Informatik
Hauptcampus

H O C H
S C H U L E
T R I E R

Systemadministration
Teil 4

Prof. Dr.-Ing. Jörn Schneider

WIEDERHOLUNG

Betriebssystemkonzepte

- **Prozesse**
- Adressraum
- Files
- Protection

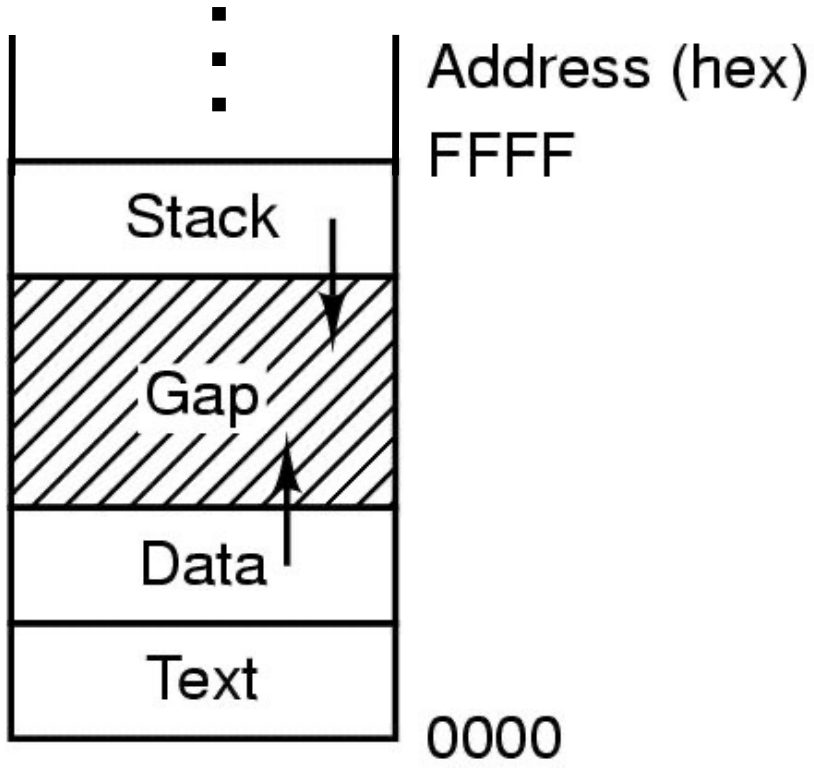
Prozess

- Instanz eines Programmes mit eigenem Ausführungskontext
- Zum Ausführungskontext gehören Ressourcen wie:
  - Befehlszähler
  - Inhalt von Statusregistern
  - Stack
  - Sonstige Daten im Hauptspeicher
  - Informationen über offene Dateien, etc.

