Script **generated by TTT**

Title: Einf_HF (13.07.2015)

Date: Mon Jul 13 14:15:26 CEST 2015

Duration: 84:16 min

Pages: 46

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

    Fakultät für Informatik, TU München

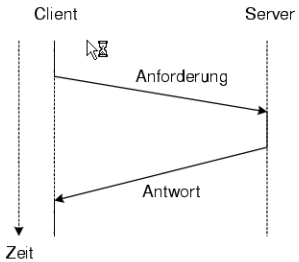
    E-Mail: schlichter@in.tum.de

    Tel.: 089-289 18654

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

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.

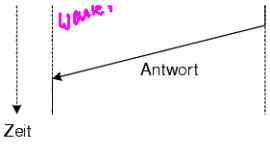
Clients sind meist a-priori beim Server nicht bekannt.

Definition: Server

Softwaresystem, 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 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

Softwaresystem, 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)
}
```

Verteilte Anwendungen

Aufteilung einer Anwendung in Komponenten (einzelne Programme auf verschiedenen Rechnern), die miteinander kommunizieren um einen Dienst zu erbringen.

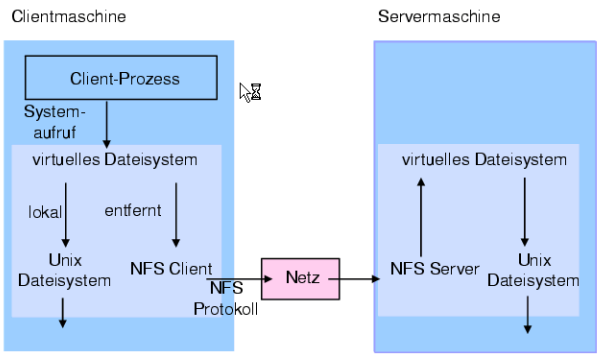
Fortschreitende Vernetzung von heterogenen Rechnern. Anwendungen zur gemeinsamen Nutzung von Ressourcen, Kommunikation von Informationen, Koordination von Aktivitäten.

Client-Server-Modell

Beispiel-Services

World Wide Web

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.

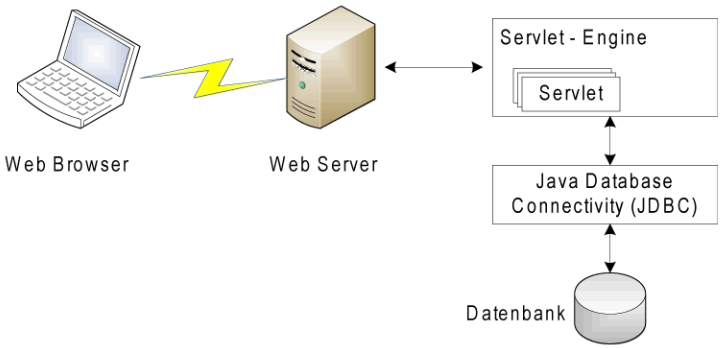
World Wide Web

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.

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

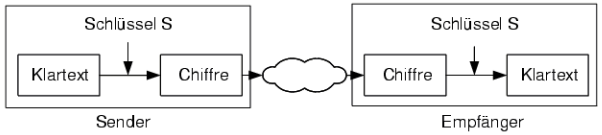
- Garantierung der Identität eines Absenders (Identitätsprüfung, Authentifizierung).
- Verhinderung von Mithören (Verschlüsselung).
- Sicherstellung der Integrität (Unverfälschtheit) von Nachrichten (Hash-Werte).
- Verhinderung des Wiedereinspielens von Nachrichten (Integritätssicherung und Zeitstempel).

Arten von Schadsoftware
Verschlüsselung
Identitätsprüfung

Generated by Targeteam

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)

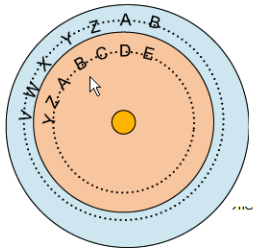
Für jede mögliche Verbindung wird ein eigener Schlüssel benötigt (Falls derselbe Schlüssel für Nachrichten an B und C benutzt wird, könnte C Nachrichten an B lesen).

Beispiele: DES, Tripple DES, IDEA

Erweiterte Caesar-Chiffre

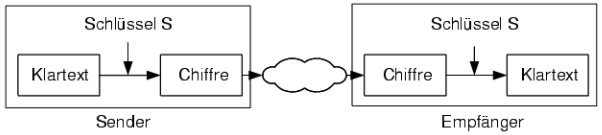
Erweiterte Caesar-Chiffre

- 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**



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).

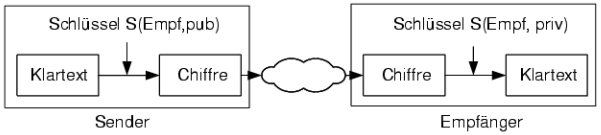
Beispiele: DES, Tripple DES, IDEA

Erweiterte Caesar-Chiffre

Generated by Targeteam

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.

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

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

Identitätsprüfung

Allgemeine Möglichkeiten

Prüfe etwas, das die Person weiß (z.B. Passwort)

Prüfe etwas, das die Person besitzt (z.B. Ausweis, Chipkarte)

Prüfe eine physikalische Charakteristik der Person (z.B. Fingerabdruck)

Prüfe Ergebnis einer unbewussten Aktion der Person (z.B. Unterschrift)

