

Datenbanken und Datensicherheit

Prof. Dr. rer. nat. Peter Gerwinski

2. Oktober 2024

Vorab: Online-Werkzeuge

- Diese Veranstaltung findet **in Präsenz** statt.
Wir versuchen aber, auch eine Online-Teilnahme zu ermöglichen.
- **Mumble**: Seminarraum 2
Fragen: Mikrofon einschalten oder über den Chat
Umfragen: über den Chat – **auch während der Präsenz-Veranstaltung**
- **VNC**: Kanal 6, Passwort: `testcvh`
Eigenen Bildschirm freigeben: VNC-Software oder Web-Interface *yesVNC*
Eigenes Kamerabild übertragen: Web-Interface *CVH-Camera*
- Allgemeine Informationen: <https://www.cvh-server.de/online-werkzeuge/>
- Notfall-Schnellzugang: <https://www.cvh-server.de/virtuelle-raeume/>
Seminarraum 2, VNC-Passwort: `testcvh`
- **Lehrmaterialien**: <https://gitlab.cvh-server.de/pgerwinski/dbs>

Was sind Datenbanken?

Datenbank = Datenbestand + System, um darauf zuzugreifen

Anforderungen an Datenbank [\[Wikipedia\]](#):

- effizient
- widerspruchsfrei
- dauerhaft

Was sind Datenbanken?

Datenbank = Datenbestand + System, um darauf zuzugreifen

Anforderungen an Datenbank [\[Wikipedia\]](#):

- effizient → Sortierung, Zugriffsalgorithmen
- widerspruchsfrei
- dauerhaft

Was sind Datenbanken?

Datenbank = Datenbestand + System, um darauf zuzugreifen

Anforderungen an Datenbank [\[Wikipedia\]](#):

- effizient → Sortierung, Zugriffsalgorithmen
- widerspruchsfrei → automatische Konsistenzprüfungen
- dauerhaft

Was sind Datenbanken?

Datenbank = Datenbestand + System, um darauf zuzugreifen

Anforderungen an Datenbank [\[Wikipedia\]](#):

- effizient → Sortierung, Zugriffsalgorithmen
- widerspruchsfrei → automatische Konsistenzprüfungen
- dauerhaft → Backup, Ausfallsicherheit

Was sind Datenbanken?

Datenbank ohne Computer



Bildquelle: https://commons.wikimedia.org/wiki/File:A_Day_in_the_Life_of_a_Wartime_Housewife-_Everyday_Life_in_London,_England,_1941_D2379.jpg

Was sind Datenbanken?

Datenbank ohne Computer

- menschliche Anwesenheit erforderlich



Bildquelle: https://commons.wikimedia.org/wiki/File:A_Day_in_the_Life_of_a_Wartime_Housewife-_Everyday_Life_in_London,_England,_1941_D2379.jpg

Was sind Datenbanken?

Datenbank ohne Computer

- menschliche Anwesenheit erforderlich
- sorgfältig geordnet für effizienten Zugriff
→ sorgfältiger Umgang erforderlich,
um Ordnung zu erhalten



Bildquelle: https://commons.wikimedia.org/wiki/File:A_Day_in_the_Life_of_a_Wartime_Housewife-_Everyday_Life_in_London,_England,_1941_D2379.jpg

Was sind Datenbanken?

Datenbank ohne Computer

- menschliche Anwesenheit erforderlich
- sorgfältig geordnet für effizienten Zugriff
→ sorgfältiger Umgang erforderlich, um Ordnung zu erhalten
- Jeweils 1 Person kann an 1 Papier arbeiten.
→ Hardware-Unterstützung für Konsistenz



Bildquelle: https://commons.wikimedia.org/wiki/File:A_Day_in_the_Life_of_a_Wartime_Housewife-_Everyday_Life_in_London,_England,_1941_D2379.jpg

Was sind Datenbanken?

Datenbank ohne Computer

- menschliche Anwesenheit erforderlich
- sorgfältig geordnet für effizienten Zugriff
→ sorgfältiger Umgang erforderlich, um Ordnung zu erhalten
- Jeweils 1 Person kann an 1 Papier arbeiten.
→ Hardware-Unterstützung für Konsistenz
- Kopien sehr aufwendig
→ sorgfältige Archivierung erforderlich



Bildquelle: https://commons.wikimedia.org/wiki/File:A_Day_in_the_Life_of_a_Wartime_Housewife-_Everyday_Life_in_London,_England,_1941_D2379.jpg

Was sind Datenbanken?

