

Script generated by TTT

Title: Grundlagen_Betriebssysteme (25.01.2013)

Date: Fri Jan 25 08:29:54 CET 2013

Duration: 89:58 min

Pages: 22



RAID



Erhöhung der Plattenkapazität durch Zusammenschluss von mehreren kleinen Festplatten zu einer großen virtuellen Platte.

⇒ RAID = redundant array of inexpensive disks.

Für das BS sieht RAID wie eine einzelne Festplatte aus.

keine Änderung an Anwendungssoftware notwendig, um ein RAID-System nutzen zu können.

üblicher Plattencontroller wird durch einen RAID Controller ersetzt.

Daten werden über die Platten verteilt, was eine parallele Verarbeitung ermöglicht.

höhere Zuverlässigkeit durch Redundanz.

Unterscheidung zwischen unterschiedlichen Varianten

RAID Level 0 bis RAID Level 6.

[RAID Level 0](#)

[RAID Level 1](#)

[RAID Level 2](#)

Die restlichen Varianten RAID Level 3 - 6 können im Tanenbaum nachgelesen werden. Kombinationen von RAID Level sind möglich, z.B. RAID 0+1.

Generated by Targeteam



RAID Level 1

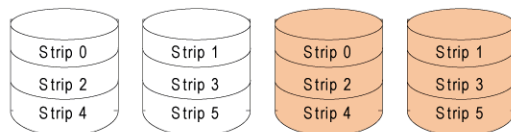


Es werden alle Platten verdoppelt.

Bei einem Schreibvorgang wird jeder Strip doppelt geschrieben.

Bei einem Lesevorgang können beide Platten genutzt werden.

Sehr gute Ausfallsicherheit.



Spiegelplatten

Generated by Targeteam



Striping erfolgt auf Bitebene mit zusätzlichen Parity-Platten.

Alle Platten arbeiten synchron.

Sehr gute Ausfallsicherheit, mit weniger Platten als bei RAID Level 1.



Paritybits

Generated by Targeteam



Erhöhung der Plattenkapazität durch Zusammenschluss von mehreren kleinen Festplatten zu einer großen virtuellen Platte.

⇒ RAID = redundant array of inexpensive disks.

Für das BS sieht RAID wie eine einzelne Festplatte aus.

keine Änderung an Anwendungssoftware notwendig, um ein RAID-System nutzen zu können.

üblicher Plattencontroller wird durch einen RAID Controller ersetzt.

Daten werden über die Platten verteilt, was eine parallele Verarbeitung ermöglicht.

höhere Zuverlässigkeit durch Redundanz.

Unterscheidung zwischen unterschiedlichen Varianten

RAID Level 0 bis RAID Level 6.

RAID Level 0

RAID Level 1

RAID Level 2

Die restlichen Varianten RAID Level 3 - 6 können im Tanenbaum nachgelesen werden. Kombinationen von RAID Level sind möglich, z.B. RAID 0+1.

Generated by Targeteam

Ein-/Ausgabe



Hauptaufgabe eines BS: Steuerung und Überwachung aller E/A-Geräte.

Klassifikation von E/A-Geräten

Schichten eines E/A-Systems

Geräteverwaltung

RAID

Disk Scheduling

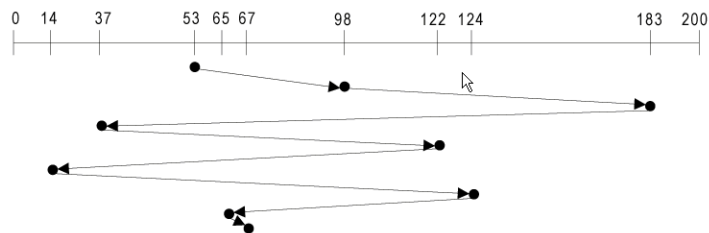
Multimedia Systems

Generated by Targeteam



Die E/A-Requests werden in der Reihenfolge ihres Eintreffens abgearbeitet (First Come-First Served). Angenommen die E/A-Requests betreffen Blöcke der Zylinder

98, 183, 37, 122, 14, 124, 65, 67.



