

# Contents

## Part I

<b>1</b>	<b>Security Risks from Vulnerabilities and Backdoors</b>	3
1.1	Harmfulness of Vulnerabilities and Backdoors	3
1.1.1	Related Concepts	6
1.1.2	Basic Topics of Research	7
1.1.3	Threats and Impacts	10
1.2	Inevitability of Vulnerabilities and Backdoors	16
1.2.1	Unavoidable Vulnerabilities and Backdoors	17
1.2.2	Contingency of Vulnerability Emergence	23
1.2.3	The Temporal and Spatial Characteristic of Cognition	26
1.3	The Challenge of Defense Against Vulnerabilities and Backdoors	29
1.3.1	Major Channels for Advanced Persistent Threat (APT) Attacks	29
1.3.2	Uncertain Unknown Threats	29
1.3.3	Limited Effect of Traditional “Containment and Repair”	31
1.4	Inspirations and Reflection	34
1.4.1	Building a System Based on “Contamination”	35
1.4.2	From Component Credibility to Structure Security	35
1.4.3	From Reducing Exploitability to Destroying Accessibility	35
1.4.4	Transforming the Problematic Scenarios	36
	References	37
<b>2</b>	<b>Formal Description of Cyber Attacks</b>	39
2.1	Formal Description Methods of Conventional Cyber Attacks	40
2.1.1	Attack Tree	40
2.1.2	Attack Graph	42
2.1.3	Analysis of Several Attack Models	44

2.2	The AS Theory . . . . .	45
2.2.1	The AS Model . . . . .	46
2.2.2	Defects in the AS Theory . . . . .	48
2.3	The MAS . . . . .	49
2.3.1	Definition and Nature of the MAS . . . . .	49
2.3.2	MAS Implementation Methods . . . . .	50
2.3.3	Limitations of the MAS . . . . .	51
2.4	New Methods of Formal Description of Cyber Attacks . . . . .	52
2.4.1	Cyber Attack Process . . . . .	52
2.4.2	Formal Description of the Attack Graph . . . . .	54
2.4.3	Formal Description of an Attack Chain . . . . .	55
2.4.4	Vulnerability Analysis of Cyber Attack Chains . . . . .	56
	References . . . . .	65
<b>3</b>	<b>Conventional Defense Technologies . . . . .</b>	<b>67</b>
3.1	Static Defense Technology . . . . .	67
3.1.1	Overview of Static Defense Technology . . . . .	67
3.1.2	Analysis of Static Defense Technology . . . . .	68
3.2	Honeypot . . . . .	76
3.2.1	Network Intrusion and Malicious Code Detection . . . . .	77
3.2.2	Capturing Samples of Malicious Codes . . . . .	78
3.2.3	Tracking and Analysis of Security Threats . . . . .	79
3.2.4	Extraction of Attack Features . . . . .	79
3.2.5	Limitations of Honeypot . . . . .	80
3.3	Collaborative Defense . . . . .	81
3.3.1	Collaborative Defense Between Intrusion Detection and Firewall . . . . .	82
3.3.2	Collaborative Defense Between Intrusion Prevention and Firewall Systems . . . . .	83
3.3.3	Collaborative Defense Between the Intrusion Prevention System and Intrusion Detection System . . . . .	84
3.3.4	Collaborative Defense Between Intrusion Prevention and Vulnerability Scanning Systems . . . . .	85
3.3.5	Collaborative Defense Between the Intrusion Prevention System and Honeypot . . . . .	85
3.4	Intrusion Tolerance Technology . . . . .	87
3.4.1	Technical Principles of Intrusion Tolerance . . . . .	87
3.4.2	Two Typical Intrusion Tolerance Systems . . . . .	91
3.4.3	Comparison of Web Intrusion Tolerance Architectures . . . . .	94
3.4.4	Differences Between Intrusion Tolerance and Fault Tolerance . . . . .	95
3.5	Sandbox Acting as an Isolation Defense . . . . .	97
3.5.1	Overview of Sandbox . . . . .	97
3.5.2	Theoretical Principles of Sandbox . . . . .	99
3.5.3	Status Quo of Sandbox Defense Technology . . . . .	100

