Preface to the Second Edition xxv
Foreword by Bruce Schneier xxvii
Preface xxix
Acknowledgments xxxv

Part I

Chapter 1  What Is Security Engineering? 3
Introduction 3
A Framework 4
Example 1–A Bank 6
Example 2–A Military Base 7
Example 3–A Hospital 9
Example 4–The Home 10
Definitions 11
Summary 15

Chapter 2  Usability and Psychology 17
Introduction 17
Attacks Based on Psychology 18
Pretexting 19
Phishing 21
Insights from Psychology Research 22
What the Brain Does Worse Than the Computer 23
Perceptual Bias and Behavioural Economics 24
Different Aspects of Mental Processing 26
Differences Between People 27
Social Psychology 28
What the Brain Does Better Than Computer 30
# Contents

- Chosen Protocol Attacks 80
- Managing Encryption Keys 82
  - Basic Key Management 83
  - The Needham-Schroeder Protocol 84
  - Kerberos 85
  - Practical Key Management 86
- Getting Formal 87
  - A Typical Smartcard Banking Protocol 87
  - The BAN Logic 88
  - Verifying the Payment Protocol 89
  - Limitations of Formal Verification 90
- Summary 91
- Research Problems 92
- Further Reading 92

## Chapter 4 Access Control 93

- Introduction 93
- Operating System Access Controls 96
  - Groups and Roles 98
  - Access Control Lists 99
  - Unix Operating System Security 100
  - Apple’s OS/X 101
  - Windows — Basic Architecture 102
  - Capabilities 103
  - Windows — Added Features 104
  - Middleware 107
    - Database Access Controls 107
    - General Middleware Issues 108
    - ORBs and Policy Languages 109
  - Sandboxing and Proof-Carrying Code 110
  - Virtualization 111
  - Trusted Computing 111
- Hardware Protection 113
  - Intel Processors, and ‘Trusted Computing’ 114
  - ARM Processors 116
  - Security Processors 116
- What Goes Wrong 117
  - Smashing the Stack 118
  - Other Technical Attacks 119
  - User Interface Failures 121
  - Why So Many Things Go Wrong 122
  - Remedies 124
  - Environmental Creep 125
- Summary 126
- Research Problems 127
- Further Reading 127
Chapter 5 Cryptography

Introduction
Historical Background
An Early Stream Cipher — The Vigenère
The One-Time Pad
An Early Block Cipher — Playfair
One-Way Functions
Asymmetric Primitives
The Random Oracle Model
Random Functions — Hash Functions
Properties
The Birthday Theorem
Random Generators — Stream Ciphers
Random Permutations — Block Ciphers
Public Key Encryption and Trapdoor One-Way Permutations
Digital Signatures
Symmetric Crypto Primitives
SP-Networks
Block Size
Number of Rounds
Choice of S-Boxes
Linear Cryptanalysis
Differential Cryptanalysis
Serpent
The Advanced Encryption Standard (AES)
Feistel Ciphers
The Luby-Rackoff Result
DES
Modes of Operation
Electronic Code Book
Cipher Block Chaining
Output Feedback
Counter Encryption
Cipher Feedback
Message Authentication Code
Composite Modes of Operation
Hash Functions
Extra Requirements on the Underlying Cipher
Common Hash Functions and Applications
Asymmetric Crypto Primitives
Cryptography Based on Factoring
Cryptography Based on Discrete Logarithms
Public Key Encryption — Diffie Hellman and ElGamal
Key Establishment
Digital Signature
Special Purpose Primitives