Generated by Targeteam

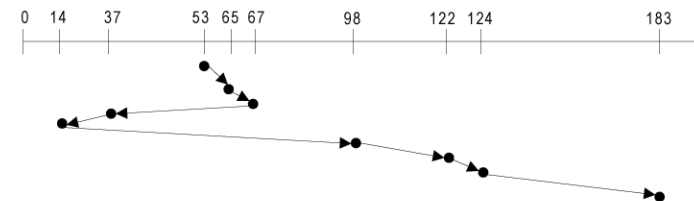
SSTF Scheduling



Beim SSTF-Verfahren (Shortest Seek Time First) wird als nächstes der E/A-Request bearbeitet, der am nächsten zur aktuellen Position ist. Die Ausgangsliste

98, 183, 37, 122, 14, 124, 65, 67 wird umsortiert zur Bearbeitungsreihenfolge

65, 67, 37, 14, 98, 122, 124, 183.



Generated by Targeteam



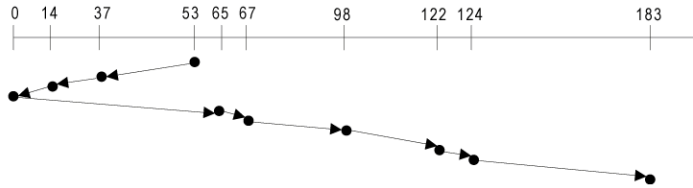
SCAN Scheduling



Der SCAN-Algorithmus bearbeitet die E/A Requests zunächst in eine Richtung bis zum Plattenende, und anschließend zurück zum anderen Plattenende. Die Ausgangsliste

98, 183, 37, 122, 14, 124, 65, 67 wird umsortiert zur Bearbeitungsreihenfolge

37, 14, 0, 65, 67, 98, 122, 124, 183.



Generated by Targeteam



Disk Scheduling



Zugriffszeit für Transfer von Daten von/zu Festplatte setzt sich zusammen aus

Suchzeit des Lese-/Schreibkopfes.

Rotationsverzögerung.

Dauer der Datenübertragung.

Reduktion der Suchzeit durch geeignetes Scheduling von E/A-Requests.

[FCFS Scheduling](#)

[SSTF Scheduling](#)

[SCAN Scheduling](#)

Generated by Targeteam



Disk Scheduling



Zugriffszeit für Transfer von Daten von/zu Festplatte setzt sich zusammen aus

Suchzeit des Lese-/Schreibkopfes.

Rotationsverzögerung.

Dauer der Datenübertragung.

Reduktion der Suchzeit durch geeignetes Scheduling von E/A-Requests.

[FCFS Scheduling](#)

[SSTF Scheduling](#)

[SCAN Scheduling](#)

Generated by Targeteam



Disk Scheduling



Multimedia Daten können in einem normalen Dateisystem gespeichert werden. Für die Auslieferung gelten jedoch spezielle Zeitbedingungen, z.B.

Auslieferung von Videodaten gemäß einer Rate von 24 - 30 Frames/Sekunde.

Unterscheidung zwischen

lokales Playback.

Streaming

Zustellung der Mediendaten von einem Server über ein Netzwerk zum Client. Unterscheidung zwischen

progressives Download.

Real-time Streaming.

Live Streaming.

On-Demand Streaming.

Beispiele von Streaming Produkten: RealPlayer, Apple Quicktime, Windows Media Player.

Generated by Targeteam

Multimedia Daten können sehr groß sein.
deshalb Komprimierung der Daten

⇒ ausreichende Rechenleistung für die Dekompression und Anzeige der Mediendaten unter Einhaltung der Zeitbedingungen.

Disk Scheduling

Generated by Targem.com

Für den Zugriff auf Mediendaten gelten die beiden Randbedingungen
Zeitbedingungen und hohe Datenrate.

Kombination von SCAN Scheduling mit EDF ("Earliest-Deadline-First").

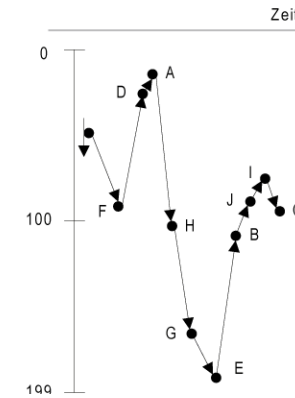
Aufträge werden entsprechend ihrer Deadline geordnet (EDF).

