1.

Record Nr.	UNISA996466572103316
Titolo	Decision and Game Theory for Security [[electronic resource]] : 6th International Conference, GameSec 2015, London, UK, November 4-5, 2015, Proceedings / / edited by Arman (MHR) Khouzani, Emmanouil Panaousis, George Theodorakopoulos
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-25594-0
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (X, 371 p. 90 illus. in color.)
Collana	Security and Cryptology ; ; 9406
Disciplina	005.8
Soggetti	Application software Computer communication systems Computer security Algorithms Management information systems Computer science Game theory Information Systems Applications (incl. Internet) Computer Communication Networks Systems and Data Security Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Game Theory, Economics, Social and Behav. Sciences
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Full Papers -- A Game-Theoretic Approach to IP Address Randomization in Decoy-Based Cyber Defense -- 1 Introduction -- 2 Related Work -- 3 Model and Preliminaries -- 3.1 Virtual Network Model -- 3.2 Adversary Model -- 4 Modeling Interaction with Single Decoy -- 4.1 Timing-Based Decoy Detection Game -- 4.2 Fingerprinting-Based Decoy Detection Game -- 5 Characterization of Optimal IP Address Randomization

Strategy by Network -- 5.1 Game Formulation -- 5.2 Optimal Strategy of the System -- 5.3 Optimal Strategy of the Adversary -- 6 Simulation Study -- 7 Conclusion -- References -- Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks -- 1 Introduction -- 1.1 Related Works -- 1.2 Organization of the Paper -- 2 Game-Theoretic Model for Cyber Insurance -- 3 Analysis of the Cyber Insurance Model -- 3.1 Separable Utilities -- 3.2 Case Study: Cyber Insurance Under Infection Dynamics -- 4 Conclusion -- References -- Beware the Soothsayer: From Attack Prediction Accuracy to Predictive Reliability in Security Games -- 1 Introduction -- 2 Background: Network Security Games -- 3 Related Work -- 4 Adversary Behavioral Models -- 4.1 The Perfectly Rational Model -- 4.2 The Quantal Response Model -- 4.3 The Subjective Utility Quantal Response Model -- 4.4 The SUQR Graph-Aware Model -- 5 Defender Strategy Generation -- 6 Human Subject Experiments -- 6.1 Experimental Overview -- 6.2 Experiment Data Composition -- 6.3 Data Analysis Metrics -- 7 Predictive Reliability Analysis -- 7.1 SSG Experiment -- 7.2 SSG Predictive Reliability -- 7.3 NSG Predictive Reliability -- 7.4 Training Set Size -- 8 Predictive Reliability Factors -- 8.1 Training Set Feature: EAS -- 9 Graph Features and Their Impacts on Predictive Reliability -- 10 Conclusion -- References -- Games of Timing for Security in Dynamic Environments. 1 Introduction -- 2 Related Work -- 2.1 Security Economics and Games of Timing -- 2.2 Theoretical Analyses of FlipIt -- 2.3 Behavioral Studies of FlipIt -- 3 Model -- 3.1 Players and Choices -- 3.2 Environment -- 3.3 Consequences -- 4 Analysis -- 5 Numerical Examples -- 6 Conclusion -- References -- Threshold FlipThem: When the Winner Does Not Need to Take All -- 1 Introduction -- 1.1 Prior Work -- 2 The Multi-party FlipIt Model -- 3 Obtaining Nash Equilibria in Continuous Time for a Stochastic Process -- 3.1 Simple Example, FlipThem0F(n,n, d,): Full Threshold, Full Reset -- 3.2 FlipThemF(n,t,d,): (n,t)-Threshold, Full Reset -- 3.3 FlipThemS(n,t,d,): (n,t)-Threshold, Single Reset -- References -- A Game Theoretic Model for Defending Against Stealthy Attacks with Limited Resources -- 1 Introduction -- 2 Game Model -- 2.1 Basic Model -- 2.2 Defender's Problem -- 2.3 Attacker's Problem -- 3 Best Responses -- 3.1 Defender's Best Response -- 3.2 Attacker's Best Response -- 3.3 Simplified Optimization Problems -- 4 Nash Equilibria -- 5 Sequential Game -- 6 Numerical Result -- 7 Conclusion -- References -- Passivity-Based Distributed Strategies for Stochastic Stackelberg Security Games -- 1 Introduction -- 2 Related Work -- 3 Model and Game Formulation -- 3.1 Defender Model -- 3.2 Adversary Model -- 3.3 Game Formulation -- 4 Passivity-Based Distributed Defense Strategy -- 4.1 Distributed Defender Strategy -- 4.2 Passivity-Based Convergence Analysis -- 5 Mitigating Side Information of Adversary -- 5.1 Deviation from Stackelberg Equilibrium -- 5.2 Optimizing the Convergence Rate -- 6 Numerical Study -- 7 Conclusions and Future Work -- References -- Combining Online Learning and Equilibrium Computation in Security Games -- 1 Introduction -- 2 Related Work -- 3 Game Model -- 3.1 Attacker Behavior Model -- 4 Background -- 4.1 Stackelberg Security Game. 4.2 Stackelberg Equilibrium -- 4.3 Nash Equilibrium -- 5 Defender Strategies -- 5.1 Online Learning with One Resource -- 5.2 Online Learning with Multiple Resources -- 6 Combined Algorithms -- 6.1 Combined Algorithm 1 -- 6.2 Combined Algorithm 2 -- 6.3 Combined Algorithm 3 -- 6.4 Combined Algorithm 4 -- 7 Experiments -- 7.1 Imprecise Stackelberg Equilibrium Strategy -- 7.2 Performance of Combined Algorithms with One Resource -- 7.3 Combinatorial Combined Algorithms -- 8 Conclusion -- References -- Interdependent Security Games Under Behavioral Probability Weighting

