Script **generated by TTT**

Title: Einf_HF (07.07.2014)

Date: Mon Jul 07 14:14:54 CEST 2014

Duration: 94:57 min

Pages: 52

Grundlagen von Rechnernetzen

- Fragestellungen des Abschnitts:
  - Welche Übertragungsmedien gibt es?
  - Was ist das Internet? Wie ist es aufgebaut?
  - Wie werden Rechner im Internet addressiert?
  - Wie sieht das Kommunikationsreferenzmodell für das Internet aus?

WAN - Wide Area Network

Über Weitverkehrsnetze (WAN) werden die lokalen Netze miteinander verbunden.

ein lokales Netz wird von einer Organisation verwaltet.

WANs werden i.a. nicht von einer einzelnen Organisation verwaltet.

Internet

Internet ist ein Verbund von Rechnernetzen auf der Basis der TCP/IP-Technologie.

Netzstruktur des Internet

Zugangsstruktur des Internet

Propagierung von Nachrichten im Internet

Backbone des Deutschen Wissenschaftsnetzes (DFN)

Monitoring Werkzeuge

Vielzahl von Werkzeugen zum Netz Monitoring

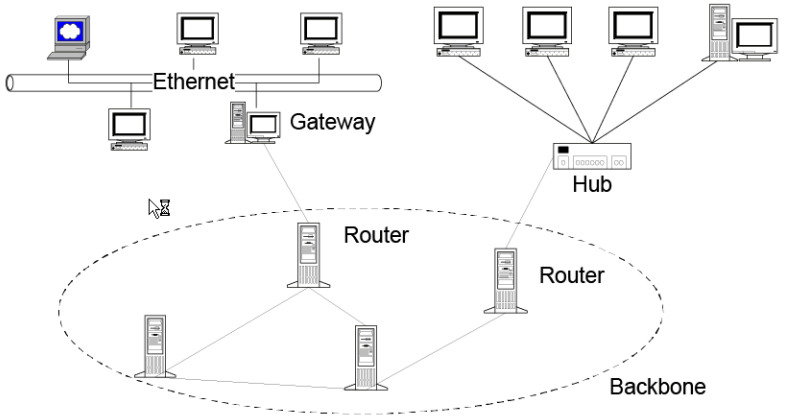
Domaintools: Informationen über Domains .

Verfolgung von Nachrichtenwegen mit traceroute.

Erreichbarkeit von Rechnern mit ping.

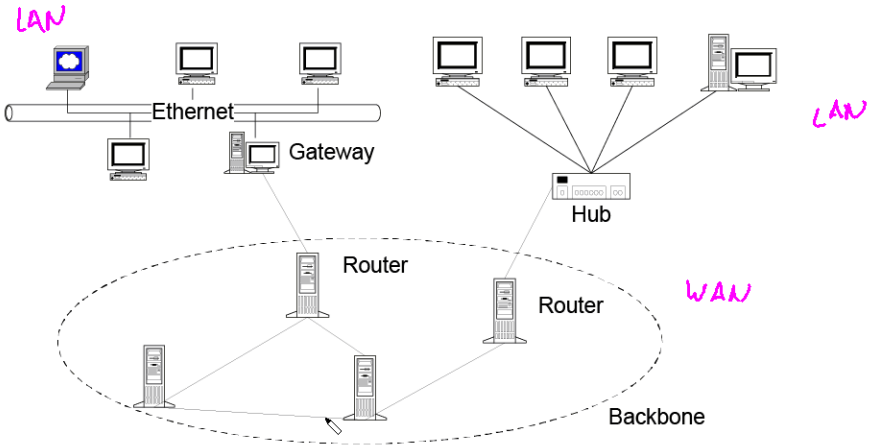
für Werkzeuge siehe auch unter Network-Tools .

Netzstruktur des Internet



Backbones sind Hochgeschwindigkeitsnetze zur Verbindung von Teilnetzen; sie sind meist redundant ausgelegt, um Ausfälle zu tolerieren.

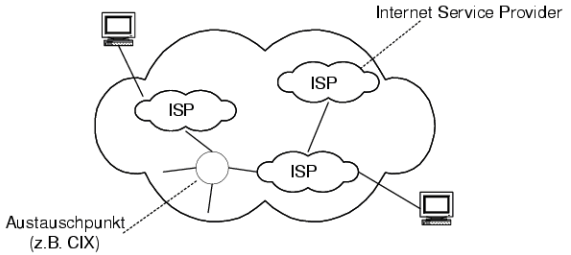
Netzstruktur des Internet



Backbones sind Hochgeschwindigkeitsnetze zur Verbindung von Teilnetzen; sie sind meist redundant ausgelegt, um Ausfälle zu tolerieren.

Generated by Targeteam

Zugangsstruktur des Internet



Neben der Internetkonnektivität kann ein ISP noch weitere Dienste bereitstellen, u.a.:

- Speicherplatz für persönliche Web-Seiten (Web-Hosting).
- ein oder mehrere Email Accounts.
- Betrieb von speziellen Anwendungsservern für den Nutzer (u.Umständen mit Wartung und Datensicherung).

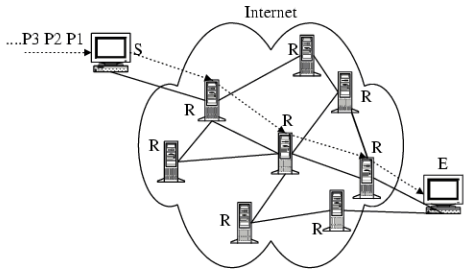
Generated by Targeteam

Propagierung von Nachrichten im Internet

Zerlegung der gesamten Nachricht in einzelne Pakete, die dann einzeln vom Sender S zum Empfänger E übertragen werden. Auf dem Weg S bis zu E werden die Pakete über mehrere Übertragungsrechner (Router) übertragen.