Zentraler Computer



Bildquelle: [https://commons.wikimedia.org/wiki/File:Ken_Thompson_\(sitting\)_and_Dennis_Ritchie_at_PDP-11_\(2876612463\).jpg](https://commons.wikimedia.org/wiki/File:Ken_Thompson_(sitting)_and_Dennis_Ritchie_at_PDP-11_(2876612463).jpg)

Was sind Datenbanken?

Zentraler Computer

- menschliche Anwesenheit erforderlich



Bildquelle: [https://commons.wikimedia.org/wiki/File:Ken_Thompson_\(sitting\)_and_Dennis_Ritchie_at_PDP-11_\(2876612463\).jpg](https://commons.wikimedia.org/wiki/File:Ken_Thompson_(sitting)_and_Dennis_Ritchie_at_PDP-11_(2876612463).jpg)

Was sind Datenbanken?

Zentraler Computer

- menschliche Anwesenheit erforderlich
- sorgfältig geordnet für effizienten Zugriff
 - Computer kann helfen, Ordnung zu erhalten

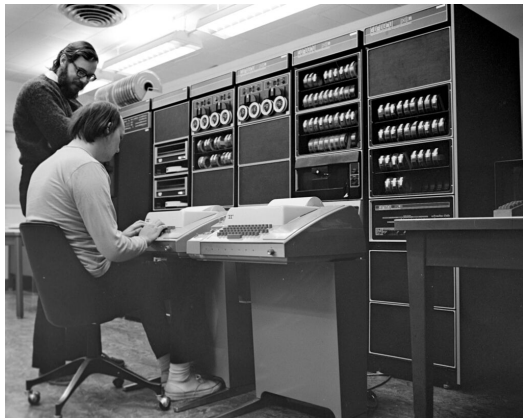


Bildquelle: [https://commons.wikimedia.org/wiki/File:Ken_Thompson_\(sitting\)_and_Dennis_Ritchie_at_PDP-11_\(2876612463\).jpg](https://commons.wikimedia.org/wiki/File:Ken_Thompson_(sitting)_and_Dennis_Ritchie_at_PDP-11_(2876612463).jpg)

Was sind Datenbanken?

Zentraler Computer

- menschliche Anwesenheit erforderlich
- sorgfältig geordnet für effizienten Zugriff
 - Computer kann helfen, Ordnung zu erhalten
- Jeweils 1 Person kann am Computer arbeiten.
 - Hardware-Unterstützung für Konsistenz

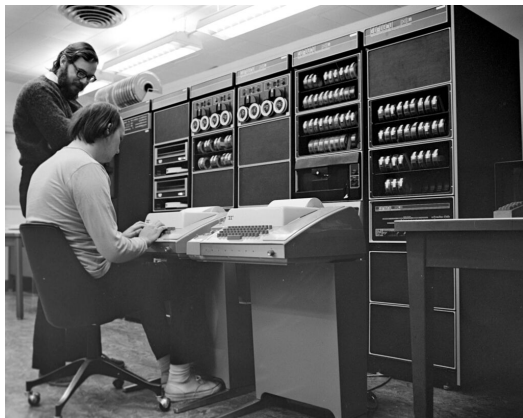


Bildquelle: [https://commons.wikimedia.org/wiki/File:Ken_Thompson_\(sitting\)_and_Dennis_Ritchie_at_PDP-11_\(2876612463\).jpg](https://commons.wikimedia.org/wiki/File:Ken_Thompson_(sitting)_and_Dennis_Ritchie_at_PDP-11_(2876612463).jpg)

Was sind Datenbanken?

Zentraler Computer

- menschliche Anwesenheit erforderlich
- sorgfältig geordnet für effizienten Zugriff
 - Computer kann helfen, Ordnung zu erhalten
- Jeweils 1 Person kann am Computer arbeiten.
 - Hardware-Unterstützung für Konsistenz
- Backups möglich



Bildquelle: [https://commons.wikimedia.org/wiki/File:Ken_Thompson_\(sitting\)_and_Dennis_Ritchie_at_PDP-11_\(2876612463\).jpg](https://commons.wikimedia.org/wiki/File:Ken_Thompson_(sitting)_and_Dennis_Ritchie_at_PDP-11_(2876612463).jpg)

Was sind Datenbanken?

