



# **Identity Management, Sebuah Solusi Keamanan Jaringan**



*Proyek Akhir Semester II – 2003/2004  
EC 5010 – Keamanan Sistem Informasi*

*Oleh:  
Nursani Rahmatullah / 13200055*

*Departemen Teknik Elektro  
Institut Teknologi Bandung*

## Abstrak

*Network*/jaringan adalah sesuatu yang berkaitan dengan hubungan (*relationship*). Dan suatu hubungan sepenuhnya berkenaan dengan kepercayaan (*trust*). Bagi sebuah perusahaan/bisnis yang harus berhadapan dengan ancaman keamanan jaringan, pentingnya suatu pengelolaan identitas menjadi sangat jelas dan signifikan.

Akses menuju jaringan bagi pihak-pihak yang tidak berwenang dan penyalahgunaan *resource* datang baik secara internal maupun eksternal. Oleh sebab itu, kemampuan untuk mengidentifikasi pengguna (*user*) dan devais yang berusaha untuk melakukan akses ke jaringan merupakan langkah awal dan yang terpenting dari setiap solusi masalah keamanan.

*Password* atau kata sandi merupakan sarana umum yang masih memegang peran dalam melindungi aset-aset penting dalam sebuah jaringan. Sistem password sederhana belum cukup untuk mengidentifikasi siapakah sebenarnya seorang user atau mengatur apa saja yang dapat diakses olehnya, terlebih lagi kadang user harus mengingat banyak password sehingga pemilihan password cenderung password-password yang mudah dipecahkan. *Hacker* masih saja berkeliaran diantara para user, pencurian password masih kerap terjadi, dan akhirnya pelanggaran dan kehilangan resource masih tetap ada.

Masalah keamanan dan akses terhadap suatu jaringan dapat diatasi dengan pengelolaan identitas. Dengan cara seperti ini, pihak-pihak yang berkepentingan dengan suatu keamanan jaringan dapat memeriksa terlebih dahulu keabsahan identitas pengguna atau devais, menetapkan kebijakan keamanan, dan menyediakan alokasi resource bagi pengguna berdasarkan fungsi kerjanya.

## I. Pendahuluan

Saat ini kita berada pada era digital dimana komunikasi dan pertukaran informasi berlangsung dalam suatu jaringan yang kian hari semakin meluas. Di dalam jaringan tersebut, pengguna (*user*) saling berinteraksi via sebuah pengenal yang merepresentasikan dirinya. Pengenal ini lazim disebut identitas user. Pengertian identitas dalam *identity management* disini lebih ditekankan pada identitas secara digital atau sering disebut *digital identity*. Identitas digital merupakan representasi identitas seseorang yang digunakan untuk berinteraksi dengan orang lain atau mesin dalam sebuah jaringan terdistribusi. Secara sederhana, identitas digital berupa pasangan ID (misalnya nama user) dan sebuah autentifikasi rahasia (misalnya *password*).

Password atau kata sandi merupakan sarana umum yang masih memegang peran dalam melindungi aset-aset penting dalam sebuah jaringan. Sistem password sederhana belum cukup untuk mengidentifikasi siapakah sebenarnya seorang user atau mengatur apa saja yang dapat diakses olehnya, terlebih lagi kadang user harus mengingat banyak password sehingga pemilihan password cenderung password-password yang mudah dipecahkan. Hacker masih saja berkeliaran diantara para user, pencurian password masih kerap terjadi, dan akhirnya pelanggaran dan kehilangan resource masih tetap ada.

Untuk aplikasi-aplikasi khusus misalnya dalam *e-commerce* dan *e-business*, sebuah identitas digital menjadi sedikit lebih kompleks, seperti penambahan profil alamat, pekerjaan, atau level gaji. Sejalan dengan perkembangan jaringan sistem komputer dan semakin kompleksnya identitas digital yang terdistribusi, maka dibutuhkan sebuah pengelolaan yang mampu mempermudah hubungan antara tiap identitas tanpa harus mengesampingkan faktor keamanan jaringan.

## II. Identity Management dan Aspek Keamanan

Perkembangan teknologi informasi yang sedemikian pesat telah mengubah wajah sistem komunikasi dan perdagangan pada saat ini. Munculnya *e-commerce* dan *e-business*, menjajikan kemudahan dan kecepatan dalam bertransaksi antar perusahaan. *E-commerce* dan *e-business* sebagai sebuah media, menawarkan beberapa konsep seperti :

- ✓ proses otomasi bisnis yang menggantikan proses manual.
- ✓ proses yang terintegrasi untuk mencapai hasil yang efektif dan efisien.
- ✓ kemudahan berkomunikasi dan mempromosikan produk atau jasa yang diperdagangkan.
- ✓ pertukaran informasi antar pelaku bisnis dengan memperkecil *human error*.
- ✓ kesepakatan dua pelaku bisnis untuk bertransaksi dengan melibatkan institusi lain sebagai fungsi pembayar.

Disamping kemudahan dan efektivitas yang ditawarkan tersebut, sistem transaksi dan interaksi dunia maya ini membawa problematika tersendiri dalam hal keamanan data dan informasi. Banyak perusahaan berpikir bahwa mereka dapat melindungi diri dari resiko keamanan komputer dengan sistem informasi yang telah mereka miliki. Namun perlu diingat bahwa serangan yang membahayakan, baik dari segi finansial maupun reputasi, akan meningkat sejalan dengan meningkatnya kemampuan koneksi. Ini sama artinya dengan semakin luasnya jaringan maka ancaman terhadap keamanan pun semakin tinggi. Kerusakan pada data dan sistem-sistem kantor dapat menjadi masalah serius, sehingga mempengaruhi kegiatan operasional harian dan kredibilitas perusahaan di hadapan para pelanggan dan masyarakat umum. Bukan perusahaan-perusahaan besar saja yang membutuhkan perlindungan terhadap kebocoran keamanan, setiap badan usaha memerlukan strategi agar terhindar dari para *hacker* atau penyusup.

