

Table of Contents

Acknowledgements	v
Abstract	vii
List of Figures.....	xiii
List of Tables	xxi
List of Abbreviations	xxiii
1 Introduction	1
1.1 Motivation	1
1.2 Problem Derivation Surveys	3
1.2.1 PDS1: »SECCRIT« Survey	4
1.2.2 PDS2: »Museum Pfalzgalerie Kaiserslautern« Survey....	6
1.2.3 PDS3: Survey in the context of the policy specification experiment	9
1.2.4 Summary and Conclusion	11
1.3 Problem Statement	12
1.4 Contribution	16
1.5 Hypotheses	19
1.5.1 Hypotheses for RQ1: Usability of Specification Paradigms.....	19
1.5.2 Hypotheses for RQ2: Elicitation.....	23
1.5.3 Hypotheses for RQ3: Formalization	25
1.5.4 Hypotheses for RQ4: Automation	26
1.6 Research Approach	27
1.7 Assumptions and Limitations.....	28
1.8 Outline.....	29
2 Foundations and Related Work	31
2.1 Research Approach	31
2.2 Elicitation of Security and Privacy Requirements	31
2.3 Policy Models and Languages.....	36
2.4 Usable Security and Privacy Policy Specification	40
2.5 Existing PAPs and Derived Specification Paradigms.....	45
2.5.1 Security and Privacy Specification Approaches and Tools.....	45
2.5.2 Overview of Derived Specification Paradigms	51
2.6 User Behavior	54
2.6.1 Intension Models	54
2.6.2 User Type Models	55
2.7 Summary and Conclusion	57

3	Policy Template Elicitation Method	61
3.1	Research Approach	62
3.2	Method Overview	64
3.3	Step 1: Information Retrieval	66
3.4	Step 2: Workshop Preparation.....	68
3.5	Step 3: Execution of Elicitation Workshop	71
3.6	Step 4: Documentation of Workshop Results	75
3.7	Step 5: Policy Template Derivation and Validation	78
3.8	Summary and Conclusion.....	81
4	Policy Template Model.....	83
4.1	Research Approach	84
4.2	Overview of Policy Template Model.....	85
4.3	Domain Sub-model	87
4.4	Security and Privacy Sub-model.....	90
4.5	Template Sub-model.....	90
4.6	Specification-Level Template Sub-model.....	93
4.7	Implementation-Level Template Sub-model.....	95
4.8	Specification Paradigm Projection Sub-model.....	98
4.9	Example	100
4.10	Summary and Conclusion.....	108
5	PAP Generation Framework	111
5.1	Research Approach	112
5.2	Reference Architecture.....	114
5.2.1	Architectural Overview.....	114
5.2.2	Concept for Embedding a Generated Policy Specification Interface into a PAP	124
5.3	Specification Paradigms.....	124
5.3.1	Selection of Specification Paradigms	124
5.3.2	Specification Paradigm Algorithms.....	127
5.4	Reference Implementation	134
5.5	Summary and Conclusion.....	140
6	Mapping Users to Specification Paradigms.....	143
6.1	Research Approach	143
6.2	Mapping Specification Paradigms to Users	144
6.2.1	User Intention Model	145
6.2.2	Example for Barriers of a PAP.....	148
6.2.3	Matching Specification Paradigms to Users	149
6.3	Mapping Specification Paradigms to Personas.....	150
6.3.1	Selection of Persona Model.....	151
6.3.2	Mapping the Specification Paradigms to the Personas of Dupree.....	151
6.4	Summary and Conclusion.....	153
7	Method for Usable PAP Generation	155
7.1	Research Approach	155
7.2	Method Overview	156

7.3	Step 1: Policy Template Elicitation	158
7.4	Step 2: Instantiation of Policy Template Model.....	159
7.5	Step 3: Instantiation of PAP Generation Framework	161
7.6	Step 4: Specification Paradigm Selection	162
7.7	Step 5: Specification of Policy with PAP.....	163
7.8	Summary and Conclusion	164
8	Evaluation for Improvements	165
8.1	Research Approach	165
8.2	Case Study: Software Cluster Project »SINNODIUM«.....	165
8.2.1	Project Summary.....	166
8.2.2	Design and Execution	166
8.2.3	Results	168
8.2.4	Observations and Lessons Learned	171
8.2.5	Threats to validity	172
8.2.6	Summary	173
8.3	Case Study: European Project »SECCRIT«	174
8.3.1	Project Summary.....	174
8.3.2	Design and Execution	175
8.3.3	Results	176
8.3.4	Observations and Lessons Learned	178
8.3.5	Threats to validity	180
8.3.6	Summary	181
8.4	Summary and Conclusion	182
9	Evaluation for Validation	185
9.1	Research Approach	185
9.2	Case Study: Software Campus Project »BeSure«	186
9.2.1	Project Summary.....	186
9.2.2	Design and Execution	187
9.2.3	Results	190
9.2.4	Observations and Lessons Learned	194
9.2.5	Threats to validity	198
9.2.6	Summary	199
9.3	Case Study: »Digital Villages«	200
9.3.1	Project Summary.....	200
9.3.2	Design and Execution	201
9.3.3	Results	203
9.3.4	Observations and Lessons Learned	207
9.3.5	Threats to validity	208
9.3.6	Summary	209
9.4	Policy Specification Experiment	210
9.4.1	Design and Execution	211
9.4.2	Data Analysis and Results.....	217
9.4.3	Discussion.....	235
9.4.4	Threats to validity	238
9.4.5	Summary and Conclusion	239
9.5	Summary and Conclusions	241

10 Summary and Future Work	249
10.1 Methodological and Technological Contributions.....	250
10.2 Empirical Contributions.....	251
10.3 Validation Results.....	253
10.4 Open Issues and Future Work.....	256
References	261
Appendix A Security Policy Template Elicitation	269
A.1 Elicitation Techniques.....	269
A.2 Documentation Techniques.....	275
A.3 Validation Techniques	278
A.4 Prioritization Techniques	280
A.5 Generic Attacker Roles, Threats and Countermeasures.....	281
Appendix B PAP Generation Framework.....	285
B.1 XML Schema for Policy Vocabularies	285
Appendix C The Personas of the Dupree Model.....	291
Appendix D Case Study: »SECCRIT«	295
D.1 Excerpt of »SECCRIT« Study Results	295
D.2 Example of Policy Template in Policy Vocabulary	301
Appendix E Case Study: »BeSure«	305
E.1 Excerpt of »BeSure« Study Results	305
Appendix F Case Study: »Digital Villages«	309
F.1 Excerpt of »Digital Villages« Study Results.....	309
Appendix G Policy Specification Experiment.....	311
G.1 Invitation Email	311
G.2 Experiment Handout	312
G.3 Screenshots of Experiment	314
G.4 Sample Solution	334
G.5 Detailed Results of Statistical Analyses.....	337
G.6 Raw Data	351
Lebenslauf	353