1. Record Nr. UNISA996464400903316

Titolo	Decision and game theory for security : 12th international conference, GameSec 2021, virtual event, October 25-27, 2021 : proceedings / / Branislav Bosansky [and three others] (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-90370-2
Descrizione fisica	1 online resource (385 pages)
Collana	Lecture Notes in Computer Science ; ; v.13061
Disciplina	005.8
Soggetti	Computer security Game theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Theoretical Foundations in Equilibrium Computation -- Computing Nash Equilibria in Multiplayer DAG-Structured Stochastic Games with Persistent Imperfect Information -- 1 Introduction -- 2 Imperfect-Information Naval Strategic Planning Problem -- 3 Algorithm -- 4 Procedure for Computing Degree of Nash Equilibrium Approximation -- 5 Experiments -- 6 Conclusion -- References -- Two Algorithms for Computing Exact and Approximate Nash Equilibria in Bimatrix Games -- 1 Introduction -- 1.1 Notation -- 1.2 Outline of the Paper -- 2 Preliminaries -- 2.1 Strategically Equivalent Games -- 2.2 Approximate Nash Equilibrium -- 3 A Fast Algorithm to Compute Strategically Equivalent Zero-Sum Games -- 3.1 Algorithmic Implications for Matrices in Mmn(R) -- 3.2 A Simple Example: Rock-Paper-Scissors -- 3.3 Algorithm and Simulations -- 3.4 Numerical Results -- 4 Approximate Nash Equilibrium Through an Affine Transformation -- 4.1 Approximate Nash Equilibrium -- 4.2 Algorithmic Implementation -- 4.3 Numerical Simulation -- 5 Conclusion -- A Some Auxiliary Results on Mmn(R) -- References -- Separable Network Games with Compact Strategy Sets -- 1 Introduction -- 2 Network Games -- 3 Example: Security Game -- 3.1 Security Game with the Tullock Function -- 4 Polynomial Network Games -- 4.1 Moment-Based Formulation --

4.2 Nonnegative Polynomials Using Sums of Squares -- 4.3 Hierarchy of Semidefinite Relaxations -- 4.4 Examples -- 5 Conclusions -- References -- Machine Learning and Game Theory -- Countering Attacker Data Manipulation in Security Games -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 Stackelberg Security Games (SSGs) -- 3.2 Partial Behavior Deception Model -- 3.3 Cognitive Hierarchy Approach -- 4 Finding Non-deceptive Attacker Behavior -- 4.1 Characterizing Deceptive Attacker's Behavior.
4.2 RaBiS: Characterizing Behavior of Non-deceptive Attacker -- 4.3 Principled Approach for Low-Data Challenge -- 5 Maximin to Optimize Defender Utility -- 6 Experiments -- 7 Conclusion -- A Appendix -- A. 1 Proof of Theorem 1 -- References -- Scalable Optimal Classifiers for Adversarial Settings Under Uncertainty -- 1 Introduction -- 1.1 Related Work -- 2 Model -- 2.1 Setting and Notation -- 2.2 Preliminary: Reduction of Dimensionality -- 2.3 Model Discussion -- 3 BNE Characterization and Computation -- 3.1 Equilibrium Characterization -- 3.2 Scalable Approximate Computation -- 3.3 Numerical Illustration -- 4 Online Learning -- 5 Concluding Remarks -- References -- Learning Generative Deception Strategies in Combinatorial Masking Games -- 1 Introduction -- 2 Related Work -- 3 Deception Through Attribute Masking -- 4 Computing Equilibrium Deception Strategies -- 4.1 Computing the Attacker's Best Response -- 4.2 Computing the Defender's Best Response -- 4.3 Computing Equilibrium Deception -- 4.4 Scalable Approximation of Equilibrium Deception Through Generative Adversarial Masking -- 5 Extension to Multiple Devices -- 6 Experiments -- 6.1 Near-Optimality of Generative Adversarial Masking -- 6.2 Systematic Large-Scale Experiments -- 7 Case Study -- 8 Conclusion -- References -- Network Games with Strategic Machine Learning -- 1 Introduction -- 2 Game Model -- 2.1 Interdependent in Decision Outcomes (Type 1) -- 2.2 Interdependent in Observable Features (Type 2) -- 3 Equilibrium Analysis-Linear Mechanisms -- 3.1 Type 1 Model Analysis -- 3.2 Type 2 Model Analysis -- 4 Equilibrium Analysis-Linear Threshold Mechanisms -- 4.1 Type 1 Model Analysis -- 4.2 Type 2 Model Analysis -- 5 Numerical Results -- 5.1 Type 1 Model, Linear Mechanism -- 5.2 Type 2 Model, Linear Mechanism -- 5.3 Type 1 Model, Linear Threshold Mechanism.
