

1. Record Nr.	UNINA9910135024403321
Autore	Tan Ying <1964->
Titolo	Artificial immune system : applications in computer security // Ying Tan
Pubbl/distr/stampa	Hoboken, New Jersey : , : Wiley, , 2016 [Piscataway, New Jersey] : , : IEEE Xplore, , [2016]
ISBN	1-119-07627-7 1-119-07652-8 1-119-07658-7
Descrizione fisica	1 online resource (240 p.)
Classificazione	COM083000
Disciplina	005.8
Soggetti	Artificial immune systems Computer security Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	-- Preface xiii -- About Author xxi -- Acknowledgements xxiii -- 1 Artificial Immune System 1 -- 1.1 Introduction 1 -- 1.2 Biological Immune System 2 -- 1.2.1 Overview 2 -- 1.2.2 Adaptive Immune Process 3 -- 1.3 Characteristics of BIS 4 -- 1.4 Artificial Immune System 6 -- 1.5 AIS Models and Algorithms 8 -- 1.5.1 Negative Selection Algorithm 8 -- 1.5.2 Clonal Selection Algorithm 9 -- 1.5.3 Immune Network Model 11 -- 1.5.4 Danger Theory 12 -- 1.5.5 Immune Concentration 13 -- 1.5.6 Other Methods 14 -- 1.6 Characteristics of AIS 15 -- 1.7 Applications of Artificial Immune System 16 -- 1.7.1 Virus Detection 16 -- 1.7.2 Spam Filtering 16 -- 1.7.3 Robots 20 -- 1.7.4 Control Engineering 21 -- 1.7.5 Fault Diagnosis 22 -- 1.7.6 Optimized Design 22 -- 1.7.7 Data Analysis 22 -- 1.8 Summary 22 -- 2 Malware Detection 27 -- 2.1 Introduction 27 -- 2.2 Malware 28 -- 2.2.1 Definition and Features 28 -- 2.2.2 The Development Phases of Malware 29 -- 2.3 Classic Malware Detection Approaches 30 -- 2.3.1 Static Techniques 31 -- 2.3.2 Dynamic Techniques 31 -- 2.3.3 Heuristics 32 -- 2.4 Immune Based Malware

Detection Approaches 34 -- 2.4.1 An Overview of Artificial Immune System 34 -- 2.4.2 An Overview of Artificial Immune System for Malware Detection 35 -- 2.4.3 An Immune Based Virus Detection System Using Affinity Vectors 36 -- 2.4.4 A Hierarchical Artificial Immune Model for Virus Detection 38 -- 2.4.5 A Malware Detection Model Based on a Negative Selection Algorithm with Penalty Factor 2.5 Summary 43 -- 3 Immune Principle and Neural Networks Based Malware Detection 47 -- 3.1 Introduction 47 -- 3.2 Immune System for Malicious Executable Detection 48 -- 3.2.1 Non-self Detection Principles 48 -- 3.2.2 Anomaly Detection Based on Thickness 48 -- 3.2.3 Relationship Between Diversity of Detector Representation and Anomaly Detection Hole 48 -- 3.3 Experimental Dataset 48 -- 3.4 Malware Detection Algorithm 49 -- 3.4.1 Definition of Data Structures 49 -- 3.4.2 Detection Principle and Algorithm 49. 3.4.3 Generation of Detector Set 50 -- 3.4.4 Extraction of Anomaly Characteristics 50 -- 3.4.5 Classifier 52 -- 3.5 Experiment 52 -- 3.5.1 Experimental Procedure 53 -- 3.5.2 Experimental Results 53 -- 3.5.3 Comparison With Matthew G. Schultz's Method 55 -- 3.6 Summary 57 -- 4 Multiple-Point Bit Mutation Method of Detector Generation 59 -- 4.1 Introduction 59 -- 4.2 Current Detector Generating Algorithms 60 -- 4.3 Growth Algorithms 60 -- 4.4 Multiple Point Bit Mutation Method 62 -- 4.5 Experiments 62 -- 4.5.1 Experiments on Random Dataset 62 -- 4.5.2 Change Detection of Static Files 65 -- 4.6 Summary 65 -- 5 Malware Detection System Using Affinity Vectors 67 -- 5.1 Introduction 67 -- 5.2 Malware Detection Using Affinity Vectors 68 -- 5.2.1 Sliding Window 68 -- 5.2.2 Negative Selection 68 -- 5.2.3 Clonal Selection 69 -- 5.2.4 Distances 70 -- 5.2.5 Affinity Vector 71 -- 5.2.6 Training Classifiers with Affinity Vectors 71 -- 5.3 Evaluation of Affinity Vectors based malware detection System 73 -- 5.3.1 Dataset 73 -- 5.3.2 Length of Data Fragment 73 -- 5.3.3 Experimental Results 73 -- 5.4 Summary 74 -- 6 Hierarchical Artificial Immune Model 79 -- 6.1 Introduction 79 -- 6.2 Architecture of HAIM 80 -- 6.3 Virus Gene Library Generating Module 80 -- 6.3.1 Virus ODN Library 82 -- 6.3.2 Candidate Virus Gene Library 82 -- 6.3.3 Detecting Virus Gene Library 83 -- 6.4 Self-Nonself Classification Module 84 -- 6.4.1 Matching Degree between Two Genes 84 -- 6.4.2 Suspicious Program Detection 85 -- 6.5 Simulation Results of Hierarchical Artificial Immune Model 86 -- 6.5.1 Data Set 86 -- 6.5.2 Description of Experiments 86 -- 6.6 Summary 89 -- 7 Negative Selection Algorithm with Penalty Factor 91 -- 7.1 Introduction 91 -- 7.2 Framework of NSAPF 92 -- 7.3 Malware signature extraction module 93 -- 7.3.1 Malware Instruction Library (MIL) 93 -- 7.3.2 Malware Candidate Signature Library 94 -- 7.3.3 NSAPF and Malware Detection Signature Library 96 -- 7.4 Suspicious Program Detection Module 97. 7.4.1 Signature Matching 97 -- 7.4.2 Matching between Suspicious Programs and the MDSL 97 -- 7.4.3 Analysis of Penalty Factor 98 -- 7.5 Experiments and Analysis 99 -- 7.5.1 Experimental Datasets 99 -- 7.5.2 Experiments on Henchiri dataset 100 -- 7.5.3 Experiments on CILPKU08 Dataset 103 -- 7.5.4 Experiments on VX Heavens Dataset 104 -- 7.5.5 Parameter Analysis 104 -- 7.6 Summary 105 -- 8 Danger Feature Based Negative Selection Algorithm 107 -- 8.1 Introduction 107 -- 8.1.1 Danger Feature 107 -- 8.1.2 Framework of Danger Feature Based Negative Selection Algorithm 107 -- 8.2 DFNSA for Malware Detection 109 -- 8.2.1 Danger Feature Extraction 109 -- 8.2.2 Danger Feature Vector 110 -- 8.3 Experiments 111 -- 8.3.1 Datasets 111 -- 8.3.2 Experimental Setup 111 -- 8.3.3 Selection of Parameters 112 -- 8.3.4 Experimental Results 113 -- 8.4 Discussions 113 -- 8.4.1 Comparison of Detecting Feature Libraries 113 -- 8.4.2 Comparison of