Grundproblem bei digitaler Übermittlung von Passworten oder anderen Identitätsbeweisen in verteilten Systemen ist die Kopierbarkeit. Mögliche Lösungen sind:

Verschlüsselte Übermittlung des Passworts (immer noch kopierbar ...)

Eine andere Möglichkeit ist die "digitale Unterschrift".

Digitale Unterschrift

Zusammenfassung

Diese Lehrveranstaltung gab eine umfassende Einführung in die verschiedenen Aspekte, Methoden und Technologien der Informatik, insbesondere

Datenbanken und Informationssysteme

Datenstrukturen, Algorithmen und Codierung von Information

Grundlagen der Programmierung und Software-Entwicklungstechnik (Software Engineering)

Rechnerarchitektur, Betriebssysteme

Rechnernetze und Verteilte Systeme mit Client-Server-Architekturen

- 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/

Einführung in die Informatik für ar
Übersicht
Einführung
Was ist Informatik?
Computer
Darstellung von Informati
Datenbanken und Informatic
Rechnerarchitektur
Systemsoftware
Grundlagen der Programmie
Datenstrukturen und Algorith
Software-Entwicklung
Grundlagen von Rechnerne
Anwendungen von Rechner
Zusammenfassung

Bits und Bytes

Grundlage der Darstellung im Rechner.

Bits

Abkürzung für "Binary digits".

"Bit": kleinstmögliche Informationsheit. Zwei mögliche Werte, z.B. Ja / Nein, Wahr / Falsch, Links / Rechts.

Oft: 0 / 1. Technisch: elektrische Ladungen (0 = ungeladen, 1 = geladen), elektrische Spannungen (0 = 0 Volt, 1 = 5 Volt) oder Magnetisierungen.

Bitfolgen : falls mehr als zwei Werte notwendig. (z.B. Frage: "Woher kommt der Wind?" - Süd, West, Ost oder Nord).

Bitfolge	Himmelsrichtung
000	Süd
001	West
010	Nord
011	Ost
100	Südost
101	Nordwest
110	Nordost
111	Südwest

Je zusätzlichem Bit: doppelte Anzahl der möglichen Bitfolgen. 2^N mögliche

Einführung in die Informatik für ar
Übersicht
Einführung
Was ist Informatik?
Computer
Darstellung von Informati
Datenbanken und Informatic
Rechnerarchitektur
Systemsoftware
Grundlagen der Programmie
Datenstrukturen und Algorith
Software-Entwicklung
Grundlagen von Rechnerne
Anwendungen von Rechner
Zusammenfassung

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

Einführung in die Informatik für ar
Übersicht
Einführung
Datenbanken und Informatic
Dateisysteme
Datenbanksysteme
Datenbankentwurf
Relationale Datenbanksy
WWW - Informationssyste
Rechnerarchitektur
Systemsoftware
Grundlagen der Programmie
Datenstrukturen und Algorith
Software-Entwicklung
Grundlagen von Rechnerne
Anwendungen von Rechner
Zusammenfassung

Datenmodell

Die Daten in einem Datenbanksystem bilden ein abstrahiertes Spiegelbild einer Miniwelt.
⇒ Verwendung von Datenmodellen.

Definition: Ein **Datenmodell** ist ein (oft mathematischer) Formalismus

mit einer Notation zur Beschreibung und Definition der Datenobjekte und deren Struktur,

einer Menge von Operationen zur Manipulation der Daten.

Nicht beschrieben werden Abläufe, Interaktion zwischen Objekten oder zeitliches Verhalten.

Beispiele

Entity-Relationship-Modell (ER-Modell), Objektorientiertes Modell, Hierachisches Modell.

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

