## Contents

Preface ............................................. xv

Acknowledgments .................................. xix

1 Introduction ................................... 1

1.1 The purpose and fundamentals of access control 2
    1.1.1 Authorization versus authentication 3
    1.1.2 Users, subjects, objects, operations, and permissions 4
    1.1.3 Least privilege 5

1.2 A brief history of access control 6
    1.2.1 Access control in the mainframe era 6
    1.2.2 Department of Defense standards 8
    1.2.3 Clark-Wilson model 9
    1.2.4 Origins of RBAC 9

1.3 Comparing RBAC to DAC and MAC 17

1.4 RBAC and the enterprise 18
    1.4.1 Economics of RBAC 19
    1.4.2 Authorization management and resource provisioning 20

References ........................................ 24

2 Access Control: Properties, Policies, and Models ....................................... 27

2.1 Access control: objectives and enforcement artifacts 27

2.2 Access control: core entities and principles 30
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1 Subjects and objects</td>
<td>30</td>
</tr>
<tr>
<td>2.2.2 Principles of secure design</td>
<td>31</td>
</tr>
<tr>
<td>2.3 Reference monitor and security kernel</td>
<td>33</td>
</tr>
<tr>
<td>2.3.1 Completeness</td>
<td>34</td>
</tr>
<tr>
<td>2.3.2 Isolation</td>
<td>35</td>
</tr>
<tr>
<td>2.3.3 Verifiability</td>
<td>36</td>
</tr>
<tr>
<td>2.3.4 The reference monitor—necessary, but not sufficient</td>
<td>37</td>
</tr>
<tr>
<td>2.4 Access control matrix</td>
<td>37</td>
</tr>
<tr>
<td>2.5 Access control data structures</td>
<td>42</td>
</tr>
<tr>
<td>2.5.1 Capability lists and access control lists (ACLs)</td>
<td>42</td>
</tr>
<tr>
<td>2.5.2 Protection bits</td>
<td>44</td>
</tr>
<tr>
<td>2.6 Discretionary access control (DAC) policies</td>
<td>44</td>
</tr>
<tr>
<td>2.7 MAC policies and models</td>
<td>45</td>
</tr>
<tr>
<td>2.7.1 Bell-LaPadula model</td>
<td>46</td>
</tr>
<tr>
<td>2.8 Biba’s integrity model</td>
<td>47</td>
</tr>
<tr>
<td>2.9 The Clark-Wilson model</td>
<td>48</td>
</tr>
<tr>
<td>2.10 The Chinese wall policy model</td>
<td>50</td>
</tr>
<tr>
<td>2.11 The Brewer-Nash model</td>
<td>51</td>
</tr>
<tr>
<td>2.12 Domain-type enforcement (DTE) model</td>
<td>52</td>
</tr>
<tr>
<td>References</td>
<td>54</td>
</tr>
<tr>
<td>3 Core RBAC Features</td>
<td>57</td>
</tr>
<tr>
<td>3.1 Roles versus ACL groups</td>
<td>59</td>
</tr>
<tr>
<td>3.2 Core RBAC</td>
<td>61</td>
</tr>
<tr>
<td>3.2.1 Administrative support</td>
<td>61</td>
</tr>
<tr>
<td>3.2.2 Permissions</td>
<td>62</td>
</tr>
<tr>
<td>3.2.3 Role activation</td>
<td>64</td>
</tr>
<tr>
<td>3.3 Mapping the enterprise view to the system view</td>
<td>65</td>
</tr>
<tr>
<td>3.3.1 Global users and roles and indirect role privileges</td>
<td>68</td>
</tr>
<tr>
<td>3.3.2 Mapping permissions into privileges</td>
<td>69</td>
</tr>
<tr>
<td>4 Role Hierarchies</td>
<td>73</td>
</tr>
<tr>
<td>4.1 Building role hierarchies from flat roles</td>
<td>74</td>
</tr>
<tr>
<td>4.2 Inheritance schemes</td>
<td>75</td>
</tr>
<tr>
<td>4.2.1 Direct privilege inheritance</td>
<td>75</td>
</tr>
<tr>
<td>4.2.2 Permission and user membership inheritance</td>
<td>76</td>
</tr>
</tbody>
</table>
6.2.2 Configuring RBAC for MAC using dynamic constraints