5.4 Type 2 Model, Linear Threshold Mechanism -- 6 Discussion -- 6.1 Comparisons with Previous Works -- 7 Conclusion -- A Proof of Lemma1 -- B Proof of Proposition1 -- C Proof of Proposition2 -- D Proof of Lemma2 -- E Proof of Proposition3 -- F Proof of Lemma3 -- G Proof of Lemma4 -- H Proof of Lemma5 -- I Proof of Lemma6 -- J Proof of Proposition4 -- K Proof of Proposition5 -- References -- No Time to Lie: Bounds on the Learning Rate of a Defender for Inferring Attacker Target Preferences -- 1 Introduction -- 2 Related Work -- 3 Model -- 4 Lower Bound on the Number of Observations -- 5 Upper Bound on the Number of Observations -- 6 Simulation Results -- 7 Conclusion -- A Proof of Lemma4 -- B Proof of Lemma5 -- References -- When Should You Defend Your Classifier? -- 1 Introduction -- 2 Related Work -- 3 The Advanced Adversarial Classification Game -- 3.1 Adversary -- 3.2 Defender -- 3.3 Cost of Pure Strategies -- 3.4 Utility of Mixed Strategies -- 3.5 Expected Payouts for Mixed Strategies -- 4 Game Instantiation and Analysis -- 4.1 Best Response Analysis of the Adversary -- 4.2 Best Response Analysis of the Defender -- 4.3 (Fully) Mixed Nash Equilibria -- 4.4 Results -- 5 Discussion -- 6 Conclusion -- References -- Ransomware -- A Mechanism Design Approach to Solve Ransomware Dilemmas -- 1 Introduction -- 2 Related Work -- 3 System Model -- 4 Proposed Mechanisms -- 4.1 Ransomware-Dilemma-1 -- 4.2 Ransomware-Dilemma-2 -- 5 Smart-Contract

Implementation -- 6 Conclusion -- References -- Winning the Ransomware Lottery -- 1 Introduction -- 2 Related Work -- 3 Probability and Lotteries -- 4 Paying to Play -- 4.1 Lowering the Value of Payments -- 4.2 Increasing Costs -- 4.3 Decreasing Payment Probability -- 5 Lowering the Stakes -- 5.1 Decreasing Attack Success -- 5.2 Cyber Insurance -- 5.3 Use of Decrypters -- 5.4 Off-Site Backups.
