## Contents

**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
Passwords 31
- Difficulties with Reliable Password Entry 32
- Difficulties with Remembering the Password 33
- Naive Password Choice 34
- User Abilities and Training 35
  - Design Errors 37
  - Operational Issues 39
- Social-Engineering Attacks 40
- Trusted Path 42
- Phishing Countermeasures 43
  - Password Manglers 43
  - Client Certs or Specialist Apps 44
  - Using the Browser’s Password Database 44
  - Soft Keyboards 45
  - Customer Education 45
  - Microsoft Passport 46
- Phishing Alert Toolbars 47
- Two-Factor Authentication 47
- Trusted Computing 48
- Fortified Password Protocols 49
- Two-Channel Authentication 49
- The Future of Phishing 50

System Issues 52
- Can You Deny Service? 53
- Protecting Oneself or Others? 53
- Attacks on Password Entry
  - Interface Design 54
  - Eavesdropping 55
  - Technical Defeats of Password Retry Counters 55
- Attacks on Password Storage
  - One-Way Encryption 56
  - Password Cracking 57
  - Absolute Limits 57
- CAPTCHAs 59

Summary 60
Research Problems 61
Further Reading 61

Chapter 3 Protocols 63
Introduction 63
Password Eavesdropping Risks 65
Who Goes There? — Simple Authentication 66
  - Challenge and Response 70
  - The MIG-in-the-Middle Attack 73
  - Reflection Attacks 76
- Manipulating the Message 78
- Changing the Environment 79
<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Cryptography</th>
<th>129</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>129</td>
<td></td>
</tr>
<tr>
<td>Historical Background</td>
<td>130</td>
<td></td>
</tr>
<tr>
<td>An Early Stream Cipher — The Vigenère</td>
<td>131</td>
<td></td>
</tr>
<tr>
<td>The One-Time Pad</td>
<td>132</td>
<td></td>
</tr>
<tr>
<td>An Early Block Cipher — Playfair</td>
<td>134</td>
<td></td>
</tr>
<tr>
<td>One-Way Functions</td>
<td>136</td>
<td></td>
</tr>
<tr>
<td>Asymmetric Primitives</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>The Random Oracle Model</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>Random Functions — Hash Functions</td>
<td>140</td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td>141</td>
<td></td>
</tr>
<tr>
<td>The Birthday Theorem</td>
<td>142</td>
<td></td>
</tr>
<tr>
<td>Random Generators — Stream Ciphers</td>
<td>143</td>
<td></td>
</tr>
<tr>
<td>Random Permutations — Block Ciphers</td>
<td>144</td>
<td></td>
</tr>
<tr>
<td>Public Key Encryption and Trapdoor One-Way Permutations</td>
<td>146</td>
<td></td>
</tr>
<tr>
<td>Digital Signatures</td>
<td>147</td>
<td></td>
</tr>
<tr>
<td>Symmetric Crypto Primitives</td>
<td>149</td>
<td></td>
</tr>
<tr>
<td>SP-Networks</td>
<td>149</td>
<td></td>
</tr>
<tr>
<td>Block Size</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>Number of Rounds</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>Choice of S-Boxes</td>
<td>151</td>
<td></td>
</tr>
<tr>
<td>Linear Cryptanalysis</td>
<td>151</td>
<td></td>
</tr>
<tr>
<td>Differential Cryptanalysis</td>
<td>152</td>
<td></td>
</tr>
<tr>
<td>Serpent</td>
<td>153</td>
<td></td>
</tr>
<tr>
<td>The Advanced Encryption Standard (AES)</td>
<td>153</td>
<td></td>
</tr>
<tr>
<td>Feistel Ciphers</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td>The Luby-Rackoff Result</td>
<td>157</td>
<td></td>
</tr>
<tr>
<td>DES</td>
<td>157</td>
<td></td>
</tr>
<tr>
<td>Modes of Operation</td>
<td>160</td>
<td></td>
</tr>
<tr>
<td>Electronic Code Book</td>
<td>160</td>
<td></td>
</tr>
<tr>
<td>Cipher Block Chaining</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Output Feedback</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Counter Encryption</td>
<td>162</td>
<td></td>
</tr>
<tr>
<td>Cipher Feedback</td>
<td>163</td>
<td></td>
</tr>
<tr>
<td>Message Authentication Code</td>
<td>163</td>
<td></td>
</tr>
<tr>
<td>Composite Modes of Operation</td>
<td>164</td>
<td></td>
</tr>
<tr>
<td>Hash Functions</td>
<td>165</td>
<td></td>
</tr>
<tr>
<td>Extra Requirements on the Underlying Cipher</td>
<td>166</td>
<td></td>
</tr>
<tr>
<td>Common Hash Functions and Applications</td>
<td>167</td>
<td></td>
</tr>
<tr>
<td>Asymmetric Crypto Primitives</td>
<td>170</td>
<td></td>
</tr>
<tr>
<td>Cryptography Based on Factoring</td>
<td>170</td>
<td></td>
</tr>
<tr>
<td>Cryptography Based on Discrete Logarithms</td>
<td>173</td>
<td></td>
</tr>
<tr>
<td>Public Key Encryption — Diffie Hellman and ElGamal</td>
<td>174</td>
<td></td>
</tr>
<tr>
<td>Key Establishment</td>
<td>175</td>
<td></td>
</tr>
<tr>
<td>Digital Signature</td>
<td>176</td>
<td></td>
</tr>
<tr>
<td>Special Purpose Primitives</td>
<td>178</td>
<td></td>
</tr>
</tbody>
</table>
xvi 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
Compartmentation and the Lattice 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
Summary
Research Problems
Further Reading
### 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
Tampering with the Supply 401
Tampering with the Instrument 401
High-Tech Attacks 402
The Digital Tachograph Project 403
System Level Problems 404
Other Problems 405
The Resurrecting Duckling 407
Postage Meters 408
Summary 412
Research Problems 413
Further Reading 414