6.3 Implementing RBAC on MLS systems
   6.3.1 Roles and privilege sets
   6.3.2 Assignment of categories to privilege sets
   6.3.3 Assignment of categories to roles
   6.3.4 Example of MLS to RBAC mapping

6.4 Running RBAC and MAC simultaneously

References

7 Privacy and Regulatory Issues

7.1 Privacy requirements and access control framework
   7.1.1 Incorporating privacy policies into the policy specification module
   7.1.2 Enhance RBAC model with privacy-related entities and relationships
   7.1.3 Justifications for additional entities in the RBAC model
   7.1.4 Business purpose entity
   7.1.5 Data usage entity
   7.1.6 Privacy-aware RBAC model

7.2 Integrate privacy policy support in the role engineering process
   7.2.1 Identifying business purposes and role-business purpose relationship instances
   7.2.2 Identifying business purpose-task relationship instances
   7.2.3 Identifying data usage entities and data usage-data object relationship instances

7.3 Authorization using privacy-RBAC-ACF

7.4 RBAC and regulatory compliance
   7.4.1 Sarbanes-Oxley Act compliance
   7.4.2 Gramm-Leach-Bliley Act and HIPAA compliance
   7.4.3 Compliance and the RBAC model
   7.4.4 Considerations in using RBAC in regulatory compliance

References

8 RBAC Standards and Profiles

8.1 The ANSI/INCITS RBAC standard
   8.1.1 Overview
   8.1.2 The RBAC reference model
   8.1.3 Functional specification overview
   8.1.4 Functional specification for core RBAC
8.1.5 Functional specification for hierarchical RBAC ............................................. 176
8.1.6 Functional specification for static separation of duty (SSD) relation .............. 179
8.1.7 Functional specification for a DSD relation ................................................ 180
8.1.8 Options and packaging ................................................................................. 181
8.1.9 Other RBAC standards ................................................................................ 183

8.2 XACML profile for role-based access control .................................................... 185
References ............................................................................................................. 186

9 Role-Based Administration of RBAC ................................................................. 189

9.1 Background and terminology ......................................................................... 189
9.2 URA02 and PRA02 .......................................................................................... 192
9.3 Crampton-Loizou administrative model .......................................................... 196
  9.3.1 Flexibility of administrative scope .............................................................. 197
  9.3.2 Decentralization and autonomy ................................................................. 198
  9.3.3 A family of models for hierarchical administration ..................................... 198
9.4 Role control center .......................................................................................... 203
  9.4.1 Inheritance and the role graph .................................................................. 204
  9.4.2 Constraints .................................................................................................. 206
  9.4.3 Role views ................................................................................................... 206
  9.4.4 Delegation of administrative permissions .................................................... 207
  9.4.5 Decentralization and autonomy .................................................................. 210
References ............................................................................................................. 212

10 Role Engineering ................................................................................................ 213

10.1 Scenario-driven role-engineering approach ................................................. 215
  10.1.1 Scenarios and roles ..................................................................................... 216
  10.1.2 Steps in the scenario-driven process ............................................................. 217
10.2 Goal driven/hybrid role engineering approach ............................................... 220
10.3 Tools for role discovery and role management ............................................... 224
  10.3.1 Sage DNA .................................................................................................. 226
  10.3.2 Role Miner .................................................................................................. 227
  10.3.3 SmartRoles .................................................................................................. 228
  10.3.4 Contouring Engine ...................................................................................... 229
10.4 Example RBAC installations .......................................................................... 229
10.5 Role engineering: health care example ............................................................ 232
  10.5.1 Identify and model usage scenarios .............................................................. 232
11 Enterprise Access Control Frameworks
Using RBAC and XML Technologies . . . . . 239

