Database Security

Thursday, 09 October 2025 20:23

Deretan kasus kebocoran data pribadi pengguna akhir-akhir ini merupakan salah satu contoh dari jenis ancaman...

- ○ Loss of integrity
- ○ Loss of availability
- ● Loss of confidentiality
- ○ Lost in translation

Berikut merupakan cara-cara yang dapat menjaga keamanan dari basis data, kecuali...

- ○ Inference Control
- ○ Access Control
- ● Reinforce Doors
- ○ Encryption

Melakukan pencegahan pengambilan data individual dapat dilakukan dengan menerapkan...

- ● Inference Control
- ○ Access Control
- ○ Flow Control
- ○ Encryption

Log basis data yang mencatat semua operasi yang dilakukan pada basis data sering disebut....

- ○ Inference Control
- ○ Access Control
- ○ Flow Control
- ● Audit Trail

Penerapan covert channels merupakan salah satu contoh dari...

- ○ Inference Control
- ○ Access Control
- ● Flow Control
- ○ Encryption

Seorang DBA dapat melakukan pemberian akses baik pada level akun maupun relasi.

- ● true
- ○ false

Pada star property subject S tidak diperbolehkan untuk menulis pada objek O kecuali class(S) <= class(O).

- ● true
- ○ false

Pada public-key encryption digunakan kunci yang sama untuk proses encryption dan decyrption

- ○ true
- ● false

Basisdata sebuah perusahaan mengandung relasi-relasi berikut:

Pegawai = (IDPegawai, Nama, TanggalLahir, Gaji, IDManajer, IDJabatan)
Departemen = (IDDepartemen, NamaDepartemen, IDLokasi, Anggaran)
Lokasi = (IDLokasi, Kota, Provinsi, Negara)
Jabatan = (IDJabatan, NamaJabatan, GajiMin, GajiMax, IDDepartemen)
FK: Pegawai(IDManajer) → Pegawai(IDPegawai)
Pegawai(IDJabatan) → Jabatan(IDJabatan)
Departemen(IDLokasi) → Lokasi(IDLokasi)
Jabatan(IDDepartemen) → Departemen(IDDepartemen)

Diberikan juga user-user (bisa user perorangan maupun user aplikasi) basis data dan jabatan atau tugas pokoknya sebagai berikut:

User	Jabatan / Deskripsi Fungsi
Devan	Manajer untuk pegawai dengan IDPegawai = {101,102,103,104,105}. Sedangkan Devan memiliki IDPegawai 120
Jimmy	Staff HRD Provinsi Jawa Barat
Karin	Direktur Utama
Sistem Informasi Pegawai (SIP)	Menampilkan data-data pegawai yang ada di perusahaan

Dengan menggunakan akses kontrol DAC, buatlah model akses antara semua user dengan relasi atau view yang ada di basis data tsb. Kalian bisa membuat view jika memang dibutuhkan (sertakan juga script untuk membuat viewnya). Tuliskan asumsi jika diperlukan.

Di sebuah perusahaan, security classes dibagi menjadi 4 level : Top Secret (TS) >= Secret (S) >= Confidential (C) >= Unclassified
Diketahui table karyawan dengan menggunakan mandatory access control sebagai berikut:

IDKaryawan	Nama	TanggalLahir	NilaiKinerja
1234567891 S	Jonathan Christie U	15 September 1997 C	Sangat Baik S
1235674120 S	Anthony Sinisuka C	20 Oktober 1996 C	Baik S

a) Gambarkan data yang akan dilihat oleh Harry sebagai karyawan yang memiliki klasifikasi Secret
b) Gambarkan data yang akan dilihat oleh Edward sebagai karyawan yang memiliki klasifikasi Unclassified
c) Apakah Harry bisa menulis data tanggal lahir dengan klasifikasi C?

Basisdata sebuah sekolah mengandung relasi-relasi berikut:

Instruktur = (IDInstruktur, Nama, TanggalLahir, Alamat, JenisKelamin, NoTelp, Email)
Pelajaran = (IDPelajaran, NamaPelajaran, Beban)
Pengajaran = (IDInstruktur, IDPelajaran, Semester, Tahun, Ruang, JamPelajaran)
FK: Pengajaran(IDInstruktur) → Instruktur(IDInstruktur)
Pengajaran(IDPelajaran) → Pelajaran(IDPelajaran)

Tuliskan perintah SQL untuk memberikan/mencabut otorisasi kepada *user* atau *role* berikut ini. Buat *role* dan *view* jika diperlukan (tuliskan pula perintahnya).
a) *User* A dapat membaca data Instruktur, Pelajaran, dan Pengajaran, tetapi tidak dapat melakukan perubahan apa pun terhadap data tersebut.
b) Seorang instruktur kepala berhak untuk menambah, mengubah, dan menghapus data Instruktur dan meneruskan *privileges* tersebut kepada *user* lain. *User* B dan C adalah instruktur kepala.
c) User D hanya dapat membaca data Pengajaran untuk IDInstruktur = 12345 dan pada Tahun = 2014.
d) Terkait soal butir a, mencabut hak user A untuk membaca data Pengajaran.
e) Terkait soal butir b, mencabut semua hak *user* B atas data Instruktur, termasuk mencabut hak semua user lain yang pernah diberikan hak yang sama oleh *user* B.

