"The 'bible' for cybersecurity, which needs to be consulted as we struggle to solve this enormous threat to our national security."
—**JOHN M. POINDEXTER,** PhD, VADM, USN (ret), Former National Security Advisor

ENGINEERING **TRUSTWORTHY** SYSTEMS

Get Cybersecurity Design Right the First Time

O. SAMI SAYDJARI

FOREWORD BY BRIAN SNOW

Mc
Graw
Hill
Education

Praise for *Engineering Trustworthy Systems*

"This is the 'bible' for cybersecurity, which needs to be consulted as we struggle to solve this enormous threat to our national security."

—John M. Poindexter, PhD, VADM, U.S. Navy (ret.),
Former National Security Advisor to President Reagan

"This book is a technical tour de force! Neatly organized between these covers is a comprehensive review of how to think about designing and building trusted (secure) systems, representing decades of experience and deep thought by the author. Sami presents the material clearly, including diagrams, charts, and extensive pointers to outside references. He has also crafted useful summaries and questions for further thought, making this book useful as either a valued reference or as an advanced textbook. Not only does Sami describe techniques to use in designing trustworthy systems, but he also describes shortcomings—he's not trying to 'sell' a particular method.

This is the book I have wanted for over a decade, for use in my advanced information security systems course. This will occupy an honored position on my bookshelf between Ross Anderson's *Security Engineering* and Michael Howard's *Writing Secure Code*. If you are involved with any aspect of designing or evaluating trustworthy systems, it should be on your bookshelf too."

—Eugene Spafford,
Professor of Computer Science and
leader of the CERIAS Project, Purdue University

"Sami Saydjari is today's cybersecurity Renaissance man. Sami was the first to recognize that failed cybersecurity could one day deliver societal existential change equivalent to nuclear warfare. His early tenacity led to DARPA's first cybersecurity research investment. This book is a definitive textbook on cybersecurity, and will become the instructional foundation for future trustworthy systems. Like the genius of Da Vinci, this book delivers insightful philosophy, deep understanding, practical guidance, and detailed instruction for building future systems that mitigate cybersecurity threats!"

—Dr. Marv Langston, cybersecurity technologies consultant;
former Naval Officer, DARPA office director,
U.S. Navy's first CIO, and U.S. Defense Department Deputy CIO

"Sami is one of the great experts in our field and he has produced one of the finest and most complete works in our field. It should be your priority to purchase and read this amazing book! For anyone desiring a comprehensive treatment of the cybersecurity discipline, this is definitely the book. It's an impressive work that covers the important issues in a complete and accurate manner."

—Dr. Edward G. Amoroso, CEO of TAG Cyber, and former CSO, AT&T

Praise for *Engineering Trustworthy Systems* (cont.)

"Sami Saydjari's career has spanned most of the history of cybersecurity, and in this book he distills the lessons of a lifetime. This book is both comprehensive and easy to read, making its concepts widely accessible. It is notable for its emphasis on looking at a system as a whole, not just an aggregation of components, and for helping readers understand how to value information and how to deal with risk. I urge those building the systems that will be part of tomorrow's critical cyberinfrastructure, which now extends into our factories, airplanes, cars, and homes, to read this book and apply its techniques. Until we learn to build on the lessons of the past, the future of cybersecurity will continue to resemble the present."

—Carl Landwehr, IEEE Fellow and member of
the National Cybersecurity Hall of Fame

"Saydjari has written an authoritative, timeless, and practical guide to cybersecurity. The architecture of the book allows the reader to gain knowledge across a wide range of areas from strategy and risk management, to the technical design concepts of engineering a trustworthy system with security and safety at its core. Each chapter concludes with a set of critical thinking questions. If organizations—corporate or government—take a disciplined approach in answering these questions, their understanding of the risks to their mission can only increase. We are reminded that society's dependency on information technology is growing and new technologies are introducing even more risk to our way of life. Saydjari presents multiple methods to assess risk and diagnose an organization's strengths and weaknesses. He then presents a thoughtful approach to effective risk reduction, taking into account cost and mission impact. This book underscores that our opponent's reach, speed, and understanding of our vulnerabilities currently outmatch our defenses, which is why we must learn how to invest in creating/designing/engineering the most trustworthy systems. Our future depends on it."

—Melissa Hathaway, cyber advisor to Presidents George W. Bush and
Barack H. Obama, now President of Hathaway Global Strategies
advising countries and companies around the world

"In *Engineering Trustworthy Systems*, Sami perfectly captures the asymmetrical nature of cyberwarfare. This text will help level the playing field and put the adversary on their heels and is required reading for any organization building or running a security testing team. Focusing on the 'hack' is a mistake, and Sami explains how and why bringing the strategist and tactician together builds a truly effective test team. Following the lessons from this text will transform test teams from hackers to cyber guardians."

—Jim Carnes, former Chief of Security Testing Center at the DOD

"Sami Saydjari's valuable new book reflects decades of experience in designing and building secure computer systems. His approach to risk management for secure system design is innovative and well worth reading."

—Steven B. Lipner, member of the National Cybersecurity Hall of Fame

"This book brings together all of the important aspects in cybersecurity design for the first time to include all of the myriad cybersecurity perspectives, the types and impact of failure, and the latest thinking in mitigation strategy. I can see this book becoming an essential and complete reference for the new student of cybersecurity as well as for the well-experienced professional. Sami's thoughts and insights give the book an excellent structure and relevant examples that make even the most difficult concepts easy to digest."

—Tom Longstaff, Chair, Computer Science, Cybersecurity,
and Information Systems Engineering Programs,
The Johns Hopkins University Engineering for Professionals

"As a long-standing proponent of rigorous, first principles design, I can endorse this book with unbridled enthusiasm. Cybersecurity practitioners, designers, and researchers will all find that the lessons in this book add inestimable, tangible value to their missions. The depth and breadth of this book are truly impressive."

—Roy Maxion, PhD, Research Professor,
Computer Science Department, Carnegie Mellon University

"'Yet another cybersecurity book' this is not. Its real strength lies in going beyond the requisite scary attack stories and empty claims straight to the heart of very real operational problems that undermine current defensive capabilities and strategies. It does this to encourage the reader to think more carefully about the kinds of strategic design and planning that are so often lacking in building sustainable, evolvable, and comprehensive cyber protections. I highly recommend this book to those who actually have to make cyber defense work."

