ORACLE LABEL SECURITY
PADA ORACLE DATABASE 10g

Kusnawi, S.Kom

Abstrak

Oracle Label Security memungkinkan kontrol akses mencapai baris yang spesifik dari database sehingga user dapat mengakses ke data yang perlu saja. User dengan berbagai level privilege dapat memiliki hak untuk melihat atau mengubah baris data yang dilabeli.

I. Pendahuluan

A. Keamanan Database

Keperluan keamanan database timbul dari kebutuhan untuk melindungi data. Pertama, dari kehilangan dan kerusakan data. Kedua, adanya pihak yang tidak diijinkan hendak mengakses atau mengubah data. Permasalahan lainnya mencakup perlindungan data dari *delay* yang berlebihan dalam mengakses atau menggunakan data, atau mengatasi gangguan *denial of service*.

Kontrol akses terhadap terhadap informasi yang sensitif merupakan perhatian terutama oleh manajer, pekerja di bidang informasi, *application developer*, dan DBA. Kontrol akses selektif berdasarkan authorisasi keamanan dari level user dapat menjamin kerahasiaan tanpa batasan yang terlalu luas. Level dari kontrol akses ini menjamin rahasia informasi sensitif yang tidak akan tersedia untuk orang yang tidak diberi ijin (authorisasi) bahkan terhadap user umum yang memiliki akses terhadap informasi yang dibutuhkan, kadang-kadang pada tabel yang sama.

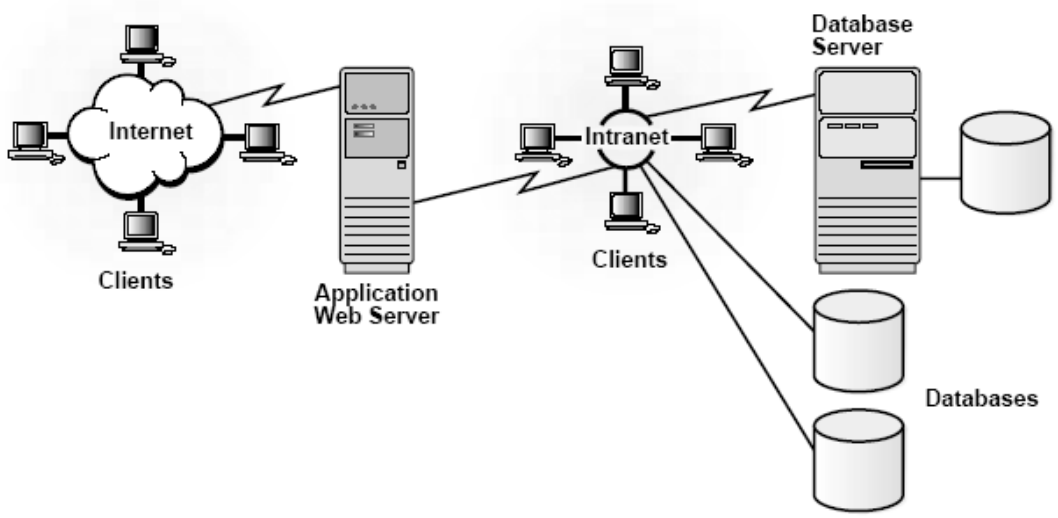
B. Mitos pada Keamanan Data

Secara umum desain solusi kemanan pada bidang keamanan data tidak efektif karena prinsip yang salah. Berikut ini adalah beberapa mitos keamanan yang sering digunakan :

- *Hackers* menyebabkan sebagian besar pembobolan keamanan.
  Pada kenyataannya 80% data hilang karena orang dalam.
- Enkripsi dapat mengamankan data.
  Kenyataannya enkripsi hanyalah salah satu pendekatan untuk mengamankan data. Keamanan juga mensyaratkan kontrol akses integritas data, ketersediaan sistem, dan audit.
- *Firewall* dapat mengamankan data
  Kenyataannya 40% Internet *break-ins* terjadi karena digunakannya *firewall*.

C. Ruang Lingkup Keamanan Data

Keamanan pada komputer mencakup perlindungan data yang terkomputerisasi dan proses modifikasi, perusakan, atau delay yang tidak diijinkan. Pada masa internet, ancaman terhadap data meningkat secara eksponensial. Gb.1 dibawah ini menunjukkan lingkungan komputasi kompleks yang harus tercakup dalam perencanaan keamanan data.



