

Inhaltsverzeichnis

Abkürzungsverzeichnis	XIII
1 Einleitung.....	1
2 IT-Sicherheit und Intrusion Detection.....	5
2.1 IT-Sicherheit	5
2.2 Sicherheitsmechanismen.....	7
2.3 Intrusion-Detection-Systeme	9
2.3.1 Ereigniskomponenten und Audit	10
2.3.2 Analyse- und Datenbankkomponenten	12
2.3.3 Reaktionskomponenten.....	18
2.4 Fazit	19
3 Missbrauchserkennung	21
3.1 Systemmodell und Informationsarten	22
3.2 Aktuelle Herausforderungen	25
3.2.1 Fehllalarme	26
3.2.2 Effiziente Erkennung	27
3.2.3 Fazit	28
4 Beispiele	29
4.1 Beispielumgebung Solaris	29
4.1.1 Schwachstellen.....	29
4.1.2 Audit-Funktion.....	31
4.2 Beispielattacken	32
4.2.1 Login-Attacke	33
4.2.2 PATH-Attacke	35
4.2.3 Link-Attacke	37
4.2.4 Nebenläufige Link-Attacke.....	39
5 Semantische Aspekte von Angriffssignaturen.....	41
5.1 Aktive Datenbanksysteme	42
5.1.1 Ereignisse in aktiven Datenbanken.....	42
5.1.2 Unterschiede zum Signaturkonzept	43

5.2	Ereignisse – Begriffseinführung	44
5.3	Dimensionen der Semantik von Signaturen.....	49
5.4	Ereignismuster	51
5.4.1	Typ und Reihenfolge	52
5.4.2	Häufigkeit	53
5.4.3	Kontinuität	56
5.4.4	Nebenläufigkeit.....	56
5.4.5	Kontextbedingungen.....	57
5.5	Selektion der Schrittinstanzen.....	57
5.6	Konsum von Schrittinstanzen	59
5.6.1	Aktionsfolgen und Aktionssemantik.....	60
5.6.2	Auswahl von Schrittkombinationen.....	60
5.6.3	Schrittkombinationen.....	62
5.7	Zusammenfassung	65
6	Modell für Angriffssignaturen.....	67
6.1	Signaturnetze – Das allgemeine Modell	67
6.2	Modellierungselemente im Detail.....	69
6.2.1	Plätze.....	69
6.2.2	Transitionen	70
6.2.3	Kanten.....	72
6.2.4	Token	72
6.2.5	Schaltregel	75
6.2.6	Charakteristische Netztopologien	80
6.3	Eine Beispielsimulation	86
6.4	Formale Definition eines Signaturnetzes	89
6.5	Ausdrucksstärke.....	98
6.5.1	Ereignismuster	98
6.5.2	Instanzelektion	106
6.5.3	Instanzkonsum	106
6.6	Verwandte Ansätze	108
6.6.1	Automatenbasierte Signaturmodellierung	108
6.6.2	Graphenbasierte Signaturmodellierung	110
6.6.3	Netzbasierte Signaturmodellierung.....	110
6.7	Zusammenfassung	111
7	Beschreibung von Angriffssignaturen.....	113
7.1	Signaturentwicklung	113
7.2	Regelbasierte Signaturbeschreibung.....	115
7.2.1	Expertensysteme	116
7.2.2	Expertensystembasierte Missbrauchserkennung	117

7.2.3	Probleme expertensystembasierter Missbrauchs- erkennung.....	119
7.2.4	Regelbasierte Signaturbeschreibung.....	123
7.3	SHEDEL – Eine einfache ereignisbasierte Beschreibungssprache.....	123
7.3.1	Beschreibungselemente von SHEDEL	124
7.3.2	Beispiele.....	127
7.3.3	Diskussion.....	131
7.4	EDL.....	132
7.4.1	Basiskonzepte	132
7.4.2	Beispiel	139
7.4.3	Diskussion.....	141
7.5	Alternative Beschreibungszugänge.....	142
7.6	Zusammenfassung	144
8	Analyseverfahren	147
8.1	Stand der Technik	148
8.1.1	Abbildung in separate Programm-Module.....	148
8.1.2	Expertensystembasierte Analysen	151
8.2	Optimierungsstrategien.....	159
8.2.1	Strategie 1: Ereignistypbasierte Transitionsindizierung	159
8.2.2	Strategie 2: Tokenunabhängige Prüfung von Intra- Ereignis-Bedingungen	160
8.2.3	Strategie 3: Wertebasierte Tokenindizierung.....	161
8.2.4	Strategie 4: Gemeinsame Ausdrücke	164
8.2.5	Strategie 5: Kostenbasierte Bedingungspriorisierung.....	165
8.2.6	Diskussion.....	166
8.3	Das Analysewerkzeug SAM	168
8.4	Experimentelle Evaluierung.....	170
8.4.1	Testszenario	171
8.4.2	Vorgehensweise und Messumgebungen	176
8.4.3	Messergebnisse und Diskussion	177
8.5	Zusammenfassung	182
9	Zusammenfassung und Ausblick.....	185
10	Anhang.....	187
10.1	Signatur der nebenläufigen Link-Attacke in EDL	187
	Index.....	193
	Literatur	197