<table>
<thead>
<tr>
<th>Chapter 5 Cryptography</th>
<th>129</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>129</td>
</tr>
<tr>
<td>Historical Background</td>
<td>130</td>
</tr>
<tr>
<td>An Early Stream Cipher — The Vigenère</td>
<td>131</td>
</tr>
<tr>
<td>The One-Time Pad</td>
<td>132</td>
</tr>
<tr>
<td>An Early Block Cipher — Playfair</td>
<td>134</td>
</tr>
<tr>
<td>One-Way Functions</td>
<td>136</td>
</tr>
<tr>
<td>Asymmetric Primitives</td>
<td>138</td>
</tr>
<tr>
<td>The Random Oracle Model</td>
<td>138</td>
</tr>
<tr>
<td>Random Functions — Hash Functions</td>
<td>140</td>
</tr>
<tr>
<td>Properties</td>
<td>141</td>
</tr>
<tr>
<td>The Birthday Theorem</td>
<td>142</td>
</tr>
<tr>
<td>Random Generators — Stream Ciphers</td>
<td>143</td>
</tr>
<tr>
<td>Random Permutations — Block Ciphers</td>
<td>144</td>
</tr>
<tr>
<td>Public Key Encryption and Trapdoor One-Way Permutations</td>
<td>146</td>
</tr>
<tr>
<td>Digital Signatures</td>
<td>147</td>
</tr>
<tr>
<td>Symmetric Crypto Primitives</td>
<td>149</td>
</tr>
<tr>
<td>SP-Networks</td>
<td>149</td>
</tr>
<tr>
<td>Block Size</td>
<td>150</td>
</tr>
<tr>
<td>Number of Rounds</td>
<td>150</td>
</tr>
<tr>
<td>Choice of S-Boxes</td>
<td>151</td>
</tr>
<tr>
<td>Linear Cryptanalysis</td>
<td>151</td>
</tr>
<tr>
<td>Differential Cryptanalysis</td>
<td>152</td>
</tr>
<tr>
<td>Serpent</td>
<td>153</td>
</tr>
<tr>
<td>The Advanced Encryption Standard (AES)</td>
<td>153</td>
</tr>
<tr>
<td>Feistel Ciphers</td>
<td>155</td>
</tr>
<tr>
<td>The Luby-Rackoff Result</td>
<td>157</td>
</tr>
<tr>
<td>DES</td>
<td>157</td>
</tr>
<tr>
<td>Modes of Operation</td>
<td>160</td>
</tr>
<tr>
<td>Electronic Code Book</td>
<td>160</td>
</tr>
<tr>
<td>Cipher Block Chaining</td>
<td>161</td>
</tr>
<tr>
<td>Output Feedback</td>
<td>161</td>
</tr>
<tr>
<td>Counter Encryption</td>
<td>162</td>
</tr>
<tr>
<td>Cipher Feedback</td>
<td>163</td>
</tr>
<tr>
<td>Message Authentication Code</td>
<td>163</td>
</tr>
<tr>
<td>Composite Modes of Operation</td>
<td>164</td>
</tr>
<tr>
<td>Hash Functions</td>
<td>165</td>
</tr>
<tr>
<td>Extra Requirements on the Underlying Cipher</td>
<td>166</td>
</tr>
<tr>
<td>Common Hash Functions and Applications</td>
<td>167</td>
</tr>
<tr>
<td>Asymmetric Crypto Primitives</td>
<td>170</td>
</tr>
<tr>
<td>Cryptography Based on Factoring</td>
<td>170</td>
</tr>
<tr>
<td>Cryptography Based on Discrete Logarithms</td>
<td>173</td>
</tr>
<tr>
<td>Public Key Encryption — Diffie Hellman and ElGamal</td>
<td>174</td>
</tr>
<tr>
<td>Key Establishment</td>
<td>175</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>176</td>
</tr>
<tr>
<td>Special Purpose Primitives</td>
<td>178</td>
</tr>
</tbody>
</table>
Chapter 6  Distributed Systems  185
Introduction 185
Concurrency 186
Using Old Data Versus Paying to Propagate State 186
Locking to Prevent Inconsistent Updates 188
The Order of Updates 188
Deadlock 189
Non-Convergent State 190
Secure Time 191
Fault Tolerance and Failure Recovery 192
Failure Models 193
Byzantine Failure 193
Interaction with Fault Tolerance 194
What Is Resilience For? 195
At What Level Is the Redundancy? 196
Service-Denial Attacks 198
Naming 200
The Distributed Systems View of Naming 200
What Else Goes Wrong 204
Naming and Identity 204
Cultural Assumptions 206
Semantic Content of Names 207
Uniqueness of Names 207
Stability of Names and Addresses 208
Adding Social Context to Naming 209
Restrictions on the Use of Names 210
Types of Name 211
Summary 211
Research Problems 212
Further Reading 213

