Contents

Introduction **1**

PART ONE: SECURING BUSINESS DATA

Chapter 1: How the Mainframe Provides Security **7**
- How RACF Does Access Checking 9
- The RACF Access Checking Diagram 10

Chapter 2: RACF Special Privileges **13**
- Logging Special Privilege Activities 14
- Mitigating the Risk of Special Privileges 15
- Alternatives to the OPERATIONS Privilege 16
- Summary 17

Chapter 3: The Data Security Monitor (DSMON) **19**
- How to Produce DSMON Reports 20
- Understanding DSMON Reports 20
- Summary 28

Chapter 4: Security Event Logging and Auditing **29**
- Auditing User Activity 31
- Auditing Resources at the Profile Level 31
- Using the GLOBALAUDIT Operand 32
- Auditing Resources at the Class Level 32
- Auditing Users with Special Privileges 34

Auditing Profile Changes 34
Auditing Failures to RACF Commands 35
RACF Automatic Loggings 35
The Importance of Security Log Retention 35
Summary 37

Chapter 5: The Global Access Checking (GAC) Table 39
The Benefits of GAC 40
The Security Concerns of GAC 40
Implementing GAC 41
Mitigating the Security Risks of GAC 42
The Benefits of GAC Mirror Profiles 44
Good Candidates for GAC Processing 45
Summary 46

Chapter 6: Understanding the FACILITY Class 49
Storage Administration Profiles 50
z/OS UNIX Profiles 50
RACF Profiles 50
Other Profiles 51
Security Administration of FACILITY Class Profiles 51
The FACILITY Class's Documentation 52
Third-Party Vendor Products 52
In-House Developed Products 52
FACILITY Class Profiles: A Word of Caution 52

Chapter 7: The Benefits of the SEARCH Command 55
Creating RACF Commands 55
Cleaning Up the RACF Database 56
Listing Profiles, User IDs, and Groups 57
Revoking User IDs 57
Finding Duplicate UIDs and GIDs 58
Searching a User's Access to Profiles 59
Finding Discrete Profiles 59
Summary 59

Chapter 8: WARNING Mode and Its Implications 61
The Proper Use of WARNING Mode 62
The Incorrect Use of WARNING Mode 63
Finding All Profiles in WARNING Mode 63
Make Sure WARNING Mode Is Justified 64
Remove WARNING Mode Where Inappropriate 64
Summary 64

Chapter 9: Understanding z/OS UNIX Security 65
How z/OS UNIX Security Works 66
Planning for z/OS UNIX Security 67
Unique UIDs and GIDs Recommended 68
The SUPERUSER Privilege 69
Auditing z/OS UNIX 70
Implementing z/OS UNIX Controls 71
FACILITY Class Considerations 71
UNIXPRIV Class Considerations 73
Other z/OS UNIX Considerations 73

Chapter 10: The Benefits of RACF Commands in Batch Mode 75
Capturing the Results of RACF Commands 76
Automating a Process 77
Performing an Action Repeatedly 77
Entering Groups of RACF Commands 78
When Batch Mode Is the Only Method 79
Summary 79

Chapter 11: Security Administration: Beyond the Basics 81
Doing It Right the First Time 82
Being Inquisitive 84
Understanding RACF User Profile Segments 86
What Is a RACF Discrete Profile? 87
What Are Undefined RACF User IDs? 88
Universal Access (UACC) Considerations 89
The Restricted Attribute 90

Disaster Recovery Considerations 90
What Are RACF "Grouping Classes"? 91
What Is RACF "Undercutting"? 92
What Is a RACF "Back-Stop" Profile? 92
Why User IDs Must Not Be Shared 93
Granting Temporary Access to Resources 94
Creating "Fully-Qualified" Generic Profiles 94
Specifying Strong Passwords 95
RACF Global Options 96
Summary 99

PART TWO: SECURING THE z/OS OPERATING SYSTEM

Chapter 12: APF-Authorized Libraries 103
What Is the Risk? 103
Finding APF-Authorized Libraries 104
How Do You Mitigate This Risk? 105
Summary 107

Chapter 13: The System Management Facility (SMF) 109
What Is the Risk? 110
How Do You Mitigate This Risk? 110
Summary 112

Chapter 14: Operating System Data Sets 113
System Parameter Libraries 113
System Catalogs 115
Assorted Operating System Data Sets 116
Summary 117

Chapter 15: RACF Databases 119
What Is the Risk? 119
How Do You Mitigate This Risk? 120
Summary 122

Chapter 16: RACF Exits 123
What Is the Risk? 124
How Do You Mitigate This Risk? 124
Summary 126

Chapter 17: System Exits 127
What Is the Risk? 128
How Do You Mitigate This Risk? 128
Summary 128

Chapter 18: Started Procedures 131
What Is the Risk? 132
How Do You Mitigate This Risk? 133
Summary 135

Chapter 19: Tape Bypass Label Processing (BLP) 137
What Is the Risk? 137
How Do You Mitigate This Risk? 139
Summary 139

Chapter 20: The SYS1.UADS Data Set 141
A Brief History of SYS1.UADS 142
How SYS1.UADS Works with RACF 143
Keeping SYS1.UADS Current 144
Summary 145

Chapter 21: The System Display and Search Facility (SDSF) 147
What Is the Risk? 147
How Do You Mitigate This Risk? 148

Chapter 22: The Program Properties Table (PPT) 151
What Is the Risk? 151
How Do You Mitigate This Risk? 152

Chapter 23: Special-Use Programs 155
What Is the Risk? 156
How Do You Mitigate This Risk? 156

PART THREE: SECURITY INFRASTRUCTURE MATTERS

Chapter 24: Application and Batch ID Security 159
Segregate Production from Non-Production 159
Batch IDs Must Not Share Application Data 160
Production JCL Must Not Refer to Personal Data Sets 160
Be Careful About SURROGAT Class Access 161
Restrict Direct Update Access to Production Data 162

Chapter 25: Security Architecture 163
Internal Vs. External Security 164
The Benefits of External (RACF) Security 165
Centralized Security or Decentralized Security? 166

Chapter 26: The RACF Unload Database 169
How It Was Done Before 170
Creating the RACF Unload Database 170
The Benefits of the RACF Unload Database 171
The Uses of the RACF Unload Database 171
Getting Quick Answers Using TSO 173
Summary 176

Chapter 27: Increasing Your Productivity 177
Use REXX and CLISTs 178
Learn More About ISPF Edit Capabilities 178
Join Online User Groups 180
Find a Mentor 180
Use RACF Help Functions 181
Use Online Manuals 181
Get Free Utilities 182
Subscribe to Vendor Publications 182
Use Native RACF Commands 183
Learn DFSORT 183
Summary 183

Chapter 28: Security Compliance 185

Chapter 29: Security Best Practices 187

Implement Role-Based Security 188
Periodically De-Clutter Your Security Database 190
Handle Employee Transfers and Terminations As They Occur 190
Identify Your Important Data 191
Assign Ownership to All Data 192
Keep All Security Within RACF 193
Log Accesses to Important Data 193
Conduct Periodic Reviews of All Access Rights 193
Implement Change Management for Production JCL 194
Report and Monitor Security Activities 195
Implement Segregation of Duties 196
Require Approval Before Granting Access 196
Summary 196

Chapter 30: Security Add-On Products 197

The Benefits of RACF Add-On Products 198
Simplified Security Administration 199
Security Monitoring 199
Password Resets 200
Security Reporting 200
Security Compliance and Enforcement 200
Summary 200

Epilogue 201

Index 203