

Oracle Advanced Security pada Oracle9i



NINYOMAN VICTORIA P
23202073

BIDANG KHUSUS TEKNOLOGI INFORMASI
PROGRAM STUDI TEKNIK ELEKTRO
PROGRAM PASCASARJANA
INSTITUT TEKNOLOGI BANDUNG
2004

DAFTAR ISI

KEAMANAN DI INTERNET	3
SOLUSI DARI ORACLE	4
PUBLIK KEY INFRASTRUCTURE (PKI)	5
Secure Socket Layer	6
Hardware Acceleration Support	7
Tempat Penyimpanan Private Key dan Sertifikat yang Aman	7
Oracle Wallet Manager	7
Entrust Integration	8
Keuntungan Public Key Infrastructure	8
INTEGRATED DIRECTORY DAN SECURITY	9
Masalah Administrasi User	10
Keuntungan Integrated Directory dan Security	11
Mekanisme Integrated Directory dan Security	12
Single Sign-On	13
Directory Services	15
SCHEMA-INDEPENDENT USER	17
ENKRIPSI	18
Issue Enkripsi	20
Tantangan Enkripsi	22
Solusi Oracle untuk Enkripsi Data Tersimpan	26
AUTENTIKASI	27
Autentikasi Berbasis Oracle	27
Autentikasi Berbasis Host	29
Autentikasi Berbasis Pihak Ketiga	29
Autentikasi Berbasis Public Key Infrastructure	30
Autentikasi Jarak Jauh	31
Autentikasi Melalui Middle Tier	31
Autentikasi Mutual untuk Komputasi Terdistribusi yang Aman	32
VIRTUAL PRIVATE DATABASE	32
Keuntungan Virtual Private Database	34
Kebijakan Keamanan Granular	35
Query yang Termodifikasi secara Dinamis	35
Konteks Aplikasi yang Aman	36
Mekanisme Akses Data	36
Cara Kerja Virtual Private Database	37
AUDITING	38
Auditing Granular	38
Audit Secara Efisien	39
Audit yang Diperluas	39
Audit untuk Aplikasi Three-Tier	39
Audit secara Aktif	40
KESIMPULAN	40
DAFTAR PUSTAKA	42

Oracle Advanced Security pada Oracle9i

Seiring dengan semakin banyaknya kegiatan bisnis yang dilakukan melalui Web, pengamanan terhadap data dalam pergerakannya dan adanya identifikasi terhadap user menjadi sesuatu faktor yang semakin dipertimbangkan. Manajemen user dan pengimplementasian infrastruktur penunjang keamanan telah menjadi item teratas dalam checklist “Hal Yang Harus Dilakukan, Hal Yang Harus Dilakukan Dengan Benar” dari seorang administrator basis data. Seiring dengan pertumbuhan Oracle sebagai pilihan utama untuk aktivitas penyimpanan data, data mining, dan pengadaan bisnis yang cerdas (intelligent business), sebuah variasi solusi untuk faktor keamanan yang mampu mengakomodasi ragam tantangan untuk faktor yang sama telah tersedia dalam kumpulan teknologi Oracle.

Pada awal tahun 90-an, aplikasi client server telah mulai dipergunakan secara luas dan mengalami pertumbuhan pesat. Kebutuhan akan adanya kerahasiaan data dan autentikasi user menggunakan perangkat keamanan telah ada sejak saat itu. Pada akhir tahun 90-an, seiring dengan terjadinya ledakan pertumbuhan internet dan kegiatan perdagangan yang dilakukan melalui Internet, terjadi pula ledakan jumlah user yang membutuhkan akses terhadap sejumlah aplikasi. Saat ini, manajemen dan administrasi user telah menjadi kebutuhan penting untuk sebuah bisnis.

KEAMANAN DI INTERNET

Menurut survey atas serangan keamanan yang dilakukan oleh Computer Security Institute dan FBI pada tahun 1998, terdapat beberapa tipe serangan keamanan yang menyebabkan kerugian secara finansial paling besar. Tipe-tipe serangan dan kerugian yang disebabkan (dalam dollar US) secara berurutan adalah sebagai berikut : Akses dari pihak dalam yang tidak berwenang (\$2,809,000), pencurian informasi (\$ 1,677,000), kecurangan telekomunikasi (\$ 539,000), kecurangan finansial (\$ 388,000), sabotase (\$ 86,000), dan penetrasi sistem oleh pihak luar (\$ 86,000).

Dari uraian diatas, tampak bahwa aspek keamanan memegang peranan yang sangat penting. Secara prinsip, terdapat beberapa masalah keamanan yang dewasa ini membutuhkan perhatian, khususnya dalam halmelaksanakan bisnis melalui Internet, yaitu :

- ☐ Privasi dari komunikasi, misalnya apakah order atau pesanan seseorang dapat dibaca atau dimodifikasi dalam perjalanannya?
- ☐ Penyimpanan data penting secara aman, misalnya apakah nomor kartu kredit seseorang disimpan secara aman?
- ☐ Akses kontrol yang granular, misalnya apakah customer hanya dapat melihat pesanannya sendiri?
- ☐ Pengetahuan akan user, misalnya siapa sajakah pengakses data dari Web?
- ☐ Skalabilitas, misalnya dapatkah aplikasi yang dibangun melayani lebih dari 100.000 user?
- ☐ Fleksibilitas, misalnya dapatkah aplikasi yang dibangun memberikan layanan keamanan berdasarkan kebutuhan yang berbeda untuk karyawan dan customer?

SOLUSI DARI ORACLE

Oracle Advanced Security menyediakan enkripsi jaringan dan sejumlah mekanisme autentikasi andal, layanan sign-on tunggal, dan protokol keamanan yang mendukung standar industri. Tantangan untuk administrator basis data atau manajer IT yang dapat diselesaikan dengan Oracle Advanced Security dapat dibagi menjadi :

- ☐ Pengetahuan mengenai user (dengan menyediakan layanan autentikasi yang andal untuk user, basis data, dan server web , dalam beberapa kasus mengaktifkan sign-on tunggal)
- ☐ Skalabilitas (mekanisme Enterprise User Management, dilakukan dengan mengintegrasikan Oracle Internet Directory dengan sejumlah mekanisme autentikasi yang bervariasi)
- ☐ Menjamin privasi jaringan komunikasi (dengan mekanisme enkripsi jaringan)
- ☐ Menyediakan media penyimpan data pribadi yang aman (dengan melakukan enkripsi terhadap data yang disimpan)
- ☐ Menyediakan kontrol akses yang granular (dengan Virtual Private Database)
- ☐ Kemudahan penggunaan (dengan menggunakan mekanisme schema-independent user)

- Fleksibilitas (fasilitas konfigurasi yang fleksibel).

Berikut akan dibahas secara lebih dalam mengenai beberapa solusi dari Oracle untuk menjawab tantangan dalam aspek keamanan seperti tersebut diatas.

I. PUBLIC KEY INFRASTRUCTURE (PKI)

Public Key Infrastructure (PKI) meliputi teknologi, kebijakan, dan prosedur yang digunakan dalam proses autentikasi berdasarkan prinsip public key cryptography, dengan tujuan untuk mewujudkan terciptanya pertukaran informasi secara aman. Komponen utama dari PKI adalah :

Digital Certificate, yang digunakan untuk pengidentifikasian user, mesin, ataupun basis data (identitas digital).

Public dan Private Key, yang membentuk dasar dari PKI untuk komunikasi secara aman yang didasarkan pada sebuah private key rahasia dan sebuah public key matematis yang berkaitan.

Secure Sockets Layer (SSL) yang merupakan protokol Internet untuk standar industri yang didasarkan pada prinsip public key cryptography untuk menyediakan autentikasi, enkripsi, dan integritas data. SSL mendukung 2 mode autentikasi, yaitu :

- autentikasi server (kepada client)
- autentikasi mutual (antara client dan server)

Certificate Authority (CA) yang berperan sebagai penyedia digital certificate yang terpercaya dan independent.

Komponen tambahan yang tidak kalah pentingnya yang memungkinkan pengimplementasian PKI adalah tempat penyimpanan sertifikat dan key yang aman, perangkat manajemen untuk permintaan sertifikat, pengaturan user, dan perlindungan terhadap kerahasiaan user dan sebuah directory service untuk melakukan proses identifikasi dan otorisasi terhadap user, mesin, dan basis data.

SECURE SOCKET LAYER (SSL)

Protokol Secure Socket Layer digunakan di Internet untuk memberikan identitas digital kepada user dan mencegah terjadinya penyadapan pesan. SSL yang didukung dalam Oracle Advanced Security melakukan proses enkripsi terhadap trafik jaringan dan menyediakan pengecekan integritas, mengautentikasi client dan server Oracle, dan membawa mekanisme single sign-on yang didasarkan pada public key dalam lingkungan Oracle. Protokol SSL menyediakan enkripsi dan integritas data melalui penggunaan cipher, yang merupakan sekumpulan tipe autentikasi, enkripsi, dan integritas data. Baik client maupun server masing-masing memiliki daftar cipher yang disupportnya dan pada saat sebuah inisiasi transaksi SSL, mereka menegosiasikan cipher yang akan digunakan selama koneksi tersebut berlangsung.

Salah satu contoh dari cipher suite adalah RSA untuk autentikasi dengan 3DES untuk enkripsi dan SHA-1 untuk integritas data. Diantara algoritma enkripsi yang disediakan oleh SSL untuk Oracle Advanced Security adalah RC4, DES, dan Triple DES. Algoritma Triple DES (3DES) merupakan sebuah alat yang andal dalam melindungi data karena algoritma ini menggunakan lebih dari satu 56-bit key yang digunakan oleh DES standar. 3DES semakin banyak digunakan oleh organisasi seperti bank dan institusi keuangan yang membutuhkan tingkat keamanan yang tinggi. Algoritma SHA-1 (Secure Hashing Algorithm) merupakan sarana untuk melakukan pengecekan integritas data yang merupakan hal baru untuk lingkungan Oracle. Algoritma ini membangkitkan sebuah fungsi hash untuk melindungi transmisi data dan menjamin paket tidak dimodifikasi selama proses transmisi.



Gambar 1. Protokol SSL mengamankan komunikasi antara Internet dan Oracle

HARDWARE ACCELERATION SUPPORT

Oracle Advanced Security 9i Release 2 memperbaiki performansi dari proses handshake SSL dengan mendelegasikan operasi public key cryptographic menjadi sebuah perangkat hardware accelerator menggunakan BSAFE Hardware API.

TEMPAT PENYIMPANAN PRIVATE KEY DAN CERTIFICATE YANG AMAN

Untuk dapat melakukan proses autentikasi, SSL harus memiliki sebuah private key dan sebuah sertifikat. Dalam lingkungan Oracle, Oracle Wallet merupakan tempat penyimpanan material ini. Ia menyimpan X.509v3 certificate, private key, dan data tambahan seperti trusted certificate yang diproses oleh SSL. Wallet ini dilindungi oleh sebuah password untuk keamanan yang lebih ketat. Pihak manapun, user, basis data Oracle, dan/atau Oracle Internet Directory yang berpartisipasi dalam transaksi SSL harus memiliki sebuah wallet. Ini digunakan untuk mengautentikasi user untuk mengakses beragam layanan seperti server data dan server aplikasi. User harus mengingat hanya satu password, yang digunakan untuk membuka wallet yang dimilikinya.

