

CONTENTS

Foreword	xiii
Acknowledgments	xvii
Introduction	xix

Part I Introduction

❖ 1 Presenting Web Services	3
Defining Web Services	4
Introducing the XML Family	6
XML for Communication	11
An Example Web Services Scenario	12
Practical Tools	19
❖ 2 Presenting Security	21
The Building Blocks of Security	22
Confidentiality	23
Integrity	27
Nonrepudiation	29
Authentication	32
Authorization	35
Availability	36
Peeling Back the Layers of Security	37
Network Layer	37
Session and Transport Layers	38
Application Layer: S/MIME	39

❖ 3	New Challenges and New Threats	41
	Web Services Security Challenges	43
	The Challenge of Security Based on the End User of a Web Service	43
	End-User Access to a Web Service: A Practical Example	44
	The Challenge of Maintaining Security While Routing Between Multiple Web Services	48
	The Challenge of Abstracting Security from the Underlying Network	50
	Meeting the Challenges: New Technologies for Web Services Security	51
	Persistent Security	51
	Web Services Security Threats	55
	Web Application Security	55
	The Role of Firewalls for Web Services	57

Part II XML Security

❖ 4	XML Signature	63
	Making Sense of XML Signature	65
	An XML Signature Is a Digital Signature Expressed in XML	65
	An XML Signature May Be Placed Inside an XML Document	71
	XML Signature Allows Multiple Documents to Be Signed	74
	XML Signature Is “XML-Aware Signature”	75
	Uses of XML Signature for Web Services Security	75
	Persistent Integrity	75
	Nonrepudiation: How Useful Is the KeyInfo Element?	76
	Authentication	76
	Creating and Validating an XML Signature	77
	Creating an XML Signature	77
	Validating an XML Signature	79
	Checklist	81
❖ 5	XML Encryption	83
	Introduction to XML Encryption	84
	Persistent Encryption for Web Services Transactions	84
	XML-Aware Encryption	85
	Encryption Scenarios	87
	Encrypting an XML Element and Its Contents	87
	Encrypting the Content of an XML Element	88
	Encrypting Arbitrary Data (Including XML)	88
	CipherValue and CipherReference	89

Encryption Steps	90
Step 1: Choose an Encryption Algorithm	90
Step 2: Obtain and (Optionally) Represent the Encryption Key	92
Step 3: Serialize the Data into UTF-8 Encoding	94
Step 4: Perform the Encryption	94
Step 5: Specify the Data Type	94
Process the EncryptedData Structure	95
Decryption Steps	95
Step 1: Determine the Algorithm, Parameters, and ds: KeyInfo	95
Step 2: Locate the Key	95
Step 3: Decrypt the Data	95
Step 4: Process XML Elements or XML Element Content	96
Step 5: Process Data that Is Not an XML Element or XML Element Content	96
Code Examples	96
Encrypting an XML Element Using Triple-DES	96
Decrypting Using the IBM XML Security Suite DecryptionContext	98
The Overlap with XML Signature	98
Using XML Encryption on a Signed Document	98
Using XML Signature on an Encrypted Document	99
Checklist	99
❖ 6 SAML	101
How SAML Enables “Portable Trust”	102
Introducing the Three Types of Assertions	106
SAML Architecture	109
Deploying SAML	113
VeriSign’s Trust Services Integration Kit	114
Checklist	118
❖ 7 XACML	119
Introduction to XACML	120
Basic Concepts of Access Control	121
Rules in XACML	121
Definition of a Rule in XACML: Target, Effect, and Conditions	122
A “Policy” in XACML	125
Digital Rights Management	134
Security Considerations When Using XACML	134
Checklist	136

❖ 8	XML Key Management Specification (XKMS)	137
	Public Key Infrastructure	138
	PKI in Five Easy Points	139
	XKMS and PKI	140
	The XKMS Protocol	143
	XML Key Information Service Specification	147
	XML Key Registration Service Specification	153
	Advanced Protocol Features of XKMS 2.0	160
	Compound Requests	160
	Asynchronous Processing	160
	Checklist	162

Part III Security in SOAP: Presenting WS-Security

❖ 9	WS-Security	165
	Introduction to WS-Security	166
	WS-Security Abstractions	166
	IBM/Microsoft Web Services Security Road Map	167
	WS-Security Elements and Attributes	170
	Error Handling in WS-Security	177
	SAML and WS-Security	178
	Code Example: Using the Microsoft WSE	179
	Checklist	181

Part IV Security in Web Services Frameworks

❖ 10	.NET and Passport	185
	Ticket, Please: A Kerberos Overview	186
	Passport	188
	Prelude to the Login Process	188
	The Login Process	189
	Attacks Against Passport	191
	Malicious Partner Applications	193
	Privacy	193
	Web Services and .NET	194
	Framework	194
	Threats Against .NET Services	196
	Threats Against .NET Servers	199
	Protecting Your Servers	200
	Checklist	201

❖ 11 The Liberty Alliance Project	203
What Does the Liberty Alliance Project Have To Do with Web Services?	204
Terms to Remember	205
Creating Circles of Trust Among Identity Providers and Service Providers	206
Single Sign-On	209
Identity Federation	210
Name Registration	217
Liberty Leading Web Services	221
Defederating a Local Identity	223
Single Logout	224
Security in Liberty	225
Liberty Today, Liberty Tomorrow	225
Give Me Liberty or Give Me Passport	226
❖ 12 UDDI and Security	227
UDDI Overview	228
Securing Transactions with the UDDI Services	232
Explaining the UDDI Roles	233
Authenticating and Authorizing Publishers	235
Authenticating and Authorizing Subscribers	242
Checklist	246

Part V Conclusion

❖ 13 ebXML	249
ebXML	250
Business Processes	250
Collaboration Protocol Profile and Agreement	250
Message Services	251
Registry Information and Services	251
ebXML Security Overview	251
ebXML Registry Security	252
Overview	252
Standards Requirements	252
Registry Security Conclusions	253
ebXML Message Security	254
Overview	254
Standards Overview	254
Authorization and Authentication	254
Data Integrity and/or Confidentiality Attacks	254

Denial of Service and/or Spoofing	254
ebXML Standards Overview	255
Message Security Conclusions	257
❖ 14 Legal Considerations	259
The Role of Contract Law and Evidence in Online Security	260
If Security Is the Answer, Then Exactly What Is the Question?	261
Legal Components: A Primer	261
Digital Signing	262
Dispelling the Myths	264
Mapping Legal Components to Technical Security Components	266
Applying the Law to Particular Technologies	270
Web Services: An Overview of Legally Relevant Technical Trends	270
SAML: The Legality of “Distributed Trust”	274
SSL: Legally, How Secure Is It?	278
Biometrics: Is Seeing Believing?	278
Conclusions	279
Legal Security Is Holistic	280
Effective Security Depends on Shared Cultural Assumptions	280
The Best Security Is Designed to Fail Successfully	281
Checklist	282
❖ A Case Studies	285
Local Government Service Portal	286
Project Overview	286
Security Factors Identified	287
Security Measures Deployed	287
Foreign Exchange Transactions	287
Project Overview	288
Security Factors Identified	288
Security Measures Deployed	289
XML Gateway Rollout	290
Project Overview	290
Security Factors Identified	290
Security Measures Deployed	291
Index	301