Script **generated by TTT**

Title: Grundlagen_Betriebssysteme (20.01.2016)

Date: Wed Jan 20 13:18:04 CET 2016

Duration: 42:59 min

Pages: 9

Schutzmechanismen

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

Generated by Targeteam

Ebenen des Zugriffschutzes

Man unterscheidet die folgenden Ebenen des Zugriffsschutzes.

Maschinenschutz : Kontrolle des physischen Zugangs zum Rechensystem.

Zugangskontrolle : Kontrolle des logischen Zugangs zum Rechensystem, d.h. Ausführung von Aufträgen im Rechensystem.

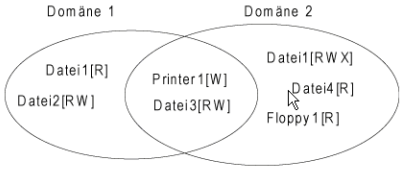
Berechtigungskontrolle : Kontrolle des Benutzerzugriffs auf einzelne Datenbestände und die Ausführung einzelner Dienste.

Systemschutz : Gewährleistung der Integrität der Schutzmechanismen.

Generated by Targeteam

Schutzdomänen

Definition: Eine **Schutzdomäne** ist eine Menge von (Objekt, Rechte) Paaren.



R = read, W = write, X = execute

Verknüpfung eines Prozesses mit einer Schutzdomäne.

zu jedem Zeitpunkt wird ein Prozess in einer Schutzdomäne ausgeführt.

Beispiel Unix: bei Ausführung eines Systemaufrufs wechselt der Prozess vom Benutzermodus in den Systemmodus ("kernel mode") ⇒ entspricht einem Wechsel der Schutzdomäne.

Das Paar (Prozess P, Schutzdomäne D) wird als ***Subjekt*** bezeichnet.

Der Zugriffswunsch eines Subjektes S auf ein Objekt o ist definiert als (D, o, a), wobei D die Schutzdomäne und a die Zugriffsart ist.

Matrix-Datenstruktur

Generated by Targeteam

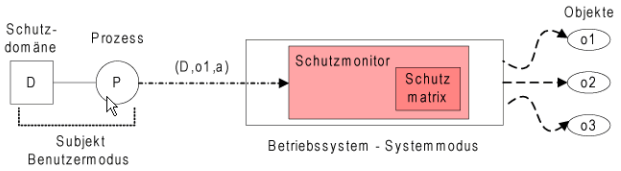
Matrix-Datenstruktur

Konzeptuell verwendet ein Betriebssystem eine Matrix-Datenstruktur, um die Zuordnung Objekt-Schutzdomäne zu verfolgen.

	Objekt					
Domäne	Datei1	Datei2	Datei3	Datei4	Printer1	Floppy 1
1	read	read write	read write		write	
2	read write execute		read write	read	write	read

Schutzmonitor

Jeder Zugriff (D, o, a) eines Subjektes S wird mit Hilfe eines Schutzmonitors überprüft.



der Schutzmonitor ist vertrauenswürdig.

Subjekte können in keinem Fall auf Objekte unter Umgehung des Schutzmonitors zugreifen.

neue Prozesse müssen sich gegenüber dem Schutzmonitor authentifizieren.

Schutzmatrix

Das Konzept der Schutzmatrix wurde von B. Lampson eingeführt. Es verknüpft Schutzdomänen mit den zu schützenden Objekten.

Schutzdomänen

Schutzmonitor

Schutzmatrix ist typischerweise sehr groß und dünn besetzt ⇒ eine direkte Implementierung ist deshalb nicht sinnvoll.

Zugriffskontrollliste

Capability-Liste

Zusammenfassung: Zugriffskontrolllisten und Capability-Listen haben in gewisser Weise komplementäre Eigenschaften

ACLs erlauben das selektive Zurücknehmen von Rechten.

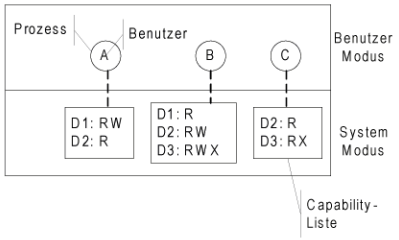
Capabilities können weitergegeben werden.

Capability-Liste

Capability-Listen ("Zugriffsausweislisten") realisieren die ***zeilenweise*** Speicherung der Schutzmatrix.

jeder Prozess besitzt eine Menge von Capabilities, die die erlaubten Zugriffe auf Objekte repräsentieren.

Element einer Capability-Liste besteht aus Paar (Objekt, Zugriffsarten).



Capabilities müssen geschützt werden, um Modifikationen durch den Prozess selbst zu verhindern. Alternativen sind

Speicherung im geschützten Bereich des Betriebssystems.

Capabilities sind zwar im Benutzermodus dem Prozess zugeordnet; sie sind jedoch verschlüsselt.

Capabilities können zeitlich begrenzt werden.

Schutzmatrix

Das Konzept der Schutzmatrix wurde von B. Lampson eingeführt. Es verknüpft Schutzdomänen mit den zu schützenden Objekten.

Schutzdomänen

Schutzmonitor

Schutzmatrix ist typischerweise sehr groß und dünn besetzt ⇒ eine direkte Implementierung ist deshalb nicht sinnvoll.

Zugriffskontrollliste

Capability-Liste

Zusammenfassung: Zugriffskontrolllisten und Capability-Listen haben in gewisser Weise komplementäre Eigenschaften

ACLs erlauben das selektive Zurücknehmen von Rechten.

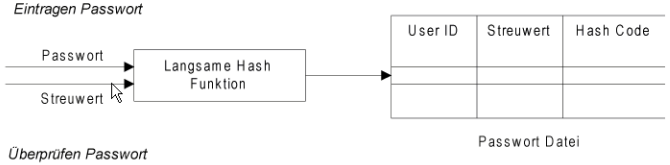
Capabilities können weitergegeben werden.

Authentifizierung

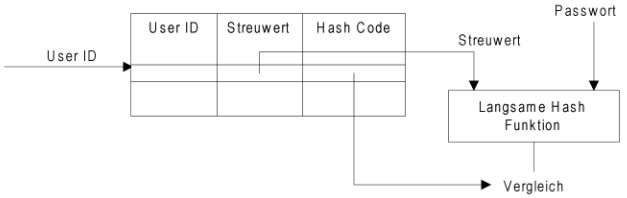
Authentifizierung eines Nutzers erfolgt meist über Login-Name und dem zugehörigen Passwort.

Generierung eines Hash Code aus dem Passwort und einem Streuwert fester Länge.

Eintragen Passwort



Überprüfen Passwort



Ziele des Streuwerts

Duplikate von Passwörter sollen in der Passwort Datei nicht erkennbar sein.

Erhöht den Aufwand für offline Attacken auf die Passwort Datei.

nicht erkennbar, ob eine Person dasselbe Passwort auf 2 oder mehreren Systemen nutzt.