Rechtevergabe in Datenbanksystemen

Zugriffsrechte

`(AutorisierungsID, DB-Ausschnitt, Operation)`

- AutorisierungsID ist interne Kennung eines “Datenbankbenutzers”
- Datenbank-Ausschnitte: Relationen und Sichten
- DB-Operationen: Lesens, Einfügen, Ändern, Löschen

Rechtevergabe in SQL II

Erläuterungen:

- In `<Rechte>`-Liste: **all** bzw. Langform **all privileges** oder Liste aus **select**, **insert**, **update**, **delete**
- Hinter **on**: Relationen- oder Sichtname
- Hinter **to**: Autorisierungsidentifikatoren (auch **public**, **group**)
- spezielles Recht: Recht auf die Weitergabe von Rechten (**with grant option**)

Datenschutz und Zugriffskontrolle

- Rechtevergabe in Datenbanksystemen
- Autorisierung und Authentifikation
- Statistische Datenbanken

Rechtevergabe in SQL

grant `<Rechte>`
on `<Tabelle>`
to `<BenutzerListe>`
[**with grant option**]

Zurücknahme von Rechten

revoke `<Rechte>`
on `<Tabelle>`
from `<BenutzerListe>`
[**restrict** | **cascade**]

- **restrict**: Falls Recht bereits an Dritte weitergegeben: Abbruch von **revoke**
- **cascade**: Rücknahme des Rechts mittels **revoke** an alle Benutzer propagiert, die es von diesem Benutzer mit **grant** erhalten haben

Statistische Datenbanken

- Einzeleinträge unterliegen Datenschutz, statistische Informationen (aggregierte Werte)
- Zugriffsüberwachung muß Zugriff auf Daten über Einzeleinträge verhindern!
- Bsp.: Benutzer X darf Daten über Kontoinhaber sowie statistische Daten wie Kontosummen sehen

Autorisierung für public

create view `MeineAufträge` **as**
select *
from `AUFTRAG`
where `KName =` **user**;
grant select, **insert**
on `MeineAufträge`
to public;

“Jeder Benutzer kann seine Aufträge sehen und neue Aufträge einfügen (aber nicht löschen!).”

Authentifikation und Autorisierung

Nachweis der Identität von Benutzern:

- *Was der Benutzer weiß:* Paßwörter, PINs, Geburtsdatum der Mutter, ...
- *Was der Benutzer besitzt:* etwa Scheckkarte oder Schlüssel
- *Was der Benutzer selbst hat:* Fingerabdrücke, Stimme, ...

Statistische Datenbanken II

Person X ist selbst Kontoinhaber, will Kontostand von Y herausfinden

X weiß, daß Y nicht in Magdeburg lebt, hat abgefragt, daß in Magdeburg mehr als n Kontoinhaber leben, daher erlaubt:

```
select sum(Kontostand)
from Konto
where Name = :X or Ort = 'Magdeburg'
```

```
select sum(Kontostand)
from Konto
where Name = :Y or Ort = 'Magdeburg'
```


Statistische Datenbanken: Beispiel

```
select count (*) from Konto where Ort = 'Teterow'
```

nur ein Treffer $\rightsquigarrow$ dann Kontoinhaber bestimmen:

```
select Name from Konto where Ort = 'Teterow'
```

erlaubte Anfrage liefert Einzelergebnis:

```
select sum(Kontostand) from Konto where Ort = 'Teterow'
```

Regel: in Aggregation müssen mindestens n Tupel eingehen

Statistische Datenbanken III

Statistische Anfragen sollten nicht erlaubt werden, die paarweise einen Durchschnitt von mehr als m vorgegebenen Tupeln betreffen.

- Ergebnisgröße n
- Größe der Überlappung der Ergebnismengen m
- *Sind nur Ergebnisse von Aggregatfunktionen erlaubt, dann benötigt eine Person $1 + (n-2)/m$ Anfragen, um einen einzelnen Attributwert zu ermitteln.*