*Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005)*
*Yogyakarta, 18 Juni 2005*
*ISBN: 979-756-061-6*

# IMPLEMENTASI PENGAMANAN DATABASE DENGAN ORACLE SECURITY SERVER

**Ilham M. Said, Harunur Rasyid**
*Staff Pengajar Jurusan Teknik Informatika*
*Universitas Muhammadiyah Gresik*

**Abstrak**

*Dalam beberapa tahun terakhir ini, data yang tersimpan di dalam sebuah perusahaan yang mengunakan aplikasi database tumbuh secara ekponensial. Seiring dengan meningkatnya akses terhadap data tersebut meningkat pula faktor resiko keamanannya. Keamanan terhadap data yang tersimpan dalam database menjadi sesuatu yang sangat penting, terutama menghadapi isu-isu keamanan data yaitu: kerahasian, othentikasi, keutuhan dan bukti tindakan. Oracle Security Server menjadi sebuah alternatif solusi untuk memecahkan keempat isu keamanan data diatas. Oracle sebagai salah satu produk database yang berbasis enterprise telah memberikan suatu lingkungan yang cukup lengkap dalam menangani masalah data dan keamanan. Selanjutnya solusi tersebut diaplikasikan berupa setting aplikasi yang terdiri dari penerapan othentikasi dengan menggunakan RADIUS, penerapan integrity dengan menggunakan metode enkripsi MD5, dan penerapan enkripsi dengan menggunakan metode DES.*

*Hasil uji coba aplikasi menunjukkan bahwa aplikasi ini telah menunjukkan kemampuannya secara maximal dalam pengamanan jaringan. Dengan adanya permintaan login tidak hanya ke database tetapi juga login ke sistem. Ketika login ke database betul tetapi login ke sistem salah, koneksi tetap akan di tolak.*

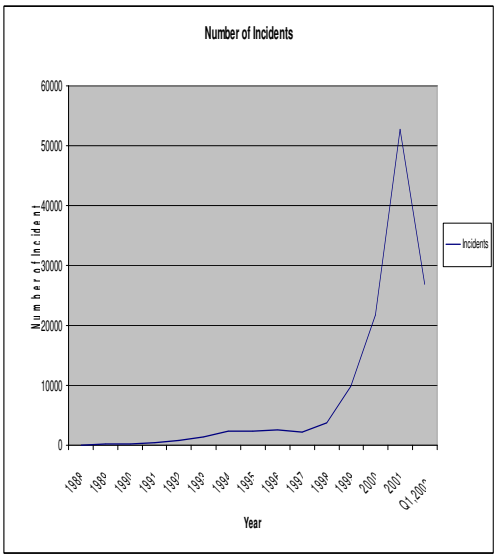
***Kata Kunci**: Oracle, Radius, Md5 Dan Des*

## 1. Pendahuluan

Security adalah salah satu kebutuhan dasar manusia *(Robert J Muller*, 1997). Pada era internet seperti sekarang ini, security menjadi hal yang sangat penting dalam menjamin setiap aktifitas yang dilakukan oleh manusia ketika melakukan suatu transaksi melalui internet. Karena pada dasarnya jaringan komputer Internet yang sifatnya publik dan global adalah tidak aman (*Onno W Purbo dan Tony Wiharjito*, 2000). Ini dibuktikan dengan adanya kejahataan-kejahatan di dunia internet, seperti: pencurian nomer kartu kredit, pembobolan suatu sistem, baik dilakukan secara serius untuk merusak atau hanya sekedar iseng untuk memuaskan keingintahuan. Hal-hal diatas, dapat terjadi karena data yang terkirim dari satu komputer ke komputer lain akan melewati beberapa komputer, dimana memberi kesempatan kepada user untuk menyadap ataupun melakukan perubahan data tersebut. Security menjadi suatu syarat mutlak ketika suatu komputer terhubung dengan internet dapat dipertegas dengan laporan-laporan tentang insiden keamanan jaringan komputer seperti yang dapat ditunjukkan dengan data-data di bawah ini:

