1. Record Nr.   UNINA9910488713403321

   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 --

Sommario/riassunto	ss.