Contents

List of Figures xv

List of Tables xvii

Foreword xix

Preface xxii

Chapter 1 Introduction 1

1.1 Background 1

1.2 Distributed Systems 2

1.2.1 Characteristics of Distributed Systems 2

1.2.2 Types of Distributed System 3

1.2.3 Different Distributed Architectures 7

1.2.4 Challenges in Designing Distributed Systems 9

1.3 Distributed Systems Security 12

1.3.1 Enterprise IT – A Layered View 12

1.3.2 Trends in IT Security 15

1.4 About the Book 18

1.4.1 Target Audience 18

References 19

Chapter 2 Security Engineering 21

2.1 Introduction 21

2.2 Secure Development Lifecycle Processes – An Overview 22

2.2.1 Systems Security Engineering Capability Maturity Model (SSE-CMM) 23

2.2.2 Microsoft’s Security Development Lifecycle (SDL) 24

2.2.3 Comprehensive Lightweight Application Security Process (CLASP) 27

2.2.4 Build Security In 29

2.3 A Typical Security Engineering Process 30

2.3.1 Requirements Phase 31

2.3.2 Architecture and Design Phase 32
2.3.3 Development (Coding) Phase
2.3.4 Testing Phase
2.4 Important Security Engineering Guidelines and Resources
2.4.1 Security Requirements
2.4.2 Architecture and Design
2.4.3 Secure Coding
2.4.4 Security Testing
2.5 Conclusion
References

Chapter 3 Common Security Issues and Technologies

3.1 Security Issues
3.1.1 Authentication
3.1.2 Authorization
3.1.3 Data Integrity
3.1.4 Confidentiality
3.1.5 Availability
3.1.6 Trust
3.1.7 Privacy
3.1.8 Identity Management
3.2 Common Security Techniques
3.2.1 Encryption
3.2.2 Digital Signatures and Message Authentication Codes
3.2.3 Authentication Mechanisms
3.2.4 Public Key Infrastructure (PKI)
3.2.5 Models of Trust
3.2.6 Firewalls
3.3 Conclusion
References

