

# Inhaltsverzeichnis

Abkürzungsverzeichnis . . . . .	ix
<b>1 Einleitung</b>	<b>1</b>
1.1 Problemidentifikation . . . . .	1
1.2 Ziele und Lösungsansätze . . . . .	4
1.3 Relevante Publikationen . . . . .	5
<b>2 Stand der Technik</b>	<b>7</b>
2.1 Gliederung des Kapitels . . . . .	7
2.2 Model-Driven Engineering . . . . .	7
2.2.1 Anforderungs- und Architekturmodellierung . . . . .	7
2.2.2 Modellbasiertes Testen . . . . .	13
2.3 Sicherheitsorientierte Engineering-Verfahren . . . . .	16
2.3.1 CORAS . . . . .	16
2.3.2 Fehlerbaumanalyse . . . . .	17
2.3.3 Threat Modeling . . . . .	18
2.3.4 Secure Tropos . . . . .	19
2.3.5 UMLsec . . . . .	22
2.3.6 SecureUML . . . . .	25
2.3.7 Model-Checking . . . . .	25
2.3.8 Common Criteria . . . . .	27
2.3.9 Testverfahren . . . . .	29
2.4 Monitoring und Management . . . . .	32
2.4.1 Security Information and Event Monitoring . . . . .	32
2.4.2 Information Security Indicators . . . . .	33
2.5 Fazit . . . . .	35
<b>3 Modelle</b>	<b>37</b>
3.1 Modellierung und Analyse des Sicherheitsproblems . . . . .	37
3.1.1 Grundbegriffe zur Beschreibung des Sicherheitsproblems . . . . .	37
3.1.2 Metamodell . . . . .	45
3.1.3 Charakterisierung der Bedrohungen . . . . .	48
3.1.4 Charakterisierung des Angreifers . . . . .	49
3.1.5 Charakterisierung der Widerstandsfähigkeit . . . . .	49
3.1.6 Charakterisierung des Schutzniveaus . . . . .	51

3.1.7	Ableitung funktionaler Sicherheitsanforderungen . . . . .	51
3.1.8	Auswertung des Sicherheitsproblems . . . . .	53
3.2	Betrieb sicherer Anwendungen . . . . .	58
3.2.1	Metamodell . . . . .	60
3.2.2	Charakterisierung der Ausführungsumgebung . . . . .	62
3.2.3	Charakterisierung der Konfiguration . . . . .	64
3.2.4	Charakterisierung externer Sicherheitspolitiken . . . . .	66
<b>4</b>	<b>Fallstudie</b>	<b>71</b>
4.1	Charakterisierung des Systems . . . . .	72
4.2	Das SMGW-Schutzprofil . . . . .	75
4.2.1	Werte . . . . .	75
4.2.2	Annahmen . . . . .	77
4.2.3	Bedrohungen . . . . .	79
4.2.4	Sicherheitsziele . . . . .	80
4.2.5	Organisatorische Sicherheitspolitiken . . . . .	85
4.3	Schutzprofil und Notwendigkeit einer Engineering-orientierten Sicht . . . . .	85
4.4	Formulierung des Sicherheitsproblems im Engineering . . . . .	86
4.4.1	Zu schützende Werte . . . . .	86
4.4.2	Szenarien . . . . .	91
4.4.3	Bedrohungen . . . . .	93
4.4.4	Charakterisierung der Angreifer . . . . .	96
4.4.5	Systempolitiken . . . . .	101
4.4.6	Systemmodell . . . . .	103
4.4.7	Angriffe . . . . .	105
4.4.7.1	Bedrohungs- und Angriffsanalyse . . . . .	106
4.4.7.2	Hardware-basierende Angriffe . . . . .	108
4.4.7.3	DMA-Angriffe . . . . .	109
4.4.7.4	Angriffe gegen Web-Anwendungen . . . . .	109
4.4.7.5	Detouring-Angriffe . . . . .	110
4.4.7.6	Angriffe gegen kryptografische Verfahren . . . . .	111
4.5	Sicherheitsmechanismen . . . . .	112
4.5.1	TR-03109 und Schutzprofil . . . . .	112
4.5.2	Sicherheitsmechanismen . . . . .	113
4.5.2.1	Startvorgang . . . . .	113
4.5.2.2	Laufzeitphase der SMGW-Anwendungen . . . . .	123
4.6	Formulierung des Sicherheitsproblems im betrieblichen Kontext . . . . .	133
4.6.1	Ausführungsumgebung . . . . .	133
4.6.1.1	Externe Entitäten im LMN . . . . .	133
4.6.1.2	Externe Entitäten im HAN . . . . .	134
4.6.1.3	Externe Entitäten im WAN . . . . .	135
4.6.1.4	Externe Entitäten im CLS . . . . .	136

4.6.2	Konfiguration . . . . .	136
4.6.3	Externe Sicherheitspolitiken . . . . .	138
4.7	Sicherheitsorientierter Test . . . . .	140
4.7.1	Ansatz und Besonderheiten . . . . .	140
4.7.2	Integration in den Entwicklungszyklus . . . . .	141
4.8	Ergebnisse der Fallstudie . . . . .	143
4.8.1	Besonderheiten des SMGW-Schutzprofils und der technischen Richtlinie	144
4.8.2	Verbesserungsansätze . . . . .	145
4.8.2.1	Verbesserungsansätze im Kontext des Startvorgangs . . . . .	145
4.8.2.2	Verbesserungsansätze für die Laufzeitphase . . . . .	147
<b>5</b>	<b>Zusammenfassung</b>	<b>149</b>
5.1	Erkenntnisse . . . . .	149
5.2	Limitierungen . . . . .	150
5.3	Zukünftige Arbeiten . . . . .	150
<b>A</b>	<b>Bedrohungs- und Angriffsanalyse</b>	<b>151</b>
	<b>Abbildungsverzeichnis</b>	<b>175</b>
	<b>Tabellenverzeichnis</b>	<b>178</b>
	<b>Literaturverzeichnis</b>	<b>179</b>