Aufträge mit derselben Deadline werden entsprechend SCAN Reihenfolge abgearbeitet.

Aufträge mit ähnlichen Deadlines können entsprechend der SCAN Reihenfolge umsortiert werden, solange die Zeitbedingungen noch eingehalten werden.

Einteilung der Aufträge in Zeitbereiche (z.B. 100 ms)

Auftrag	Deadline	Zylinder
A	150	25
B	201	112
C	399	95
D	94	31
E	295	185
F	78	85
G	165	150
H	125	101
I	300	85
J	210	90



Disk Scheduling

Zeitbedingungen und hohe Datenrate.

Kombination von SCAN Scheduling mit EDF ("Earliest-Deadline-First").

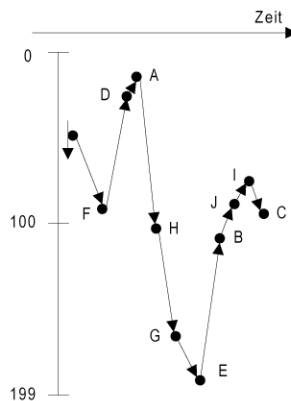
Aufträge werden entsprechend ihrer Deadline geordnet (EDF).

Aufträge mit derselben Deadline werden entsprechend SCAN Reihenfolge abgearbeitet.

Aufträge mit ähnlichen Deadlines können entsprechend der SCAN Reihenfolge umsortiert werden, solange die Zeitbedingungen noch eingehalten werden.

Einteilung der Aufträge in Zeitbereiche (z.B. 100 ms)

Auftrag	Deadline	Zylinder
A	150	25
B	201	112
C	399	95
D	94	31
E	295	185
F	78	85
G	165	150
H	125	101
I	300	85
J	210	90



Generated by Targem.com

Eigenschaften von Multimedia Systemen

Multimedia Daten können sehr groß sein.

deshalb Komprimierung der Daten

⇒ ausreichende Rechenleistung für die Dekompression und Anzeige der Mediendaten unter Einhaltung der Zeitbedingungen.

Disk Scheduling

Generated by Targem.com



Fragestellungen

Dieser Abschnitt behandelt die Sicherheitsproblematik in zentralen Rechensystemen. Dazu werden verschiedene Schutzmechanismen auf Betriebssystemebene vorgestellt.

Zugriffsschutz in Rechensystemen.

Schutzmatrix, insbesondere Zugriffskontrolllisten und Capability-Listen.

Mobiler Code.

[Motivation](#)

[Schutzmechanismen](#)

[Mobiler Code](#)

Generated by Targeteam



Beispiel: Login-Attrappe



Nutzung von Login-Attrappen in Rechnerumgebungen, wo Rechner von mehreren Benutzern verwendet werden, um geschützte Benutzerpasswörter zu erfassen (z.B. in Informatikhalle der Informatik-Fakultät).

Angreifer startet ein Benutzerprogramm, das am Bildschirm einen Login-Screen simuliert.

Der ahnungslose Benutzer tippt Benutzernamen und sein privates Passwort.

Angreiferprogramm speichert Benutzernamen und Passwort in einer Datei.

Angreiferprogramm terminiert das aktuelle Shell-Programm ("kill" Systemaufruf) ⇒ Login-Sitzung des Angreifers wird beendet und regulärer Login-Screen wird angezeigt.

Abhilfe: Login-Sequenz wird durch Tastensequenz gestartet, die von einem Benutzerprogramm nicht erfasst werden kann, z.B. CTRL-ALT-DEL bei Windows 2000.

Generated by Targeteam



Motivation



Was versteht man unter Sicherheit im Bezug auf Rechensysteme?