Kita boleh saja sudah merasa cukup aman, namun pertimbangkan hasil survei yang dilakukan di Amerika Serikat (AS) baru-baru ini. Jumlah serangan hacker naik 28 persen di semester pertama tahun 2002, sehingga rata-ratanya adalah 32 serangan per perusahaan setiap minggunya. Yang lebih mengkhawatirkan lagi adalah temuan yang menyatakan bahwa sebagian besar perusahaan tidak menyadari kalau dirinya telah diserang oleh para hacker.

Walaupun dapat dikatakan bahwa internet telah merevolusikan dunia usaha, namun internet juga menimbulkan berbagai kelemahan. Delapan puluh lima persen perusahaan hingga kini telah melaporkan terjadinya kebocoran keamanan, dan 64 persen melaporkan kerugian finansial yang mencapai US\$ 120 juta per tahunnya sebagai akibat dari serangan-serangan ini. Untuk menghindari serangan ini, ada beberapa langkah yang bisa kita ambil, yakni:

- Memahami Resiko

Setiap bisnis memiliki kelemahan dan prioritasnya sendiri-sendiri. Sebuah kebijakan keamanan dapat dibuat dengan memahami resiko internal dan eksternal yang dihadapi perusahaan. Kita tidak dapat melindungi diri kita sendiri kecuali kita telah mengetahui ancaman internal dan eksternal yang kita hadapi dan seberapa serius ancaman-ancaman tersebut.

Ancaman eksternal menjadi lebih serius jika jaringan sudah meluas ke para pemasok, pelanggan, dan mitra. Hal ini mengindikasikan bahwa keamanan jaringan harus mendapat prioritas utama. Ancaman eksternal meliputi pengguna yang tidak mempunyai wewenang seperti para hacker, penyabot dan pencuri, di samping itu juga termasuk pengguna-pengguna jaringan yang tidak melindungi komputer mereka dengan baik, sehingga memberi kesempatan kepada yang tak berhak untuk menggunakannya.

Resiko internal yang penting namun tidak disadari oleh sebagian besar perusahaan adalah kesalahan dalam pengelolaan identitas karyawan yang sudah meninggalkan organisasi, sehingga mereka masih bisa mengakses jaringan. Disamping itu, kebijakan keamanan juga harus meliputi resiko-resiko yang berkaitan dengan kerusakan peralatan dan bencana alam seperti kebakaran, banjir dan kecelakaan.

- Mencari Titik Lemah

Bagaikan mencari jarum di tumpukan jerami, kadang kala kesan itulah yang muncul pada pencarian titik lemah yang tersembunyi. Tidak semua resiko yang dihadapi dapat dilihat dengan jelas, terutama jika sebuah perusahaan tidak memiliki tenaga ahli teknologi informasi (TI) yang bekerja penuh untuk perusahaan.

Salah satu cara untuk mengidentifikasi resiko ini adalah dengan meminta pihak ketiga yang independen untuk melakukan audit terhadap sistem keamanan kita. Dengan demikian kita dapat menemukan kelemahan-kelemahan yang ada sebelum kita membeli perangkat lunak dan perangkat keras keamanan.

Banyak produk pengelolaan keamanan yang ada di pasar saat ini menawarkan solusi yang bersifat menyeluruh dan menyerupai *control panel* terhadap sistem secara keseluruhan. Kemampuan untuk melihat keseluruhan sistem sebagai sebuah control panel

memungkinkan para administrator untuk mengidentifikasi dan menentukan hubungan yang ada antara kelemahan yang satu dengan yang lainnya, dan kemudian mengambil langkah yang tepat untuk mengatasinya.

- Menangkal bahaya virus

Virus-virus telah menyebabkan kerusakan dan kerugian finansial yang tidak sedikit. Seperti ancaman kelemahan lainnya, kerugian ini dirasakan baik oleh perusahaan besar maupun kecil.

Jika kita tidak ingin kehilangan data karena virus, maka kita harus melaksanakan tinjauan rutin, memasang *patch*, dan meng-*update* tanda-tanda kelemahan. Perlindungan yang terbaik adalah kebijakan, prosedur, serta teknologi. Karyawan harus diberikan instruksi yang tegas perihal penerimaan *e-mail* yang mencurigakan dan apa yang mereka harus lakukan jika terinfeksi. Kalau hal itu dirasa kurang efektif, maka kita membutuhkan sebuah manajemen yang dapat menjamin konsistensi di seluruh aspek bisnis termasuk didalamnya upaya pencegahan terhadap serangan virus.

- Jangan Memberi Kemudahan bagi Para Hacker

Beberapa kesalahan yang umum dilakukan perusahaan-perusahaan dan karyawan, sehingga data mereka mudah diserang, yakni:

- ✓ Menginstal sistem-sistem operasi dan aplikasi-aplikasi dengan menggunakan *default*.
- ✓ Password atau kata sandi yang lemah (sekitar 40 persen dari kita menggunakan kata "kata sandi" tersebut).
- ✓ *Back up* data yang tidak lengkap.
- ✓ Membiarkan *port* yang tidak diperlukan tetap terbuka.
- ✓ Paket data tidak disaring (*filter*). Penyaringan dibutuhkan untuk memastikan alamat penerima dan pengirim yang benar.

Terdapat beberapa langkah pencegahan yang dapat meningkatkan keamanan, terutama terhadap ancaman-ancaman internal. Antara lain, menggunakan perangkat lunak

pengelolaan kata sandi untuk membantu karyawan memilih kata sandi yang kuat. Selain itu, menerapkan tanggal berlaku kata sandi. Menciptakan autentifikasi yang lebih kuat dengan mengombinasikan kata sandi dengan *biometric* (jika ada) seperti sidik jari, suara, atau retina mata.

Sekilas tampak bahwa masalah-masalah yang diutarakan di atas merupakan masalah umum yang dihadapi bagi sebuah sistem informasi data digital seperti layaknya sebuah jaringan. Namun terdapat beberapa aspek menonjol seperti: kesalahan dalam pengelolaan identitas karyawan (user); pertimbangan bahwa sistem harus mampu menghadapi ancaman kecelakaan fisik seperti kerusakan alat, bencana alam atau kebakaran; deteksi dini terhadap ancaman pada titik-titik lemah; dan pengelolaan kata sandi (password) yang baik.