a. Tahun 1996, *U.S Federal Computer Incident Response Capability* (FedCIRC) melaporkan bahwa lebih dari 2500 insiden di sistem komputer atau jaringan komputer yang disebakan oleh gagalnya sistem keamanan atau adanya usaha membobol sistem keamanan (*David J. Icove*,1997 )
b. Juga di tahun 1996, *FBI National Computer Crime Squad*, Washington D.C, memperkirakan kejahatan komputer yang terdeteksi kutang dari 15 %, dan hanya 10 % angka itu yang dilaporkan (*David J. Icove*, 1997 )
c. Di Inggris, 1996 *NCC Inforamtion Security Breaches Survey* menunjukkan bahwa kejahatan kompuetr menaik 200 % dari tahun 1995 ke 1996. Survey ini juga menunjukkan bahwa kerugian yang diderita rata-rata US $30.000 untuk setiap insiden, ditunjukkan juga beberapa organisasi yang mengalami kerugian sampai US $1.5 juta (*Budi Rahardjo*,1998)
d. FBI melaporkan kasus persidangan yang berhubungan dengan kejahatan komputer meroket 950 % dari tahun 1996 ke tahun 1997, dengan penangkapan dari 4 ke 42, dan terbukti di pengadilan naik 88 %, dari 16 ke 30 kasus (*Budi Rahardjo*,1998)
e. Grafik yang menggambarkan kenaikan jumlah serangan ke internet (*CERT-CC Statistics*, 1988-2002*)*

*ISBN: 979-756-061-6*




**Gambar I.** Jumlah insiden

Ada beberapa contoh akibat jebolnya sistem keamanan yaitu:

a. 1988. Keamanan sistem mail *sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem internet. Kegiatan ini dapat diklasifikasikan sebagai "*denial of service attack*". Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar US $100. Di tahun 1990 Morris dihukum dan hanya didenda US $10,000
b. 10 Maret 1997. Seseorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport lokal (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachusetts (http://www.news.com/News/Item/0,4,20226,00.html )

Setelah melihat begitu vitalnya peran security, maka dalam merencanakan sistem keamanan jaringan komputer harus direncanakan dan harus dipahami dengan baik agar dapat melindungi investasi dan sumber daya di dalam jaringan komputer tersebut secara efektif. Ada beberapa hal yang harus diperhatikan sebelum melakukan perencanaan kebijaksanaan (*policy*) keamanan jaringan komputer, yaitu:

1. Resiko
   Resiko adalah suatu kemungkinan di mana penyusup berhasil mengakses komputer di dalam jaringan yang dilindungi.
2. Acaman (*threat*)
   Pada dasarnya, ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal ke dalam suatu jaringan computer.
3. Kelemahan
   Kelemahan mengambarkan seberapa kuat sistem keamana suatu jaringan komputer terhadap jaringan kompuer yang lain, dan kemungkinan bagi seseorang untuk mendapatkan akses ilegal ke dalamnya. (*Onno W Purbo dan Tony Wiharjito*, 2000)

Menurut Garfinkel (*Budi Rahardjo*, 1998) keamanan komputer meliputi 4 aspek yaitu:

1. *Privacy*
   Inti utama aspek privacy adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.
2. *Integrity*
   Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi.
3. *Authentication*
   Aspek yang berhubungan dengan metode untuk menyatakan bahwa informasi itu adalah asli, atau orang yang akan mengambil informasi atau orang yang memberikan informasi adalah orang dimaksud
4. *Availability*
   Aspek ini berhubungan dengan ketersediaan informasi ketika dibutuhkan

## 2. Metodologi Penelitian

a. Alat yang digunakan
   - Satu perangkat server
   - Satu perangkat komputer sebagai client
   - Software Oracle 8i Enterprise Edition
   - Buku, literatur dan data dari sumber lain yang mendukung
b. Prosedur Kerja
   - Membaca buku, literatur dan data-data
   - Melakukan instalasi Oracle 8i Enteprise Edition
   - Melakukan konfigurasi Oracle Advance Security 8.1.7

## 3. Landasan Teori

### 3.1 Security Server

Adalah salah satu konsep dalam security jaringan dimana terdapat sever yang bertugas sebagai authorization dan authentication terhadap segala sesuatu tindakan yang akan masuk ke dalan sistem.

