9th Conference on Decision and Game Theory for Security – GameSec 2018

Seattle, WA, USA

29TH – 31ST OCT 2018

Call for Papers

Recent advances in information and communication technologies pose significant security challenges that impact all aspects of modern society. The *9th Conference on Decision and Game Theory for Security* in Seattle, Washington, USA, focuses on protection of heterogeneous, large-scale and dynamic systems as well as managing security risks faced by critical infrastructures through rigorous and practically-relevant analytical methods. *GameSec 2018* invites novel, high-quality theoretical and practical-relevant contributions, which apply decision and game theory, as well as related techniques such as distributed optimization, dynamic control and mechanism design, to build resilient, secure, and dependable networked systems. The goal of *GameSec 2018* is to bring together academic and industrial researchers in an effort to identify and discuss the major technical challenges and recent results that highlight the connections between game theory, control, distributed optimization, economic incentives and real-world security, reputation, trust and privacy problems.

TOPICS INCLUDE (BUT NOT RESTRICTED TO)

- Game theory, control, and mechanism design for security and privacy
- Decision making for cybersecurity and security requirements engineering
- Security and privacy for the Internet-of-Things, cyber-physical systems, cloud computing, resilient control systems, and critical infrastructure
- Pricing, economic incentives, security investments, and cyber insurance for dependable and secure systems
- Risk assessment and security risk management
- Security and privacy of wireless and mobile communications, including user location privacy
- Socio-technological and behavioral approaches to security
- Empirical and experimental studies with game, control, or optimization theory-based analysis for security and privacy
- Adversarial Machine Learning and the role of AI in system security

TUTORIAL TRACK ON "GAME THEORY AND DECEPTION"

Cyber attacks on both databases and critical infrastructure have threatened public and private sectors. Meanwhile, ubiquitous tracking and wearable computing have infringed upon privacy. Advocates and engineers have recently proposed using defensive deception as a means to leverage the information asymmetry typically enjoyed by attackers as a tool for defenders. In this tutorial, we give the audience an overview on the application of game theory to model deception for cybersecurity and privacy. The goal of this tutorial is to elaborate the taxonomy of deception, to provide the state-of-art literature, and to discuss recent advances in deceptive technologies in cybersecurity and privacy.

SPECIAL TRACK ON "ADVERSARIAL AI"

AI techniques have made significant inroads into security applications, such as crime prediction and detection in physical security, and intrusion and malware detection in cybersecurity. An important challenge in such adversarial applications of AI is that sophisticated malicious parties can manipulate the AI decision process, for example, by changing the decision environment or poisoning data used for learning, in order to degrade its effectiveness. The research area of *Adversarial AI* aims to understand vulnerabilities of AI systems to such adversarial tampering, as well as to develop techniques which make intelligent autonomous decision making robust to adversarial subversion. This special track invites submissions on approaches for attacking and defending AI systems, including research on adversarial machine learning, planning in adversarial settings, adversarial crowdsourcing, and more broadly on the use of AI in security and privacy.

GENERAL CHAIRS

Tamer Başar (Univ. of Illinois at U-C)
Radha Poovendran (Univ. of Washington)

TPC CHAIR

Linda Bushnell (Univ. of Washington)

TUTORIAL TRACK CHAIR

Quanyan Zhu (New York Univ.)

SPECIAL TRACK CHAIR

Eugene Vorobeychik (Vanderbilt Univ.)

LOCAL ARRANGEMENTS CHAIR

Lillian Ratliff (Univ. of Washington)

PUBLICITY CHAIRS

Europe: Dario Bauso (Univ. Sheffield)
Asia/Australia: Jun Moon (UNIST)
North America: Miroslav Pajic (Duke Univ.)

WEB CHAIR

Andrew Clark (WPI)

STEERING BOARD

Tansu Alpcan (The Univ. of Melbourne)
John S. Baras (Univ. of Maryland)
Tamer Başar (Univ. of Illinois at U-C)
Anthony Ephremides (Univ. of Maryland)
Milind Tambe (Univ. of Southern California)

IMPORTANT DATES

Abstract submission (optional): 1 June 2018
Paper submission: 25 June 2018 (extended)
Decision notification: 6 August 2018
Camera-ready submission: 13 August 2018
Conference: **29th – 31st October 2018**

Photo © www.seanhoyt.com