Pengelolaan identitas (*identity management*) mampu menyediakan sistem yang terintegrasi untuk dapat menjalankan fungsi pengamanan secara lebih efisien sehingga mampu mengatasi masalah-masalah yang telah disebutkan di atas secara lebih menyeluruh. Pengelolaan identitas lebih diidentikkan dengan sistem keamanan autentifikasi, otorisasi dan administrasi (3A). Sebenarnya bukan hanya aspek keamanan saja yang dititikberatkan oleh sebuah sistem pengelolaan identitas, lebih dari itu menyangkut efisiensi kerja, produktivitas, dan keuntungan bisnis.

Perusahaan-perusahaan saat ini mulai membangun *e-business on demand* bagi karyawan, pelanggan, mitra dan pemasok mereka, sehingga pengotomatisasian proses pengelolaan kebijakan keamanan dan identitas pengguna yang berjumlah besar akan menjadi cara yang paling efektif untuk mengurangi biaya dan membangun sebuah infrastruktur yang dapat diandalkan

### III. Mengenal Identity Management

*Network*/jaringan adalah sesuatu yang berkaitan dengan hubungan (*relationship*). Dan suatu hubungan sepenuhnya berkenaan dengan kepercayaan (*trust*). Bagi sebuah perusahaan/bisnis yang harus berhadapan dengan ancaman keamanan jaringan, pentingnya suatu pengelolaan identitas menjadi sangat jelas dan signifikan.

Akses menuju jaringan bagi pihak-pihak yang tidak berwenang dan penyalahgunaan resource datang baik secara internal maupun eksternal. Oleh sebab itu, kemampuan untuk mengidentifikasi pengguna (*user*) dan devais yang berusaha untuk melakukan akses ke jaringan merupakan langkah awal dan yang terpenting dari setiap solusi masalah keamanan.

Masalah keamanan dan akses terhadap suatu jaringan dapat diatasi dengan pengelolaan identitas. Dengan cara seperti ini, pihak-pihak yang berkepentingan dengan suatu keamanan jaringan dapat memeriksa terlebih dahulu keabsahan identitas pengguna atau devais, menetapkan kebijakan keamanan, dan menyediakan alokasi resource bagi pengguna berdasarkan fungsi kerjanya.

Sistem seperti ini harus mencakup setiap elemen pada jaringan, bukan hanya server-server yang memiliki potensi mudah diserang. Sebuah pengelolaan identitas harus diintegrasikan dengan komponen-komponen lain dari pengamanan jaringan yang komprehensif, termasuk penyediaan koneksi yang aman dan sistem pertahanan terhadap ancaman. Menemukan sebuah solusi yang mampu mengakomodasi seluruh persoalan ini dapat menjadi sebuah tantangan tersendiri.

Perkembangan teknologi informasi dan semakin rentannya sebuah jaringan terhadap serangan atau ancaman kerusakan telah mendorong vendor-vendor ternama dalam memasarkan produk sistem keamanan yang terintegrasi. IBM hadir dengan merk software Tivoli, yaitu perangkat lunak pengelolaan keamanan dan identitas yang mencakup produk-produk seperti IBM Tivoli Access Manager, IBM Tivoli Identity Manager dan IBM Tivoli Risk Manager. Computer Associates memasuki pasaran dengan produk eTrust Identity dan Access Management Suite, dan masih banyak lagi.

Software-software pengelolaan identitas ini membantu dalam mengkonsolidasikan data identitas dan mengotomatisasikan penggunaan hak akses karyawan, kontraktor, mitra bisnis dan para pelanggan ke berbagai aplikasi dan sumber daya berdasarkan kebijakan bisnis yang ada. Hal ini akan membantu perusahaan perusahaan mengurangi biaya TI dan meningkatkan keamanan.

#### **a. Konsep Identity Management**

Pengelolaan identitas pada dasarnya mengkombinasikan proses dan teknologi untuk mengelola dan mengamankan akses menuju informasi/resource sekaligus melindungi profil identitas user. Setiap user (atau devais) diidentifikasi lalu akses masing-masing user dikontrol sesuai dengan hak dan batasan yang diberikan. Identity management memiliki kemampuan untuk mengelola hal tersebut tersebut secara efektif baik untuk user di dalam maupun di luar perusahaan/organisasi (karyawan, pelanggan, patner bisnis, atau bahkan sebuah aplikasi, pada dasarnya semua orang atau alat yang hendak berhubungan dengan perusahaan/organisasi)

Banyak definisi yang diberikan oleh para pakar dalam menjelaskan konsep pengelolaan identitas. Penamaan yang diberikan pun beragam; Identity Management (IM, IdM, IDM), Identity and Access Management (IAM), Secure Identity Management (SIM), Digital Identity (DI, DID), Identity and Security Management (ISM). Namun demikian konsep pengelolaan identitas secara umum dapat dipandang sebagai suatu cara untuk:

- Mendefinisikan identitas dari sebuah entitas/obyek (orang,tempat, alat)
- Menyimpan informasi-informasi yang berkaitan dengan entitas tersebut, seperti nama/pengenal, dalam sebuah tempat penyimpanan (biasanya direktori aktif) yang aman, fleksibel, dan dapat disesuaikan.
- Menjadikan informasi-informasi tersebut dapat diakses melalui beberapa ketentuan.
- Menyediakan infrastruktur yang baik, terdistribusi dan memiliki performansi yang tinggi.
- Mengatur hubungan antara resource dan entitas/obyek sesuai dengan konteks dan dalam waktu tertentu.

Mengutip seorang pakar keamanan jaringan, Bruce Schneier, “Siapapun dapat membuat rambu-rambu, atau bahkan sebuah lampu lalu lintas, namun dibutuhkan sebuah pola pikir yang sepenuhnya berbeda untuk menyusun suatu sistem pengatur lalu lintas kota besar yang ramai.” Itulah sebabnya mengapa sebuah perusahaan perlu memiliki sistem pengelolaan identitas yang menjadi bagian integral dari sebuah jaringan informasinya.