Betriebssystemkonzepte

- Prozesse
- **Adressraum**
- Files
- Protection

Speichersegmente



- Processes have three segments: text, data, stack

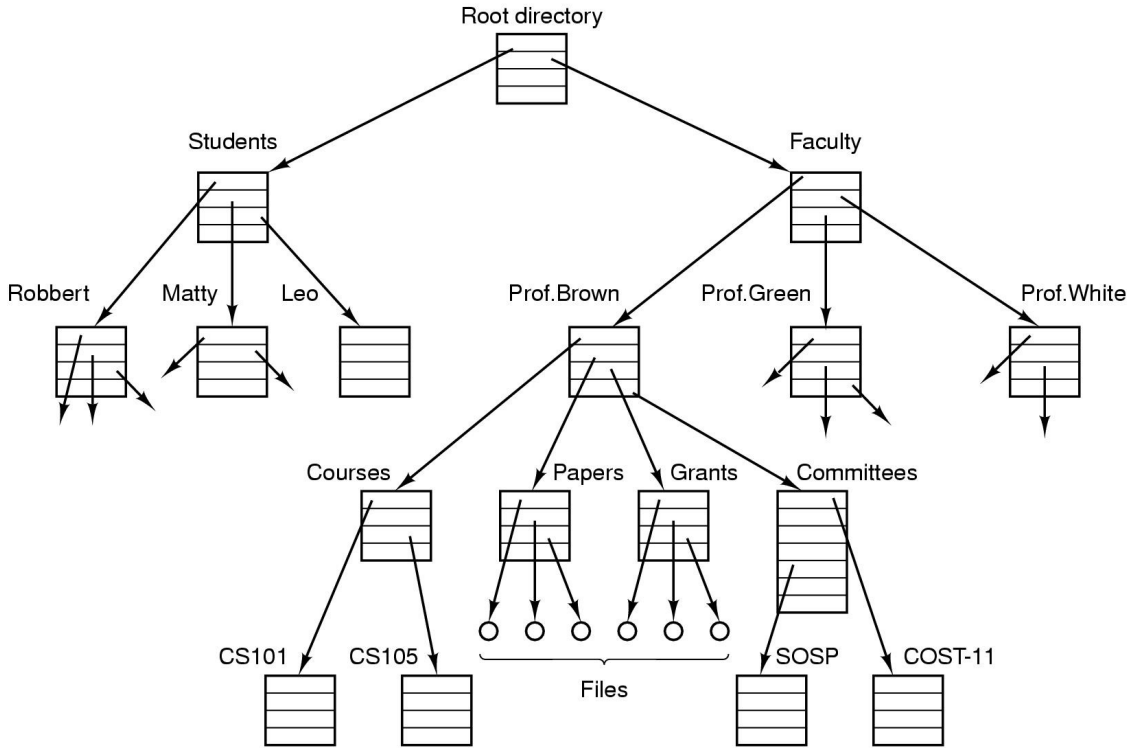
Paging: Ablaufschritte

1. Bei Page Fault wird Trap (Interrupt) ausgelöst
2. OS sichert wenig benutzte Page auf Festplatte
3. OS lädt angefragte Page in Speicher
4. OS ändert MMU Mapping, d.h. die Seitentabelle des Prozesses
5. OS kehrt zum Befehl zurück, der Trap auslöste

Betriebssystemkonzepte

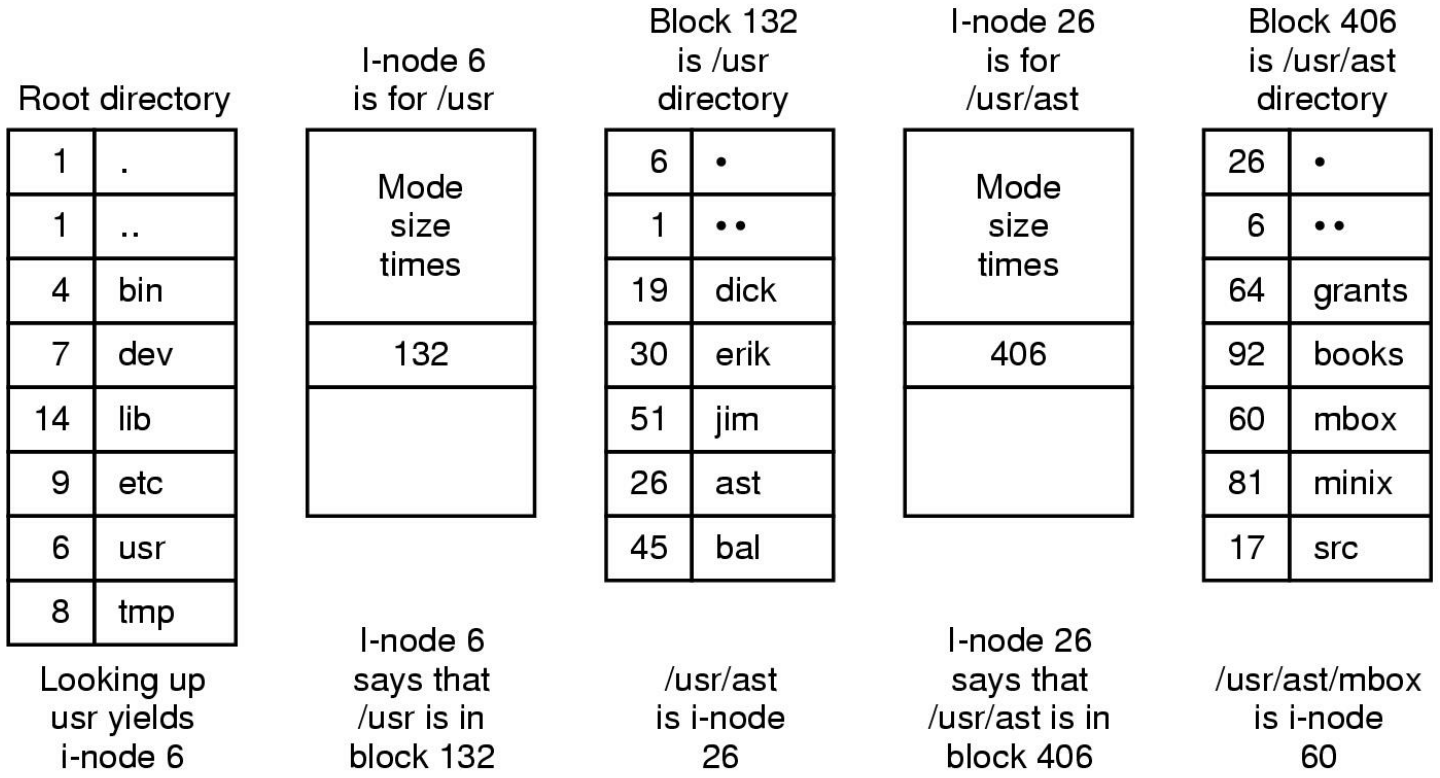
- Prozesse
- Adressraum
- **Files**
- Protection