—Kymie Tan, Systems Engineer, Jet Propulsion Lab

"O. Sami Saydjari addresses cybersecurity using a comprehensive and straightforward approach that draws on examples from other fields, such as biology and astronomy, to enhance clarity and purpose. *Engineering Trustworthy Systems* is a well-timed tome that strikes a balance between Saydjari's many years of experience as one of DARPA's top cybersecurity experts and the ubiquitous nature of technology in our daily lives. His style is personable and digestible for those without any formal computer science training. Read this book—and learn from one of the best."

—Teri Shors, Professor, Dept. of Biology, University of Wisconsin Oshkosh;
Author of *Understanding Viruses*

"This book provides a refreshing look at cybersecurity by acknowledging the need for systems engineering. The book also emphasizes that cybersecurity is important for the sake of mission assurance, which is very important, but all too often overlooked by IT security personnel."

—Joe Weiss, PE, CISM, CRISC, ISA Fellow, IEEE Senior Member,
Managing Director ISA99 (Industrial Automation and Control Systems Security)

This page intentionally left blank

ENGINEERING TRUSTWORTHY SYSTEMS

Get Cybersecurity Design Right the First Time

O. Sami Saydjari

Mc Graw Hill Education

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

Copyright © 2018 by O. Sami Saydjari. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

ISBN: 978-1-26-011818-6
MHID: 1-26-011818-5

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-011817-9, MHID: 1-26-011817-7.

eBook conversion by codeMantra
Version 1.0

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at www.mhprofessional.com.

Information has been obtained by McGraw-Hill Education from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill Education, or others, McGraw-Hill Education does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education's prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." McGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

This book is dedicated to Andrew Saydjari, my amazing son, and his brilliant peers who will shape the future during what will surely be a tumultuous time in human history.

About the Author

Mr. O. Sami Saydjari has been a visionary thought-leader in cybersecurity for over three decades, working for elite organizations, including the Defense Advanced Research Projects Agency (DARPA), National Security Agency, and NASA, among others. He has published more than a dozen landmark papers in the field, provided consultation to national leadership on cybersecurity policy, and educated the public through interviews with major media such as CNN, PBS, ABC, the *New York Times, Financial Times*, the *Wall Street Journal*, and *Time* magazine. Follow the author on Twitter @SamiSaydjari and visit www.samisaydjari.com and www.EngineeringTrustworthySystems.com for more information.

About the Technical Editors

Earl Boebert wrote his first computer program as an undergraduate at Stanford in 1958. He then served in the U.S. Air Force as an EDP Officer, where he was awarded the Air Force Commendation Medal for an Air Force–wide project. He then joined Honeywell, where he worked on military, aerospace, and security systems, and received Honeywell's highest award for technical achievement. He was the Chief Scientist and technical founder of Secure Computing Corporation, where he led the development of the Sidewinder security server. He then finished his career as a Senior Scientist at Sandia National Laboratories.

He is listed as an inventor on 13 patents and is coauthor of a book on formal software verification and another which analyzes the causes of the Deepwater Horizon disaster. He has participated in 11 studies and workshops of the National Academies of Sciences, Engineering, and Medicine and in 2011 was named a National Associate of the Academies.

Peter G. Neumann (Neumann@CSL.sri.com) is in his 47th year at SRI International, where he is Chief Scientist of the Computer Science Lab. Prior to that, he was at Bell Labs in Murray Hill, New Jersey, throughout the 1960s, with extensive involvement in the Multics development. He has AM, SM, and PhD degrees from Harvard, and a Dr rerum naturalium from Darmstadt. He is a Fellow of the ACM, IEEE, and AAAS. In 1985, he created the ACM Risks Forum (http://catless.ncl.ac.uk/Risks/), which he moderates. His 1995 book, *Computer-Related Risks*, is still timely! He has taught at Darmstadt, Stanford, U.C. Berkeley, and the University of Maryland. See his website (http://www.csl.sri.com/users/neumann/) for further background and URLs for papers, reports, testimonies, and musings.

Contents at a Glance

Part I What Do You Want?

1 What's the Problem? 3
2 Cybersecurity Right-Think 25
3 Value and Mission: Know Thyself 37
4 Harm: Mission in Peril 51
5 Approximating Reality 65

Part II What Could Go Wrong?

6 Adversaries: Know Thy Enemy 89
7 Forests of Attack Trees 115

Part III What Are the Building Blocks of Mitigating Risk?

8 Countermeasures: Security Controls 131
9 Trustworthy Hardware: Bedrock 155
10 Cryptography: A Sharp and Fragile Tool 167
11 Authentication 189
12 Authorization 199
13 Detection Foundation 225
14 Detection Systems 237
15 Detection Strategy 257
16 Deterrence and Adversarial Risk 273

Part IV How Do You Orchestrate Cybersecurity?

17 Cybersecurity Risk Assessment 287
18 Risk Mitigation and Optimization 313
19 Engineering Fundamentals 331
20 Architecting Cybersecurity 351
21 Assuring Cybersecurity: Getting It Right 369
22 Cyber Situation Understanding: What's Going On 381
23 Command and Control: What to Do About Attacks 401

Part V Moving Cybersecurity Forward

24 Strategic Policy and Investment 429
25 Thoughts on the Future of Cybersecurity 443

Part VI Appendix and Glossary

A Resources 467
Glossary 483

Index 523

Contents

Foreword xxxix
Acknowledgments xli
Introduction. xliii

Part I What Do You Want?

Chapter 1 What's the Problem?. 3
Overview. 3
Learning Objectives 4
1.1 Baking in Trustworthiness: Design-Time. 5
1.1.1 What Is Trust? 5
1.1.2 Trust and Belief. 7
1.1.3 Engineering 7
1.1.4 Why Trust? 7
1.2 Operational Perspective: Basic Questions 8
1.2.1 Am I Under Attack?. 9
1.2.2 What Is the Nature of the Attack?. 10
1.2.3 What Is the Mission Impact So Far?. 12
1.2.4 What Is the Potential Mission Impact? 13
1.2.5 When Did It Start?. 13
1.2.6 Who Is Attacking? 13
1.2.7 What Are They Trying to Do? 14
1.2.8 What Is the Attacker's Next Step?. 14
1.2.9 What Can I Do About It? 15
1.2.10 What Are My Options and How Effective Will Each Option Be? 15
1.2.11 How Will My Mitigation Actions Affect Operation? 15
1.2.12 How Do I Better Defend Myself in the Future? 15
1.3 Asymmetry of Cyberspace Effects 16
1.3.1 Dimensionality 16
1.3.2 Nonlinearity 17
1.3.3 Coupling. 17
1.3.4 Velocity. 17
1.3.5 Manifestation 18
1.3.6 Detectability 18

