

# Contents

<b>1. Introduction</b> .....	1
1.1 Motivation .....	1
1.2 Problem Statement .....	4
1.3 Solution .....	4
1.4 Unaddressed Related Issues .....	6
1.5 Structural Overview .....	7
<b>2. Patterns in Software Development</b> .....	11
2.1 Introduction .....	11
2.2 Pattern History .....	12
2.3 Basic Pattern Concepts .....	13
2.4 Collections of Patterns .....	15
2.5 Pattern Classification Approaches .....	16
2.6 Writing Patterns .....	19
2.6.1 Pattern Mining Approaches .....	20
2.6.2 Quality Assurance by Community Processes .....	20
2.6.3 Integration of Patterns .....	23
2.7 Problem Solving with Patterns .....	24
2.8 Summary .....	25
<b>3. Ontologies</b> .....	29
3.1 Introduction .....	29
3.2 Security Knowledge Process .....	30
3.3 Knowledge Representation with Ontologies .....	31
3.4 Development of Ontologies .....	33
3.4.1 Design Criteria .....	33
3.4.2 Methodologies .....	35
3.4.3 Ontology Representation Languages .....	37
3.4.4 Tool Support .....	41
3.5 Summary .....	44
<b>4. The Human Factor</b> .....	45
4.1 Introduction .....	45
4.2 Case Studies .....	45

4.2.1	Internet/Telephony Integration . . . . .	46
4.2.2	Instant Messaging . . . . .	48
4.2.3	Findings . . . . .	51
4.3	Why Security Fails . . . . .	52
4.4	Related Work . . . . .	54
4.5	Summary . . . . .	54
<b>5.</b>	<b>Classifying Security Improvement Artifacts . . . . .</b>	<b>57</b>
5.1	Introduction . . . . .	57
5.2	Classification Framework . . . . .	59
5.2.1	Security Engineering . . . . .	59
5.2.2	System Engineering . . . . .	60
5.2.3	The Zachman Framework . . . . .	62
5.2.4	Classification Metrics . . . . .	62
5.3	Requirements Definition . . . . .	65
5.3.1	Evaluation Criteria . . . . .	65
5.3.2	Security Management Standards . . . . .	66
5.3.3	Security Policy . . . . .	67
5.3.4	Summary . . . . .	68
5.4	Analysis . . . . .	68
5.4.1	Goal Trees . . . . .	68
5.4.2	Risk Analysis . . . . .	69
5.4.3	Work Factor Concept . . . . .	70
5.4.4	Prioritization Schemes . . . . .	71
5.4.5	Summary . . . . .	74
5.5	Architecture and Design . . . . .	74
5.5.1	Modeling Techniques . . . . .	74
5.5.2	Formal Methods . . . . .	75
5.5.3	Summary . . . . .	76
5.6	Building . . . . .	76
5.6.1	Secure Programming Guidelines . . . . .	76
5.6.2	Security Building Blocks . . . . .	77
5.6.3	Best Security Practices . . . . .	78
5.6.4	Summary . . . . .	79
5.7	Testing . . . . .	79
5.7.1	Conceptual Testing . . . . .	79
5.7.2	Runtime Testing . . . . .	81
5.7.3	Summary . . . . .	82
5.8	Summary and Conclusions . . . . .	82
5.8.1	Summary . . . . .	82
5.8.2	Conclusions . . . . .	84

<b>6. Toward a Security Core Ontology</b> .....	87
6.1 Introduction .....	87
6.2 Related Work .....	88
6.3 Methodology .....	89
6.4 Definitions of Concepts .....	90
6.5 Relations between Concepts .....	94
6.6 Summary .....	96
<b>7. Foundations of Security Patterns</b> .....	97
7.1 Introduction .....	97
7.2 Security Pattern Example .....	98
7.3 History of Security Patterns .....	99
7.3.1 Pioneering Security Patterns .....	99
7.3.2 Other Contributions .....	101
7.3.3 Security Pattern Community .....	102
7.4 What Is a Security Pattern? .....	102
7.4.1 Security Pattern Template .....	103
7.4.2 Application of Security Patterns .....	104
7.4.3 Forces Related to Security .....	105
7.4.4 Organizing Security Patterns .....	107
7.5 Mining Security Patterns .....	109
7.5.1 Completeness of Security Pattern Collections .....	110
7.5.2 Security Information Providers .....	110
7.5.3 Security Standards as Sources for Pattern Mining .....	113
7.6 Summary and Conclusions .....	118
7.6.1 Summary .....	118
7.6.2 Conclusions .....	119
<b>8. A Theoretical Model for Security Patterns</b> .....	121
8.1 Introduction .....	121
8.2 Related Work .....	122
8.3 Modeling Security Patterns .....	122
8.4 Core Definitions .....	127
8.5 Primary Security Pattern Relations .....	130
8.6 Internal and External Coverage .....	135
8.7 Why Coverage Implies a State of Security .....	136
8.8 Summary and Conclusions .....	138
8.8.1 Summary .....	138
8.8.2 Conclusions .....	139
<b>9. New Applications of Security Patterns</b> .....	141
9.1 Introduction .....	141
9.2 A Security Pattern Search Engine .....	142
9.2.1 A Pattern-Based Expert System? .....	142
9.2.2 Use Cases .....	143

9.2.3	Prototype .....	145
9.2.4	Related Work .....	146
9.3	Enhancing Security Patterns with Meta-information .....	147
9.3.1	Codifying the Knowledge Base and Inference Rules ....	147
9.3.2	Basic Applications .....	149
9.4	Advanced Techniques .....	151
9.4.1	Improvement of Search and Retrieval Capabilities ....	152
9.4.2	Considering Side-Effects .....	153
9.4.3	Maintaining Security Pattern Repositories .....	155
9.5	Summary and Conclusions .....	157
9.5.1	Summary .....	157
9.5.2	Conclusions .....	158
<b>10.</b>	<b>Summary and Outlook</b> .....	<b>161</b>
<b>A.</b>	<b>Sources for Mining Security Patterns</b> .....	<b>167</b>
<b>B.</b>	<b>Example Security Patterns and Annotations</b> .....	<b>171</b>
<b>C.</b>	<b>Ontology Development</b> .....	<b>179</b>
<b>D.</b>	<b>F-Logic Primer</b> .....	<b>185</b>
<b>E.</b>	<b>Gaining Security Expertise</b> .....	<b>189</b>
	<b>References</b> .....	<b>195</b>
	<b>Index</b> .....	<b>207</b>