Pakete können unterschiedliche Wege durch das Internet nehmen, und auch unterschiedlich lange unterwegs sein, d.h. Pakete können in unterschiedlicher Reihenfolge ankommen als sie abgeschickt wurden. Der Empfangsrechner muss die empfangenen Pakete in der korrekten Reihenfolge zusammensetzen, d.h. jedes Paket braucht eine Sequenznummer.

In regelmäßigen Abständen werden Informationen über die angeschlossenen Übertragungsstrecken ausgetauscht, d.h. ist Leitung gestört, ist Leitung überlastet etc. Jeder Router hat eine Tabelle aufgrund der er entscheidet, welchen weiteren Weg ein Paket zum Empfänger nehmen soll.

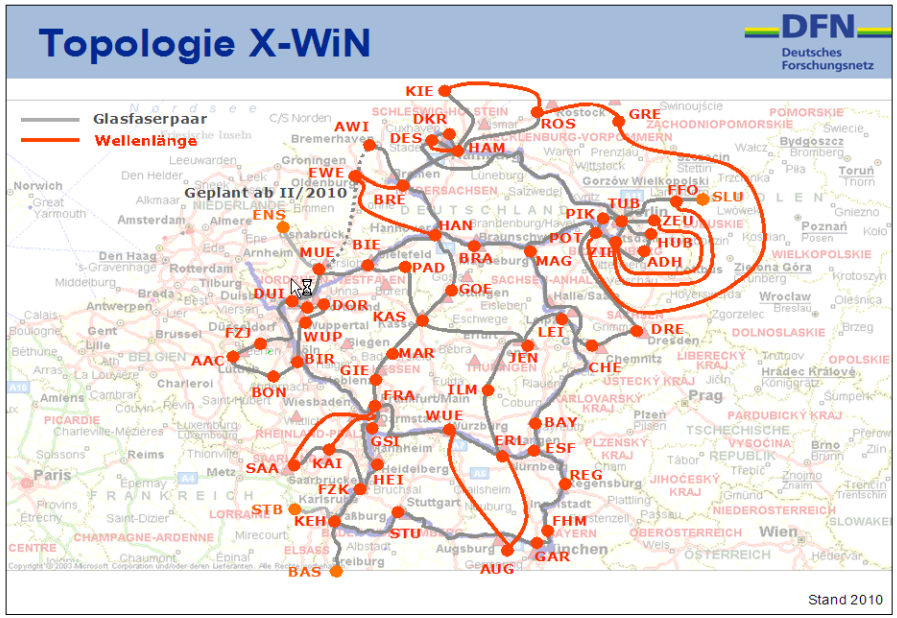


Animation Routing

Generated by Targeteam

Backbone des Deutschen Wissenschaftsnetzes (DFN)

Deutsches Forschungsnetz (DFN); siehe auch das Münchner Wissenschaftsnetz (MWN)



WAN - Wide Area Network

Über Weitverkehrsnetze (WAN) werden die lokalen Netze miteinander verbunden.

ein lokales Netz wird von einer Organisation verwaltet.

WANs werden i.a. nicht von einer einzelnen Organisation verwaltet.

Internet

Internet ist ein Verbund von Rechnernetzen auf der Basis der TCP/IP-Technologie.

Netzstruktur des Internet

Zugangsstruktur des Internet

Propagierung von Nachrichten im Internet

Backbone des Deutschen Wissenschaftsnetzes (DFN)

Monitoring Werkzeuge

Vielzahl von Werkzeugen zum Netz Monitoring

Domaintools: Informationen über Domains .

Verfolgung von Nachrichtenwegen mit traceroute.

Erreichbarkeit von Rechnern mit ping.

für Werkzeuge siehe auch unter Network-Tools .

Grundlagen von Rechnernetzen

- Fragestellungen des Abschnitts:
  - Welche Übertragungsmedien gibt es?
  - Was ist das Internet? Wie ist es aufgebaut?
  - Wie werden Rechner im Internet addressiert?
  - Wie sieht das Kommunikationsreferenzmodell für das Internet aus?

TCP/IP Referenzmodell

Das TCP/IP-Referenzmodell ist auf die Internet-Protokolle zugeschnitten. Es ist der de-facto Standard;

Zur Kommunikation zwischen Rechnern über ein Rechnernetz sind Protokolle notwendig. Ein ***Protokoll*** besteht aus einer Menge von Datenstrukturen (Nachrichtenaufbau) und Konventionen, wie der Ablauf der Kommunikation stattfindet und wie die Informationen jeweils zu interpretieren sind, z.B. Syntax der Nachrichten, Folge und Bedeutung von Nachrichten.

Zur Reduzierung der Komplexität beim Entwurf eines offenen Rechnernetzes wird das Netz in aufeinander aufbauende Protokoll-Schichten unterteilt.

Prinzipien für Schichtung

Zur Gliederung der Kommunikationsaufgaben werden in Netzwerken funktionale Ebenen, so genannte Schichten (layer), unterschieden.

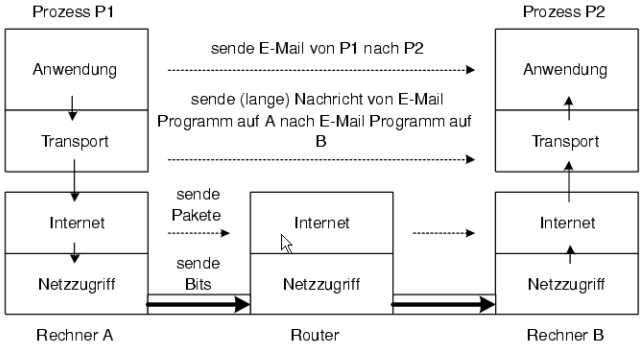
jede Schicht repräsentiert eine Abstraktionsebene

jede Schicht führt eine wohldefinierte Funktion aus

schmale Schnittstellen zwischen Schichten, um Informationsfluss zu minimieren

Funktion einer Schicht ist aufgrund von international spezifizierten Standardprotokollen definiert

Aufbau des Internet-Schichtenmodells



Gepunktete Pfeile repräsentieren logische Übertragungen.