Verzeichnisstruktur



File system for a university department

Verzeichnisse und i-Nodes



The steps in looking up */usr/ast/mbox*

Betriebssystemkonzepte

- Prozesse
- Adressraum
- Files
- **Protection**

Beispiel UNIX (I)

- Prozesse können auf Speicherbereiche anderer Prozesse nur zugreifen, wenn dies explizit erlaubt ist
  - Beispiel: Kommunikation über Shared Memory
- Benutzer haben eindeutige Nummer: UID
  - 0 = root
- Benutzer gehören zu mindestens einer Gruppe
- Gruppen haben eindeutige Nummer: GID
- Prozess erbt UID und GID des startenden Users

Beispiel UNIX (II)

- Dateien haben einen Besitzer, eine Gruppe und Rechte für:
  - User (=Besitzer)
  - Group (=Gruppe)
  - Others (=Alle anderen)
- Für jede Kategorie drei Basisrechte:
  - r = read
  - w = write
  - x = execute
- Beispiel: ***rwxr-x--x***
  - Besitzer: lesen, schreiben und ausführen
  - Gruppe: lesen und ausführen
  - Rest: ausführen

WIEDERHOLUNG - ENDE

Teil 4

- Was ist ein Rechnersystem?
- Was ist ein Betriebssystem?
- Aufgaben eines Systemadministrators
- Rechneraufbau
- Betriebssystemkonzepte
- **Benutzer**

Warum mehrere Benutzer?

- Kosten
  - Historisch:
    - Mehrfachnutzung des gleichen Systems (Batch Systeme)
- Personalisierung
- Datenschutz

Konzepte zum Thema Benutzer

- Anmeldung
  - Authentifizierung
  - Ausführungsumgebung
- Rechte
  - CPU
  - Speicher (Arbeitsspeicher)
  - Prozesse
  - Dateien
  - Speicherplatz (Hintergrundspeicher, z.B. Festplatte)

Authentifizierung

- Authentifizieren – <griech.> die Echtheit bezeugen
- Identifizieren des Benutzers und überprüfen, ob die „Behauptung“ glaubwürdig ist

