# Table of Contents

ABOUT THE AUTHORS xv
PREFACE xvii
ACKNOWLEDGMENTS xxi

I Introduction to Software Security Assessment

1 SOFTWARE VULNERABILITY FUNDAMENTALS 3
   Introduction 3
   Vulnerabilities 4
   Security Policies 5
   Security Expectations 7
   The Necessity of Auditing 9
   Auditing Versus Black Box Testing 11
   Code Auditing and the Development Life Cycle 13
   Classifying Vulnerabilities 14
   Design Vulnerabilities 14
   Implementation Vulnerabilities 15
   Operational Vulnerabilities 16
   Gray Areas 17

   Common Threads 18
   Input and Data Flow 18
   Trust Relationships 19
   Assumptions and Misplaced Trust 20
   Interfaces 21
   Environmental Attacks 21
   Exceptional Conditions 22
   Summary 23

2 DESIGN REVIEW 25
   Introduction 25
   Software Design Fundamentals 26
   Algorithms 26
   Abstraction and Decomposition 27
   Trust Relationships 28
   Principles of Software Design 31
   Fundamental Design Flaws 33
   Enforcing Security Policy 36
   Authentication 36
   Authorization 38
   Accountability 40
   Confidentiality 41
# Table of Contents

4 **APPLICATION REVIEW PROCESS** 91
   Introduction 91
   Overview of the Application Review Process 92
   Rationale 92
   Process Outline 93
   Preassessment 93
   Scoping 94
   Application Access 95
   Information Collection 96
   Application Review 97
   Avoid Drowning 98
   Iterative Process 98
   Initial Preparation 99
   Plan 101
   Work 103
   Reflect 105
   Documentation and Analysis 106
   Reporting and Remediation Support 108

3 **OPERATIONAL REVIEW** 67
   Introduction 67
   Exposure 68
      Attack Surface 68
      Insecure Defaults 69
      Access Control 69
      Unnecessary Services 70
      Secure Channels 71
      Spoofing and Identification 72
      Network Profiles 73
   Web-Specific Considerations 73
      HTTP Request Methods 73
      Directory Indexing 74
      File Handlers 74
      Authentication 75
      Default Site Installations 75
      Overly Verbose Error Messages 75
      Public-Facing Administrative Interfaces 76
   Protective Measures 76
      Development Measures 76
      Host-Based Measures 79
      Network-Based Measures 83
   Summary 89

Integrity 45
Availability 48
Threat Modeling 49
   Information Collection 50
   Application Architecture Modeling 53
   Threat Identification 59
   Documentation of Findings 62
   Prioritizing the Implementation Review 65
   Summary 66
## Table of Contents

**Test Cases** 139  
**Code Auditor's Toolbox** 147  
**Source Code Navigators** 148  
**Debuggers** 151  
**Binary Navigation Tools** 155  
**Fuzz-Testing Tools** 157  
**Case Study: OpenSSH** 158  
**Preassessment** 159  
**Implementation Analysis** 161  
**High-Level Attack Vectors** 162  
**Documentation of Findings** 164  
**Summary** 164

### II Software Vulnerabilities

#### 5 MEMORY CORRUPTION 167  
**Introduction** 167  
**Buffer Overflows** 168  
  - **Process Memory Layout** 169  
  - **Stack Overflows** 169  
  - **Off-by-One Errors** 180  
  - **Heap Overflows** 183  
  - **Global and Static Data Overflows** 186  
**Shellcode** 187  
**Writing the Code** 187  
**Finding Your Code in Memory** 188  
**Protection Mechanisms** 189  
**Stack Cookies** 190  
**Heap Implementation Hardening** 191  
**Nonexecutable Stack and Heap Protection** 193  
**Address Space Layout Randomization** 194  
**SafeSEH** 194  
**Function Pointer Obfuscation** 195  
**Assessing Memory Corruption Impact** 196  
**Where Is the Buffer Located in Memory?** 197  
**What Other Data Is Overwritten?** 197  
**How Many Bytes Can Be Overwritten?** 198  
**What Data Can Be Used to Corrupt Memory?** 199  
**Are Memory Blocks Shared?** 201  
**What Protections Are in Place?** 202  
**Summary** 202

