
Sicherheit unter dem Betriebssystem Unix

herausgegeben von
Dr. Heinrich Kersten
Dr. Hartwig Kreutz
Bundesamt für Sicherheit in der
Informationstechnik - BSI

Technische Hochschule Darmstadt	
FACHBEREICH INFORMATIK	
B I B L I O T H E K	
Inventar-Nr.:	21076
Sachgebiete:	D.5.V
Standort:	1994

R. Oldenbourg Verlag München Wien 1991

Inhalt

1.	Einleitung	1
1.1	Zielsetzung der Studie	1
1.2	Vorgehensweise	2
1.3	Zusammenfassung der Studienergebnisse	3
2.	Überblick	7
2.1	Übersicht über die Entwicklung von Unix	7
2.2	Standardisierung von Unix	9
2.3	Arbeiten zum Thema Sicherheit in Unix-Systemen	12
3.	Beschreibung sicherheitsrelevanter Funktionen	15
3.1	Testumgebung und Unterlagen	15
3.2	Das Unix Subjekt-Modell	15
3.3	Das Unix Objekt-Modell	18
3.4	Subjekt/Objekt-Schutzmechanismen	22
3.5	Sicherheitsrelevante Basisfunktionen auf dem Objekt/Subjektmodell	25
3.6	Systemintegrität	35
4.	Beschreibung wichtiger Systemsubjekte/-objekte	37
4.1	Sicherheitsrelevante Systemsubjekte	37
4.2	Sicherheitsrelevante Systemobjekte	40
5.	Implementierung des Sicherheitsmodells	49
5.1	Kern	49
5.2	Software Memory Management	53
6.	Sicherheitsrelevante Aufgaben	55
6.1	Administrative Aufgaben	55
6.2	Wie schützt man sich gegen ungewünschte Zugriffe?	58
6.3	Wie erweitere ich meine Rechte?	58
6.4	Benutzererkennung und ID	60
6.5	Zugriffe für mehrere Einzelpersonen	60
7.	Sicherheitsrisiken in Unix-Systemen	61
7.1	Implementierung eines Sicherheitskonzepts	61
7.2	Paßwörter	62
7.3	Der Superuser	63
7.4	Privilegierte Benutzer	64
7.5	Systemprogramme	65
7.6	Böswillige Programme	66
7.7	Verdeckte Kanäle	68

7.8	Benutzung des Systems	68
7.9	Linken von Directories	69
7.10	Trennung von Benutzeroberfläche und Kern	69
7.11	Hardware-Eigenschaften	70
7.12	Verhalten bei Fehlern	70
7.13	Szenarien für Systemangriffe/Praktische Beispiele	71
7.14	Was ist bei setuid-Programmen zu beachten?	72
7.15	Besondere Stärken und Schwächen von Unix	73
8.	Maßnahmen zur Gewährleistung/Erhöhung der Sicherheit in bestehenden Systemen	75
8.1	Organisatorische Maßnahmen	75
8.2	Einfache zusätzliche Funktionen	76
8.3	Änderungen der Betriebssystemquellen	77
8.4	Verfahren zur Einschränkung der Nutzung	77
8.5	Ändern der Besitzer	79
9.	Klassifizierung nach den TCSEC	81
9.1	Zuordnung von Unix zu den Gruppen der TCSEC	81
9.2	Gegenüberstellung der C1-Anforderungen und Unix-Funktionen	81
9.3	Anforderungen für Klasse C2	85
9.4	Anforderungen der Gruppe B	88
9.5	Erweiterungen zum Erreichen höherer Klassen	88
9.6	Bei einer Prüfung zu berücksichtigende Komponenten	89
9.7	Probleme bei der Anwendung der TCSEC auf Unix	89
10.	Klassifizierung nach einem nationalen Kriterienkatalog ...	93
10.1	Bei Unix implementierte Mechanismen	93
11.	Pflichtenheft für ein sicheres Unix	97
11.1	Überblick	97
11.2	Vorgehensweise für Erweiterungen	97
11.3	Zusammenstellung der Anforderungen	98
11.4	Ein Beispiel für ein C2-System – UTX32/S	101
12.	Alternativen für Beurteilungskriterien	103
12.1	Der theoretische Ansatz	103
12.2	Beurteilungskriterien für vorhandene Systeme	104
12.3	Anwendung eines Schichtenmodells auf Unix	104
12.4	Analyse anderer Systeme	105
Anhang A. Glossar		107
Anhang B. Kommandos und Systemaufrufe		111
Anhang C. Literaturverzeichnis		115