1.4 The Cybersecurity Solution Landscape 18
1.4.1 Information Assurance Science and Engineering 19
1.4.2 Defensive Mechanisms 20
1.4.3 Cybersensors and Exploitation 20
1.4.4 Cyber Situation Understanding 20
1.4.5 Cyber Actuation 20
1.4.6 Cyber Command and Control 21
1.4.7 Cyber Defense Strategy and Tactics 21
1.5 Ounces of Prevention and Pounds of Cure 21
Conclusion 22
Questions 22
Chapter 2 Cybersecurity Right-Think 25
Overview. 25
Learning Objectives 26
2.1 It's About Risk 26
2.2 The Cybersecurity Trade-off: Performance and Functionality 26
2.2.1 User-Friendliness 28
2.2.2 Time to Market 29
2.2.3 Employee Morale 29
2.2.4 Missed Opportunity 30
2.2.5 Opportunity Cost 30
2.2.6 Quantity of Service or Product 31
2.2.7 Quality of Service or Product. 31
2.2.8 Cost of Service or Product 32
2.2.9 Limited Resources 33
2.3 Theories of Security Come from Theories of Insecurity 33
2.4 They Come at You Through the Weeds 33
2.5 Top-Down Meets Bottom-Up 34
2.6 Cybersecurity Is a Live Orchestra, Not a Recorded Instrument 35
Conclusion 35
Questions 36
Chapter 3 Value and Mission: Know Thyself 37
Overview. 37
Learning Objectives 38
3.1 Focus on Mission and Value 38
3.1.1 Avoid Concentrating Value. 39
3.1.2 Beware the Complacency of Trust 39
3.2 Confidentiality: Value of Secrecy from Adversaries 40
3.2.1 Acquired-Knowledge Secrets. 40
3.2.2 Planning Secrets 41
3.2.3 Stolen Secrets 42
3.2.4 Means-of-Stealing-Secrets Secrets 43

3.3 Confidentiality: Beware the Tyranny of Secrecy 44
3.3.1 Secrecy Is Tenuous 44
3.3.2 Secrecy Is Expensive 44
3.3.3 Secrecy Can Be Self-Defeating 45
3.3.4 Secrecy Is Self-Breeding 45
3.3.5 Secrecy Creates a Form of Corrupting Power and Impediment to Operation 46
3.4 Confidentiality: Changing the Value Proposition 46
3.4.1 Minimize Secrecy and Dependency on Secrecy 46
3.4.2 Minimize Impact of Loss of Secrecy 47
3.5 Integrity: The Root of All Trustworthiness Value 47
3.6 Availability: An Essential Yet Tenuous Value 48
Conclusion 48
Questions 49
Chapter 4 Harm: Mission in Peril 51
Overview 51
Learning Objectives 52
4.1 Focus on Strategic Risks 52
4.1.1 What Is Strategic Risk? 52
4.1.2 Expected Harm 53
4.1.3 The Range of Risks 54
4.1.4 The Meaning of Focus 54
4.2 Harm Is About Mission 54
4.2.1 Elicitation of Harm 55
4.2.2 Aggregating Harm Statements 55
4.2.3 Representative Harm Lists 55
4.3 Critical Asset Inventory: Data 55
4.3.1 Data Asset Types 56
4.3.2 Data Value Spectrum 56
4.3.3 Criticality Classes 56
4.3.4 Criticality Levels 57
4.4 A Template for Exploring Mission Harm 58
4.5 Harm Is in the Eye of the Beholder 61
4.5.1 Gravity of Harm: Consensus 61
4.5.2 Drawing Conclusions 61
4.6 Sometimes Belief Is More Powerful than Truth 61
4.6.1 Destroying Value 62
4.6.2 Frustrating to Address: Life Is Unfair 62
Conclusion 62
Questions 63

Chapter 5 Approximating Reality . . . 65
Overview. . . . 65
Learning Objectives . . . 66
5.1 The Complexity of State: Why Model? . . . 66
5.2 Levels of Abstraction: At What Levels . . . 67
5.3 What to Model and Why. . . . 68
5.3.1 The Target System . . . 68
5.3.2 Users . . . 69
5.3.3 Adversaries . . . 70
5.3.4 Measures/Countermeasures . . . 70
5.4 Models Are Always Wrong, Sometimes Useful. . . . 71
5.4.1 Incompleteness of Essentials . . . 71
5.4.2 Inaccuracy . . . 72
5.4.3 Non-Timeliness . . . 73
5.5 Model Views . . . 75
5.5.1 Defender's View . . . 75
5.5.2 Adversary's View . . . 77
5.5.3 Attacking the Views Themselves . . . 79
5.6 Defense Models Must Consider Failure Modes . . . 80
5.7 Assume Adversaries Know Defender's System . . . 82
5.8 Assume Adversaries Are Inside Defender's System . . . 83
Conclusion . . . 84
Questions . . . 85

Part II What Could Go Wrong?

Chapter 6 Adversaries: Know Thy Enemy . . . 89
Overview. . . . 89
Learning Objectives . . . 90
6.1 Know Your Adversaries . . . 91
6.1.1 Intentions. . . . 91
6.1.2 Capabilities . . . 92
6.1.3 Attacker Resources and Defender Resources . . . 92
6.1.4 Risk Tolerance. . . . 93
6.1.5 Strategic Goals . . . 93
6.1.6 Tactics. . . . 94
6.2 Assume Smart Adversaries . . . 95
6.3 Assume Adversaries Don't Play Fair . . . 96
6.3.1 Going Around Security Controls . . . 96
6.3.2 Going Beneath Security Controls . . . 96
6.3.3 Attacking the Weakest Link . . . 98
6.3.4 Violating a Design Assumption . . . 99
6.3.5 Using Maintenance Modes. . . . 100

6.3.6 Using Social Engineering 100
6.3.7 Using Bribery and Blackmail to Subvert Insiders. 101
6.3.8 Taking Advantage of Temporary Bypasses 101
6.3.9 Taking Advantage of Temporary Connections. 102
6.3.10 Taking Advantage of Natural System Failure 103
6.3.11 Exploiting Bugs You Did Not Even Know You Had. 104
6.3.12 Compromising External Systems that a System Trusts. 104
6.4 Anticipate Attack Escalation. 105
6.5 Red Teams 106
6.5.1 Opposing Force. 107
6.5.2 Red Team Characteristics. 107
6.5.3 Other Types of Red Teams 108
6.6 Cyberspace Exercises 109
6.6.1 Red Versus Blue 109
6.6.2 Pure Versus Hybrid 110
6.6.3 Purple Collaboration 111
6.7 Red Team Work Factor: Measuring Difficulty. 112
Conclusion 113
Questions 113

