



Contents

Introduction	xiii
Acknowledgments	xvii
About the Authors	xviii
Chapter 1 The Journey Toward Information Security: An Overview	1
Five Essentials for Making the Journey	2
Roadmap for Information System Security	2
Security Objectives	4
Security Services	6
Security Mechanisms	6
Strategy for Achieving Information Security	10
Navigational Tools for Achieving Information Security	13
Computer Security	14
Data/Information Security	14
Communications/Network Security	14
Administrative/Management Security	15
Personnel Security	15
Operations Security	16
Resources for Achieving Information Security	16
People	16
Technology	17
Processes	17
Time	18
How the System Security Certified Practitioner Participates	18
Conclusion	18

Chapter 2	Domain 1: Access Controls	19
	Our Goals	19
	Domain Definition	20
	Why Control Access?	21
	Protection of Assets and Resources	22
	Assurance of Accountability	23
	Prevention of Unauthorized Access	23
	DoS/DDoS Attacks	24
	Spamming	26
	Brute Force Attacks	27
	Masquerade Attacks	27
	Man-in-the-Middle Attacks	28
	Self-Inflicted DoS	28
	Types of Access Controls	29
	Physical Controls	29
	Logical Controls	30
	Access Control Mechanisms	31
	Token-Based Access Controls	32
	Characteristics-Based Access Controls	32
	System Level Access Controls	33
	Account-Level Access Controls	35
	Privileged Accounts	35
	Individual and Group I&A Controls	35
	Password Management and Policy	36
	Role-Based Access Controls	39
	Session-Level Access Controls	39
	Data-Level Access Controls	40
	Handling and Storing Output and Media	41
	Sample Questions	45
Chapter 3	Domain 2: Administration	51
	Our Goals	51
	What Is Security Administration?	52
	Security Administration Concepts and Principles	53
	Security Equation	54
	System Life Cycle	54
	Security Development Life Cycle	56
	Data/Information Storage	59
	Primary Storage	60
	Secondary Storage	60
	Real (Physical) Memory	60
	Volatile Memory	60
	Virtual Memory	61
	Storage Access Methods	62
	Policies and Practices	63
	Employment Policies	63
	Security Policies	65

Standards	67
Guidelines	68
Procedures	68
Information Classification	69
Security Modes of Operation	72
Dedicated Mode	72
System High Mode	72
Compartmented Mode	73
Partitioned Security Mode	73
Multilevel Mode	73
Trusted Computing Base (TCB)	73
Security Kernel	73
Reference Monitor	74
Process Isolation	74
Traffic Analysis	74
OSI 7 Layer Model	74
Configuration Management	76
Building Your Roadmap	77
Starting with Policy	78
Defining Specific Requirements	80
Implementing Security Mechanisms	80
Common Technology-Based Security Mechanisms	81
Administering Security in an Operational System or Enterprise	88
Access to the Firewall Platform	88
Firewall Platform Operating System Builds	89
Logging Functionality	90
Firewall Selection	91
Firewall Environment	91
Firewall Policy	93
Recommendations for Firewall Administration	98
Placement of VPN Servers	98
Security Awareness Training	99
Users	99
Management	100
Executives	101
Sample Questions	102
Chapter 4 Domain 3: Auditing and Monitoring	109
Our Goals	109
Domain Definition	110
Auditing	111
Audit Characteristics	111
Components to Audit	112
External/Internal Network Boundary Auditing	112
Internal/Subnet Boundary Auditing	118
Server Audit	119
User Workstations	120

Data to Collect During an Audit	126
Making Sense of Data	127
Data/Information Management	127
Conducting a Security Review (Audit)	128
Planning Stage	128
The Policies	129
Reporting Requirements	130
Implementation Stage	132
Monitoring	132
Monitoring Characteristics	133
Components to Monitor	133
Network Monitoring	133
Security Monitoring	133
Keystroke Monitoring	134
Intrusion Detection Systems (IDSs)	134
Types of IDSs	134
Data to Collect during Monitoring	135
Computer Forensics	140
Sample Questions	144
Chapter 5 Domain 4: Risk, Response, and Recovery	151
Goal of Chapter	151
Domain Definition	151
Risk	152
What Is Risk?	152
Major System Elements at Risk	153
Assets	153
Threats	155
Vulnerability	155
Controls	156
Safeguards	156
Countermeasures	156
Exposure	157
Risk Analysis	157
Risk Assessment	157
Threats versus Vulnerabilities	158
Analyzing Risk	159
Quantitative Risk Analysis	159
Qualitative Risk Analysis	161
Automated Risk Assessment	161
What to Do with Risk?	162
Why Assess Risk?	163
What Is Risk Management?	163
An Effective Risk-Assessment Methodology	163
Step 1: System Characterization	164
Step 2: Threat Identification	168