Chapter 13 Nuclear Command and Control 415
Introduction 415
The Evolution of Command and Control 417
The Kennedy Memorandum 418
Authorization, Environment, Intent 419
Unconditionally Secure Authentication 420
Shared Control Schemes 422
Tamper Resistance and PALs 424
Treaty Verification 426
What Goes Wrong 427
Secrecy or Openness? 429
Summary 430
Research Problems 430
Further Reading 430

Chapter 14 Security Printing and Seals 433
Introduction 433
History 434
Security Printing 435
Threat Model 436
Security Printing Techniques 437
Packaging and Seals 443
Substrate Properties 443
The Problems of Glue 444
PIN Mailers 445
Systemic Vulnerabilities 446
Peculiarities of the Threat Model 447
Anti-Gundecking Measures 448
The Effect of Random Failure 449
Materials Control 450
Not Protecting the Right Things 451
The Cost and Nature of Inspection 451
Evaluation Methodology 453
Summary 454
Research Problems 454
Further Reading 455
# Contents

## Chapter 15  Biometrics 457
- Introduction 457
- Handwritten Signatures 458
- Face Recognition 461
- Bertillonage 464
- Fingerprints 464
  - Verifying Positive or Negative Identity Claims 466
  - Crime Scene Forensics 469
- Iris Codes 472
- Voice Recognition 475
- Other Systems 476
- What Goes Wrong 477
- Summary 481
- Research Problems 482
- Further Reading 482

## Chapter 16  Physical Tamper Resistance 483
- Introduction 483
- History 485
- High-End Physically Secure Processors 486
- Evaluation 492
- Medium Security Processors 494
  - The iButton 494
  - The Dallas 5000 Series 495
  - FPGA Security, and the Clipper Chip 496
- Smartcards and Microcontrollers 499
  - History 500
  - Architecture 501
  - Security Evolution 501
  - The State of the Art 512
    - Defense in Depth 513
    - Stop Loss 513
- What Goes Wrong 514
  - The Trusted Interface Problem 514
  - Conflicts 515
  - The Lemons Market, Risk Dumping and Evaluation 516
  - Security-By-Obscurity 517
  - Interaction with Policy 517
  - Function Creep 518
- So What Should One Protect? 518
- Summary 520
- Research Problems 520
- Further Reading 520

## Chapter 17  Emission Security 523
- Introduction 523
- History 524
Contents

- Technical Surveillance and Countermeasures 526
  - Passive Attacks 530
    - Leakage Through Power and Signal Cables 530
      - Red/Black Separation 530
      - Timing Analysis 531
      - Power Analysis 531
    - Leakage Through RF Signals 534
  - Active Attacks 538
    - Tempest Viruses 538
    - Nonstop 539
    - Glitching 540
    - Differential Fault Analysis 540
    - Combination Attacks 540
    - Commercial Exploitation 541
  - Defenses 541
- Optical, Acoustic and Thermal Side Channels 542
- How Serious are Emsec Attacks? 544
  - Governments 544
  - Businesses 545
- Summary 546
- Research Problems 546
- Further Reading 546

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
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