1. Record Nr. UNISA996418284703316

Titolo	Decision and game theory for security : 11th International Conference, GameSec 2020, College Park, MD, USA, October 28-30, 2020, proceedings / / Quanyan Zhu [and three others] (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] ©2020
ISBN	3-030-64793-5
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XI, 518 p. 131 illus., 111 illus. in color.)
Collana	Lecture notes in computer science ; ; 12513
Disciplina	005.8
Soggetti	Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Machine Learning and Security -- Distributed Generative Adversarial Networks for Anomaly Detection -- Learning and Planning in the Feature Deception Problem -- A Realistic Approach for Network Traffic Obfuscation using Adversarial Machine Learning -- Adversarial Deep Reinforcement Learning based Adaptive Moving Target Defense -- Lie Another Day: Demonstrating Bias in a Multi-Round Cyber Deception Game of Questionable Veracity -- Cyber Deception -- Exploiting Bounded Rationality in Risk-based Cyber Camouflage Games -- Farsighted Risk Mitigation of Lateral Movement Using Dynamic Cognitive Honeypots -- Harnessing the Power of Deception in Attack Graph-Based Security Games -- Decoy Allocation Games on Graphs with Temporal Logic Objectives -- Popular Imperceptibility Measures in Visual Adversarial Attacks are Far from Human Perception -- Cyber-Physical System Security -- Secure Discrete-Time Linear-Quadratic Mean-Field Games -- Detection of Dynamically Changing Leaders in Complex Swarms from Observed Dynamic Data -- Moving Target Defense for Robust Monitoring of Electric Grid Transformers in Adversarial Environments -- Security of Network Systems -- Blocking Adversarial Inuence in Social Networks -- Normalizing Flow Policies for Multi-agent Systems -- A Game Theoretic Framework for Software Diversity for Network Security -- Partially Observable Stochastic Games for Cyber Deception against Network Epidemic -- Combating Online

Counterfeits: A Game-Theoretic Analysis of Cyber Supply Chain Ecosystem -- Theoretic Foundations of Security Games -- On the Characterization of Saddle Point Equilibrium for Security Games with Additive Utility -- MASAGE: Model-Agnostic Sequential and Adaptive Game Estimation -- Using One-Sided Partially Observable Stochastic Games for Solving Zero-Sum Security Games with Sequential Attacks -- A Data-Driven Distributionally Robust Game using Wasserstein Distance -- Security Games over Lexicographic Orders -- Game Theory on Attack Graph for Cyber Deception -- Attacking Machine Learning Models for Social Good -- A Review of Multi Agent Perimeter Defense Games -- Hardware Security and Trust: A New Battlefield of Information -- A Data Mining Friendly Anonymization Scheme for System Logs using Distance Mapping -- Security Games with Insider Threats -- Securing Next-Generation Wireless Networks: Challenges and Opportunities. .

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th International Conference on Decision and Game Theory for Security, GameSec 2020,held in College Park, MD, USA, in October 2020. Due to COVID-19 pandemic the conference was held virtually The 21 full papers presented together with 2 short papers were carefully reviewed and selected from 29 submissions. The papers focus on machine learning and security; cyber deception; cyber-physical systems security; security of network systems; theoretic foundations of security games; emerging topics.