

H.6 Kombination der Verfahren

- Einsatz verschiedener Verfahren für verschiedene Betriebsmittel
 - ◆ Interne Betriebsmittel:
Verhindern von Verklemmungen durch totale Ordnung der Betriebsmittel (z.B. IBM Mainframe-Systeme)
 - ◆ Hauptspeicher:
Verhindern von Verklemmungen durch Entzug des Speichers (z.B. durch Swap out)
 - ◆ Betriebsmittel eines Jobs:
Angabe der benötigten Betriebsmittel beim Starten; Einsatz der Vermeidungsstrategie durch Feststellen unsicherer Zustände
 - ◆ Hintergrundspeicher (Swap space):
Vorausbelegung des Hintergrundspeichers

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

H-Deadlock.doc (1998-01-26 10:51)

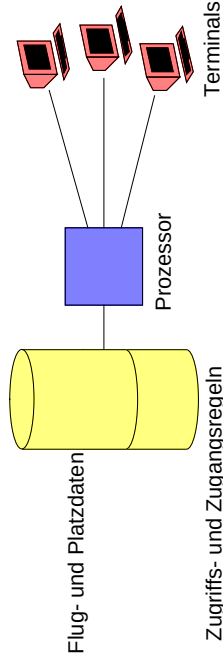
H.33

Reproduktion ist ohne Verwendung dieser Vorlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, gestattet. Bei der Reproduktion des Dokuments ist der Name des Autors anzugeben.

I Datensicherheit und Zugriffsschutz

I.1 Problemstellung

- Beispiel: Zugang zu einer Datenbank zur Flugreservierung und -buchung



- ◆ Was sind mögliche Beeinträchtigungen der Datensicherheit?

SP I

Systemprogrammierung I

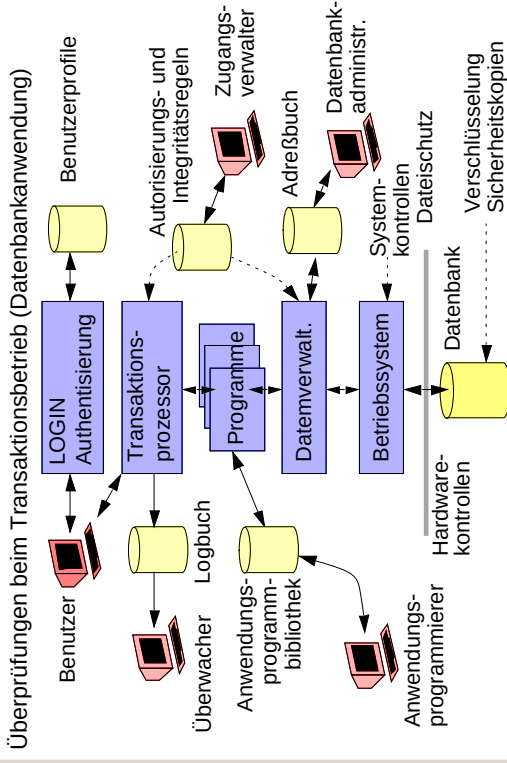
© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc (1998-01-28 09:05)

I.1

Reproduktion ist ohne Verwendung dieser Vorlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, gestattet. Bei der Reproduktion des Dokuments ist der Name des Autors anzugeben.

I.1 Problemstellung (2)



SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc (1998-01-28 09:05)

I.2

Reproduktion ist ohne Verwendung dieser Vorlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, gestattet. Bei der Reproduktion des Dokuments ist der Name des Autors anzugeben.

1 Umgebung der Rechenanlage

▲ Naturkatastrophen

- ◆ Erdbeben, Vulkanausbrüche etc. können Rechenanlage und Datenbestand zerstören

▲ Unfälle

- ◆ Gasexplosion, Kühlwasserlecks in der Klimaanlage oder Ähnliches zerstören Rechner und Daten

▲ Böswillige Angriffe

- ◆ Zerstörung der Rechenanlage und des Datenbestands durch Sabotage (Bombenanschlag, Brandanschlag etc.)

▲ Unbefugter Zutritt zu den Räumen des Rechenzentrums

- ◆ Diebstahl von Datenträgern
- ◆ Zerstörung von Daten
- ◆ Zugang zu vertraulichen Daten

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc (1998-01-28 09:05)

I.3

Reproduktion ist ohne Verwendung dieser Vorlage, außer zu Lehrzwecken an der Universität Erlangen-Nürnberg, gestattet. Bei der Reproduktion des Dokuments ist der Name des Autors anzugeben.

