1. Record Nr. UNINA9910830628803321

Titolo	Game theory and machine learning for cyber security / / editors, Charles A. Kamhoua [et al.]
Pubbl/distr/stampa	Hoboken, NJ : , : John Wiley & Sons, Inc., , [2021] ©2021
ISBN	1-119-72394-9 1-119-72395-7 1-119-72391-4
Descrizione fisica	1 online resource (547 pages)
Disciplina	005.8
Soggetti	Computer networks - Security measures Game theory Machine learning
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title Page -- Copyright -- Contents -- Editor Biographies -- Contributors -- Foreword -- Preface -- Chapter 1 Introduction -- 1.1 Artificial Intelligence and Cybersecurity -- 1.1.1 Game Theory for Cybersecurity -- 1.1.2 Machine Learning for Cybersecurity -- 1.2 Overview -- References -- Part I Game Theory for Cyber Deception -- Chapter 2 Introduction to Game Theory -- 2.1 Overview -- 2.2 Example TwoPlayer ZeroSum Games -- 2.3 NormalForm Games -- 2.3.1 Solution Concepts -- 2.4 ExtensiveForm Games -- 2.4.1 Solution Concepts -- 2.5 Stackelberg Game -- 2.5.1 Solution Concept -- 2.5.2 Stackelberg Security Games -- 2.5.3 Applications in Cybersecurity -- 2.6 Repeated Games -- 2.6.1 Solution Concepts -- 2.6.2 Applications in Cybersecurity -- 2.7 Bayesian Games -- 2.7.1 Solution Concepts -- 2.7.2 Applications in Cybersecurity -- 2.8 Stochastic Games -- 2.8.1 Solution Concepts -- 2.8.2 Applications in Cybersecurity -- References -- Chapter 3 Scalable Algorithms for Identifying Stealthy Attackers in a GameTheoretic Framework Using Deception -- 3.1 Introduction -- 3.2 Background -- 3.3 Case Studies -- 3.3.1 Case Study 1: Attackers with Same Exploits but Different Goals -- 3.3.2 Case Study 2: Attackers with

