

Zugriffskontrolle: Aufgaben und Fragen zur Lernkontrolle

1. Grundwissen

12.06.08

- Erläutern Sie das Grundmodell für die Zugangs- und Zugriffskontrolle (**Bild 1.1**) und erklären Sie die damit im Zusammenhang stehenden Begriffe **Subjekt** und **Objekt**!
- Erläutern Sie das Modell der Zugriffsmatrix. Leiten Sie daraus die Begriffe Zugriffskontrollliste und Berechtigungsliste ab.
- Erläutern Sie mit Hilfe von Beispielen die Begriffe

- Sicherheitsebene
- Sicherheitslabel, Ermächtigung und Sicherheitsklassifizierung.
- Dominanzrelation

- Erläutern Sie anschaulich die Sicherheitspolitik des Bell-LaPadula-Modells.

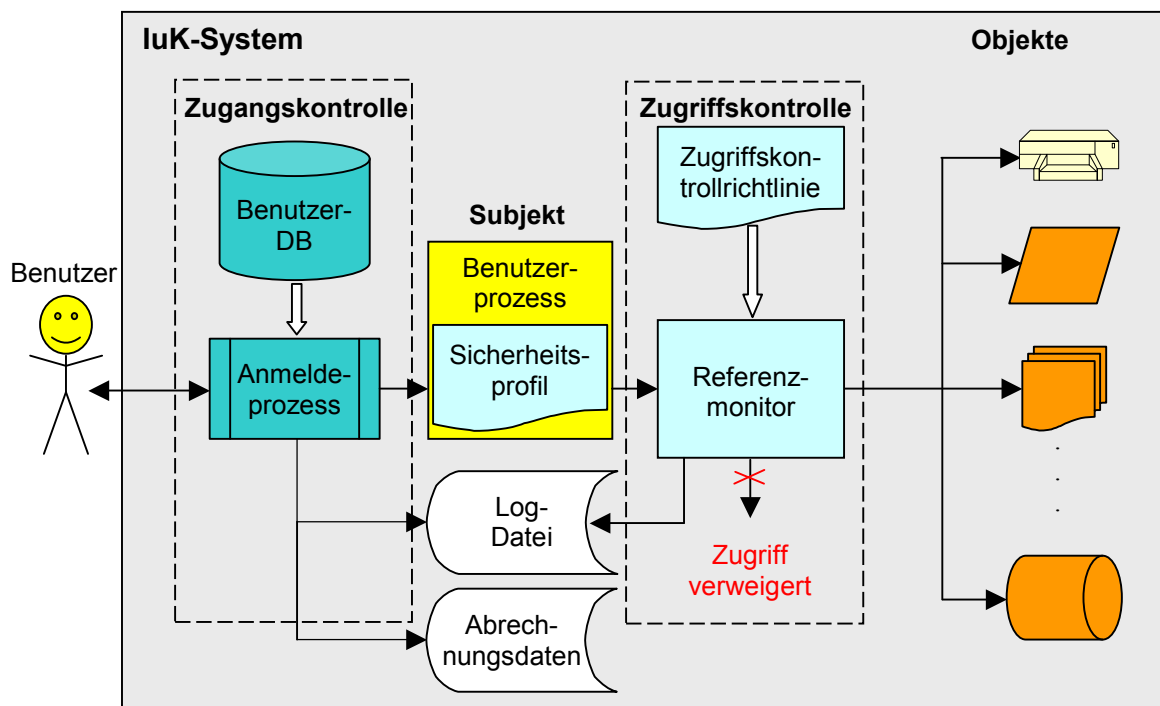


Bild 1.1 Zur Positionierung von Zugangs- und Zugriffskontrolle in luK-Systemen

2. Informationsflussmodellierung (*Lattice*)06.01.06

leer

3. Systembestimmte Zugriffskontrolle

26.06.08

In einer Hochschule sei der Zugriff auf elektronisch gespeicherte Informationen nach dem Prinzip „Systembestimmte Zugriffskontrolle“ geregelt. Hierfür sind definiert:

Sicherheitsattribute: $\mathbf{L} = \{\text{öffentlich}, \text{sensibel}, \text{geschützt}\}$ mit $\text{öffentlich} < \text{sensibel} < \text{geschützt}$ und
 Sicherheitskategorien: $\mathbf{C} = \{\text{Professor}, \text{Student}, \text{Verwaltung}\}$

a) Ergänzen Sie die folgende Tabelle, indem Sie eintragen, ob die jeweilige Dominanz-Relation wahr oder falsch ist.