Chapter 7 Forests of Attack Trees. 115
Overview. 115
Learning Objectives 116
7.1 Attack Trees and Forests 116
7.1.1 Attack Tree Structure 116
7.1.2 Deriving Attack Scenarios 117
7.1.3 From Trees to Forests 118
7.2 System Failures Predict Cybersecurity Failures. 119
7.2.1 Inspirational Catastrophes 119
7.2.2 The 10x Rule 119
7.2.3 Feigning Failure 120
7.3 Understanding Failure Is the Key to Success: The Five Whys. 120
7.3.1 Why Five Whys?. 120
7.3.2 Projecting Fishbones 121
7.4 Forests Should Be Representative, Not Exhaustive. 121
7.5 Drive Each Attack Tree Layer by Asking How 123
7.6 Go as Deep as Needed and No Deeper. 125
7.7 Beware of External Dependencies 125
7.7.1 Just in Time 125
7.7.2 Information Dependency 126
7.7.3 Creating Redundancy 126
Conclusion 127
Questions 127

Part III What Are the Building Blocks of Mitigating Risk?

Chapter 8 Countermeasures: Security Controls 131
Overview. 131
Learning Objectives 132
8.1 Countermeasures: Design to Purpose. 133
8.2 Ensure Attack-Space Coverage (Defense in Breadth). 133
8.3 Defense in Depth and Breadth 134
8.4 Multilevel Security, Trusted Code, Security Kernels 136
8.4.1 Multilevel Security. 136
8.4.2 Trusted Code. 138
8.4.3 Security Kernel and the Reference Monitor 138
8.5 Integrity and Type Enforcement 140
8.5.1 Multilevel Integrity 140
8.5.2 Type Enforcement 141
8.6 Cybersecurity Usability 143
8.6.1 Invisible 144
8.6.2 Transparent 144
8.6.3 Clear 145
8.6.4 Easy to Understand 145
8.6.5 Reliable 146
8.6.6 Fast 146
8.6.7 Reversible. 146
8.6.8 Adaptable. 147
8.6.9 Traceable 147
8.6.10 Reviewable. 148
8.7 Deploy Default Secure 149
8.8 Costs 149
8.8.1 Cost Always Matters 149
8.8.2 Time-to-Deploy Matters 150
8.8.3 Impact to Mission Matters 150
8.8.4 Pareto Rule: 80/20 151
8.8.5 Opportunity Cost Is a Key Part of Cost 151
8.8.6 How Much to Invest in Cybersecurity 151
8.8.7 Optimizing Zero-Sum Cybersecurity Budgets 152
Conclusion 152
Questions 153
Chapter 9 Trustworthy Hardware: Bedrock 155
Overview. 155
Learning Objectives 155
9.1 Foundation of Trust 156
9.2 Instruction Set Architectures 158
9.3 Supervisors with Rings and Things 158

9.4 Controlling Memory: Mapping, Capabilities, and Tagging . . . 159
9.4.1 Memory Mapping . . . 160
9.4.2 Capabilities . . . 160
9.4.3 Tagging . . . 162
9.5 Software in Hardware . . . 162
9.5.1 Microcode . . . 162
9.5.2 Firmware . . . 162
9.5.3 Secure Bootstrapping . . . 163
9.6 Buses and Controllers . . . 163
Conclusion . . . 164
Questions . . . 164
Chapter 10 Cryptography: A Sharp and Fragile Tool . . . 167
Overview . . . 167
Learning Objectives . . . 168
10.1 What Is Cryptography? . . . 168
10.2 Key Space . . . 169
10.3 Key Generation . . . 171
10.4 Key Distribution . . . 173
10.4.1 Transmission to Intended Recipients . . . 173
10.4.2 Storage . . . 174
10.4.3 Loading . . . 175
10.5 Public-Key Cryptography . . . 175
10.5.1 The Math . . . 176
10.5.2 Certificates and Certificate Authorities . . . 177
10.5.3 Performance and Use . . . 178
10.5.4 Side Effect of Public-Key Cryptography . . . 179
10.6 Integrity . . . 179
10.7 Availability . . . 182
10.7.1 Positive Effects . . . 182
10.7.2 Negative Effects . . . 182
10.8 Chinks in the Cryptographic Armor . . . 184
10.8.1 Quantum Cryptanalytics: Disruptive Technology . . . 184
10.8.2 P=NP . . . 185
10.9 Cryptography Is Not a Panacea . . . 185
10.10 Beware of Homegrown Cryptography . . . 186
Conclusion . . . 186
Questions . . . 187
Chapter 11 Authentication . . . 189
Overview . . . 189
Learning Objectives . . . 189
11.1 Entity Identification: Phase 1 of Authentication . . . 191
11.2 Identity Certification: Phase 2 of Authentication . . . 191
11.3 Identity Resolution: Phase 3 of Authentication . . . 193

11.4 Identity Assertion and Identity Proving: Phases 4 and 5 of Authentication 194
11.5 Identity Decertification: Phase 6 of Authentication 194
11.6 Machine-to-Machine Authentication Chaining 195
Conclusion 196
Questions 196

Chapter 12 Authorization 199
Overview 199
Learning Objectives 200
12.1 Access Control 200
12.1.1 Discretionary Access Control 201
12.1.2 Mandatory Access Control 203
12.1.3 Covert Channels 205
12.1.4 Identity-Based Access Control 206
12.1.5 Attribute-Based Access Control 207
12.2 Attribute Management 210
12.2.1 User Attributes and Privilege Assignment 210
12.2.2 Resource Attribute Assignment 211
12.2.3 Attribute Collection and Aggregation 211
12.2.4 Attribute Validation 213
12.2.5 Attribute Distribution 215
12.3 Digital Policy Management 216
12.3.1 Policy Specification 216
12.3.2 Policy Distribution 217
12.3.3 Policy Decision 218
12.3.4 Policy Enforcement 218
12.4 Authorization Adoption Schemas 220
12.4.1 Direct Integration 221
12.4.2 Indirect Integration 221
12.4.3 Alternative Integration 221
Conclusion 222
Questions 222

Chapter 13 Detection Foundation 225
Overview 225
Learning Objectives 225
13.1 The Role of Detection 226
13.2 How Detection Systems Work 227
13.3 Feature Selection 228
13.3.1 Attack Manifestation in Features 229
13.3.2 Manifestation Strength 229
13.3.3 Mapping Attacks to Features 230
13.3.4 Criteria for Selection 230