Untuk mengetahui sejauh mana pentingnya hal ini, seseorang perlu memahami struktur dari suatu sistem keamanan yang terintegrasi serta teknologi-teknologi yang terlibat di dalamnya. Ada tiga komponen penting dalam sebuah sistem keamanan terintegrasi yang komprehensif, yaitu: privasi, proteksi, serta kontrol/pengawasan.

- Privasi membutuhkan koneksi yang aman dan teknologi-teknologi seperti IP Security (IP Sec) dan Secure Socket Layer (SSL) VPN, yang membantu untuk meyakinkan bahwa komunikasi dalam sebuah WAN atau LAN merupakan komunikasi yang aman.
- Proteksi membutuhkan pertahanan yang kuat dalam menghadapi ancaman internal maupun eksternal. Proteksi ini dapat berupa *firewall* dan sistem pencegah penyusupan.
- Kontrol membutuhkan sistem identitas yang cermat dan teliti termasuk kontrol terhadap suatu akses.

Hanya sebuah pendekatan terkoordinasilah yang mampu merangkai teknologi-teknologi ini menjadi sebuah struktur *network* yang dapat memenuhi kebutuhan keamanan jaringan pada saat ini. Ketiga komponen di atas bergantung pada pengelolaan identitas dalam suatu jaringan.

Melakukan sebuah pengelolaan identitas berarti meyakinkan bahwa orang yang tepat mendapatkan informasi yang tepat pada waktu yang tepat pula. Pada saat ini sebuah identitas telah menjadi lebih luas jangkauannya, dari seorang klien dan desktop PC-nya yang bersifat statis menjadi sebuah devais yang bersifat mobile dan klien yang selalu berpindah-pindah tempat. Dengan semakin luasnya cakupan yang harus dikelola, maka tugas seorang administrator juga menjadi bertambah. Ia harus mengetahui siapa saja yang berada dalam jaringan pada waktu tertentu, informasi apa saja yang boleh diakses olehnya, dan kemana saja user tersebut dapat menggunakan aksesnya.

Sebuah manajemen identitas harus melakukan:

1. Kontrol akses, hanya mengizinkan entitas yang berhak saja yang boleh memasuki jaringan, dan mengontrol tindakan yang dilakukan entitas tersebut sesaat setelah memasuki jaringan.

2. Pemisahan akses, secara otomatis mengatur akses berdasarkan identitas yang telah diverifikasi sebelumnya.
3. Melindungi jaringan, menjaga para user dari membuka peluang diserangnya jaringan seperti *distributed denial of service*, baik user tersebut sengaja atau tidak.
4. Mencegah terjadinya penyusupan, dengan mengatur pertahanan dari serangan, mengkarantinakan sistem yang terkena serangan sehingga tidak mempengaruhi jaringan secara keseluruhan, kemudian melakukan perbaikan.

Mengelola seluruh elemen ini sama artinya dengan menjalankan sebuah sistem yang memenuhi dua kriteria penting. Pertama, sistem ini harus mudah disesuaikan (*versatile*) karena batasan dari network cenderung selalu berubah akibat sering bergantinya user. Sebagai contoh dipecatnya beberapa karyawan, pergantian kontraktor, diperolehnya pelanggan baru. Seluruh perubahan user ini harus ditangani dengan baik sekaligus menjaga agar bisnis tetap berjalan.

Kriteria yang kedua adalah kemampuan untuk melihat situasi dan bertindak dengan cepat. Administrator jaringan atau divisi TI harus dapat melihat apa yang sedang terjadi dalam sebuah jaringan. Pelanggaran keamanan tidak boleh dibiarkan terus terjadi selama sehari-hari yang dapat mengancam informasi yang terdapat dalam jaringan.

#### **b. Pelaku dan Peran dalam Pengelolaan Identitas**

Dalam pengelolaan identitas terdapat beberapa pihak yang memainkan peranan :

- Pelaku dan peran Manusia

Pelaku Manusia	Peran
Individu	<ul style="list-style-type: none"> <li>✓ Memiliki identitas</li> <li>✓ Mendapatkan informasi identitas individu lain yang sedang berkomunikasi dengannya</li> </ul>
Identity Information Manager	Bertanggung jawab terhadap informasi individu dalam jaringan,
Information System Manager	Bertanggung jawab terhadap desain dan operasional dari infrastruktur komunikasi dan informasi sebuah jaringan.

Developer of tools and application	Mendesain dan mengimplementasikan tool-tool dan aplikasi untuk Identity Management
------------------------------------	--

- Pelaku dan peran devais

Devais	Peran
Secure ID Devive	Membantu user menunjukkan identitasnya Contoh: <ul style="list-style-type: none"> <li>✓ magnetic stripe card</li> <li>✓ finger print reader</li> </ul>
Enterprise Computer	<ul style="list-style-type: none"> <li>✓ Menyimpan informasi/data yang diakses oleh user.</li> <li>✓ Memberikan layanan bagi user</li> </ul>
Directory	Menyimpan informasi mengenai identitas user
Client Computer	<ul style="list-style-type: none"> <li>✓ penyimpanan data pribadi</li> <li>✓ menjalankan aplikasi lokal</li> </ul>
Dump Computer	Menyediakan akses ke layanan dan informasi.

### Direktori

Direktori dalam arti luas bertugas menyimpan identitas dan informasi-informasi yang berkaitan dengan identitas tersebut. Dalam sistem yang besar biasanya terdapat beberapa direktori. Identitas dan informasi yang terdapat di dalam masing-masing direktori saling berhubungan dan terstruktur, sehingga memudahkan administrator untuk mengubah, menambah, menghapus, dan menonaktifkan identitas.

### Client computer

Masing-masing individu menggunakan devais yang bermacam-macam untuk mengakses informasi atau layanan atau untuk menjalankan aplikasi lokal. Devais-devais

tersebut dapat berupa personal computer (PC), personal digital assistant (PDA), atau ponsel.

