

THE ART OF

# SOFTWARE SECURITY ASSESSMENT

IDENTIFYING AND PREVENTING SOFTWARE  
VULNERABILITIES

---

**MARK DOWD**  
**JOHN MCDONALD**  
**JUSTIN SCHUH**

Software security is a critical concern for organizations of all sizes. This book provides a comprehensive guide to identifying and preventing software vulnerabilities, from basic concepts to advanced techniques.

The authors, Mark Dowd, John McDonald, and Justin Schuh, are experts in the field and have developed a unique approach to software security assessment. They provide practical advice and real-world examples to help readers understand the risks and threats to their software systems.

This book is essential reading for anyone involved in software development, IT operations, or information security. It will help you protect your organization's software assets and ensure that your systems remain secure and reliable.

◆ Addison-Wesley

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco  
New York • Toronto • Montreal • London • Munich • Paris • Madrid  
Cape Town • Sydney • Tokyo • Singapore • Mexico City

# Software Security Assessment

## Common Threads

### Input and Data Flow

### Trust Relationships

### Assumptions and Misplaced Trust

### Interfaces

### Environmental Attacks

### Exceptional Conditions

### Summary

# 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

---

Integrity 45	<b>4 APPLICATION REVIEW PROCESS 91</b>
Availability 48	Introduction 91
Threat Modeling 49	Overview of the Application Review Process 92
Information Collection 50	Rationale 92
Application Architecture Modeling 53	Process Outline 93
Threat Identification 59	Preassessment 93
Documentation of Findings 62	Scoping 94
Prioritizing the Implementation Review 65	Application Access 95
Summary 66	Information Collection 96
<b>3 OPERATIONAL REVIEW 67</b>	Application Review 97
Introduction 67	Avoid Drowning 98
Exposure 68	Iterative Process 98
Attack Surface 68	Initial Preparation 99
Insecure Defaults 69	Plan 101
Access Control 69	Work 103
Unnecessary Services 70	Reflect 105
Secure Channels 71	Documentation and Analysis 106
Spoofing and Identification 72	Reporting and Remediation Support 108
Network Profiles 73	Code Navigation 109
Web-Specific Considerations 73	External Flow Sensitivity 109
HTTP Request Methods 73	Tracing Direction 111
Directory Indexing 74	Code-Auditing Strategies 111
File Handlers 74	Code Comprehension Strategies 113
Authentication 75	Candidate Point Strategies 119
Default Site Installations 75	Design Generalization Strategies 128
OverlyVerbose Error Messages 75	Code-Auditing Techniques 133
Public-Facing Administrative Interfaces 76	Internal Flow Analysis 133
Protective Measures 76	Subsystem and Dependency Analysis 135
Development Measures 76	Rereading Code 136
Host-Based Measures 79	Desk-Checking 137
Network-Based Measures 83	
Summary 89	

Test Cases	139	SafeSEH	194
Code Auditor's Toolbox	147	Function Pointer Obfuscation	195
Source Code Navigators	148	Assessing Memory Corruption	
Debuggers	151	Impact	196
Binary Navigation Tools	155	Where Is the Buffer Located in	
Fuzz-Testing Tools	157	Memory?	197
Case Study: OpenSSH	158	What Other Data Is	
Preassessment	159	Overwritten?	197
Implementation Analysis	161	How Many Bytes Can Be	
High-Level Attack Vectors	162	Overwritten?	198
Documentation of Findings	164	What Data Can Be Used to	
Summary	164	Corrupt Memory?	199
<b>II Software Vulnerabilities</b>		Are Memory Blocks Shared?	201
<b>5 MEMORY CORRUPTION</b>	<b>167</b>	What Protections Are in	
Introduction	167	Place?	202
Buffer Overflows	168	Summary	202
Process Memory Layout	169		
Stack Overflows	169	<b>6 C LANGUAGE ISSUES</b>	<b>203</b>
Off-by-One Errors	180	Introduction	203
Heap Overflows	183	C Language Background	204
Global and Static Data		Data Storage Overview	204
Overflows	186	Binary Encoding	207
Shellcode	187	Byte Order	209
Writing the Code	187	Common Implementations	209
Finding Your Code in		Arithmetic Boundary	
Memory	188	Conditions	211
Protection Mechanisms	189	Unsigned Integer Boundaries	213
Stack Cookies	190	Signed Integer Boundaries	220
Heap Implementation		Type Conversions	223
Hardening	191	Overview	224
Nonexecutable Stack and Heap		Conversion Rules	225
Protection	193	Simple Conversions	231
Address Space Layout		Integer Promotions	233
Randomization	194	Integer Promotion	
		Applications	235
		Usual Arithmetic Conversions	238