13.4 Feature Extraction 231
13.5 Event Selection 231
13.6 Event Detection. 232
13.7 Attack Detection. 232
13.8 Attack Classification. 233
13.9 Attack Alarming 233
13.10 Know Operational Performance Characteristics for Sensors. 233
Conclusion 234
Questions 235

Chapter 14 Detection Systems. 237
Overview. 237
Learning Objectives 238
14.1 Types of Detection Systems 238
14.1.1 Signature-Based 238
14.1.2 Anomaly Detection 241
14.2 Detection Performance: False Positives,
False Negatives, and ROCs 245
14.2.1 Feature Selection 245
14.2.2 Feature Extraction 248
14.2.3 Event Selection 249
14.2.4 Attack Detection 249
14.2.5 Attack Classification 250
14.2.6 Attack Alarming. 251
14.3 Drive Detection Requirements from Attacks 251
14.4 Detection Failures. 252
14.4.1 Blind Sensors 252
14.4.2 Below Noise Floor 252
14.4.3 Below Alert Threshold 253
14.4.4 Improper Placement 253
14.4.5 Natural Failure 254
14.4.6 Successfully Attacked 254
14.4.7 Blocked Sensor Input 255
14.4.8 Blocked Report Output. 255
Conclusion 255
Questions 256

Chapter 15 Detection Strategy. 257
Overview. 257
Learning Objectives 257
15.1 Detect in Depth and Breadth 258
15.1.1 Breadth: Network Expanse. 258
15.1.2 Depth: Network Expanse 260
15.1.3 Breadth: Attack Space 261
15.1.4 Depth: Attack Space 261

15.2 Herd the Adversary to Defender's Advantage 262
15.3 Attack Epidemiology 263
15.4 Detection Honeypots 264
15.5 Refining Detection 264
    15.5.1 Running Alerts to Ground 264
    15.5.2 Learning More About an Attack 265
15.6 Enhancing Attack Signal and Reducing Background Noise 266
    15.6.1 Reducing the Noise Floor 267
    15.6.2 Boosting Attack Signal 269
    15.6.3 Lowering the Alert Threshold 270
Conclusion 270
Questions 271

Chapter 16 Deterrence and Adversarial Risk 273
Overview 273
    Learning Objectives 273
16.1 Deterrence Requirements 274
    16.1.1 Reliable Detection: Risk of Getting Caught 274
    16.1.2 Reliable Attribution 275
    16.1.3 Meaningful Consequences 276
16.2 All Adversaries Have Risk Thresholds 277
16.3 System Design Can Modulate Adversary Risk 277
    16.3.1 Detection Probability 278
    16.3.2 Attribution Probability 278
    16.3.3 Consequence Capability and Probability 278
    16.3.4 Retaliation Capability and Probability 279
    16.3.5 Risky Behavior 279
16.4 Uncertainty and Deception 279
    16.4.1 Uncertainty 279
    16.4.2 Deception 280
16.5 When Detection and Deterrence Do Not Work 280
Conclusion 281
Questions 282

Part IV How Do You Orchestrate Cybersecurity?

Chapter 17 Cybersecurity Risk Assessment 287
Overview 287
    Learning Objectives 288
17.1 A Case for Quantitative Risk Assessment 288
17.2 Risk as a Primary Metric 289
17.3 Why Measure? 290
    17.3.1 Characterize 290
    17.3.2 Evaluate 291
    17.3.3 Predict 291
    17.3.4 Improve 292

17.4 Evaluate Defenses from an Attacker's Value Perspective 292
17.5 The Role of Risk Assessment and Metrics in Design 293
17.6 Risk Assessment Analysis Elements 295
17.6.1 Develop Mission Model 295
17.6.2 Develop System Model 295
17.6.3 Develop Adversary Models 296
17.6.4 Choose Representative Strategic Attack Goals............... 297
17.6.5 Estimate Harm Using Wisdom of Crowds 298
17.6.6 Estimate Probability Using Wisdom of Crowds 299
17.6.7 Choose Representative Subset.......................... 301
17.6.8 Develop Deep Attack Trees 301
17.6.9 Estimate Leaf Probabilities and Compute Root 303
17.6.10 Refine Baseline Expected Harm 305
17.6.11 Harvest Attack Sequence Cut Sets => Risk Source 306
17.6.12 Infer Attack Mitigation Candidates from Attack Sequences.. 308
17.7 Attacker Cost and Risk of Detection............................. 309
17.7.1 Resources... 309
17.7.2 Risk Tolerance.. 309
Conclusion 309
Questions 310
Chapter 18 Risk Mitigation and Optimization.................................313
Overview... 313
Learning Objectives 313
18.1 Develop Candidate Mitigation Packages 315
18.2 Assess Cost of Mitigation Packages.............................. 317
18.2.1 Direct Cost 317
18.2.2 Mission Impact....................................... 318
18.3 Re-estimate Leaf Node Probabilities and Compute Root Node Probability 320
18.4 Optimize at Various Practical Budget Levels....................... 323
18.4.1 Knapsack Algorithm 323
18.4.2 Sensitivity Analysis 325
18.5 Decide Investment 326
18.6 Execute 327
Conclusion 327
Questions 328
Chapter 19 Engineering Fundamentals...331
Overview... 331
Learning Objectives 331
19.1 Systems Engineering Principles................................... 332
19.1.1 Murphy's Law 332
19.1.2 Margin of Safety...................................... 336
19.1.3 Conservation of Energy and Risk 336

19.1.4 Keep It Simple, Stupid . . . 337
19.1.5 Development Process . . . 338
19.1.6 Incremental Development and Agility . . . 339
19.2 Computer Science Principles . . . 340
19.2.1 Modularity and Abstraction . . . 340
19.2.2 Layering . . . 342
19.2.3 Time and Space Complexity: Understanding Scalability . . . 343
19.2.4 Focus on What Matters: Loops and Locality . . . 344
19.2.5 Divide and Conquer and Recursion . . . 345
Conclusion . . . 347
Questions . . . 348
Chapter 20 Architecting Cybersecurity . . . 351
Overview . . . 351
Learning Objectives . . . 351
20.1 Reference Monitor Properties . . . 352
20.1.1 Functional Correctness . . . 352
20.1.2 Non-Bypassable . . . 355
20.1.3 Tamperproof . . . 355
20.2 Simplicity and Minimality Breed Confidence . . . 355
20.3 Separation of Concerns and Evolvability . . . 356
20.4 Security Policy Processing . . . 356
20.4.1 Policy Specification . . . 357
20.4.2 Policy Decision Making . . . 358
20.4.3 Policy Enforcement . . . 360
20.5 Dependability and Tolerance . . . 360
20.5.1 Cybersecurity Requires Fail Safety . . . 360
20.5.2 Expect Failure: Confine Damages Using Bulkheads . . . 361
20.5.3 Tolerance . . . 362
20.5.4 Synergize Prevention, Detect-Response, and Tolerance . . . 364
20.6 Cloud Cybersecurity . . . 365
Conclusion . . . 366
Questions . . . 367
Chapter 21 Assuring Cybersecurity: Getting It Right . . . 369
Overview . . . 369
Learning Objectives . . . 369
21.1 Cybersecurity Functionality Without Assurance Is Insecure . . . 370
21.2 Treat Cybersecurity Subsystems as Critical Systems . . . 371
21.3 Formal Assurance Arguments . . . 371
21.3.1 Cybersecurity Requirements . . . 372
21.3.2 Formal Security Policy Model . . . 374
21.3.3 Formal Top-Level Specification . . . 374
21.3.4 Security-Critical Subsystem Implementation . . . 375
21.4 Assurance-in-the-Large and Composition . . . 376
21.4.1 Composition . . . 376
21.4.2 Trustworthiness Dependencies . . . 376

