



Contents

FOREWORD	xix
ACKNOWLEDGMENTS	xxi
INTRODUCTION	xxiii

PART I Quick Start

1 General Security Best Practices	3
Security Policies	4
Different Policies for Different Needs	5
Understanding Security Requirements	6
Policy Creation	6
Practical Policies	6
The Tenets of Security	8
Security by Design	8
Defense in Depth	9
Least Privileges	9
Risk Analysis	10
Document Your Risk Analysis	11
Expect the Unexpected	11
Contingency Planning and Incident Response	12
Snapshots and Situational Awareness	13
Cover All the Areas	13
Hardening the Infrastructure	14
The Operating System	15
The Network	16
The Application Server	18

2 Securing the Database	21
Securing (Default) User Accounts	22
Lock Down Example	23
Throw Out Anything Stale	29
Oracle Passwords	29
Application Password Authentication Using Oracle's Native Password Store	30
Checking for Weak or Default Passwords	32
Impossible Passwords	35
Managing and Ensuring Good Passwords	36
Limiting Database Resources	41
Resource Limits	41
Default Roles	42
CONNECT	42
RESOURCE	43
DBA	44
PUBLIC Privileges	45
When to Grant Privileges to PUBLIC	45
Oracle Supplied Objects	46
Securing the Network	49
Encryption	49
Database Listener	50

PART II

Identification and Authentication

3 Understanding Identification and Authentication	55
Importance of Identification and Authentication	56
Identification Methods	57
User-Supplied Identification	57
Technological Identification	58
Identity Crisis	59
Spoofing	59
Identity Theft	60
Authentication	60
Methods	61
Best Practices for Secure Authentication	62
Single Sign-On	63
Why Single Sign-On Exists	63
Challenges to Single Sign-On	63
Database I&A	64
Associating Users with Database Schemas	64
Separate Users and Data	67
Identity Preservation	67
Determining the Appropriate Level of I&A	67

4 Connection Pools and Proxy Authentication	69
Heritage	70
Host-Based Identification and Authentication	70
Client-Server Identification and Authentication	73
Web Applications	74
The Stateless Environment	75
Web Databases	75
Connection Pools	78
Oracle Implicit Connection Cache	79
Security Risks	82
Session Pools and the Oracle OCI Connection Pool	84
OCI Connection Pool Example	84
Password Management Risk	87
Proxy Authentication	88
Proxy Example	88
Proxy Authentication Database Setup	91
Proxy Authentication Modes	96
Forcing Proxy Authentication	98
5 Identity Management and Enterprise Users	99
Identity Management	100
Directory Services	100
IM Components	101
Oracle Internet Directory (OiD)	102
Enterprise Users	102
History	102
Setting Up EUS	103
LDAP Setup	103
Database Setup	103
Applying EUS	107
Creating the Enterprise User	108
The Connection Process	109
User-Schema Mappings	110
Creating the Shared Schemas	110
Directory Mappings	112
Mapping Permutations Example	112
Exclusive Schemas	117
Considerations	119
Single Credentials and Performance	119
Dependencies	120
6 Identification and Authentication for Web Applications	121
Application Processes for Identification and Authentication	122
Integrated Authentication	122
Creating the Application User	123
Connecting the Application User to the Database	125

Getting the User Identity	127
Database Account Setup	129
User Database Account(s)	130
Authentication Blueprint	130
Performance	132
Proxy Authentication Alternatives	134
Application Directed Security	134
Application User Proxy—Client Identifiers	136
Leveraging Database Security with Anonymous Connection Pools	143
Identifying Information	148

PART III

Authorizations and Auditing

7 Privileges and Roles	153
Access Control, Authorizations, and Privileges	154
Access Control	154
Enforcing Access Control	154
Authorizations	154
Privileges	155
System Privileges	155
Object Privileges	159
Synonyms	162
System and Object Privileges Together	163
Privilege Persistence	164
Roles	169
Role Hierarchies	169
Designing for Definer and Invoker Rights	173
Selective Privilege Enablement	175
Selective Privilege Use Cases	178
Password-Protected Roles	181
Password-Protected Role Example	181
Password-Protected Roles and Proxy Authentication	182
Challenges to Securing the Password	183
Secure Application Roles	184
Secure Application Role Example	184
Global Roles and Enterprise Roles	189
Creating and Assigning Global and Enterprise Roles	189
Combining Standard and Global/Enterprise Roles	192
Using Roles Wisely	192
Too Many Roles	192
Naming	192
Dependencies	193
Example—Putting the Pieces Together	194
Application Authentication	194
Verifying the User	195
Setting the Secure Application Role	197
Securing the Source	198

