Hardware-Based Computer Security Techniques to Defeat Hackers

From Biometrics to Quantum Cryptography

Roger Dube
CONTENTS

1 THE ELEMENTS OF COMPUTER SECURITY 1

Cryptography, 2
Symmetric Key Cryptography, 2
Asymmetric Key Cryptography, 3

Passwords and Keys, 5
Password/Key Strength, 6
Password/Key Storage and Theft, 8

Passwords and Authentication, 9
Something You Know, 9
Something You Have, 9
Something You Are, 10

Random-Number Generators, 11
Pseudo-Random-Number Generators (PRGs), 12
Hardware-Based Random-Number Generators, 12
Hybrid Hardware/Software Random-Number Generators, 13

Key Generation, 13

Security and the Internet, 14

References, 16
2 CRYPTOGRAPHY APPROACHES AND ATTACKS

Symmetric Key Cryptography, 17
One-Time Pad, 18
DES and Triple DES, 19
International Data-Encryption Algorithm, 24
Rivest Cipher 4, 24
Blowfish, 28
Advanced Encryption Standard, 29
Quantum Cryptography, 31
Hash Algorithms, 36
The Birthday Paradox and Hash Algorithms, 36

References, 39

3 KEY GENERATION AND DISTRIBUTION APPROACHES AND ATTACKS

Key Generation, 41
Software Key Generation, 43
Hardware Key Generation, 47
Noise-Based Approaches, 47
Noisy Diodes and Resistors, 47
Radio-Frequency Sources, 48
Brownian-Motion Devices, 48
Quantum Devices, 49
Nuclear Decay Devices, 49
Optical Devices, 50
Other Hardware Sources of Randomness, 51

Key Distribution, 51
Key Distribution for Software-Based PRGs, 52
7  SECURE MEMORY MANAGEMENT AND TRUSTED EXECUTION TECHNOLOGY  

The Need for Secure Memory Management, 91
Buffer Overflows, 92
Memory Pointer Attacks, 92
The Impact of Memory-Management Attacks, 93
Minimizing Memory-Management Attacks, 93
Platform-Design Considerations, 94
Trusted Execution Technology, 94
  Protected Execution, 95
  Protected Storage, 95
  Protected Input, 95
  Protected Graphics, 95
Environment Authentication and Protected Launch, 96
Domain Manager, 96
Platform and Hardware Requirements, 96
Unplanned Events, 99
Privacy and User Control, 99

8  THE TRUSTED PLATFORM MODULE  

The Need for Increased Network and PC Security, 101
Trust, 103
The Need for a Trusted Platform Module, 103
The Concept of Trusted Computing, 104
The Trusted Platform Module, 105
  Structure of the TPM, 107
  The TPM’s Primary Roles, 108
  TPM and Rootkits, 109
Complications Introduced by TPM, 109
Residual Vulnerabilities, 110
Privacy and Digital Rights Management, 111
Concluding Observations on TPM, 113
References, 114

9 FIELD-PROGRAMMABLE GATE ARRAYS 115

Background, 115
Why Use an FPGA?, 116
Security Considerations, 119
Attack Vectors, 120
  Black-Box Attacks, 121
  Readback Attacks, 122
  SRAM FPGAs, 123
  Antifuse FPGAs, 123
  Flash FPGAs, 124
  Indirect Attacks, 124
Preventing Attacks, 124
References, 125

10 HARDWARE-BASED AUTHENTICATION 127

Who is at the Other End?, 127
Authentication of a Person, 128
  Enrollment, 129
  Recognition, 129
  The Use of Multiple Biometrics, 131
Common Biometric Technologies, 132
  Signature, 132
  Face, 133
Gait, 133
Keystroke Timing, 134
Fingerprint, 134
Voiceprint, 136
Retinal Scan, 137
Iris Scan, 138
Palm Print, 138
Hand Geometry, 138
Infrared Thermogram, 139
DNA, 139
Authentication of a Device, 140
Authentication of the Surrounding Environment, 141
Wifi Hotspot, 141
IP address, 142
Clock Skew, 142
GPS, 143
Radio-Frequency Measurements, 144
Radio-Frequency Spectrum, 144
Location Fingerprints, 144
References, 145

11 A CLOSER LOOK AT BIOMETRICS 147

Fingerprint Scanners, 147
Optical Fingerprint Scanners, 148
Ultrasonic Fingerprint Scanners, 152
Capacitance Fingerprint Scanners, 152
E-Field Fingerprint Scanners, 153
The Basics of Fingerprint Analysis, 153
Iris Scans, 156
   Lens, 159
   Detector, 160
Illumination, 160
   Detector Enclosure, 160
   Human Interface, 160
   Algorithm, 161
Retinal Scans, 161
   Illumination, 162
   Detector, 163
   Scanner, 163
   Enclosure, 164
   User Interface, 164
   Performance, 164
References, 165

12 TOKENS: SOMETHING YOU HAVE 167

Overview, 167
Radio-Frequency IDs, 168
   Passive RFID, 168
   Active RFIDs, 170
   RFID Attack Vectors, 171
      RF Sniffing, 171
Smart Cards, 173
   Smart-Card Attack Vectors, 175
Interactive Tokens, 177
   Synchronization, 178
   Token Attack Vectors, 179
Seed Attacks, 179
Man-in-the-Middle Attacks, 179
References, 179

13 LOCATION TECHNOLOGIES 181
Overview, 181
Location’s Place in Security, 181
Geolocation, 182
   Key Requirements for Proper Operation of Geolocation, 184
   Assisted GPS, 186
Geolocation Attack Vectors, 186
   Jammers, 186
   Attenuation, 187
   Artificial Constellations, 187
   Fraudulent Timing Pulses, 187
   Corruption of Assist and Initial Location Information, 188
   Possible Protection Measures, 188
Wi-Fi Hot-Spot Triangulation, 189
   Wi-Fi Location Attack Vectors, 191
      Jamming, 191
      File Compromise on the Client and Server, 191
      Spoofing, 192
      Inadvertent Confusion, 192
Time of Flight, 192
   TOF Attack Vectors, 193
Short-Range Beacons, 193
RF Power Spectrum, 194
   Power-Spectrum Attack Vectors, 194
RF Signatures, 195
   RF Signature Attack Vectors, 195
IP Address and Clock Skew, 196
   Clock-Skew Attack Vectors, 197
References, 197

14 PUTTING IT ALL TOGETHER 199

Overview, 199
The Checklist, 200
Common Elements, 201
   Cryptographic Algorithm, 201
      Symmetric vs. Asymmetric Cryptography, 201
      Decisions Required, 202
   Key Generation, 202
      Decisions Required, 203
   Hash Algorithm for Digital Signatures, 203
      Decisions Required, 203
Specific Elements, 203
   Cryptographic Coprocessor, 204
      Decisions Required, 204
   Secure Bootstrap, 204
      Decisions Required, 204
   TPM, 205
      Decisions Required, 206
   Secure Memory Management, 206
      Decisions Required, 206
   TET, 206
      Decisions Required, 207