Zentraler Computer,
Zugriff von Arbeitsplätzen aus



Bildquelle: https://commons.wikimedia.org/wiki/File:Computergebouw_van_KLM_voor_automatische_boekingsmethode_Corda_in_Amstelveen._,_Bestanddeelnr_923-3365.jpg

Was sind Datenbanken?

Zentraler Computer,
Zugriff von Arbeitsplätzen aus

- Arbeiten auf
Entfernung möglich



Bildquelle: https://commons.wikimedia.org/wiki/File:Computergebouw_van_KLM_voor_automatische_boekingsmethode_Corda_in_Amstelveen._,_Bestanddeelnr_923-3365.jpg

Was sind Datenbanken?

Zentraler Computer, Zugriff von Arbeitsplätzen aus

- Arbeiten auf Entfernung möglich
- sorgfältig geordnet für effizienten Zugriff
→ Computer kann helfen, Ordnung zu erhalten



Bildquelle: https://commons.wikimedia.org/wiki/File:Computergebouw_van_KLM_voor_automatische_boekingsmethode_Corda_in_Amstelveen._,_Bestanddeelnr_923-3365.jpg

Was sind Datenbanken?

Zentraler Computer, Zugriff von Arbeitsplätzen aus

- Arbeiten auf Entfernung möglich
- sorgfältig geordnet für effizienten Zugriff
→ Computer kann helfen, Ordnung zu erhalten
- Mehrere Personen können unbemerkt gleichzeitig an denselben Daten arbeiten.
→ Computer muß helfen, Konsistenz zu erhalten



Was sind Datenbanken?

Zentraler Computer, Zugriff von Arbeitsplätzen aus

- Arbeiten auf Entfernung möglich
- sorgfältig geordnet für effizienten Zugriff
→ Computer kann helfen, Ordnung zu erhalten
- Mehrere Personen können unbemerkt gleichzeitig an denselben Daten arbeiten.
→ Computer muß helfen, Konsistenz zu erhalten
- Backups möglich



Was sind Datenbanken?

Zentraler Computer,
öffentlicher Zugriff



Bildquelle: https://commons.wikimedia.org/wiki/File:Shopping_online_with_bank_card.jpg

Was sind Datenbanken?

Zentraler Computer, öffentlicher Zugriff

- Selbstbedienung auf Entfernung möglich



Bildquelle: https://commons.wikimedia.org/wiki/File:Shopping_online_with_bank_card.jpg

Was sind Datenbanken?

Zentraler Computer, öffentlicher Zugriff

- Selbstbedienung auf Entfernung möglich
- sorgfältig geordnet für effizienten Zugriff
→ Computer muß selbständig Ordnung erhalten



Was sind Datenbanken?

Zentraler Computer, öffentlicher Zugriff

- Selbstbedienung auf Entfernung möglich
- sorgfältig geordnet für effizienten Zugriff
→ Computer muß selbständig Ordnung erhalten
- Mehrere Personen können unbemerkt gleichzeitig an denselben Daten arbeiten.
→ Computer muß selbständig Konsistenz erhalten



Was sind Datenbanken?

Zentraler Computer, öffentlicher Zugriff

- Selbstbedienung auf Entfernung möglich
- sorgfältig geordnet für effizienten Zugriff
→ Computer muß selbständig Ordnung erhalten
- Mehrere Personen können unbemerkt gleichzeitig an denselben Daten arbeiten.
→ Computer muß selbständig Konsistenz erhalten
- Backups möglich



Bildquelle: https://commons.wikimedia.org/wiki/File:Shopping_online_with_bank_card.jpg

Was sind Datenbanken?

Zentraler Computer, öffentlicher Zugriff

- Selbstbedienung auf Entfernung möglich
- sorgfältig geordnet für effizienten Zugriff
→ Computer muß selbständig Ordnung erhalten
- Mehrere Personen können unbemerkt gleichzeitig an denselben Daten arbeiten.
→ Computer muß selbständig Konsistenz erhalten
- Backups möglich
- Bessere Zugriffsmöglichkeiten → Datensicherheit wird Herausforderung



Bildquelle: https://commons.wikimedia.org/wiki/File:Shopping_online_with_bank_card.jpg

Was ist Datensicherheit?

