

Anirban Chakrabarti

# Grid Computing Security

With 87 Figures and 12 Tables

 Springer

# Contents

- Preface .....v**
  - Organization .....vi
  - Acknowledgments .....vii
- 1 Introduction..... 1**
  - 1.1 Background..... 1
  - 1.2 Grid Computing Overview ..... 3
    - 1.2.1 Evolution of Grid Computing ..... 4
    - 1.2.2 Benefits of Grid Computing..... 6
    - 1.2.3 Grid Computing Issues and Concerns..... 8
  - 1.3 About the Book..... 11
    - 1.3.1 Target Audience ..... 12
    - 1.3.2 Organization of the Book..... 12
- 2 Overview of Security ..... 15**
  - 2.1 Introduction ..... 15
    - 2.1.1 Characteristics of Secure System ..... 15
    - 2.1.2 Security Threats ..... 16
  - 2.2 Different Encryption Schemes..... 17
  - 2.3 Different Authentication Schemes..... 20
    - 2.3.1 Shared Secret Based Authentication ..... 20
    - 2.3.2 Public Key Based Authentication ..... 21
    - 2.3.3 Third Party Authentication Schemes ..... 21
  - 2.4 Different Integrity Schemes..... 22
    - 2.4.1 Message Authentication Code (MAC)..... 22
    - 2.4.2 Keyed MAC ..... 23
  - 2.5 Standard Protocols ..... 24
    - 2.5.1 Public Key Infrastructure ..... 24
    - 2.5.2 Secure Socket Layer (SSL) ..... 27
    - 2.5.3 Kerberos ..... 27
    - 2.5.4 IP Security (IPSec)..... 29
  - 2.6 Chapter Summary ..... 31

|                                                            |               |
|------------------------------------------------------------|---------------|
| <b>3 Taxonomy of Grid Security Issues .....</b>            | <b>33</b>     |
| 3.1 Introduction .....                                     | 33            |
| 3.1.1 Grid Security Taxonomy .....                         | 35            |
| 3.2 Architecture Related Issues .....                      | 36            |
| 3.2.1 Information Security .....                           | 36            |
| 3.2.2 Authorization .....                                  | 37            |
| 3.2.3 Service Security .....                               | 38            |
| 3.3 Infrastructure Related Issues.....                     | 40            |
| 3.3.1 Host Security Issues .....                           | 40            |
| 3.3.2 Network Security Issues.....                         | 41            |
| 3.4 Management Related Issues .....                        | 42            |
| 3.4.1 Credential Management .....                          | 43            |
| 3.4.2 Trust Management .....                               | 44            |
| 3.4.3 Monitoring .....                                     | 45            |
| 3.5 Chapter Summary .....                                  | 46            |
| <br><b>4 Grid Information Security Architecture .....</b>  | <br><b>49</b> |
| 4.1 Introduction .....                                     | 49            |
| 4.2 Grid Security Infrastructure (GSI).....                | 50            |
| 4.2.1 Grid Security Model.....                             | 52            |
| 4.3 Authentication in GSI.....                             | 54            |
| 4.3.1 Certificate based Authentication .....               | 54            |
| 4.3.2 Password based Authentication .....                  | 57            |
| 4.3.3 Integration with Kerberos .....                      | 59            |
| 4.4 Delegation in GSI .....                                | 59            |
| 4.5 An Example: Security in Globus Toolkit 4.0 (GT4) ..... | 61            |
| 4.5.1 Message Protection in GT4.....                       | 61            |
| 4.5.2 Delegation in GT4.....                               | 64            |
| 4.6 Chapter Summary .....                                  | 65            |
| <br><b>5 Grid Authorization Systems .....</b>              | <br><b>67</b> |
| 5.1 Introduction .....                                     | 67            |
| 5.1.1 Different Access Control Models.....                 | 69            |
| 5.1.2 Push vs. Pull Authorizations .....                   | 72            |
| 5.2 Characteristics of Grid Authorization Systems .....    | 74            |
| 5.2.1 Scalability Issues.....                              | 75            |
| 5.2.2 Security Issues .....                                | 76            |
| 5.2.3 Revocation Issues.....                               | 77            |
| 5.2.4 Inter-operability Issues.....                        | 79            |
| 5.2.5 Grid Authorization Systems.....                      | 79            |

