

---

## Contents

---

### Part I The Basics of SOA Security Engineering

---

<b>1</b>	<b>Introduction</b>	3
1.1	Service Oriented Architecture	3
1.1.1	Interoperability and Security Issues in SOA	4
1.1.2	Model Driven Security Engineering	5
1.2	Problem Description	6
1.3	Contribution	7
1.3.1	ProSecO	8
1.3.2	SECTET	8
1.4	Related Work	9
1.4.1	Model Driven Security	9
1.4.2	Formal Systems Engineering	10
1.4.3	Pattern-based Approaches	11
1.4.4	Tools and Frameworks	11
1.4.5	Workflow Management	12
<b>2</b>	<b>SOA - Standards &amp; Technology</b>	15
2.1	Service Oriented Architectures	15
2.1.1	Principles of SOA	16
2.1.2	Motivating Example	16
2.2	Web Services	17
2.2.1	Basic Definition	18
2.2.2	Service Invocation	18
2.2.3	Service Description and Discovery	20
2.3	The Web Services Specification Stack	20
2.3.1	Transport Layer	21
2.3.2	Messaging Layer	21
2.3.3	Description Layer	22
2.3.4	Discovery Layer	22
2.3.5	Quality of Service Layer	22

2.3.6	Web Services Security Standards . . . . .	23
2.3.7	Services Composition Layer . . . . .	23
<b>3</b>	<b>Basic Concepts of SOA Security . . . . .</b>	<b>27</b>
3.1	What Is (SOA) Security? . . . . .	27
3.2	Security Objectives . . . . .	29
3.3	Security Policies . . . . .	30
3.3.1	Basic Security Policies . . . . .	31
3.3.2	Policy Models . . . . .	32
3.3.3	Advanced Security Policies . . . . .	36
3.4	Security Analysis . . . . .	38
3.4.1	Security Requirements . . . . .	38
3.4.2	Attacks . . . . .	38
3.5	Web Services Security Standards . . . . .	41
3.5.1	Confidentiality, Integrity, and Authenticity . . . . .	41
3.5.2	Authentication . . . . .	42
3.5.3	Advanced Web Services Security Standards . . . . .	44
<b>4</b>	<b>Domain Architectures . . . . .</b>	<b>47</b>
4.1	Model Driven Software Development . . . . .	47
4.1.1	The Unified Modeling Language . . . . .	48
4.1.2	The Meta-Object Facility . . . . .	48
4.1.3	Model Driven Software Development . . . . .	49
4.1.4	Model Driven Architecture . . . . .	50
4.1.5	Model Driven Security . . . . .	51
4.2	A Definition of Model Driven Software Development . . . . .	51
4.3	Domain Specific Languages . . . . .	52
4.4	The Target Architecture . . . . .	54
4.5	Model-(to-model)-to-code Transformation . . . . .	54
4.6	Domain Architecture . . . . .	56
4.7	Framework . . . . .	57
4.8	Model Driven Security . . . . .	57
4.8.1	Definition . . . . .	57
4.8.2	Extensions to the Problem Space . . . . .	57

---

## Part II Realizing SOA Security

---

<b>5</b>	<b>Sectino – A Motivating Case Study from E-Government . . .</b>	<b>65</b>
5.1	Problem Context . . . . .	65
5.2	Project Mission . . . . .	66
5.3	Expected Benefits . . . . .	66
5.4	Scenario Description . . . . .	67
5.4.1	Requirements . . . . .	68
5.4.2	Security Requirements . . . . .	69
5.5	Results . . . . .	70

<b>6</b>	<b>Security Analysis</b>	71
6.1	Overview	71
6.1.1	Modularity	72
6.1.2	Traceability	73
6.1.3	Model-driven Configuration of Security Services	73
6.1.4	Tight Integration of Functional and Security Aspects	73
6.1.5	Security as a Process	73
6.2	Functional System View	74
6.2.1	Level of Interaction	74
6.2.2	Level of Abstraction	74
6.2.3	Functional Meta-models	75
6.2.4	Global Functional Meta-model	75
6.2.5	Local Functional Meta-model	77
6.3	Security Analysis Process	79
6.3.1	Security Concepts	79
6.3.2	The Security Micro-process	81
6.3.3	Elaborate Functional Model	82
6.3.4	Define Security Objectives	82
6.3.5	Identify Dependencies	83
6.3.6	Security Requirements Engineering	83
6.3.7	Threat and Risk Analysis	85
6.3.8	Security Control Engineering	86
6.4	Access Control	86
6.5	Related Work	89
6.5.1	Standards and Baseline Protection	89
6.5.2	Security Management	89
6.5.3	Security Analysis in the Software Process	90
6.5.4	Formal Approaches to Security Requirements Specification	90
<b>7</b>	<b>Modeling Security Critical SOA Applications</b>	93
7.1	The SECTET Domain Specific Language	93
7.1.1	Domain Definition	93
7.1.2	Global Workflow	94
7.1.3	Local Workflow	94
7.1.4	SECTET Model Views	96
7.1.5	Security Policies	98
7.2	The DSL Meta-models	100
7.2.1	The Workflow View	101
7.2.2	The Interface View	107
7.3	Integrating Security into the DSL	114