ORACLE WALLET MANAGER

Oracle Wallet Manager merupakan sebuah perangkat Graphical User Interface (GUI) pada basis data client yang terutama ditujukan untuk digunakan oleh seorang administrator basis data untuk meminta sertifikat dari sebuah certificate authority atas nama user dari sebuah certificate authority dan menyediakan interface manajemen wallet yang bervariasi. Administrator dapat mengatur informasi wallet mengenai aplikasi dan basis data secara terpusat. Oracle Wallet Manager memungkinkan pengaturan wallet dilakukan secara mudah. Ia membuat key dan mengatur pilihan credential untuk sebuah user. Sebuah wallet memuat sebuah sertifikat, private key yang terenkripsi, dan trust point untuk user. Keseluruhan wallet ini berada dalam keadaan terenkripsi.

Oracle juga menyediakan Oracle Enterprise Login Assistant dan Enterprise Login Assistant Servlet kepada end user untuk mengakses Oracle Wallet mereka dan kemampuan untuk mengatur fungsionalitas wallet secara sederhana. Oracle Enterprise Login Assistant merupakan sebuah alat bantu untuk melakukan single sign-on. Ia memungkinkan user untuk melakukan login pada aplikasi secara otomatis. Alat bantu ini menyediakan sebagian fungsionalitas dari wallet manager yang diperlukan untuk membuka sebuah user wallet dan memampukan aplikasi untuk menggunakan wallet yang telah terbuka tersebut untuk mengautentikasi user secara otomatis.

ENTRUST INTEGRATION

Oracle telah membuat modifikasi produk secara spesifik untuk memampukan customer Entrust untuk memasukkan Entrust single sign-on ke dalam aplikasi mereka yang terhubung dengan basis data Oracle. Modifikasi ini memungkinkan customer Oracle untuk memasukkan Entrust-based single sign-on dan solusi PKI kedalam aplikasi mereka. Dengan mengintegrasikannya dengan Entrust/PKI, Oracle memberikan dukungan kepada customer yang mengimplementasikan aplikasi dalam sebuah lingkungan client-server dan memilih Entrust sebagai vendor PKI mereka.

KEUNTUNGAN PUBLIC KEY INFRASTRUCTURE

- ⊕ PKI didasarkan pada standar dan memungkinkan dilakukannya kerjasama antar teknologi yang bervariasi yang mendukung standar yang sama, untuk menciptakan sebuah sistem keamanan yang andal (interoperability technology).
- ⊕ Mampu mengakomodasi perkembangan jumlah user sebagai pemakai Internet sampai level jutaan

Hal ini dimungkinkan karena user memelihara sendiri sertifikat mereka, dan karena autentikasi terhadap sertifikat tersebut melibatkan pertukaran data hanya antara server dan client (dalam arti tidak terdapat server autentikasi sebagai pihak ketiga yang dibutuhkan berada dalam keadaan online), maka tidak terdapat batasan jumlah user yang dapat didukung oleh penggunaan PKI.

- ⊕ Memungkinkan adanya delegated trust, yaitu sebuah user yang telah memperoleh sertifikat dari sebuah CA yang telah dikenali dan dipercaya dapat mengautentikasi dirinya sendiri kepada sebuah server pada saat pertama dirinya terhubung ke server tersebut, walaupun sebelumnya user tersebut belum terdaftar pada server tersebut.

- ⊕ Memungkinkan user memilih trust provider

Oracle memungkinkan user untuk menginstall trusted root certificate dari CA pilihan mereka, memungkinkan server untuk mengenali dan memvalidasi sertifikat yang dikeluarkan oleh CA tersebut. Oracle bekerja sama dengan vendor terkemuka yang memberikan layanan dan produk PKI untuk memberikan jaminan bahwa trusted root CA mereka akan terinstall pada Oracle9i, sehingga memungkinkan customer untuk menginstall Oracle9i dan secara langsung mengintegrasikannya dengan PKI berdasar pada sertifikat dari vendor tersebut.

- ⊕ Implementasi PKI Oracle memungkinkan terjadinya single sign-on

Single sign-on (SSO) adalah sebuah aksi untuk melakukan proses login dalam satu saat, kemudian mendapatkan akses terhadap sejumlah server atau aplikasi dengan menggunakan credential autentikasi tunggal. User menggunakan username dan password tunggal untuk mengakses sejumlah aplikasi basis data.

II. INTEGRATED DIRECTORY DAN SECURITY

Beberapa tantangan yang dihadapi oleh sebuah perusahaan dewasa ini adalah pengaturan informasi mengenai user, memelihara agar informasi user selalu merupakan informasi terakhir dari user yang bersangkutan, dan mengamankan akses terhadap semua informasi yang terdapat dalam sebuah perusahaan.

MASALAH ADMINISTRASI USER

Fasilitas Integrated Directory dan Security yang disediakan Oracle9i ini berkaitan dengan masalah administrasi user. Masalah yang terjadi dengan administrasi user pada umumnya adalah sebagai berikut :

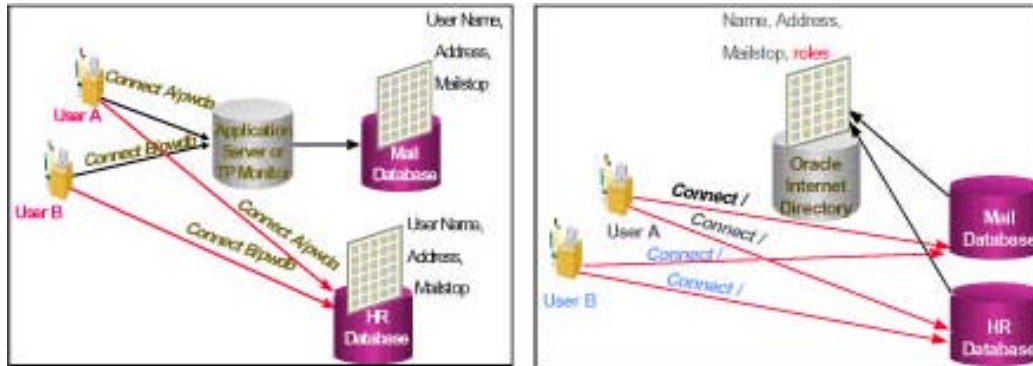
- **User memiliki terlalu banyak password**

Banyaknya aplikasi basis data yang harus diakses oleh user seringkali menyebabkan user harus memiliki banyak password. Hal ini menimbulkan kemungkinan penyebab masalah keamanan di waktu mendatang, terutama karena dengan banyaknya password ini, user seringkali harus menuliskan semua password mereka pada sebuah kertas karena mengalami kesulitan untuk mengingat semua password tersebut. Disamping itu, hal yang potensi menimbulkan masalah keamanan lain adalah karena harus membuat banyak password, user seringkali membuat password yang mudah ditebak, atau membuat password yang sama untuk mengakses semua aplikasi basis data yang dibutuhkannya.

- **Terdapat terlalu banyak user account yang harus dikelola**

Hal ini menyimpan potensi untuk menimbulkan masalah keamanan karena :

- ☐ Semakin banyak user account yang harus dimaintain oleh seorang administrator, semakin besar usaha yang dibutuhkan untuk mampu melakukan proses maintain tersebut dengan baik, sehingga dapat meminimalkan kemungkinan terjadinya masalah keamanan.
- ☐ Terdapat data yang tidak efektif (redundant), karena informasi yang umum atau sama untuk seorang user tersimpan pada terlalu banyak tempat (misal pada basis data Human Resource, basis data mail, dan sebagainya).
- ☐ Kurangnya faktor penyimpanan data yang terpusat menyebabkan resiko keamanan yang semakin besar. Dalam hal ini kemungkinan besar terdapat banyak user account lama yang sebenarnya tidak terpakai, demikian pula halnya dengan privilege user yang sudah usang dan tidak berlaku, yang dapat disalahgunakan.



Gambar 2. Security / Directory Integration

Oracle Advanced Security mengakomodasi kebutuhan akan adanya tingkat keamanan yang tinggi, single sign-on, dan manajemen user yang terpusat dengan menawarkan layanan keamanan dan direktori yang terintegrasi (integrated security and directory services), secara khusus dengan menyimpan dan mengelola informasi user dalam sebuah direktori yang mendukung Lightweight Directory Access Protocol (LDAP). Lebih dari satu aplikasi Oracle pada saat yang bersamaan dapat mengandalkan sebuah definisi yang umum dan terpusat dari sebuah user untuk menentukan aplikasi, layanan, dan server mana yang dapat diakses oleh user, dan privilege apa yang dimiliki oleh seorang user untuk melakukan hal tersebut.

KEUNTUNGAN INTEGRATED DIRECTORY DAN SECURITY

Keuntungan dari penggunaan layanan keamanan dan direktori yang terintegrasi adalah sebagai berikut :

- ⊕ Dimungkinkannya mekanisme single sign-on terhadap lebih dari satu basis data Oracle yang terdapat dalam seluruh enterprise.
- ⊕ Hanya terdapat satu user account dalam satu enterprise, yang menggantikan konsep lebih dari satu account untuk tiap user.
- ⊕ Mengurangi biaya kepemilikan secara keseluruhan dengan penggunaan Single Station Administration (SSA).
- ⊕ Public Key Infrastructure (PKI) yang terintegrasi dengan baik dan berbasis standar.
- ⊕ Tingkat keamanan yang lebih baik melalui mekanisme manajemen otorisasi yang terpusat dan autentikasi yang andal.

MEKANISME INTEGRATED DIRECTORY DAN SECURITY PADA ORACLE

Mekanisme layanan keamanan dan direktori yang terintegrasi yang disediakan oleh Oracle Advanced Security meliputi komponen Oracle sebagai berikut :

Oracle Wallet Manager – sebuah perangkat yang digunakan untuk melindungi dan mengelola sertifikat user, key, dan trustpoint.

Oracle Enterprise Login Assistant – sebuah perangkat yang mudah digunakan, yang memungkinkan dilakukannya mekanisme single sign-on untuk user.

Oracle Internet Directory – sebuah layanan direktori yang compliant dengan LDAPv3, dibangun pada basis data Oracle9i, yang menyimpan informasi mengenai user dan role dalam suatu enterprise.

Oracle Enterprise Security Manager – sebuah perangkat administrasi yang disediakan melalui Oracle Enterprise Manager, yang memungkinkan administrator untuk mengelola user enterprise dan role enterprise dalam Oracle Internet Directory, dan melintasi lebih dari satu basis data Oracle9i, dari sebuah console tunggal.

Oracle9i – sebuah server data yang mengambil role dari user enterprise dari Oracle Internet Directory dan melakukan autentikasi terhadap user melalui SSL.