Chapter 7  Economics  215
Introduction 215
Classical Economics 216
Monopoly 217
Public Goods 219
Information Economics 220
The Price of Information 220
The Value of Lock-In 221
Asymmetric Information 223
## xiv Contents

- Game Theory 223
  - The Prisoners’ Dilemma 225
  - Evolutionary Games 226
- The Economics of Security and Dependability 228
  - Weakest Link, or Sum of Efforts? 229
  - Managing the Patching Cycle 229
  - Why Is Windows So Insecure? 230
  - Economics of Privacy 232
  - Economics of DRM 233
- Summary 234
- Research Problems 235
- Further Reading 235

## Part II

### Chapter 8 Multilevel Security 239

- Introduction 239
- What Is a Security Policy Model? 240
- The Bell-LaPadula Security Policy Model 242
  - Classifications and Clearances 243
  - Information Flow Control 245
  - The Standard Criticisms of Bell-LaPadula 246
  - Alternative Formulations 248
  - The Biba Model and Vista 250
- Historical Examples of MLS Systems 252
  - SCOMP 252
  - Blacker 253
  - MLS Unix and Compartmented Mode Workstations 253
  - The NRL Pump 254
  - Logistics Systems 255
  - Sybard Suite 256
  - Wiretap Systems 256
- Future MLS Systems 257
  - Vista 257
  - Linux 258
  - Virtualization 260
  - Embedded Systems 261
- What Goes Wrong 261
  - Composability 261
  - The Cascade Problem 262
  - Covert Channels 263
  - The Threat from Viruses 265
  - Polyinstantiation 266
  - Other Practical Problems 267
- Broader Implications of MLS 269
## Chapter 9 Multilateral Security

**Introduction**

- Compartmentation, the Chinese Wall and the BMA Model
- The Chinese Wall
- The BMA Model
- The Threat Model
- The Security Policy
- Pilot Implementations
- Current Privacy Issues

**Inference Control**

- Basic Problems of Inference Control in Medicine
- Other Applications of Inference Control
- The Theory of Inference Control
  - Query Set Size Control
  - Trackers
  - More Sophisticated Query Controls
  - Cell Suppression
  - Maximum Order Control and the Lattice Model
  - Audit Based Control
  - Randomization
  - Limitations of Generic Approaches
  - Active Attacks
  - The Value of Imperfect Protection
- The Residual Problem

---

## Chapter 10 Banking and Bookkeeping

**Introduction**

- The Origins of Bookkeeping
- Double-Entry Bookkeeping
- A Telegraphic History of E-commerce

**How Bank Computer Systems Work**

- The Clark-Wilson Security Policy Model
- Designing Internal Controls
- What Goes Wrong

**Wholesale Payment Systems**

- SWIFT

---

**Further Reading**
xvi Contents

What Goes Wrong 337
Incentives and Injustices 341
Credit Cards 343
Fraud 344
Forgery 345
Automatic Fraud Detection 346
The Economics of Fraud 347
Online Credit Card Fraud — the Hype and the Reality 348
Smartcard-Based Banking 350
EMV 351
Static Data Authentication 352
Dynamic Data Authentication 356
Combined Data Authentication 356
RFID 357
Home Banking and Money Laundering 358
Summary 361
Research Problems 362
Further Reading 363

Chapter 11 Physical Protection 365
Introduction 365
Threats and Barriers 366
Threat Model 367
Deterrence 368
Walls and Barriers 370
Mechanical Locks 372
Electronic Locks 376
Alarms 378
How not to Protect a Painting 379
Sensor Defeats 380
Feature Interactions 382
Attacks on Communications 383
Lessons Learned 386
Summary 387
Research Problems 388
Further Reading 388