#### 6 C LANGUAGE ISSUES 203  
**Introduction** 203  
**C Language Background** 204  
**Data Storage Overview** 204  
  - **Binary Encoding** 207  
  - **Byte Order** 209  
**Common Implementations** 209  
**Arithmetic Boundary Conditions** 211  
**Unsigned Integer Boundaries** 213  
**Signed Integer Boundaries** 220  
**Type Conversions** 223  
**Overview** 224  
**Conversion Rules** 225  
**Simple Conversions** 231  
**Integer Promotions** 233  
**Integer Promotion Applications** 235  
**Usual Arithmetic Conversions** 238
<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usual Arithmetic Conversion</td>
</tr>
<tr>
<td>Applications 242</td>
</tr>
<tr>
<td>Type Conversion Summary 244</td>
</tr>
<tr>
<td>Type Conversion</td>
</tr>
<tr>
<td>Vulnerabilities 246</td>
</tr>
<tr>
<td>Signed/Unsigned Conversions 246</td>
</tr>
<tr>
<td>Sign Extension 248</td>
</tr>
<tr>
<td>Truncation 259</td>
</tr>
<tr>
<td>Comparisons 265</td>
</tr>
<tr>
<td>Operators 271</td>
</tr>
<tr>
<td>The sizeof Operator 271</td>
</tr>
<tr>
<td>Unexpected Results 272</td>
</tr>
<tr>
<td>Pointer Arithmetic 277</td>
</tr>
<tr>
<td>Pointer Overview 277</td>
</tr>
<tr>
<td>Pointer Arithmetic Overview 278</td>
</tr>
<tr>
<td>Vulnerabilities 280</td>
</tr>
<tr>
<td>Other C Nuances 282</td>
</tr>
<tr>
<td>Order of Evaluation 282</td>
</tr>
<tr>
<td>Structure Padding 284</td>
</tr>
<tr>
<td>Precedence 287</td>
</tr>
<tr>
<td>Macros/Preprocessor 288</td>
</tr>
<tr>
<td>Typos 289</td>
</tr>
<tr>
<td>Summary 296</td>
</tr>
<tr>
<td>7 PROGRAM BUILDING BLOCKS 297</td>
</tr>
<tr>
<td>Introduction 297</td>
</tr>
<tr>
<td>Auditing Variable Use 298</td>
</tr>
<tr>
<td>Variable Relationships 298</td>
</tr>
<tr>
<td>Structure and Object Mismanagement 307</td>
</tr>
<tr>
<td>Variable Initialization 312</td>
</tr>
<tr>
<td>Arithmetic Boundaries 316</td>
</tr>
<tr>
<td>Type Confusion 319</td>
</tr>
<tr>
<td>Lists and Tables 321</td>
</tr>
<tr>
<td>Auditing Control Flow 326</td>
</tr>
<tr>
<td>Looping Constructs 327</td>
</tr>
<tr>
<td>Flow Transfer Statements 336</td>
</tr>
<tr>
<td>Switch Statements 337</td>
</tr>
<tr>
<td>Auditing Functions 339</td>
</tr>
<tr>
<td>Function Audit Logs 339</td>
</tr>
<tr>
<td>Return Value Testing and Interpretation 340</td>
</tr>
<tr>
<td>Function Side-Effects 351</td>
</tr>
<tr>
<td>Argument Meaning 360</td>
</tr>
<tr>
<td>Auditing Memory Management 362</td>
</tr>
<tr>
<td>ACC Logs 362</td>
</tr>
<tr>
<td>Allocation Functions 369</td>
</tr>
<tr>
<td>Allocator Scorecards and Error Domains 377</td>
</tr>
<tr>
<td>Double-Frees 379</td>
</tr>
<tr>
<td>Summary 385</td>
</tr>
<tr>
<td>8 STRINGS AND METACHARACTERS 387</td>
</tr>
<tr>
<td>Introduction 387</td>