Aggregatfunktionen und Gruppierung

Aggregatfunktionen führen Berechnungen durch und liefern als Ergebnis einen einzelnen Wert

SELECT AVG(GebJahr) FROM Mitarbeiter; # liefert das Durchschnitts-Geburtsjahr

SELECT SUM(GebJahr) FROM Mitarbeiter; # liefert die Summe aller Geburtsjahre

SELECT COUNT(GebJahr) FROM Mitarbeiter; # liefert die Anzahl der Mitarbeiter, die Geburtsjahr angegeben haben

SELECT MIN(GebJahr) FROM Mitarbeiter; # liefert den jüngsten Mitarbeiter

SELECT MAX(GebJahr) FROM Mitarbeiter; # liefert den ältesten Mitarbeiter

SELECT AVG(GebJahr) FROM Mitarbeiter WHERE PersNr > 2000;

liefert das Durchschnitts-Geburtsjahr mit Personalnummern höher als 2000

SELECT AbtID, AVG(GebJahr) FROM Mitarbeiter GROUP BY AbtID;

liefert das Durchschnitts-Geburtsjahr in den einzelnen Abteilungen

SELECT AbtID, AVG(GebJahr) FROM Mitarbeiter GROUP BY AbtID HAVING COUNT (*) > 1;

liefert das Durchschnitts-Geburtsjahr zu den Abteilungen, die mehr als einen Mitarbeiter haben

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

Befehlsvorrat

Transportbefehle

z.B. LOAD, STORE. LOAD: Transportieren von Daten vom Arbeitsspeicher in ein Register; STORE spezifiziert den umgekehrten Weg.

Arithmetische und logische Befehle

z.B. ADD, SUB, AND, OR, CMP

Schiebebefehle

z.B. SH (Shift links, rechts), ROT (Schieben im Kreis)

Sprungbefehle

z.B. JMP (Jump), JGT (Jump Greater Than) - (bedingte) Änderung der Ablaufreihenfolge

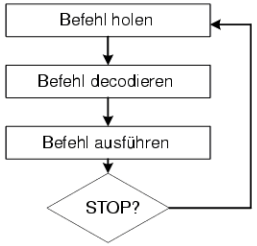
Sonderbefehle

Behandlung von Unterbrechungen (z.B. Alarm bei Division durch 0), Änderungen des Maschinenstatus, Rückmeldungen von E/A Geräten, Laden von Prozessbeschreibungen, Synchronisationsbefehle bei Speicherzugriff etc.

Befehlszyklus

Ausführung eines Maschinenbefehls: festes Schema (Bereitstellung, Bereitstellen der Operanden, Befehl entschlüsseln, Ausführung). Dieses Schema heißt Befehlszyklus.

Sequentielle Bearbeitung



kein ausführbares Programm ⇒ Ausführung von NOP ("No Operation").

Fließband Bearbeitung (Pipelining)

Codierung ganzer Zahlen

Codierung im Binärsystem. Zwei Ziffern 0,1 ("Bits") geben Anzahl von Zweierpotenzen an. Vgl. Dezimalsystem: Zehn Ziffern geben Anzahl von Zehnerpotenzen an.

Beispiel

Dezimalsystem: $148 = 1 * 10^2 + 4 * 10^1 + 8 * 10^0$

Binärsystem: $1010 = 1 * 2^3 + 0 * 2^2 + 1 * 2^1 + 0 * 2^0$ (= 10 im Dezimalsystem)

Formel für Wert einer Binärsystem-Zahl

$$W = \sum_{i=0}^{n-1} \left(b_i \times 2^{n-1-i} \right)$$

mit den Binärziffern $b_i \in \{0,1\}$ und n ist die Anzahl der verwendeten Bits (d.h. eine n-stellige Zahl). Beachte, es wird die Folge $b_0\, b_1 \ldots b_{n-1}$ betrachtet.

Beispiel

eine ganze Zahl sei als 8 bit lange Zahl zur Basis 2 dargestellt

$$W\,(00001101_2) = 0 \times 2^7 + \ldots + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 8 + 4 + 1 = 13_{10}$$

Verfahren zur Umwandlung

Feste Ziffernanzahl

Typisch: Feste Bitzahl, meist ebenfalls Zweierpotenz. Z.B. 4 Bit, 16 Bit, 32 Bit oder 64 Bit. Aktuell entweder 32 oder 64 Bit verwendet. Mit n Bit codierbar: Werte 0 bis 2^n -1.

