

1. Record Nr.	UNINA9910632494403321
Autore	Xu Shengjie
Titolo	Cybersecurity in Intelligent Networking Systems
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2022 ©2023
ISBN	1-119-78413-1 1-119-78410-7 1-119-78412-3
Descrizione fisica	1 online resource (147 pages)
Collana	IEEE Press Ser.
Altri autori (Persone)	QianYi HuRose Qingyang
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title Page -- Copyright -- Contents -- About the Authors -- Preface -- Acknowledgments -- Acronyms -- Chapter 1 Cybersecurity in the Era of Artificial Intelligence -- 1.1 Artificial Intelligence for Cybersecurity -- 1.1.1 Artificial Intelligence -- 1.1.2 Machine Learning -- 1.1.2.1 Supervised Learning -- 1.1.2.2 Unsupervised Learning -- 1.1.2.3 Semisupervised Learning -- 1.1.2.4 Reinforcement Learning -- 1.1.3 DataDriven Workflow for Cybersecurity -- 1.2 Key Areas and Challenges -- 1.2.1 Anomaly Detection -- 1.2.2 Trustworthy Artificial Intelligence -- 1.2.3 Privacy Preservation -- 1.3 Toolbox to Build Secure and Intelligent Systems -- 1.3.1 Machine Learning and Deep Learning -- 1.3.1.1 NumPy -- 1.3.1.2 SciPy -- 1.3.1.3 Scikitlearn -- 1.3.1.4 PyTorch -- 1.3.1.5 TensorFlow -- 1.3.2 PrivacyPreserving Machine Learning -- 1.3.2.1 Syft -- 1.3.2.2 TensorFlow Federated -- 1.3.2.3 TensorFlow Privacy -- 1.3.3 Adversarial Machine Learning -- 1.3.3.1 SecML and SecML Malware -- 1.3.3.2 Foolbox -- 1.3.3.3 CleverHans -- 1.3.3.4 Counterfit -- 1.3.3.5 MintNV -- 1.4 Data Repositories for Cybersecurity Research -- 1.4.1 NSLKDD -- 1.4.2 UNSWNB15 -- 1.4.3 EMBER -- 1.5 Summary -- Notes -- References -- Chapter 2 Cyber Threats and Gateway Defense -- 2.1 Cyber Threats -- 2.1.1 Cyber Intrusions -- 2.1.2 Distributed Denial of Services Attack --