</tr>
<tr>
<td>C String Handling 388</td>
</tr>
<tr>
<td>Unbounded String Functions 388</td>
</tr>
<tr>
<td>Bounded String Functions 393</td>
</tr>
<tr>
<td>Common Issues 400</td>
</tr>
<tr>
<td>Metacharacters 407</td>
</tr>
<tr>
<td>Embedded Delimiters 408</td>
</tr>
<tr>
<td>NUL Character Injection 411</td>
</tr>
<tr>
<td>Truncation 414</td>
</tr>
<tr>
<td>Common Metacharacter Formats 418</td>
</tr>
<tr>
<td>Path Metacharacters 418</td>
</tr>
<tr>
<td>C Format Strings 422</td>
</tr>
<tr>
<td>Shell Metacharacters 425</td>
</tr>
<tr>
<td>Perl open() 429</td>
</tr>
<tr>
<td>SQL Queries 431</td>
</tr>
<tr>
<td>Metacharacter Filtering 434</td>
</tr>
<tr>
<td>Eliminating Metacharacters 434</td>
</tr>
</tbody>
</table>
9 UNIX I: PRIVILEGES AND FILES 459
Introduction 459
UNIX 101 460
Users and Groups 461
Files and Directories 462
Processes 464
Privilege Model 464
Privileged Programs 466
User ID Functions 468
Group ID Functions 475
Privilege Vulnerabilities 477
Reckless Use of Privileges 477
Dropping Privileges
Permanently 479
Dropping Privileges
Temporarily 486
Auditing Privilege-Management
Code 488
Privilege Extensions 491
File Security 494
File IDs 494
File Permissions 495
Directory Permissions 498
Privilege Management with File
Operations 499
File Creation 500
Directory Safety 503
Filenames and Paths 503
Dangerous Places 507
Interesting Files 508
File Internals 512
File Descriptors 512
Inodes 513
Directories 514
Links 515
Symbolic Links 515
Hard Links 522
Race Conditions 526
TOCTOU 527
The stat() Family of Functions 528
File Race Redux 532
Permission Races 533
Ownership Races 534
Directory Races 535
Temporary Files 538
Unique File Creation 538
File Reuse 544
Temporary Directory
Cleaners 546
The Stdio File Interface 547
Opening a File 548
Reading from a File 550
Writing to a File 555
Closing a File 556
Summary 557
<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Invocation 565</td>
</tr>
<tr>
<td>Indirect Invocation 570</td>
</tr>
<tr>
<td>Process Attributes 572</td>
</tr>
<tr>
<td>Process Attribute Retention 573</td>
</tr>
<tr>
<td>Resource Limits 574</td>
</tr>
<tr>
<td>File Descriptors 580</td>
</tr>
<tr>
<td>Environment Arrays 591</td>
</tr>
<tr>
<td>Process Groups, Sessions, and Terminals 609</td>
</tr>
<tr>
<td>Interprocess Communication 611</td>
</tr>
<tr>
<td>Pipes 612</td>
</tr>
<tr>
<td>Named Pipes 612</td>
</tr>
<tr>
<td>System V IPC 614</td>
</tr>
<tr>
<td>UNIX Domain Sockets 615</td>
</tr>
<tr>
<td>Remote Procedure Calls 618</td>
</tr>
<tr>
<td>RPC Definition Files 619</td>
</tr>
<tr>
<td>RPC Decoding Routines 622</td>
</tr>
<tr>
<td>Authentication 623</td>
</tr>
<tr>
<td>Summary 624</td>
</tr>
</tbody>
</table>