21.4.3 Avoiding Dependency Circularity. 377
21.4.4 Beware of the Inputs, Outputs, and Dependencies 378
21.4.5 Violating Unstated Assumptions. 378
Conclusion 379
Questions 379

Chapter 22 Cyber Situation Understanding: What's Going On 381
Overview. 381
Learning Objectives 382
22.1 Situation Understanding Interplay with Command and Control 382
22.2 Situation-Based Decision Making: The OODA Loop 383
22.3 Grasping the Nature of the Attack. 385
22.3.1 What Vulnerability Is It Exploiting? 385
22.3.2 Which Paths Are the Attacks Using? 385
22.3.3 Are the Attack Paths Still Open?. 387
22.3.4 How Can the Infiltration, Exfiltration, and Propagation Paths Be Closed?. 388
22.4 The Implication to Mission 389
22.4.1 Increased Risk. 391
22.4.2 Contingency Planning. 391
22.4.3 Nature and Locus Guiding Defense 392
22.5 Assessing Attack Damages 392
22.6 Threat Assessment 393
22.7 The State of Defenses 393
22.7.1 Health, Stress, and Duress 394
22.7.2 Status 394
22.7.3 Configuration Maneuverability 395
22.7.4 Progress and Failure 396
22.8 Dynamic Defense Effectiveness 396
Conclusion 397
Questions 398

Chapter 23 Command and Control: What to Do About Attacks 401
Overview. 401
Learning Objectives 402
23.1 The Nature of Control 402
23.1.1 Decision Cycle 402
23.1.2 Speed Considerations 403
23.1.3 Hybrid Control 403
23.2 Strategy: Acquiring Knowledge 404
23.2.1 Analogy 405
23.2.2 Direct Experience. 406
23.2.3 Vicarious Experience 406
23.2.4 Simulation 407
23.3 Playbooks 409
23.3.1 Game Theory 409
23.3.2 Courses of Action in Advance 410

23.3.3 Criteria for Choosing Best Action 412
23.3.4 Planning Limitations 415
23.4 Autonomic Control 416
23.4.1 Control Theory 416
23.4.2 Role of Autonomic Control 418
23.4.3 Autonomic Action Palette 419
23.5 Meta-Strategy 420
23.5.1 Don’t Overreact 421
23.5.2 Don’t Be Predictable 422
23.5.3 Stay Ahead of the Attackers 422
Conclusion 423
Questions 424

Part V Moving Cybersecurity Forward

Chapter 24 Strategic Policy and Investment 429
Overview 429
Learning Objectives 430
24.1 Cyberwar: How Bad Can Bad Get? 430
24.1.1 Scenario 432
24.1.2 Call to Action 432
24.1.3 Barriers to Preparation Action 433
24.1.4 Smoking Gun 433
24.2 Increasing Dependency, Fragility, and the Internet of Things 434
24.2.1 Societal Dependency 434
24.2.2 Just-in-Time Everything 435
24.2.3 The Internet of Things 435
24.2.4 Propagated Weakness 435
24.3 Cybersecurity in the Virtual World: Virtual Economy 436
24.3.1 Booming Game Economy: Virtual Gold Rush 436
24.3.2 Digital Currency Such as Bitcoin 436
24.3.3 Virtual High-Value Targets 436
24.3.4 Start from Scratch? 437
24.4 Disinformation and Influence Operations: Fake News 437
24.4.1 What’s New? 437
24.4.2 Hacking Wetware 438
24.4.3 Polluting the Infosphere 439
Conclusion 439
Questions 440

Chapter 25 Thoughts on the Future of Cybersecurity 443
Overview 443
Learning Objectives 444
25.1 A World Without Secrecy 444
25.1.1 Timed Release 445
25.1.2 Minimize Generation 445
25.1.3 Zero-Secrecy Operations 445

25.2 Coevolution of Measures and Countermeasures 446
25.3 Cybersecurity Space Race and Sputnik. 447
25.3.1 Gaining the Ultimate Low Ground 447
25.3.2 Stuxnet and the Cyberattack Genie 447
25.3.3 Georgia and Hybrid Warfare 448
25.3.4 Estonia and Live-Fire Experiments 448
25.3.5 Responsibility for Defending Critical Information Infrastructure 448
25.4 Cybersecurity Science and Experimentation. 450
25.4.1 Hypothesis Generation 452
25.4.2 Experimental Design 453
25.4.3 Experiment Execution. 453
25.5 The Great Unknown: Research Directions. 454
25.5.1 Hard Research Problems 454
25.5.2 Are Cybersecurity Problems Too Hard? 456
25.5.3 Research Impact and the Heilmeier Catechism 456
25.5.4 Research Results Dependability 459
25.5.5 Research Culture: A Warning 459
25.6 Cybersecurity and Artificial Intelligence 460
Conclusion 462
Questions 463