Chapter 4 Host-Level Threats and Vulnerabilities

4.1 Background
4.1.1 Transient Code Vulnerabilities
4.1.2 Resident Code Vulnerabilities
4.2 Malware
4.2.1 Trojan Horse
4.2.2 Spyware
4.2.3 Worms/Viruses
4.3 Eavesdropping
4.3.1 Unauthorized Access to Confidential Data – by Users
4.3.2 Unauthorized Access to Protected or Privileged Binaries – by Users
4.3.3 Unauthorized Tampering with Computational Results
4.3.4 Unauthorized Access to Private Data – by Jobs
4.4 Job Faults
<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Infrastructure-Level Threats and Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Introduction</td>
</tr>
<tr>
<td>5.2</td>
<td>Network-Level Threats and Vulnerabilities</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Denial-of-Service Attacks</td>
</tr>
<tr>
<td>5.2.2</td>
<td>DNS Attacks</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Routing Attacks</td>
</tr>
<tr>
<td>5.2.4</td>
<td>Wireless Security Vulnerabilities</td>
</tr>
<tr>
<td>5.3</td>
<td>Grid Computing Threats and Vulnerabilities</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Architecture-Related Issues</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Infrastructure-Related Issues</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Management-Related Issues</td>
</tr>
<tr>
<td>5.4</td>
<td>Storage Threats and Vulnerabilities</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Security in Storage Area Networks</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Security in Distributed File Systems</td>
</tr>
<tr>
<td>5.5</td>
<td>Overview of Infrastructure Threats and Vulnerabilities</td>
</tr>
<tr>
<td>References</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Application-Level Threats and Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Introduction</td>
</tr>
<tr>
<td>6.2</td>
<td>Application-Layer Vulnerabilities</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Injection Vulnerabilities</td>
</tr>
<tr>
<td>6.2.2</td>
<td>Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Improper Session Management</td>
</tr>
<tr>
<td>6.2.4</td>
<td>Improper Error Handling</td>
</tr>
<tr>
<td>6.2.5</td>
<td>Improper Use of Cryptography</td>
</tr>
<tr>
<td>6.2.6</td>
<td>Insecure Configuration Issues</td>
</tr>
<tr>
<td>6.2.7</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>6.2.8</td>
<td>Canonical Representation Flaws</td>
</tr>
<tr>
<td>6.2.9</td>
<td>Overflow Issues</td>
</tr>
<tr>
<td>6.3</td>
<td>Conclusion</td>
</tr>
<tr>
<td>References</td>
<td></td>
</tr>
<tr>
<td>Further Reading</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 7  Service-Level Threats and Vulnerabilities 115
7.1 Introduction 115
7.2 SOA and Role of Standards 116
  7.2.1 Standards Stack for SOA 116
7.3 Service-Level Security Requirements 117
  7.3.1 Authentication 117
  7.3.2 Authorization and Access Control 118
  7.3.3 Auditing and Nonrepudiation 118
  7.3.4 Availability 118
  7.3.5 Confidentiality 119
  7.3.6 Data Integrity 119
  7.3.7 Privacy 119
  7.3.8 Trust 119
  7.3.9 Federation and Delegation 119
7.4 Service-Level Threats and Vulnerabilities 120
  7.4.1 Anatomy of a Web Service 120
7.5 Service-Level Attacks 122
  7.5.1 Known Bug Attacks 122
  7.5.2 SQL Injection Attacks 123
  7.5.3 XPath and XQuery Injection Attacks 124
  7.5.4 Blind XPath Injection 126
  7.5.5 Cross-Site Scripting Attacks 126
  7.5.6 WSDL Probing 128
  7.5.7 Enumerating Service from WSDL 128
  7.5.8 Parameter-Based Attacks 129
  7.5.9 Authentication Attacks 131
  7.5.10 Man-in-the-Middle Attacks 133
  7.5.11 SOAP Routing Attacks 134
  7.5.12 SOAP Attachments Virus 136
  7.5.13 XML Signature Redirection Attacks 136
  7.5.14 XML Attacks 136
  7.5.15 Schema-Based Attacks 139
  7.5.16 UDDI Registry Attacks 139
7.6 Services Threat Profile 140
7.7 Conclusion 140
References 142
Further Reading 143

Chapter 8  Host-Level Solutions 145
8.1 Background 145
8.2 Sandboxing 145
  8.2.1 Kernel-Level Sandboxing 146
  8.2.2 User-Level Sandboxing 147
  8.2.3 Delegation-Based Sandboxing 148
  8.2.4 File-System Isolation 148
### 8.3 Virtualization

- **8.3.1 Full-System Virtualization**
- **8.3.2 Para Virtualization**
- **8.3.3 Shared-Kernel Virtualization**
- **8.3.4 Hosted Virtualization**
- **8.3.5 Hardware Assists**
- **8.3.6 Security Using Virtualization**
- **8.3.7 Future Security Trends Based on Virtualization**
- **8.3.8 Application Streaming**

### 8.4 Resource Management

- **8.4.1 Advance Reservation**
- **8.4.2 Priority Reduction**
- **8.4.3 Solaris Resource Manager**
- **8.4.4 Windows System Resource Manager**
- **8.4.5 Citrix ARMTech**
- **8.4.6 Entitlement-Based Scheduling**

### 8.5 Proof-Carrying Code

### 8.6 Memory Firewall

### 8.7 Antimalware

- **8.7.1 Signature-Based Protection**
- **8.7.2 Real-Time Protection**
- **8.7.3 Heuristics-Based Worm Containment**
- **8.7.4 Agent Defense**

### 8.8 Conclusion

### References

---

### Chapter 9  Infrastructure-Level Solutions

9.1 Introduction

9.2 Network-Level Solutions

- **9.2.1 Network Information Security Solutions**
- **9.2.2 Denial-of-Service Solutions**
- **9.2.3 DNS Solution – DNSSEC**
- **9.2.4 Routing Attack Solutions**
- **9.2.5 Comments on Network Solutions**

9.3 Grid-Level Solutions

- **9.3.1 Architecture Security Solutions**
- **9.3.2 Grid Infrastructure Solutions**
- **9.3.3 Grid Management Solutions**
- **9.3.4 Comments on Grid Solutions**