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Was ist Datensicherheit?

- Vertraulichkeit (CIA)
- Integrität (confidentiality)
- Verfügbarkeit (integrity)
- Verfügbarkeit (availability)

Was ist Datensicherheit?

- | | | |
|-------------------|-------------------|-------------------|
| | (CIA) | |
| • Vertraulichkeit | (confidentiality) | → Verschlüsselung |
| • Integrität | (integrity) | |
| • Verfügbarkeit | (availability) | |

Was ist Datensicherheit?

- | | | |
|-------------------|-------------------|-----------------------|
| | (CIA) | |
| • Vertraulichkeit | (confidentiality) | → Verschlüsselung |
| • Integrität | (integrity) | → Konsistenzprüfungen |
| • Verfügbarkeit | (availability) | |

Was ist Datensicherheit?

- | | | |
|-------------------|-------------------|------------------------------|
| | (CIA) | |
| • Vertraulichkeit | (confidentiality) | → Verschlüsselung |
| • Integrität | (integrity) | → Konsistenzprüfungen |
| • Verfügbarkeit | (availability) | → Backups, Ausfallsicherheit |

Was ist Datensicherheit?

(CIA)

- Vertraulichkeit (confidentiality) → Verschlüsselung
- Integrität (integrity) → Konsistenzprüfungen
- Verfügbarkeit (availability) → Backups, Ausfallsicherheit
- Identifizierbarkeit
(Authentizität, Nichtabstreitbarkeit, Zurechenbarkeit)
→ Passwörter, Signaturen

Was ist Datensicherheit?

(CIA)

- Vertraulichkeit (confidentiality) → Verschlüsselung
- Integrität (integrity) → Konsistenzprüfungen
- Verfügbarkeit (availability) → Backups, Ausfallsicherheit

- Identifizierbarkeit
(Authentizität, Nichtabstreitbarkeit, Zurechenbarkeit)
→ Passwörter, Signaturen

bzw.

- Anonymität
(plausible Abstreitbarkeit, Nichtzurechenbarkeit)
→ Pseudonymisierung, Anonymisierung

In dieser Lehrveranstaltung

- Kurzeinführung: Unix-Shell
- Kurzeinführung: TCP/IP
- relationale Datenbank-Management-Systeme (DBMS)
- SQL-Programmierung
- sonstige Datenbank-Management-Systeme

- Kurzeinführung: Kryptographie
- Kryptographie in der Praxis:
Passwörter, Verschlüsselung, Signaturen,
Schlüssel-Infrastrukturen
- Netzwerksicherheit
- Sicherheit von Web-Anwendungen
- Datenschutz

In dieser Lehrveranstaltung

- Kurzeinführung: Unix-Shell
- Kurzeinführung: TCP/IP
- relationale Datenbank-Management-Systeme (DBMS)
- SQL-Programmierung
- sonstige Datenbank-Management-Systeme

- Kurzeinführung: Kryptographie
- Kryptographie in der Praxis:
Passwörter, Verschlüsselung, Signaturen,
Schlüssel-Infrastrukturen
- Netzwerksicherheit
- Sicherheit von Web-Anwendungen
- Datenschutz



Änderungen
vorbehalten

In dieser Lehrveranstaltung

3 Praktikumsversuche

1. Selbstbau eines einfachen DBMS
2. Selbstbau einer prototypischen, sicheren Datenbankanwendung
3. E-Mail-Verschlüsselung

Prüfungsleistung: Klausur



Änderungen
vorbehalten

In dieser Lehrveranstaltung

3 Praktikumsversuche

0. Praxiserfahrung mit Unix und TCP/IP
1. Selbstbau eines einfachen DBMS
2. Selbstbau einer prototypischen, sicheren Datenbankanwendung
3. E-Mail-Verschlüsselung

Keine festen Abgabetermine, sondern:
Angebot zum betreuten Arbeiten im DV-Pool,
Vorzeigen (Testieren) der Ergebnisse

Prüfungsleistung: Klausur



Änderungen
vorbehalten

Datenbanken und Datensicherheit

<https://gitlab.cvh-server.de/pgerwinski/dbs>

1 Einführung

- 1.1 Was sind Datenbanken?
- 1.2 Was ist Datensicherheit?
- 1.3 In dieser Lehrveranstaltung

2 Kurzeinführung Unix

- 2.1 Grundkonzepte
- 2.2 Die Kommandozeile: Grundlagen
- 2.3 Dateisysteme
- 2.4 Ein- und Ausgabeströme
- 2.5 Pipes
- 2.6 Verzweigungen und Schleifen

3 Kurzeinführung TCP/IP

...