Gb.1 Lingkungan dari Kebutuhan Keamanan Data
(Sumber : http://download-west.oracle.com/)

Staff keamanan, administrator, dan programmer aplikasi harus melindungi database dan server dimana database berada. Mereka harus mengatur dan melindungi hak user pada database internal, dan menjamin privasi *electronic commerce* sebagaimana pelanggan yang mengakses database tersebut.

D. Aspek Keamanan Data

Dalam mengamankan data, standard yang harus dipenuhi ialah :

1. Confidentiality

Confidentiality berarti sistem mengijinkan user hanya untuk melihat data yang diperbolehkan. Contoh aspek yang tercakup didalamnya ialah Autentikasi user dan kontrol akses sampai ke tingkat terkecil (*granule*), yaitu kontrol akses dapat dibedakan untuk tabel, view, baris, dan kolom tertentu dari database.

2. Integritas

Integritas data berarti data diproteksi dari penghapusan dan kerusakan ketika berada dalam database dan ketika ditransmisikan pada jaringan, misalnya Pengaturan hak kontrol akses sehingga hanya user tertentu yang diijinkan mengubah data.

3 Availability

Sistem yang aman mampu menyediakan data ke user yang diijinkan tanpa *delay*. Serangan *denial of service* berusaha untuk menahan user untuk mengakses dan menggunakan sistem ketika dibutuhkan. Misalnya seorang administrator harus memilik cara yang memadai untuk mengatur populasi user.

II. Oracle Label Security

A. Konsep Oracle Label Security

Oracle Label Security (OLS) memungkinkan administrator untuk mengubah aturan akses kontrol berdasarkan label ketika kontrol akses standard tidak memadai. OLS menghubungkan akses terhadap baris pada tabel berdasarkan label yang terdapat didalam baris. Suatu label berhubungan dengan setiap *session* database, dan OLS memberi hak terhadap session tersebut. Secara ringkas, berikut ini dijelaskan bagaimana OLS bekerja :

1. Dibuat aturan keamanan untuk mengidentifikasi bagaimana data harus diamankan dengan memberi spesifikasi komponen keamanan.
2. User label mendefinisikan aturan keamanan tingkat baris apa yang mungkin untuk setiap user.
3. Pada setiap tabel yang membutuhkan keamanan tingkat baris, ditambahkan kolom khusus yang disebut kolom label.

4. Selama akses data, suatu proses yang disebut *access mediation* menentukan ijin yang dibutuhkan untuk mengakses baris, dan tindakan apa yang dapat dilakukan ketika baris itu diakses.

Untuk memenuhi kebutuhan kontrol akses tersebut dilakukan pendekatan sebagai berikut

1. Discretionary Access Control

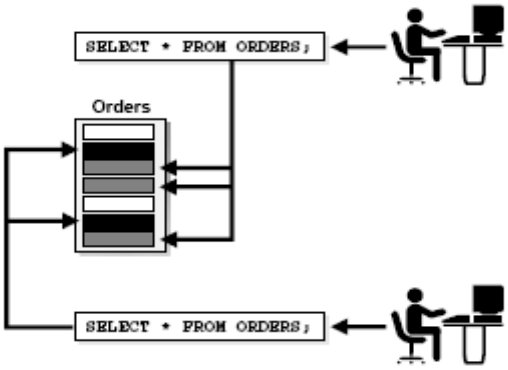
Oracle menyediakan Discretionary Access Control (DAC) pada setiap tabel yaitu kontrol akses terhadap informasi melalui *privilege* (SELECT, INSERT, UPDATE, DELETE) yang mengijinkan operasi Structured Query Language (SQL) yang berhubungan pada tabel.

2. Label

Label memungkinkan aturan kontrol akses yang kompleks diluar apa yang tercakup dalam DAC dengan menggunakan data dalam baris. Ketika aturannya diterapkan, satu kolom baru ditambahkan pada setiap baris data. Kolom ini menyimpan label yang menandakan sensitivitas setiap baris. Akses level ditentukan dengan membandingkan identitas dan label user dengan sensitivitasnya di baris tersebut. DAC dan Oracle Label Security (OLS) menentukan kriteria apakah akses pada suatu baris diijinkan atau ditolak.