-- 1 Introduction -- 2 Probability Weighting -- 3 Interdependent Security Games -- 4 Total Effort Game with Probability Weighting: Homogeneous Players -- 4.1 Comparative Statics -- 4.2 Social Optimum -- 5 Weakest Link and Best Shot Games -- 6 Total Effort Game with Heterogeneous Players -- 7 Discussion and Conclusion -- References -- Making the Most of Our Regrets: Regret-Based Solutions to Handle Payoff Uncertainty and Elicitation in Green Security Games -- 1 Introduction -- 2 Background and Related Work -- 3 Behavioral Modeling Validation -- 3.1 Dataset Description -- 3.2 Learning Results -- 4 Behavioral Minimax Regret (MMRb) -- 5 ARROW Algorithm: Boundedly Rational Attacker -- 5.1 R.ARROW: Compute Relaxed MMRb -- 5.2 M.ARROW: Compute MRb -- 6 ARROW-Perfect Algorithm: Perfectly Rational Attacker -- 6.1 R.ARROW-Perfect: Compute Relaxed MMR -- 6.2 M.ARROW-Perfect: Compute Max Regret -- 7 UAV Planning for Payoff Elicitation (PE) -- 8 Experimental Results -- 8.1 Synthetic Data -- 8.2 Real-World Data -- 9 Summary -- References -- A Security Game Model for Environment Protection in the Presence of an Alarm System -- 1 Introduction -- 2 Problem Formulation -- 3 Finding the Best Signal--Response Strategy -- 3.1 Computing D's actions -- 3.2 A Heuristic Algorithm -- 3.3 Solving SRG--v.