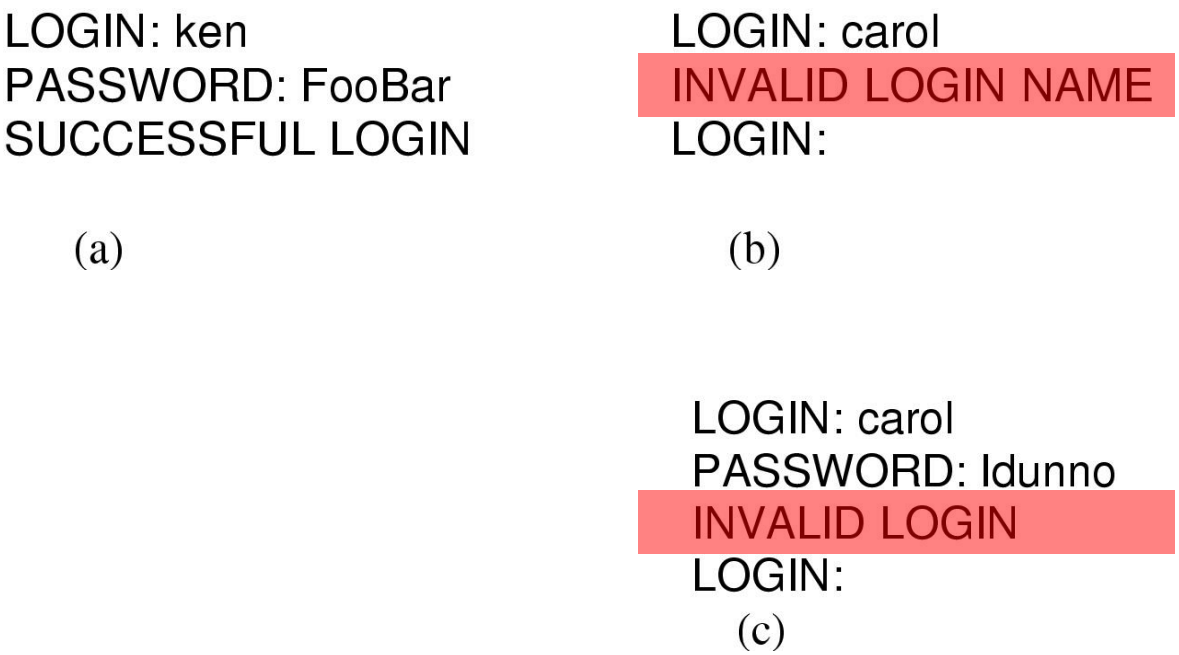
User Authentication

Basic Principles. Authentication must identify:

1. Something the user knows
2. Something the user has
3. Something the user is

This is done before user can use the system

Authentication Using Passwords



(a) A successful login

(b) Login rejected after name entered

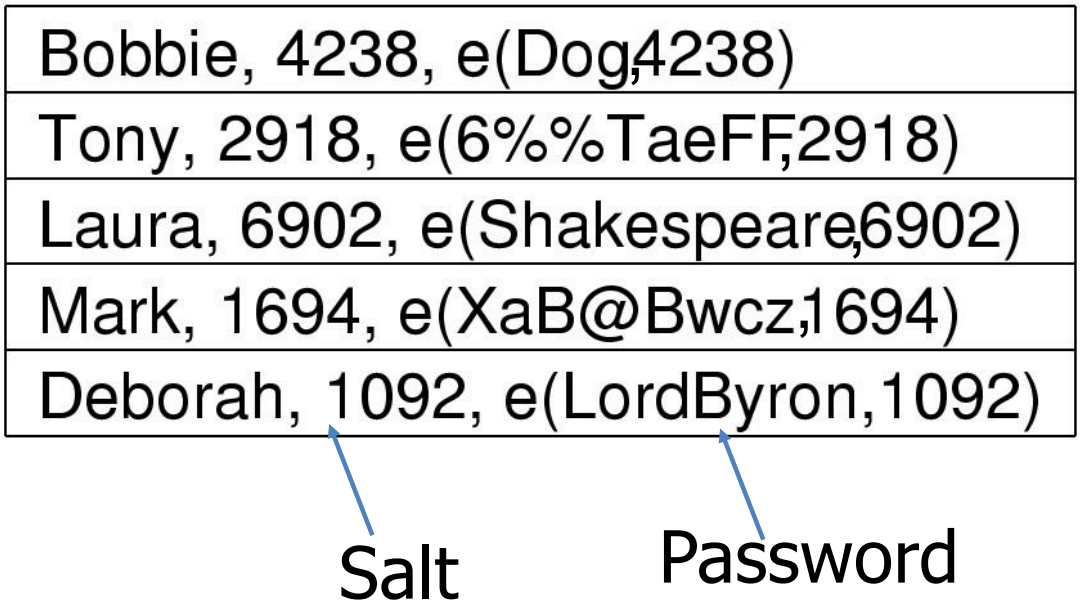
(c) Login rejected after name and password typed