Chapter 12 Monitoring and Metering 389
Introduction 389
Prepayment Meters 390
Utility Metering 392
How the System Works 393
What Goes Wrong 395
Taxi Meters, Tachographs and Truck Speed Limiters 397
The Tachograph 398
What Goes Wrong 399
How Most Tachograph Manipulation Is Done 400
## Chapter 15 Biometrics

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>457</td>
</tr>
<tr>
<td>Handwritten Signatures</td>
<td>458</td>
</tr>
<tr>
<td>Face Recognition</td>
<td>461</td>
</tr>
<tr>
<td>Bertillonage</td>
<td>464</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>464</td>
</tr>
<tr>
<td>Verifying Positive or Negative Identity Claims</td>
<td>466</td>
</tr>
<tr>
<td>Crime Scene Forensics</td>
<td>469</td>
</tr>
<tr>
<td>Iris Codes</td>
<td>472</td>
</tr>
<tr>
<td>Voice Recognition</td>
<td>475</td>
</tr>
<tr>
<td>Other Systems</td>
<td>476</td>
</tr>
<tr>
<td>What Goes Wrong</td>
<td>477</td>
</tr>
<tr>
<td>Summary</td>
<td>481</td>
</tr>
<tr>
<td>Research Problems</td>
<td>482</td>
</tr>
<tr>
<td>Further Reading</td>
<td>482</td>
</tr>
</tbody>
</table>

## Chapter 16 Physical Tamper Resistance

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>483</td>
</tr>
<tr>
<td>History</td>
<td>485</td>
</tr>
<tr>
<td>High-End Physically Secure Processors</td>
<td>486</td>
</tr>
<tr>
<td>Evaluation</td>
<td>492</td>
</tr>
<tr>
<td>Medium Security Processors</td>
<td>494</td>
</tr>
<tr>
<td>The iButton</td>
<td>494</td>
</tr>
<tr>
<td>The Dallas 5000 Series</td>
<td>495</td>
</tr>
<tr>
<td>FPGA Security, and the Clipper Chip</td>
<td>496</td>
</tr>
<tr>
<td>Smartcards and Microcontrollers</td>
<td>499</td>
</tr>
<tr>
<td>History</td>
<td>500</td>
</tr>
<tr>
<td>Architecture</td>
<td>501</td>
</tr>
<tr>
<td>Security Evolution</td>
<td>501</td>
</tr>
<tr>
<td>The State of the Art</td>
<td>512</td>
</tr>
<tr>
<td>Defense in Depth</td>
<td>513</td>
</tr>
<tr>
<td>Stop Loss</td>
<td>513</td>
</tr>
<tr>
<td>What Goes Wrong</td>
<td>514</td>
</tr>
<tr>
<td>The Trusted Interface Problem</td>
<td>514</td>
</tr>
<tr>
<td>Conflicts</td>
<td>515</td>
</tr>
<tr>
<td>The Lemons Market, Risk Dumping and Evaluation</td>
<td>516</td>
</tr>
<tr>
<td>Security-By-Obscurity</td>
<td>517</td>
</tr>
<tr>
<td>Interaction with Policy</td>
<td>517</td>
</tr>
<tr>
<td>Function Creep</td>
<td>518</td>
</tr>
<tr>
<td>So What Should One Protect?</td>
<td>518</td>
</tr>
<tr>
<td>Summary</td>
<td>520</td>
</tr>
<tr>
<td>Research Problems</td>
<td>520</td>
</tr>
<tr>
<td>Further Reading</td>
<td>520</td>
</tr>
</tbody>
</table>

## Chapter 17 Emission Security

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>523</td>
</tr>
<tr>
<td>History</td>
<td>524</td>
</tr>
</tbody>
</table>
Chapter 18  **API Attacks**  547
Introduction  547
API Attacks on Security Modules  548
  The XOR-To-Null-Key Attack  549
  The Attack on the 4758  551
  Multiparty Computation, and Differential Protocol Attacks  552
  The EMV Attack  553
API Attacks on Operating Systems  554
Summary  555
Research Problems  557
Further Reading  557