Bedeutung der Schichten

Netzzugriff : bietet eine Übertragungsmöglichkeit einzelner Dateneinheiten (Bits) unter bestimmten Zeitbedingungen an; Nachrichtenübertragung zwischen zwei benachbarten Rechnern.

Aufgaben: Übertragung von Bitsequenzen, Berücksichtigung der Eigenschaften der Übertragungsmodi (elektrisch, Lichtwelle), Fehlererkennung und Fehlerkorrektur

Internet : fehlerfreie Übermittlung eines Pakets von einem Endrechner, über ein Netz von Routern (Vermittlungsrechnern) hinweg, bis hin zum zweiten Endrechner;

Aufgaben: Zusammenschaltung von Teilstrecken zu einer End-zu-End Verbindung, Wegewahl und Adressierung, fügt Netzwerk-Header hinzu.

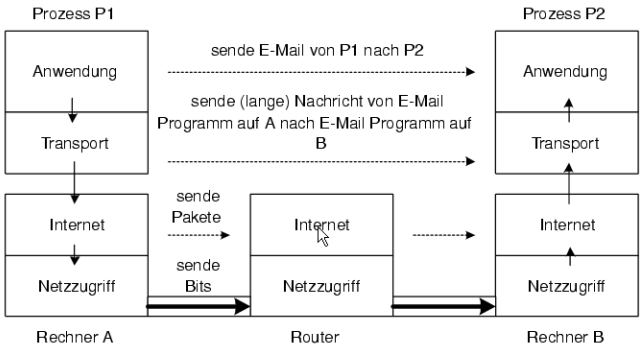
Transport : fehlerfreier Transport von Nachrichten zwischen zwei kommunizierenden Prozessen auf zwei Endrechnern;

Aufgaben: netzunabhängiger Transport von Nachrichten zwischen zwei Endsystemen; passt die vom Anwendungssystem geforderte Übertragungsqualität an die vom darunterliegenden Transportnetz angebotene Übertragungsqualität an; fügt Transport-Header hinzu.

Beispiele: Transmission Control Protocol (TCP: Internet), User Datagram Protocol (UDP: Internet).

Anwendung : es sind verschiedene Applikationsdienst-Elemente festgelegt; deren Auswahl hängt von den ablaufenden Anwendungen ab, z.B. Dateizugriff (FTP), Fernverarbeitung (Telnet), Elektronische Post (SMTP), Name Service, WWW (HTTP).

Aufbau des Internet-Schichtenmodells



Gepunktete Pfeile repräsentieren logische Übertragungen.

Generated by Targeteam

IP-Adresskonzept

Teil des TCP/IP-Referenzmodells ist die Festlegung der Adressierung von Rechnern im Netz. Dazu erhält jedes Computersystem eine eindeutige "Rufnummer", seine IP-Adresse. Eine IP-Adresse besteht aus vier Byte. Diese werden üblicherweise dezimal durch Punkte getrennt geschrieben, z.B. 131.159.24.30

Die weltweit eindeutige Vergabe von IP-Adressen übernehmen die NICs (Network Information Center). In Deutschland ist das beispielsweise das **DENIC** .

Adressklassen

Neben den IP-Adressen können Computersysteme noch einen oder mehrere einfach zu merkende Namen bekommen, wie z.B. www.in.tum.de. Die möglichen letzten Silben (top level domain) sind global festgelegt, die zweitletzte Silbe wird von jeweils zuständigen Stellen vergeben (für die .de-Domäne beispielsweise DE-NIC)

Durch den Boom des Internet werden die Adressen bereits knapp; deshalb Erweiterung der IP-Adressen auf 128 Bit (IPv6 Adresskonzept).

Eine Netzverbindung zwischen 2 entfernten Prozessen wird charakterisiert durch:

verwendetes Protokoll, z.B. TCP.

Adresse des lokalen Prozesses, d.h. IP-Adresse und Portnummer des lokalen Rechners.

Adresse des entfernten Prozesses, d.h. IP-Adresse und Portnummer des entfernten Rechners.

Adressklassen

IP-Adressen werden in Blöcke zusammengefasst um die Netzverwaltung zu erleichtern. Die Adresse besteht dazu aus Netz-ID und Host-ID. Nur die Netz-IDs werden zentral vom Network Information Center vergeben. Die Klasse gibt an, wie groß der Byte-Anteil der Netz-ID ist.

	bit 0 … 8 … 16 … 24 … 31	Subnetze	Hosts/pro Netz
A	0 | Netz-ID (7) | Host-ID	126	16.777.214
B	10 | Netz-ID (14) | Host-ID	16.382	65.534
C	110 | Netz-ID (21) | Host	64.547	254
D	1110 | Multicast-Adressen		
E	11110 | reserviert		

Klasse A: Adressbereich 1.0.0.0 - 127.255.255.255

Klasse B: Adressbereich 128.0.0.0 - 191.255.255.255

Klasse C: Adressbereich 192.0.0.0 - 223.255.255.255

Klasse D: Adressbereich 224.0.0.0 - 239.255.255.255 (verwendet durch Videokonferenzsysteme)

Klasse E: Adressbereich 240.0.0.0 - 247.255.255.255

IP-Adresskonzept

Teil des TCP/IP-Referenzmodells ist die Festlegung der Adressierung von Rechnern im Netz. Dazu erhält jedes Computersystem eine eindeutige "Rufnummer", seine IP-Adresse. Eine IP-Adresse besteht aus vier Byte. Diese werden üblicherweise dezimal durch Punkte getrennt geschrieben, z.B. 131.159.24.30

Die weltweit eindeutige Vergabe von IP-Adressen übernehmen die NICs (Network Information Center). In Deutschland ist das beispielsweise das DENIC .

