Contents

Foreword **xvii**

Preface **xix**

Part I **Introduction**

Chapter 1 **Motivation and Objectives** **1**
Why Do We Need Security Patterns? 1
Some Basic Definitions 3
The History of Security Patterns 5
Industrial Use of Security Patterns 6
Other Approaches to Building Secure Systems 6

Chapter 2 **Patterns and Security Patterns** **7**
What is a Security Pattern? 7
The Nature of Security Patterns 8
Pattern Descriptions and Catalogs 10
The Anatomy of a Security Pattern 11
Pattern Diagrams 17
How Can We Classify Security Patterns? 17
Pattern Mining 19
Uses for Security Patterns 20
How to Evaluate Security Patterns and their Effect on Security 21
Threat Modeling and Misuse Patterns 22
Fault Tolerance Patterns 22

apter 3 A Secure Systems Development Methodology 23
Adding Information to Patterns 23
A Lifecycle-Based Methodology 24
Using Model-Driven Engineering 27

rt II Patterns

apter 4 Patterns for Identity Management 31
Introduction 32
Circle of Trust 34
Identity Provider 36
Identity Federation 38
Liberty Alliance Identity Federation 44

apter 5 Patterns for Authentication 51
Introduction 51
Authenticator 52
Remote Authenticator/Authorizer 56
Credential 62

apter 6 Patterns for Access Control 71
Introduction 71
Authorization 74
Role-Based Access Control 78
Multilevel Security 81
Policy-Based Access Control 84
Access Control List 91
Capability 96
Reified Reference Monitor 100
Controlled Access Session 104
Session-Based Role-Based Access Control 107
Security Logger and Auditor 111

apter 7 Patterns for Secure Process Management 117
Introduction 117
Secure Process/Thread 120
Controlled-Process Creator 126
Controlled-Object Factory 129
Controlled-Object Monitor 132
Protected Entry Points 136
Protection Rings 139

Chapter 8 Patterns for Secure Execution and File Management 145
Introduction 145
Virtual Address Space Access Control 146
Execution Domain 149
Controlled Execution Domain 151
Virtual Address Space Structure Selection 156

Chapter 9 Patterns for Secure OS Architecture and Administration 163
Introduction 163
Modular Operating System Architecture 165
Layered Operating System Architecture 169
Microkernel Operating System Architecture 174
Virtual Machine Operating System Architecture 179
Administrator Hierarchy 184
File Access Control 187

Chapter 10 Security Patterns for Networks 193
Introduction 194
Abstract Virtual Private Network 195
IPSec VPN 200
TLS Virtual Private Network 202
Transport Layer Security 205
Abstract IDS 214
Signature-Based IDS 219
Behavior-Based IDS 224

Chapter 11 Patterns for Web Services Security 231
Introduction 231
Application Firewall 234
XML Firewall 242
XACML Authorization 248
XACML Access Control Evaluation 254
Web Services Policy Language 260
WS-Policy 263
WS-Trust 272
SAML Assertion 279

hapter 12 Patterns for Web Services Cryptography 285
Introduction 286
Symmetric Encryption 288
Asymmetric Encryption 295
Digital Signature with Hashing 301
XML Encryption 309
XML Signature 317
WS-Security 330

hapter 13 Patterns for Secure Middleware 337
Introduction 337
Secure Broker 339
Secure Pipes and Filters 347
Secure Blackboard 353
Secure Adapter 358
Secure Three-Tier Architecture 362
Secure Enterprise Service Bus 366
Secure Distributed Publish/Subscribe 372
Secure Model-View-Controller 375

apter 14 Misuse Patterns 383
Introduction 383
Worm 390
Denial-of-Service in VoIP 397
Spoofing Web Services 403

apter 15 Patterns for Cloud Computing Architecture 411
Introduction 411
Infrastructure-as-a-Service 413
Platform-as-a-Service 423
Software-as-a-Service 431

rt III Use of the Patterns

apter 16 Building Secure Architectures 441
Enumerating Threats 442
The Analysis Stage 445
The Design Stage 448
Secure Handling of Legal Cases 451
SCADA Systems 459
Medical Applications 466
Conclusions 478

Chapter 17 Summary and the Future of Security Patterns 479
Summary of Patterns 479
Future Research Directions for Security Patterns 494
Security Principles 496
The Future 497

Appendix A Pseudocode for XACML Access Control Evaluation 499

Glossary 501

References 509

Index of Patterns 543

Index 547