"There are a number of secure programming books on the market, but none that go as deep as this one. The depth and detail exceeds all books that I know about by an order of magnitude."

—**Halvar Flake,** CEO and head of research, SABRE Security GmbH

THE ART OF SOFTWARE SECURITY ASSESSMENT

Identifying and Preventing Software Vulnerabilities

MARK DOWD
JOHN McDONALD
JUSTIN SCHUH

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

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

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

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
Code Navigation 109
External Flow Sensitivity 109
Tracing Direction 111
Code-Auditing Strategies 111
Code Comprehension Strategies 113
Candidate Point Strategies 119
Design Generalization Strategies 128
Code-Auditing Techniques 133
Internal Flow Analysis 133
Subsystem and Dependency Analysis 135
Rereading Code 136
Desk-Checking 137

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

Usual Arithmetic Conversion Applications 242
Type Conversion Summary 244
Type Conversion Vulnerabilities 246
Signed/Unsigned Conversions 246
Sign Extension 248
Truncation 259
Comparisons 265
Operators 271
The sizeof Operator 271
Unexpected Results 272
Pointer Arithmetic 277
Pointer Overview 277
Pointer Arithmetic Overview 278
Vulnerabilities 280
Other C Nuances 282
Order of Evaluation 282
Structure Padding 284
Precedence 287
Macros/Preprocessor 288
Typos 289
Summary 296

7 PROGRAM BUILDING BLOCKS 297
Introduction 297
Auditing Variable Use 298
Variable Relationships 298
Structure and Object Mismanagement 307
Variable Initialization 312
Arithmetic Boundaries 316
Type Confusion 319
Lists and Tables 321
Auditing Control Flow 326
Looping Constructs 327
Flow Transfer Statements 336
Switch Statements 337
Auditing Functions 339
Function Audit Logs 339
Return Value Testing and Interpretation 340
Function Side-Effects 351
Argument Meaning 360
Auditing Memory Management 362
ACC Logs 362
Allocation Functions 369
Allocator Scorecards and Error Domains 377
Double-Frees 379
Summary 385

8 STRINGS AND METACHARACTERS 387
Introduction 387
C String Handling 388
Unbounded String Functions 388
Bounded String Functions 393
Common Issues 400
Metacharacters 407
Embedded Delimiters 408
NUL Character Injection 411
Truncation 414
Common Metacharacter Formats 418
Path Metacharacters 418
C Format Strings 422
Shell Metacharacters 425
Perl open() 429
SQL Queries 431
Metacharacter Filtering 434
Eliminating Metacharacters 434

Escaping Metacharacters 439
Metacharacter Evasion 441
Character Sets and Unicode 446
Unicode 446
Windows Unicode Functions 450
Summary 457

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

10 UNIX II: PROCESSES 559
Introduction 559
Processes 560
Process Creation 560
fork() Variants 562
Process Termination 562
fork() and Open Files 563
Program Invocation 565

Direct Invocation 565
Indirect Invocation 570
Process Attributes 572
Process Attribute Retention 573
Resource Limits 574
File Descriptors 580
Environment Arrays 591
Process Groups, Sessions, and Terminals 609
Interprocess Communication 611
Pipes 612
Named Pipes 612
System V IPC 614
UNIX Domain Sockets 615
Remote Procedure Calls 618
RPC Definition Files 619
RPC Decoding Routines 622
Authentication 623
Summary 624

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

Mailslots 705
Mailslot Permissions 705
Mailslot Squatting 706
Remote Procedure Calls 706
RPC Connections 706
RPC Transports 707
Microsoft Interface Definition Language 708
IDL File Structure 708
Application Configuration Files 710
RPC Servers 711
Impersonation in RPC 716
Context Handles and State 718
Threading in RPC 721
Auditing RPC Applications 722
COM 725
COM: A Quick Primer 725
DCOM Configuration Utility 731
DCOM Application Identity 732
DCOM Subsystem Access Permissions 733
DCOM Access Controls 734
Impersonation in DCOM 736
MIDL Revisited 738
Active Template Library 740
Auditing DCOM Applications 741
ActiveX Security 749
Summary 754

13 Synchronization and State 755

Introduction 755
Synchronization Problems 756
Reentrancy and Asynchronous-Safe Code 757
Race Conditions 759
Starvation and Deadlocks 760
Process Synchronization 762
System V Process Synchronization 762
Windows Process Synchronization 765
Vulnerabilities with Interprocess Synchronization 770
Signals 783
Sending Signals 786
Handling Signals 786
Jump Locations 788
Signal Vulnerabilities 791
Signals Scoreboard 809
Threads 810
PThreads API 811
Windows API 813
Threading Vulnerabilities 815
Summary 825

III Software Vulnerabilities in Practice

14 Network Protocols 829

Introduction 829
Internet Protocol 831
IP Addressing Primer 832
IP Packet Structures 834
Basic IP Header Validation 836
IP Options Processing 844
Source Routing 851
Fragmentation 853
User Datagram Protocol 863
Basic UDP Header Validation 864
UDP Issues 864
Transmission Control Protocol 864
Basic TCP Header Validation 866
TCP Options Processing 867

TCP Connections 869
TCP Streams 872
TCP Processing 880
Summary 890

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

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

Path Confusion 1091
Perl 1093
SQL Injection 1093
File Access 1094
Shell Invocation 1095
File Inclusion 1095
Inline Evaluation 1095
Cross-Site Scripting 1096
Taint Mode 1096
PHP 1096
SQL Injection 1097
File Access 1098
Shell Invocation 1099
File Inclusion 1101
Inline Evaluation 1101
Cross-Site Scripting 1103
Configuration 1104
Java 1105
SQL Injection 1106
File Access 1107
Shell Invocation 1108
File Inclusion 1108
JSP File Inclusion 1109
Inline Evaluation 1110
Cross-Site Scripting 1110
Threading Issues 1111
Configuration 1112
ASP 1113
SQL Injection 1113
File Access 1115
Shell Invocation 1115
File Inclusion 1116
Inline Evaluation 1117
Cross-Site Scripting 1118
Configuration 1118
ASP.NET 1118
SQL Injection 1118
File Access 1119
Shell Invocation 1120
File Inclusion 1120
Inline Evaluation 1121
Cross-Site Scripting 1121
Configuration 1121
ViewState 1121
Summary 1123

BIBLIOGRAPHY 1125

INDEX 1129