1. Record Nr. UNISA996464488703316

Autore	Chen Xiaofeng
Titolo	Cyber security meets machine learning / / Xiaofeng Chen, Willy Susilo, Elisa Bertino
Pubbl/distr/stampa	Singapore : , : Springer, , [2021] ©2021
ISBN	981-336-726-1
Descrizione fisica	1 online resource (168 pages)
Disciplina	006.31
Soggetti	Machine learning - Technique Machine learning - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Contents -- IoT Attacks and Malware -- 1 Introduction -- 2 Background -- 2.1 Cybersecurity Kill Chains -- 2.2 Major IoT Security Concerns -- 3 Attack Classification -- 3.1 Passive/Information Stealing Attacks -- 3.2 Service Degradation Attacks -- 3.3 DDoS Attacks -- 4 IoT Malware Analysis and Classification -- 5 AI-Based IDS Solutions -- 6 Conclusion -- References -- Machine Learning-Based Online Source Identification for Image Forensics -- 1 Introduction -- 2 Related Work -- 2.1 Features Engineering for Image Source Identification -- 2.2 Statistical Learning-Based Image Source Identification -- 3 Proposed Scheme: OSIU -- 3.1 Unknown Sample Triage -- 3.2 Unknown Image Discovery -- 3.3 (K+1) -class Classification -- 4 Experiments and Results -- 4.1 Dataset and Experiment Settings -- 4.2 Features -- 4.3 Evaluation Metrics -- 4.4 Performance of Triaging Unknown Samples -- 4.5 Performance of OSIU -- 5 Conclusion -- References -- Reinforcement Learning Based Communication Security for Unmanned Aerial Vehicles -- 1 Introduction -- 2 Communication Security for Unmanned Aerial Vehicles -- 2.1 UAV Communication Model -- 2.2 Attack Model -- 3 Reinforcement Learning Based UAV Communication Security -- 3.1 Reinforcement Learning Based Anti-Jamming Communications -- 3.2 Reinforcement Learning Based UAV Communications Against Smart Attacks -- 4 UAV Secure Communication Game -- 4.1 Game Model --

4.2 Nash Equilibrium of the Game -- 5 Related Work -- 5.1 General Anti-jamming Policies in UAV-Aided Communication -- 5.2 Reinforcement Learning in Anti-jamming Communication -- 5.3 Game Theory in Anti-jamming Communication -- 6 Conclusion -- References -- Visual Analysis of Adversarial Examples in Machine Learning -- 1 Introduction -- 2 Adversarial Examples -- 3 Generation of Adversarial Examples -- 4 Properties of Adversarial Examples.
5 Distinguishing Adversarial Examples -- 6 Robustness of Models -- 7 Challenges and Research Directions -- 8 Conclusion -- References -- Adversarial Attacks Against Deep Learning-Based Speech Recognition Systems -- 1 Introduction -- 2 Background and Related Work -- 2.1 Speech Recognition -- 2.2 Adversarial Examples -- 2.3 Related Work -- 3 Overview -- 3.1 Motivation -- 3.2 Technical Challenges -- 4 White-Box Attack -- 4.1 Threat Model of White-Box Attack -- 4.2 The Detail Decoding Process of Kaldi -- 4.3 Gradient Descent to Craft Audio Clip -- 4.4 Practical Adversarial Attack Against White-Box Model -- 4.5 Experiment Setup of CommanderSong Attack -- 4.6 Evaluation of CommanderSong Attack -- 5 Black-Box Attack -- 5.1 Threat Model of Black-Box Attack -- 5.2 Transferability Based Approach -- 5.3 Local Model Approximation Approach -- 5.4 Alternate Models Based Generation Approach -- 5.5 Experiment Setup of Devil's Whisper Attack -- 5.6 Evaluation of Devil's Whisper Attack -- 6 Defense -- 7 Conclusion -- Appendix -- References -- A Survey on Secure Outsourced Deep Learning -- 1 Introduction -- 2 Deep Learning -- 2.1 Brief Survey on Deep Learning -- 2.2 Architecture of Deep Learning -- 2.3 Main Computation in Deep Learning -- 3 Outsourced Computation -- 3.1 Brief Survey on Outsourced Computation -- 3.2 System Model -- 3.3 Security Requirements -- 4 Outsourced Deep Learning -- 4.1 Brief Review on Outsourced Deep Learning -- 4.2 Privacy Concerns in Outsourced Deep Learning -- 4.3 Privacy-Preserving Techniques for Outsourced Deep Learning -- 4.4 Taxonomy Standard -- 4.5 Privacy-Preserving Training Outsourcing -- 4.6 Privacy-Preserving Inference Outsourcing -- 5 Conclusion and Future Research Perspectives -- References.

Sommario/riassunto

ss.