Modern societies are becoming dependent on information, automation, and communication technologies more than ever. Managing the security of the emerging systems, many of them safety critical, poses significant challenges. The 11th Conference on Decision and Game Theory for Security will take place from October 28-30, 2020 at College Park, Maryland, USA. It focuses on protection of heterogeneous, large-scale and dynamic cyber-physical systems as well as managing security risks faced by critical infrastructures through rigorous and practically relevant analytical methods. GameSec 2020 invites novel, high-quality theoretical and practically relevant contributions, which apply decision and game theory, as well as related techniques such as optimization, machine learning, dynamic control and mechanism design, to build resilient, secure, and dependable networked systems. The goal of GameSec 2020 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, machine learning, economic incentives and real-world security, reputation, trust and privacy problems.

**MAIN TOPICS**

- 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

**Special Track on “Machine Learning and Cyber Security”**

Machine learning provides a set of useful analytic and decision-making tools for a wide range of applications. Security research aims to address the issue of protecting networks from adversarial behaviors. The confluences between the two are increasingly important as we witness recent advances in adversarial machine learning and machine learning for security big data processing. This special track invites submissions on various data-centric models and approaches. For submissions, please use the topic “Machine Learning and Cyber Security.”

**Call for Papers**

**GENERAL CHAIR**
John S. Baras (University of Maryland)
Radha Poovendran (University of Washington)

**TPC CHAIR**
Quanyan Zhu (New York University)

**PUBLICATION CHAIR**
Juntao Chen (Fordham University)

**SPECIAL SESSION CHAIR**
Charles Kamhoua (Army Research Laboratory)

**PUBLICITY CHAIR**
Junaid Farooq (University of Michigan)
Stefan Rass (Universität Klagenfurt, Austria)
Arunesh Sinha (Singapore University of Management)

**WEB CHAIRS**
Andrew Clark (Worcester Polytechnic Institute)

**STEERING BOARD**
Tansu Alpcan (University of Melbourne)
John S. Baras (University of Maryland)
Tamer Başar (University of Illinois at U-C)
Anthony Ephremides (University of Maryland)
Radha Poovendran (University of Washington)
Milind Tambe (Harvard University)

**IMPORTANT DATES**

Abstract submission (optional): July 20, 2020
Paper submission: July 27, 2020 (firm)
Decision notification: August 31, 2020
Camera-ready submission: September 14, 2020
Conference: October 28 – October 30, 2020