Dalam aplikasinya pengelolaan identitas juga harus mendukung berbagai sarana akses menuju jaringan baik intranet, extranet, dan internet yang antar lain meliputi *direct connection*, *proxied connection*, *firewall*, dan *wireless connection*. Identitas yang dimaksud disini bergantung pada elemen-elemen :

- Siapa anda
- Konteks yang berlaku
- Profil anda

Elemen 'siapa anda' diverifikasi oleh proses autentifikasi yang akan dijelaskan setelah ini. Identitas digital bergantung pada konteks, karena masing-masing dari user memainkan peran yang berbeda dalam konteks yang berbeda. Pada suatu saat kita bisa berlaku sebagai karyawan, namun pada saat yang lain peran kita bisa berubah menjadi *customer* sesuai konteks yang berlaku saat kita ingin melakukan hubungan/akses ke jaringan. Antara karyawan dan customer tentu mendapat kebijakan yang berbeda pada saat melakukan akses, oleh sebab itu identitas memiliki hubungan yang erat dengan profil. Profil meliputi informasi, *tool*, *preference*, dan *resource* untuk setiap identitas.

## **IV. Aspek-aspek Fungsional pada Identity Management**

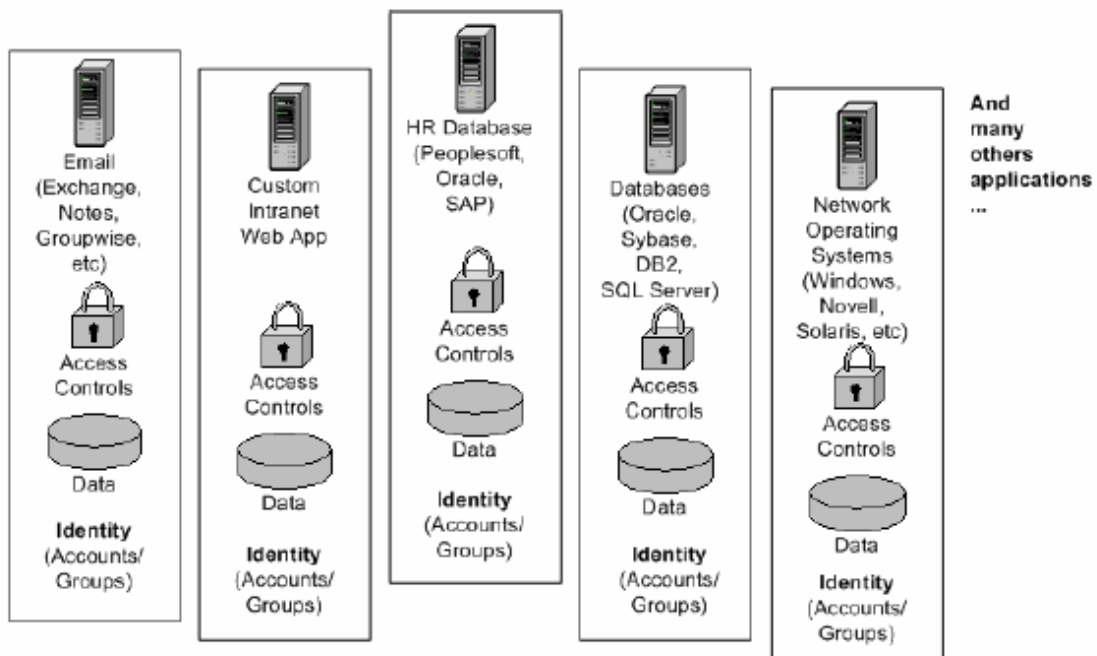
Pada bab-bab sebelumnya telah dipaparkan sebuah pandangan mengenai konsep identity management dan hubungannya dengan keamanan jaringan. Dapat dipahami bahwa sebuah konsep pengelolaan dalam identity management harus mampu mengakomodasi perkembangan identitas yang semakin meluas (*federated identity*). Konsep ini mempertimbangkan antara kemajuan teknologi dengan kebijakan dan strategi bisnis.

Bab ini mencoba untuk menggali lebih dalam komponen-komponen apa saja yang dibutuhkan untuk mendukung sebuah pengelolaan yang baik dalam identity management.

Secara garis besar identity management meliputi autentikasi, password management, provisioning, dan access control.

### a. Autentikasi

Autentikasi merupakan inti dari konsep identity management. Sistem keamanan pada saat ini umumnya menggunakan pendekatan pengaturan secara terpisah, yaitu setiap aplikasi mengelola informasi dari tiap-tiap identitas, hak-haknya, dan kontrol untuk mengatur akses ke aplikasi seperti yang diilustrasikan pada gambar di bawah ini,



sumber: realtimepublishers.com

Autentikasi merupakan proses awal untuk menyatakan (memverifikasi) bahwa seseorang atau sebuah entitas sesuai dengan identitas yang dimilikinya. Proses ini dilakukan melalui beberapa cara penentuan menurut respon user. Jika seorang user ingin melakukan akses, ada beberapa jalan untuk menunjukkan bahwa yang bersangkutan sesuai dengan identitas yang diberikannya:

- sesuatu yang anda tahu, seperti nomer identitas, password, PIN
- sesuatu yang anda punya, seperti kartu kredit, SIM, ATM, passport
- sesuatu yang berarti anda, seperti sidik jari, retina, DNA, suara, tanda tangan

Dari beberapa cara yang disebutkan di atas, password merupakan cara dianggap lebih efektif sebagai sebuah bentuk proses autentifikasi. Namun demikian password menjadi sebuah paradoks. Password yang baik adalah password yang tidak mudah dipecahkan, tapi password yang seperti itu biasanya sangat sulit untuk diingat. Masalah akan semakin rumit dari prespektif pengguna atau user, hal yang menjadi masalah adalah kadang user memiliki password yang berbeda untuk mengakses aplikasi yang berbeda, sehingga jika aplikasi yang ada berjumlah banyak maka user akan memiliki banyak jumlah password yang harus diingatnya sehingga dipilih password-password yang mudah diingat atau menuliskan daftar password disembarang tempat (biasanya di samping komputer) yang belum tentu aman.