3.6	Computer Immune Technology . . . . .	102
3.6.1	Overview of Immune Technology . . . . .	102
3.6.2	Artificial Immune System Status . . . . .	103
3.7	Review of Conventional Defense Methods . . . . .	106
	References. . . . .	109
<b>4</b>	<b>New Approaches to Cyber Defense . . . . .</b>	<b>113</b>
4.1	New Developments in Cyber Defense Technologies. . . . .	113
4.2	Trusted Computing . . . . .	116
4.2.1	Basic Thinking Behind Trusted Computing . . . . .	116
4.2.2	Technological Approaches of Trusted Computing. . . . .	117
4.2.3	New Developments in Trusted Computing . . . . .	123
4.3	Tailored Trustworthy Spaces . . . . .	129
4.3.1	Preconditions . . . . .	130
4.3.2	Tailored Trustworthy Spaces (TTS). . . . .	133
4.4	Mobile Target Defense. . . . .	135
4.4.1	MTD Mechanism. . . . .	136
4.4.2	Roadmap and Challenges of MTD . . . . .	138
4.5	Blockchain . . . . .	139
4.5.1	Basic Concept . . . . .	140
4.5.2	Core Technologies . . . . .	141
4.5.3	Analysis of Blockchain Security . . . . .	143
4.6	Zero Trust Security Model. . . . .	144
4.6.1	Basic Concept . . . . .	145
4.6.2	Forrester’s Zero Trust Security Framework . . . . .	146
4.6.3	Google’s Solution . . . . .	147
4.7	Reflections on New Cyber Defense Technologies. . . . .	150
	References. . . . .	155
<b>5</b>	<b>Analysis on Diversity, Randomness, and Dynamicity . . . . .</b>	<b>159</b>
5.1	Diversity. . . . .	160
5.1.1	Overview . . . . .	160
5.1.2	Diversity of the Executors . . . . .	161
5.1.3	Diversity of the Execution Space. . . . .	165
5.1.4	Differences Between Diversity and Pluralism. . . . .	169
5.2	Randomness. . . . .	170
5.2.1	Overview . . . . .	170
5.2.2	Address Space Randomization . . . . .	171
5.2.3	Instruction System Randomization . . . . .	173
5.2.4	Kernel Data Randomization. . . . .	175
5.2.5	Cost of Introduction. . . . .	177
5.3	Dynamicity. . . . .	181
5.3.1	Overview . . . . .	181
5.3.2	Dynamic Defense Technology . . . . .	185
5.3.3	Dynamicity Challenges . . . . .	193

5.4	Case of OS Diversity Analysis . . . . .	194
5.4.1	Statistical Analysis Data Based on the NVD . . . . .	195
5.4.2	Common OS Vulnerabilities . . . . .	196
5.4.3	Conclusions . . . . .	200
5.5	Chapter Summary . . . . .	202
	References . . . . .	204
<b>6</b>	<b>Revelation of the Heterogeneous Redundancy Architecture . . . . .</b>	<b>207</b>
6.1	Introduction . . . . .	207
6.2	Addressing the Challenge of Uncertain Failures . . . . .	209
6.2.1	Proposal of the Problem . . . . .	209
6.2.2	Enlightenment from TRA . . . . .	210
6.2.3	Formal Description of TRA . . . . .	212
6.3	The Role of Redundancy and Heterogeneous Redundancy . . . . .	214
6.3.1	Redundancy and Fault Tolerance . . . . .	214
6.3.2	Endogenous Functions and Structural Effects . . . . .	216
6.3.3	Redundancy and Situational Awareness . . . . .	216
6.3.4	From Isomorphism to Heterogeneity . . . . .	217
6.3.5	Relationship Between Fault Tolerance and Intrusion Tolerance . . . . .	220
6.4	Voting and Ruling . . . . .	221
6.4.1	Majority Voting and Consensus Mechanism . . . . .	221
6.4.2	Multimode Ruling . . . . .	222
6.5	Dissimilar Redundancy Structure . . . . .	223
6.5.1	Analysis of the Intrusion Tolerance Properties of the DRS . . . . .	227
6.5.2	Summary of the Endogenous Security Effects of the DRS . . . . .	231
6.5.3	Hierarchical Effect of Heterogeneous Redundancy . . . . .	232
6.5.4	Systematic Fingerprint and Tunnel-Through . . . . .	234
6.5.5	Robust Control and General Uncertain Disturbances . . . . .	235
6.6	Anti-attack Modeling . . . . .	239
6.6.1	The GSPN Model . . . . .	240
6.6.2	Anti-attack Considerations . . . . .	241
6.6.3	Anti-attack Modeling . . . . .	244
6.7	Anti-aggression Analysis . . . . .	246
6.7.1	Anti-general Attack Analysis . . . . .	246
6.7.2	Anti-special Attack Analysis . . . . .	258
6.7.3	Summary of the Anti-attack Analysis . . . . .	264
6.8	Conclusion . . . . .	266
6.8.1	Conditional Awareness of Uncertain Threats . . . . .	266
6.8.2	New Connotations of General Robust Control . . . . .	266
6.8.3	DRS Intrusion Tolerance Defect . . . . .	267
6.8.4	DRS Transformation Proposals . . . . .	269
	References . . . . .	271