Authentication Using Passwords

```
LBL> telnet elxsi
ELXSI AT LBL
LOGIN: root
PASSWORD: root
INCORRECT PASSWORD, TRY AGAIN
LOGIN: guest
PASSWORD: guest
INCORRECT PASSWORD, TRY AGAIN
LOGIN: uucp
PASSWORD: uucp
WELCOME TO THE ELXSI COMPUTER AT LBL
```

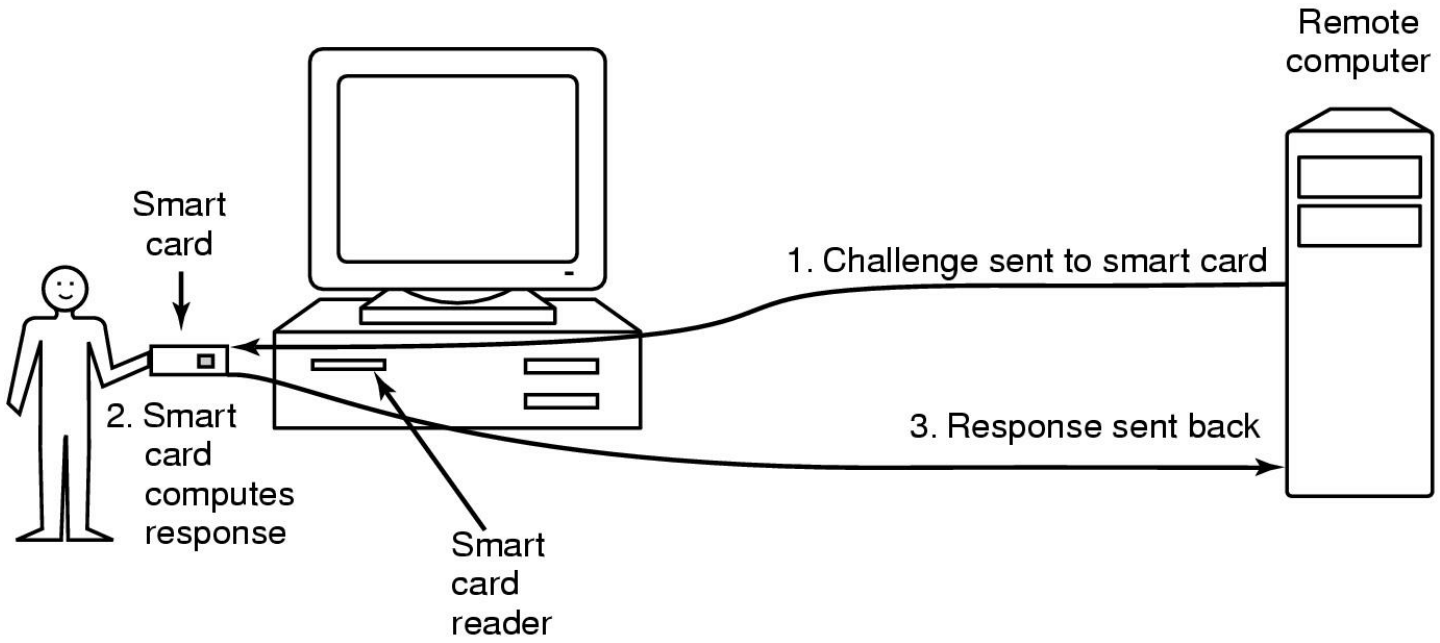
- How a cracker broke into LBL
  - a U.S. Dept. of Energy research lab