Pengelolaan password dapat mengatasi masalah ini dengan *single sign on* atau *password synchronization*, sehingga user hanya sekali saja menggunakan passwordnya untuk dapat menjalankan banyak aplikasi yang membutuhkan autentifikasi. Subbab berikutnya akan menjelaskan hal ini.

## **b. Password management**

Password management memiliki tiga fungsi dasar

- *Self-service password reset*, fungsi ini dapat digunakan user untuk mengubah sendiri password yang hilang karena lupa. User harus menjawab “pertanyaan” yang sebelumnya telah dibuat dan dijawab oleh user yang bersangkutan pada saat membuat password yang pertama.
- *Password synchronization*, fungsi ini memudahkan user sehingga user hanya menggunakan sebuah password untuk banyak aplikasi. Jika sebuah password telah direset, maka semua password akan diperbaharui secara otomatis.
- *Password policy enforcement*, fungsi ini menetapkan kebijakan mengenai format password baru yang boleh digunakan. Format ini sesuai dengan syarat dari sistem operasi (seperti jumlah karakter yang digunakan) atau kebijakan keamanan dari perusahaan (seperti larangan menggunakan password yang sama dengan sebelumnya).

Password management sangat dibutuhkan untuk mengamankan akses menuju jaringan. Lazimnya password management secara sederhana dilakukan dengan memberikan standar bagi nama *account*. Dalam kaitannya dengan identity management, password management mengelola password sesuai dengan kebijakan yang diberlakukan, misalnya ketentuan mengenai kombinasi sintaks yang boleh digunakan dan masa berlaku password tersebut. Identity management menjamin konsistensi kebijakan tersebut untuk setiap sistem pada jaringan.

Sintaks berhubungan dengan format atau komposisi karakter yang dapat digunakan pada password. Format atau komposisi ini harus seragam atau konsisten pada tiap-tiap sistem. Kriteria-kriteria kebijakan yang dapat dipergunakan antara lain:

- panjang minimum dan maksimum password
- jumlah minimum dan maksimum karakter yang digunakan
- jumlah minimum dan maksimum huruf yang digunakan
- jumlah minimum dan maksimum tanda baca yang digunakan
- exclusion (contohnya, kata-kata yang spesifik dan variasi nama account)
- tipe-tipe karakter yang berurutan
- contoh beberapa karakter
- password yang unik
- pemeriksaan password secara sekuensial

Sedangkan untuk masa berlaku dan ketentuan waktu untuk password, dapat digunakan kriteria-kriteria seperti di bawah ini:

- tenggang waktu minimum dan maksimum penggantian password
- penghitungan waktu atau jumlah password, sebelum password yang sama digunakan kembali
- jumlah hitungan kesalahan pemasukan password sebelum sistem terkunci untuk user yang bersangkutan
- durasi atau lamanya sistem terkunci
- pertanyaan-pertanyaan apa saja untuk keperluan mereset password kelak.

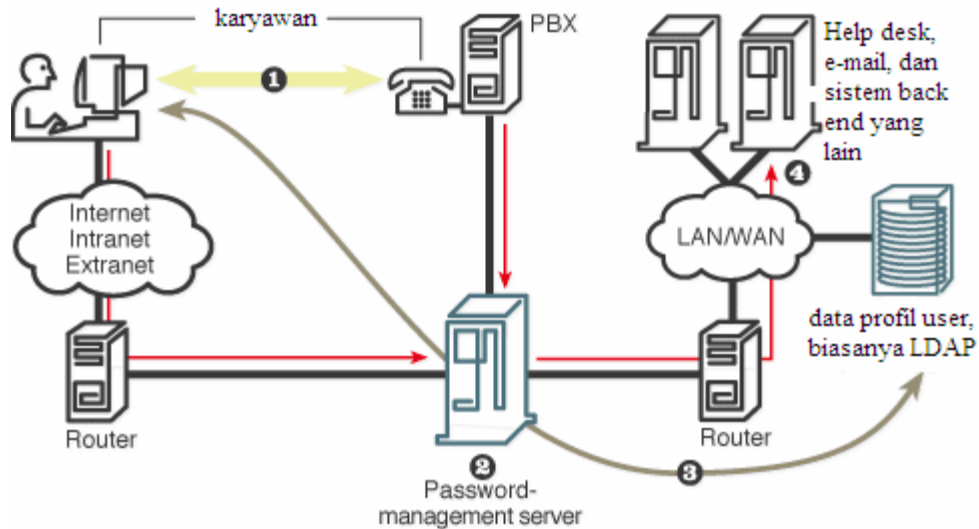
Untuk menjamin keamanan dalam password management, sebaiknya turut dipertimbangkan juga proses enkripsi password sebelum disimpan, pengamanan akses menuju tempat disimpannya password tersebut, dan menjamin keamanan proses validasi sebuah password.

Dalam sebuah perusahaan atau bisnis yang bersifat komersial, masalah pengelolaan password bagi karyawan menjadi cukup signifikan. Perusahaan harus mengeluarkan biaya tambahan dengan membuat semacam *help desk* atau *support center* untuk menangani kasus user yang lupa passwordnya atau kasus user yang ingin mereset passwordnya. Dengan password management user dapat mengatur dan mengatasi sendiri masalah-masalah password yang dihadapinya seperti mereset password. Setelah direset password management akan melakukan sinkronisasi terhadap semua sistem sehingga user dapat mengakses sistem-sistem tersebut. Terdapat vendor-vendor terkemuka untuk produk-produk password management, antara lain BindView, Blokade, Courion, dan Symark Software. Namun banyak juga vendor-vendor besar yang menyertakan produk password managementnya bersama produk identity management, antara lain Oblix, Waveset, Computer Associates, dan Protocom Development System.