Disamping itu, layanan keamanan dan direktori yang terintegrasi dari Oracle juga membutuhkan komponen non Oracle, yaitu **Certificate Authority (CA)**, yaitu sebuah certificate authority yang compliant dengan X.509 yang berfungsi membuat digital certificate.

Untuk mengatasi masalah administrasi tersebut, Oracle9i menawarkan 2 solusi, yaitu mekanisme Single Sign-On, dan penggunaan Directory Services. Berikut akan dibahas secara lebih detail solusi tersebut.

SINGLE SIGN-ON

Mekanisme ini digunakan untuk mengatasi masalah kemungkinan sebuah user memiliki terlalu banyak password. Untuk memungkinkan dilakukannya mekanisme ini, terdapat beberapa alat bantu yang dapat digunakan, yaitu:

KERBEROS

Kerberos merupakan sebuah protokol autentikasi jaringan yang dirancang untuk menyediakan akses yang aman dalam sebuah lingkungan terdistribusi. Bekerja bersamaan dengan sebuah layanan keamanan terpusat, Kerberos menggunakan cryptography yang andal sehingga sebuah client dan server dapat membuktikan identitas mereka satu dengan yang lain melalui sebuah kanal yang tidak aman. Kemudian, client dan server dapat mengenkripsi semua komunikasi yang terjadi diantara mereka untuk menjamin privasi dan integritas data selama berlangsungnya hubungan.

Bagaimana Kerberos bekerja

Integrasi Kerberos dari Oracle Advanced Security terletak pada layanan keamanan terpusat terpercaya (Kerberos Key Distribution Center) yang menggunakan rahasia untuk memberikan "ticket granting tickets" (TGT) untuk suatu perioda waktu tertentu yang terbatas untuk client yang meminta akses terhadap basis data. Sebuah permintaan hubungan terhadap suatu basis data dari sebuah client memberikan TGT kepada basis data yang kemudian akan berkomunikasi dengan Key Distribution Center (KDC) Kerberos sebagai bagian dari proses autentikasi, dalam rangka memberikan konfirmasi bahwa TGT tersebut masih valid dan user tersebut merupakan user yang valid.

Client basis data dapat melakukan autentikasi dengan menggunakan tiket Kerberos yang diberikan oleh server MIT Kerberos, Cybersafe Trust Broker dan tiket MIT yang dikeluarkan oleh Windows 2000 KDC. Hal ini memungkinkan user desktop untuk memiliki hanya sebuah credential tunggal untuk lingkungan Windows dan Oracle mereka sehingga dapat menyediakan sebuah solusi sign-on tunggal dalam sebuah lingkungan 2-tier atau 3 tier.

X.509 CERTIFICATE

Oracle Advanced Security mempercayakan proses autentikasi user kepada wallet yang dimiliki oleh client. Hal ini membutuhkan pemrosesan SSL untuk membangun sebuah jalur yang aman antara client dan server dan server basis data dengan directory LDAP-compliant. Mekanisme autentikasi menggunakan SSL dan X.509v3 certificate, membutuhkan Oracle wallet untuk diinstall baik pada client maupun server.

Meskipun hal ini merupakan sebuah mekanisme yang sangat efektif untuk menjamin integritas proses autentikasi, ia membutuhkan pemrosesan SSL dan wallet di sisi client. Karena pencocokan SSL certificate membutuhkan sebuah sertifikat X.509 yang dikeluarkan oleh sebuah Certificate Authority yang terpercaya untuk masing-masing user, overhead pemrosesan ini dapat menjadi sangat berpengaruh untuk organisasi berukuran besar. Baik SSL maupun wallet Oracle harus diinstall pada client dan server.

RADIUS (REMOTE DIAL-IN USER SERVICE)

RADIUS (RFC #2138) merupakan sebuah sistem distribusi yang mengamankan akses jarak jauh untuk layanan jaringan dan telah dijadikan sebuah standar industri untuk akses jarak jauh dan akses terkendali terhadap jaringan. RADIUS menggunakan credential dan akses informasi didefinisikan dalam server RADIUS untuk memungkinkan server eksternal ini melakukan autentikasi, otorisasi, dan layanan akuntansi jika dibutuhkan.

RADIUS dari Oracle mendukung sebuah implementasi dari protokol client RADIUS yang memungkinkan basis data untuk melakukan autentikasi, otorisasi, dan fungsi akuntansi untuk user RADIUS. Ia akan mengirimkan permintaan autentikasi kepada server RADIUS dan bertindak sesuai dengan respon yang diberikan oleh server tersebut. Autentikasi dapat terjadi baik dalam mode sinkron maupun asinkron dan hal tersebut merupakan bagian dari konfigurasi Oracle untuk dukungan RADIUS.

Bagaimana RADIUS bekerja

Saat sebuah user meminta sebuah koneksi terhadap sebuah basis data, Oracle memberikan respon berupa sebuah tantangan. Tantangan dan respon user terhadap tantangan tersebut dikirim ke sebuah server RADIUS untuk diverifikasi. Basis data menginterpretasikan respon server RADIUS untuk mengizinkan atau menolak akses terhadap basis data. Jika layanan akuntansi dimungkinkan, proses ini akan dimulai segera sesudah koneksi diberikan dan diakhiri saat adanya permintaan pemutusan hubungan dari user.

Oracle 9i Advanced Security Release 2 memungkinkan otorisasi pada RADIUS untuk diberikan kepada user RADIUS pada saat melakukan hubungan dengan basis data. Hal ini merupakan fitur tambahan yang dapat dikonfigurasi oleh administrator basis data.

DIRECTORY SERVICES

Solusi ini diberikan oleh Oracle untuk mengatasi masalah kemungkinan adanya terlalu banyak user account. Dengan menggunakan directory services terdapat beberapa keuntungan, yaitu :

- Tempat penyimpanan informasi user yang terpusat
- Pengaturan user dan privilege yang terpusat
- Jumlah user account yang lebih sedikit

Sebuah tantangan yang telah menjadi ciri khas dari sistem terdistribusi manapun, termasuk sistem three-tier, adalah informasi aplikasi pada umumnya tersebar di seluruh organisasi, yang menyebabkan kemungkinan terjadinya data yang redundant, inconsistent, dan sulit untuk dikelola. Directory dipertimbangkan sebagai sebuah mekanisme terbaik untuk membuat informasi organisasi tersedia dan dapat diakses oleh sejumlah sistem berbeda yang terdapat dalam organisasi tersebut. Directory juga memungkinkan organisasi untuk mengakses atau membagikan informasi dengan tipe tertentu melalui Internet, misalnya melalui sebuah virtual private network. Kecenderungan penggunaan directory ini telah dipercepat dengan pertumbuhan Lightweight Directory Access Protocol (LDAP) dewasa ini.

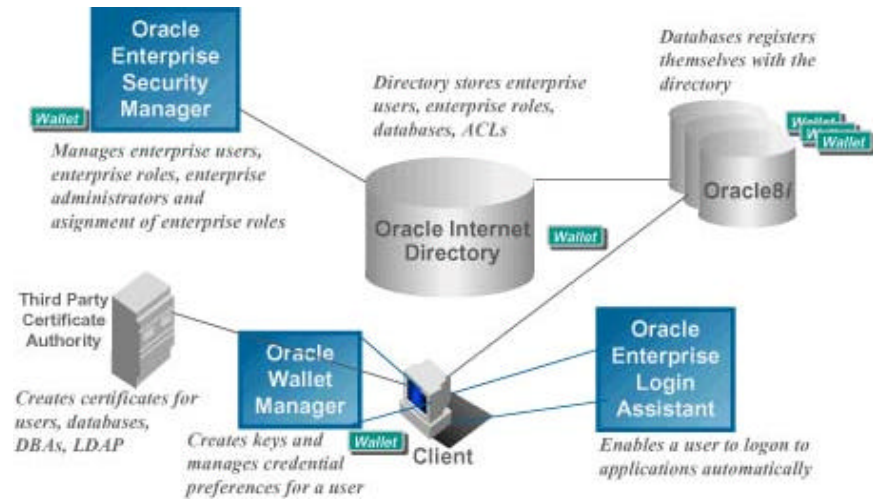
Directory informasi yang menspesifikasikan atribut privilege atau akses dari suatu user bersifat sensitif, karena perubahan yang dilakukan oleh pihak yang tidak berwenang

terhadap informasi ini dapat menyebabkan terjadinya pemberian akses yang tidak semestinya atau penolakan terhadap privilege atau akses yang dimiliki oleh suatu user. Sebuah directory yang menyimpan informasi ini harus menjamin bahwa hanya administrator keamanan dari sistem yang berwenang yang dapat melakukan modifikasi terhadap informasi privilege atau akses yang tersimpan dalam directory tersebut.

Oracle Internet Directory mendukung atribut pengontrolan level akses dan autentikasi user yang bersifat optional dan andal dengan menggunakan SSL, dan dapat dikonfigurasi sehingga hanya user tertentu yang terautentikasi dengan baik yang dimungkinkan untuk melakukan update informasi directory mengenai privilege atau akses user.

Oracle9i mendukung role enterprise : kumpulan privilege yang teradministrasi secara terpusat, tersimpan dalam Oracle Internet Directory, atau directory dari partner terpilih yang sesuai dengan kriteria keamanan yang ditetapkan Oracle. Role enterprise memungkinkan otorisasi user secara andal dan terpusat. Disamping itu, seorang administrator juga dapat menambahkan kemampuan untuk role enterprise (memberikannya kepada lebih dari satu user) tanpa harus melakukan update terhadap otorisasi user tersebut satu persatu. Oracle Enterprise Security Manager menyediakan sebuah alat untuk mengatur definisi user secara terpusat dan memberikan role, menyebabkan tingkat kemudahan administrasi user yang relatif rendah. Keuntungan lain dari administrasi terpusat seperti ini adalah keamanan menjadi mudah diatur, organisasi cenderung lebih menyukai implementasi aspek keamanan yang andal secara keseluruhan.

Oracle menggunakan Oracle Internet Directory, directory standar LDAP untuk manajemen terpusat dalam lingkungan Oracle. Basis data Oracle9i menggunakan kelebihan untuk mengatur user, proses autentikasi terhadap credential user, dan otorisasi user secara terpusat. Oracle Internet Directory berfungsi sebagai inti dimana administrasi terpusat mutlak diperlukan.



Gambar 3. Infrastruktur Enterprise User Management

III. SCHEMA-INDEPENDENT USER

Mekanisme ini merupakan bagian dari integrasi security/directory yang berkaitan erat dengan autentikasi client menggunakan SSL. Dengan adanya penggunaan direktori tersebut, jumlah user account akan menjadi lebih sedikit.

Dalam mekanisme ini, lebih dari satu user dapat berbagi sebuah skema basis data, sehingga pembuatan user pada masing-masing basis data tidak diperlukan lagi.

