

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>9</b>
1.1	Problemstellung . . . . .	9
1.2	Stand der Technik . . . . .	10
1.3	Zielsetzung der Arbeit . . . . .	10
1.4	Aufbau der Arbeit . . . . .	10
<b>I</b>	<b>Grundlagen</b>	<b>11</b>
<b>2</b>	<b>Sicherheit</b>	<b>13</b>
2.1	Grundbegriffe . . . . .	13
2.2	Denial-of-Service . . . . .	14
2.2.1	Ressourcenbelegung . . . . .	14
2.2.2	Protokollabweichung . . . . .	15
2.2.3	Mischformen . . . . .	15
2.3	Firewall . . . . .	15
2.3.1	Idee und Funktionsprinzip . . . . .	16
2.3.2	Zustandslos vs. Zustandsbehaftet . . . . .	17
<b>3</b>	<b>BPEL</b>	<b>19</b>
3.1	Historie . . . . .	19
3.2	Anwendungsbereiche . . . . .	20
3.3	Prozess, Instanz und Ausführungsumgebung . . . . .	20
3.4	Sprachkonstrukte . . . . .	22
3.4.1	Aktivitäten . . . . .	22
3.4.2	Gültigkeitsbereich, Fehlerbehandlung und Kompensation . . . . .	24
3.4.3	Prozessvariablen . . . . .	24
3.4.4	Links und Bedingungen . . . . .	25
3.4.5	Nachrichtenkorrelation . . . . .	25
<b>II</b>	<b>Konzept</b>	<b>27</b>
<b>4</b>	<b>Ausgangssituation</b>	<b>29</b>
4.1	Sicherheit in BPEL . . . . .	29
4.1.1	Integrität und Vertraulichkeit . . . . .	29
4.1.2	Verfügbarkeit . . . . .	29
4.2	Vorüberlegungen . . . . .	30

4.2.1	Schutzziel . . . . .	30
4.2.2	Schutzmethode . . . . .	30
4.2.3	Schutz gegen Angriffe mit Protokollabweichung . . . . .	31
4.3	Protokollschichtung bei BPEL . . . . .	31
4.3.1	Global und lokal beschriebene Protokolle . . . . .	32
4.3.2	Schutz bei lokalen Protokollbeschreibungen . . . . .	32
4.3.3	Schutz bei Protokollschichtung . . . . .	33
4.4	Zustandsverfolgung in der Firewall . . . . .	33
<b>5</b>	<b>Schutzkonzept</b>	<b>35</b>
5.1	Idee der Nachfolgermenge . . . . .	35
5.2	Der Nachfolgermengen-Automat . . . . .	35
5.2.1	Semantik der Zustände . . . . .	36
5.2.2	Transitionen und Konditionen . . . . .	38
5.2.3	Startzustand und Endzustand . . . . .	39
5.3	Der Nachfolgermengen-Algorithmus . . . . .	39
5.3.1	Vorherzustände, Nachherzustände . . . . .	40
5.3.2	Abbildung von Aktivitäten auf Teilautomaten . . . . .	40
5.3.3	Auflösung der Vorher- und Nachherzustände . . . . .	44
5.4	Flow - Nebenläufigkeit und Nachfolge . . . . .	46
5.4.1	Nebenläufigkeit im Nachfolgermengen-Automaten . . . . .	46
5.4.2	Erweiterung des Nachfolgermengen-Automaten . . . . .	48
<b>6</b>	<b>Instanzverwaltung und Schutzwirkung</b>	<b>53</b>
6.1	Identifikation von Web-Service-Nachrichten . . . . .	53
6.2	Nachrichtenzuordnung und Schutzwirkung . . . . .	54
6.2.1	Korrelationsgruppen und Eigenschaften . . . . .	54
6.2.2	Kandidatenlisten . . . . .	55
6.3	Instanzverwaltung und Termination . . . . .	55
<b>III</b>	<b>Implementierung</b>	<b>57</b>
<b>7</b>	<b>Rahmenbedingungen</b>	<b>59</b>
7.1	Ablaufumgebung . . . . .	59
7.1.1	Architektur . . . . .	59
7.1.2	Ereignisverkettung . . . . .	59
7.1.3	Erreichbarkeit von Nachrichten . . . . .	61
7.1.4	Abgeleitete Vorgaben . . . . .	62
7.2	Optimierungsziele . . . . .	63
7.2.1	Minimierung des Speicherbedarfs . . . . .	63
7.2.2	Minimierung der Verarbeitungszeit pro Nachricht . . . . .	63
7.2.3	Minimierung der Entscheidungszeit . . . . .	63
7.2.4	Maximierung der Genauigkeit bei der Zustandsverfolgung . . . . .	63
7.2.5	Maximierung der Skalierbarkeit . . . . .	63
7.2.6	Maximierung der Unabhängigkeit von der BPEL-Engine . . . . .	64
7.2.7	Maximierung der Erweiterbarkeit der Implementierung . . . . .	64