Authentication Using Passwords



The use of salt to defeat precomputation of encrypted passwords

Authentication Using a Physical Object



- Magnetic or chip cards
  - magnetic stripe cards
  - chip cards: stored value cards, smart cards

Authentifizierung über biometrische Merkmale

- Fingerabdrucksensor
- Gesichtserkennung
- Stimmerkennung
- …

ANMELDUNGSVORGANG

Anmeldungsvorgang - klassisch

1. Benutzer gibt seinen Usernamen an
2. System verlangt Passwort
3. Benutzer gibt Passwort ein
4. System überprüft Passwort
5. Benutzer wird im System registriert
6. Vorbereitung/Ausführung der Benutzerumgebung
7. Benutzer kann arbeiten
8. Benutzer meldet sich ab
9. System registriert Abmeldung

Beispiel UNIX (I)

- Beim anmelden, suche nach User (z.B. notroot) in
  - /etc/passwd
- Username gefunden ➔
  - Verschlüsseln eingegebenes Passwort
  - Vergleich mit abgelegtem Passwort
- Vergleich OK ➔
  - Starte Shell

Beispiel UNIX (II)

- /etc/passwd
- Jede Zeile ein User, mit Einträgen:
  - Benutzername
  - Verschlüsseltes Passwort (**heute: ‚x', da Passwort in /etc/shadow**)
  - UID (User ID)
  - GID (ID der primären Gruppe des Users)
  - Kommentarfeld (Name des Benutzers)
  - Home-Verzeichnis
  - Shell die der User verwendet
- Bsp.:
  `hugo:x:1047:1000:Hugo Müller:/home/hugo:/bin/bash`

Beispiel UNIX (III)

- /etc/shadow
- Enthält verschlüsselte Passwörter anstelle von /etc/passwd
- Steuert Passwort Aging

Beispiel UNIX (IV)