---

|          |                                                                                             |            |
|----------|---------------------------------------------------------------------------------------------|------------|
| 5.3      | VO Level Authorization Systems .....                                                        | 80         |
| 5.3.1    | Community Authorization Service (CAS) .....                                                 | 80         |
| 5.3.2    | Virtual Organization Membership Service (VOMS) .....                                        | 87         |
| 5.3.3    | Enterprise Authorization and Licensing Service (EALS) ....                                  | 88         |
| 5.4      | Resource Level Authorization Systems .....                                                  | 90         |
| 5.4.1    | Akenti .....                                                                                | 90         |
| 5.4.2    | Privilege and Role Management Infrastructure Standards<br>Validation (PERMIS) Project ..... | 94         |
| 5.4.3    | Authorization Using GridMap .....                                                           | 100        |
| 5.5      | Comparing the Different Authorization Systems .....                                         | 100        |
| 5.5.1    | Comparison .....                                                                            | 100        |
| 5.5.2    | Roadmap to Grid Authorization Systems .....                                                 | 103        |
| 5.6      | Chapter Summary .....                                                                       | 103        |
| <b>6</b> | <b>Service Level Security in Grid Systems .....</b>                                         | <b>105</b> |
| 6.1      | Introduction .....                                                                          | 105        |
| 6.1.1    | Components of Service .....                                                                 | 106        |
| 6.1.2    | Service Vulnerabilities .....                                                               | 106        |
| 6.2      | DoS Attacks and Countermeasures .....                                                       | 108        |
| 6.2.1    | Effect of DoS attacks .....                                                                 | 108        |
| 6.2.2    | Distributed Denial-of-Service Attacks .....                                                 | 111        |
| 6.2.3    | Existing DoS Countermeasures .....                                                          | 118        |
| 6.2.4    | Preventive DoS Counter-measures .....                                                       | 119        |
| 6.2.5    | Reactive DoS Countermeasures .....                                                          | 123        |
| 6.2.6    | Comparison between DoS Countermeasures .....                                                | 126        |
| 6.3      | QoS Violation Attacks and Countermeasures .....                                             | 127        |
| 6.3.1    | Different Types of QoS Violation Attacks .....                                              | 128        |
| 6.3.2    | Existing Solutions .....                                                                    | 129        |
| 6.4      | Chapter Summary .....                                                                       | 131        |
| <b>7</b> | <b>Host Level Security .....</b>                                                            | <b>133</b> |
| 7.1      | Introduction .....                                                                          | 133        |
| 7.2      | Data Protection Issue .....                                                                 | 135        |
| 7.2.1    | Application Level Sandboxing .....                                                          | 136        |
| 7.2.2    | Virtualization .....                                                                        | 138        |
| 7.2.3    | Flexible Kernel Systems .....                                                               | 145        |
| 7.2.4    | Sandboxing .....                                                                            | 149        |
| 7.3      | Job Starvation Issue .....                                                                  | 154        |
| 7.3.1    | Advanced Reservation Techniques .....                                                       | 155        |
| 7.3.2    | Priority Reduction Techniques .....                                                         | 156        |
| 7.4      | Chapter Summary .....                                                                       | 157        |

