

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Security for Web Services and Security Goals	1
1.2	Privacy	3
1.3	Goals and Scope of the Book and its Intended Audience	4
1.4	An Overview of the Book's Content	5
<b>2</b>	<b>Web Service Technologies, Principles, Architectures, and Standards</b>	<b>9</b>
2.1	SOA and Web Services Principles	10
2.2	Web Services Architecture	13
2.3	Web Services Technologies and Standards	13
2.3.1	SOAP	15
2.3.2	Web Services Description Language (WSDL)	16
2.3.3	Service Discovery: Universal Description, Discovery and Integration (UDDI)	18
2.3.4	Considerations	21
2.4	Web Services Infrastructure	22
<b>3</b>	<b>Web Services Threats, Vulnerabilities, and Countermeasures</b>	<b>25</b>
3.1	Threats and Vulnerabilities Concept Definition	26
3.2	Threat Modeling	28
3.3	Vulnerability Categorizations and Catalogs	36
3.4	Threat and Vulnerabilities Metrics	40
<b>4</b>	<b>Standards for Web Services Security</b>	<b>45</b>
4.1	The Concept of Standard	47
4.2	Web Services Security Standards Framework	48
4.3	An Overview of Current Standards	49
4.3.1	"Near the wire" security standards	49
4.3.2	XML Data Security	51
4.3.3	Security Assertions Markup Language (SAML)	53

4.3.4	SOAP Message Security .....	56
4.3.5	Key and Trust Management standards .....	60
4.3.6	Standards for Policy Specification .....	64
4.3.7	Access Control Policy Standards .....	67
4.4	Implementations of Web Services Security Standards .....	73
4.5	Standards-related Issues .....	74
<b>5</b>	<b>Digital Identity Management and Trust Negotiation .....</b>	<b>79</b>
5.1	Overview of Digital Identity Management .....	80
5.2	Overview of Existing Proposals .....	82
5.2.1	Liberty Alliance .....	83
5.2.2	WS-Federation .....	86
5.2.3	Comparison of Liberty Alliance and WS-Framework ...	89
5.2.4	Other Digital Identity Management Initiatives .....	90
5.3	Discussion on Security of Identity Management Systems ....	93
5.4	Business Processes .....	95
5.4.1	Deploying Multifactor Authentication for Business Processes .....	96
5.4.2	Architecture .....	97
5.5	Digital Identity Management in Grid Systems .....	97
5.6	The Trust Negotiation Paradigm and its Deployment using SOA .....	100
5.7	Trust Negotiation and Digital Identity Management .....	101
5.7.1	Automated Trust Negotiation and Digital Identity Management Systems: Differences and Similarities ....	102
5.8	Integrating Identity Management and Trust Negotiations ....	105
5.8.1	Architecture of a SP in FAMTN .....	107
5.8.2	An Example of a Use Case: FSP in Liberty Web Services Framework .....	108
5.9	Negotiations in an FAMTN Federation .....	109
5.9.1	Ticketing system in an FAMTN Federation .....	109
5.9.2	Implementing Trust Tickets Through Cookies .....	110
5.9.3	Negotiation in Identity Federated Systems .....	112
5.10	Bibliographic Notes .....	113
<b>6</b>	<b>Access Control for Web Services .....</b>	<b>115</b>
6.1	Approaches to Enforce Access Control for Web Services .....	116
6.2	WS-AC <sub>1</sub> : An Adaptive Access Control Model for Stateless Web Services .....	118
6.2.1	The WS-AC <sub>1</sub> Model .....	120
6.2.2	WS-AC <sub>1</sub> Identity Attribute Negotiation .....	125
6.2.3	WS-AC <sub>1</sub> Parameter Negotiation .....	128
6.3	An Access Control Framework for Conversation-Based Web services .....	132
6.3.1	Conversation-Based Access Control .....	133

6.3.2	Access Control and Credentials .....	134
6.3.3	k-Trust Levels and Policies .....	135
6.3.4	Access Control Enforcement .....	136
6.3.5	K-Trustworthiness Levels Computation.....	138
6.3.6	Architecture of the Enforcement System.....	145
<b>7</b>	<b>Secure Publishing Techniques.....</b>	<b>147</b>
7.1	The Merkle Signatures .....	148
7.1.1	Merkle Signatures for Trees .....	148
7.1.2	Merkle Signatures for XML Documents .....	149
7.1.3	Merkle Hash Verification for Documents with Partially Hidden Contents .....	150
7.2	Application of the Merkle Signature to UDDI Registries .....	152
7.2.1	Merkle Signature Representation .....	152
7.2.2	Merkle Hash Path Representation .....	153
7.2.3	A Comparison of Merkle Signatures with XML Signatures .....	154
7.3	Bibliographic Notes .....	157
<b>8</b>	<b>Access Control for Business Processes .....</b>	<b>159</b>
8.1	Access Control for Workflows and Business Processes .....	161
8.2	Web Services Business Process Execution Language (WS-BPEL) .....	164
8.3	RBAC-WS-BPEL: An Authorization Model for WS-BPEL Business Processes .....	166
8.4	RBAC XACML: Authorization Schema .....	170
8.5	Business Process Constraint Language .....	170
8.6	RBAC-WS-BPEL Authorization Specification .....	171
8.7	RBAC-WS-BPEL Enforcement .....	172
8.8	RBAC-WS-BPEL System Architecture .....	174
8.9	Handling <HumanActivity> activity Execution and RBAC-WS-BPEL Enforcement .....	176
<b>9</b>	<b>Emerging Research Trends .....</b>	<b>179</b>
9.1	Security as a Service .....	179
9.1.1	Motivations .....	180
9.1.2	Reference Framework for Security Services .....	181
9.1.3	Authentication Service .....	182
9.2	Privacy for Web Services .....	186
9.2.1	P3P and the Privacy-Aware RBAC Model .....	187
9.2.2	Privacy-Preserving Data Management Techniques .....	192
9.2.3	W3C Privacy Requirements for Web Services and Research Issues .....	193
9.3	Semantic Web Security .....	194
9.4	Concluding Remarks .....	195

**XII     Contents**

**A   Access Control** ..... 197

    A.1 Basic Notions ..... 197

        A.1.1 The Protection Matrix Model ..... 198

        A.1.2 Access Control Lists and Capability Lists..... 199

        A.1.3 Negative Authorizations..... 199

    A.2 Role-Based Access Control..... 200

    A.3 Concluding Remarks ..... 204

**References** ..... 205

**Index** ..... 223