Fitur ini memperluas keuntungan yang diperoleh dengan penggunaan integrasi directory dengan memungkinkan basis data untuk mendelegasikan administrasi dari identitas dan privilege user kepada directory yang bersangkutan. Sebuah schemaless user adalah user basis data yang identitasnya tersimpan dalam tempat penyimpanan LDAP yang terpusat, secara khusus disebut Oracle Internet Directory. Saat user ini melakukan hubungan dengan basis data tersebut, basis data akan bertanya kepada directory apakah user tersebut terdaftar pada directory tersebut. Jika user tersebut telah terdaftar, maka directory harus memberikan informasi mengenai pemetaan user tersebut ke suatu skema tertentu, dan role apa yang dimiliki oleh user tersebut.

Untuk lebih memahaminya, berikut adalah satu contoh. Misalkan terdapat 500 user dari sebuah aplikasi HRAPP, yang membutuhkan akses terhadap data pada beberapa basis data dalam enterprise tersebut. Menyimpan 500 user account pada masing-masing basis data merupakan hal yang sangat tidak efektif. Sebagai penggantinya, Oracle9i memungkinkan administrator sistem untuk membuat sebuah skema (shared schema) HRAPPUSER, dengan privilege yang berkesesuaian, pada masing-masing basis data, kemudian membuat 500 user enterprise pada sebuah Oracle Internet Directory. Saat mereka terhubung ke basis data tertentu, user-user ini akan dipetakan ke skema HRAPPUSER, dan akan mewarisi privilege yang berhubungan dengan HRAPPUSER, akan tetapi akan mendapatkan pula privilege tambahan yang sesuai dengan role yang diberikan kepada mereka pada directory. Meskipun user-user ini berbagi sebuah skema, masing-masing identitas user ini dihubungkan dengan sesi mereka masing-masing oleh basis data yang bersangkutan, dan dapat digunakan untuk pengontrolan akses atau keperluan audit tertentu.

Fitur berbagi skema ini memiliki beberapa keuntungan. Pertama, ia mengurangi beban administratif yang berhubungan dengan pengaturan user dalam sebuah enterprise, dan memungkinkan terciptanya manajemen yang efektif dari sebuah komunitas user yang jauh lebih besar dari yang sebelumnya dimungkinkan untuk diakomodasi. Selain itu, dimasa yang akan datang ia akan menyediakan sebuah mekanisme untuk mengintegrasikan manajemen account dan privilege user dalam layer-layer pada sebuah sistem multi-tier, selama layer menengah juga memungkinkan adanya pengaturan identitas dan privilege user dalam directory tersebut. Pada sistem seperti ini, user baru beserta privilege mereka akan didaftarkan sebanyak satu kali pada directory tersebut, dan hal ini akan memberikan akses yang tepat terhadap layer menengah dan juga basis data manapun yang mereka butuhkan. Dimasa mendatang, terdapat kemungkinan untuk membangun sistem three-tier dimana user baru dapat mendaftarkan diri mereka sendiri dengan sebuah server web, dan kemudian server web ini akan membuat sebuah entry untuk user-user ini dalam directory tersebut, untuk memberikan akses untuk informasi dalam basis data yang sesuai.

IV. ENKRIPSI

Internet menyebabkan timbulnya tantangan baru dalam aspek keamanan informasi, khususnya untuk organisasi yang mulai bergerak untuk menjalankan e-business. Sebagian

besar dari tantangan tersebut dapat teratasi oleh mekanisme sebagai berikut : autentikasi yang andal untuk mengidentifikasi user, kontrol akses secara detail untuk membatasi apa saja yang dapat dilihat dan dilakukan oleh user, proses audit untuk akuntabilitas, dan enkripsi jaringan untuk melindungi kerahasiaan data yang bersifat sensitif selama proses transmisi.

Enkripsi merupakan sebuah komponen penting dari beberapa solusi tersebut. Sebagai contoh, SSL yang merupakan sebuah protokol berstandar untuk enkripsi jaringan dan autentikasi pada Internet, menggunakan enkripsi untuk mengautentikasi user secara andal, dengan menggunakan X.509 digital certificate. SSL juga menggunakan enkripsi untuk menjamin kerahasiaan data, dan checksum kriptografi untuk menjamin integritas data. Sebagian besar penggunaan enkripsi ini bersifat transparan terhadap user atau aplikasi. Sebagai contoh, sebagian besar browser mendukung SSL, dan user pada umumnya tidak harus melakukan suatu hal yang khusus untuk mengaktifkan enkripsi SSL.

Oracle telah menyediakan enkripsi jaringan antara client basis data dengan basis data Oracle sejak Oracle7. Oracle Advanced Security, sebuah fitur pada Oracle9i, menyediakan proses pengecekan enkripsi dan kriptografi yang terintegrasi untuk protokol apapun yang didukung oleh Oracle9i, termasuk Net8, Java Database Connectivity (JDBC), dan Internet Intra-Orb Protocol (IIOP). Oracle Advanced Security juga mendukung SSL untuk koneksi Net8, "thick" JDBC, dan IIOP.

Walaupun enkripsi bukan satu-satunya faktor yang dapat menjamin terciptanya sistem yang aman, akan tetapi enkripsi merupakan sebuah alat yang penting untuk mengakomodasi ancaman keamanan tertentu, dan akan semakin penting seiring dengan perkembangan e-business, terutama dalam area enkripsi dari data yang tersimpan. Sebagai contoh, saat nomor kartu kredit dilindungi dalam perjalanan ke sebuah situs web dengan menggunakan SSL, nomor ini pada umumnya tersimpan dalam suatu tempat yang tidak terenkripsi, baik itu pada sistem file, dimana sangat mungkin ada pihak yang dapat masuk kedalam host dan mendapatkan hak akses sebagai root, ataupun dalam basis data. Walaupun basis data dapat dikonfigurasi untuk mempunyai tingkat keamanan yang baik, akan tetapi basis data ini tetap dapat disusupi oleh pihak yang tidak berwenang jika terjadi salah konfigurasi terhadap host tersebut.

ISSUE ENKRIPSI

Disamping terdapat banyak alasan yang kuat untuk mengenkripsi data, terdapat pula alasan yang kurang baik untuk melakukan enkripsi data. Enkripsi tidak memecahkan semua masalah keamanan, dan bahkan dapat membuat beberapa masalah menjadi lebih buruk. Berikut akan dijelaskan beberapa konsep yang kurang tepat mengenai enkripsi dari data yang tersimpan.

1. Enkripsi bukan merupakan kontrol terhadap akses

Pada umumnya organisasi memiliki kebutuhan untuk membatasi akses terhadap data hanya untuk mereka yang benar-benar harus berhubungan dengan data yang bersangkutan. Sebagai contoh, sebuah sistem sumber daya manusia mungkin membatasi karyawan hanya dapat melihat data kepegawaian masing-masing, sementara manajer memiliki wewenang untuk melihat semua karyawan yang bekerja dibawah tanggung jawabnya.

Tipe kebijakan keamanan yang membatasi akses dan hanya memberikan akses kepada mereka yang berkepentingan seperti ini, secara khusus telah diakomodasi oleh mekanisme kontrol akses. Basis data Oracle telah menyediakan mekanisme kontrol akses yang andal dan terevaluasi secara independent sejak bertahun-tahun yang lalu. Dewasa ini, Oracle 9i telah menambahkan kemampuan untuk melakukan fungsi kontrol akses menjadi lebih baik dan detail, melalui kemampuan Virtual Private Database yang dimilikinya.

Sebuah prinsip dasar dibalik enkripsi data yang tersimpan adalah mekanisme tersebut tidak seharusnya tercampur dengan mekanisme kontrol akses., Suatu user yang memiliki privilege SELECT untuk sebuah tabel tidak seharusnya dibatasi oleh mekanisme enkripsi untuk melihat keseluruhan data yang berhak dilihatnya. Sama halnya dengan (misalnya) penggunaan sebuah key untuk enkripsi sebagian dari sebuah tabel, dan penggunaan key lain untuk enkripsi sebagian dari tabel lain, hal ini akan menambah overhead proses dekripsi data sebelum user dapat membacanya. Jika mekanisme kontrol akses dapat diimplementasikan dengan baik, maka terdapat sedikit tambahan aspek keamanan yang disediakan oleh basis data itu sendiri dari enkripsi, user yang memiliki privilege untuk mengakses data dalam basis data tersebut tidak memiliki privilege yang berkurang atau lebih sebagai akibat dari

digunakannya enkripsi. Maka dari itu, enkripsi seharusnya tidak digunakan untuk memecahkan masalah kontrol akses.

2. Seorang administrator basis data (DBA) harus mengakses semua data

Sejumlah organisasi memiliki kepedulian mengenai DBA, terutama karena mereka hampir memiliki semua privilege, sehingga mereka dapat melihat semua data dalam basis data. Organisasi-organisasi ini berpendapat bahwa tugas DBA adalah mengelola basis data, akan tetapi tidak seharusnya dapat melihat semua data yang tersimpan dalam basis data tersebut. Mereka mempertimbangkan untuk membagi fungsi DBA, tidak mengkonsentrasikan semua privilege kepada satu orang.

Sangat menggoda untuk berpikir bahwa mengenkripsi semua data (atau sebagian besar data) akan memecahkan masalah tersebut, akan tetapi ternyata terdapat cara yang lebih baik untuk mencapai tujuan ini, dengan menggunakan mekanisme kontrol akses. Pertama, Oracle mendukung pemisahan fungsi DBA melalui role SYSDBA dan SYSOPER. SYSDBA memiliki semua privilege, sedangkan SYSOPER hanya memiliki sekumpulan privilege yang terbatas. Lebih dari itu, sebuah organisasi dapat membuat role yang lebih kecil meliputi sejumlah privilege terhadap sistem. Sebagai contoh, role untuk seorang JR_DBA mungkin tidak meliputi semua privilege dalam sistem, akan tetapi hanya meliputi privilege yang tepat untuk diberikan kepada seorang administrator basis data junior.

Enkripsi dari data yang tersimpan tidak seharusnya tercampur dengan fungsi administrasi basis data. Penggunaan enkripsi yang tidak pada tempatnya dapat menimbulkan masalah keamanan lain. Sebagai contoh, jika pengenkripsian data menyebabkan data menjadi rusak, maka sebuah masalah keamanan telah timbul, yaitu data menjadi tidak memiliki arti dan mungkin tidak dapat dipulihkan kembali.

3. Pengenkripsian semua hal akan membuat data menjadi aman

Jika enkripsi dilakukan terhadap sebuah basis data secara keseluruhan, maka akan menjadi tidak efisien. Semua data harus didekripsi sebelum dibaca, diubah, atau dihapus. Enkripsi sangat berkaitan erat dengan tingkat performansi sistem. Pengenkripsian terhadap semua data akan sangat berpengaruh terhadap performansi sistem. Ketersediaan data adalah

sebuah aspek penting dari keamanan, dan jika pengenkripsian data membuat data menjadi tidak tersedia, maka dapat dikatakan enkripsi yang dilakukan telah menimbulkan masalah keamanan baru.