## Table of Contents

---

Usual Arithmetic Conversion	Flow Transfer Statements	336
Applications	Switch Statements	337
Type Conversion Summary	Auditing Functions	339
Type Conversion	Function Audit Logs	339
Vulnerabilities	Return Value Testing and Interpretation	340
Signed/Unsigned Conversions	Function Side-Effects	351
Sign Extension	Argument Meaning	360
Truncation	Auditing Memory Management	362
Comparisons	ACC Logs	362
Operators	Allocation Functions	369
271	Allocator Scorecards and Error Domains	377
The sizeof Operator	Double-Frees	379
Unexpected Results	Summary	385
Pointer Arithmetic	<b>8 STRINGS AND METACHARACTERS</b>	387
277	Introduction	387
Pointer Overview	C String Handling	388
Pointer Arithmetic Overview	Unbounded String Functions	388
Vulnerabilities	Bounded String Functions	393
Other C Nuances	Common Issues	400
282	Metacharacters	407
Order of Evaluation	Embedded Delimiters	408
Structure Padding	NUL Character Injection	411
Precedence	Truncation	414
Macros/Preprocessor	Common Metacharacter Formats	418
Typos	Path Metacharacters	418
Summary	C Format Strings	422
<b>7 PROGRAM BUILDING BLOCKS</b>	Shell Metacharacters	425
297	Perl open()	429
Introduction	SQL Queries	431
Auditing Variable Use	Metacharacter Filtering	434
Variable Relationships	Eliminating Metacharacters	434
Structure and Object		
Mismanagement		
Variable Initialization		
Arithmetic Boundaries		
Type Confusion		
Lists and Tables		
Auditing Control Flow		
Looping Constructs		

Escaping Metacharacters	439	Interesting Files	508
Metacharacter Evasion	441	File Internals	512
Character Sets and Unicode	446	File Descriptors	512
Unicode	446	Inodes	513
Windows Unicode Functions	450	Directories	514
Summary	457	Links	515
<b>9 UNIX I: PRIVILEGES AND FILES</b>	<b>459</b>	Symbolic Links	515
Introduction	459	Hard Links	522
UNIX 101	460	Race Conditions	526
Users and Groups	461	TOCTOU	527
Files and Directories	462	The stat() Family of Functions	528
Processes	464	File Race Redux	532
Privilege Model	464	Permission Races	533
Privileged Programs	466	Ownership Races	534
User ID Functions	468	Directory Races	535
Group ID Functions	475	Temporary Files	538
Privilege Vulnerabilities	477	Unique File Creation	538
Reckless Use of Privileges	477	File Reuse	544
Dropping Privileges		Temporary Directory	
Permanently	479	Cleaners	546
Dropping Privileges		The Stdio File Interface	547
Temporarily	486	Opening a File	548
Auditing Privilege-Management		Reading from a File	550
Code	488	Writing to a File	555
Privilege Extensions	491	Closing a File	556
File Security	494	Summary	557
File IDs	494	<b>10 UNIX II: PROCESSES</b>	<b>559</b>
File Permissions	495	Introduction	559
Directory Permissions	498	Processes	560
Privilege Management with File		Process Creation	560
Operations	499	fork() Variants	562
File Creation	500	Process Termination	562
Directory Safety	503	fork() and Open Files	563
Filenames and Paths	503	Program Invocation	565
Dangerous Places	507		

## Table of Contents

---

Direct Invocation	565	Auditing ACL Permissions	652
Indirect Invocation	570	Processes and Threads	654
Process Attributes	572	Process Loading	654
Process Attribute Retention	573	ShellExecute and	
Resource Limits	574	ShellExecuteEx	655
File Descriptors	580	DLL Loading	656
Environment Arrays	591	Services	658
Process Groups, Sessions, and		File Access	659
Terminals	609	File Permissions	659
Interprocess Communication	611	The File I/O API	661
Pipes	612	Links	676
Named Pipes	612	The Registry	680
System V IPC	614	Key Permissions	681
UNIX Domain Sockets	615	Key and Value Squatting	682
Remote Procedure Calls	618	Summary	684
RPC Definition Files	619	<b>12 WINDOWS II: INTERPROCESS</b>	
RPC Decoding Routines	622	<b>COMMUNICATION</b>	<b>685</b>
Authentication	623	Introduction	685
Summary	624	Windows IPC Security	686
<b>11 WINDOWS I: OBJECTS AND THE FILE</b>		The Redirector	686
<b>SYSTEM</b>	<b>625</b>	Impersonation	688
Introduction	625	Window Messaging	689
Background	626	Window Stations Object	690
Objects	627	The Desktop Object	690
Object Namespaces	629	Window Messages	691
Object Handles	632	Shatter Attacks	694
Sessions	636	DDE	697
Security IDs	637	Terminal Sessions	697
Logon Rights	638	Pipes	698
Access Tokens	639	Pipe Permissions	698
Security Descriptors	647	Named Pipes	699
Access Masks	648	Pipe Creation	699
ACL Inheritance	649	Impersonation in Pipes	700
Security Descriptors Programming		Pipe Squatting	703
Interfaces	649		