11 Windows I: Objects and the File System 625

| Introduction 625 |
| Background 626 |
| Objects 627 |
| Object Namespaces 629 |
| Object Handles 632 |
| Sessions 636 |
| Security IDs 637 |
| Logon Rights 638 |
| Access Tokens 639 |
| Security Descriptors 647 |
| Access Masks 648 |
| ACL Inheritance 649 |
| Security Descriptors Programming Interfaces 649 |
| Auditing ACL Permissions 652 |
| Processes and Threads 654 |
| Process Loading 654 |
| ShellExecute and ShellExecuteEx 655 |
| DLL Loading 656 |
| Services 658 |
| File Access 659 |
| File Permissions 659 |
| The File I/O API 661 |
| Links 676 |
| The Registry 680 |
| Key Permissions 681 |
| Key and Value Squatting 682 |
| Summary 684 |

12 Windows II: Interprocess Communication 685

| Introduction 685 |
| Windows IPC Security 686 |
| The Redirector 686 |
| Impersonation 688 |
| Window Messaging 689 |
| Window Stations Object 690 |
| The Desktop Object 690 |
| Window Messages 691 |
| Shatter Attacks 694 |
| DDE 697 |
| Terminal Sessions 697 |
| Pipes 698 |
| Pipe Permissions 698 |
| Named Pipes 699 |
| Pipe Creation 699 |
| Impersonation in Pipes 700 |
| Pipe Squatting 703 |
15 FIREWALLS 891
Introduction 891
Overview of Firewalls 892
Proxy Versus Packet Filters 893
Attack Surface 895
Proxy Firewalls 895
Packet-Filtering Firewalls 896
Stateless Firewalls 896
TCP 896
UDP 899
FTP 901
Fragmentation 902
Simple Stateful Firewalls 905
TCP 905
UDP 906
Directionality 906
Fragmentation 907
Stateful Inspection Firewalls 909
Layering Issues 911
Spoofing Attacks 914
Spoofing from a Distance 914
Spoofing Up Close 917
Spooky Action at a Distance 919
Summary 920

16 NETWORK APPLICATION
PROTOCOLS 921
Introduction 921
Auditing Application Protocols 922
Collect Documentation 922
Identify Elements of Unknown Protocols 923
Match Data Types with the Protocol 927
Data Verification 935
Access to System Resources 935
Hypertext Transfer Protocol 937
Header Parsing 937
Accessing Resources 940
Utility Functions 941
Posting Data 942
Internet Security Association and Key Management Protocol 948
Payloads 952
Payload Types 956
Encryption Vulnerabilities 971
Abstract Syntax Notation (ASN.1) 972
Basic Encoding Rules 975
Canonical Encoding and Distinguished Encoding 976
Vulnerabilities in BER, CER, and DER Implementations 977
Packed Encoding Rules (PER) 979
XML Encoding Rules 983
XER Vulnerabilities 984
Domain Name System 984
Domain Names and Resource Records 984
Name Servers and Resolvers 986
Zones 987
Resource Record Conventions 988
Basic Use Case 989
DNS Protocol Structure Primer 990
Table of Contents

DNS Names 993
Length Variables 996
DNS Spoofing 1002
Summary 1005

17 WEB APPLICATIONS 1007
Introduction 1007
Web Technology Overview 1008
The Basics 1009
Static Content 1009
CGI 1009
Web Server APIs 1010
Server-Side Includes 1011
Server-Side Transformation 1012
Server-Side Scripting 1013
HTTP 1014
Overview 1014
Versions 1017
Headers 1018
Methods 1020
Parameters and Forms 1022
State and HTTP
Authentication 1027
Overview 1028
Client IP Addresses 1029
Referer Request Header 1030
Embedding State in HTML and
URLs 1032
HTTP Authentication 1033
Cookies 1036
Sessions 1038
Architecture 1040
Redundancy 1040
Presentation Logic 1040
Business Logic 1041
N-Tier Architectures 1041
Business Tier 1043
Web Tier:
Model-View-Controller 1044
Problem Areas 1046
Client Visibility 1046
Client Control 1047
Page Flow 1048
Sessions 1049
Authentication 1056
Authorization and Access
Control 1057
Encryption and SSL/TLS 1058
Phishing and Impersonation 1059
Common Vulnerabilities 1060
SQL Injection 1061
OS and File System
Interaction 1066
XML Injection 1069
XPath Injection 1070
Cross-Site Scripting 1071
Threading Issues 1074
C/C++ Problems 1075
Harsh Realities of the Web 1075
Auditing Strategy 1078
Summary 1081

18 WEB TECHNOLOGIES 1083
Introduction 1083
Web Services and Service-Oriented
Architecture 1084
SOAP 1085
REST 1085
AJAX 1085
Web Application Platforms 1086
CGI 1086
Indexed Queries 1086
Environment Variables 1087