<b>7</b>	<b>DHR Architecture</b>	273
7.1	Dynamic Heterogeneous Redundant Architecture	274
7.1.1	Basic Principles of DHRA	275
7.1.2	Goals and Effects of DHR	280
7.1.3	Typical DHR Architecture	287
7.1.4	Atypical DHR Architecture	291
7.2	The Attack Surface of DHR	293
7.3	Functionality and Effectiveness	295
7.3.1	Creating a Cognition Dilemma for the Target Object	295
7.3.2	DFI to Present Uncertainty	296
7.3.3	Making It Difficult to Exploit the Loopholes of the Target Object	296
7.3.4	Increasing the Uncertainty for an Attack Chain	297
7.3.5	Increasing the Difficulty for MR Escape	298
7.3.6	Independent Security Gain	299
7.3.7	Strong Correlation Between the Vulnerability Value and the Environment	299
7.3.8	Making It Difficult to Create a Multi-target Attack Sequence	300
7.3.9	Measurable Generalized Dynamization	301
7.3.10	Weakening the Impact of Homologous Backdoors	301
7.4	Reflections on the Issues Concerned	302
7.4.1	Addressing Uncertain Threats with Endogenous Mechanisms	302
7.4.2	Reliability and Credibility Guaranteed by the Structural Gain	304
7.4.3	New Security-Trustable Methods and Approaches	304
7.4.4	Creating a New Demand in a Diversified Market	305
7.4.5	The Problem of Super Escape and Information Leaking	306
7.5	Uncertainty: An Influencing Factor	307
7.5.1	DHR Endogenous Factors	307
7.5.2	DHR-Introduced Factors	310
7.5.3	DHR-Combined Factors	310
7.5.4	Challenges to a Forced Breakthrough	311
7.6	Analogical Analysis Based on the Coding Theory	312
7.6.1	Coding Theory and Turbo Codes	312
7.6.2	Analogic Analysis Based on Turbo Encoding	315
7.6.3	Some Insights	326
7.7	DHR-Related Effects	328
7.7.1	Ability to Perceive Unidentified Threats	328
7.7.2	Distributed Environmental Effect	328
7.7.3	Integrated Effect	329
7.7.4	Architecture-Determined Safety	329

7.7.5	Changing the Attack and Defense Game Rules in Cyberspace. . . . .	330
7.7.6	Creating a Loose Ecological Environment . . . . .	331
7.7.7	Restricted Application . . . . .	333
	References. . . . .	337