Setelah kita memutuskan penggunaan password management, ada beberapa hal yang harus diperhatikan, antara lain:

- dimana informasi mengenai password itu disimpan, apakah menggunakan data base sendiri atau bergantung pada source informasi user yang telah ada
- bagaimana cara pengamanannya, lebih jauh lagi enkripsi apa yang digunakan, dan bagaimana proses tersebut diamankan
- metode akses apa yang digunakan oleh end user (contoh: HTTP, VoiceML, SMS, atau WML)
- standar apa yang dimiliki, standar utama biasa berupa Lightweight Directory Access Protocol (LDAP) sebagai sebuah direktori dan SQL untuk akses data base.

Untuk lebih sedikit memahami password management secara praktis, perhatikan gambar dibawah ini:



sumber: <http://www.nwfusion.com>

Keterangan :

1. Seorang user ingin mengganti password melalui PC, telepon, atau devais front end yang lain
2. Password sever membalas dengan menyodorkan satu atau beberapa pertanyaan yang dapat disimpan dalam data base yang terenkripsi.
3. Setelah mendapat jawaban yang sesuai user dapat memasukkan password yang baru dan server memberikan ketentuan sesuai dengan kebijakan password yang telah ditetapkan. Kemudian user melakukan sinkronisasi terhadap semua back end sistem.
4. server dapat menjalankan help desk, meng-update audit log, memberi peringatan, atau melakukan fungsi yang lain sehingga administrator mengetahui adanya pergantian password.

### c. Provisioning

Fungsi ini mengotomasi pembuatan dan penghapusan penghapusan satu atau beberapa account dan menyediakan resource yang bersesuaian bagi user account tersebut. Provisioning mempermudah proses pemberian akses dengan cepat bagi user seperti karyawan, kontraktor, patner, atau pelanggan untuk mengakses resource informasi,

proses ini sekaligus meningkatkan keamanan dengan melakukan deprovisioning sesaat setelah user tersebut dicabut hak aksesnya.

Kasus klasik yang menunjukkan pentingnya fungsi provisioning dalam kaitannya dengan identity management adalah sebagai berikut. Misalkan ada karyawan yang masuk ke sebuah perusahaan. Karyawan tersebut belum dapat bekerja secara efektif hingga ia mendapatkan hak akses resource yang sesuai dengan perannya. Ketika karyawan baru bergabung dengan perusahaan, maka biasanya ia membutuhkan beberapa layanan yang perlu diakses untuk melakukan pekerjaannya. Umumnya karyawan tersebut membutuhkan email account, akses menuju portal perusahaan atau Customer Relationship Management (CRM) atau menuju Enterprise Resource Planning (ERP). Karyawan juga butuh akses ke aplikasi yang bersifat *self service*, layanan *remote access networking*, firewall dan masih banyak lagi.

Proses pengaturan untuk memberikan akses user ke layanan dan aplikasi-aplikasi tersebut merupakan pekerjaan yang cukup intens. Karyawan harus meminta account ke bagian administrator, lalu administrator memasukkan informasi mengenai identitas user ke dalam aplikasi, kemudian mengirimkan profil account ke user. Proses ini dapat memakan waktu berhari-hari sebelum seorang user mendapatkan hak aksesnya. Proses ini berulang untuk setiap aplikasi, dan berulang kembali saat terjadi perubahan status user atau saat user meninggalkan perusahaan.

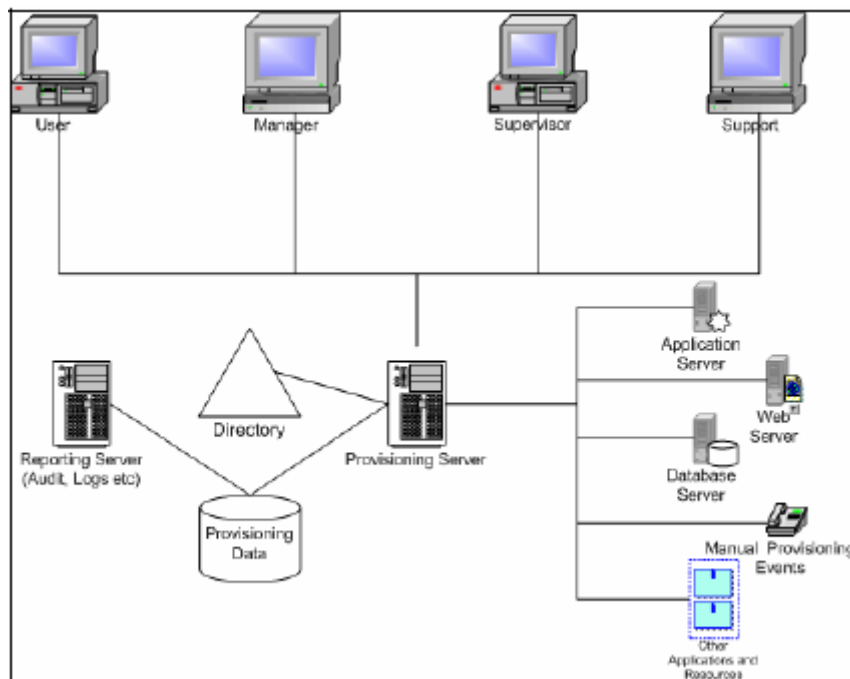
Provisioning dapat melakukan otomasi untuk proses-proses yang telah disebutkan di atas. Fungsi ini menjamin jika pada saat karyawan baru memasuki sistem sumber daya manusia (human resource) sebuah perusahaan, maka pemasukan data-data informasi mengenai karyawan tersebut akan menjalankan proses pembuatan email account, user ID, pemberitahuan pada administrator dari Network Operating System (NOS), dan akhirnya account NOS untuk user tadi selesai dibuat. Proses yang berlangsung secara otomatis ini membawa keuntungan baik bagi user maupun perusahaan, yaitu:

- Biaya untuk provisioning bagi user baru akan turun drastis dan efisiensi akan meningkat karena pengelola-pengelola aplikasi tidak lagi berulang kali memasukkan informasi mengenai user yang sama.

- User-user dapat dibuatkan account dengan daftar default dan wewenang berdasarkan tanggung jawab/perannya, hal ini meningkatkan aspek keamanan sistem.
- Dengan proses otomatisasi yang relative cepat maka akan diperoleh efisiensi waktu sehingga produktivitas kerja user akan meningkat.