3. Virtual Private Database

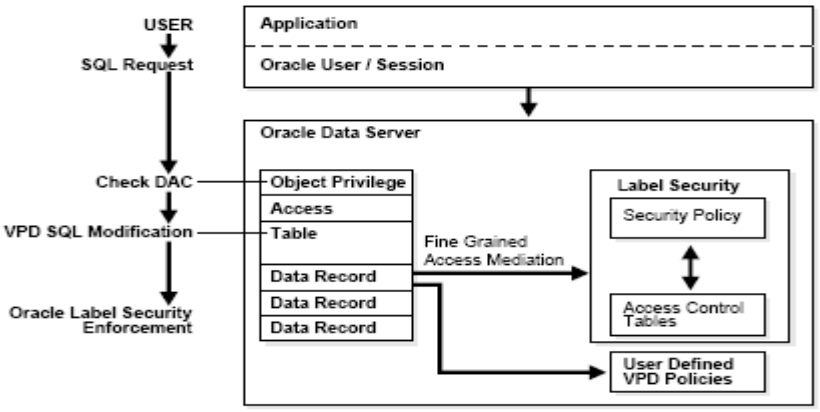
OLS bergantung pada konsep Virtual Private Database (VPD) untuk memperluas keamanan pada level baris. Secara esensial, ketika aturan bisnis dipersiapkan melalui OLS, VPD menambahkan kriteria seleksi tambahan yang perlu ke setiap pernyataan SQL yang dikeluarkan untuk membatasi akses user ke hanya data yang perlu. Kelebihan dari VPD ialah aplikasi aturan ditangani “dibalik layar” tanpa diketahui user. Misalnya, diterapkan aturan sehingga user SCOTT hanya dapat melihat baris pada tabel ORDERS yang ditandai USERID-nya saja, VPD menambahkan kriteria seleksi (WHERE ORDERS.USERID = ‘SCOTT’) pada query. Hal ini dapat diterapkan pula pada user lainnya yang hanya dapat melihat data yang diperbolehkan seperti yang digambarkan berikut ini :



Gb.2 Teknologi VPD Oracle
(Sumber : http://download-west.oracle.com/)

B. Arsitektur Oracle Label Security

Aplikasi user dalam session Oracle menghasilkan SQL Request. Oracle mengecek *privilege* DAC, menjamin bahwa user memiliki *privilege* SELECT pada tabel. Kemudian dicek apakah aturan VPD telah diterapkan pada tabel untuk menjamin bahwa tabel tersebut diproteksi. Pernyataan SQL diubah pada proses selanjutnya. Hal tersebut digambarkan dalam arsitektur Oracle Label Security sebagai berikut :



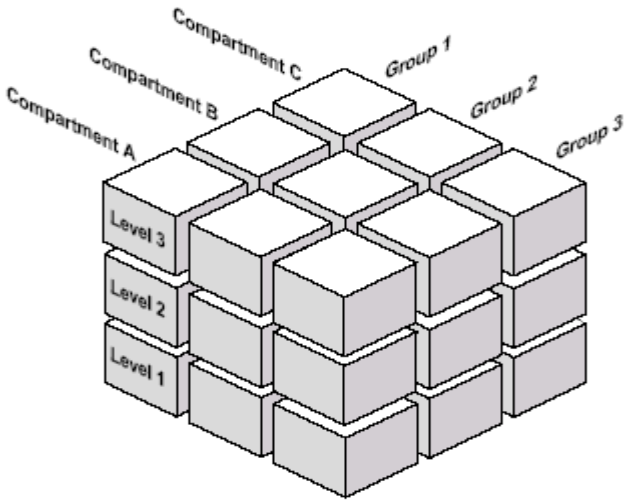
Gb.3 Arsitektur Oracle Label Security
(Sumber : http://download-west.oracle.com/)

C. Komponen Oracle Label Security

Keamanan dengan label menambah perlindungan data diluar DAC yang menentukan operasi yang dapat dilakukan user terhadap data dalam suatu objek, seperti tabel atau *view*. Aturan OLS mengontrol akses terhadap data dalam tiga dimensi :

- Data Label : menunjukkan level dan karakteristik sensitivitas baris dan kriteria tambahan yang harus dipenuhi user untuk mengakses baris tersebut.
- User Label : menunjukkan level sensitivitas user ditambah kompartemen dan grup yang membatasi akses user ke data yang diberi label.
- Aturan *Privilege* : user diberi hak spesifik untuk menjalankan operasi khusus atau untuk mengakses data diluar authorisasi label mereka.