## Part II

<b>8</b>	<b>Original Meaning and Vision of Mimic Defense . . . . .</b>	<b>341</b>
8.1	Mimic Disguise and Mimic Defense . . . . .	341
8.1.1	Biological Mimicry . . . . .	341
8.1.2	Mimic Disguise . . . . .	343
8.1.3	Two Basic Security Problems and Two Severe Challenges . . . . .	345
8.1.4	An Entry Point: The Vulnerability of an Attack Chain . . . . .	347
8.1.5	Build the Mimic Defense. . . . .	348
8.1.6	Original Meaning of Mimic Defense. . . . .	352
8.2	Mimic Computing and Endogenous Security . . . . .	354
8.2.1	The Plight of HPC Power Consumption . . . . .	354
8.2.2	Original Purpose of Mimic Calculation. . . . .	355
8.2.3	Vision of Mimic Calculation . . . . .	356
8.2.4	Variable Structure Calculation and Endogenous Security . . . . .	360
8.3	Vision of Mimic Defense. . . . .	361
8.3.1	Reversing the Easy-to-Attack and Hard-to-Defend Status . . . . .	362
8.3.2	A Universal Structure and Mechanism . . . . .	364
8.3.3	Separation of Robust Control and Service Functions . . . . .	364
8.3.4	Unknown Threat Perception . . . . .	365
8.3.5	A Diversified Eco-environment . . . . .	366
8.3.6	Achievement of Multi-dimensional Goals. . . . .	367
8.3.7	Reduce the Complexity of Security Maintenance . . . . .	368
	References. . . . .	369
<b>9</b>	<b>The Principle of Cyberspace Mimic Defense . . . . .</b>	<b>371</b>
9.1	Overview . . . . .	371
9.1.1	Core Ideology. . . . .	372
9.1.2	Eradicating the Root Cause for Cyber Security Problems. . . . .	373
9.1.3	Biological Immunity and Endogenous Security . . . . .	374
9.1.4	Non-specific Surface Defense . . . . .	379
9.1.5	Integrated Defense . . . . .	379
9.1.6	GRC and the Mimic Structure . . . . .	380
9.1.7	Goals and Expectations . . . . .	381
9.1.8	Potential Application Targets. . . . .	386
9.2	Cyberspace Mimic Defense. . . . .	388
9.2.1	Underlying Theories and Basic Principles. . . . .	390
9.2.2	Mimic Defense System . . . . .	396

9.2.3	Basic Features and Core Processes . . . . .	411
9.2.4	Connotation and Extension Technologies . . . . .	417
9.2.5	Summary and Induction. . . . .	419
9.2.6	Discussions of the Related Issues . . . . .	421
9.3	Structural Representation and Mimic Scenarios . . . . .	430
9.3.1	Uncertain Characterization of the Structure . . . . .	430
9.3.2	Mimic Scenario Creation. . . . .	432
9.3.3	Typical Mimic Scenarios . . . . .	433
9.4	Mimic Display . . . . .	435
9.4.1	Typical Modes of Mimic Display . . . . .	435
9.4.2	Considerations of the MB Credibility . . . . .	438
9.5	Anti-attack and Reliability Analysis . . . . .	440
9.5.1	Overview . . . . .	440
9.5.2	Anti-attack and Reliability Models . . . . .	441
9.5.3	Anti-attack Analysis. . . . .	445
9.5.4	Reliability Analysis . . . . .	480
9.5.5	Conclusion. . . . .	487
9.6	Differences Between CMD and HIT (Heterogeneous Intrusion Tolerance). . . . .	488
9.6.1	Major Differences . . . . .	488
9.6.2	Prerequisites and Functional Differences . . . . .	490
9.6.3	Summary . . . . .	491
	References. . . . .	492
<b>10</b>	<b>Engineering and Implementation of Mimic Defense . . . . .</b>	<b>495</b>
10.1	Basic Conditions and Constraints . . . . .	495
10.1.1	Basic Conditions . . . . .	495
10.1.2	Constraints . . . . .	496
10.2	Main Realization Mechanisms. . . . .	497
10.2.1	Structural Effect and Functional Convergence Mechanism. . . . .	498
10.2.2	One-Way or Unidirectional Connection Mechanism. . . . .	498
10.2.3	Policy and Schedule Mechanism . . . . .	499
10.2.4	Mimic Ruling Mechanism . . . . .	500
10.2.5	Negative Feedback Control Mechanism . . . . .	500
10.2.6	Input Allocation and Adaptation Mechanism . . . . .	501
10.2.7	Output Agency and Normalization Mechanism. . . . .	501
10.2.8	Sharding/Fragmentation Mechanism. . . . .	502
10.2.9	Randomization/Dynamization/Diversity Mechanism . . . . .	502
10.2.10	Virtualization Mechanism . . . . .	503
10.2.11	Iteration and Superposition Mechanism . . . . .	504
10.2.12	Software Fault Tolerance Mechanism . . . . .	505
10.2.13	Dissimilarity Mechanism. . . . .	506
10.2.14	Reconfiguration Mechanism . . . . .	507
10.2.15	Executor's Cleaning and Recovery Mechanism . . . . .	507

