Contents

1 Introduction **1**

1.1 Motivation . . . 1

1.2 Causal Trusted Computing Bases . . . 2

1.3 Challenges and Contributions . . . 3

1.4 Organization . . . 4

2 Related Work **7**

2.1 Policy-controlled Operating Systems . . . 7

2.1.1 Flask Security Architecture . . . 7

2.1.2 Rule Set Based Access Control . . . 9

2.1.3 Policy Machine . . . 10

2.1.4 Summary . . . 11

2.2 Reducing the Size and Complexity of TCBs . . . 11

2.2.1 Nizza Security Architecture . . . 11

2.2.2 Other Approaches . . . 13

2.3 Security Models . . . 13

2.3.1 Model-based Security Policy Engineering . . . 14

2.3.2 Access Control Models . . . 15

2.3.3 Information Flow Control Models . . . 16

2.4 Summary . . . 17

3 Security Model Core **19**

3.1 Security Model Family Tree . . . 19

3.2 Core Definition . . . 23

3.3 Core Specialization . . . 25

3.4 Model Re-engineering . . . 28

3.4.1 Multilevel Security Models . . . 28

3.4.2 MLS Model for a Web Service Composition System Policy . . . 29

3.4.3 Role-based Access Control Models . . . 31

3.4.4 Use Case RBAC Security Policy . . . 33

3.4.5 RBAC Model for the HIS Policy . . . 34

3.4.6 Attribute-based Access Control Models . . . 36

3.4.7 ABAC Model for an Online Entertainment Store Policy . . . 39

3.4.8 Summary . . . 41

3.5 Model Core Evaluation . . . 41

3.5.1 Expressive Power . . . 41

3.5.2 Model Engineering Costs . . . 46

3.5.3 Summary . . . 48

3.6 Model Core Related Work . . . 48

3.7 Conclusion . . . 50

Bibliografische Informationen
http://d-nb.info/1048402649

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

4 Causal Trusted Computing Bases 53
4.1 Requirements and Prerequisites . . . 53
4.1.1 Security Model Core for TCB Engineering . . . 54
4.1.2 Design Requirements . . . 55
4.1.3 Hardware and Architecture Dependencies . . . 57
4.2 TCB Design . . . 58
4.3 Policy-independent Runtime Environment . . . 64
4.3.1 Security Policy Manager . . . 64
4.3.2 Memory Manager . . . 67
4.3.3 Thread Manager . . . 69
4.3.4 Transaction Manager . . . 72
4.3.5 Inter Thread Communication . . . 75
4.3.6 Trusted Persistent Storage Manager . . . 77
4.3.7 Cryptographer . . . 81
4.3.8 Entity Identification Server . . . 82
4.3.9 Generic Object Manager . . . 83
4.3.10 Authenticator . . . 86
4.3.11 Summary . . . 87
4.4 Policy-dependent Runtime Environment . . . 87
4.4.1 Engineering Approach . . . 88
4.4.2 Abstract Security Model Functionality . . . 90
4.4.3 Abstract Model Instance Functionality . . . 104
4.4.4 Causal Dependencies . . . 106
4.4.5 Summary . . . 119
4.5 Policy-dependent RTE for the RBAC HIS Policy . . . 120
4.5.1 RBAC Security Model Functions . . . 120
4.5.2 Interceptor . . . 137
4.5.3 Executable RBAC HIS Policy . . . 138
4.6 Conclusion . . . 140

5 Specification Engineering 143
5.1 Specification Fundamentals . . . 144
5.2 Requirements for TCB Specifications . . . 145
5.3 TCB Specification Approach . . . 146
5.4 TCB Specification Method . . . 147
5.4.1 Specification of a Core-based Security Model . . . 148
5.4.2 Specification of a Model Instance . . . 152
5.5 Summary . . . 155

6 Evaluation 157
6.1 Evaluation Goals and Methods . . . 158
6.2 Functional Redundancy of the Policy-dependent RTE . . . 159
6.2.1 Redundancy across Multiple `Security Model Functions` Components . 159
6.2.2 Redundancy within a `Security Model Functions` Component . . . 160
6.2.3 Summary . . . 160
6.3 Expressive Power and Modeling Effort of Core-based Model Engineering . . . 161
6.4 Implementation Effort for Policy Substitution . . . 162
6.4.1 Prototype Implementation of a Policy-dependent RTE . . . 162

6.4.2 Implementation Effort . . . 164
6.5 Formal TCB Specifications . . . 167
6.6 Summary . . . 169

7 Conclusion 171

8 Future Work 173

Appendix 175

A Security Models 175
A.1 Notation . . . 175
A.2 MLS Model . . . 175
A.3 RBAC Model . . . 177
A.4 ABAC Model . . . 180

B Health Information System Model Instance 183
B.1 Initial State and Extension Values . . . 183
B.2 Authorization Scheme . . . 185

C Formal Rule System 189
C.1 Mapping . . . 189
C.2 Matrix . . . 194

D TCB Specification for the RBAC HIS Policy 201
D.1 Context `rbac_static` . . . 201
D.2 Context `rbac_state` . . . 202
D.3 Context `rbac_userhandling` . . . 204
D.4 Context `rbac_sessionhandling` . . . 205
D.5 Context `rbac_rolehandling` . . . 206
D.6 Context `rbac_conditions` . . . 208
D.7 Context `rbac` . . . 210
D.8 Context `healthcare_context` . . . 210
D.9 Context `healthcare_generic` . . . 213
D.10 Context `healthcare` . . . 216

List of Abbreviations 223

List of Figures 226

List of Tables 227

Bibliography 228