Dominanzrelation	wahr/falsch?
$(\text{öffentlich}, \{\text{Professor}, \text{Student}\}) \leq (\text{geschützt}, \{\text{Professor}, \text{Student}\})$	
$(\text{öffentlich}, \{\text{Professor}, \text{Student}\}) \leq (\text{sensibel}, \{\text{Student}, \text{Verwaltung}\})$	
$(\text{öffentlich}, \{\text{Professor}, \text{Student}\}) \leq (\text{öffentlich}, \{\text{Professor}, \text{Student}, \text{Verwaltung}\})$	
$(\text{sensibel}, \{\emptyset\}) \leq (\text{öffentlich}, \{\text{Professor}, \text{Student}, \text{Verwaltung}\})$	
$(\text{geschützt}, \{\text{Verwaltung}\}) \leq (\text{geschützt}, \{\text{Professor}, \text{Verwaltung}\})$	
$(\text{geschützt}, \{\text{Verwaltung}\}) \leq (\text{geschützt}, \{\text{Student}\})$	

Es sei nun angenommen, dass der Referenzmonitor des Zugriffskontrollsystem das Informationsfluss-Modell von BELL und LAPADULA durchsetzt. Für Subjekte der Sicherheitskategorien Verwaltung ($\sim s1$) bzw. Student ($\sim s2$) gelten die Ermächtigungen:

Verwaltung: $sl(s1) = (\text{geschützt}, \{\text{Verwaltung}\})$
 Student: $sl(s2) = (\text{sensibel}, \{\text{Student}\})$

Für die Objekte $o1 \dots o4$ gelten die Sicherheitsklassifikationen:

$o1$: $sl(o1) = (\text{öffentlich}, \{\emptyset\})$
 $o2$: $sl(o2) = (\text{sensibel}, \{\text{Student}\})$
 $o3$: $sl(o3) = (\text{sensibel}, \{\text{Verwaltung}\})$
 $o4$: $sl(o4) = (\text{geschützt}, \{\text{Verwaltung}\})$.

Die folgende Zugriffskontrollmatrix regelt die Zugriffsberechtigungen der Subjekte auf die Objekte.

	Objekt: o1	Objekt: o2	Objekt: o3	Objekt: o4
Verwaltung: s1	read-write execute		read-write	read-only append
Student: s2	read-only execute	read-write	read-only	
...				

Das Diagramm in **Bild 3.1** zeigt die für die Subjekte vorgesehenen Zugriffsoperationen.

b) Prüfen Sie für jede der zehn Zugriffsoperationen deren Konformität mit den Regeln des Sicherheitsmodells von BELL und LAPADULA und notieren Sie mit Begründung, welche Operationen der Referenzmonitor zulassen darf und welche er unterbinden muss!

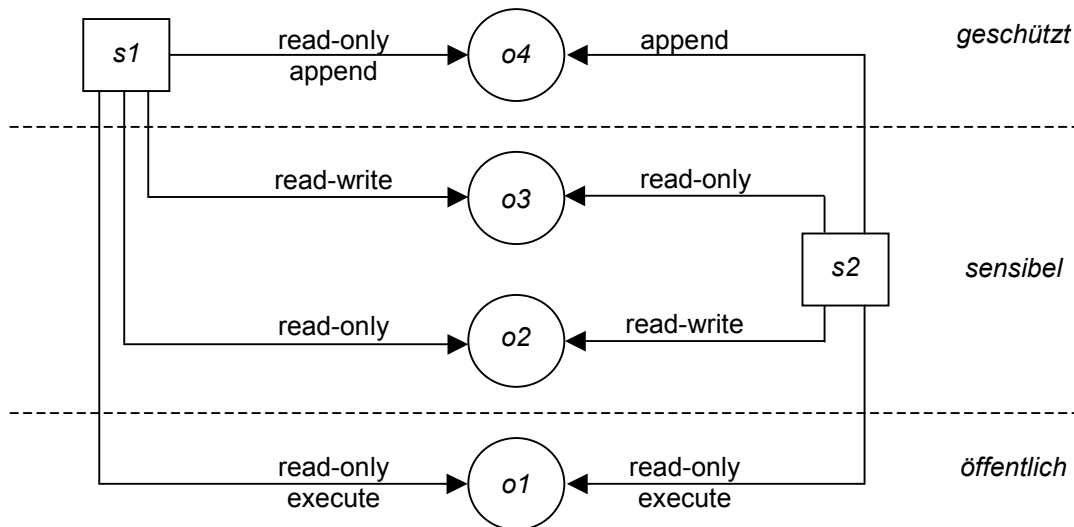
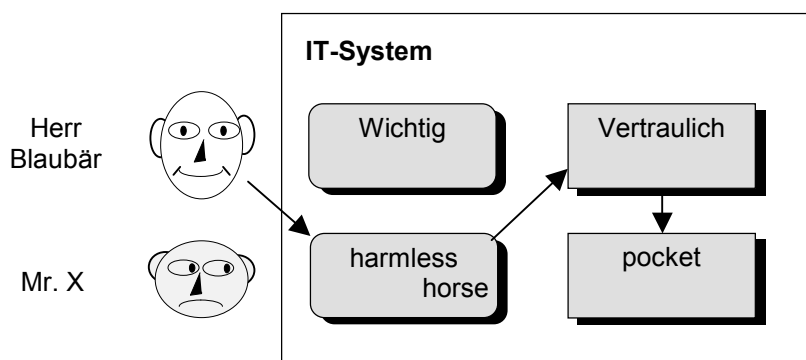