2	Systemsoftware		
	▲	Versagen der Schutzmechanismen	
	◆	System läßt Unbefugte auf Daten zugreifen oder Operationen ausführen	
	▲	Durchsickern von Informationen	
	◆	Anwender können anhand scheinbar unauffälligen Systemverhaltens Rückschlüsse auf vertrauliche Daten ziehen (<i>Covert channels</i>)	
3	Systemprogrammierer		
	▲	Umgehen oder Abschalten der Schutzmechanismen	
	▲	Installation eines unsicheren Systems	
	◆	erlaubt dem Systemprogrammierer die Schutzmechanismen von außen zu umgehen	
SP I	Systemprogrammierung I © Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998 Reproduktion oder andere Verwendung dieser Unterlagen ohne in schriftlicher Form die Zustimmung der Universität Erlangen-Nürnberg ist ausdrücklich untersagt.		
			I.4
4	Rechnerhardware		
	▲	Versagen der Schutzmechanismen	
	◆	erlauben nicht-autorisierten Zugriff	
	▲	Fehlerhaft Befehlsausführung	
	◆	Zerstörung von wichtigen Daten	
	▲	Abstrahlungen	
	◆	erlaubt Ausspähen von Daten	
5	Datenbasis		
	▲	Falsche Zugriffsregeln	
	◆	erlauben nicht-autorisierten Zugriff	
SP I	Systemprogrammierung I © Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998 Reproduktion oder andere Verwendung dieser Unterlagen ohne in schriftlicher Form die Zustimmung der Universität Erlangen-Nürnberg ist ausdrücklich untersagt.		
			I.5

6	Operateur		
	▲	Kopieren vertraulicher Datenträger	
	▲	Diebstahl von Datenträgern	
	▲	Initialisierung mit unsicherem Zustand	
	◆	Operateur schaltet beispielsweise Zugriffskontrolle ab	
7	Sicherheitsbeauftragter		
	▲	Fehlerhafte Spezifikation der Sicherheitspolitik	
	◆	dadurch Zugang für Unbefugte zu vertraulichen Daten oder	
	◆	Änderungen von Daten durch Unbefugte möglich	
SP I	Systemprogrammierung I © Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998 Reproduktion oder andere Verwendung dieser Unterlagen ohne in schriftlicher Form die Zustimmung der Universität Erlangen-Nürnberg ist ausdrücklich untersagt.		
			I.6
8	Kommunikationssystem		
	▲	Abhören der Kommunikationsleitungen	
	◆	z.B. Telefonverbindung bei Modemnutzung oder serielle Schnittstellen	
	◆	Ermitteln von Paßwörtern und Benutzerkennungen	
	◆	Zugriff auf vertrauliche Daten	
	◆	unbefugte Datenveränderungen	
9	Terminal		
	▲	Ungeschützter Zugang zum Terminal	
	◆	Nutzen einer fremden Benutzerkennung	
	◆	Zugriff auf vertrauliche Daten	
	◆	unbefugte Datenveränderungen	
SP I	Systemprogrammierung I © Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998 Reproduktion oder andere Verwendung dieser Unterlagen ohne in schriftlicher Form die Zustimmung der Universität Erlangen-Nürnberg ist ausdrücklich untersagt.		
			I.7

10 Benutzer

- ▲ Nutzen anderer Kennungen
- ◆ erlauben nicht-autorisierten Zugriff
- ◆ unbefugte Datenveränderungen
- ◆ unbefugte Weitergabe von Informationen

11 Anwendungsprogrammierung

- ▲ Nichteinhalten der Spezifikation
- ◆ Umgehen der Zugriffskontrollen

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc 1998-01-28 09.05

Reproduktion oder die oder Verwendung dieser Unterlagen ohne in Schriftwechsel mit der Universität Erlangen-Nürnberg constituiert die Zustimmung des Autors.

I.8

12 "Tracker Queries"

- Beispiel: Datenbanksysteme
- ◆ Zugriff auf Einzelinformationen ist verboten (Vertraulichkeit)
- ◆ statistische Informationen sind erlaubt
- ▲ Grenzen möglicher Sicherheitsmaßnahmen:
Zugriff auf Einzelinformationen dennoch möglich
- ◆ geeignete Anfragen kombinieren (*Tracker queries*)
- Beispiel: Gehaltsdatenbank

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc 1998-01-28 09.05

Reproduktion oder die oder Verwendung dieser Unterlagen ohne in Schriftwechsel mit der Universität Erlangen-Nürnberg constituiert die Zustimmung des Autors.

I.9

12

"Tracker Queries" (2)

■ Tabelle der Datenbankbeiträge:

Nr.	Name	Geschl.	Fach	Stellung	Gehalt	Spenden
1	Albrecht	m	Inf.	Prof.	60.000	150
2	Bergner	m	Math.	Prof.	45.000	300
3	Cäsar	w	Math.	Prof.	75.000	600
4	David	w	Inf.	Prof.	45.000	150
4	Engel	m	Stat.	Prof.	54.000	0
5	Frech	w	Stat.	Prof.	66.000	450
6	Groß	m	Inf.	Angest.	30.000	60
8	Hausner	m	Math.	Prof.	54.000	1500
9	Ibel	w	Inf.	Stud.	9.000	30
10	Jost	m	Stat.	Angest.	60.000	45
11	Knapp	w	Math.	Prof.	75.000	300
12	Ludwig	m	Inf.	Stud.	9.000	0

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc 1998-01-28 09.05

Reproduktion oder die oder Verwendung dieser Unterlagen ohne in Schriftwechsel mit der Universität Erlangen-Nürnberg constituiert die Zustimmung des Autors.