Objektorientierte Programmierung

Softwaresystem realisiert durch Menge von Objekten. Gegensatz prozedurale Programmierung: Anweisungen im Vordergrund.

Objektorientiertes Programmieren: Daten im Vordergrund. In Objekten zusammengefasst ("Verkapselung"). Funktionen lokal bei Objekten definiert.

Die Funktionen werden Methoden genannt.

Objekt - Klasse

Erzeugen eines Objekts

Vererbung

Datenstrukturen

Datenstruktur = Menge von Daten eines bestimmten Typs zusammen mit den auf der Menge ausführbaren Zugriffsoperationen.

Beispiel: natürliche Zahlen zusammen mit Grundrechenoperationen

Bei Programmierung wichtiges Hilfsmittel zur Organisation der Daten für die maschinelle Verarbeitung.

Listen

Queue - Warteschlange

Eine weitere grundlegende Datenstruktur sind Queues, die mit Warteschlangen vergleichbar sind (FIFO-Prinzip, first-in-first-out).

`put()` : fügt ein Element am Ende der Warteschlange hinzu

`get()` : entnimmt ein Element am Anfang der Warteschlange und liefert es zurück

Realisierung als verkettete Liste oder als Array (falls maximale Größe bekannt).

Graphen

Suchverfahren

Gegeben: Menge von Datensätzen. Gesucht: Datensatz mit bestimmter Eigenschaft.

Mengen von Datensätzen

Üblicherweise in Reihung oder Liste gespeichert.

Annahme für die folgenden Verfahren: Daten in einer Reihung gespeichert.

Lineare Suche

Binäre Suche

Suchverfahren Animation

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.

Komplexitätsklassen

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.

Komplexitätsklassen

Generated by Targeteam

Auswahl einer Programmiersprache

Prinzipiell Programmiersprachen gleichwertig: alle Algorithmen formulierbar. Praktische Unterschiede helfen bei Auswahl für Entwicklungsprojekt.

Empfehlungen

wenn ...	... dann
einfache Programme, Anwendungserweiterungen	Basic, Visual Basic, Python, Perl
Datenbank-Anwendung und komplexe Programmlogik	C, C++ , Java
Datenbank-Anwendung und einfache Programmlogik	SQL, Reportgenerator
Technisch-wissenschaftliche Anwendung und (Datenbank oder komplexe E/A-Strukturen) und Portabilität	C, C++, Java
(System-Software oder PC-Anwendung) und Portabilität	C, C++, Java
Künstliche Intelligenz-Anwendung	Prolog, LISP
Internet-Anwendung und Portabilität	Java, PHP, Python

Software-Entwicklung

"Vorgehen bei der Entwicklung von Softwaresystemen". Vorgehensmodelle für die Entwicklung von Programmen, Modelle für Analyse und Entwurf.

- Fragestellungen des Abschnitts:
  - Welche Kategorien von Programmiersprachen gibt es ?

    interpretierte und übersetzte Sprachen
  - Wie kann man bei der Konzeption und der Realisierung eines Software-Programms geeignet vorgehen?

    Modellierung der verschiedenen Aspekte, z.B. Daten, Abläufe und Interaktion mit dem Benutzer.

Programmiersprachen

Software-Engineering

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)

Komplexität von Software-Projekten

Vorgehensmodelle

Strukturierte Programmierung

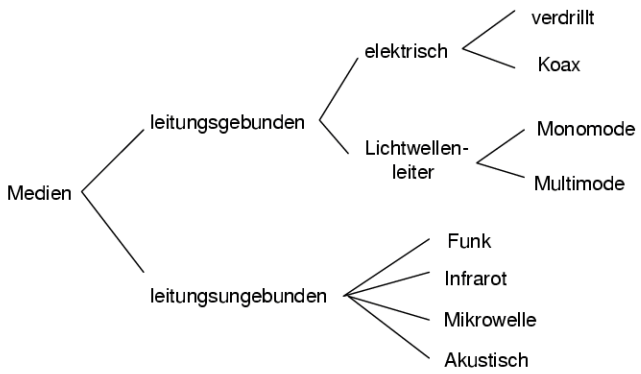
Modellierung

Modelle für Analyse und Entwurf

