8. Datensicherheit

- Anforderungen an ein DBMS
  - Identifikation und Authentisieren von Benutzern
  - Autorisierung und Zugriffskontrolle
  - Aufzeichnung von sicherheitsrelevanten Aktionen eines Benutzers
- typische Schwachstellen der Systeme
  - Mißbrauch von Autorität (Diebstahl von Daten)
  - logisches Schließen und Aggregation
  - Maskierung (Datenzugriff von nicht-autorisierte Benutzer)
  - Umgehung der Zugriffskontrolle (Ausnutzung von Sicherheitslücken)
  - Durchstöbern von zugänglichen Daten (z. B. Paßwort-Dateien)
  - Trojanische Pferde (Simulation eines Programms)
  - versteckte Kanäle (Lesen der Datenbank über das Dateisystem)
- Sicherheitsstrategien
  - DAC: Discretionary Access Control
  - MAC: Mandatory Access Control

8.1 9.1 DAC

- Menge von Objekten
  - passive Komponenten, die Informationen enthalten, z. B. Relationen.
- Menge von Subjekten
  - aktive Komponenten, die Information weitergeben, z. B. Benutzer, Transaktion
- Menge von Zugriffstypen
  - z. B. insert, delete, update, select … from … where
- Menge von Prädikate
  - definieren für ein Subjekt und ein Objekt ein Zugriffsfenster.

Ein Zugriffsregel ist ein 4-Tupel (o, s, t, p):
Subjekt s darf Operation auf Objekte vom Typ o anwenden, die Prädikat p erfüllen.

- Weitergabe von Rechten
  - Subjekt s darf das Recht (o,t,p) an andere Subjekte weitergeben.

Zugriffskontrolle in SQL

- basiert auf einer Realisierung der DAC-Sicherheitsstrategie
- Sichtenkonzept wird benutzt, um Prädikate auf Objekten anzugeben.

Identifikation und Authentisieren

- über Paßwortabfrage geregelt
- in ORACLE sollte es vermieden werden,
  - Paßwörter in eSQL-Programmen explizit anzugeben
  - sqlplus mit dem Paßwort in der Kommandozeile aufzurufen

Autorisierung und Zugriffskontrolle

- Erteilen eines Zugriffsrechts:

  grant T (A_{i1}, A_{i2}, …, A_{in}) on R to S
  - A_{i1}, …, A_{in} sind Attribute der Relation R bzw. der Sicht R.
  - T ist eine der Operationen delete, insert, select, update
    auf Relationen zusätzlich: alter, references

- Weitergabe von erteilten Zugriffsrechte
  - grant-Befehl + with grant option
- Beispiel:
  grant select on Ware to schneider with grant option

Zurücknehmen der Rechte

- revoke T (A_{i1},…,A_{in}) on R from S
- revoke-Befehl + cascade
  - Rechte werden zusätzlich von den Subjekten entzogen, die diese indirekt von dem Subjekt S bezogen haben.

Auditing

- Aufzeichnen von kritischen Operationen
  z. B. audit insert, delete, update on Ware

Implizite Autorisierung

- Probleme bei einer expliziten Autorisierung
  - Regelmengen können sehr groß und unübersichtlich sein
  - ineffiziente Überprüfung, ob Zugriffsrechte vorliegen
- Einordnung von Subjekten, Objekten und Operationen in eine Hierarchie

Implizite Autorisierung von Subjekten durch Rollenhierarchien

- Benutzer können in verschiedenen Rollen auftreten
- in ORACLE:
  - Erzeugen neuer Rollen
  - Rechtevergabe an Rollen
  - Benutzer können in mehreren Rollen auftreten

Implizite Autorisierung von Objekten

- Objekt-Hierarchie:
  Datenbank -- Schema -- Relationen -- Tupel -- Attribut

8.2 MAC

- entsprang aus den Sicherheitsbedürfnissen von militärischen Einrichtungen
  - Mißbrauch der Weitergabe von Information durch autorisierte Benutzer
- Objekte und Subjekte sind Stufen einer Sicherheitshierarchie zugeteilt:
  - clear(s): Sicherheitsstufe eines Subjekts
  - class(o): Sicherheitsstufe eines Objekts
- Zugriffsregeln
  - Subjekt s darf Objekt o nur dann lesen, wenn clear(s) ≥ class(o).
  - Objekt o muß mit mindestens der Einstufung des Subjekts geschrieben werden, d. h. es gilt dann clear(s) ≤ class(o).
- Probleme:
  - Zusammenarbeit von Subjekten mit verschiedenen clear-Werten ist schwierig.
  - Objekte sehr leicht in oberen Stufen der Hierarchie landen, ohne daß diese dort wirklich hingehören.

8.3 Multilevel-Datenbanken

- Problem für DAC und MAC:
  - Benutzer können mitbekommen, auf welche Daten Sie keine Zugriffsrechte haben.
- Beispiel:

TC	Name	NC	Adresse	AC	Konto	KC
g	Müller	g	Marburg	g	200,-	sg
sg	Nobody	sg	Bahamas	sg	1000000,-	sg

  - jedem Attribut ist noch ein Sicherheitsstufe zugeordnet
  - Attribut TC bezeichnet die Sicherheitsstufe des Datensatzes
  - Benutzer, die auf geheime (g) Information zugreifen erhalten folgende Relation

TC	Name	NC	Adresse	AC	Konto	KC
g	Müller	g	Marburg	g	---	g

Was passiert, wenn jetzt “Nobody” eingefügt wird?

Polyinstanzierung

- erlaubt gleichzeitig mehrere Zustände einer Relation, wobei höchstens ein Zustand in einer Sicherheitsstufe vorliegt.
- Schema einer Multilevel-Relation: $\{A_1, C_1, A_2, C_2, \ldots, A_n, C_n, TC\}$
  - A_i sind die gewöhnlichen Attribute der Relation
  - C_i gibt die Sicherheitsstufe des Attributs A_i
  - TC bezeichnet die Sicherheitsstufe des gesamten Datensatzes
- Welche Integritätsbedingungen gelten in Multilevel-Relationen? (siehe Kemper/Eickler)
  - Entity-Integrität
    (i) Schlüsselattribute dürfen keinen Nullwert enthalten
    (ii) Sicherheitsstufe aller Schlüsselattribute muß identisch sein
    (iii) Nichtschlüssel-Attribute müssen mindestens die Sicherheitsstufe des Schlüssels besitzen.
  - Null-Integrität
    Nullwerte besitzen die gleiche Sicherheitssufe wie der Schlüssel des Datensatzes.
  - Interinstanzintegrität
    Regelt die erlaubten Zustände der verschiedenen Instanzen.
  - Polyinstanziierungsintegrität:
    folgende funktionale Abhängigkeiten gelten: $\{K, C_K, C_i\} \rightarrow A_i$