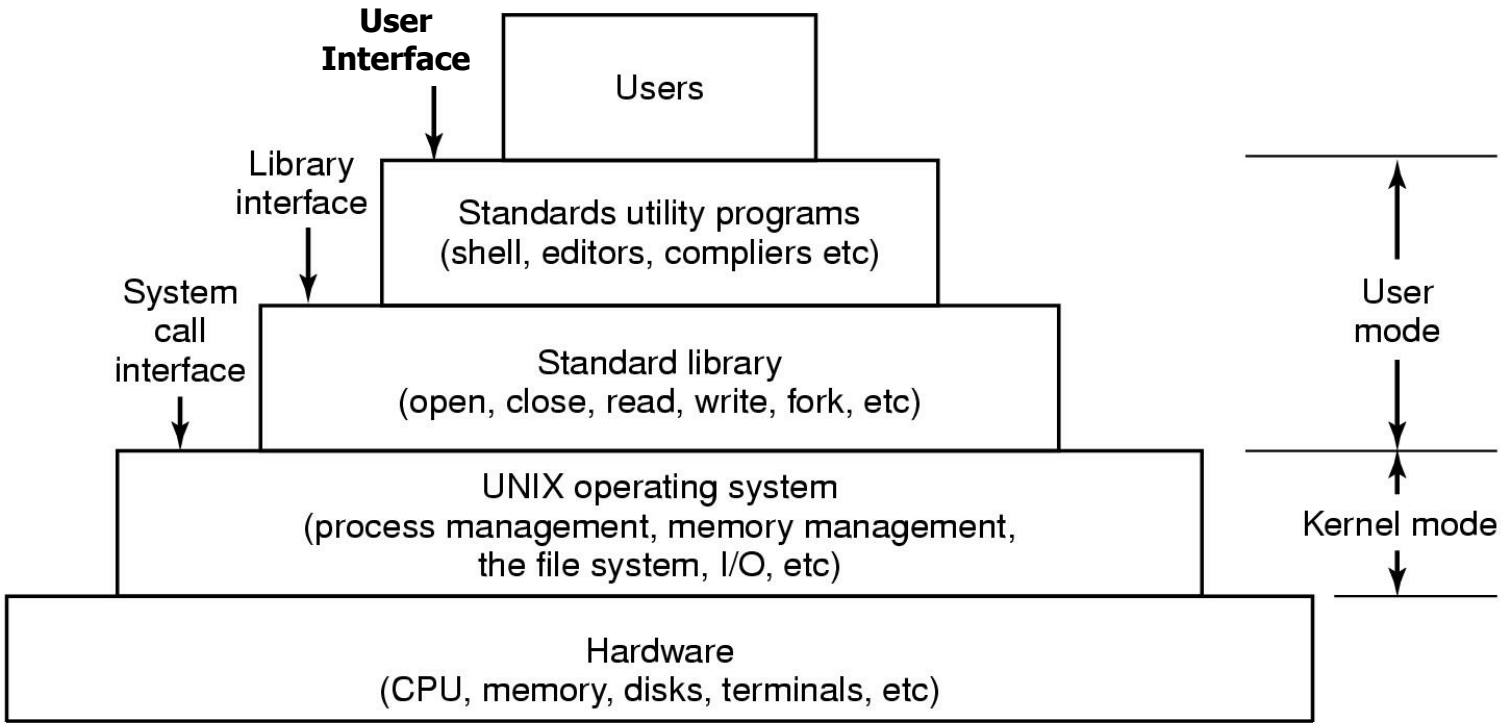
- Bei erfolgreicher Anmeldung:
  - Eintrag in utmp file (Ubuntu Linux: /var/log/utmp)
    - Anzeige über `who`
  - Setzen der Umgebungsvariablen
  - Wechsel in Home-Verzeichnis
  - Ausführung der Login Skripte in aktueller Prozessumgebung, z.B.:
    - .profile
    - .bashrc

RECHTE

Rechteebenen

- Hardware
- Betriebssystem
- Systemprogramme
- Anwendungssoftware

UNIX


User Interface
Users
Library interface
Standards utility programs (shell, editors, compliers etc)
System call interface
Standard library (open, close, read, write, fork, etc)
UNIX operating system (process management, memory management, the file system, I/O, etc)
Hardware (CPU, memory, disks, terminals, etc)
User mode
Kernel mode

Quizfragen

- Wie wird verhindert, dass Anwender unberechtigt in Kernelmodus wechseln?
- Wie erfolgt ein Wechsel in den Kernelmodus überhaupt?