Adressklassen

Neben den IP-Adressen können Computersysteme noch einen oder mehrere einfach zu merkende Namen bekommen, wie z.B. www.in.tum.de. Die möglichen letzten Silben (top level domain) sind global festgelegt, die zweitletzte Silbe wird von jeweils zuständigen Stellen vergeben (für die .de-Domäne beispielsweise DE-NIC)

Durch den Boom des Internet werden die Adressen bereits knapp; deshalb Erweiterung der IP-Adressen auf 128 Bit (IPv6 Adresskonzept).

Eine Netzverbindung zwischen 2 entfernten Prozessen wird charakterisiert durch:

verwendetes Protokoll, z.B. TCP.

Adresse des lokalen Prozesses, d.h. IP-Adresse und Portnummer des lokalen Rechners.

Adresse des entfernten Prozesses, d.h. IP-Adresse und Portnummer des entfernten Rechners.

Referenzmodell

Ein Referenzmodell beschreibt den Aufbau und das Zusammenwirken der Netzwerkprotokolle. Beispiele sind

ISO/OSI Protokollfamilie

TCP/IP Protokollsuite (Referenzmodell des Internet; TCP = Transmission Control Protocol, IP = Internet Protokoll)

TCP/IP Referenzmodell

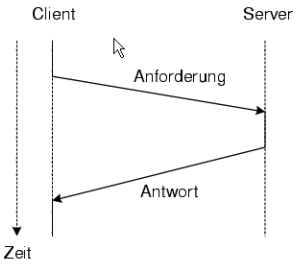
IP-Adresskonzept

Sicherung gegen Fehler

Client-Server-Modell

Möglichkeit zur Strukturierung von (verteilten) Anwendungen: ***Server*** stellen Dienste zur Verfügung, die von (den Servern) vorher unbekannten ***Clients*** in Anspruch genommen werden können.

Client und Server



Client ruft Operation eines Servers auf, erhält ggf. Ergebnis zurück. Während Operation wird Ablauf des Client meist unterbrochen.

Definition: Client

Anwendungsteil, der auf Anforderung einen Dienst von einem Server erhält.

Clients sind meist a-priori beim Server nicht bekannt.

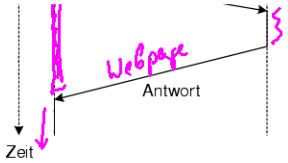
Definition: Server

Subsystem, das bestimmten Dienst für a-priori unbekannte Clients zur Verfügung stellt.

Client und Server kommunizieren über Nachrichten.

Antwort bestätigt Empfang der Anforderung durch den Server.

Client-Server-Modell



Client ruft Operation eines Servers auf, erhält ggf. Ergebnis zurück. Während Operation wird Ablauf des Client meist unterbrochen.

Definition: Client

Anwendungsteil, der auf Anforderung einen Dienst von einem Server erhält.

Clients sind meist a-priori beim Server nicht bekannt.

Definition: Server

Subsystem, das bestimmten Dienst für a-priori unbekannte Clients zur Verfügung stellt.

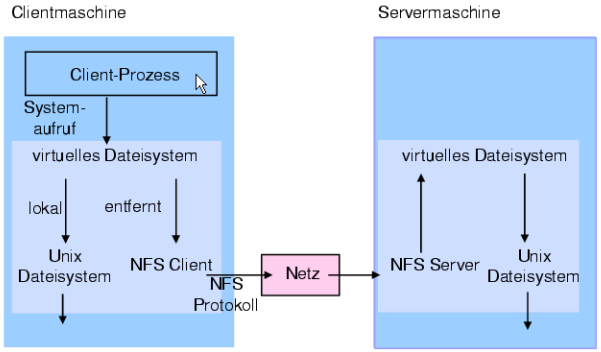
Client und Server kommunizieren über Nachrichten.

Antwort bestätigt Empfang der Anforderung durch den Server.

Server sind Prozesse, die kontinuierlich eine Schleife folgender Form abarbeiten:

```
while (true) {
   receive (empfangsport, anforderung)
   führe anforderung aus und erzeuge antwort
   send (sendeport, antwort)
}
```

Beispiel NFS (Network File System)



Beispiel-Services

Datei-Service

Entfernte, zentralisierte Datenspeicherung für Arbeitsplatzrechner.

Beispiel NFS (Network File System)

Namens-Service

Entfernte, zentralisierte Namensverwaltung für Objekte (Dateien, andere Server, Services, Drucker, Benutzer etc.).

Zeit-Service

Synchronisierte Systemzeit für Rechner.

World Wide Web

Organisiert nach Client/Server Architektur.

Zieladresse wird mit Hilfe einer URL angegeben

Beispiel: http://www11.in.tum.de:80/lehre/vorlesungen/

http:// gibt das Kommunikationsprotokoll für den Zugriff auf Web-Seiten an.

www11.in.tum.de gibt den Web-Server an.

lehre/vorlesungen/ gibt ein Verzeichnis/Dokument innerhalb des Web-Servers an.

Standardport des Web-Servers: 80.

