reactive systems is the ability to adapt with respect to underlying contexts and respond to complex and continuously changing dynamic environments. A typical architecture for implementing adaptive security consists of mechanisms that perform prevention, detection, response, and prediction.

Dynamic systems and environments where the underlying operational contexts and attack surfaces are frequently changing require solid and fundamental security mechanism. The attack surface exposed to an adversary should be minimized and unpredictable at any given time. The security system in such environments should recommend the best and most secure adaptive configurations and actions in response to the changes in the environment. Modeling and decision making in such uncertain environment is also a challenging problem that needs rigor mathematical and analytical foundation and security schemes.

Analytical models are mathematical abstractions of problems by which the solutions to the abstract model explain the changes in the real problem domain. The mathematical representation and abstraction of the problem take into account several factors such as relationships between observed variables and noises that explain the variance or uncertainty observed in the system. Recent advances in mathematical and data-driven decision making and in particular data mining, machine learning, and more importantly deep learning have enabled researchers to model dynamic domains more precisely.

This special issue focuses on security and privacy problems and challenges related to adaptive security. The call seeks research articles and review articles identifying novel challenges and approaches to model adaptive security in dynamic and continuously changing environments.

Potential topics include but are not limited to the following:

- Theoretical foundation and analytical reasoning of adaptive security
- Deep learning and machine learning-based approaches of adaptive security
- Optimization of security policies
- Economical modeling of security
- Heuristic-based security enforcement
- Risk assessment and threat modeling of adaptive security
- Probabilistic and uncertainty modeling
- Genetic and evolutionary approaches
- Adaptive security in Internet of Things and cyberphysical systems
- Adaptive security protocols, policies, and requirements
- Adaptive and context-aware access controls
- Empirical studies and industrial experiences related to adaptive security

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/amdm/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Akbar S. Namin, Texas Tech University, Lubbock, USA
akbar.namin@ttu.edu

Guest Editors
Rakesh M. Verma, University of Houston, Houston, USA
rmverma@cs.uh.edu

Rattikorn Hewett, Texas Tech University, Lubbock, USA
rattikorn.hewett@ttu.edu

Submission Deadline
Friday, 28 June 2019

Publication Date
November 2019