

Inhaltsverzeichnis

1 Einleitung	1
1.1 Problemstellung und Zielsetzung	1
1.2 Thematische Abgrenzung der Arbeit	3
1.3 Die Arbeit im Überblick	4
2 Von klassischer zu mehrseitiger IT-Sicherheit	7
2.1 Interpretation des IT-Sicherheitsbegriffs	7
2.2 Datenschutz	8
2.3 Klassische schutzwürdige Belange	9
2.4 Mehrseitige IT-Sicherheit	10
2.5 Realisierung mehrseitig sicherer Systeme	12
3 Audit und Intrusion Detection	13
3.1 Die Sicherheitsfunktion Audit	13
3.1.1 Funktionale Integration und Informationsgehalt	14
3.1.2 Zu erwartende Datenaufkommen	17
3.1.3 Schutz der Funktionseinheiten und Auditdaten	18
3.1.4 Analyse der Auditdaten	20
3.2 Intrusion Detection	21
3.2.1 Grundlegende Analysekonzepte	21
3.2.2 Die Analysekonzepte im Vergleich	23
3.3 Intrusion Detection-Systeme	26
3.3.1 Eine Klassifikation	26

7.1.13	Weiterentwicklung des Intrusion Detection-Systems	94
7.2	De-/Pseudonymisierungskonzept für AID	95
7.2.1	Pseudonymisierung mittels der Agenten	95
7.2.2	Depseudonymisierung durch das Expertensystem	96
7.2.3	Signaturen mit selektivem Nutzerbezug	96
7.2.4	Archivierung von Auditdaten und Analyseergebnissen	97
7.3	Verwendbare LiSA-basierte Chiffrierverfahren	98
7.3.1	Anforderungen an die Kryptofunktionen	98
7.3.2	Die Kryptobibliothek LiSA	99
	Stromchiffren	100
	Blockchiffren	101
7.4	Die Implementation	102
7.4.1	Implementation typ- und komponentenspezifischer Funktionen	102
7.4.2	Skalierbarer Pseudonymisierungsumfang	103
7.4.3	Erweiterung der Agenten	103
7.4.4	Modifikation des Expertensystems	104
8	Bewertung des Ansatzes	105
8.1	Die verwendeten Kryptoalgorithmen	105
8.2	Die verursachte Mehrbelastung	107
8.2.1	Mehrbelastung der überwachten Zielsysteme	107
8.2.2	Mehrbelastung der Überwachungsstation	109
8.3	Vertraulichkeitsschutz der Implementation	110
8.3.1	Resistenz des DES	111
8.3.2	Resistenz des RC5	112
8.3.3	Der verwendete Chiffriermodus	113
8.3.4	Die zugrundeliegenden Blockgrößen	114
8.3.5	Der erreichte Vertraulichkeitsschutz	114
8.4	Einige kryptographische Alternativen	115
8.4.1	Vergrößerung der Blockgrößen für long-Einträge	115

8.4.2	Injective Verschlüsselung	115
8.4.3	Extensivere Verschlüsselung von Pfaden	116
8.4.4	Datensensitives Padding	116
8.5	Grenzen, Restrisiken und flankierende Maßnahmen	117
8.5.1	Schwachpunkte von Kryptosystemen	117
8.5.2	Pseudonymes Audit in kleineren Netzen	117
8.5.3	Qualität und Sensitivität der Wissensbasen	118
8.5.4	Verwendung vertrauenswürdiger Wissensbasen	119
9	Pseudonymes Audit in den Common Criteria	121
9.1	Harmonisierung der IT-Sicherheitskriterien	121
9.2	Funktionale Struktur des Teil 2 der CC	123
9.3	Funktionale Vorgaben für pseudonymes Audit	124
9.3.1	Bestandsaufnahme zur Pseudonymität	124
9.3.2	Bestandsaufnahme der Vorgaben zu Audit	126
9.4	Bewertung	127
10	Abschließende Anmerkungen und Ausblick	129
Literaturverzeichnis		132
A	Das AID-Auditdatenformat	143
B	Auszüge aus den CC 2.0	145