Übertragungsmedien

Kriterien zur Kategorisierung

Einteilung der Übertragungsstrecken

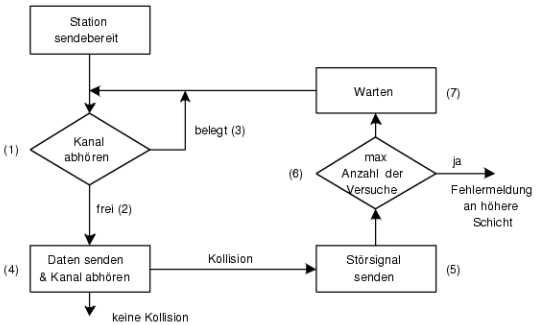


Übertragungsraten

Die Leistungsfähigkeit einer Verbindung in Rechnernetzen gibt man üblicherweise in Form einer Übertragungsrate an. Übertragungsraten werden in Bit pro Sekunde angegeben, d.h. pro Sekunde können über die Verbindung die genannte Zahl von Bits übertragen werden.

Klassifizierung der Netze nach Datenrate und Entfernung

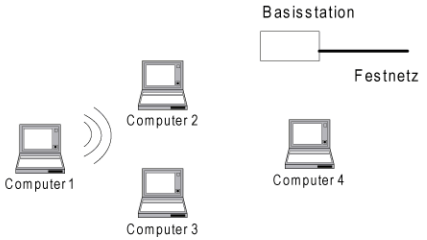
Ablauf des Zugriffsverfahrens



1. Sendewillige Station (Rechner) überwacht Übertragungsmedium (Bus)
2. Übertragungsmedium frei, dann kann Übertragung beginnen
3. Übertragungsmedium belegt, kurze Zeit später Übertragungsmedium erneut überprüfen
4. Während der Übertragung wird Kanal simultan abgehört; falls gesendete Information und abgehörte Information unterschiedlich, dann wurde eine Kollision festgestellt, d.h. ein anderer Rechner hat auch mit der Übertragung begonnen.
5. Bei Kollision Senden eines Störsignals
6. Warten gemäß Backoff Strategie; Berechnung der Wartezeit abhängig von der Anzahl der Wiederholungen und von Zufallszahlen, d.h. Auswahl von Zufallszahlen aus [0,1], [0,2], [0,4], [0,8],..

verwenden i.a. eine modifizierte Form von CSMA/CD ⇒ CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance).

alle Rechner eines bestimmten drahtlosen LAN senden auf der gleichen Funkfrequenz (z.B. 2,4 Ghz Bereich).



Ablauf des Verfahrens, falls Computer 1 an Computer 2 senden möchte.

Computer 1 überprüft, ob gerade ein anderer Rechner sendet.

falls nein sendet Computer 1 eine Steuernachricht an Computer 2, in dem er seinen Übertragungswunsch kundtut.

Computer 2 antwortet mit einer Steuernachricht an Computer 1, in dem er seine Bereitschaft kundtut.

bei Erkennen einer Steuernachricht warten alle anderen Rechner bis die Übertragung der Nachricht von Computer 1 abgeschlossen ist.

Computer 1 sendet seine Nachricht an Computer 2.

Das World Wide Web (WWW bzw. Web) ist ein über das Internet abrufbares Informationssystem, basierend auf dem Hypertext-Ansatz.

Hypertext

Einführung in HTML

Cascading Style-Sheets (CSS)

Generated by Targeteam

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.

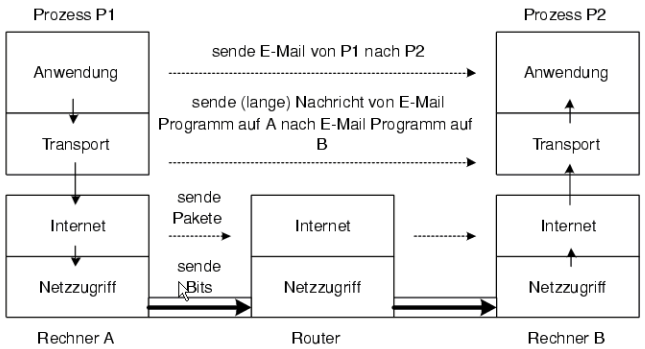
Zur Reduzierung der Komplexität beim Entwurf eines offenen Rechnernetzes wird das Netz in aufeinander aufbauende Protokoll-Schichten unterteilt.

Prinzipien für Schichtung

Aufbau des Internet-Schichtenmodells

Bedeutung der Schichten

Generated by Targeteam



Gepunktete Pfeile repräsentieren logische Übertragungen.

Generated by Targeteam

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).

Anwendungen von Rechnernetzen

- Fragestellungen des Abschnitts:
  - Was versteht man unter dem Client/Server-Modell?
  - Was versteht man unter Verschlüsselung? Welche grundlegenden Verfahren gibt es?
  - Was versteht man unter digitalen Signaturen?

Verteilte Anwendungen

Sicherheit in verteilten Systemen

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