Sebaliknya, hal yang memberikan manfaat adalah meakukan enkripsi terhadap data yang tersimpan secara offline. Sebagai contoh, sebuah organisasi dapat menyimpan data cadangan (backup) untuk satu perioda selama 6 bulan atau 1 tahun, pada suatu lokasi terpisah. Tentu saja sebelum hal ini dilakukan, harus dipastikan bahwa tetap terdapat kontrol akses terhadap data tersebut. Bagaimanapun juga, mungkin terdapat keuntungan dari pengenkripsian data sebelum disimpan, dan karena data ini tidak diakses secara online, maka tidak akan mempengaruhi performansi sistem.

TANTANGAN ENKRIPSI

1. Data yang Terindeks

Beberapa kesulitan timbul dalam penanganan data terindeks. Sebagai contoh, sebuah perusahaan mungkin menggunakan nomor identitas nasional sebagai nomor identifikasi untuk karyawannya. Perusahaan ini berpendapat nomor identitas ini merupakan informasi yang sangat sensitif, sehingga ingin melakukan enkripsi data pada kolom EMPLOYEE_NUMBER pada tabel EMPLOYEES. Karena EMPLOYEE_NUMBER memiliki harga yang unik, penggunaan indeks akan meningkatkan performansi.

Jika mekanisme DBMS_OBFUSCATION_TOOLKIT digunakan untuk melakukan enkripsi data pada kolom tersebut, maka sebuah indeks pada kolom tersebut akan mengandung harga yang terenkripsi. Indeks tetap dapat digunakan untuk pengecekan kesamaan, dan tidak dapat digunakan untuk keperluan lain. Sebagai contoh, kode berikut dapat digunakan untuk mengambil informasi nama dari seorang karyawan dengan nomor identifikasi yang diberikan.

```
SELECT * FROM emp WHERE employee_number =  
DBMS_OBFUSCATION_TOOLKIT.DESEncrypt(key, 12345);
```

Sebagai alternatif, sebuah perusahaan yang ingin melakukan enkripsi terhadap nomor identitas nasional tersebut dapat membuat sebuah identifier unik untuk karyawannya, dan membuat sebuah indeks untuk nomor karyawan ini, akan tetapi mempertahankan nomor

karyawan dalam teks yang tidak terenkripsi. Nomor identitas ini dapat berupa kolom terpisah, dan sebuah aplikasi dapat melakukan enkripsi dan dekripsi terhadap nilai tersebut secara tepat.

2. Manajemen Key

Manajemen key, baik meliputi pembangkitan dan penyimpanan yang aman dari cryptographic key, merupakan aspek penting dari enkripsi. Jika key tersebut tidak tersimpan dengan baik, maka akan menjadi jauh lebih mudah untuk merusak enkripsi tersebut.

3. Pembangkitan Key

Pembangkitan key merupakan aspek penting dari enkripsi. Key dibangkitkan secara otomatis melalui sebuah pembangkit nomor acak (random-number generator), dari sebuah umpan kriptografi. Jika pembangkit nomor acak tersebut merupakan sebuah pembangkit nomor yang andal, maka key yang dibangkitkan mungkin merupakan key yang aman. Netscape telah mempublikasikan lubang dalam implementasi SSL yang mereka lakukan beberapa tahun yang lalu bahwa ditemukan fakta bahwa 2 atau 3 elemen dari pembangkit nomor acak mereka ternyata tidak benar-benar bekerja secara acak (serial nomor mesin dan nomor hari). Key enkripsi untuk SSL memiliki panjang key yang efektif sebanyak 9 bit daripada 40 bit seperti yang sering disarankan, karena kelemahan mekanisme pembangkitan key ini. Sebuah key untuk SSL dapat dengan mudah dipecahkan, bukan karena algoritma enkripsi yang lemah, akan tetapi karena key tersebut didapatkan dengan mudah.

4. Penyimpanan Key

Penyimpanan key merupakan aspek yang paling penting dan paling sulit dari mekanisme enkripsi. Untuk mengembalikan data yang terenkripsi dengan sebuah key simetris, key tersebut harus dapat diakses oleh aplikasi atau user yang akan melakukan enkripsi tersebut. Key tersebut harus cukup mudah untuk diambil sehingga user dapat mengakses data yang terenkripsi pada saat dibutuhkan tanpa pengurangan performansi secara drastis. Akan tetapi key tersebut juga harus tersimpan dengan cukup aman sehingga tidak dapat diakses oleh pihak yang tidak berwenang. Tiga pilihan penyimpanan key yang dapat dilakukan adalah :

Menyimpan key pada basis data

Penyimpanan data pada basis data tidak selalu dapat menyediakan keamanan yang 'tidak tertembus', jika yang ingin dilakukan adalah menghindari kemungkinan pengaksesan data terenkripsi oleh DBA (karena seorang DBA yang memiliki semua privilege dapat mengakses tabel dengan key enkripsi), akan tetapi hal tersebut dapat memberikan keamanan yang baik dari ancaman pihak yang tidak berwenang.

Dengan sedikit tambahan yang dilakukan pada mekanisme enkripsi, dapat memberikan hasil enkripsi yang jauh lebih sulit untuk dipecahkan. Sebagai contoh, enkripsi terhadap Social Security Number (SSN) dapat dilakukan dengan cara melakukan beberapa transformasi data tambahan terhadap employee_number sebelum digunakan untuk mengenkripsi SSN, misalnya melakukan proses XOR antara employee_number dengan tanggal lahir karyawan.

Sebagai perlindungan tambahan, pada sebuah enkripsi yang dilakukan dengan PL/SQL, bagian body dari data yang terenkripsi dapat dibungkus (wrapped) dengan menggunakan perangkat pembungkus sehingga data tersebut tidak dapat dibaca. Sebuah fungsi kemudian dapat digunakan untuk memanggil fungsi DBMS_OBFUSCATION_TOOLKIT enkripsi atau dekripsi dengan key yang termuat dalam paket tersebut.

Selain mekanisme pembungkusan tersebut tidak dapat dipecahkan oleh pihak yang tidak berwenang, mekanisme tersebut juga membuat jauh lebih sulit bagi seorang penyusup untuk mendapatkan key yang digunakan. Untuk membuatnya menjadi lebih sulit, key dapat dibagi dalam paket tersebut, dan kemudian digunakan prosedur untuk menggabungkannya kembali sebelum digunakan.

Keuntungan dari penyimpanan key dalam basis data ini adalah sebagai berikut :

- User yang memiliki akses secara langsung terhadap tabel tidak dapat melihat data dalam bentuk yang jelas, atau tidak dapat mengambil key yang digunakan untuk melakukan dekripsi terhadap data.

- Akses untuk melakukan dekripsi terhadap data dapat dikontrol melalui sebuah prosedur yang memilih data (yang terenkripsi), mengambil key dekripsi dari tabel key, dan mentransformasikannya sebelum dapat digunakan untuk melakukan dekripsi terhadap data.
- Algoritma transformasi data disembunyikan dari pihak yang berwenang dengan membungkus prosedur
- Akses SELECT baik untuk tabel data dan tabel key tidak menjamin bahwa user yang memiliki akses ini dapat melakukan dekripsi terhadap data, karena key telah ditransformasikan sebelum digunakan.
- Kelemahan dari pendekatan ini adalah user yang mempunyai akses SELECT baik untuk tabel data dan tabel key yang dapat memiliki key dari algoritma transformasi, dapat memecahkan skema enkripsi ini.

Menyimpan key pada sistem operasi

Menyimpan key pada sistem operasi (misalnya dalam sebuah flat file) merupakan sebuah pilihan lain. Oracle9i memungkinkan panggilan terhadap PL/SQL yang dapat digunakan untuk mengambil key enkripsi. Jika key tersimpan dalam sistem operasi, dan melakukan panggilan terhadapnya, maka data tersebut akan berada dalam keadaan aman sebatas perlindungan yang dilakukan terhadap sistem operasi. Jika kepedulian utama kita untuk menyimpan key dalam basis data adalah basis data dapat disusupi melalui sistem operasi, maka penyimpanan key pada sistem operasi dapat mempermudah penyusup untuk mengambil data yang terenkripsi daripada menyimpan key tersebut pada basis data.

Menyerahkan penyimpanan key kepada user

Pada teknik ini, user menyimpan key untuk digunakan dengan aplikasi. Metoda ini mungkin merupakan metoda yang paling mengandung resiko karena 40% dari panggilan untuk help desk berasal dari user yang melupakan password mereka, dan dari hal ini dapat terlihat resiko memberikan wewenang kepada user untuk mengatur penyimpanan key enkripsi. Dalam pendekatan ini, kemungkinan yang dapat terjadi adalah user melupakan sebuah key enkripsi atau menyimpan key pada suatu tempat yang tidak terlindungi, yang dapat menyebabkan kelemahan aspek keamanan. Jika

seorang user melupakan sebuah key enkripsi atau meninggalkan sebuah perusahaan, maka data tersebut tidak akan dapat dikembalikan kedalam bentuk asalnya.

5. Transmisi Key

Jika key yang digunakan akan dikirimkan oleh aplikasi kepada basis data, maka harus dilakukan enkripsi terhadap key tersebut. Penggunaan enkripsi jaringan, seperti yang disediakan oleh Oracle Advanced Security akan melindungi data selama berada dalam keadaan transit, dari kemungkinan modifikasi atau intersepsi, termasuk key kriptografi.

6. Perubahan Key Enkripsi

Saran yang bijak untuk keamanan adalah dengan mengubah key enkripsi secara periodik. Untuk data tersimpan, hal ini membutuhkan proses dekripsi terhadap data secara periodik, dan melakukan proses enkripsi ulang terhadap data dengan key lain. Hal ini mungkin dilakukan pada saat data tidak sedang diakses oleh siapapun, yang menimbulkan tantangan lain, khususnya untuk aplikasi berbasis web untuk enkripsi nomor kartu kredit, karena tentu saja mematikan aplikasi untuk penggantian key enkripsi tidak mungkin dilakukan.

Disamping itu perlu juga dipertimbangkan kemungkinan terjadi sesuatu hal yang tidak diinginkan selama pergantian key tersebut. Jika tidak, akan terdapat kemungkinan tidak dapat dilakukan proses dekripsi terhadap data karena pergantian key yang gagal.

SOLUSI ORACLE UNTUK ENKRIPSI DATA TERSIMPAN

Oracle Advanced Security menyediakan :

1. Algoritma Enkripsi

Beberapa algoritma enkripsi yang disediakan oleh Oracle adalah :

DES

Prosedur dan fungsi dalam DES membutuhkan sebuah key sepanjang 64 bit, yang berjalan dalam mode chiper block chaining (CBC).

Triple DES

Triple DES dapat berjalan baik pada mode 2key atau 3-key. Mode 2-key membutuhkan sebuah key sepanjang 128 bit, sementara mode 3-key membutuhkan sebuah key dengan panjang minimal 192 bit. Kedua mode tersebut menggunakan mode outer cipher block chaining.

