Contents

1 **Introduction** 1

1.1 System and Security Engineering 1

1.2 Security and Security Risk Management Standards 2

1.3 Security Development Approaches 4

1.4 Domain-Specific Languages for Security Modelling 4

1.5 Model-Driven Security 5

1.6 Modelling Perspectives of Secure Software Systems 6

1.7 Running Example 9

1.8 Exercises 12

Part I Security Risk Management

2 **Domain Model for Information Systems Security Risk Management** 17

2.1 Domain Model 17

2.1.1 Asset-Related Concepts 17

2.1.2 Risk-Related Concepts 19

2.1.3 Risk Treatment-Related Concepts 20

2.2 Relationships and Multiplicities 20

2.3 Metrics 22

2.4 Process 22

2.5 ISSRM Application Example 23

2.6 Further Reading 27

2.7 Exercises 29

3 **Security Risk** 31

3.1 System Assets 31

3.2 Risk Analysis 33

3.3 Harm: Malicious Software 34

3.4 Taxonomy of Security Errors 36

3.5 Security Threats 37

Matulevi?ius, Raimundas
Fundamentals of secure system modelling

digitalisiert durch:
IDS Basel Bern

3.6 Threat Agent 39
3.7 Further Reading 41
3.8 Exercises 41

4 Security Requirements 43
4.1 Security Criterion 43
4.2 Requirements Definition 44
4.3 Security Requirements Classification 45
4.4 How to Specify Security Requirements 50
4.5 Related (to Security) Requirements 52
4.6 Further Reading 56
4.7 Exercises 58

Part II Modelling Languages for Security Risk Management

5 Security Risk-Oriented BPMN 63
5.1 Business Process Model and Notation 63
5.2 Security Risk Management Using BPMN 64
5.2.1 Semantics 65
5.2.2 Abstract Syntax 65
5.2.3 Concrete Syntax 68
5.3 Example 69
5.4 Further Reading 72
5.5 Exercises 75

6 Security Risk-Aware Secure Tropos 77
6.1 Tropos and Secure Tropos 77
6.2 Security Risk Management Using Secure Tropos 79
6.2.1 Semantics and Concrete Syntax 79
6.2.2 Abstract Syntax 81
6.3 Examples 86
6.4 Further Reading 89
6.5 Exercises 91

7 Security Risk-Oriented Misuse Cases 93
7.1 Use and Misuse Cases 93
7.2 Security Risk Management Using Misuse Cases 94
7.2.1 Semantics and Concrete Syntax 94
7.2.2 Abstract Syntax 95
7.3 Examples 98
7.4 Textual Misuse Cases 101
7.5 Further Reading 103
7.6 Exercises 104

8 Mal-activities for Security Risk Management 107
8.1 Activity and Mal-activity Diagrams 107
8.2 Security Risk Management Using Mal-activities 108

8.2.1 Semantics and Concrete Syntax 108
8.2.2 Abstract Syntax 110
8.3 Example 112
8.4 Further Reading 113
8.5 Exercises 113

Part III Model-Driven Security Development and Application

9 Transformations Between Security Risk-Oriented Modelling Languages 119
9.1 Transformation Basis 119
9.1.1 Transformation Method 119
9.1.2 Comparison of Modelling Languages 120
9.2 Transforming from Security Risk-Oriented BPMN to Security Risk-Aware Secure Tropos 125
9.3 Transforming from Security Risk-Aware Secure Tropos to Security Risk-Oriented Misuse Cases 129
9.4 Transforming from Security Risk-Oriented Misuse Cases to Mal-activities for Security Risk Management 135
9.5 Further Reading 141
9.6 Exercises 144

10 Role-Based Access Control 147
10.1 Family of RBAC Models 147
10.2 RBAC Administration 149
10.3 RBAC Modelling Languages 150
10.3.1 SecureUML 150
10.3.2 UMLsec 153
10.3.3 Comparison 156
10.3.4 Transformation 158
10.4 Model-Driven Security 162
10.5 Further Reading 165
10.6 Exercises 167

11 Secure System Development Using Patterns 171
11.1 Security Patterns 171
11.2 Security Pattern Taxonomy 172
11.3 Security Risk-Oriented Patterns 174
11.4 Security Requirements Elicitation from Business Processes 180
11.4.1 SREBP Method 182
11.4.2 Pattern Application 185
11.5 Further Reading 193
11.6 Exercises 194

Part IV Concluding Remarks

12 Secure System Development 199
12.1 Secure System Development Processes 199
12.1.1 Microsoft Secure System Development Lifecycle 200
12.1.2 OWASP CLASP 201
12.1.3 Seven Touchpoints 202
12.1.4 Comparison 204
12.2 Security Approaches in Secure Systems Development Processes 204
12.3 Tools 206
12.4 Exercises 207

References 209