Step 3: Vulnerability Identification	173
Step 4: Control Analysis	178
Step 5: Likelihood Determination	180
Step 6: Impact Analysis	180
Step 7: Risk Determination	183
Step 8: Control Recommendations	185
Step 9: Results Documentation	186
Response	188
What Is a Response?	188
Incident Response Steps	191
How Do You Plan?	191
Recovery	198
What Is Contingency Planning?	198
Emergency Response	199
Restoration and Recovery	203
CP Testing	204
Sample Questions	208
Chapter 6 Domain 5: Cryptography	215
Our Goals	216
Domain Definition	216
Definitions of Cryptographic Terms	217
The History of Cryptology: An Overview	221
Caesar Shift Cipher (Mono-Alphabetic Substitution)	222
Vigenère Square (Polyalphabetic Substitution)	225
Vernam Cipher	226
Rotor Machines	229
Code Talkers	232
DES	232
Public Key Cryptography	232
Clipper Chip	232
Security and Cryptography	233
Confidentiality	234
Integrity	234
Encryption Techniques	235
How Encryption Is Used	236
How the Plaintext Is Processed	237
Number of Keys	239
Common Cryptographic Systems	242
Data Encryption Standard (DES)	243
Triple DES	243
RSA	244
Elliptic Curve Cryptography (ECC)	245
Advanced Encryption Standard (AES)	245

IDEA	245
Kerberos	245
Cryptography in Networks	246
Internet Protocol Security (IPSec)	246
Authentication Header (AH)	246
Encapsulating Security Payload (ESP)	246
Secure Socket Layer (SSL)	246
Secure HyperText Transport Protocol (S-HTTP)	246
Cryptography for Email	247
Secure Multipurpose Internet Mail Extensions (s/MIME)	247
Pretty Good Privacy (PGP)	247
Privacy Enhanced Mail (PEM)	247
Cryptography for E-Commerce	247
Secure Electronic Transaction (SET)	248
Transaction Layer Security (TLS)	248
What Is a Public Key Infrastructure (PKI)?	248
Steganography	250
Watermarks	251
Cryptanalysis	251
Known Plain-Text Approach	251
Ciphertext-Only Approach	252
Chosen Plain-Text Approach	252
Cryptography and the Federal Government	253
Sample Questions	254
Chapter 7 Domain 6: Data Communications	261
Our Goals	261
Domain Definition	262
Data Communication Fundamentals	262
Physical Aspects of Data Communications	263
Analog Signals	263
Digital Signals	264
Conducted Media	265
Copper Wire	265
Coaxial Cable	266
Fiber Optics	266
Radiated Media	266
Radio Waves	267
Microwave	267
Satellites	267
Infrared	269
Transmission Approaches	270
Bandwidth	270
Broadband versus Narrowband	270
Spread Spectrum	271
Networks	271
Local Area Networks (LANs)	272
Wide Area Networks (WANs)	272

Metropolitan Area Networks (MANs)	272
Intranets	273
The Internet	273
Extranets	274
Virtual Private Networks (VPNs)	275
VPN Security	275
VPN Modes of Operation	276
Peer Authentication	276
Public Key Certificate	276
One-Time Password	277
Password	277
Policy Configuration	277
VPN Operation	278
Physical Topologies	279
Star Topology	279
Bus Topology	280
Ring Topology	280
Logical Topologies	281
Bus	281
Ring	282
Standards	282
IEEE Standards	282
802.X Standards	282
Ethernet	282
Fast Ethernet	283
Gigabit Ethernet	283
International Organization for Standardization (ISO)	283
American National Standards Institute (ANSI)	284
International Telecommunication Union (ITU)	284
Protocols	284
The X Protocols	284
X.400	284
X.500	285
X.509	285
X.25	285
Transmission Control Protocol/Internet Protocol (TCP/IP)	285
User Datagram Protocol (UDP)	285
NetBEUI	285
Wireless Access Protocol (WAP)	286
Remote Access Protocols	286
Remote Access Services (RAS)	286
Remote Authentication Dial-In User Service (RADIUS)	286
Internet Protocol Security (IPSec)	286
Secure Sockets Layer (SSL) or Transport Layer Security (TLS)	287
Layer 2 Tunneling Protocol (L2TP)	287
Point-to-Point Tunneling Protocol (PPTP)	288