2.1.3 Malware and Shellcode -- 2.2 Gateway Defense Approaches --
2.2.1 Network Access Control -- 2.2.2 Anomaly Isolation -- 2.2.3
Collaborative Learning -- 2.2.4 Secure Local Data Learning -- 2.3
Emerging Datadriven Methods for Gateway Defense -- 2.3.1 Semi
supervised Learning for Intrusion Detection -- 2.3.2 Transfer Learning
for Intrusion Detection -- 2.3.3 Federated Learning for Privacy
Preservation -- 2.3.4 Reinforcement Learning for Penetration Test.
2.4 Case Study: Reinforcement Learning for Automated Postbreach
Penetration Test -- 2.4.1 Literature Review -- 2.4.2 Research Idea --
2.4.3 Training Agent Using Deep QLearning -- 2.5 Summary --
References -- Chapter 3 Edge Computing and Secure Edge Intelligence
-- 3.1 Edge Computing -- 3.2 Key Advances in Edge Computing --
3.2.1 Security -- 3.2.2 Reliability -- 3.2.3 Survivability -- 3.3 Secure
Edge Intelligence -- 3.3.1 Background and Motivation -- 3.3.2 Design
of Detection Module -- 3.3.2.1 Data Preprocessing -- 3.3.2.2 Model
Learning -- 3.3.2.3 Model Updating -- 3.3.3 Challenges Against
Poisoning Attacks -- 3.4 Summary -- References -- Chapter 4 Edge
Intelligence for Intrusion Detection -- 4.1 Edge Cyberinfrastructure --
4.2 Edge AI Engine -- 4.2.1 Feature Engineering -- 4.2.2 Model
Learning -- 4.2.3 Model Update -- 4.2.4 Predictive Analytics -- 4.3
Threat Intelligence -- 4.4 Preliminary Study -- 4.4.1 Dataset -- 4.4.2
Environmental Setup -- 4.4.3 Performance Evaluation -- 4.4.3.1
Computational Efficiency -- 4.4.3.2 Prediction Accuracy -- 4.5
Summary -- References -- Chapter 5 Robust Intrusion Detection -- 5.1
Preliminaries -- 5.1.1 Median Absolute Deviation -- 5.1.2 Mahalanobis
Distance -- 5.2 Robust Intrusion Detection -- 5.2.1 Problem
Formulation -- 5.2.2 Step 1: Robust Data Preprocessing -- 5.2.3 Step
2: Bagging for Labeled Anomalies -- 5.2.4 Step 3: Oneclass SVM for
Unlabeled Samples -- 5.2.4.1 Oneclass Classification -- 5.2.4.2
Algorithm of Optimal Sampling Ratio Section -- 5.2.5 Step 4: The Final
Classifier -- 5.3 Experimental and Evaluation -- 5.3.1 Experiment
Setup -- 5.3.1.1 Datasets -- 5.3.1.2 Environmental Setup -- 5.3.1.3
Evaluation Metrics -- 5.3.2 Performance Evaluation -- 5.3.2.1 Step 1 --
5.3.2.2 Step 2 -- 5.3.2.3 Step 3 -- 5.3.2.4 Step 4 -- 5.4 Summary --
References.
Chapter 6 Efficient Preprocessing Scheme for Anomaly Detection --
6.1 Efficient Anomaly Detection -- 6.1.1 Related Work -- 6.1.2
Principal Component Analysis -- 6.2 Proposed Preprocessing Scheme
for Anomaly Detection -- 6.2.1 Robust Preprocessing Scheme -- 6.2.2
RealTime Processing -- 6.2.3 Discussion -- 6.3 Case Study -- 6.3.1
Description of the Raw Data -- 6.3.1.1 Dimension -- 6.3.1.2 Predictors
-- 6.3.1.3 Response Variables -- 6.3.2 Experiment -- 6.3.3 Results --
6.4 Summary -- References -- Chapter 7 Privacy Preservation in the Era
of Big Data -- 7.1 Privacy Preservation Approaches -- 7.1.1
Anonymization -- 7.1.2 Differential Privacy -- 7.1.3 Federated
Learning -- 7.1.4 Homomorphic Encryption -- 7.1.5 Secure Multiparty
Computation -- 7.1.6 Discussion -- 7.2 PrivacyPreserving Anomaly
Detection -- 7.2.1 Literature Review -- 7.2.2 Preliminaries -- 7.2.2.1
Bilinear Groups -- 7.2.2.2 Asymmetric Predicate Encryption -- 7.2.3
System Model and Security Model -- 7.2.3.1 System Model -- 7.2.3.2
Security Model -- 7.3 Objectives and Workflow -- 7.3.1 Objectives --
7.3.2 Workflow -- 7.4 Predicate EncryptionBased Anomaly Detection
-- 7.4.1 Procedures -- 7.4.2 Development of Predicate -- 7.4.3
Deployment of Anomaly Detection -- 7.5 Case Study and Evaluation --
7.5.1 Overhead -- 7.5.2 Detection -- 7.6 Summary -- References --
Chapter 8 Adversarial Examples: Challenges and Solutions -- 8.1
Adversarial Examples -- 8.1.1 Problem Formulation in Machine
Learning -- 8.1.2 Creation of Adversarial Examples -- 8.1.3 Targeted

and Nontargeted Attacks -- 8.1.4 Blackbox and Whitebox Attacks --
8.1.5 Defenses Against Adversarial Examples -- 8.2 Adversarial Attacks
in Security Applications -- 8.2.1 Malware -- 8.2.2 Cyber Intrusions --
8.3 Case Study: Improving Adversarial Attacks Against Malware
Detectors -- 8.3.1 Background.
8.3.2 Adversarial Attacks on Malware Detectors -- 8.3.3 MalConv
Architecture -- 8.3.4 Research Idea -- 8.4 Case Study: A Metric for
Machine Learning Vulnerability to Adversarial Examples -- 8.4.1
Background -- 8.4.2 Research Idea -- 8.5 Case Study: Protecting Smart
Speakers from Adversarial Voice Commands -- 8.5.1 Background --
8.5.2 Challenges -- 8.5.3 Directions and Tasks -- 8.6 Summary --
References -- Index -- EULA.