Weitere Kommunikationsprotokolle

https:// Kommunikationsprotokoll für den gesicherten Zugriff auf Web-Seiten.

file:// Zugriff auf Dateien am lokalen Rechner.

ftp:// Zugriff auf Dateien an einem entfernten Rechner; Nutzung des Filetransfer Dienstes.

mailto: verschicken von Emails an die angegebene Adresse.

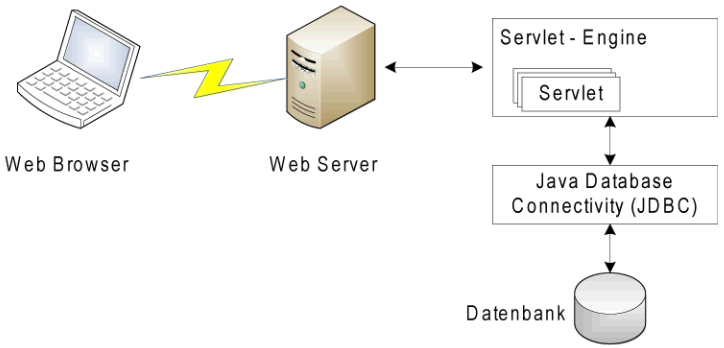
Methoden des http Protokolls

GET: anfordern einer Ressource (z.B. eine Web-Seite), die mittels einer URL spezifiziert ist.

PUT: dient dazu eine Ressource (z. B. eine Web-Seite) unter Angabe der Ziel-URL auf einen Webserver hochzuladen.

Anbindung einer Datenbank

Mit Hilfe von Informationen aus Datenbanken können Inhalte von Web-Seiten dynamisch gestaltet werden; dazu Abruf der DB-Information über Servlets und spezielle Schnittstellen, z.B. Java DB Connectivity (JDBC).



Sicherheit in verteilten Systemen

Ein wichtiger Aspekt eines Rechnersystems besteht darin, dass Daten nicht von Unbefugten abgefragt werden können. Bei nicht-vernetzten Systemen läßt sich dies durch eine Sicherung des physikalischen Zugangs zu den Rechnern und einfache Passwortsysteme garantieren. Bei verteilten Systemen werden zusätzliche Dienste benötigt.

Sicherheitsanforderungen

- Garantierung der Identität eines Absenders (Identitätsprüfung, Authentifizierung).
- Verhinderung von Mithören (Verschlüsselung).
- Sicherstellung der Integrität (Unverfälschtheit) von Nachrichten (Hash-Werte).
- Verhinderung des Wiedereinspielens von Nachrichten (Integritätssicherung und Zeitstempel).

Arten von Schadsoftware

Verschlüsselung

Identitätsprüfung

Arten von Schadsoftware

Schadsoftware ("Malware") sind Programme, die Aktionen ausführen, die unerwünscht und meist schädlich sind.

- Computerviren: sich selbst verbreitende Programme, die sich in anderen Programmen einschleusen.
- Computerwurm: vervielfältigt sich selbst, wenn die Software, in die es eingebettet ist, ausgeführt wird.
- Trojanisches Pferd: Software, die vortäuscht eine nützliche Anwendung zu sein, und somit dazu verführt, sie auszuführen.
- SPAM: unerwünschte Nachrichten, die dem Empfänger unverlangt zugestellt werden.
- Spyware: forscht den Rechner und das Verhalten des jeweiligen Nutzers ohne dessen Wissen aus und sendet die Daten an den Hersteller der Spyware.
- Phishing: Versuche, um an geheime Daten eines Nutzers zu gelangen.
- Adware: bei normaler Installation oder beim Herunterladen nützlicher Software wird Reklamesoftware installiert.
- Dialer: bauen heimlich im Hintergrund über das Telefonnetz eine Wählverbindung zu teueren 0190 bzw. 0900 -Nummern auf.

Verschlüsselung

Verschlüsselung bedeutet, dass man Daten für die Übertragung oder Speicherung so codiert, dass sie nur vom beabsichtigten Empfänger wieder in "Klartext" zurückcodiert werden können. Für alle eventuellen "Mithörer" bleiben die Daten eine uninterpretierbare Bitfolge.

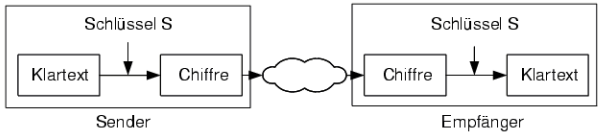
- Web-Adresse: https://..... ⇒ Daten werden verschlüsselt zwischen Web Browser und Web Server übertragen (z.B. für Online Bestellungen bei Amazon).
- Es gibt zwei grundlegende Verfahrensklassen für die Verschlüsselung von Daten: symmetrische Verschlüsselung und asymmetrische Verschlüsselung.

Symmetrische Verschlüsselung

Asymmetrische Kryptosysteme

Symmetrische Verschlüsselung

Beide Partner (Sender und Empfänger) kennen einen geheimen Schlüssel, der zum Ver- und zum Entschlüsseln verwendet wird. Eine Kenntnis des Schlüssels erlaubt Zugriff auf die Daten.



Austausch des geheimen Schlüssels über einen anderen, sicheren Kommunikationskanal (z.B. persönlich, Brief)

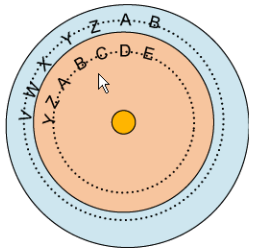
Für jede mögliche Verbindung wird ein eigener Schlüssel benötigt (Falls derselbe Schlüssel für Nachrichten an B und C benutzt wird, könnte C Nachrichten an B lesen).