Shared Exploits and Different Goals -- 3.3.3 Case Study 3: Attackers with Shared Exploits but Same Goals -- 3.4 Game Model -- 3.5 Defender Decision Making -- 3.6 Attacker Decision Making -- 3.7 Simulation Results -- 3.8 Scalability -- 3.8.1 Heuristics -- 3.9 Evaluation of Heuristics -- 3.10 Conclusions and Future Direction -- References -- Chapter 4 Honeypot Allocation Games over Attack Graphs for Cyber Deception -- 4.1 Introduction -- 4.2 System and Game Model -- 4.2.1 Attack Graph -- 4.2.2 General Game Formulation -- 4.2.2.1 Defender Action -- 4.2.2.2 Attacker Action -- 4.2.3 Reward Function -- 4.2.4 Mixed Strategy.
4.2.5 System Parameters -- 4.3 Allocating Honeypots Model -- 4.3.1 The Algorithm -- 4.4 Dynamic Honeypot Allocation -- 4.4.1 Mixed Strategy, State Evolution, and Objective Function -- 4.4.2 QMinmax Algorithm -- 4.5 Numerical Results -- 4.6 Conclusion and Future Work -- Acknowledgment -- References -- Chapter 5 Evaluating Adaptive Deception Strategies for Cyber Defense with Human Adversaries -- 5.1 Introduction -- 5.1.1 HoneyGame: An Abstract Interactive Game to Study Deceptive Cyber Defense -- 5.2 An Ecology of Defense Algorithms -- 5.2.1 Static Pure Defender -- 5.2.2 Static Equilibrium Defender -- 5.2.3 Learning with Linear Rewards (LLR) -- 5.2.4 Best Response with Thompson sampling (BRTS) -- 5.2.5 Probabilistic Best Response with Thompson Sampling (PBRTS) -- 5.2.6 Follow the Regularized Leader (FTRL) -- 5.3 Experiments -- 5.3.1 Measures -- 5.4 Experiment 1 -- 5.4.1 Participants -- 5.4.2 Procedure -- 5.4.3 Results -- 5.4.3.1 Average Rewards -- 5.4.3.2 Attacks on Honeypots -- 5.4.3.3 Switching Behavior -- 5.4.3.4 Attack Distribution -- 5.5 Experiment 2 -- 5.5.1 Participants -- 5.5.2 Results -- 5.5.2.1 Average Rewards -- 5.5.2.2 Attacks on Honeypots -- 5.5.2.3 Switching Behavior -- 5.5.2.4 Attack Distribution -- 5.6 Towards Adaptive and Personalized Defense -- 5.7 Conclusions -- Acknowledgements -- References -- Chapter 6 A Theory of Hypergames on Graphs for Synthesizing Dynamic Cyber Defense with Deception -- 6.1 Introduction -- 6.2 AttackDefend Games on Graph -- 6.2.1 Game Arena -- 6.2.2 Specifying the Security Properties in LTL -- 6.3 Hypergames on Graphs -- 6.4 Synthesis of Provably Secure Defense Strategies Using Hypergames on Graphs -- 6.4.1 Synthesis of Reactive Defense Strategies -- 6.4.2 Synthesis of Reactive Defense Strategies with Cyber Deception -- 6.5 Case Study -- 6.6 Conclusion -- References.
Part II Game Theory for Cyber Security -- Chapter 7 Minimax Detection (MAD) for Computer Security: A Dynamic Program Characterization -- 7.1 Introduction -- 7.1.1 Need for Cohesive Detection -- 7.1.2 Need for Strategic Detection -- 7.1.3 Minimax Detection (MAD) -- 7.2 Problem Formulation -- 7.2.1 System Model -- 7.2.2 Defense Model -- 7.2.3 Threat Model -- 7.2.4 Game Model -- 7.3 Main Result -- 7.3.1 Complexity Analysis -- 7.4 Illustrative Examples -- 7.5 Conclusion -- Acknowledgements -- References -- Chapter 8 Sensor Manipulation Games in Cyber Security -- 8.1 Introduction -- 8.2 Measurement Manipulation Games -- 8.2.1 SaddlePoint Equilibria -- 8.2.2 Approximate SaddlePoint Equilibrium -- 8.3 SensorReveal Games -- 8.3.1 Nash Equilibria -- 8.4 Conclusions and Future Work -- References -- Chapter 9 Adversarial Gaussian Process Regression in Sensor Networks -- 9.1 Introduction -- 9.2 Related Work -- 9.3 Anomaly Detection with Gaussian Process Regression -- 9.4 Stealthy Attacks on Gaussian Process Anomaly Detection -- 9.5 The Resilient Anomaly Detection System -- 9.5.1 Resilient Anomaly Detection as a Stackelberg Game -- 9.5.2 Computing an Approximately Optimal Defense -- 9.6 Experiments -- 9.7 Conclusions -- References --