9.4 Storage-Level Solutions

- **9.4.1 Fiber-Channel Security Protocol (FC-SP) – Solution for SAN Security**
- **9.4.2 Distributed File System (DFS) Security**
- **9.4.3 Comments on Storage Solutions**

9.5 Conclusion

References
## Chapter 10  Application-Level Solutions 205

10.1 Introduction  
10.2 Application-Level Security Solutions  
  10.2.1 Input Validation Techniques 206  
  10.2.2 Secure Session Management 208  
  10.2.3 Cryptography Use 210  
  10.2.4 Preventing Cross-Site Scripting 213  
  10.2.5 Error-Handling Best Practices 214  
10.3 Conclusion 215  
References 215

## Chapter 11  Service-Level Solutions 217

11.1 Introduction  
11.2 Services Security Policy  
  11.2.1 Threat Classification 218  
11.3 SOA Security Standards Stack  
  11.3.1 Inadequacy of SSL for Web Services 219  
11.4 Standards in Depth  
  11.4.1 XML Signature 221  
  11.4.2 XML Encryption 221  
  11.4.3 Web-Services Security (WS Security) 223  
  11.4.4 Security Assertions Mark-Up Language (SAML) 226  
  11.4.5 WS Policy 228  
  11.4.6 WS Trust 229  
  11.4.7 WS Security Policy 234  
  11.4.8 WS Secure Conversation 234  
  11.4.9 XKMS (XML Key Management Specification) 234  
  11.4.10 WS Privacy and P3P 235  
  11.4.11 Federated Identity Standards – Liberty Alliance Project and WS Federation 238  
  11.4.12 WS-I Basic Security Profile 238  
  11.4.13 Status of Standards 240  
11.5 Deployment Architectures for SOA Security  
  11.5.1 Message-Level Security and Policy Infrastructure 241  
  11.5.2 XML Firewalls 241  
11.6 Managing Service-Level Threats  
  11.6.1 Combating SQL and XPath Injection Attacks 247  
  11.6.2 Combating Cross-Site Scripting Attacks 248  
  11.6.3 Combating Phishing and Routing Attacks 248  
  11.6.4 Handling Authentication Attacks 249  
  11.6.5 Handling Man-in-the-Middle Attacks 251  
  11.6.6 Handling SOAP Attachment Virus Attacks 253  
  11.6.7 Handling Parameter-Tampering Attacks 254  
  11.6.8 XML Attacks 254  
  11.6.9 Known-Bug Attacks 257
Chapter 12  Case Study: Compliance in Financial Services  

12.1 Introduction  
12.2 SOX Compliance  
  12.2.1 Identity Management  
  12.2.2 Policy-Based Access Control  
  12.2.3 Strong Authentication  
  12.2.4 Data Protection and Integrity  
12.3 SOX Security Solutions  
  12.3.1 People  
  12.3.2 Process  
  12.3.3 Technology  
12.4 Multilevel Policy-Driven Solution Architecture  
  12.4.1 Logical Architecture and Middleware  
12.5 Conclusion  
References  
Further Reading  

Chapter 13  Case Study: Grid  

13.1 Background  
13.2 The Financial Application  
13.3 Security Requirements Analysis  
  13.3.1 Confidentiality Requirement Analysis  
  13.3.2 Authentication Requirement Analysis  
  13.3.3 Single Sign-On and Delegation Requirement Analysis  
  13.3.4 Authorization Requirement Analysis  
  13.3.5 Identity Management Requirement Analysis  
  13.3.6 Secure Repository Requirement Analysis  
  13.3.7 Trust Management Requirement Analysis  
  13.3.8 Monitoring and Logging Requirement Analysis  
  13.3.9 Intrusion Detection Requirement Analysis  
  13.3.10 Data Protection and Isolation Requirement Analysis  
  13.3.11 Denial of Service Requirement Analysis  
13.4 Final Security Architecture  

Chapter 14  Future Directions and Conclusions  

14.1 Future Directions  
  14.1.1 Cloud Computing Security  
  14.1.2 Security Appliances
14.1.3 Usercentric Identity Management 294
14.1.4 Identity-Based Encryption (IBE) 295
14.1.5 Virtualization in Host Security 296

14.2 Conclusions 297
References 300
Further Reading 300

Index 303