OLS menggunakan tiga dimensi untuk mendefinisikan *user's permission* untuk mengakses data dalam baris, yaitu level, kompartemen dan grup. Gambar dibawah ini mengilustrasikan ketiga dimensi tersebut.



Gb. 4 Klasifikasi Data Secara Logis
(Sumber : http://download-west.oracle.com/)

Level adalah tingkatan yang menyatakan sensitivitas informasi. Semakin sensitif informasi, semakin tinggi pula levelnya. Setiap label harus memiliki satu level.

Untuk setiap level, administrator mendefinisikan bentuk numerik dan karakter, misalnya :

Bentuk Numerik	Bentuk Panjang	Bentuk Pendek
40	HIGHLY_SENSITIVE	HS
30	SENSITIVE	S
20	CONFIDENTIAL	C
15	PUBLIC	P

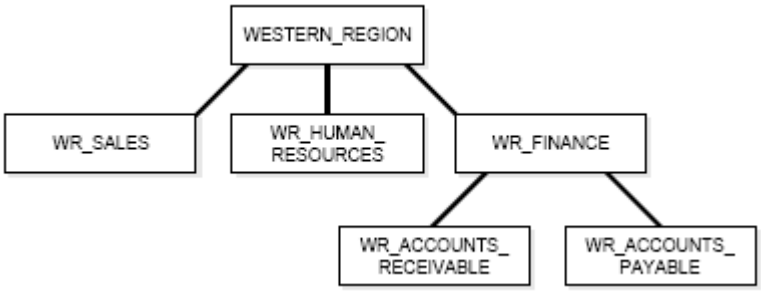
Tabel.1 Contoh Level

Kompartemen mengidentifikasi daerah yang menggambarkan sensitivitas data label, memberikan tingkatan yang lebih halus/detil dalam satu level. Kompartemen berhubungan dengan data dengan satu atau lebih daerah keamanan. Semua data yang berhubungan dengan proyek tertentu dapat dilabeli dengan kompartemen yang sama. Berikut ini diberikan contoh dari satu set kompartemen :

Bentuk Numerik	Bentuk Panjang	Bentuk Pendek
85	FINANSIAL	FINCL
65	CHEMICAL	CHEM
35	OPERASIONAL	OP

Tabel.2 Contoh Kompartemen

Grup mengidentifikasi organisasi yang memiliki atau mengakses data, seperti EASTERN_REGION, WESTERN_REGION, WR_SALES. Semua data yang berhubungan dengan departemen tertentu dapat memiliki grup departemen dalam label. Grup berguna untuk mengontrol distribusi data, dan sebagai reaksi terhadap perubahan organisasi. Grup bersifat hirarki dimana data label dibuat berdasarkan infrastruktur organisasi. Grup dapat dihubungkan dengan grup *parent*. Misalkan :



Gb.5 Contoh Hirarki Grup
(Sumber : http://download-west.oracle.com/)

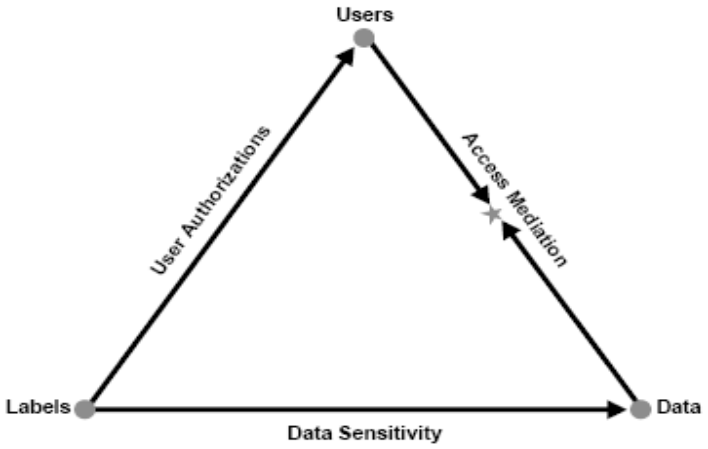
Pada Gb.5, grup WESTERN_REGION terdiri dari tiga subgrup : WR_SALES, WR_HUMAN_RESOURCES, dan WR_FINANCE. Subgrup WR_FINANCE dibagi lagi menjadi WR_ACCOUNTS_RECEIVABLE dan WR_ACCOUNTS_PAYABLE. Tabel dibawah ini menunjukkan struktur organisasi diatas dalam bentuk grup OLS.