<b>8 Konzeptumsetzung</b>	<b>65</b>
8.1 Übersicht	65
8.2 Der BPEL-Parser	66
8.3 Realisierung des Nachfolgermengen-Automaten	67
8.3.1 Auswertung von Transitionsbedingungen	69
8.3.2 Instantiierung und Termination	69
8.3.3 Grafische Aufbereitung mit DOT	69
8.4 Realisierung des Nachfolgermengen-Algorithmus	70
8.4.1 Kreuzweben und weitere Verarbeitungsschritte	71
8.4.2 Terminationserkennung	71
8.4.3 Realisierung von Nebenläufigkeit	72
8.5 Nachrichtenkorrelation	72
8.5.1 Globale Zuordnungen	73
8.5.2 Ereignisbasierte Evaluation von XPath-Ausdrücken	73
8.5.3 Realisierung der Nachrichtenverarbeitung	74
8.5.4 Korrelationsmengen und Kandidatenlisten	75
<b>9 Evaluation</b>	<b>77</b>
9.1 Testprozess und Entwicklertests	77
9.2 Test der Schutzwirkung	78
9.2.1 Kennzahlen der Angriffe	78
9.2.2 Auswertung	79
9.3 Test der Zustandsverwaltung	79
9.3.1 Kennzahlen des Angriffs	80
9.3.2 Auswertung	80
<b>IV Diskussion</b>	<b>81</b>
<b>10 Bewertung der Implementierung</b>	<b>83</b>
10.1 Einschränkungen der Implementierung gegenüber dem Konzept	83
10.1.1 Auswertung von Konditionen	83
10.1.2 Fehler- und Kompensationsverarbeitung	84
10.1.3 Erreichbarkeit von Nachrichten	84
10.2 Vorteil des ereignisbasierten Ansatzes	84
10.3 Umsetzung der Optimierungsziele	84
10.3.1 Minimierung des Speicherbedarfs pro Prozessinstanz	84
10.3.2 Minimierung der Verarbeitungszeit pro Nachricht	85
10.3.3 Minimierung der Entscheidungszeit	85
10.3.4 Maximierung der Genauigkeit bei der Zustandsverfolgung	85
10.3.5 Maximierung der Skalierbarkeit	86
10.3.6 Maximierung der Unabhängigkeit von der BPEL-Engine	86
10.3.7 Maximierung der Erweiterbarkeit der Implementierung	86
<b>11 Gesamtbewertung und Ausblick</b>	<b>87</b>
11.1 Offene Probleme	87
11.1.1 Fehlerbehandlung und Kompensation	87
11.1.2 Nebenläufigkeitsprobleme mit <code>pick</code>	87
11.1.3 Praxistauglichkeit des Konzeptes	88
11.2 Fazit	88

11.3 Ausblick . . . . .	88
<b>V Anhänge</b>	<b>89</b>
<b>A BPEL-Beispieldokument</b>	<b>91</b>
<b>B Testprozess</b>	<b>95</b>