4 Finding the Best Patrolling Strategy -- 4.1 Computing the Best Placement -- 4.2 Robustness to Missed Detections -- 5 Experimental Evaluation -- 6 Conclusions and Future Research -- References -- Determining a Discrete Set of Site-Constrained Privacy Options for Users in Social Networks Through Stackelberg Games -- 1 Introduction -- 2 Related Work -- 3 Problem Statement -- 4 Model Overview -- 4.1 User Model -- 4.2 Site Model for the Determination of a Discrete Set of Privacy Options for Shared Content -- 5 An Approximation Algorithm for Arbitrary Graphs - A Simulation -- 6 Experimental Results -- 6.1 Experimental Results: Peer Pressure Effects on Privacy Preferences -- 6.2 Experimental Results: Iterative Approximation of Privacy Preferences -- 7 Conclusion -- References -- Approximate Solutions for Attack Graph Games with Imperfect Information -- 1 Introduction -- 2 Background and Definitions -- 3 Imperfect Information HP Allocation Game -- 3.1 Nature Actions -- 3.2 Defender's Actions -- 3.3 Attacker's Actions -- 3.4 Players' Utilities -- 3.5 Solution Concepts -- 4 Game Approximations -- 4.1 Perfect Information Game Approximation -- 4.2 Zero-Sum Game Approximation -- 4.3 Commitment to Correlated Equilibrium -- 5 Algorithms -- 5.1 Single Oracle -- 5.2 Attacker's Optimal Attack Policy -- 5.3 Linear Program for Upper Bounds -- 6 Experiments -- 6.1 Networks and Attack Graphs -- 6.2 Analytical Approach for CURB for Unstructured Network -- 6.3 Scalability -- 6.4 Solution Quality -- 6.5 Quality of ZS Approximations -- 6.6 Sensitivity Analysis -- 6.7 Case Study -- 7 Conclusion -- References -- When the Winning Move is Not to Play: Games of Deterrence in Cyber Security -- 1 Introduction -- 2 Background -- 2.1 Concepts of Deterrence -- 2.2 Information Asymmetries in Security -- 2.3 Adversary Scenarios -- 3 Deterrence as an Information Asymmetry.

3.1 Deterrence as Screening: An Example of Tactical Deterrence -- 3.2 Deterrence as Signalling: An Example of Operational Deterrence -- 3.3 Discussion -- 4 Related Work -- 5 Conclusions -- References -- Sequentially Composable Rational Proofs -- 1 Introduction -- 2 Rational Proofs -- 3 Profit vs. Reward -- 4 Sequential Composition -- 4.1 Motivating Example -- 4.2 Sequentially Composable Rational Proofs -- 4.3 Sequential Rational Proofs in the PCP Model -- 4.4 Sequential Composition and the Unique Inner State Assumption -- 5 Our Protocol -- 5.1 Efficiency -- 5.2 Proofs of (Stand-Alone) Rationality -- 5.3 Proof of Sequential Composability -- 6 Results for FFT Circuits -- 6.1 FFT

Circuit for Computing a Single Coefficient -- 6.2 Mixed Strategies for Verification -- 7 Conclusion -- References -- Flip the Cloud: Cyber-Physical Signaling Games in the Presence of Advanced Persistent Threats -- 1 Introduction -- 2 System Model -- 2.1 Cloud-Device Signaling Game -- 2.2 FlipIt Game for Cloud Control -- 3 Solution Concept -- 3.1 Signaling Game Equilibrium -- 3.2 FlipIt Game Equilibrium -- 3.3 Gestalt Equilibrium of GCC -- 4 Analysis -- 4.1 Signaling Game Analysis -- 4.2 FlipIt Analysis -- 4.3 GCC Analysis -- 5 Cloud Control Application -- 5.1 Dynamic Model for Cloud Controlled Unmanned Vehicles -- 5.2 Control of Unmanned Vehicle -- 5.3 Filter for High Risk Cloud Commands -- 6 Conclusion and Future Work -- A Derivation of Signaling Game Equilibria -- A.1 Separating Equilibria -- A.2 Pooling Equilibria -- References -- Short Papers -- Genetic Approximations for the Failure-Free Security Games -- 1 Introduction -- 2 Definitions -- 3 Genetic Approximations for the Failure-Free Satisfiability Games -- 3.1 Genetic Algorithm (GA) -- 4 Adaptive Genetic Algorithm (AGA) -- 5 Conclusions -- References.
To Trust or Not: A Security Signaling Game Between Service Provider and Client.

Sommario/riassunto

This book constitutes the refereed proceedings of the 6th International Conference on Decision and Game Theory for Security, GameSec 2015, held in London, UK, in November 2015. The 16 revised full papers presented together with 5 short papers were carefully reviewed and selected from 37 submissions. Game and decision theory has emerged as a valuable systematic framework with powerful analytical tools in dealing with the intricacies involved in making sound and sensible security decisions. For instance, game theory provides methodical approaches to account for interdependencies of security decisions, the role of hidden and asymmetric information, the perception of risks and costs in human behaviour, the incentives/limitations of the attackers, and much more. Combined with our classical approach to computer and network security, and drawing from various fields such as economic, social and behavioural sciences, game and decision theory is playing a fundamental role in the development of the pillars of the "science of security".