1. Record Nr. UNINA9910555189803321

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

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