2. Algoritma Integritas : MD5, SHA1

3. Enkripsi berbasis Java

Oracle mengimplementasikan 2 tipe driver JDBC. Tipe JDBC Thick digunakan untuk client C-based Net8, sedangkan tipe JDBC Thin mendukung applet yang dapat didownload. Implementasi Oracle Advanced Security Java memungkinkan adanya koneksi yang aman dari client Thin JDBC ke basis data. Pada enkripsi berbasis Java ini, algoritma yang digunakan adalah DES, RC4 (dengan menggunakan key sepanjang 40 bit dan 56 bit), dan fungsi Hash MD5. Terdapat beberapa keuntungan dari mekanisme enkripsi berbasis Java, yaitu :

- ❑ Developer dapat membangun applet Java yang berfungsi mentransmisikan data melalui kanal yang aman.
- ❑ Koneksi yang aman antara server layer middle menggunakan Java Server Pages dengan Oracle9i
- ❑ Kanal yang terenkripsi antara Oracle9i dengan basis data lama yang memampukan ASO
- ❑ Menyempurnakan dukungan enkripsi yang diberikan oleh Oracle9i

V. AUTENTIKASI

Basis dari sistem keamanan adalah mekanisme identifikasi dan otorisasi user yang andal. Oracle9i mendukung sejumlah pilihan mekanisme autentikasi user, yaitu sebagai berikut :

AUTENTIKASI BERBASIS ORACLE

Dalam hal ini, yang digunakan adalah password, atau X.509 certificate. Pada autentikasi Oracle berbasis password, setiap user Oracle harus memiliki sebuah username dan password. Untuk dapat terhubung ke basis data, user yang diautentikasi secara tepat oleh sistem operasi harus memberikan username dan password basis datanya. Pada skema berbasis password, untuk menjamin keamanan, harus dipastikan bahwa password yang digunakan dapat diubah secara teratur, memiliki tingkat kompleksitas yang cukup tinggi, dan tidak mudah untuk diterka.

Oracle9i menyediakan fasilitas manajemen password yang andal secara built in. Hal ini memungkinkan administrator untuk :

- ☐ Menggunakan password dengan panjang minimum.
- ☐ Menjamin kompleksitas password (sebagai contoh, password memuat simbol atau angka, dan juga karakter alfabet).
- ☐ Menolak password yang dapat ditebak dengan mudah, seperti nama akhir dari seorang user atau nama perusahaan.

Administrator dapat mencegah adanya usaha penebakan password dengan mengunci account secara otomatis setelah sejumlah entry yang berisi password yang tidak tepat dilakukan. Password dapat dibuat habis masa berlakunya setelah satu periode tertentu untuk menjamin bahwa user mengubah passwordnya secara regular. Administrator dapat pula mencegah kemungkinan terjadinya penggunaan ulang password, baik secara permanen maupun untuk suatu periode waktu tertentu. Preferensi untuk password dapat diberikan kepada seluruh enterprise, kelompok user, ataupun user individu dengan menggunakan profil user, untuk menyediakan tingkat fleksibilitas yang lengkap untuk sebuah organisasi untuk mengimplementasikan pilihan keamanan yang diinginkan.

Dalam sebuah sistem terdistribusi, sebuah password yang dikirimkan dari client ke server dapat mengandung resiko keamanan. Jika password tersebut dikirimkan dalam bentuk yang tidak terenkripsi, penyusup yang mengintai data dapat membaca password tersebut. Protokol password Oracle menyediakan keamanan untuk komunikasi password antara client-server dan server-server dengan mengenkripsi password yang dikirimkan melalui sebuah jaringan. Protokol password Oracle menggunakan sebuah session key yang valid untuk sebuah usaha untuk melakukan koneksi tunggal ke satu basis data untuk mengenkripsi password user. Masing-masing usaha yang dilakukan untuk membuka

koneksi menggunakan sebuah key yang terpisah untuk enkripsi, membuat enkripsi semakin sulit untuk diuraikan. Setelah sebuah password yang terenkripsi dikirimkan kepada server, server akan melakukan proses dekripsi terhadapnya, dan kemudian melakukan proses enkripsi ulang terhadapnya dengan menggunakan algoritma Data Encryption Standard (DES) didasarkan pada algoritma enkripsi searah dan membandingkannya dengan password yang tersimpan dalam basis data. Jika keduanya sesuai, user akan terhubung ke basis data. Protokol password Oracle digunakan untuk mengenkripsi semua password pada saat terjadinya usaha pembukaan sebuah koneksi, baik koneksi lokal, koneksi dari client ke server, maupun koneksi antar server. Oracle9i juga mendukung administrasi jarak jauh yang dilindungi oleh password, bahkan ketika basis data tidak tersedia. User yang terhubung sebagai SYSDBA dan SYSOPER melakukan hubungan dengan menggunakan password yang bersifat user-specific, menyediakan akuntabilitas individual untuk user yang memiliki privilege ini.

AUTENTIKASI BERBASIS HOST

Fasilitas identifikasi dan autentikasi dari Oracle9i juga memungkinkan user untuk diautentikasi dengan menggunakan mekanisme sistem operasi, menggabungkan informasi username dan password dan memungkinkan user untuk memasuki sebuah aplikasi tanpa harus menspesifikasikan sebuah username dan password.

AUTENTIKASI BERBASIS PIHAK KETIGA

Oracle Advanced Security, sebuah pilihan untuk Oracle9i, mendukung teknologi autentikasi dari sejumlah pihak ketiga, seperti Kerberos, DCE, smart card, dan autentikasi biometric (Identix), dan juga integrasi dengan ISM dari Bull dan Access Manager dari ICL. Teknologi hardware dan software ini memverifikasi identitas seorang user dengan cara yang lebih andal daripada penggunaan password. Sebagai contoh, kartu SecurID memungkinkan autentikasi dengan 2 faktor – sesuatu yang dimiliki user (kartu) dan sesuatu yang diketahui user (sebuah PIN). Sebagian besar layanan autentikasi jariah ini juga memungkinkan mekanisme single sign-on untuk user. User mengautentikasi diri mereka sendiri hanya sebanyak 1 kali kepada sebuah layanan terpusat (pada Kerberos) dan kemudian dapat melakukan koneksi ke lebih dari satu aplikasi atau basis data tanpa memerlukan credential

tambahan. Disamping itu, perangkat apapun yang compliant dengan RADIUS (Remote Authentication Dial-In User Service) dapat diintegrasikan dengan Oracle9i untuk memungkinkan mekanisme autentikasi user yang andal. Integrasi Oracle9i dengan provider keamanan pihak ketiga menawarkan pilihan untuk customer diantara sejumlah mekanisme autentikasi yang andal dan layanan single sign-on.

AUTENTIKASI BERBASIS PUBLIC KEY INFRASTRUKTUR

Oracle9i memperkenalkan single sign-on untuk user Oracle melalui penggunaan X.509 digital certificate dan sebuah protokol autentikasi yang dimilikinya. Keuntungan dari X.509 certificate adalah ia dapat digunakan untuk mengidentifikasi sebuah individu dalam suatu organisasi secara unik, sehingga memungkinkan autentikasi yang andal. Disamping itu, seorang user hanya perlu mengingat password untuk membuka Oracle walletnya, dan tidak perlu mengingat begitu banyak password. Sertifikat dan key private yang termuat dalam wallet digunakan untuk mengautentikasi user untuk sejumlah layanan, termasuk server aplikasi dan server data, yang tidak lagi harus menyimpan dan mengatur password lokal untuk user.

Oracle Advanced Security menawarkan single sign-on berbasis PKI yang telah disempurnakan dengan menggunakan X.509v3 certificate untuk melakukan autentikasi melalui SSL, yang merupakan standar autentikasi Internet. Disamping mekanisme autentikasi yang andal, SSL memungkinkan kerahasiaan data jaringan dan integritas data untuk sejumlah tipe koneksi : LDAP (Lightweight Directory Access Protocol), IIOP (Internet Intra-ORB Protocol), dan Net8.

Oracle Wallet Manager memungkinkan manajemen credential user yang berbasis PKI, yaitu : private key user, sertifikat, dan daftar trustpoint, daftar root certificate yang dipercaya oleh user. Wallet ini dilindungi oleh enkripsi yang andal berbasis password.

Pada sebagian besar kasus, suatu user tidak membutuhkan akses terhadap wallet saat wallet tersebut telah dikonfigurasi, akan tetapi dapat dengan mengakses walletnya dengan menggunakan Oracle Enterprise Login Assistant, sebuah perangkat login yang sangat mudah digunakan yang menyembunyikan kompleksitas dari sebuah private key dan sertifikat dari

user. Ketika user telah berhasil membuka wallet tersebut dengan aman, mereka kemudian dapat melakukan koneksi terhadap sejumlah basis data melalui SSL, tanpa membutuhkan password tambahan.

AUTENTIKASI JARAK JAUH

Oracle Advanced Security memungkinkan adanya autentikasi user jarak jauh dengan menggunakan RADIUS, sebuah protokol standar yang digunakan untuk autentikasi user, otorisasi, dan akuntansi. RADIUS, sebuah standar yang diajukan oleh Internet Engineering Task Force (IETF) merupakan sebuah sarana yang populer untuk memampukan dilakukannya autentikasi user jarak jauh.

Oracle Advanced Security menyediakan sebuah interface yang dapat digunakan dengan layanan autentikasi yang diberikan pihak ketiga manapun yang mendukung protokol RADIUS. Keuntungan bagi customer adalah sejumlah perangkat autentikasi (misalnya token atau smart card) dapat digunakan untuk melakukan autentikasi kepada basis data Oracle9i, sepanjang mekanisme atau perangkat tersebut mendukung protokol RADIUS.

AUTENTIKASI MELALUI MIDDLE TIER

Pada aplikasi yang menggunakan sebuah middle tier yang padat, seperti pemantauan proses transaksi, penting untuk dapat menjaga identitas client yang melakukan koneksi ke layer ini. Salah satu keuntungan dari penggunaan middle tier adalah pengumpulan koneksi, untuk memungkinkan sejumlah user untuk mengakses sebuah server data tanpa mengharuskan masing-masing user tersebut memiliki koneksi yang terpisah. Pada lingkungan seperti ini, harus terdapat kemampuan untuk memulai dan memutuskan koneksi dengan sangat cepat, tanpa menimbulkan overhead seperti yang ditimbulkan jika tiap koneksi terhadap basis data dibangun secara terpisah dan masing-masing harus terautentikasi. Untuk lingkungan seperti ini, Oracle9i menawarkan autentikasi n-tier. Sebuah session dibuat melalui Oracle Call Interface, sehingga aplikasi dapat memungkinkan sejumlah session user dalam sebuah session tunggal basis data. Session ini memungkinkan

masing-masing user untuk diautentikasi oleh sebuah password basis data tanpa adanya overhead yang mungkin timbul dengan adanya koneksi basis data terpisah, disamping itu juga menjaga identitas user yang sebenarnya melalui middle tier.