Bentuk numeric	Bentuk Panjang	Bentuk Pendek	Grup Orang Tua
	WESTERN_REGION	WR	
1000	WR_SALES	WR_SAL	WR
1100	WR_HUMAN_RESOURCES	WR_HR	WR
1200	WR_FINANCE	WR_FIN	WR
1300	WR_ACCOUNTS_PAYABLE	WR_AP	WR_FIN
1310	WR_ACCOUNTS_RECEIVABLE	WR_AR	WR_FIN
1330			

Tabel.3 Contoh Grup

D. Kontrol Akses

Untuk dapat mengakses data yang diproteksi OLS, user harus memiliki authorisasi berdasarkan label yang didefinisikan. Dibawah ini ditunjukkan hubungan antara user, data, dan label.



Gb.6 Hubungan Antara User, Data, dan Label
(Sumber : http://download-west.oracle.com/)

- Data label menspesifikasi sensitivitas baris data.
- User label memberikan authorisasi ke user yang benar.
- *Access mediation* antara user dan baris data bergantung pada label.

Selama *access mediation*, OLS membandingkan nilai yang tersimpan didalam kolom label dengan label *permission* user. Jika user diberi hak yang memadai untuk mengakses baris, maka transaksi berlanjut. Untuk menjalankan perintah SELECT, user harus diberi akses *read mode*. Untuk menjalankan perintah Data Manipulation Language (INSERT, UPDATE, DELETE, atau MERGE), user harus diberi akses *write mode*.

E. Privilege

Privilege adalah authorisasi yang diberikan pada user untuk mengakses data. OLS membagi *privilege* menjadi 2 bagian, yaitu :

1. Special Access Privileges

Authorisasi user dapat diubah dengan salah satu dari *privilege* berikut ini :

- **READ**

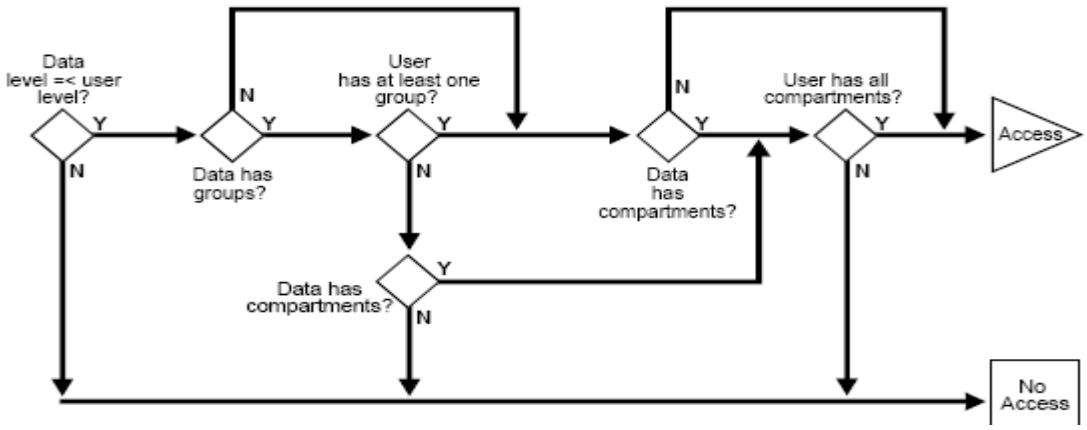
User dengan *privilege* READ dapat membaca semua data yang diproteksi, tanpa menghiraukan authorisasinya atau label *session*. User dengan privilege ini juga dapat menulis baris data jika dia memiliki akses write berdasarkan authorisasi labelnya. Privilege ini berguna bagi sistem administrator yang harus mengekspor data, tetapi tidak diijinkan untuk mengubah data. Hal ini juga berguna untuk membuat *report* dan meng-*compile* informasi, tetapi tidak mengubah data.