I.10

12

"Tracker Queries" (3)

- Anfragen und Antworten:
- ◆ Anzahl('w'): 5
- ◆ Anzahl('w' und (nicht 'Inf' oder nicht 'Prof.')): 4
- ◆ mittlere Spende('w'): 306
- ◆ mittlere Spende('w' und (nicht 'Inf' oder nicht 'Prof.')): 345
- Berechnung:
- ◆ Spende('David'): $306 * 5 - 345 * 4 = 1530 - 1380 = 150$

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc 1998-01-28 09.05

Reproduktion oder die oder Verwendung dieser Unterlagen ohne in Schriftwechsel mit der Universität Erlangen-Nürnberg constituiert die Zustimmung des Autors.

I.11

I.2 Zugriffslisten

- Identifikation von Subjekten, Objekten und Berechtigungen
 - ◆ Subjekt: Person oder Benutzerkennung im System (repräsentiert jemanden, der Aktionen ausführen kann)
 - ◆ Objekt: Komponente des Systems (repräsentiert Ziel einer Aktion)
 - ◆ Berechtigung: z.B. Leseberechtigung auf einer Datei (repräsentiert die Erlaubnis für die Ausführung einer Aktion)
- Erfassung der Berechtigungen in einer Subjekt-Objekt-Matrix: Zugriffsliste (*Access control list, ACL*)

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc: 1998-01-28 09:05

Reproduzieren oder Abdruck ist ohne Genehmigung der Universität Erlangen-Nürnberg strafbar. Jeder der Zustimmung des Autors.

I.12

1 Beispiel für Zugriffslisten

- Personaldatensatz
 - ◆ besteht aus: **Name**, **Abteilung**, **Personalnummer**, **Lohn- oder Gehaltsgruppe**
- Personaldateien (Objekte)
 - ◆ D_{LA} : Personaldaten der leitenden Angestellten
 - ◆ D_{AN} : Personaldaten der sonstigen Angestellten
 - ◆ D_{AR} : Personaldaten der Arbeiter
- Prozeduren (gehören zu den Aktionen)
 - ◆ R_{LA} : Lesen von Pers.-Nr. und Lohn-/Gehaltsgr. aus D_{LA}
 - ◆ $R_{AN/AR}$: Lesen von Pers.-Nr. und Lohn-/Gehaltsgr. aus D_{AN} oder D_{AR}
 - ◆ R_{post} : Lesen von Name, Abteilung und Pers.-Nr.

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc: 1998-01-28 09:05

Reproduzieren oder Abdruck ist ohne Genehmigung der Universität Erlangen-Nürnberg strafbar. Jeder der Zustimmung des Autors.

I.13

1 Beispiel für Zugriffslisten (2)

- Benutzer (Subjekte)
 - ◆ S_{pers} : Leiter des Personalbüros
 - Besitzer aller Dateien und Prozeduren
 - Lese- und Schreibrecht für alle Dateien
 - Aufrufrecht für alle Prozeduren
 - ◆ S_{stellv} : Sachbearb. leitende Angestellte, stellvertr. Leiter Personalbüro
 - Lese- und Schreibrecht für D_{AN} und D_{AR}
 - Aufrufrecht für R_{LA}
 - ◆ S_{sach} : Sachbearbeiter Angestellte u. Arbeiter
 - Aufrufrecht für $R_{AN/AR}$
 - ◆ S_{post} : Poststelle
 - Aufrufrecht für R_{post} auf alle Dateien

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc: 1998-01-28 09:05

Reproduzieren oder Abdruck ist ohne Genehmigung der Universität Erlangen-Nürnberg strafbar. Jeder der Zustimmung des Autors.

I.14

1 Beispiel für Zugriffslisten (3)

- Berechtigungen werden in Matrix ausgedrückt:

	D_{LA}	D_{AN}	D_{AR}	R_{LA}	$R_{AN/AR}$	R_{post}
S_{pers}	O, R, W	O, R, W	O, R, W	O, I	O, I	O, I
S_{stellv}		R, W	R, W	I		
S_{sach}					I	
S_{post}						I
R_{LA}	R					
$R_{AN/AR}$		R	R			
R_{post}	R	R	R			

- O = *Owner*, Besitzer der Datei oder Prozedur
- R = *Read*; volle Leseberechtigung
- W = *Write*; volle Schreibberechtigung
- I = *Invoke*; Aufrufberechtigung

SP I

Systemprogrammierung I

© Franz J. Hauck, Universität Erlangen-Nürnberg, IMMD IV, 1998

I-Security.doc: 1998-01-28 09:05

Reproduzieren oder Abdruck ist ohne Genehmigung der Universität Erlangen-Nürnberg strafbar. Jeder der Zustimmung des Autors.

I.15