

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Motivation . . . . .	1
1.2	Running Example . . . . .	6
1.2.1	Regular Use Case . . . . .	6
1.2.2	Break-Glass Use Case . . . . .	8
1.2.3	Post-Access Investigations . . . . .	11
1.3	Methodology . . . . .	11
1.4	Thesis Structure . . . . .	13
<b>2</b>	<b>Background</b>	<b>15</b>
2.1	Information Security . . . . .	15
2.2	Access Control . . . . .	18
2.2.1	Concepts . . . . .	18
2.2.2	Access Control Models . . . . .	21
2.2.3	Distributed Access Control Systems . . . . .	29
2.2.4	XACML . . . . .	31
<b>3</b>	<b>A Generic Break-Glass Model</b>	<b>37</b>
3.1	Requirements of Break-Glass . . . . .	37
3.2	Abstract Model . . . . .	41
3.3	Core Model . . . . .	43
3.4	Constraints Model . . . . .	45
<b>4</b>	<b>Policy Definition: Pre-Access</b>	<b>51</b>
4.1	Authorization Infrastructure . . . . .	51
4.1.1	Break-Glass Architecture . . . . .	51
4.1.2	Policy Permissions and Policy State . . . . .	53
4.1.3	Policy State Administration . . . . .	59
4.1.4	Policy Language . . . . .	66
4.1.5	Expressing Regular Privileges for Healthcare . . . . .	68
4.2	Break-Glass Policies . . . . .	74
4.2.1	Policy Structure . . . . .	75

4.2.2	Modeling Break Glass . . . . .	77
4.2.3	Stateful Break-Glass . . . . .	78
4.2.4	Constraints Model in XACML . . . . .	85
4.3	Expressing Exceptional Privileges . . . . .	88
<b>5</b>	<b>User Information: At-Access</b>	<b>93</b>
5.1	Override Measurement . . . . .	93
5.1.1	Information Sources . . . . .	95
5.1.2	Merging Algorithms . . . . .	97
5.1.3	Identifying Mentors . . . . .	99
5.2	Recording the System State . . . . .	101
5.2.1	Versioning System State and Security State . . . . .	101
5.2.2	Logging Break-Glass Accesses . . . . .	102
5.2.3	Recording At-Access Information . . . . .	103
<b>6</b>	<b>Analysis: Post-Access</b>	<b>107</b>
6.1	Post-Access Break-Glass Analysis . . . . .	107
6.2	Analysis Infrastructure . . . . .	111
6.2.1	Authorization Infrastructure . . . . .	111
6.2.2	PDP Analysis Extension . . . . .	114
6.3	Policy-Driven Analysis . . . . .	120
6.3.1	Automated Analysis with Post-Access Information . . . . .	121
6.3.2	Preserving Analysis Knowledge . . . . .	122
<b>7</b>	<b>Implementation</b>	<b>125</b>
7.1	Break-Glass Landscape . . . . .	125
7.2	Analysis Workbench . . . . .	131
<b>8</b>	<b>Related Work</b>	<b>137</b>
8.1	Pre-Staging Emergency Accounts and Roles . . . . .	138
8.2	Categorization of Permissions . . . . .	139
8.3	Break-Glass Models . . . . .	147
8.3.1	Post-Access Models . . . . .	147
8.3.2	RBAC Extensions . . . . .	149
8.3.3	Process-Based Approaches . . . . .	152
8.3.4	Multi-Level Security Adoptions . . . . .	155
8.3.5	Delegation-Based Models . . . . .	157
8.3.6	XACML-Based Approaches . . . . .	159
8.4	Field Tests . . . . .	161

---

<b>9</b>	<b>Evaluation</b>	<b>165</b>
9.1	Requirements vs. Properties . . . . .	165
9.2	Classification of Break-Glass . . . . .	167
9.3	Generalized Break-Glass Models . . . . .	169
<b>10</b>	<b>Discussion and Conclusion</b>	<b>177</b>
10.1	Contributions . . . . .	177
10.2	Research Questions . . . . .	178
10.3	Discussion . . . . .	182
10.3.1	Properties of the Break-Glass Model . . . . .	182
10.3.2	Applications of the Break-Glass Model . . . . .	187
10.3.3	Obligations vs. Third Access Control Decision . . . . .	189
10.3.4	Non-Overridable DENY Decisions vs. Constraints . . . . .	191
10.3.5	Possible Model Variants . . . . .	192
10.4	Future Work . . . . .	194
10.5	Conclusion . . . . .	195
	<b>Bibliography</b>	<b>197</b>
<b>A</b>	<b>Glossary</b>	<b>209</b>
<b>B</b>	<b>Acronyms</b>	<b>211</b>
<b>C</b>	<b>Code Samples</b>	<b>215</b>
C.1	XACML Sample Policy . . . . .	215
C.2	Lattice Evaluation Algorithm in Java . . . . .	217

Break-Glass

Handling Exceptional Situations in Access Control

Petritsch, H.

2014, XIII, 220 p. 15 illus., Softcover

ISBN: 978-3-658-07364-0