Jemand : Unterscheidung von Personen und Gruppen von Personen

davon abhalten : durch technische und organisatorische Maßnahmen

einige : Begrenzung durch unser Vorstellungsvermögen

unerwünschte Dinge zu tun :

- 1) nicht autorisiert Daten lesen (Geheimhaltung, Vertraulichkeit),
- 2) nicht autorisiert Daten schreiben (Integrität),
- 3) unter "falscher Flagge" arbeiten (Authentizität),
- 4) nicht autorisiert Ressourcen verbrauchen (Verfügbarkeit),
usw.

zu tun .

Unterscheidung zwischen Angriffen von

innen .

außen .

Beispiel: Login-Attrappe

Beispiel: Virus

Beispiel: Pufferüberlauf



Beispiel: Login-Attrappe



Nutzung von Login-Attrappen in Rechnerumgebungen, wo Rechner von mehreren Benutzern verwendet werden, um geschützte Benutzerpasswörter zu erfassen (z.B. in Informatikhalle der Informatik-Fakultät).

Angreifer startet ein Benutzerprogramm, das am Bildschirm einen Login-Screen simuliert.

Der ahnungslose Benutzer tippt Benutzernamen und sein privates Passwort.

Angreiferprogramm speichert Benutzernamen und Passwort in einer Datei.

Angreiferprogramm terminiert das aktuelle Shell-Programm ("kill" Systemaufruf) ⇒ Login-Sitzung des Angreifers wird beendet und regulärer Login-Screen wird angezeigt.

Abhilfe: Login-Sequenz wird durch Tastensequenz gestartet, die von einem Benutzerprogramm nicht erfasst werden kann, z.B. CTRL-ALT-DEL bei Windows 2000.

Generated by Targeteam



Beispiel: Virus



Ein **Virus** ist ein Programm, dessen Code an ein anderes Programm angefügt ist und sich auf diese Weise reproduziert. Zusätzlich kann ein Virus noch andere Funktionen aufrufen, z.B. Löschen von Dateien, Senden von Nachrichten etc.

Virus schläft bis infiziertes Programm ausgeführt wird.

Start des infizierten Programms führt zur Virusreproduktion.

Ausführung der Virusfunktion ist u.U. mit einem zeitlichen Datum versehen.

mögliche Virustypen sind

Boot Sector Virus .

Macro Virus . Programme wie Word oder Excel erlauben dem Benutzer das Schreiben von Macroprogrammen (Visual Basic).

Ausführbares Programm als Virus .

Verbreitung von Viren

Früher diente der Austausch von Datenträgern (z.B. Floppy Disk), jetzt das Internet als Attachment zu Emails

Lesen des Adressbuchs und automatische Generierung von Emails mit Virus Attachment an alle Adressbucheinträge (z.B. von Microsoft Outlook).

Generated by Targeteam



Beispiel: Pufferüberlauf



Durch einen künstlich herbeigeführten Pufferüberlauf kann ein Angreifer die Ausführung seines eigenen Programms veranlassen und oft auch noch die Systemadministrator-Berechtigung (root) erlangen.

[Hintergrund](#)

[Veränderung der Rücksprungsadresse](#)

Gegenmaßnahmen

Unterscheidung

sichere Programmierung.

Maßnahmen zur Übersetzungszeit.

Maßnahmen zur Laufzeit.

Generated by Targeteam



Implementierung der Unix Funktion `gets` (get string from stdin)

keine Möglichkeit zur Spezifikation der Anzahl der zu lesenden Zeichen

```

char *gets(char *dest) {
    int c = getc();
    char *p = dest;
    while (c != EOF && c != '\n') {
        *p++ = c; c = getc();
    }
    *p = '\0';
    return dest;
}

```

ähnliche Probleme auch bei anderen Unix Funktionen

`strcpy`: kopiert einen String beliebiger Länge

`scanf`, `fscanf`, `sscanf`: mit `%s` Konvertierungsspezifikation.

[Angreifbarer Buffer Code](#)

Generated by Targeteam



Angreifbarer Buffer Code



```

void echo() {
    char buf[4]; /* sehr klein */
    gets(buf);
    puts(buf);
}

int main() {
    printf("Type a string:");
    echo();
    return 0;
}

```

unix> bufdemo

Type a string: **123**

123

unix> bufdemo

Type a string: **12345**

Segmentation Fault

Keller von main
Rückkehradresse

Information

