

Contents

1	Introduction	1
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
2	Background	15
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
3	A Generic Break-Glass Model	37
3.1	Requirements of Break-Glass	37
3.2	Abstract Model	41
3.3	Core Model	43
3.4	Constraints Model	45
4	Policy Definition: Pre-Access	51
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
5	User Information: At-Access	93
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
6	Analysis: Post-Access	107
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
7	Implementation	125
7.1	Break-Glass Landscape	125
7.2	Analysis Workbench	131
8	Related Work	137
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

9	Evaluation	165
9.1	Requirements vs. Properties	165
9.2	Classification of Break-Glass	167
9.3	Generalized Break-Glass Models	169
10	Discussion and Conclusion	177
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
	Bibliography	197
A	Glossary	209
B	Acronyms	211
C	Code Samples	215
C.1	XACML Sample Policy	215
C.2	Lattice Evaluation Algorithm in Java	217