10.2.16	Diversified Compilation Mechanism . . . . .	509
10.2.17	Mimic Structure Programming . . . . .	510
10.3	Major Challenges to Engineering Implementation . . . . .	511
10.3.1	Best Match of Function Intersection . . . . .	511
10.3.2	Complexity of Multimode Ruling . . . . .	512
10.3.3	Service Turbulence. . . . .	513
10.3.4	The Use of Open Elements . . . . .	514
10.3.5	Execution Efficiency of Mimic Software. . . . .	515
10.3.6	Diversification of Application Programs . . . . .	516
10.3.7	Mimic Defense Interface Configuration . . . . .	518
10.3.8	Version Update. . . . .	520
10.3.9	Loading of Non-cross-Platform Application . . . . .	521
10.3.10	Re-synchronization and Environment Reconstruction . . . . .	522
10.3.11	Simplifying Complexity of Heterogeneous Redundancy Realization . . . . .	523
10.4	Testing and Evaluation of Mimic Defense. . . . .	527
10.4.1	Analysis of Mimic Defense Effects . . . . .	527
10.4.2	Reference Perimeter of Mimic Defense Effects . . . . .	530
10.4.3	Factors to Be Considered in Mimic Defense V erification and Test. . . . .	533
10.4.4	Reflections on Quasi-stealth Evaluation . . . . .	545
10.4.5	Mimic Ruling-Based Measurable Review. . . . .	546
10.4.6	Mimic Defense Benchmark Function Experiment . . . . .	548
10.4.7	Attackers' Perspective . . . . .	556
	References. . . . .	560
<b>11</b>	<b>Foundation and Cost of Mimic Defense . . . . .</b>	<b>561</b>
11.1	Foundation for Mimic Defense Realization. . . . .	561
11.1.1	Era of Weak Correlation of Complexity to Cost . . . . .	561
11.1.2	High Efficiency Computing and Heterogeneous Computing . . . . .	562
11.1.3	Diversified Ecological Environment . . . . .	564
11.1.4	Standardization and Open Architecture. . . . .	565
11.1.5	Virtualization Technology . . . . .	566
11.1.6	Reconfiguration and Reorganization . . . . .	567
11.1.7	Distributed and Cloud Computing Service . . . . .	568
11.1.8	Dynamic Scheduling . . . . .	570
11.1.9	Feedback Control. . . . .	571
11.1.10	Quasi-Trusted Computing . . . . .	571
11.1.11	Robust Control. . . . .	572
11.1.12	New Developments of System Structure Technologies . . . . .	572
11.2	Analysis of Traditional Technology Compatibility . . . . .	573
11.2.1	Naturally Accepting Traditional Security Technologies . . . . .	573



11.2.2	Naturally Carrying Forward the Hardware Technological Advances . . . . .	575
11.2.3	Strong Correlation to Software Technological Development . . . . .	576
11.2.4	Depending on the Open and Plural Ecological Environment. . . . .	576
11.3	Cost of Mimic Defense Implementation . . . . .	576
11.3.1	Cost of Dynamicity . . . . .	577
11.3.2	Cost of Heterogeneity . . . . .	577
11.3.3	Cost of Redundancy . . . . .	579
11.3.4	Cost of Cleanup and Reconfiguration . . . . .	579
11.3.5	Cost of Virtualization. . . . .	580
11.3.6	Cost of Synchronization. . . . .	580
11.3.7	Cost of Ruling . . . . .	581
11.3.8	Cost of Input/Output Agency. . . . .	583
11.3.9	Cost of One-Way Connection . . . . .	584
11.4	Scientific and Technological Issues to Be Studied and Solved . . . . .	585
11.4.1	Scientific Issues Needing Urgent Study in the CMD Field. . . . .	585
11.4.2	Engineering and Technical Issues Needing Urgent Solution in the CMD Field . . . . .	586
11.4.3	Defense Effect Test and Evaluation . . . . .	593
11.4.4	Comprehensive Use of Defense Capability . . . . .	594
11.4.5	Issues Needing Continuous Attention . . . . .	595
11.4.6	Emphasizing the Natural and Inspired Solutions. . . . .	595
	References. . . . .	596
<b>12</b>	<b>Examples of Mimic Defense Application . . . . .</b>	<b>597</b>
12.1	Mimic Router Verification System. . . . .	597
12.1.1	Threat Design. . . . .	597
12.1.2	Designing Idea . . . . .	598
12.1.3	DHR-Based Router Mimic Defense Model. . . . .	600
12.1.4	System Architecture Design. . . . .	602
12.1.5	Mimic Transformation of the Existing Network . . . . .	608
12.1.6	Feasibility and Security Analysis. . . . .	609
12.2	Network Storage Verification System . . . . .	610
12.2.1	Overall Plan . . . . .	610
12.2.2	Arbiter . . . . .	612
12.2.3	Metadata Server Cluster. . . . .	613
12.2.4	Distributed Data Server . . . . .	613
12.2.5	The Client. . . . .	614
12.2.6	System Security Test and Result Analysis. . . . .	615