8 Effective Auditing for Accountability	201
The Security Cycle	202
Auditing for Accountability	203
Auditing Provides the Feedback Loop	203
Auditing Is Not Overhead	203
Audit Methods	204
Application Server Logs	204
Application Auditing	205
Application Audit Example	205
Trigger Auditing	211
Trigger Audit Example	211
Autonomous Transactions and Auditing	214
Data Versioning	216
Flashback Version Query	217
Flashback Transaction Query	218
Standard Database Auditing	220
Mandatory Auditing	220
Auditing SYS	220
Enabling Standard Auditing	222
Auditing By User, Privilege, and Object	222
Auditing Best Practices	223
Determining the Audit Status	227
Extending the Audit Data with Client Identifiers	228
Performance Test	231
Caveats	233
Fine-Grained Auditing	233
Audit Conditions	233
Column Sensitivity	237
Capturing SQL	239
Acting on the Audit	239
Caveats	243

PART IV

Fine-Grained Access Control

9 Application Contexts for Security and Performance	247
Application Context	248
Default USERENV Context	249
Local Context	251
Creating an Application Context	251
Setting Context Attributes and Values	252
Applying the Application Context to Security	255
Secure Use	258
Common Mistakes	258
Global Context	261
Uses	261
Examples	261
External and Initialized Globally	273

10 Implementing Fine-Grained Access Controls with Views	277
Introduction to Fine-Grained Access	278
Object Access	278
Fine-Grained Access	279
Secure Views	279
Views for Column-Level Security	281
Views for Row-Level Security	288
Viewing Problems	291
11 Row-Level Security with Virtual Private Database	293
The Need for Virtual Private Databases	294
Row-Level Security Quick Start	295
Quick Start Example	295
RLS In-Depth	297
Benefits	297
Setup	298
The RLS Layer of Security	305
RLS Exemption	308
Debugging RLS Policies	310
Partitioned Fine-Grained Access Control	320
Column Sensitive VPD	320
VPD Performance	322
Bind Variables	322
Code Location	323
Policy Caching	323
Caching Caution	332
Comparing VPD Performance to View-Based RLS	333
12 Oracle Label Security	337
Classifying Data	338
OLS Ancestry	339
Labels and Mandatory Access Control	339
Trusted Oracle	340
Oracle Label Security	341
How OLS Works	342
Installing OLS	342
Implementing Label Security	342
Label Example	343
Creating the Policy	343
Label Components	346
Levels	347
Creating Labels	348
Applying the Policy	350
Authorizing Access	352
Testing the Labels	353
Special OLS Privileges	354
Compartments	357

Adding Data to OLS Protected Tables	361
Groups	365
Using the Default Session Label	371
Comparing the Labels	374
Hiding the Label	375
Changing the Hidden Status	375
Writing to OLS Protected Tables	379
Understanding Write Authorizations	379
Groups and Compartments Dependency	383
Tips and Tricks	387
Restricted Updates to the Labels	387
Trusted Procedures	389
Label Functions	391
Storing the Labels in OID	394
Using Labels with Connection Pools and Shared Schemas	394
OLS Consideration Factors	395
VPD Versus Label Security	396
Advantages of OLS	396
Advantages of VPD	396
VPD and OLS	397
13 Database Encryption	401
Encryption 101	402
The Basics	403
Encryption Choices	403
When to Use Database Encryption	406
Reasons Not to Encrypt	407
Reasons to Encrypt	408
DBMS_CRYPTO	408
Encryption Routines	409
DBMS_CRYPTO Simple Example	410
DATA_CRYPTO Package	411
Encryption Examples	415
Encrypting Character, Numbers, and Dates	415
Encrypting CLOBs and BLOBs	419
Encryption In-Depth	422
Keys, Data, and IVs	422
Storing Encrypted Data	426
Encrypted Data Sizes	429
Hashing	432
DBMS_CRYPTO Hashing	433
Message Authentication Codes	435
Performance	437
Key Management	441
Key Management Options	442
The Best Key Management Strategy	450

PART V
Appendixes

A	Setting Up the Security Manager	453
B	DATA_CRYPT0 Package	457
C	DBMS_CRYPT0 Performance Test Results	479
	Index	489