|                                                              |                |
|--------------------------------------------------------------|----------------|
| <b>8 Grid Network Security .....</b>                         | <b>159</b>     |
| 8.1 Introduction .....                                       | 159            |
| 8.1.1 Grid Network Security Issues .....                     | 159            |
| 8.2 Firewalls .....                                          | 161            |
| 8.2.1 Different Types of Firewalls .....                     | 163            |
| 8.2.2 Firewalls and Grid – Issues .....                      | 165            |
| 8.2.3 Firewalls and Web Services .....                       | 167            |
| 8.3 Virtual Private Networks (VPN) .....                     | 168            |
| 8.3.1 VPNs and Grid – Types of VPNs .....                    | 169            |
| 8.3.2 VPNs and Grid – Issues .....                           | 170            |
| 8.3.3 VPNs and Grid – Some Solutions .....                   | 171            |
| 8.4 Secure Routing .....                                     | 173            |
| 8.4.1 Impacts of Routing Table “Poisoning” .....             | 173            |
| 8.4.2 Different Routing Protocols .....                      | 175            |
| 8.4.3 Routing Attacks and Countermeasures .....              | 175            |
| 8.5 Multicasting .....                                       | 178            |
| 8.5.1 Secure Multicasting .....                              | 178            |
| 8.6 Sensor Grids .....                                       | 182            |
| 8.6.1 Security in Sensor Networks – Issues .....             | 183            |
| 8.6.2 Existing Solutions .....                               | 186            |
| 8.7 High Performance Interconnects .....                     | 188            |
| 8.7.1 10-Gigabit Ethernet .....                              | 188            |
| 8.7.2 Infiniband Architecture (IBA) .....                    | 188            |
| 8.7.3 Some High Performance Security Solutions .....         | 189            |
| 8.8 Chapter Summary .....                                    | 190            |
| <br><b>9 Grid Credential Management Systems .....</b>        | <br><b>193</b> |
| 9.1 Introduction .....                                       | 193            |
| 9.1.1 Types of Credentials .....                             | 194            |
| 9.1.2 Characteristics of Credential Management Systems ..... | 195            |
| 9.1.3 Different Credential Management Systems .....          | 197            |
| 9.1.4 Centralized Vs. Federated Credential Management .....  | 198            |
| 9.2 Credential Repositories .....                            | 200            |
| 9.2.1 Smart Cards .....                                      | 200            |
| 9.2.2 Virtual Smart Cards .....                              | 201            |
| 9.2.3 MyProxy Online Credential Repository .....             | 202            |
| 9.3 Federated Credential Management Systems .....            | 205            |
| 9.3.1 Virtualized Credential Manager (VCMan) .....           | 206            |
| 9.3.2 KX.509 .....                                           | 208            |
| 9.3.3 Liberty Alliance for Federated Identity .....          | 209            |
| 9.3.4 Shibboleth Identity Federation .....                   | 210            |
| 9.4 Chapter Summary .....                                    | 212            |