Model dibuat dengan prinsip *least privilege*, setiap pengguna hanya diberi hak akses minimum yang diperlukan untuk menjalankan fungsinya. Berikut merupakan asumsi yang digunakan:

1. Semua pengguna yang disebutkan hanya membutuhkan akses untuk membaca data (SELECT)
2. Sebagai Direktur Utama, Karin memiliki wewenang untuk melihat semua data di semua tabel untuk keperluan pengawasan dan pengambilan keputusan
3. Sebagai Manajer, Devan hanya dapat melihat data lengkap dari pegawai yang berada di bawah manajemennya secara langsung
4. Sebagai Staff HRD Provinsi Jawa Barat, Jimmy hanya dapat melihat data pegawai yang bekerja di lokasi provinsi tersebut, dan karena perannya di HRD, Jimmy diizinkan melihat informasi gaji
5. Aplikasi Sistem Informasi Pegawai berfungsi untuk menampilkan data umum pegawai. Untuk melindungi privasi, sistem ini tidak diizinkan untuk menampilkan kolom gaji

Pembuatan view:

1. View untuk Manajer (Devan) → menampilkan data pegawai dengan IDManajer 120

```
CREATE VIEW pegawai_dengan_manajer_devan AS
SELECT *
FROM Pegawai
WHERE IDManajer = 120;
```

2. View untuk Staff HRD (Jimmy)

```
CREATE VIEW pegawai_jawa_barat AS
SELECT *
FROM Pegawai p
JOIN Jabatan j ON p.IDJabatan = j.IDJabatan
JOIN Departemen d ON j.IDDepartemen = d.IDDepartemen
JOIN Lokasi l ON d.IDLokasi = l.IDLokasi
WHERE l.Provinsi = 'Jawa Barat';
```

3. View untuk SIP

```
CREATE VIEW pegawai AS
SELECT IDPegawai, Nama, TanggalLahir, IDManajer, IDJabatan
FROM Pegawai;
```

Pemberian hak akses (model akses kontrol):

1. Hak akses untuk Manajer (Devan)

```
GRANT SELECT ON pegawai_dengan_manajer_devan TO “Devan”;
```

2. Hak akses untuk Staff HRD (Jimmy)

```
GRANT SELECT ON pegawai_jawa_barat TO “Jimmy”;
```

3. Hak akses untuk SIP

```
GRANT SELECT ON pegawai TO “Sistem Informasi Pegawai”;
```

4. Hak akses untuk Direktur Utama (Karin)

```
GRANT SELECT ON Pegawai TO “Karin”;
GRANT SELECT ON Departemen TO “Karin”;
GRANT SELECT ON Lokasi TO “Karin”;
GRANT SELECT ON Jabatan TO “Karin”;
```

a) Gambarkan data yang akan dilihat oleh Harry sebagai karyawan yang memiliki klasifikasi Secret

IDKaryawan	Nama	TanggalLahir	NilaiKinerja
1234567891	Jonathan Christie	15 September 1997	Sangat Baik
1235674120	Anthony Sinisuka	20 Oktober 1996	Baik

b) Gambarkan data yang akan dilihat oleh Edward sebagai karyawan yang memiliki klasifikasi Unclassified

IDKaryawan	Nama	TanggalLahir	NilaiKinerja
NULL	Jonathan Christie	NULL	NULL
NULL	NULL	NULL	NULL

c) Apakah Harry bisa menulis data tanggal lahir dengan klasifikasi C?
Tidak bisa, karena Harry memiliki klasifikasi Secret, sedangkan klasifikasi objek data TanggalLahir adalah Confidential, dan S <= C. Aturan menulis data (*star property*) harus memenuhi syarat class(Harry) >= class(Data) apabila ingin menulis data.

a) *User* A dapat membaca data Instruktur, Pelajaran, dan Pengajaran, tetapi tidak dapat melakukan perubahan apa pun terhadap data tersebut

```
GRANT SELECT ON Instruktur TO “A”;
GRANT SELECT ON Pelajaran TO “A”;
GRANT SELECT ON Pengajaran TO “A”;
```

b) Seorang instruktur kepala berhak untuk menambah, mengubah, dan menghapus data Instruktur dan meneruskan *privileges* tersebut kepada *user* lain. *User* B dan C adalah instruktur kepala

```
// bikin role instruktur_kepala
CREATE ROLE instruktur_kepala

// transfer privilege
GRANT INSERT, UPDATE, DELETE ON Instruktur TO instruktur_kepala WITH
GRANT OPTION;

GRANT instruktur_kepala TO “B”, “C”;
```

c) *User* D hanya dapat membaca data Pengajaran untuk IDInstruktur = 12345 dan pada Tahun = 2014

```
CREATE VIEW pengajaran_d AS
SELECT *
FROM Pengajaran
WHERE IDInstruktur = ‘12345’ AND Tahun = 2014;

GRANT SELECT ON pengajaran_d TO “D”;
```

d) Terkait soal butir a, mencabut hak *user* A untuk membaca data Pengajaran

```
REVOKE SELECT ON Pengajaran FROM “A”;
```

e) Terkait soal butir b, mencabut semua hak *user* B atas data Instruktur, termasuk mencabut hak semua *user* lain yang pernah diberikan hak yang sama oleh *user* B

```
REVOKE INSERT, UPDATE, DELETE ON Instruktur FROM “B” CASCADE;
```