Bild 3.1: Zugriffsoperationen der Subjekte s1 und s2 auf die Objekte o1 ... o4.

4. Benutzerbestimmte versus Systembestimmte Zugriffskontrolle

06.01.06

In dieser Aufgabe sollen Maßnahmen gegen Angriffe auf die Vertraulichkeit und die Integrität von Daten untersucht werden. Hierzu wird zunächst das in **Bild 4.1** skizzierte Szenario betrachtet. Dort sind die Zugriffsrechte auf die Programme 'Wichtig' und 'harmless' sowie die Dateien 'Vertraulich' und 'pocket' benutzerdefiniert über eine Zugriffskontrollmatrix geregelt. Der als Gast eingeloggte Angreifer Mr. X hat es auf eine Kopie der Datei 'Vertraulich' abgesehen und benutzt hierfür das in 'harmless' versteckte Trojanische Pferd 'horse'. Wird das scheinbar harmlose Programm 'harmless' von Herrn Blaubär ausgeführt, so kopiert 'horse' den Inhalt der Datei 'Vertraulich' in die Datei 'pocket' und Mr. X hat sein Ziel erreicht.



Zugriffskontromatrix

	Wichtig	Vertraulich	harmless	pocket
Blaubär	r w x	r w	x	w
Mr. X			r w x	r w

Bild 4.1: Angriff auf die Vertraulichkeit einer Datei mit Hilfe eines Trojanischen Pferdes

- a) Der Erfolg des Angriffs auf die Vertraulichkeit der Daten kann durch Verwendung eines Sicherheitssystems mit den Sicherheitsebenen "öffentlich" und "geheim" für die Objekte und entsprechenden Ermächtigungen für die Subjekte nach der Methode von BELL und LAPADULA verhindert werden (**Bild 4.2**).

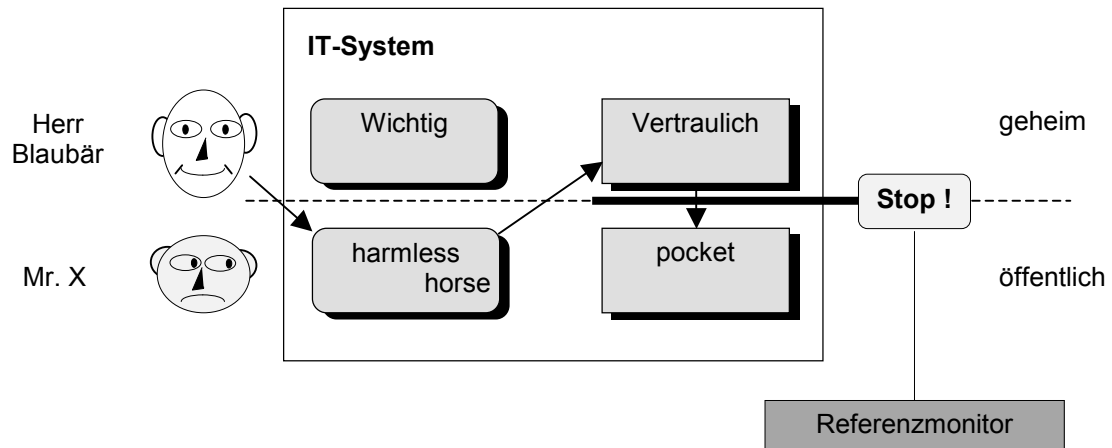


Bild 4.2: Zweischichtiges Sicherheitssystem mit Referenzmonitor

Wie sind die Objekte einzustufen und welche Ermächtigungen sind den Subjekten zuzuordnen?
Welche Regeln muss der Sicherheitsmonitor durchsetzen?

- b) Ist das unter a) entwickelte Verfahren auch gegen Angriffe auf die Datenintegrität - z.B. durch Viren - erfolgreich? Wenn nein, was müsste an den BELL-LAPADULA-Regeln geändert werden? Ist jetzt noch die Wahrung von Vertraulichkeit gewährleistet?