12.3	Mimic-Structured Web Server Verification System . . . . .	617
12.3.1	Threat Analysis . . . . .	617
12.3.2	Designing Idea . . . . .	618
12.3.3	System Architecture Design . . . . .	619
12.3.4	Functional Unit Design . . . . .	621
12.3.5	Prototype Design and Realization . . . . .	628
12.3.6	Attack Difficulty Evaluation . . . . .	629
12.3.7	Cost Analysis . . . . .	634
12.4	Cloud Computing and Virtualization Mimic Construction . . . . .	634
12.4.1	Basic Layers of Cloud Computing . . . . .	635
12.4.2	Cloud Computing Architecture Layers . . . . .	635
12.4.3	Virtualized DHR Construction . . . . .	637
12.5	Application Consideration for Software Design . . . . .	638
12.5.1	Effect of Randomly Invoking Mobile Attack Surface . . . . .	639
12.5.2	Guard Against Hidden Security Threats from Third Parties . . . . .	639
12.5.3	Typical Mimic Defense Effects . . . . .	639
12.6	Commonality Induction of System-Level Applications . . . . .	640
	References . . . . .	640
<b>13</b>	<b>Testing and Evaluation of the Mimic Defense Principle Verification System . . . . .</b>	<b>643</b>
13.1	Mimic Defense Principle Verification in the Router Environment . . . . .	644
13.1.1	Design of Test Methods for Mimic-Structured Routers . . . . .	644
13.1.2	Basic Router Function and Performance Test . . . . .	646
13.1.3	Test of the Mimic Defense Mechanism and Result Analysis . . . . .	648
13.1.4	Defense Effect Test and Result Analysis . . . . .	654
13.1.5	Test Summary of Mimic-Structured Router . . . . .	662
13.2	Mimic Defense Principle Verification in the Web Server Environment . . . . .	662
13.2.1	Design of Test Methods for Mimic-Structured Web Servers . . . . .	662
13.2.2	Basic Functional Test and Compatibility Test for Web Servers . . . . .	664
13.2.3	Mimic Defense Mechanism Test and Result Analysis . . . . .	667
13.2.4	Defense Effect Test and Result Analysis . . . . .	668
13.2.5	Web Server Performance Test . . . . .	674
13.2.6	Summary of the Web Principle Verification System Test . . . . .	678
13.3	Test Conclusions and Prospects . . . . .	678
	References . . . . .	681

<b>14</b>	<b>Application Demonstration and Current Network</b>	
	<b>Testing of Mimic Defense</b> . . . . .	683
14.1	Overview . . . . .	683
14.2	Application Demonstration of the Mimic-Structured Router . . . .	684
	14.2.1 Status Quo of the Pilot Network . . . . .	685
	14.2.2 Current Network Testing . . . . .	693
14.3	Mimic-Structured Web Server . . . . .	696
	14.3.1 Application Demonstration . . . . .	696
	14.3.2 Current Network Testing . . . . .	710
14.4	Mimic-Structured Domain Name Server (MSDN Server) . . . . .	721
	14.4.1 Application Demonstration . . . . .	721
	14.4.2 Testing and Evaluation . . . . .	729
14.5	Conclusions and Prospects. . . . .	734