



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

Chapter 3	A Secure Systems Development Methodology	23
	Adding Information to Patterns	23
	A Lifecycle-Based Methodology	24
	Using Model-Driven Engineering	27
Part II	Patterns	
Chapter 4	Patterns for Identity Management	31
	Introduction	32
	Circle of Trust	34
	Identity Provider	36
	Identity Federation	38
	Liberty Alliance Identity Federation	44
Chapter 5	Patterns for Authentication	51
	Introduction	51
	Authenticator	52
	Remote Authenticator/Authorizer	56
	Credential	62
Chapter 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
Chapter 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

Chapter 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
Chapter 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
Chapter 14 Misuse Patterns	383
Introduction	383
Worm	390
Denial-of-Service in VoIP	397
Spoofing Web Services	403
Chapter 15 Patterns for Cloud Computing Architecture	411
Introduction	411
Infrastructure-as-a-Service	413
Platform-as-a-Service	423
Software-as-a-Service	431
Part III Use of the Patterns	
Chapter 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

Security is a hard job. In the field of cryptography, add some firewall and password protection to the mix, and you have a very complex task.

When I started work in the field of security in the mid 1990s, I met many people who thought they could secure their applications. They used certain ingredients of security measures and applied them to whatever problems they had. Even worse sometimes they didn't use existing ingredients, but built their own—making the same errors made in hundreds of previous projects. And practice proved them wrong: security was never simple—it isn't always at least one magnitude. There's always an unexpected side effect. There's always something that you miss if you are not an expert. Front page news regularly proves that we obviously never learn.

Key reasons for insecure applications are:

- Lack of time due to aggressive deadlines and tight budgets
- Lack of knowledge—IT experts are usually not security experts
- Lack of priorities—functionality and performance usually come first

That's why we are literally doomed to failure. Hackers have an easy job critiquing a system, stealing or changing data and leaving without a trace. Sometimes the victim doesn't even know that something really had happened until his new designs are somewhere copied by a competitor, or supposedly protected customer data is published on public web sites. Or a journalist gets a list of a terrorist's new story even worse, modern applications are becoming more and more complex—think of megatrends like mobility and cloud computing. Borders disappear and the means of protecting known areas is difficult.

In traditional engineering we have hundreds of years of knowledge that has evolved over time. We know how to build bridges that survive rain, wind and earthquakes. We know how to build solid cars that give you a good chance of surviving a crash. We know of proven solutions to problems in specific contexts. Written down, these are called a patterns, paradigms that have also been applied to software engineering for quite some time. Towards the end of the 1990s we now work on patterns that were dedicated to security