Mailslots	705	Process Synchronization	762
Mailslot Permissions	705	System V Process	
Mailslot Squatting	706	Synchronization	762
Remote Procedure Calls	706	Windows Process	
RPC Connections	706	Synchronization	765
RPC Transports	707	Vulnerabilities with Interprocess	
Microsoft Interface Definition		Synchronization	770
Language	708	Signals	783
IDL File Structure	708	Sending Signals	786
Application Configuration		Handling Signals	786
Files	710	Jump Locations	788
RPC Servers	711	Signal Vulnerabilities	791
Impersonation in RPC	716	Signals Scoreboard	809
Context Handles and State	718	Threads	810
Threading in RPC	721	PThreads API	811
Auditing RPC Applications	722	Windows API	813
COM	725	Threading Vulnerabilities	815
COM: A Quick Primer	725	Summary	825
DCOM Configuration Utility	731	<hr/>	
DCOM Application Identity	732	<b>III Software Vulnerabilities in Practice</b>	
DCOM Subsystem Access		<b>14 NETWORK PROTOCOLS</b>	829
Permissions	733	Introduction	829
DCOM Access Controls	734	Internet Protocol	831
Impersonation in DCOM	736	IP Addressing Primer	832
MIDL Revisited	738	IP Packet Structures	834
Active Template Library	740	Basic IP Header Validation	836
Auditing DCOM Applications	741	IP Options Processing	844
ActiveX Security	749	Source Routing	851
Summary	754	Fragmentation	853
<b>13 SYNCHRONIZATION AND STATE</b>	755	User Datagram Protocol	863
Introduction	755	Basic UDP Header Validation	864
Synchronization Problems	756	UDP Issues	864
Reentrancy and		Transmission Control Protocol	864
Asynchronous-Safe Code	757	Basic TCP Header Validation	866
Race Conditions	759	TCP Options Processing	867
Starvation and Deadlocks	760		

## Table of Contents

---

TCP Connections	869	Identify Elements of Unknown Protocols	923
TCP Streams	872	Match Data Types with the Protocol	927
TCP Processing	880	Data Verification	935
Summary	890	Access to System Resources	935
<b>15 FIREWALLS</b>	<b>891</b>	Hypertext Transfer Protocol	937
Introduction	891	Header Parsing	937
Overview of Firewalls	892	Accessing Resources	940
Proxy Versus Packet Filters	893	Utility Functions	941
Attack Surface	895	Posting Data	942
Proxy Firewalls	895	Internet Security Association and Key Management Protocol	948
Packet-Filtering Firewalls	896	Payloads	952
Stateless Firewalls	896	Payload Types	956
TCP	896	Encryption Vulnerabilities	971
UDP	899	Abstract Syntax Notation (ASN.1)	972
FTP	901	Basic Encoding Rules	975
Fragmentation	902	Canonical Encoding and Distinguished Encoding	976
Simple Stateful Firewalls	905	Vulnerabilities in BER, CER, and DER Implementations	977
TCP	905	Packed Encoding Rules (PER)	979
UDP	906	XML Encoding Rules	983
Directionality	906	XER Vulnerabilities	984
Fragmentation	907	Domain Name System	984
Stateful Inspection Firewalls	909	Domain Names and Resource Records	984
Layering Issues	911	Name Servers and Resolvers	986
Spoofing Attacks	914	Zones	987
Spoofing from a Distance	914	Resource Record Conventions	988
Spoofing Up Close	917	Basic Use Case	989
Spooky Action at a Distance	919	DNS Protocol Structure Primer	990
Summary	920		
<b>16 NETWORK APPLICATION PROTOCOLS</b>	<b>921</b>		
Introduction	921		
Auditing Application Protocols	922		
Collect Documentation	922		

## Table of Contents

---

DNS Names	993	
Length Variables	996	
DNS Spoofing	1002	
Summary	1005	
<b>17 WEB APPLICATIONS 1007</b>		
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	
<b>18 WEB TECHNOLOGIES 1083</b>		
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	

## Table of Contents

---

Path Confusion	1091	Cross-Site Scripting	1110
Perl	1093	Threading Issues	1111
SQL Injection	1093	Configuration	1112
File Access	1094	ASP	1113
Shell Invocation	1095	SQL Injection	1113
File Inclusion	1095	File Access	1115
Inline Evaluation	1095	Shell Invocation	1115
Cross-Site Scripting	1096	File Inclusion	1116
Taint Mode	1096	Inline Evaluation	1117
PHP	1096	Cross-Site Scripting	1118
SQL Injection	1097	Configuration	1118
File Access	1098	ASP.NET	1118
Shell Invocation	1099	SQL Injection	1118
File Inclusion	1101	File Access	1119
Inline Evaluation	1101	Shell Invocation	1120
Cross-Site Scripting	1103	File Inclusion	1120
Configuration	1104	Inline Evaluation	1121
Java	1105	Cross-Site Scripting	1121
SQL Injection	1106	Configuration	1121
File Access	1107	ViewState	1121
Shell Invocation	1108	Summary	1123
File Inclusion	1108	<b>BIBLIOGRAPHY</b>	<b>1125</b>
JSP File Inclusion	1109	<b>INDEX</b>	<b>1129</b>
Inline Evaluation	1110		