Script **generated by TTT**

Title: Grundlagen_Betriebssysteme (18.01.2016)

Date: Mon Jan 18 13:45:36 CET 2016

Duration: 87:16 min

Pages: 16

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

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

Multimedia Systems

Multimedia umfasst eine Vielzahl, heute populärer Applikationen

- Audio und Video Clips (z.B. MP3 und MPEG Dateien).
- Live Webcasts.

Mögliche Endgeräte für den Empfang von Multimedia Daten

- Desktop PCs oder mobile Endgeräte, wie PDAs, Smartphones.

Zustellung von Mediendaten

Eigenschaften von Multimedia Systemen

Generated by Targeteam

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

Sicherheit in Rechensystemen

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

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

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 Benutzername und sein privates Passwort.

Angreiferprogramm speichert Benutzername 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.

Beispiel: Virus

Ein ***Virus*** ist ein Programm, dessen Code an ein anderes Programm anfügt 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).

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

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

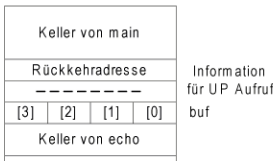
Type a string: ***123***

123

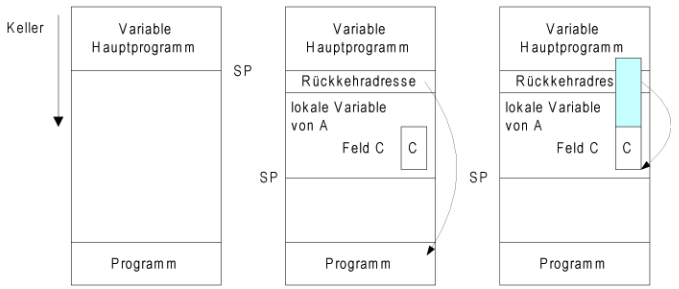
unix> bufdemo

Type a string: ***12345***

Segmentation Fault



Veränderung der Rücksprungadresse



Falls das attackierte Programm mit root-Berechtigung (setuid root in Unix) abläuft, läuft das aufgerufene Programm im Puffer auch mit root-Berechtigung.

Angreifer kann seiner aufrufenden Shell root-Berechtigung verleihen.

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 Rücksprungadresse

Gegenmaßnahmen

Unterscheidung

sichere Programmierung.

Maßnahmen zur Übersetzungszeit.

Maßnahmen zur Laufzeit.

Sicherheit in Rechensystemen

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

Anforderungen

Für einen Schutzmechanismus gelten die folgenden Anforderungen

alle Objekte eines Systems müssen eindeutig und fälschungssicher identifiziert werden.

externer Benutzer eines Systems muss eindeutig und fälschungssicher identifiziert werden ⇒ Authentifizierung.

Zugriff auf Objekte sollte nur über zugehörige Objektverwaltung geschehen.

Zugriff auf Objekte nur, wenn Zugreifer die nötige Rechte hat.

Rechte müssen fälschungssicher gespeichert werden; Weitergabe von Rechten darf nur kontrolliert erfolgen.

Prinzip der minimalen Rechte.

grundlegenden Schutzmechanismen sollen ohne großen Aufwand überprüft werden können.

Schutzmechanismen

Schutz von gespeicherter Information vor Diebstahl, unerwünschter Manipulation und Verletzung der Vertraulichkeit ist ein zentrales Anliegen in allen Mehrbenutzersystemen.

Anforderungen

Ebenen des Zugriffschutzes

Schutzmatrix

Authentifizierung

Schutzmechanismen

Schutz von gespeicherter Information vor Diebstahl, unerwünschter Manipulation und Verletzung der Vertraulichkeit ist ein zentrales Anliegen in allen Mehrbenutzersystemen.