---

|                                                                |                |
|----------------------------------------------------------------|----------------|
| <b>10 Managing Trust in the Grid.....</b>                      | <b>215</b>     |
| 10.1 Introduction .....                                        | 215            |
| 10.1.1 Definition of Trust.....                                | 215            |
| 10.1.2 Reputation and Trust .....                              | 217            |
| 10.1.3 Categories of Trust Functions .....                     | 218            |
| 10.2 Trust Management Systems.....                             | 221            |
| 10.2.1 Life Cycle of Trust Management Systems .....            | 223            |
| 10.2.2 Characteristics of Trust Management Systems .....       | 225            |
| 10.3 Reputation-Based Trust Management Systems .....           | 228            |
| 10.3.1 PeerTrust – A P2P Trust Management System .....         | 228            |
| 10.3.2 XenoTrust Trust Management System .....                 | 231            |
| 10.3.3 NICE Trust Management System.....                       | 233            |
| 10.3.4 Secure Grid Outsourcing (SeGO) System .....             | 236            |
| 10.4 Policy-Based Trust Management Systems .....               | 238            |
| 10.4.1 PeerTrust Trust Negotiation .....                       | 238            |
| 10.4.2 TrustBuilder.....                                       | 240            |
| 10.4.3 Trust Negotiation for the Grid.....                     | 242            |
| 10.5 Comparing the Trust Management Systems .....              | 243            |
| 10.5.1 Generic Understanding of Trust Management Systems ..... | 243            |
| 10.5.2 Applicability of the Trust Management Systems .....     | 245            |
| 10.6 Chapter Summary .....                                     | 246            |
| <br><b>11 Grid Monitoring.....</b>                             | <br><b>247</b> |
| 11.1 Introduction .....                                        | 247            |
| 11.1.1 Stages of Monitoring .....                              | 248            |
| 11.1.2 Requirements of Distributed Monitoring System.....      | 250            |
| 11.2 Grid Monitoring Architecture (GMA).....                   | 251            |
| 11.3 Different Monitoring Tools/Frameworks .....               | 253            |
| 11.3.1 Simple Network Management Protocol (SNMP).....          | 254            |
| 11.3.2 Different System Monitoring Tools .....                 | 255            |
| 11.3.3 Ganglia .....                                           | 256            |
| 11.3.4 Hawkeye Monitoring System .....                         | 258            |
| 11.3.5 Relational GMA (RGMA).....                              | 259            |
| 11.3.6 Globus Monitoring and Discovery System (MDS) .....      | 261            |
| 11.3.7 Management of Adaptive Grid Infrastructure (MAGI) ..... | 263            |
| 11.3.8 GlueDomains.....                                        | 265            |
| 11.4 Discussions on the Different Monitoring Systems .....     | 266            |
| 11.4.1 Comparison .....                                        | 266            |
| 11.4.2 Applicability .....                                     | 268            |
| 11.5 Chapter Summary .....                                     | 269            |

|                                                           |            |
|-----------------------------------------------------------|------------|
| <b>12 Putting it All Together.....</b>                    | <b>271</b> |
| 12.1 Security in the European Data Grid (EDG).....        | 271        |
| 12.1.1 Authentication and Delegation.....                 | 271        |
| 12.1.2 Credential Management.....                         | 272        |
| 12.1.3 Job Execution .....                                | 272        |
| 12.2 An Enterprise Case Study.....                        | 274        |
| 12.2.1 Overview of the Security Architecture.....         | 275        |
| 12.3 Chapter Summary.....                                 | 278        |
| <b>13 Conclusion .....</b>                                | <b>281</b> |
| 13.1 Looking at the Future .....                          | 281        |
| 13.1.1 Identity Based Encryption (IBE).....               | 281        |
| 13.1.2 Application Oriented Networking (AON).....         | 282        |
| 13.2 Summarizing the Security Issues in Grid .....        | 283        |
| 13.2.1 Immediate Issues .....                             | 284        |
| 13.2.2 Medium-term Issues .....                           | 285        |
| 13.2.3 Long-term Issues .....                             | 287        |
| 13.3 Summarizing the Security Solutions in the Grid ..... | 289        |
| 13.3.1 Solutions to Immediate Issues .....                | 289        |
| 13.3.2 Solutions to Medium Term Issues.....               | 290        |
| 13.3.3 Solutions to Long Term Issues .....                | 291        |
| <b>Appendix.....</b>                                      | <b>293</b> |
| A.1 Web Services .....                                    | 293        |
| A.1.1 Components of Web Services .....                    | 294        |
| A.2 Web Services Security.....                            | 296        |
| A.2.1 WS-Security .....                                   | 299        |
| A.2.2 WS-Policy* .....                                    | 301        |
| A.2.3 WS-SecureConversation.....                          | 302        |
| A.2.4 Security Assertions Markup Language (SAML).....     | 304        |
| A.2.5 eXtensible Access Control Markup Language .....     | 306        |
| A.3 Open Grid Services Architecture (OGSA) .....          | 307        |
| A.3.1 Open Grid Services Infrastructure (OGSI).....       | 308        |
| A.3.2 Web Services Critique of OGSI .....                 | 309        |
| A.3.2 Web Services Resource Framework (WSRF) .....        | 310        |
| <b>Bibliography.....</b>                                  | <b>313</b> |
| <b>Index.....</b>                                         | <b>329</b> |