

---

# Contents

---

## Part I Prologue

---

<b>1</b>	<b>Introduction</b> . . . . .	3
1.1	Overview . . . . .	9
1.2	Outline . . . . .	12
1.3	How to Use this Book . . . . .	13
<b>2</b>	<b>Walk-through: Using UML for Security</b> . . . . .	15
2.1	Security Requirements Capture with Use Case Diagrams . . . . .	16
2.2	Secure Business Processes with Activity Diagrams . . . . .	16
2.3	Physical Security Using Deployment Diagrams . . . . .	17
2.4	Security-Critical Interaction with Sequence Diagrams . . . . .	18
2.5	Secure States Using Statechart Diagrams . . . . .	20
<b>3</b>	<b>Background</b> . . . . .	21
3.1	Security Engineering . . . . .	21
3.2	Unified Modeling Language . . . . .	24
3.2.1	Use Case Diagrams . . . . .	25
3.2.2	Class Diagrams . . . . .	26
3.2.3	Statechart Diagrams . . . . .	26
3.2.4	Sequence Diagrams . . . . .	28
3.2.5	Activity Diagrams . . . . .	30
3.2.6	Deployment Diagrams . . . . .	30
3.2.7	Subsystems . . . . .	31
3.2.8	UML Extension Mechanisms . . . . .	32
3.3	Analyzing UML Models . . . . .	34
3.3.1	Notation . . . . .	34
3.3.2	Outline of Formal Semantics . . . . .	35
3.3.3	Modeling Cryptography . . . . .	36
3.3.4	Security Analysis of UML Diagrams . . . . .	38
3.3.5	Important Security Properties . . . . .	41

---

**Part II Developing Secure Systems**

---

- 4 Model-based Security Engineering with UML** . . . . . 49
  - 4.1 UMLsec Profile . . . . . 49
    - 4.1.1 Requirements on a UML Extension for Development of Security-Critical Systems . . . . . 49
    - 4.1.2 The Extension . . . . . 50
    - 4.1.3 Addressing the Requirements . . . . . 66
  - 4.2 Design Principles for Secure Systems . . . . . 68
  - 4.3 Applying Security Patterns . . . . . 70
  - 4.4 Notes . . . . . 72
  - 4.5 Discussion . . . . . 73
  
- 5 Applications** . . . . . 75
  - 5.1 Secure Channels . . . . . 75
  - 5.2 A Variant of the Internet Protocol TLS . . . . . 80
  - 5.3 Common Electronic Purse Specifications . . . . . 88
    - 5.3.1 Purchase Transaction . . . . . 90
    - 5.3.2 Load Transaction . . . . . 99
  - 5.4 Developing Secure Java Programs . . . . . 118
    - 5.4.1 Access Control in Java . . . . . 118
    - 5.4.2 Design Process . . . . . 120
    - 5.4.3 Example: Financial Application . . . . . 122
  - 5.5 Further Applications . . . . . 125
    - 5.5.1 Modeling and Verification of a Bank Application . . . . . 125
    - 5.5.2 Biometric Authentication System . . . . . 127
    - 5.5.3 Automotive Emergency Application . . . . . 127
    - 5.5.4 German Electronic Health Card . . . . . 128
    - 5.5.5 Electronic Purse for the Oktoberfest . . . . . 128
    - 5.5.6 Electronic Signature Architecture in Insurance Companies . . . . . 128
  - 5.6 Notes . . . . . 129
  - 5.7 Discussion . . . . . 129

---

**Part III Tool Support**

---

- 6 Tool support for UMLsec** . . . . . 133
  - 6.1 Extending UML CASE Tools with Analysis Tools . . . . . 133
    - 6.1.1 Meta-Object Facility (MOF) . . . . . 134
    - 6.1.2 XML-Based Data-Binding with MDR . . . . . 136
  - 6.2 Automated Tools for UMLsec . . . . . 137
    - 6.2.1 Tool Functionality . . . . . 137
    - 6.2.2 Implementation Details . . . . . 139

6.2.3	Model-Checking UMLsec Specifications	141
6.2.4	Automated Theorem Proving	142
6.2.5	Prolog-Based Attack Generation	142
6.3	Linking Models to Runtime Data: SAP R/3 Permissions	142
6.3.1	Automated Analysis of Security Rules	144
6.3.2	Instance Data	147
6.3.3	Evaluating Rules	151
6.4	Linking Models to Code	155
6.4.1	Test-Sequence Generation	155
6.4.2	Code Generation and Code Analysis	158
6.5	Notes	158
6.6	Discussion	159
<b>7</b>	<b>A Formal Foundation</b>	<b>161</b>
7.1	UML Machines	161
7.2	UML Machine Systems	169
7.3	Refinement	172
7.4	Rely-Guarantee Specifications	176
7.5	Reasoning About Security Properties	177
7.5.1	Refinement	180
7.5.2	Secrecy	182
7.5.3	Integrity	184
7.5.4	Authenticity	185
7.5.5	Freshness	185
7.5.6	Secure Information Flow	187
7.6	Notes	188
7.7	Discussion	189
<b>8</b>	<b>Formal Systems Development with UML</b>	<b>191</b>
8.1	Formal Semantics for a Fragment of UML	191
8.1.1	General Concepts	194
8.1.2	Class Diagrams	201
8.1.3	Statechart Diagrams	202
8.1.4	Sequence Diagrams	212
8.1.5	Activity Diagrams	217
8.1.6	Deployment Diagrams	219
8.1.7	Subsystems	220
8.2	Development with UML	226
8.2.1	Refinement	226
8.2.2	Rely-Guarantee Specifications	230
8.2.3	Reasoning About Security Properties in UML	230
8.3	Notes	231
8.4	Discussion	233

---

**Part IV Epilogue**


---

<b>9</b>	<b>Further Material</b> .....	237
9.1	More on the UMLsec Approach .....	237
9.2	Other Approaches to Security Engineering .....	238
9.2.1	Software Engineering and Security .....	238
9.2.2	Other Approaches Using UML .....	238
9.2.3	Formal Methods Applied to Security .....	240
9.2.4	Other Non-functional Requirements .....	242
<b>10</b>	<b>Outlook</b> .....	243

---

**Part V Appendices**


---

<b>A</b>	<b>Towards UML 2.0</b> .....	247
<b>B</b>	<b>The Semantics of UML Machine Rules</b> .....	249
<b>C</b>	<b>Proofs</b> .....	253
C.1	UML Machines .....	253
C.2	Refinement .....	254
C.3	Rely-Guarantee Specifications .....	256
C.4	Reasoning About Security Properties .....	257
C.5	Formal Systems Development with UML .....	262
C.6	Secure Channels .....	264
C.7	A Variant of the Internet Protocol TLS .....	265
C.8	Common Electronic Purse Specifications .....	270
C.8.1	Purchase Transaction .....	270
C.8.2	Load Transaction .....	274
	<b>References</b> .....	277
	<b>Index</b> .....	305