Part VI Appendix and Glossary

Appendix Resources **467**
Glossary. **483**

Index **523**

This page intentionally left blank

Table of Figures

1-1 History of cybersecurity technologies and attacks 5
1-2 Anatomy of a top-down attack design 6
1-3 Physiology of a bottom-up attack execution example 11
1-4 Attack description: Code Red Worm 11
1-5 Determining the nature of a network-based cyberattack 12
1-6 Defense description: Firewalls 14
1-7 The cybersecurity solution landscape and interrelationships. 19
2-1 The cybersecurity-functionality-performance trade-off 27
3-1 Attack description: secrecy attack 41
4-1 Attack description: distributed denial of service. 53
4-2 Levels of data criticality 58
5-1 Attack description: buffer overflow 67
5-2 U.S. classification hierarchy in which a person cleared at a given level can see data at that level and lower. 69
5-3 Attack description: social engineering and phishing 70
5-4 A model of a system including users, adversaries, and dynamic measures/countermeasures. Users (defense operators) apply measures/countermeasures to keep the system in a secure state, while the adversary applies measures/countermeasures to achieve their attack goals. 71
5-5 Attack description: supply chain attack 72
5-6 Systems engineering "V" showing steps of design and mapping in which faults can be introduced 72
5-7 Issuing cybersecurity commands involves a complex and hidden sequence of actions that are subject to attack, error, and delay at each step. 74
5-8 The processing path of data packet showing delay, error, and attack opportunity to consider. 75
5-9 A defender's model of a real system can be thought of as a projection of the complex real system onto a simpler abstract model system.. 76
5-10 Cybersecurity-relevant security state is complex and dynamic. The adversary and the defender both have models approximating the state that are inaccurate in some ways and useful. These models derive decision making. 78

5-11 Chain of dependability threats [ALVI90] 81
5-12 Programming tools used in the creation of executable programs are all subject to attack. 83
6-1 Attack description: ransomware 93
6-2 Security controls are like slats in a fence; attacks from outside a system can go around the fence, through the lowest slat, or underneath the fence. 97
6-3 Degree to which security controls depend on a variety of different underlying mechanisms to work correctly 98
6-4 Cross-site scripting attack description 103
6-5 Attack description: cyber-physical systems 106
6-6 An example process of a vulnerability assessment team 109
7-1 The OR and AND symbols borrowed from digital logic gates. 116
7-2 Simple example of a goal-directed tree using the "Three Little Pigs" fairy tale story 117
7-3 The simple attack tree example with the alternative of using dynamite added to the mix, making the tree deeper and more complex. 118
7-4 Linear five-whys style failure analysis on a fatal airplane crash. 121
7-5 A more complex fishbone-style five-whys analysis considering multiple systems 122
7-6 Abstract view of attacker goal space, where proximity means similarity 122
7-7 Strategic attacker goals placed into equivalence classes 123
7-8 Example of using a process-sequence pattern to refine a goal from one level to the next 124
7-9 Example showing a device type enumeration analysis pattern for refining an attack goal 124
8-1 Abstract representation of the attack space where dots represent attack classes and size represents attack likelihood. . . 134
8-2 Illustration of the concept of defense in breadth with the regions showing coverage of a subset of the attack space that each of several security controls address. 135
8-3 Illustration of defense-in-depth where each region represents a security control's coverage and overlaps show multiple coverage and therefore depth 136
8-4 Simple security—users with a given clearance can read data classified at their clearance level or below. 137
8-5 Layering of traditional operating system to create differing trust requirements 138
8-6 Depiction of rings of trust and privilege in hardware modes supporting software of varying degrees of trustworthiness. 140

8-7 Generic data processing pipeline that is difficult for multilevel integrity policy to handle 141
8-8 Generic data flow pipeline with a corresponding access control matrix in which programs have been assigned domains, and data have been assigned types. 142
8-9 Type enforcement example of a print labeler and spooler pipeline 143
9-1 Computer system layers with hardware at the foundation of trust. 157
9-2 Processing sequence diagram for supervisor/kernel operation with user applications 159
9-3 Memory mapping to protect memory from accidental or intentional manipulation. 160
9-4 Application 2 creates a memory sharing capability and passes it to application 1 through the kernel. The capability generated by application 2 for its virtual page 3 enables application 1 to request access and gain access via physical page 6.. 161
9-5 Internally, a computer is really a system of active computer elements connected by a master bus. 163
10-1 Basics of the cryptographic encryption and decryption process 169
10-2 Defense description: Advanced Encryption Standard (AES) 170
10-3 Example showing how one might translate letters into binary to create a key (don’t do this!) 171
10-4 Demonstration of how nonrandom human attempts at randomness are. 172
10-5 Cryptographic key generation and the three steps of key distribution, with compromise possibilities at each step. . . . 174
10-6 Public-key cryptography process flow, also known as asymmetric-key cryptography because the decryption key is different from the encryption key 176
10-7 Combining traditional cryptography for fast encryption and public-key cryptography for key distribution offers the best of both worlds. 179
10-8 Example of error detection and error correction using complete redundancy 180
10-9 Attack description: man-in-the-middle attack 181
11-1 Authentication chain concept in which a user action goes through four non-person entities acting as proxies. 190
11-2 The six phases of the authentication life cycle shown in three groups: registration (which sets up identity), authentication (which proves identity during operations), and management (which updates or deletes identities). 191

11-3 The three types of unique identifying schemas or authentication factors and how they combine to create multifactor authentication (human-to-machine) 193
11-4 Defense panel: public-key certificate and identity management 195
12-1 Example of discretionary access control for authorization using access control lists, shown on the right, where the access rights for each subject to that object are explicitly listed. "Others" means all subjects other than the owner. 202
12-2 Sensitivity labels in a strict hierarchy (on left) versus a simple security lattice with compartments (on right) 204
12-3 A Trojan horse program unwittingly installed at a high level by a high-level user (Secret) attempting to establish covert communication with a receiving program at the lower level (Unclassified) 205
12-4 Formation of user attributes based on mission and function associations 208
12-5 Example of the labeling of resource attributes (Personally Identifiable Information, Protected Health Information, and Human Resource Only) to the resources (Objects 1 through 8). 209
12-6 Attribution creation and assignment sequence diagram showing the process to create a new attribute and assign it to a user in preparation for making access control decisions based on that attribute. 211
12-7 Attribute collection and aggregation of sources (left), validation and refreshing of attributes (center), and the publication and distribution process to consumers (right) 212
12-8 Valid attribute *definition* space (left) versus *assigned* attribute space that uses defined attributes (right). 213
12-9 Policy authoring, collection, and aggregation (left); validation and refreshing (middle); and publication process to policy consumers (right). 217
12-10 Steps of policy decision and enforcement processing within a protecting subsystem 220
13-1 Synergy between prevention and detection measures in terms of covering the attack space, represented by the attack arrows traversing from right to left. Aligned holes represent system vulnerabilities. 227
13-2 Intrusion detection system layers of abstraction. The layers are ordered into three different groupings: features at the foundation, events built on features in the middle, and attacks at the top. 228