5.5 Impact of Mitigations -- 6 Conclusion -- References -- Combating Ransomware in Internet of Things: A Games-in-Games Approach for Cross-Layer Cyber Defense and Security Investment -- 1 Introduction -- 1.1 Related Work -- 1.2 Organization of the Paper -- 2 Problem Formulation -- 2.1 Basic Settings -- 2.2 Multi-phase Multi-stage Game Formulation -- 2.3 Cyber Markov Game for Ransomware Penetration -- 2.4 Solution Concept -- 3 Ransomware Game Analysis -- 3.1 Risk Assessment Outcome of the Cyber Markov Game -- 3.2 Equilibria of the Ransomware Game -- 4 Sensitivity Analysis and Impact of Human Factors -- 4.1 Impact of the Security Budget -- 4.2 Impact of Human Factors and Prospect Theory -- 5 Case Studies and Discussion -- 5.1 Model Implementation -- 5.2 Outcome of Cyber Markov Game -- 5.3 Impact of Budget -- 5.4 Prospect Theory -- 6 Conclusion -- A Proof in the Budget Dilemma -- References -- Cyber-physical Systems Security -- A Game-Theoretic Framework for Controlled Islanding in the Presence of Adversaries -- 1 Introduction -- 2 Related Work -- 3 Model and Preliminaries -- 3.1 Power System Model -- 3.2 Stackelberg Game -- 4 Problem Formulation -- 4.1 Adversary Model -- 4.2 Grid Operator Model -- 4.3 Interaction Model Between the Grid Operator and Adversary -- 5 Solution Approach -- 5.1 Mixed Integer Nonlinear Bi-level Optimization Formulation -- 5.2 Double Oracle Algorithm Based Approach -- 6 Numerical Evaluations -- 6.1 Simulation Setup -- 6.2 Case Study Results -- 7 Conclusion -- References -- Game Theoretic Hardware Trojan Testing Under Cost Considerations -- 1 Introduction -- 2 Game Theoretic Trojan Testing Under Cost Considerations -- 3 Game Theoretic Trojan Testing Under a Cost Budget Constraint -- 3.1 NE Under Sufficient Cost Budget of the Defender -- 3.2 NE Under Insufficient Cost Budget of the Defender -- 4 Numerical Results -- 5 Conclusion.
References -- Strategic Remote Attestation: Testbed for Internet-of-Things Devices and Stackelberg Security Game for Optimal Strategies -- 1 Introduction -- 2 Background -- 2.1 Software Vulnerabilities and Exploitation in IoT Devices -- 2.2 IoT Remote Attestation -- 2.3 Stackelberg Security Games -- 3 Testbed Design and Development -- 3.1 Testbed Components -- 3.2 Testbed Development -- 4 Game-Theoretic Model of Remote Attestation -- 4.1 Environment and Players -- 4.2 Strategy Spaces -- 4.3 Utility Functions -- 4.4 Solution Concept -- 5 Analysis of Optimal Attestation Strategies -- 5.1 Case 1: Single Device and Single Attestation Method -- 5.2 Case 2: Multiple Devices and Single Device Class -- 5.3 Case 3: Multiple Devices and Multiple Device Classes -- 6 Numerical Results -- 6.1 Experimental Results from the Remote Attestation Testbed -- 6.2 Evaluation of Game-Theoretic Model and Optimal Strategies -- 7 Related Work -- 7.1 IoT Security Testbeds -- 7.2 Remote Attestation -- 7.3 Stackelberg Security Games -- 8 Conclusion and Future Work -- References -- Innovations in Attacks and Defenses -- Bet and Attack: Incentive Compatible Collaborative Attacks Using Smart Contracts -- 1 Introduction -- 2 A Model for a CSC-Based Collaborative Attack -- 2.1 Blockchain Model -- 2.2 Threat Model -- 2.3 Attack Model -- 3 Game Theoretic Model and Analysis -- 3.1 Attackers Contribution -- 3.2 Interdependent Attackers Game (IAG) -- 3.3 Equilibrium Analysis -- 4 Exploring Incentive

Compatibility -- 4.1 Mechanism Formulation -- 4.2 Incentive Compatible Property -- 4.3 Budget Constraint -- 4.4 Voluntary Participation Constraint -- 4.5 Fairness -- 5 Numerical Simulations and Discussion -- 6 Conclusion -- References -- Combating Informational Denial-of-Service (IDoS) Attacks: Modeling and Mitigation of Attentional Human Vulnerability -- 1 Introduction -- 1.1 Related Works.
1.2 Notations and Organization of the Paper.