### 3.2 Oracle Security Server

Adalah suatu produk security dimana mendukung authorization tersentral dan authentication terdistribusi di dalam lingkungan Oracle. Authentication memberikan keyakinan bahwa yang mengakses satu atau lebih Oracle Database Server adalah valid. Authorization memberikan kepastian bahwa sekelompok orang yang telah diberi hak akses hanya dapat

*ISBN: 979-756-061-6*

mengoperasikan menurut privelege dia dimana telah didefinisikan oleh seorang administrator.

### 3.3 Cryptography

Cryptography adalah suatu ilmu awal tentang security informasi melalui perubahan bentuk data dengan cara dibalik. Cryptography adalah ilmu besar sejak jaman kuno. Julius Caesar memakai kata sederhana untuk mengantikan *chiper* dimana masih mengacu pada namanya. Pembangunan komputasi seacara digital telah merevolusi cryptography, dan telah membuatnya lebih komplek dan aman.

Cryptography modern mengandung sebuah algoritma dan satu atau lebih kunci. Algoritma cryptography atau disebut juga chiper adalah sebuah prosedur untuk merubah data dari *plaintext* (bentuk yang masih terbaca) ke *chipertext* (bentuk yang sudah diproteksi) dan sebaliknya. Proses ini lebih umum disebut *encryption* dan proses kebalikannya disebut *decryption*. Kunci adalah sebagai parameter dari algoritma tersebut. Untuk melakukan perubahan dari plaintext ke chipertext atau sebaliknya dibutuhkan keduanya, kunci maupun algoritma.

Algoritma modern didesain sehingga user hanya tahu algoritma dan chipertextnya tetapi tidak dengan kuncinya, tidak dapat secara mudah merubah dalam bentuk plaintext dari chipertext yang telah diketahui. Normalnya algoritma di distribusikan secara luas atau umum ketika pengetahuan kunci dibatasi untuk user yang berhak, sejak pengetahuan tentang kunci menambahkan access ke data yang telah di enkripsi dengan kunci tersebut. Indikasi kekuatan algoritma dilihat dari ukuran kunci, yang mana menjadi hal yang sulit bagi para penyerang untuk merubah chipertext ke plaintext tanpa pengetahuan tentang kunci terlebih dulu.

### 3.4 Private-Key Cryptography

Private-Key Cryptography adalah algoritma cryptography yang didesain bahwa kunci yang dipakai untuk enkripsi maupun deskripsi adalah sama. Disebut juga dengan algoritma "secret-key" atau "symmetric-key".

Sebagai contoh jika Donna dan Ali ingin berkomunikasi, mereka harus tahu kunci rahasia yang akan digunakan, dan pertukaran kunci tersebut harus diyakini melewati proses yang aman. Jika kemudian Ali ingin berkomunikasi dengan Michael merekan harus memakai kunci rahasia yang lain sehinnga Donna tidak dapat membaca pesan mereka. Contoh dari aplikasi algoritma secret-key adalah:

a. Data Encryption Standard (DES) dari Nationat Institute of Standards and Technology (NIST), 1975
b. International Data Encryption Algorithm (IDEA) di bangun oleh 2 orang Swedia, 1990

Jika jumlah pemakai meningkat sebanyak (N) maka akan berbanding secara linear dengan jumlah peningkatan pasangan kunci rahasia sebanyak ($N^2$).