- **FULL**

Privilege ini mengijinkan akses READ dan WRITE ke semua data yang diproteksi. Algoritma READ dan WRITE tidak dipaksakan. Tetapi authorisasi Oracle SYSTEM dan OBJECT dipaksakan. Misalkan, user masih harus melakukan operasi SELECT ke tabel aplikasi. Authorisasi FULL mematikan uji *access mediation* pada level baris individual.

- **COMPACCESS**

Privilege ini mengijinkan akses ke data yang diauthorisasi baris kompartemen, tanpa bergantung dari baris grup. Jika suatu baris tidak memiliki kompartemen, maka akses ditentukan oleh authorisasi grup. Namun jika terdapat kompartemen, maka authorisasi grup di-*bypass*. Dibawah ini ditunjukkan proses evaluasi label untuk akses READ dengan *privilege* COMPACCESS.



Gb.7 Proses Evaluasi Label pada Akses Read untuk Privilege COMPACCESS

(Sumber : http://download-west.oracle.com/)

- **PROFILE_ACCESS**

Privilege ini mengijinkan akses *session* untuk mengubah label dan *privilege* user lain. *Privilege* ini sangat kuat, karena user dapat memiliki *privilege* FULL. *Privilege* ini tidak dapat diberikan ke unit program yang penting.

2. Special Row Label Privileges

Ketika label baris diset, dibutuhkan *privilege* OLS untuk mengubah label. Opsi LABEL_UPDATE harus tercakup pada label ini. Ketika user meng-*update* label baris, label baru dan lama dibandingkan, kemudian ditentukan *privilege* yang dibutuhkan. *Privilege* ini mencakup :

- **WRITEUP**

Privilege ini mengijinkan user untuk menaikkan level data dalam baris tanpa menghiraukan kompartemen atau grup. User dapat menaikkannya sampai level authorisasi maksimumnya. Misalkan, jika level suatu baris adalah UNCLASSIFIED dan level maksimum user adalah SENSITIVE, dia dapat menaikkan level baris sampai SENSITIVE, tetapi tidak dapat mengubah kompartemen.

- **WRITEDOWN**

Privilege ini mengijinkan user untuk menurunkan level data dalam baris, tanpa menghiraukan kompartemen atau grup. User dapat menurunkan level suatu baris sampai sama dengan atau lebih besar dari level authorisasi minimumnya.

- **WRITEACROSS**

Privilege ini mengijinkan user mengubah kompartemen dan grup data tanpa mengubah level sensitivitasnya. Hal ini menjamin data SENSITIVE tetap pada level SENSITIVE , tetapi pada waktu yang bersamaan dapat mengatur distribusi data. User dapat mengubah kompartemen dan grup ke bentuk lain yang valid dengan level yang sama. Dengan *privilege* ini, user dengan akses *read* ke satu grup (atau lebih) dapat memiliki akses menulis ke grup lain tanpa diberikan akses itu secara eksplisit.

III. Kesimpulan

Dari uraian diatas, maka dapat ditarik kesimpulan sebagai berikut :

1. OLS dan DAC mengontrol akses user untuk menentukan apakah akses ke suatu baris ditolak atau tidak. VPD membatasi akses user untuk data yang perlu saja.
2. Untuk mendefinisikan user permission, OLS menggunakan tiga dimensi yaitu level, kompartemen dan grup.
3. Authorisasi user dapat berubah bergantung pada privilege yang diberikan.

IV. Daftar Pustaka

http://download-west.oracle.com/docs/cd/B13789_01/network.101/b10774.pdf

http://download-west.oracle.com/docs/cd/B13789_01/network.101/b10777.pdf

http://www.databasejournal.com/features/oracle/article.php/3065431

http://download-west.oracle.com/docs/cd/B13789_01/network.101/b10773.pdf

http://otn.oracle.com/deploy/security/pdf/ds_security_db_labelsecurity_10r1_0104.pdf