11.1 Conceptual view of EAFs 239
11.2 Enterprise Access Central Model Requirements 242
  11.2.1 EAM's multiple-policy support requirement 243
  11.2.2 EAM's ease of administration requirement 243
11.3 EAM specification and XML schemas 244
11.4 Specification of the ERBAC model in the XML schema 246
  11.4.1 XML schema specifications for ERBAC model elements 247
  11.4.2 XML schema specifications for ERBAC model relations 250
11.5 Encoding of enterprise access control data in XML 253
11.6 Verification of the ERBAC model and data specifications 257
11.7 Limitations of XML schemas for ERBAC model constraint representation 258
11.8 Using XML-encoded enterprise access control data for enterprisewide access control implementation 262
11.9 Conclusions 268
References 268

12 Integrating RBAC with Enterprise IT Infrastructures . . . . . . . . . . . . . 271

12.1 RBAC for WFMSs 272
  12.1.1 Workflow concepts and WFMSs 272
  12.1.2 WFMS components and access control requirements 273
  12.1.3 Access control design requirements 274
  12.1.4 RBAC model design and implementation requirements for WFMSs 276
  12.1.5 RBAC for workflows—research prototypes 279
12.2 RBAC integration in Web environments 280
  12.2.1 Implementing RBAC entirely on the Web server 281
12.2.2 Implementing RBAC for Web server access using cookies 282
12.2.3 RBAC on the Web using attribute certificates 284

12.3 RBAC for UNIX environments 291
12.3.1 RBAC for UNIX administration 291
12.3.2 RBAC implementation within the NFS 296

12.4 RBAC in Java 299
12.4.1 Evolution of Java security models 300
12.4.2 JDK 1.2 security model and enhancement 301
12.4.3 Incorporating RBAC into JDK 1.2 security model with JAAS 304

12.5 RBAC for FDBSs 306
12.5.1 IRO-DB architecture 307
12.5.2 RBAC model implementation in IRO-DB 308

12.6 RBAC in autonomous security service modules 309

12.7 Conclusions 311
References 311

13 Migrating to RBAC—Case Study: Multiline Insurance Company 315

13.1 Background 316

13.2 Benefits of using RBAC to manage extranet users 316
13.2.1 Simplifying systems administration and maintenance 318
13.2.2 Enhancing organizational productivity 319

13.3 Benefits of using RBAC to manage employees (intranet users) 319
13.3.1 Reduction in new employee downtime 319
13.3.2 Simplified systems administration and maintenance 320

13.4 RBAC implementation costs 320
13.4.1 Software and hardware expenses 321
13.4.2 Systems administrators' labor expenses 321
13.4.3 Role engineering expenses 321

13.5 Time series of benefits and costs 322
Reference 324

14 RBAC Features in Commercial Products 325

14.1 RBAC in relational DBMS products 326
14.1.1 Informix Dynamic Server version 9.3 (IBM) 327
14.1.2 Oracle Database 10g Release (10.2) (Oracle Corporation) 329
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1.3 Sybase Adaptive Server Enterprise 15.0 (Sybase)</td>
<td>333</td>
</tr>
<tr>
<td>14.2 RBAC in enterprise security administration software</td>
<td>340</td>
</tr>
<tr>
<td>14.2.1 CONTROL-SA (BMC software)</td>
<td>342</td>
</tr>
<tr>
<td>14.2.2 DirX Identity V7.0 (Siemens)</td>
<td>346</td>
</tr>
<tr>
<td>14.2.3 SAM Jupiter (Beta Systems)</td>
<td>351</td>
</tr>
<tr>
<td>14.2.4 Tivoli Identity Manager version 1.1 (IBM)</td>
<td>356</td>
</tr>
<tr>
<td>14.3 Conclusions</td>
<td>359</td>
</tr>
<tr>
<td>References</td>
<td>360</td>
</tr>
</tbody>
</table>

**Appendix A: XML Schema for the RBAC Model** 361

**Appendix B: XML-Encoded Data for RBAC Model** 365

**About the Authors** 369

**Index** 371