### 3.5 Public-Key Cryptography

Dipublikasikan pertama kali tahun 1976 oleh Martin Hellman dan Whitfield Diffie, Public-Key Cryptography disebut juga cryptography "asymetric" adalah suatu cryptography dimana kunci yang digunakan untuk enkripsi maupun deskripsi adalah berbeda. Masing-masing orang mendapatkan pasangan kunci yaitu public key dan private key. Public key dipublikasikan sedangkan private key tetap disimpan sendiri dijaga kerahasiannya.

### 3.6 Authentication

Adalah suatu teknik untuk menjamin keaslian data. Dapat digambarkan sebagai berikut: Jika Alice meng-enkripsi datanya dengan kunci private dia, maka setiap orang dapat membacanya dengan Alice public key, tetapi tak ada seoranpun dapat menduplikat enkripsi Alice tanpa mengakses Alice private key.

### 3.7 Digital Signature

Adalah suatu kuantitas yang diasosiasikan dengan pesan dimana hanya seseorang dengan pengetahuan terhadap private-key yang dapat mengenerate, dimana dapat di verifikasi melalui pengetahuan terhadap public key.

### 3.8 Perencanaan setting yang akan dilakukan dan hasil yang diharapkan

Untuk mendapatkan hasil ujicoba yang maximal maka akan dilakukan setting terhadap othentikasi, enkripsi dan integrity sebagai berikut ini. Untuk setting terhadap othentikasi akan dilakukan dengan melakukan beberapa langkah sebagi berikut:

1. Memilih metode yang digunakan adalah RADIUS
2. Melakukan setting Other Params, dengan memasukkan nilai-nilai sebagai berikut:
   a. Host Name: nama localhost kita
   b. Secret File: alamat tempat menyimpan secret file
   c. Port Number: 1645 (nilai default)
   d. Timeout: 15 (default)
   e. Number of Retries: 3 (default)
   f. Challenge Response: ON
   g. Default Keyword: masukkan challenge
   h. Interface Class Name: masukkan DefaultRadiusInterface
   i. Send Accounting: ON

*ISBN: 979-756-061-6*

Untuk setting terhadap integrity akan dilakukan dengan melakukan beberapa langkah sebagai berikut:
1. Metode yang dipilih adalah MD5
2. Integrity: Server
3. Cheksum Level: Accepted

Untuk setting terhadap enkripsi akan dilakukan dengan melakukan beberapa langkah sebagi berikut:
1. Metode yang dipilih adalah DES
2. Encryption: Server
3. Encryption Type: Accepted
4. Encryption Seed: karakter random acak dengan panjang 10 sampai 70 karakter.

Kemudian setelah setting telah dilakukan semua, maka tahap selanjutnya adalah ujicoba. Dengan menggunakan SQL*Plus, kita akan mencoba koneksi dengan database, dengan memakai user yang dikenali oleh database, jika kita berhasil memasukkan password database maka akan muncul window login lagi, dimana sekarang kita diharuskan memasukkan login ke sistem, jika benar maka kita baru akan masuk ke dalam database sesuai privellege yang dimiliki oleh user, jika salah dan sebanyak 3 kali maka koneksi ditolak. Jika dalam koneksi diatas, tidak muncul window login kedua berarti setting belum sempurna dilakukan, karena window login ke dua muncul akibat kita mengaktifkan oracle security dalam sistem oracle kita.

## 4. Implementasi Sistem

### 4.1 Konsep Oracle Security Server diterapkan dalam Oracle Advance Security

Konsep Oracle Security Server di terapkan oleh Oracle dengan produknya yang berlabel Oracle Advance Security 8.1.7 dalam keluarga Oracle 8i Enterprise Edition. Oracle Advance Security tidak terdapat dalam Oracle 8i Standart Edition. Oracle Advance Security bertujuan untuk memberikan keamanan dalam jaringan intern perusahaan dan jaringan perusahaan ke internet. Dengan fasilitas yang terintegrasi yaitu : enkripsi, authentication, pelayanan single sign-on dan protokol keamanan.