AUTENTIKASI MUTUAL UNTUK KOMPUTASI TERDISTRIBUSI YANG AMAN

Autentikasi user merupakan satu hal penting, dan merupakan hal yang sama pentingnya dalam sistem terdistribusi untuk menjamin bahwa sejumlah elemen yang berpartisipasi dalam jaringan – termasuk server aplikasi, server web, server basis data – memberikan identitas yang sebenarnya. Sebagai contoh, basis data A mencoba mengakses basis data B, membutuhkan jaminan bahwa basis data B benar-benar basis data B, begitu pula sebaliknya.

Oracle9i memungkinkan transaksi terdistribusi yang aman dengan mekanisme autentikasi basis data yang andal tanpa pengungkapan credential. Autentikasi basis data mutual dan autentikasi user yang andal dicapai dengan X.509v3 certificate, tanpa menggunakan password atau sarana “hard-coded” lain yang memiliki potensi menimbulkan masalah keamanan. Lebih dari itu, administrator dapat mengkonfigurasi sistem sehingga basis data hanya mempercayai sejumlah user tertentu untuk melakukan koneksi. Sebagai contoh, sebuah aplikasi AP dimungkinkan untuk mengakses informasi mengenai karyawan dalam basis data HR untuk melakukan proses pelaporan pajak. Tidak hanya basis data AP dan HR yang melakukan autentikasi mutual, akan tetapi basis data HR dapat memberikan akses hanya kepada user tertentu dalam AP yang membutuhkan akses terhadap informasi tersebut.

VI. VIRTUAL PRIVATE DATABASE

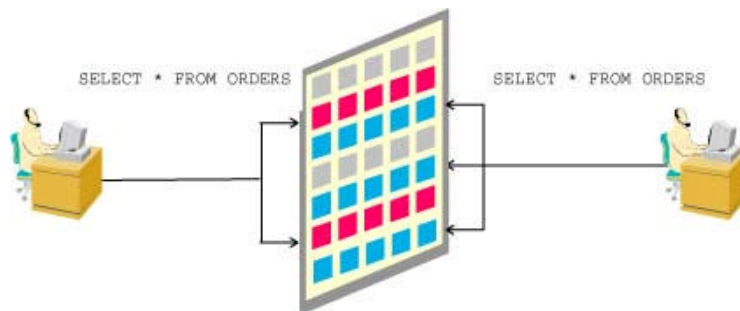
Pertumbuhan peran Internet bukan hanya sebagai sarana pemberian informasi untuk customer, akan tetapi juga sarana transaksi online, telah meningkatkan kebutuhan keamanan secara dramatis. Pemberian akses langsung kepada customer dan partner terhadap sistem mungkin mengurangi biaya yang dibutuhkan, memberikan layanan yang lebih baik, dan informasi yang lebih akurat, akan tetapi menimbulkan tantangan baru. Organisasi bukan

hanya dituntut untuk menjaga data dari kemungkinan penyusupan, akan tetapi mereka juga harus memisahkan data secara tepat, pada umumnya untuk level customer atau user individu.

Kecenderungan lain yang dilakukan oleh komunitas perusahaan adalah peningkatan fokus pada kompetensi dan mekanisme outsourcing terhadap tugas, seperti human resource, customer support, online ticketing, dan Web storefront. Sebagian besar perusahaan tersebut tertarik pada penyediaan lingkungan “hosting”, dengan sebuah infrastruktur yang terancang dengan baik dan terkomputasi, akan tetapi menghadapi tantangan dalam perancangan sistem yang menjaga data dari masing-masing perusahaan tetap terpisah dan aman satu dengan yang lain, dan tetap memungkinkan adanya personalisasi dan pilihan metoda akses data terbaik yang sesuai dengan kebutuhan masing-masing individu.

Masalah lain adalah, jika mekanisme kontrol akses diletakkan pada sebuah aplikasi, maka user mungkin melakukan bypass terhadap keamanan aplikasi tersebut. Hal ini menyebabkan organisasi harus menghabiskan sejumlah uang untuk mengimplementasikan keamanan data dalam setiap aplikasi yang mengakses data, sebuah praktek yang tidak hanya sia-sia dan duplikatif, akan tetapi juga sering menyebabkan implementasi yang tidak aman.

Oracle9i mengakomodasi adanya keragaman kebutuhan keamanan dengan memperkenalkan Virtual Private Database : server-enforced, fleksibel, kontrol akses fine-grained berdasarkan pada konteks keamanan. Kombinasi ini memungkinkan mekanisme kontrol akses dimana setiap user mendapat akses data dengan jaminan pemisahan data fisik. Masing-masing user mengakses datanya seolah-olah data tersebut tersimpan dan dikelola dalam sebuah sistem yang terpisah secara fisik.



Gambar 4. Virtual Private Database :
Customer hanya dapat melihat ordernya sendiri

KEUNTUNGAN VIRTUAL PRIVATE DATABASE

Virtual Private Database dari Oracle9i memiliki keuntungan sebagai berikut :

Pengurangan Biaya

Organisasi dapat menghasilkan penghematan biaya dalam jumlah besar dengan membangun keamanan hanya sekali, pada server data, daripada membangun sarana keamanan yang sama pada masing-masing aplikasi yang mengakses data.

Menghilangkan masalah keamanan aplikasi

User tidak akan melakukan bypass kebijakan keamanan yang dilekatkan pada aplikasi karena kebijakan keamanan berhubungan langsung dengan data. Kebijakan keamanan yang sama dilakukan secara otomatis oleh server data, terlepas dari bagaimana cara user mengakses data, baik melalui alat pembuat report, sebuah query, atau melalui sebuah aplikasi.

Kesempatan Bisnis Baru

Beberapa waktu yang lalu, organisasi tidak dapat memberikan akses langsung kepada customer dan partner terhadap sistem produksi mereka, karena jika hal ini dilakukan, maka tidak ada cara bagi mereka untuk menjaga keamanan data. Perusahaan hosting Internet tidak dapat menyediakan data untuk sejumlah perusahaan yang tersimpan dalam server data yang sama, karena mereka tidak dapat memisahkan data dari masing-masing perusahaan tersebut. Hal tersebut saat ini dimungkinkan, karena adanya mekanisme kontrol akses yang memungkinkan pengamanan data dilakukan oleh server dengan jaminan pemisahan data fisik.

Keamanan Yang Diperluas

Kontrol akses fine-grained memungkinkan customer untuk memperluas mekanisme kontrol akses yang telah disediakan oleh Oracle9i kedalam level kedetailan yang lebih baik daripada sebelumnya.

Sebagian besar aplikasi membatasi akses data dengan menggunakan view. Customer dapat menambahkan mekanisme kontrol akses yang lebih baik terhadap view untuk

meningkatkan tingkat keamanan aplikasi berbasis view, dan menghindari penulisan ulang aplikasi.

Dengan dimungkinkannya kebijakan keamanan dilekatkan kedalam tabel maupun view menyebabkan customer memiliki fleksibilitas yang mereka butuhkan untuk memperluas keamanan dari aplikasi yang telah ada dengan menggunakan view, atau dengan menghubungkan kebijakan keamanan mereka secara langsung dengan tabel, sesuai pilihan mereka.

KEBIJAKAN KEAMANAN GRANULAR

Kontrol akses fine-grained diimplementasikan pada table atau view terpilih. Sebagai contoh, untuk melakukan kebijakan keamanan “customer dapat melihat pesannya sendiri, akan tetapi tidak dapat melihat pesanan orang lain” dalam sebuah aplikasi pemesanan, seorang customer mungkin hanya membutuhkan kontrol akses fine-grained pada tabel ORDER dan ORDER_LINES, dan bukan pada semua tabel yang digunakan oleh aplikasi tersebut. Melekatkan kebijakan keamanan pada tabel atau view (dan bukannya membuat kebijakan keamanan yang diterapkan pada sistem secara keseluruhan) memungkinkan keamanan fine-grained digunakan hanya pada saat dibutuhkan.

QUERY YANG TERMODIFIKASI SECARA DINAMIS.

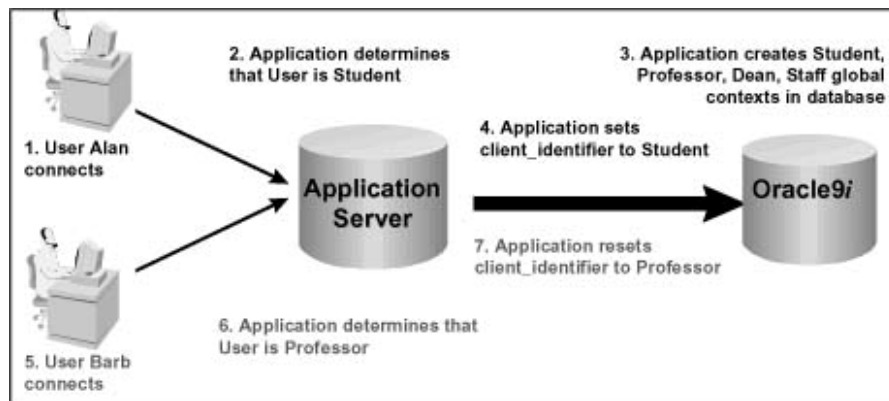
Kontrol akses fine-grained terletak pada modifikasi query secara dinamis untuk melakukan kebijakan keamanan pada obyek yang berhubungan dengan kebijakan tersebut. Dalam hal ini, query mengacu kepada pernyataan pemilihan dari sebuah tabel atau view, termasuk akses data melalui sebuah query untuk melakukan update, insert, atau delete, atau subquery, atau hanya pernyataan yang dimulai dengan SELECT.

Kontrol akses fine-grained dimungkinkan dengan menambahkan satu atau lebih kebijakan keamanan pada tabel atau view, yang diimplementasikan dengan sebuah fungsi. Seorang user yang mengakses tabel dengan kebijakan keamanan yang terdapat padanya, baik secara langsung maupun tidak langsung, menyebabkan server data memanggil fungsi keamanan tersebut, yang akan mengembalikan sebuah kondisi kontrol akses yang disebut

predikat. Oracle9i menulis ulang query secara dinamis dengan menambahkan predikat tersebut (klausa WHERE) pada pernyataan SQL user, transparan terhadap user. Sebuah fungsi dapat menyediakan fleksibilitas yang baik dalam memberikan kondisi kontrol akses : ia dapat mengembalikan predikat yang berbeda untuk masing-masing user, masing-masing kelompok user, atau masing-masing aplikasi.

KONTEKS APLIKASI YANG AMAN

Sebagian besar organisasi menginginkan keputusan kontrol akses dibuat berdasarkan sesuatu yang bersangkutan dengan user (seperti peran user dalam organisasi, unit organisasional user, dan apakah user tersebut merupakan customer atau partner). Konteks aplikasi memberikan developer aplikasi sebuah mekanisme yang mudah untuk mendefinisikan, membuat, dan memvalidasi atribut keamanan untuk menciptakan kontrol akses fine-grained dan meningkatkan kemampuan developer untuk mengimplementasikan Virtual Private Database dalam Oracle9i.