<b>8</b>	<b>Enforcing Security with the Sectet Reference Architecture</b>	121
8.1	Architectural Blueprint	121
8.2	Components	122
8.2.1	Service Components	123
8.2.2	Security Components	123
8.2.3	Supporting Security Components	126
8.3	Communication Protocols	126
8.3.1	Enforcing Confidentiality and Integrity	127
8.3.2	Enforcing Non-repudiation	128
8.4	Component Configuration	130
8.4.1	Inbound Messaging - (Executable Security Policy File)	131
8.4.2	Outbound Messaging - (Executable Security Policy Files)	136
8.4.3	Request for Compliance Check	138
8.4.4	Response Request for Compliance Check	139
8.4.5	Technology and Standards	140
<b>9</b>	<b>Model Transformation &amp; Code Generation</b>	141
9.1	Transformations in the SECTET-Framework	141
9.1.1	The Generation of Security Artefacts	141
9.1.2	The Generation of Services Artefacts	142
9.2	Security Transformations	143
9.2.1	Inbound Policy File	143
9.2.2	Outbound Policy Files	144
9.3	Services Transformations	145
9.3.1	Global Workflow to Local Workflow Translation	146
9.3.2	Global Workflow to WSDL Description	146
9.3.3	Global Workflow to XSD Schema Template	148
9.4	Implementing Transformation	149
9.4.1	Template Based Transformations	149
9.4.2	Meta-model Based Transformations	150
<b>10</b>	<b>Software &amp; Security Management</b>	153
10.1	Tool Chain	153
10.1.1	Modeling	153
10.1.2	Code Generation	154
10.1.3	Build Tools and Integrated Development Environments	155
10.1.4	The Realization Process	155
10.1.5	The Engineering Process	156
10.2	The Deployment Process	157
<b>11</b>	<b>Extending Sectet: Advanced Security Policy Modeling</b>	159
11.1	Motivation	160
11.2	Extending the DSL	161
11.2.1	A New Security Objective	161

11.2.2	Advanced Security Policies .....	162
11.2.3	Introducing the RBAC Policy Model.....	162
11.3	Modeling Policies with Dynamic Constraints .....	164
11.3.1	SECTET-PL .....	164
11.3.2	Static RBAC .....	165
11.3.3	Dynamic RBAC.....	165
11.3.4	Rights Delegation .....	167
11.4	Integrating SECTET-PL into the SECTET- Framework .....	171
11.4.1	Metamodel Extensions .....	171
11.4.2	SECTET-PL - Abstract Syntax .....	173
11.5	Extending the Reference Architecture .....	174
11.5.1	Access Control, Delegation and Privacy Policies .....	174
11.5.2	Protocol Extensions .....	179
11.5.3	PDP Extensions.....	180
11.6	SECTET-PL Transformations .....	182
11.7	Modeling Advanced Use Cases with SECTET-PL .....	182
11.7.1	Break-Glass Policy (BGP) .....	182
11.7.2	4-Eyes-Principle .....	183
11.7.3	Usage Control (UC) .....	183
11.7.4	Qualified Signature .....	183

---

### Part III A Case Study from Healthcare

---

<b>12</b>	<b>health@net – A Case Study from Healthcare .....</b>	<b>189</b>
12.1	Background.....	190
12.1.1	The Electronic Healthcare Record .....	190
12.1.2	National E-Health Initiatives .....	190
12.1.3	Technical Standards for Healthcare .....	191
12.1.4	The Austrian Data Privacy Law.....	191
12.2	health@net .....	192
12.2.1	Project Mission .....	192
12.2.2	Organizational Setting .....	193
12.2.3	Architectural Concept .....	194
12.3	health@net – Security Analysis .....	198
12.3.1	Introduction .....	198
12.3.2	Functional System View.....	198
12.3.3	Identification of Security Objectives .....	200
12.3.4	Engineering of Security Requirements .....	202
12.3.5	Conclusion .....	204
12.4	health@net – Security Concept .....	205
12.4.1	Phase 1: Service-level Security .....	205
12.4.2	Phase 2a: Static, Process-level Security.....	206
12.4.3	Phase 2b: Dynamic, Process-level Security .....	206
12.5	Realizing Security with the SECTET-Framework .....	207

XVI Contents

12.5.1 Conceptual Background .....	207
12.5.2 Model Views .....	208
12.6 health@net - Phases 2a & 2b .....	212
12.6.1 Use Cases .....	212
12.6.2 Security Architecture .....	213

---

**Part IV Appendices**

---

<b>A Mapping Tables .....</b>	<b>225</b>
A.1 Mapping Table for Inbound Policy File .....	226
A.2 Mapping Table for Outbound Policy Files .....	227
A.3 Mapping Table for BPEL Files .....	228
A.4 Mapping Table for BPEL Files (continued) .....	229
A.5 Mapping Table for WSDL Files .....	230
<b>References .....</b>	<b>231</b>
<b>Index .....</b>	<b>243</b>

Security Engineering for Service-Oriented Architectures

Hafner, M.; Breu, R.

2009, XVI, 248 p. 124 illus., Hardcover

ISBN: 978-3-540-79538-4