### 4.2 Fasilitas yang Terdapat dalam Oracle Advance Security

Oracle Advance Security menawarkan pengamanan data, integritas, single sign-on dan authorisasi akses dengan berbagai cara. Sebagai contoh: kita dapat menggunakan Secure Socket Layer atau Native Encryption untuk keamanan data. Untuk metode authentication banyak tawaran yang disediakan, misal: Kerberos, Smart Cards, dan Digital Certificates. Fasilitas Oracle Advance Security:
1. Privasi Data
2. Integritas Data
3. Authentication
4. Single Sign-On
5. Authorization

### 4.3 Implementasi Enkripsi Data dan Integritas Oracle Advance Securiy

Di dalam jaringan adalah memungkinkan client dan server intik mensupport lebih dari 1 algoritma enkripsi dan lebih dari 1 algoritma integrity. Ketika koneksi telah terjadi, server akan memilih algoritma yang dipakai , yang telah didefinisikan secara spesifik di dalam file bernama sqlnet.ora. Server akan mecari kecocokan antara algoritma yang diterapkan di server dengan algoritma yang diterapkan di client dengan cara membandingkan daftar yang ada di client dan server. Jika terdapat pesan kesalahan ORA-12650 berarti algoritma yang digunakan belum terinstall di salah satu sisi.

Parameter enkripsi dan integritas data didefinisikan dengan memodifikasi file sqlnet.ora di dalam client maupun server. Dalam Oracle Advance Security memungkinkan untuk memilih satu atau keseluruhan konfigurasi algoritma enkripsi dan integrity yang tersedia. Tetapi hanya satu algoritma enkripsi dan integrity yang dipakai dalam sekali session koneksi.

**Tabel 1.** Daftar algoritma enkripsi

| ***Nama Algoritma*** | ***Nilai Legal*** |
|---|---|
| RC4 256-bit key | RC4_256 |
| RC4 128-bit key | RC4_128 |
| RC4 56-bit key | RC4_56 |
| RC4 40-bit key | RC4_40 |
| 3-key 3DES | 3DES168 |
| 2-key 3DES | 3DES112 |
| DES 56-bit key | DES |
| DES 40-bit key | DES40 |

**Tabel 2.** Daftar algoritma integrity

| ***Nama Algoritma*** | ***Nilai Legal*** |
|---|---|
| MD5 | MD5 |
| SHA-1 | SHA1 |

### 4.4 Negoisasi enkripsi dan integrity

Ada 4 kemungkinan nilai dari konfigurasi parameter enkripsi dan integrity Oracle Advance Security. Daftar keempat nilai dari terendah level keamanannya sampai tertinngi level keamanannya adalah sebagai berikut: REJECTED, ACCEPTED, REQUESTED dan REQUIRED.

Nilai defaultnya adalah ACCEPTED.

**REJECTED**

*ISBN: 979-756-061-6*

Memilih nilai ini jika tidak ingin menggunakan pelayanan keamanan, walaupun di sisi lain memilih nilai REQUIRED. Koneksi akan gagal jika di sisi lain memilih nilai REQUIRED.

Jika nilainya selain REQUIRED koneksi akan jalan terus tanpa pelayanan keamanan.

**ACCEPTED**

Memilih nilai ini jika mengharapkan pelayanan keamanan tetap jalan jika di sisi lain dipilih nilai REQUIRED atau REQUESTED.

Di dalam skenario ini koneksi tidak membutuhkan pelayanan keamanan, tetapi memungkinkan digunakan jika di sisi lain di set nilai REQUIRED atau REQUESTED. Jika di sisi lain adalah REQUIRED atau REQUESTED dan algoritma yang cocok diketemukan, maka koneksi akan dilanjutkan tanpa kesalahan dengan pelayanan keamanan

Jika sisi lain di set REQUIRED dan algoritma tidak diketemukan, koneksi gagal dengan pesan kesalahan ORA-12650.

Jika sisi lain di set REQUESTED, ACCEPTED, REJECTED dan tidak ada algoritma yang diketemukan, koneksi akan terus tanpa pesan kesalahan tetapi tanpa pelayanan keamanan.