Gambar 5. Konteks Aplikasi Global mengkombinasikan kontrol aplikasi dan level basis data dalam sebuah lingkungan aman yang bersifat scalable

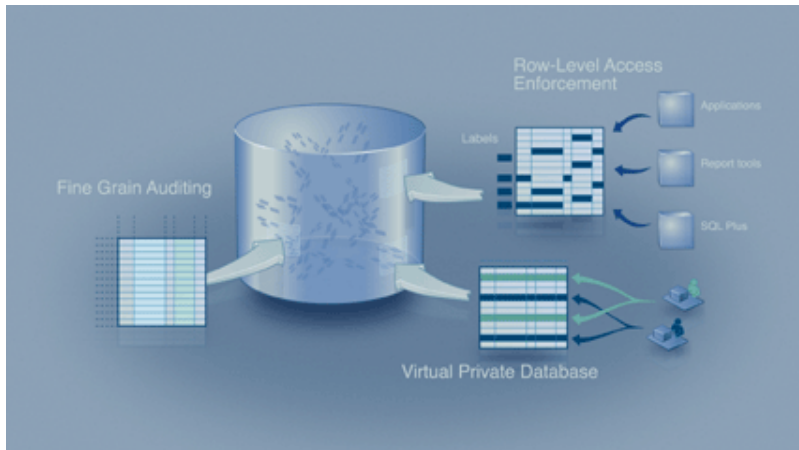
MEKANISME AKSES DATA

Pada Virtual Private Database, mekanisme akses data diatur pada level basis data, dengan beberapa hal penting sebagai berikut :

- Mekanisme kontrol akses fine-grained dicapai dengan cara melakukan kontrol akses pada server secara otomatis pada server (terlepas dari bagaimana cara akses data tersebut dilakukan).
- Konteks aplikasi akan menentukan kondisi kontrol akses
- Kebijakan keamanan yang bersangkutan, diimplementasikan dengan menggunakan fungsi yang diletakkan pada tabel atau view.
- Tidak mungkin dilakukannya bypass pada keamanan menyebabkan tidak adanya kebutuhan untuk menggunakan banyak view untuk mengimplementasikan keamanan.

CARA KERJA VIRTUAL PRIVATE DATABASE

- ☐ Mengakses sebuah obyek dengan kebijakan yang melekat padanya akan memanggil kebijakan tersebut secara otomatis, dalam hal ini kebijakan tersebut berupa fungsi.
- ☐ Fungsi kebijakan tersebut mengembalikan sebuah predikat (sebuah kondisi WHERE).
- ☐ Konteks aplikasi menentukan kebijakan yang tepat untuk masing-masing user.
- ☐ Oracle9i secara dinamis menulis ulang statement SQL dengan menambahkan predikat tersebut.



Gambar 6. Berbagai Fitur Keamanan dari Oracle9i disusun secara berlapis untuk melindungi data dari berbagai ancaman keamanan dan penyalahgunaan privilege akses

VII. AUDITING

Sebuah aspek yang penting dari kebijakan keamanan adalah mengelola catatan mengenai aktivitas sistem untuk menjamin bahwa user memiliki akuntabilitas untuk setiap aksi yang dilakukannya. Auditing memberikan bantuan dalam menghalangi user yang tidak berwenang. Mekanisme ini sangat berguna untuk menjamin bahwa user tidak menyalahgunakan wewenang yang dimilikinya. Oracle9i menyediakan fasilitas audit yang sangat luas.

AUDITING GRANULAR

Fasilitas audit dari Oracle9i memungkinkan sebuah bisnis untuk melakukan audit terhadap aktivitas basis data melalui statement, penggunaan privilege sistem, melalui user, atau melalui obyek. Sebagai contoh, seseorang dapat melakukan audit aktivitas umum seperti semua koneksi user terhadap basis data, dan aktivitas khusus seperti pembuatan tabel yang dilakukan user. Seseorang juga dapat melakukan audit terhadap hanya operasi yang sukses, atau hanya terhadap operasi yang tidak sukses. Sebagai contoh, pengauditan statement SELECT yang tidak sukses mungkin menangkap user yang mencoba mengakses data yang tidak berhak mereka lihat. Seseorang dapat mengatur pilihan default obyek audit,

sehingga obyek baru akan secara otomatis memiliki fasilitas audit sejak pertama kali obyek tersebut dibuat (sebagai contoh, sebuah tabel baru yang diaudit secara otomatis untuk statement SELECT yang tidak sukses). Catatan hasil audit ini tersimpan dalam sebuah tabel Oracle9i, membuat informasi ini dapat dilihat melalui query, atau aplikasi lain yang tepat.

AUDIT SECARA EFISIEN

Oracle9i mengimplementasikan proses audit secara efisien : statement dibangkitkan hanya satu kali baik untuk dieksekusi maupun untuk proses auditing. Disamping itu, proses audit diimplementasikan pada server yang bersangkutan, bukan pada server tambahan terpisah yang mungkin memiliki situasi yang sangat berbeda dengan statement yang sedang dieksekusi. Granularitas dan ruang lingkup dari pilihan audit ini memungkinkan customer Oracle untuk mencatat dan memonitor kegiatan basis data tertentu tanpa menyebabkan overhead performansi yang sering disebabkan oleh kegiatan audit pada umumnya.

AUDIT YANG DIPERLUAS

Untuk menyimpan informasi yang tidak secara otomatis terdapat dalam catatan audit, Oracle9i dapat menggunakan trigger untuk merancang kondisi audit dengan tujuan yang lebih spesifik dan melakukan audit terhadap isi catatan tersebut. Trigger basis data merupakan sekumpulan statemen PL/SQL atau Java yang didefinisikan oleh user, dan disimpan dalam bentuk terkompilasi. Tidak seperti stored procedure, yang dipanggil secara eksplisit oleh user, trigger basis data secara otomatis dieksekusi dalam server data berdasarkan kejadian tertentu yang telah dispesifikasikan sebelumnya. Sebuah trigger didefinisikan untuk dieksekusi baik sebelum atau sesudah proses insert, update, atau delete, sehingga saat operasi tersebut dilakukan pada tabel tersebut, trigger secara otomatis akan dijalankan.

AUDIT UNTUK APLIKASI THREE-TIER

Sebagian besar aplikasi 3-tier mengautentikasi user pada middle tier, kemudian monitor TP atau server aplikasi terhubung sebagai user dengan super-privilege dan melakukan aktivitas atas nama semua user. Dengan Oracle9i, customer Oracle bukan hanya dapat menjaga identitas client yang sesungguhnya pada middle tier dan melaksanakan

privilege minimum melalui sebuah middle tier, akan tetapi dapat pula melakukan proses audit. Catatan audit Oracle9i mencatat baik user yang telah melakukan log in dan menginisiasi koneksi, dan user yang mengatasnamakan dirinya untuk melakukan kegiatan tersebut.

AUDIT SECARA AKTIF

Sementara sebuah fasilitas audit dapat mencatat usaha yang dilakukan untuk melanggar keamanan basis data, atau bahkan pelanggaran itu sendiri, fasilitas ini tidak memberikan informasi kepada administrator pada saat pelanggaran tersebut terjadi. Dalam kenyataannya, mungkin beberapa jam, beberapa hari, atau beberapa bulan setelahnya, baru ditemukan percobaan pelanggaran oleh administrator pada saat ia melihat catatan audit. Sebagai konsekuensinya, jika salah satu tujuan dari proses audit adalah untuk mendeteksi adanya kemungkinan pelanggaran keamanan, maka harus terdapat sebuah fasilitas alarm untuk memberikan alert kepada administrator yang bersangkutan saat basis data atau sistem operasi mendeteksi adanya tingkah laku yang mencurigakan. Saat trigger digunakan untuk melakukan proses audit, Oracle9i dapat mengirimkan sebuah alarm kepada sebuah proses yang sedang menunggu, untuk memberikan informasi bahwa sebuah aktivitas yang berpotensi melakukan pelanggaran keamanan sedang terjadi.

KESIMPULAN

- Dengan menyediakan mekanisme perlindungan terhadap data secara menyeluruh dan mendalam, keamanan yang berskala Internet, dan mekanisme keamanan yang ditujukan khusus untuk aplikasi hosting, Oracle9i merupakan sebuah platform ideal untuk membangun aspek keamanan dalam sebuah sistem.
- Dengan adanya fasilitas integrasi directory, Oracle memiliki fasilitas keamanan yang berskala Internet.
- Virtual Private Database menempatkan Oracle jauh dari kompetisi.

- Oracle9i memiliki tingkat fleksibilitas tinggi, dengan beragam pilihan solusi untuk masalah keamanan.

- Oracle memungkinkan terjadinya kerjasama (interoperability) dengan penyedia solusi keamanan terdepan lainnya.

- Oracle memberikan jaminan untuk :
 1. Keamanan yang dilakukan pada server data secara andal
 2. Standar yang disesuaikan dengan perkembangan Internet untuk akses data, enkripsi, dan autentikasi (LDAP, SSL, X.509)
 3. Layanan integrated security dan directory untuk keperluan pemusatan dan manajemen user enterprise secara menyeluruh.
 4. Stamp of approval yang diperoleh melalui verifikasi secara independen yang dilakukan terhadap produk yang menawarkan solusi keamanan

DAFTAR PUSTAKA

1. Browder, Kristy, "Oracle9i New Features and Secure Solutions"
2. Heimann, John, Ng, Raymond, "Oracle9i For EBusiness : Security For Your EBusiness Applications"
3. Sinha, Rajiv, "Oracle9i Security and E-Business"
4. _____, "Oracle Advanced Security : Security and Directory Integration", November 1999
5. _____, "Lowering the Cost of Enterprise Security", November 1998
6. Wessman, Davidson, Mary Ann, Van Le, "Everybody Has Secrets : New Solutions in Stored Data Encryption", Oracle Corporation
7. _____, "Database Security in Oracle9i"
8. _____, "Database Encryption in Oracle9i", February 2001
9. _____, "Oracle Advanced Security : Enterprise User Management"
10. _____, "Oracle9i Label Security – Controlling Access to Data", January 2002
11. _____, "Oracle9i Label Security", January 2002
12. _____, "Oracle Policy Manager", October 2000
13. Smith, Howard, "Hack Proofing Oracle", Oracle Corporation UK Limited
14. _____, "Oracle9i Privacy Protections", October 2002
15. _____, "Extending the Life of Database Applications", 2003
16. _____, "Oracle Identity Management Concepts and Architecture", December 2003
17. Heimann, John H, "Securing Three-Tier Systems with Oracle8i", Oracle
18. Finnigan, Pete "Exploiting and Protecting Oracle", August 2001
19. _____, "Unbreakable : Oracle's Commitment to Security", February 2002
20. _____, "The Virtual Private Database in Oracle9iR2", January 2002
21. <http://otn.oracle.com/oramag/oracle/02-mar/o22break.html> "Building Unbreakable Systems with Oracle"
22. http://otn.oracle.com/oramag/webcolumns/2003/techarticles/newman_hackproof_pt2.html, Newman, Aaron "Hack-Proofing Oracle9i Application Server"
23. <http://otn.oracle.com/oramag/oracle/03-jul/o43security.html>, Kuhn, Darl, Roughton, Steve, "Now Securing Every Row"