Beispiele: DES, Tripple DES, IDEA

Erweiterte Caesar-Chiffre

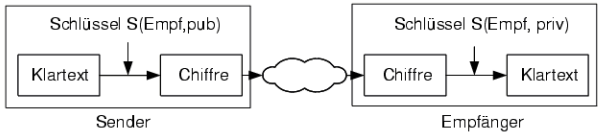
Erweiterte Caesar-Chiffre

- Verschlüsselungsanweisung: Ersetze jeden Buchstaben im Originaltext durch den Buchstaben, der n Stellen im Alphabet weiter hinten (rechts) steht.
- Entschlüsselungsanweisung: Ersetze jeden Buchstaben im verschlüsselten Text durch den Buchstaben, der n Stellen im Alphabet weiter vorne (links) steht.
- Schlüssel: n (natürliche Zahl zwischen 0 und 26)
- Beispiel
  - Originaltext: "VENI VIDI VICI", Schlüssel = 3
  - verschlüsselter Text: "YHQL YLGL YLFL"
- **Cäsar-Scheibe**



Asymmetrische Kryptosysteme

Zum Ver- und Entschlüsseln wird ein Schlüsselpaar (priv, pub) verwendet. Es existiert ein personenbezogener ***privater Schlüssel*** priv und ein ***öffentlicher Schlüssel*** pub, der allgemein zugänglich und jedem bekannt sein darf. Alle Nachrichten, die mit einem Schlüssel codiert (chiffriert) worden sind, können mit dem jeweils anderen Schlüssel wieder decodiert (dechiffriert) werden.



Für sicheren Datenaustausch wird die Nachricht mit dem öffentlichen Schlüssel des Empfängers S(Empf, pub) verschlüsselt. Dann hat nur der Empfänger selbst mit seinem privaten Schlüssel S(Empf, priv) Zugang zum Inhalt.

Geheimer Schlüssel darf nicht aus dem öffentlichen Schlüssel ableitbar sein.

Je länger der Schlüssel desto sicherer ist das System (Angriffsmöglichkeit durch Ausprobieren aller möglichen Schlüssel).

Beispiel: RSA (Schlüssellänge von 512 Bit bis 4096 Bit je nach Sicherheitsbedürfnis).

Verschlüsselung mit asymmetrischen Verfahren ist üblicherweise langsamer als mit symmetrischen Verfahren (RSA etwa um den Faktor 1000 langsamer als DES). Deshalb werden die Verfahren in der Praxis oft kombiniert.

Nutzung des asymmetrischen Kryptoverfahrens zum Austausch des geheimen Schlüssels.

Digitale Unterschrift

Durch Senden eines, mit dem privaten Schlüssel verschlüsseltem Datums kann man sich eindeutig ausweisen (eine Entschlüsselung ist nur mit dem öffentlichen Schlüssel der Person möglich).

Digitale Unterschrift = Name oder das Paar [Name, Zeitstempel] mit privatem Schlüssel verschlüsselt

Probleme mit sicherem Austausch von öffentlichen Schlüsseln.

Zertifikate

Einführung

Allgemeine grundlegende Themen in Informatik

- **Fragestellungen dieses Kapitels**
  - Übersicht über die verschiedenen Aspekte der Informatik
    - Mit welchen Bereichen beschäftigt sich Informatik?
    - Was gehört alles zu einem Computersystem?
  - Darstellung von Information
    - Was ist ein Byte?
    - Information und Nachricht

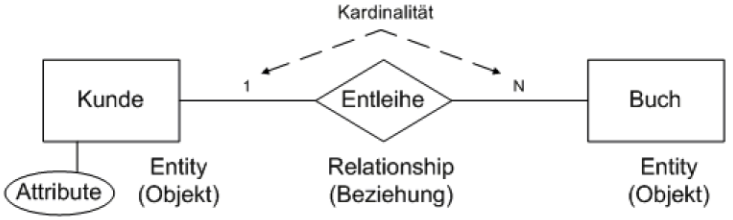
Was ist Informatik?

Computer

Darstellung von Information

ER-Modell

Entity-Relationship-Modell eignet sich zur Darstellung des Datenbankschemas.



Graphisches Hilfsmittel zur semantischen Modellierung eines Anwendungsgebietes, d.h. zum Entwurf einer Datenbank, unabhängig vom konkreten DBS.

Grundidee: Reale Welt (Mini-Welt) läßt sich durch Objekte und Beziehungen zwischen Objekten beschreiben (Objekte: Entities, Beziehungen: Relationships).

Gleichartige Entities (Objektinstanzen) werden zu Entity-Typen (vergleichbar Klassen) bzw. Relationships zu Relationship-Typen zusammengefasst.

Beispiele: Entity-Typ: "Bibliotheksbenutzer", "Buch", und Relationship-Typ: "entleiht".

Attribute bei Entities und Relationships, z.B. "Name" bei Entity "Bibliotheksbenutzer", "Entleihdatum" bei Relationship "leiht aus".

Entity-Typ

Relationship-Typ

Erweiterung auf n-stellige Beziehungen

Modellierung einer Datenbank findet auf der Ebene von Entity-Typen, Relationship-Typen und Attributen

Relationale Datenbanksysteme

Entity-Relationship-Diagramm: logisches Modell einer Datenbank. Für Implementierung in DBS: physikalisches Modell nötig.

Beispiel: relationales Datenbankmodell.

Relationales Modell

Tabellendarstellung

Normalisierung

Umsetzung des ER-Modells

Sichten

Verwendung von Sichten zur Auswahl einer Teilmenge der Tabellendaten.

Beispiel für eine Sicht: Vorname und Nachname von Kunden, die in München wohnen.

Views sind damit nichts anderes als benannte Such-Abfragen (z.B. SQL-Anfragen in MS ACCESS mit Namen).