Änderungen
vorbehalten

2 Kurzeinführung Unix

2.1 Grundkonzepte

- 1965** Vorgänger: Multics (Multiplexed Information and Computing Service)
„überladen“
- 1970** Unix: Einfachheit als Grundkonzept
- 1972** Umstellung auf neu entwickelte Programmiersprache C
- 1975** AT&T: Unix inkl. Quelltext für Universitäten
- 1977** Berkeley Software Distribution (BSD)
- 1983** GNU-Projekt
- 1987** Minix
- 1991** Linux
- 1993** FreeBSD, NetBSD
- 1994** OpenBSD
- 2000** Darwin (Mac OS X, BSD-basiert)
- 2008** Android (Linux-basiert)

2 Kurzeinführung Unix

2.1 Grundkonzepte

Unix und C: Einfachheit als Grundkonzept

- Vermeiden von Ausnahmen
- Baukastensystem

C: Hauptprogramm
= „normale“ Funktion

```
int main (int argc, char **argv)
{
    printf ("Hello, _world!\n");
    return 0;
}
```

Unix: übergeordnetes Verzeichnis = „normales“ Verzeichnis

```
cassini/home/peter/foo> ls -la
insgesamt 24
drwxr-xr-x  2 peter peter  4096 Okt  6 13:30 .
drwxr-xr-x 172 peter peter 20480 Okt  6 13:30 ..
cassini/home/peter/foo> cd ..
cassini/home/peter>
```

2 Kurzeinführung Unix

2.1 Grundkonzepte

Unix und C: Einfachheit als Grundkonzept

- Vermeiden von Ausnahmen
- Baukastensystem

C: Bibliotheken

z. B.: `printf()` = „normale“ Funktion
aus eine Bibliothek (`libc`)

Unix: Programme arbeiten zusammen

```
cassini/home/peter/bo> find . -name "*klausur*.tex" \  
| xargs grep -l "PBM-Datei"  
./2014ws/ainf/20150130.0/ainf-klausur-20150130.tex  
./2016ws/hp/20170920.0/klausur.tex  
./2016ws/hp/20170206.0/klausur.tex  
./2011ws/rarch/20120322.0/rarch-klausur-20120322.tex  
./2012ws/klausuren-gerwinski/rarch-klausur-20120322.tex  
./2013ws/ainf/20140918.0/ainf-klausur-20140918.tex  
./2017ws/hp/20180213.k1/klausur.tex  
./2017ws/hp/20180205/klausur.tex  
./2015ws/ainf/20160913/ainf-klausur-20160913.tex
```

2.2 Die Kommandozeile: Grundlagen

- Programm aufrufen: Namen eingeben, z. B.: `ls`
- Optionen: `ls -l`
- Lange Optionen (GNU-Konvention): `ls --help`
- Text schreiben: `echo "Hello, world!"`
- (String-)Variable setzen: `FOO=bar`
- Variable einlesen: `read FOO`
- Variable abrufen: `echo $FOO`
- Aus Sicherheitsgründen: `echo "$FOO"`

```
cassini/home/peter/bo> FOO=ls
cassini/home/peter/bo> echo "$FOO"
ls
cassini/home/peter/bo> $FOO
2011ws  2012ws  2013ws  doc          misc  projekte
2012ss  2013ss  briefe  material    orga
cassini/home/peter/bo>
```

2.2 Die Kommandozeile: Grundlagen

- Befehl zurückholen: Pfeiltasten \uparrow , \downarrow
- Befehl bearbeiten: Pfeiltasten \leftarrow , \rightarrow usw.
- Befehl vervollständigen: TAB
- Befehl rückwärts suchen: Ctrl+R
- Bildschirm löschen: Ctrl+L
- Befehl abbrechen: Ctrl+C

- Hilfe-Option: `ls --help`
- Unix-Handbuch – *manual*: `man ls`
(Beenden mit `q`)