**REQUESTED**

Memilih nilai ini jika menginnginkan pelayanan keamaan diaktifkan jika di sisi lain juga memerlukannya.. Dalam skenario ini, sisi ini dalam koneksi menginginkan pelayanan keamanan tetapi sebenarnya tidak membutuhkan. Pelayanan keamanan dijalankan jika di sisi lain memilih nilai ACCEPTED, REQUESTED atau REQUIRED. Algoritma yang dipakai harus cocok antara kedua sisi jika tidak pelayanan keamanan tidak dijalankan. Jika sisi lain secara spesifik memilih nilai REQUIRED ddan algoritma tidak cocok maka koneksi akan gagal.

**REQUIRED**

Memilih nilai ini jika pelayanan keamanan selalu diaktifkan atau koneksi ditolak. Dalam skenario ini, sisi ini dalam koneksi secara spesifik menghidupkan pelayanan keamanan. Koneksi gagal jika di sisi lain memilih nilai REJECTED atau algoritma tidak cocok di kedua sisi.

**Tabel 3.** Daftar matrix negoisasi ekripsi dan integrity data

| | Client | | | |
|---|---|---|---|---|
| ***Server*** | ***REJECTED*** | ***ACCEPTED*** | ***REQUESTED*** | ***REQUIRED*** |
| REJECTED | OFF | OFF | OFF | Koneksi gagal |
| ACCEPTED | OFF | OFF | ON | ON |
| REQUESTED | OFF | ON | ON | ON |
| REQUIRED | Koneksi gagal | ON | ON | ON |

## 5. Kesimpulan

a. Oracle Security Server mempunyai kemampuan pengamanan yang cukup kuat untuk menjawab masalah keamanan database dibutikan dengan permintaan login dua kali ke sistem dan ke database, dan kata kunci dapat dienkripsi sesuai dengan keinginan.
b. Jika kata kunci salah, maka sistem akan meminta dimasukkan kata kunci kembali sesuai dengan setting yang kita lakukan berapa kali kata kunci dapat di coba dimasukkan kembali, jika tetap salah maka transaksi akan ditolak.
c. Kinerja Oracle Security Server dapat berjalan maksimal jika didukung dengan hadware yang cukup tinggi spesifikasinya.

## Daftar Pustaka

1. Budiman, 2001, Pengamanan Data Dengan Algoritma RSA, Rijndael dan RIPEMD-160 CERT-CC Statistics, 1988-2002, www.cert.org.
2. Icove, D., J., June 1997, Collaring the cybercrook: an investigator's view, *IEEE Spectru*m, pp. 31-36.
3. InfoKomputer, Agustus 2002, Prima Infosarana Media, Jakarta
4. Johnson, A., March 1998, Companies Losing Millions over Rising Computer Crime, *Shake Security Journa*l, www.shake.net/crime_ march98.htm.
5. Oracle Corporation, 1997, Oracle Security Server Concept, www.oracle.com.
6. Oracle Corporation, 1999, Oracle 8i Security: New Features and Secure Solutions, www.oracle.com.
7. Oracle Corporation, 2000, Oracle ® Advanced Security: Administrator's Guide, www.oracle.com.
8. Oracle Corporation, 2001, Oracle Advanced Security: Key Management, Data Encryption and Integrity Checking, www.oracle.com.
9. Oracle Magazine, May/June 2002, www.oracle.com/oraclemagazine/
10. Oracle Magazine, July/August 2002, www.oracle.com/oraclemagazine/
11. Patenau, Razvan, 2000, *Best Practices for Secure Web Development*, razvan.peteanu@home.com.
12. Purbo, O. W., dan Wiharjito, T. 2000. *Keamanan Jaringan Internet*, Elex Media Komputindo, Jakarta.
13. Rahardjo, B., 1998, *Keamanan Sistem Informasi Berbasis Internet.*