13-3 Attacks map to and manifest in the feature space. One attack can manifest in many features (called one-to-many); many attacks can differently manifest in the same feature (called many-to-one). The thickness of the line represents how strongly the attack manifests in that feature. 230
14-1 Signature-based epidemiological model of discovery and widespread inoculation of attack signatures 240
14-2 Feature selection performance analysis showing features 11 and 14 selected because many attacks manifest in those features (signal analysis) and their implementation is plausible and cost-effective. 246
14-3 Combining feature sets determined by the attack space 247
14-4 Receiver Operating Characteristic (ROC) curves indicate the notional performance of a binary classifier. The intersecting point at the dotted lines indicates a sample point with an 80 percent true positive detection rate and a 40 percent false positive rate. 250
15-1 Attacking flow path representation from gaining a toehold through breaching internal firewalls 259
15-2 Abstraction of successive network detection layers giving a depth of detection along the attacker's entire attack path through successive subnetworks of increasing trust and protection 260
15-3 Detection in breadth by a sensor or set of sensors, covering portions of the attack space (shaded rectangles) and leaving others not covered (white area) 261
15-4 Defense in depth and breadth with respect to attack space is challenging to the adversary. 262
15-5 Attacker-defender dynamic interaction and goals with respect to attack signal detection 267
15-6 Virtualization of computational resources (hardware) used to separate user activity types and thus lower the attack noise floor. 268
15-7 Virtualization of networks to separate network traffic to reduce attack noise floor. 269
16-1 Attackers hopscotch through multiple systems in multiple countries to make attribution difficult. 275
16-2 Notional graph of exponentially increasing attack damage as a function of attack time, with early detection being able to avoid the bulk of the damage 280
17-1 Role of risk measurement in iterative design process 294
17-2 Risk assessment analysis tasks and flowchart shown in three phases (connects to risk mitigation process in Figure 18-1) 295

17-3 Example availability attack tree on a generic online banking service 302

17-4 Three cuts for the attack tree for strategic attack goal #5, each of which achieves the goal, in the chapter's running generic banking system example 307

18-1 Design feedback portion of risk assessment process; connects from risk assessment in Figure 17-2 from numbered arrows 315

18-2 Knapsack optimization example, maximizing risk reduction value with a $100K budget constraint 323

18-3 Notional optimization chart of risk reduction possible at various budget levels, also showing incremental return on investment knees in the curve 325

19-1 Relative cost multipliers of fixing defects in later life-cycle stages compared to design, shown as 1x 333

19-2 Principle of modularity with clear interfaces on the left, internal functions implementing the interface, and protected private data internal to the module, inaccessible by external modules 341

19-3 Principle of design layering to control complexity and to build up layers of abstraction 342

19-4 Example of recursion for factorial algorithm, solving a sequence of easier subproblems to get the final solution 346

20-1 Relationship among formal and informal specifications, requiring parallel and mapped specifications 353

20-2 Two-way requirements traceability map to design showing that design elements must meet requirements and that all requirements must be supported by design elements.. 354

20-3 Interaction between policy specification, policy decision making, and policy enforcement 356

20-4 Parallels in the analogy between policy processing and programming language processing. 358

20-5 Synergy between prevention, detection, and intrusion tolerance layers to create an effective complementary defense mesh 364

21-1 The cybersecurity subsystem is a subset of the larger mission system. Formal methods are applied only to the cybersecurity subsystem because of the cost and complexity of the process. 371

21-2 Abstract example of subsystem trust dependency cascade from subsystem A-3 to seven other subsystems. 377

22-1 The synergistic interplay between situation understanding and command and control guides cybersecurity design and operations. 383

22-2 The four-phase Observe-Orient-Decide-Act (OODA) decision loop that guides action. 384
22-3 Phased situation-based action guided on unfolding attack-path understanding and by timeliness of action 387
22-4 Attack tree updated from Figure 17-3 with probabilities of success where attackers have already achieved two leaf goals (marked with a check) 390
23-1 The relationship between human-speed command and control and machine-speed autonomous control 404
23-2 Cybersecurity strategy involves complex game theory, with the white-hatted defender playing multiple games against multiple dark-hatted adversaries, on game boards that are partially hidden and constantly evolving, while the rules evolve. 410
23-3 Example courses of action of increasing aggressiveness 411
23-4 Control theory and the interactions of elements requiring cybersecurity actions 417
23-5 An aviation analogy of overcontrol creating an out-of-control undamped oscillation leading to a crash 421
24-1 Critical infrastructures showing the four hypercritical infrastructures at the core, supporting all others 431
24-2 Critical infrastructure showing the complex web of interdependencies in the physical world 431
25-1 The responsibilities of the public and private sector in defending against cyberattack 450
25-2 Flow diagram exemplifying cybersecurity experimentation process, from hypothesis to conclusions 451
25-3 The Defense Advanced Research Projects Agency's Information Assurance program's space of cybersecurity research 455

This page intentionally left blank

Table of Tables

1-1 Some Historically Important Cyberattacks 8
1-2 Basic Operational Questions Regarding a Security Breach 10
1-3 Asymmetric Nature of Cyberspace Compared to Physical Space 16
2-1 Factors that Trade Off with Security 28
3-1 Types of Secrecy 40
3-2 Problems with Secrecy 44
3-3 Secrecy Minimization Worksheet Example 46
4-1 Risk is calculated by probability of an event times the consequences; shaded cells show potentially strategic risks; and values are given in exponential format. A probability of 10^{-6} means 1 chance in 10 with 6 zeros after it, or 1 in a million. 53
4-2 Criticality Types of Software and Data Based on the Three Pillars of Cybersecurity 57
4-3 Examples of Criticality Types for Six Categories 57
4-4 Sample Mission Elements for Three Sample Organizations 58
4-5 Example Template for Cybersecurity Harm Statements 59
6-1 Examples of Representative Adversary Classes 95
6-2 Summary of Roles of Red, Blue, White, and Purple Teams in Exercises 111
12-1 Example of an access control matrix. The upper left-hand cell means that subject 1 has read, write, and own access to object 1. 201
12-2 Types of access control based on two independent properties: (1) who decides access and (2) at what granularity are those decisions. The result is four separate policy classes. 207
14-1 Comparison of Signature-Based Versus Anomaly Detection Schemes with Respect to the Layered Detection Hierarchy 244
14-2 Summary of Signature-Based Versus Anomaly Detection Schemes with Respect to Strengths and Weaknesses 244
15-1 Detection in Depth and Breadth in Two Dimensions: Network Expanse and Attack Space 258
15-2 Questions and Rationale Used to Run Alerts to Ground when Investigating Suspicious Activity 265
15-3 Summary Contrasting Normal Communications with Attack-Defender Interactions 266