Models for Network Communication	288
OSI Seven-Layer Model	288
Physical Layer	288
Data Link Layer	289
Network Layer	289
Transport Layer	289
Session Layer	290
Presentation Layer	290
Application Layer	290
Security Services and Mechanisms	290
TCP/IP Network Model	291
Network Testing Techniques	291
Reasons for Testing a System	291
Security Testing and the System Development Life Cycle	292
Documentation	294
Security Management Staff	294
Senior IT Management/Chief Information Officer (CIO)	294
Information Systems Security Program Managers	295
Information Systems Security Officers	295
System and Network Administrators	295
Managers and Owners	296
Types of Security Testing	296
Network Mapping (Discovery)	297
Vulnerability Scanning	299
Penetration Testing	301
Security Testing and Evaluation	307
Password Cracking	308
Reviewing Logs	310
Checking File Integrity	311
Using Virus Detectors	312
War Dialing	313
Summary Comparisons of Network Testing Techniques	314
Prioritizing Security Testing	317
Minimum versus Comprehensive Testing	317
Prioritization Process	321
Sample Questions	324
Chapter 8 Domain 7: Malicious Code	331
Our Goals	333
Domain Definition (Subject Overview)	333
What Is Malicious Code?	333
Types and Characteristics of Malicious Code	336
Viruses	336
Virus Lifecycle	337
Macro Viruses	338
Macro Viruses	339

Polymorphic Viruses	339
Stealth Viruses	340
Multipartite Virus	340
Attack Scripts	340
Viruses and Email	340
Virus Creation	341
Virus Hoaxes	341
Worms	342
Trojan Horses	342
Trojan Horses	343
Logic Bombs	343
Malicious Code Protection	344
Malicious Code Detection System Requirements	345
Configuration Management Requirements	346
Potential Attack Mechanisms	347
Network Attacks	347
Trapdoors	347
Insider Attacks	348
Connection/Password Sniffing	348
Mobile Code	348
Potential Countermeasures	351
Malicious Code Scanning Products	351
Electronic Security	351
Trapdoor Access/Distribution	352
Network Security	352
Connection and Password Sniffing Countermeasures	352
Physical Security	353
An Overall Approach to Counter Malicious Code	353
Detection Mechanism	353
Administrative Countermeasures	356
System Backup	356
Workstation Strategy	356
Network Strategy	357
Types of Malicious Code Detection Products	357
Updates	357
Pre-Infection Prevention Products	358
Infection Prevention Products	358
Short-Term Infection Detection Products	359
Long-Term Infection Detection Products	359
Interoperability Concerns	360
Products Offering Protection at the Workstation	361
Products Offering Protection at the Network Gateway	362
Criteria for Selecting Protection Products	362
Example Cases	363
Case 1: Macro Virus Attack	363
Problem	363
Solution	363

Case 2: Polymorphic Virus Attack	365
Problem	365
Solution	366
Case 3: Trojan Horse Attack	368
Problem	368
Solution	368
Sample Questions	370
Appendix A Glossary	377
Appendix B Testing Tools	387
File Integrity Checkers	387
Network Sniffers	388
Password Crackers	389
Privilege Escalation and Back Door Tools	389
Scanning and Enumeration Tools	390
Vulnerability Scanning Tools	391
War Dialing Tools	392
Port Scanning: Nmap	392
L0pht Crack	398
LANguard File Integrity Checker	399
Using Tripwire	400
Snort	406
Appendix C References for Further Study	413
Books and Other Printed Materials	413
Web Sites	415
Web Sites of Interest to Security Administrators	416
Appendix D Answers to Sample Questions	417
Chapter 2—Domain 1: Access Controls	417
Chapter 3—Domain 2: Administration	427
Chapter 4—Auditing and Monitoring	436
Chapter 5—Domain 4: Risk, Response, and Recovery	446
Chapter 6—Domain 5: Cryptography	458
Chapter 7—Domain 6: Data Communications	467
Chapter 8—Domain 7: Malicious Code	477
What's on the CD-ROM	489
Index	493