Chapter 19  **Electronic and Information Warfare**  559
Introduction  559
Basics  560
Communications Systems  561
  Signals Intelligence Techniques  563
  Attacks on Communications  565
Protection Techniques  567
  Frequency Hopping  568
  DSSS  569
  Burst Communications  570
  Combining Covertness and Jam Resistance  571
Interaction Between Civil and Military Uses  572
Surveillance and Target Acquisition 574
  Types of Radar 574
  Jamming Techniques 575
  Advanced Radars and Countermeasures 577
  Other Sensors and Multisensor Issues 578
IFF Systems 579
Improvised Explosive Devices 582
Directed Energy Weapons 584
Information Warfare 586
  Definitions 587
  Doctrine 588
  Potentially Useful Lessons from Electronic Warfare 589
  Differences Between E-war and I-war 591
Summary 592
Research Problems 592
Further Reading 593

Chapter 20 Telecom System Security 595

Introduction 595
Phone Phreaking 596
  Attacks on Metering 596
  Attacks on Signaling 599
  Attacks on Switching and Configuration 601
Insecure End Systems 603
Feature Interaction 605
Mobile Phones 606
  Mobile Phone Cloning 607
GSM Security Mechanisms 608
  Third Generation Mobiles — 3gpp 617
Platform Security 619
So Was Mobile Security a Success or a Failure? 621
VOIP 623
Security Economics of Telecoms 624
  Frauds by Phone Companies 625
  Billing Mechanisms 627
Summary 630
Research Problems 631
Further Reading 632

Chapter 21 Network Attack and Defense 633

Introduction 633
Vulnerabilities in Network Protocols 635
  Attacks on Local Networks 636
  Attacks Using Internet Protocols and Mechanisms 638
    SYN Flooding 638
    Smurfing 639
    Distributed Denial of Service Attacks 640
Chapter 23 The Bleeding Edge

Introduction 727
Computer Games
  Types of Cheating 730
  Aimbots and Other Unauthorized Software 732
  Virtual Worlds, Virtual Economies 733
Web Applications
  eBay 734
  Google 736
  Social Networking Sites 739
Privacy Technology
  Anonymous Email — The Dining Cryptographers and Mixes 747
  Anonymous Web Browsing — Tor 749
  Confidential and Anonymous Phone Calls 751
  Email Encryption 753
  Steganography and Forensics Countermeasures 755
  Putting It All Together 757
Elections 759
Summary 764
Research Problems 764
Further Reading 765

Part III

Chapter 24 Terror, Justice and Freedom

Introduction 769
Terrorism 771
  Causes of Political Violence 772
The Psychology of Political Violence 772
The Role of Political Institutions 774
The Role of the Press 775
The Democratic Response 775
Surveillance 776
The History of Government Wiretapping 776
The Growing Controversy about Traffic Analysis 779
Unlawful Surveillance 781
Access to Search Terms and Location Data 782
Data Mining 783
Surveillance via ISPs — Carnivore and its Offspring 784
Communications Intelligence on Foreign Targets 785
Intelligence Strengths and Weaknesses 787
The Crypto Wars 789
The Back Story to Crypto Policy 790
DES and Crypto Research 792
The Clipper Chip 793
Did the Crypto Wars Matter? 794
Export Control 796
Censorship 797
Censorship by Authoritarian Regimes 798
Network Neutrality 800
Peer-to-Peer, Hate Speech and Child Porn 801
Forensics and Rules of Evidence 803
Forensics 803
Admissibility of Evidence 806
Privacy and Data Protection 808
European Data Protection 809
Differences between Europe and the USA 810
Summary 812
Research Problems 813
Further Reading 813

Chapter 25 Managing the Development of Secure Systems 815
Introduction 815
Managing a Security Project 816
A Tale of Three Supermarkets 816
Risk Management 818
Organizational Issues 819
The Complacency Cycle and the Risk Thermostat 820
Interaction with Reliability 821
Solving the Wrong Problem 822
Incompetent and Inexperienced Security Managers 823
Moral Hazard 823
Methodology 824
Top-Down Design 826
Iterative Design 827