Detection Time 114 -- 8.5 Summary 114 -- 9 Immune Concentration Based Malware Detection Approaches 117 -- 9.1 Introduction 117 -- 9.2 Generation of Detector Libraries 117 -- 9.3 Construction of Feature Vector for Local Concentration 122 -- 9.4 Parameters Optimization based on Particle Swarm Optimization 124 -- 9.5 Construction of Feature Vector for Hybrid Concentration 124 -- 9.5.1 Hybrid Concentration 124 -- 9.5.2 Strategies for Definition of Local Areas 126 -- 9.5.3 HC-based Malware Detection Method 127 -- 9.5.4 Discussions 128 -- 9.6 Experiments 130 -- 9.6.1 Experiments of Local Concentration 130 -- 9.6.2 Experiments of Hybrid Concentration 138 -- 9.7 Summary 142 -- 10 Immune Cooperation Mechanism Based Learning Framework 145 -- 10.1 Introduction 145 -- 10.2 Immune Signal Cooperation Mechanism based Learning Framework 148 -- 10.3 Malware Detection Model 151 -- 10.4 Experiments of Malware Detection Model 152 -- 10.4.1 Experimental setup 152 -- 10.4.2 Selection of Parameters 153 -- 10.4.3 Experimental Results 153 -- 10.4.4 Statistical Analysis 155. 10.5 Discussions 157 -- 10.5.1 Advantages 157 -- 10.5.2 Time Complexity 157 -- 10.6 Summary 158 -- 11 Class-wise Information Gain 161 -- 11.1 Introduction 161 -- 11.2 Problem Statement 163 -- 11.2.1 Definition of the Generalized Class 163 -- 11.2.2 Malware Recognition Problem 163 -- 11.3 Class-wise Information Gain 164 -- 11.3.1 Definition 164 -- 11.3.2 Analysis 166 -- 11.4 CIG-based Malware Detection Method 170 -- 11.4.1 Feature Selection Module 170 -- 11.4.2 Classification Module 171 -- 11.5 Dataset 172 -- 11.5.1 Benign Program Dataset 172 -- 11.5.2 Malware Dataset 172 -- 11.6 Selection of Parameter 174 -- 11.6.1 Experimental Setup 174 -- 11.6.2 Experiments of Selection of Parameter 174 -- 11.7 Experimental Results 175 -- 11.7.1 Experiments on the VXHeavens Dataset 177 -- 11.7.2 Experiments on the Henchiri Dataset 179 -- 11.7.3 Experiments on the CILPKU08 Dataset 180 -- 11.8 Discussions 180 -- 11.8.1 The Relationship Among IG-A, DFCIG-B and DFCIG-M 181 -- 11.8.2 Space Complexity 182 -- 11.9 Summary 183 -- Index 185.

---

## Sommario/riassunto

"This book focuses on the technologies and applications of artificial immune systems in malware and spam detection proposed in recent years by the computation intelligence laboratory at Peking University, China. It offers a theoretical perspective and practical solutions to graduate students, practitioners, and researchers working in the area of artificial immune system, machine learning, pattern recognition, and computer security"--

---