Abfragesprache SQL

Beispielsysteme

mySQL (Open Source), Microsoft Access, Microsoft SQL Server, Oracle, DB2 (IBM), Sybase, Informix

Microsoft Access

Datenbanken und Informationssysteme

- Fragestellungen des Abschnitts:
  - Was unterscheidet Dateisysteme von Datenbanksystemen?
  - Wie kann die Struktur der Daten in einem Datenbanksystem dargestellt werden?
  - Was sind relationale Datenbanksysteme?
  - Was sind die grundlegenden Konstrukte von HTML?

Dateisysteme

Datenbanksysteme

Datenbankentwurf

Relationale Datenbanksysteme

WWW - Informationssystem

- Fragestellungen des Abschnitts:
  - Aus welchen (Hardware-)Elementen setzt sich ein Rechner zusammen?
  - Wie kommunizieren die einzelnen Komponenten eines Rechners?
  - Wie sieht die Schnittstelle zwischen Hardware und Software aus (d.h. Maschinenbefehle)?
  - Wie werden Zahlen, Text, Bilder, und Töne intern dargestellt?

Komprimierung

Datenkompression: reduzierte Speicher- und Übertragungskosten.

Verlustfreie Kompression

Ausnutzung von Mustern und Redundanzen in den Daten; Ausnutzung der Häufigkeit von Symbolen durch Änderung der Codierung.

Verlustbehaftete Kompression

Ausnutzung von Medien- und Wahrnehmungseigenschaften, z.B. bei MP3.

- Prof. J. Schlichter
  - Lehrstuhl für Angewandte Informatik / Kooperative Systeme

    Fakultät für Informatik, TU München

    E-Mail: schlichter@in.tum.de

    Tel.: 089-289 18654

    URL: http://www11.in.tum.de/

Dateiverwaltung (externer Speicher): Transparente Verfügbarmachung von externen Speichermedien; auf Festplatte werden Informationen in Dateien gespeichert.

Prozessverwaltung : Aufteilung des Prozessors auf mehrere gleichzeitig laufende Aufgaben.

Speicherverwaltung (interner Speicher): Aufteilung des Arbeitsspeichers auf mehrere gleichzeitig laufende Aufgaben (Programme).

Ein/Ausgabegeräte-Verwaltung : Abstraktion der Geräteeigenschaften und Behandlung konkurrierender Zugriffe.

Dateiverwaltung

Verfügbarmachung von externen Speichermedien für Programme. Organisation in "Dateien" statt Umgang mit Sektoren usw.

Dateien haben Namen, Inhalt und Attribute.

Datei-Inhalt

Folge von Bytes, von Programm interpretiert, z.B. als Text, als Zahlen, als Bild, als Folge von Maschinenbefehlen.

Operationen mit Dateien

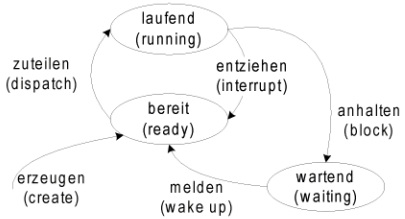
Typisch: Lesen, Schreiben, Ändern (Editieren), Kopieren, Ändern des Dateinamens, der Dateiattribute.

Dateisysteme

Physikalische Datei-Speicherung

Zustände eines Prozesses

"laufend": Prozess ist CPU zugeteilt, er kann Befehle ausführen. "wartend": auf Ende einer E/A-Übertragung.



Nur "Anhalten" durch Prozess selbst. Übrige Übergänge durch Betriebssystemkomponenten Dispatcher ("zuteilen"), Scheduler ("melden").

Das Betriebssystem verwaltet Listen der Prozesse im Zustand "bereit" oder "wartend".

In jedem Zustand kann der Prozess gelöscht, und damit aus dem System entfernt werden.

Prozess-Unterbrechungen (interrupt)

Stoppen die Prozessausführung aufgrund von Ereignissen. Beispiele: Rückmeldung eines E/A-Gerätes, Auftreten eines Alarms (z.B. Division durch 0), Ende einer Zeitscheibe (Taktgeber).

Unterbrechungen werden durch Hardware generiert (nur im Sonderfall abhängig von laufendem Prozess, z.B. Division durch 0).

Ablauf der Unterbrechungsbehandlung

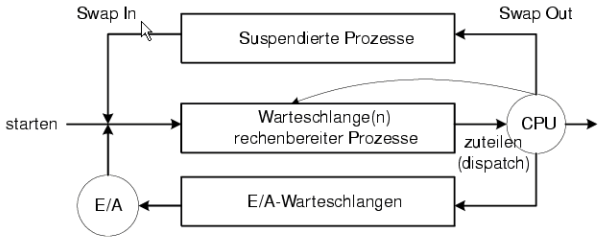
1. Während Prozess A rechnet, tritt eine Unterbrechung auf.
2. Der Prozessor setzt seine Programmausführung ***im Betriebssystem*** fort (Unterbrechungsbehandlung)
3. Der Zustand von Prozess A wird in den Prozess-Kontrollblock gespeichert
4. Die Unterbrechungsbehandlung wird ausgeführt (falls nötig)
5. Ein neuer (rechenbereiter) Prozess B wird ausgewählt (vom Scheduler)
6. Der Zustand von Prozess B wird geladen (Dispatcher)
7. Die Bearbeitung von Prozess B wird fortgesetzt (***Sprung in den Programmcode*** von B)

Unterbrechungsverarbeitung

"Interrupt-Handler": identifiziert Typ der Unterbrechung, wählt Programm zur Behandlung aus.

Prozessorzuteilung

Laufende Prozesse haben Prozessor (CPU) als exklusives Betriebsmittel. Bei Zeitmultiplexverfahren nur für gewisse Zeit ("Zeitscheibe"). Nach Ablauf wieder entzogen.



