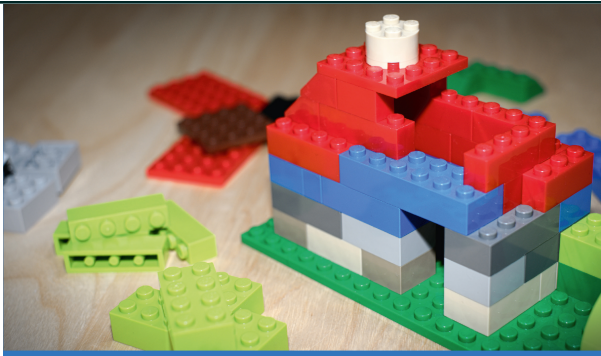




Peter Amthor (Autor)
Aspect-oriented Security Engineering
A Model-based Approach



Peter Amthor

**Aspect-oriented Security
Engineering**
A Model-based Approach



Cuvillier Verlag Göttingen
Internationaler wissenschaftlicher Fachverlag

<https://cuvillier.de/de/shop/publications/7996>

Copyright:
Cuvillier Verlag, Inhaberin Annette Jentsch-Cuvillier, Nonnenstieg 8, 37075 Göttingen,
Germany
Telefon: +49 (0)551 54724-0, E-Mail: info@cuvillier.de, Website: <https://cuvillier.de>



Contents

1	Introduction	1
1.1	Motivation	3
1.2	Aspect-oriented Engineering	5
1.3	Contributions	6
1.4	Organization	10
1.5	Writing Conventions	11
2	State of the Art	15
2.1	Analysis of Dynamic Security Models	16
2.2	Entity Labeling	17
2.3	Aspect-oriented Security Engineering	21
3	Model Foundations	25
3.1	Identity-based Access Control Models	26
3.1.1	The Access Matrix Model	27
3.1.2	The Harrison-Ruzzo-Ullman Model	28
3.2	Attribution-based Access Control Models	31
3.2.1	Role-based Access Control	31
3.2.2	Attribute-based Access Control	40
3.3	Information Flow Control	46
3.4	Implementations of Access Control Models	48
3.4.1	Discretionary and Mandatory Access Control	49
3.4.2	The SELinux Operating System	50
3.4.2.1	Security Architecture	51



3.4.2.2	Policy Semantics	53
3.4.3	The OpenMRS Middleware	55
3.4.3.1	Security Architecture	56
3.4.3.2	Policy Semantics	58
3.5	Dynamic Model Analysis	59
4	Aspects	63
4.1	The Aspect-oriented Engineering Approach	65
4.2	Policy Semantics: The Entity Labeling Aspect	68
4.2.1	Entity Set	69
4.2.2	Label Set	71
4.2.3	Label Assignment	73
4.2.4	Access Rule	74
4.2.5	Relabeling Rule	76
4.2.6	Model Constraint	77
4.2.7	Usage in Model Engineering	79
4.2.8	Entity Labeling Summary	90
4.3	Policy Analysis: The Model Core Aspect	91
4.3.1	Dynamic Component	96
4.3.2	Static Component	96
4.3.3	Transition Rule	97
4.3.3.1	State Transition Function	98
4.3.3.2	State Transition Scheme	99
4.3.4	Usage in Model Engineering	104
4.3.5	Usage in Model Analysis	110
4.3.6	Model Core Summary	116
4.4	Interrelating Aspects: Entity Labeling plus Model Core	117
4.4.1	Model Engineering	117
4.4.1.1	Model Components Specification	117
4.4.1.2	State Transition Scheme Specification	122
4.4.2	Model Analysis	135
4.4.2.1	Safety Specification	135
4.4.2.2	Heuristic Specification	140



- 5 Application to SELinux** **147**
- 5.1 Scenario 148
- 5.2 SELinux Model Specification 149
 - 5.2.1 Entity Labeling Model 149
 - 5.2.2 Core-based Model 153
 - 5.2.3 Specifying SELX Commands 154
- 5.3 Tailoring Safety Analysis to SELinux 160
 - 5.3.1 SELinux Safety 160
 - 5.3.2 SELinux Heuristic 165
- 5.4 Application in Practice 168
 - 5.4.1 Finding Decidable Cases 168
 - 5.4.2 Efficiency Optimizations 173
 - 5.4.2.1 State-Space Exploration 173
 - 5.4.2.2 Parameter Dependency Analysis 175
 - 5.4.3 Consolidated Algorithm 178
 - 5.4.4 SELX Model Instantiation 181
 - 5.4.4.1 State Space 181
 - 5.4.4.2 Model Statics 183
 - 5.4.4.3 Model Dynamics 185
 - 5.4.4.4 Model Instantiation Results 187
 - 5.4.5 Model Analysis 188
- 6 Outlook** **191**
- 7 Conclusion** **195**
- A Examples of Aspect-oriented Security Models** **199**
- A.1 ABAC 199
- A.2 RBAC 202
- B Overview of Security Models** **207**
- C Modeling Languages** **211**
- C.1 The Core-based Markup Language 212
- C.2 The Entity Labeling Markup Language 214



Glossary	217
Acronyms	221
Bibliography	225