

Inhaltsverzeichnis

1	Einleitung	1
1.1	Problemstellung	2
1.2	Zielsetzung und Beiträge der Arbeit	4
1.3	Gliederung	7
2	Grundlagen	9
2.1	Terminologie	9
2.2	Bedrohungen im Internet	10
2.2.1	Denial-of-Service-Angriffe	12
2.2.2	Wurmausbreitungen	15
2.3	Angriffserkennung	16
2.3.1	Signatur-basierte Angriffserkennung	17
2.3.2	Anomalie-basierte Angriffserkennung	18
2.4	Stand der Forschung	20
2.4.1	Systeme zur Angriffserkennung	21
2.4.1.1	Hierarchisches System zur Angriffserkennung	24
2.4.2	Methoden zur Erkennung von Anomalien	27
2.5	Angreifermodell	30
2.5.1	Angreifermodell bei Angriffen erster Ordnung	31
2.5.2	Angreifermodell bei Angriffen zweiter Ordnung	32
2.6	Netzwerksimulatoren	33
2.6.1	Der zeitdiskrete Ereignissimulator OMNeT++	35

3	Ein flexibles Rahmenwerk zur Angriffserkennung	39
3.1	Dekomposition existierender Systeme zur Angriffserkennung	39
3.2	<i>Distack</i> – Rahmenwerk zur verteilten Angriffserkennung	43
3.2.1	Architektur und Zusammenspiel der einzelnen Bestandteile	45
3.2.2	Netzwerk-Abstraktion	48
3.2.3	Anomalie- und Angriffserkennung	49
3.2.3.1	Datenzentrisches Nachrichtensystem	51
3.2.3.2	Konfiguration	52
3.2.4	Externe Kommunikation	54
3.3	Implementierung	55
3.3.1	Generische Schnittstellen des Rahmenwerks	56
3.3.2	Hierarchische Anomalie-Erkennung mit Verfeinerung	60
3.3.3	Zustandsvisualisierung der Angriffserkennung	63
3.4	Leistungsbewertung	64
4	Werkzeuge zur Evaluierung einer Erkennung verteilter Angriffe	67
4.1	<i>ReaSE</i> – Realistische Simulationsszenarien für OMNeT++	69
4.2	Erzeugung realistischer Topologien	72
4.2.1	Powerlaw-Eigenschaft der Topologien	82
4.3	Generierung von realistischem Hintergrundverkehr	85
4.3.1	Verwendete Simulationsszenarien	92
4.3.2	Selbstähnlichkeit des Verkehrs	92
4.3.3	Protokollverteilung auf Transportschicht	96
4.4	Simulation verteilter Angriffe	100
4.5	Leistungsbewertung der Simulationsumgebung <i>ReaSE</i>	102
4.5.1	Leistungsbewertung von <i>Distack</i> mit Hilfe von <i>ReaSE</i>	104
4.6	<i>PktAnon</i> – Anonymisierung von Netzverkehr	106
5	Mechanismen einer dezentralen Angriffserkennung	111
5.1	Problemstellung und Anforderungen	111
5.2	Identifikation von Angriffen auf Basis erkannter Anomalien	114
5.2.1	Stand der Forschung	114
5.2.1.1	Zur Identifikation von Angriffen nutzbare Verfahren	116

5.2.2	Iterative Identifikation von Angriffen	119
5.2.3	Modellierung der Entitäten einer Angriffserkennung	121
5.2.3.1	Verallgemeinertes Modell	121
5.2.3.2	Konkretisierung erkennbarer Anomalien	125
5.2.3.3	Konkretisierung beschreibbarer Angriffe	126
5.2.3.4	Angriffshierarchie	128
5.2.4	Autonome, adaptive Ablaufsteuerung	129
5.2.5	Identifikation von Angriffen	134
5.2.6	Implementierung	141
5.2.7	Evaluierung	145
5.2.7.1	Evaluierungsumgebung	146
5.2.7.2	Fallbeispiele anhand eines TCP SYN-DDoS-Angriffs	148
5.2.7.3	Simulative Evaluierung bei unterschiedlichen Angriffen	152
5.3	Dezentrale Kooperation verteilter Erkennungssysteme	155
5.3.1	Stand der Forschung	155
5.3.2	Dezentrale Kooperation	161
5.3.2.1	Prinzip der lokalen Validierung	163
5.3.2.2	Metrik-basierte Entscheidungsfindung	165
5.3.2.3	Nachbarfindung und Kommunikation	170
5.3.2.4	Analyse der Angreifbarkeit der dezentralen Kooperation	174
5.3.3	Implementierung	178
5.3.3.1	Erweiterung von <i>ReaSE</i> um die dezentrale Kooperation	178
5.3.3.2	Metrik-basierte Entscheidungsfindung	183
5.3.4	Evaluierung	185
5.3.4.1	Methodik	186
5.3.4.2	Erste Ergebnisse am Beispiel einfacher Szenarien	188
5.3.4.3	Simulative Evaluierung der dezentralen Kooperation	196
6	Zusammenfassung und Ausblick	207
6.1	Ergebnisse der Arbeit	207
6.2	Ausblick	210
A	Benutzbarkeit durch GUIs	211
A.1	<i>Distack</i>	211
A.2	<i>ReaSE</i>	213

B Zur Identifikation verwendbare Konkretisierung des verallgemeinerten Modells	217
C Weitere Evaluierungsergebnisse der dezentralen Kooperation	225
Literaturverzeichnis	231
Stichwortverzeichnis	249