Chapter 10 Moving Target Defense Games for Cyber Security: Theory and Applications -- 10.1 Introduction -- 10.2 Moving Target Defense Theory -- 10.2.1 Game Theory for MTD -- 10.3 SingleController Stochastic Games for Moving Target Defense -- 10.3.1 Stochastic Games -- 10.3.2 SingleController Stochastic Games -- 10.3.2.1 Numerical Example -- 10.4 A Case Study for Applying SingleController Stochastic Games in MTD The case study presented in this section is based on the work in Eldosouky et al. (). -- 10.4.1 Equilibrium Strategy Determination -- 10.4.2 Simulation Results and Analysis -- 10.5 Moving Target Defense Applications.
10.5.1 Internet of Things (IoT) Applications -- 10.5.2 Machine Learning Applications -- 10.5.3 Prospective MTD Applications -- 10.6 Conclusions -- References -- Chapter 11 Continuous Authentication Security Games -- 11.1 Introduction -- 11.2 Background and Related Work -- 11.3 Problem Formulation -- 11.3.1 User Behavior -- 11.3.2 Intrusion Detection System Model -- 11.3.3 Model of Continuous Authentication -- 11.3.4 System States without an Attacker -- 11.3.5 Attack Model -- 11.3.5.1 Listening (l(t)&amp -- equals -- r, a(t)&amp -- equals -- 0) -- 11.3.5.2 Attacking (l(t)&amp -- equals -- 0, a(t) &amp -- equals -- r) -- 11.3.5.3 Waiting (l(t)&amp -- equals -- 0, a(t) &amp -- equals -- 0) -- 11.3.6 Continuous Authentication Game -- 11.4 Optimal Attack Strategy under Asymmetric Information -- 11.4.1 MDP Formulation -- 11.4.1.1 Waiting (l(t)&amp -- equals -- 0, a(t) &amp -- equals -- 0) -- 11.4.1.2 Listening (l(t)&amp -- equals -- r, a (t)&amp -- equals -- 0) -- 11.4.1.3 Attacking (l(t)&amp -- equals -- 0, a(t)&amp -- equals -- r) -- 11.4.2 Optimality of the Threshold Policy -- 11.4.2.1 Optimality of Listening -- 11.4.2.2 Optimality of Attacking -- 11.5 Optimal Defense Strategy -- 11.5.1 Expected Defender Utility -- 11.5.2 Analysis without an Attacker -- 11.5.3 Analysis with an Attacker -- 11.6 Numerical Results -- 11.7 Conclusion and Discussion -- References -- Chapter 12 Cyber Autonomy in Software Security: Techniques and Tactics -- 12.1 Introduction -- 12.2 Background -- 12.3 Related Work -- 12.4 Model Setup -- 12.5 Techniques -- 12.6 Tactics -- 12.6.1 Model Parameters -- 12.6.2 Formalization -- 12.6.3 Finding Equilibriums -- 12.6.4 Algorithm -- 12.7 Case Study -- 12.8 Discussion -- 12.9 Conclusion -- References -- Part III Adversarial Machine Learning for Cyber Security.
Chapter 13 A Game Theoretic Perspective on Adversarial Machine Learning and Related Cybersecurity Applications -- 13.1 Introduction to Game Theoretic Adversarial Machine Learning -- 13.2 Adversarial Learning Problem Definition -- 13.3 Game Theory in Adversarial Machine Learning -- 13.3.1 Simultaneous Games -- 13.3.1.1 Zero Sum Games -- 13.3.1.2 Nash Equilibrium Games -- 13.3.2 Sequential Games -- 13.4 Simultaneous Zerosum Games in Real Applications -- 13.4.1 Adversarial Attack Models -- 13.4.1.1 FreeRange Attack -- 13.4.1.2 Restrained Attack -- 13.4.2 Adversarial SVM Learning -- 13.4.2.1 ADSVM Against Freerange Attack Model -- 13.4.2.2 ADSVM Against Restrained Attack Model -- 13.4.3 Experiment -- 13.4.3.1 Attack Simulation -- 13.4.3.2 Experimental Results -- 13.4.3.3 A Few Words on Setting Cf, C, and C -- 13.4.4 Remark -- 13.5 Nested Bayesian Stackelberg Games -- 13.5.1 Adversarial Learning -- 13.5.2 A Single Leader Single Follower Stackelberg Game -- 13.5.3 Learning Models and Adversary Types -- 13.5.3.1 Learning Models -- 13.5.3.2 Adversary Types -- 13.5.3.3 Setting Payoff Matrices for the Single Leader Multiplefollowers Game -- 13.5.4 A Single Leader Multi followers Stackelberg Game -- 13.5.5 Experiments -- 13.5.5.1 Artificial Datasets -- 13.5.5.2 Real Datasets -- 13.5.6 Remark -- 13.6 Further Discussions -- Acknowledgements -- References -- Chapter

14 Adversarial Machine Learning for 5G Communications Security -- 14.1 Introduction -- 14.2 Adversarial Machine Learning -- 14.3 Adversarial Machine Learning in Wireless Communications -- 14.3.1 Wireless Attacks Built Upon Adversarial Machine Learning -- 14.3.2 Domainspecific Challenges for Adversarial Machine Learning in Wireless Communications -- 14.3.3 Defense Schemes Against Adversarial Machine Learning -- 14.4 Adversarial Machine Learning in 5G Communications.
14.4.1 Scenario 1-Adversarial Attack on 5G Spectrum Sharing.

Sommario/riassunto

"Cyber security is a serious concern to our economic prosperity and national security. Despite an increased investment in cyber defense, cyber-attackers are becoming more creative and sophisticated. This exposes the need for a more rigorous approach to cyber security, including methods from artificial intelligence including computational game theory and machine learning. Recent advances in adversarial machine learning are promising to make artificial intelligence (AI) algorithms more robust to deception and intelligent manipulation. However, they are still vulnerable to adversarial inputs, data poisoning, model stealing and evasion attacks. The above challenges and the high risk and consequence of cyber-attacks drive the need to accelerate basic research on cyber security"-- Provided by publisher