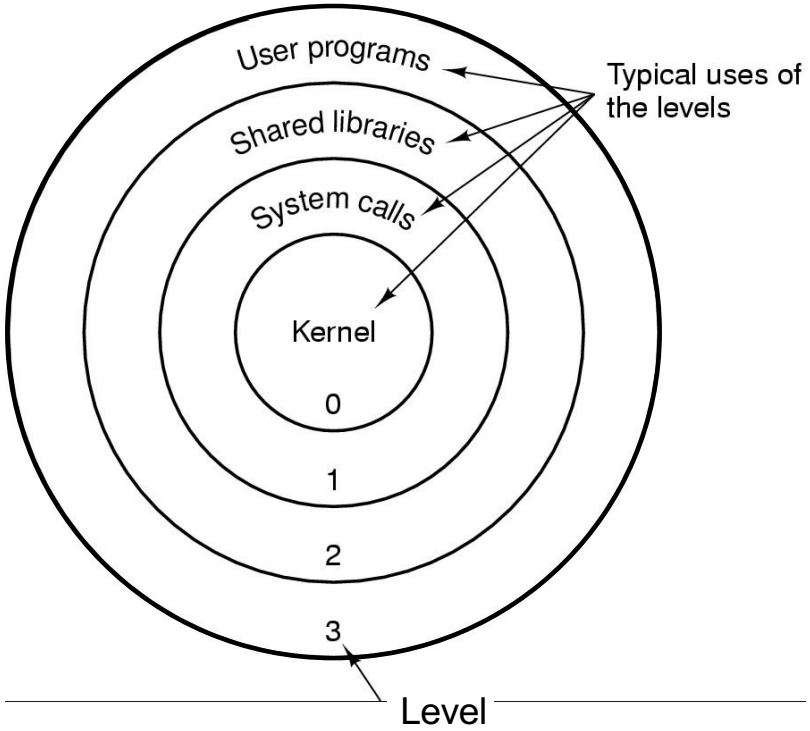
Rechte - Hardware

- CPU
  - SuperVisor Modus (Alle Register lese- und schreibbar)
  - User Mode
- Speicher
  - Memory Management Unit
- BIOS / Firmware

Wechsel in Supervisor-Modus der CPU

- Aus dem User-Modus kann durch einen Interrupt in den Supervisor-Modus gewechselt werden
- Zwei Arten von Interrupts:
  - HW-Interrupt (z.B. Tastendruck, Timer-Interrupt, Festplattencontroller)
  - SW-Interrupt (z.B. Trap bei „Division by Zero“)
- Vorgesehene Weg um Dienst des Betriebssystemkernels zu erhalten:
  - Ausführung einer System-Call Instruktion, diese löst SW-Interrupt aus, der in ISR des Kernels landet
  - Betriebssystem prüft ob aufrufender Prozess entsprechende Rechte hat

Protection on the Pentium



Rechte - Betriebssystem

- Kernelmode – Alles möglich
- User mode – Rechte eingeschränkt

Rechte - Systemprogramme

- Ausführung im Auftrag eines Users
- Nur so viel Rechte, wie erforderlich
- Nur für die erforderliche Dauer

Rechte - Anwendungsprogramme

- Haben Rechte des Benutzers
- Können eigene Rechte verwalten, z.B. :
  - ftp-Server
  - Datenbank System
  - Wiki
  - Internet Foren

Problem

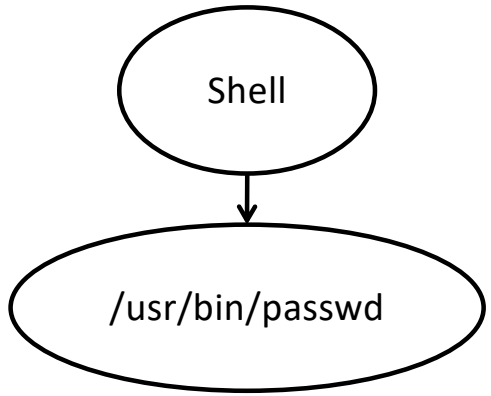
- Wie kann ein Benutzer sein Passwort ändern, wenn er dazu root-Rechte benötigt?

Bsp.: UNIX – Passwort ändern

- /etc/passwd:
  - `rw-r--r--`
- Kommando /usr/bin/passwd
  - `rwsr-xr-x`

Set User ID Bit:

chmod u+s file



Reale UID = 1047
Effektive UID = 1047

Reale UID = 1047
Effektive UID = 0

Kommandos zum ändern von /etc/passwd

- passwd
- chsh
- chfn

- usermod

Bsp. UNIX: /etc/groups

- Zuordnung User zu *secondary Groups*
  - Welchen Gruppen gehört der User neben der primären Gruppe noch an

- Bei login ist die reale GID die der primären Gruppe
- Wechsel in sekundäre Gruppe xyz mit Kommando:
  - `newgrp xyz`
  - ➔ reale GID ist die der Gruppe xyz

Kommandos zum ändern von /etc/group

- gpasswd

Ubuntu: Anlegen von Benutzern

- adduser