E/A-Warteschlangen: Prozesse, die auf Ein-/Ausgabe warten (wollen nicht rechnen). Suspendierte Prozesse: vorübergehend ausgelagert aus Arbeitsspeicher.

"Kunst des Programmierens". Grundlagen zu Datenstrukturen, Programmkonstrukte, Strukturierung von Programmen, objekt-orientierte Programmierung.

- Fragestellungen des Abschnitts:
  - Was ist ein Algorithmus?
  - Welche elementaren Datenstrukturen gibt es?
  - Was sind die grundlegenden Konstrukte einer Programmiersprache?
  - Was ist unter Objekt-orientierter Programmierung zu verstehen?
  - Was versteht man unter Modularisierung und Rekursion?

Grundlagen der Programmierung

"Kunst des Programmierens". Grundlagen zu Datenstrukturen, Programmkonstrukte, Strukturierung von Programmen, objekt-orientierte Programmierung.

- Fragestellungen des Abschnitts:
  - Was ist ein Algorithmus?
  - Welche elementaren Datenstrukturen gibt es?
  - Was sind die grundlegenden Konstrukte einer Programmiersprache?
  - Was ist unter Objekt-orientierter Programmierung zu verstehen?
  - Was versteht man unter Modularisierung und Rekursion?

Einführung

Algorithmus

Datentypen und Ausdrücke

Programmkonstrukte

Objektorientierte Programmierung

Modularisierung von Programmen

Rekursion

Generated by Targeteam

Datenstrukturen und Algorithmen

In diesem Kapitel werden einige Klassen von Algorithmen vorgestellt, insbesondere Suchverfahren und Sortierverfahren.

- Fragestellungen des Abschnitts:
  - Welche Möglichkeiten gibt es, Datenmengen im System darzustellen?
  - Welche Möglichkeiten gibt es, in Datenmengen zu suchen?
  - Welche Möglichkeiten gibt es, Datenmengen zu sortieren?
  - Was versteht man unter der Komplexität eines Algorithmus?

Komplexität

Algorithmus kann Aufwand erfordern, der "nicht vertretbar" ist. Bei algorithmischer Lösung eines Problems ist daher auch die Effizienz wesentlich.

Komplexität von Algorithmen

Ein Algorithmus ist umso effizienter, je geringer der Aufwand zu seiner Abarbeitung ist.

Aufwand bezieht sich auf bestimmte Ressourcen, z.B. Rechenzeit, Speicherplatz, Anzahl der Geräte

Je nach Ressource verschiedene Komplexitätsmaße. Wichtigste: Zeitkomplexität, Speicherplatzkomplexität.

Zu unterscheiden: Komplexität eines Algorithmus / eines Problems. Problem: zu erreichendes Ziel. Algorithmus: Vorgehen. Komplexität Problem = Komplexität effizientester bekannter Algorithmus.

Komplexitätsmaß für Algorithmus: Funktion abhängig von Größe der Eingabe. Misst Aufwand der Verarbeitung relativ zur zu verarbeitenden Information.

Beispiel

Liste Sortieren: Komplexitätsmaß abhängig von Anzahl der zu sortierenden Elemente; Brechen eines Schlüssels: Komplexitätsmaß meist abhängig von Schlüssellänge.

Algorithmen bewertet man relativ zu ihrer Komplexität.

Software-Engineering

Softwareerstellung als Ingenieurdisziplin.

Software/Engineering - Definition des Ideals

> Die Aufstellung und Befolgung guter Ingenieur-Grundsätze und Management-Praktiken, sowie die Entwicklung und Anwendung zweckdienlicher Methoden und Werkzeuge, mit dem Ziel, mit vorhersagbaren Mitteln, System- und Software-Produkte zu erstellen, die hohe, explizit vorgegebene Qualitätsansprüche erfüllen (nach A. Marco & J. Buxton, 1987)

Modelle für Analyse und Entwurf

Vor Programmierung. Unterschiedliche Modelle.

Einführung in die Informatik für andere Fachrichtungen

- Prof. J. Schlichter
  - Lehrstuhl für Angewandte Informatik / Kooperative Systeme

    Fakultät für Informatik, TU München

    E-Mail: schlichter@in.tum.de

    Tel.: 089-289 18654

    URL: http://www11.in.tum.de/

Verschlüsselung

Verschlüsselung bedeutet, dass man Daten für die Übertragung oder Speicherung so codiert, dass sie nur vom beabsichtigten Empfänger wieder in "Klartext" zurückcodiert werden können. Für alle eventuellen "Mithörer" bleiben die Daten eine uninterpretierbare Bitfolge.

> Web-Adresse: https://..... ⇒ Daten werden verschlüsselt zwischen Web Browser und Web Server übertragen (z.B. für Online Bestellungen bei Amazon).
>
> Es gibt zwei grundlegende Verfahrensklassen für die Verschlüsselung von Daten: symmetrische Verschlüsselung und asymmetrische Verschlüsselung.

Ein wichtiger Aspekt eines Rechnersystems besteht darin, dass Daten nicht von Unbefugten abgefragt werden können. Bei nicht-vernetzten Systemen läßt sich dies durch eine Sicherung des physikalischen Zugangs zu den Rechnern und einfache Passwortsysteme garantieren. Bei verteilten Systemen werden zusätzliche Dienste benötigt.

Sicherheitsanforderungen

- Garantierung der Identität eines Absenders (Identitätsprüfung, Authentifizierung).
- Verhinderung von Mithören (Verschlüsselung).
- Sicherstellung der Integrität (Unverfälschtheit) von Nachrichten (Hash-Werte).
- Verhinderung des Wiedereinspielens von Nachrichten (Integritätssicherung und Zeitstempel).

Arten von Schadsoftware

Verschlüsselung

Identitätsprüfung