Provisioning dapat langsung dijalankan begitu terjadi perubahan status pada user. Biasanya jika cara manual digunakan maka akan memakan waktu yang lama untuk menghapus account pengguna yang telah meninggalkan perusahaan. Hal ini tentu berbahaya karena user yang sudah tidak memiliki hak akses masih dapat mengakses resource perusahaan.

Berikut ini tipe arsitektur provisioning yang umum digunakan,



sumber: [realtimepublishers.com](http://realtimepublishers.com)

untuk menjelaskan bagaimana sistem ini bekerja, berikut ini langkah-langkah bagaimana proses penambahan, modifikasi dan penghapusan komponen dari user.

1. Manajer, asisten administrasi, atau administrator sistem memasukkan informasi tentang user baru, memodifikasi atau memberi tanda user yang akan dihapus

- melalui sebuah interface (biasanya berbasis Web). Kebanyakan produk provisioning saat ini mampu melakukan proses provisioning dengan menerima data langsung dari data base eksternal seperti ERP, Sales Force Automation (SFA), atau sistem CRM tanpa harus memasukkannya secara manual.
2. Informasi diteruskan ke bagian pengesah (approver) setelah sebelumnya disesuaikan dengan peraturan kebijakan yang telah ditetapkan.
  3. Setelah mendapat pengesahan, provisioning server segera mengakses sistem-sistem yang dituju, secara langsung atau melalui agen, untuk membuat user account yang baru. Untuk kasus modifikasi dan menghapus account, provisioning server terlebih dahulu mengganti informasi yang tersimpan dalam data base lalu kemudian menuju sistem yang dituju untuk mengubah atau menghapus account yang dimaksud. Secara fungsional hal ini menjamin konsistensi standar penamaan, account-account yang terhubung, informasi identitas yang konsisten, dan peran yang diberikan.

#### **d. Access Control**

Access control berperan dasar dalam mengatur cara pengaksesan dan juga memberikan kapabilitas yang jelas bagi setiap account sesuai dengan ketentuan yang dimiliki account tersebut.

Terdapat setidaknya lima elemen dasar untuk menjelaskan fungsi kontrol akses pada identity management, yaitu:

- User – entitas yang menggunakan sistem
- Peran – sebuah fungsi kerja dalam suatu konteks interaksi
- Izin – persetujuan untuk melakukan sebuah operasi pada satu obyek atau lebih
- Obyek – dapat berupa banyak hal, contohnya sebuah masukan pada sistem yang dituju (seperti nama account), resource jaringan (mis. printer), aplikasi (procurement), kebijakan (ketentuan password), dan sebagainya.
- Operasi – seperti mereset password, memodifikasi, atau menghapus account.

Keseluruhan model tersebut dipandang dari sisi user secara individual dan izin yang diberikan didasarkan pada peran yang disandang oleh user. Beberapa pendekatan yang dapat digunakan dalam penerapan access control adalah:

#### **a. User Based Access Control (UBAC)**

UBAC sering disebut access control berbasis identitas. Pendekatan ini membutuhkan seorang administrator untuk menentukan perizinan bagi setiap user sesuai dengan kebutuhan individual user.

UBAC memberikan hasil yang optimal karena perizinan yang diberikan cenderung lebih terarah sesuai dengan kebutuhan user, namun pendekatan ini dirasa berat dan mahal. Suatu hal yang mustahil bagi manajemen keamanan untuk mengetahui secara pasti akses apa yang benar-benar dibutuhkan oleh tiap-tiap user lalu menetapkan perizinan berdasarkan hal tersebut, belum lagi ia harus mengupdate perizinan tersebut secara berkala untuk menghindari perizinan yang sudah tidak berlaku.

Karena didasarkan pada kebutuhan masing-masing user, maka tidak ada pengelompokan bagi user. Tiap-tiap user mendapatkan kebijakan sendiri sesuai kebutuhan, namun sayang pada prakteknya, UBAC sering diterapkan dengan pengelompokan sehingga ada user yang mendapatkan ketentuan akses yang melebihi apa yang ia butuhkan.

#### **b. Role Based Access Control (RBAC)**

RBAC cukup populer karena konfigurasi perizinannya cukup mencapai sasaran yang diinginkan. Dalam RBAC terdapat “peran” yang berbeda-beda. Sebuah peran merepresentasikan kelompok user dengan akses menuju resource-resource tertentu. Peran ini ditetapkan berdasarkan profil user. Seorang user dapat memiliki satu atau beberapa peran, seorang super user bisa jadi diklasifikasikan pada semua peran

#### **c. Policy Based Access Control**

Pendekatan ini juga dikenal dengan Rule Set Based Access Control (RSBAC). Kebijakan yang digunakan dalam access control adalah peraturan-peraturan yang menentukan hak akses user.

Contoh umum yang sering digunakan adalah ketentuan yang mengatur akses user pada dokumen-dokumen internal perusahaan melalui internet. Ketentuan tersebut dapat berupa pembatasan jumlah dokumen yang dapat diakses atau didownload oleh user dalam

selang waktu tertentu. Dapat pula ketentuan dalam membatasi akses ke situs-situs tertentu atau halaman web tertentu.

#### **d. Content Dependent Access Control (CDAC)**

Pendekatan ini merupakan metode untuk mengontrol akses user ke resource berdasarkan isi dari resource. CDAC umumnya digunakan untuk melindungi database yang mengandung data-data penting yang sensitif.

CDAC mempunyai beberapa kesulitan antara lain resource butuh diperiksa (scanned) dahulu isinya sebelum akses diterima, dalam beberapa implementasi hal ini memperlambat akses user.

#### **e. Context Based Access Control (CBAC)**

Pada CBAC, keputusan bahwa apakah seorang user dapat mengakses sebuah resource atau tidak bukan hanya didasarkan semata-mata dari siapakah user dan resource apa yang diakses, namun juga didasarkan pada urutan langkah/event sebelum akses tersebut dilakukan.

Sebagai contoh sebuah sistem yang tidak mengizinkan seorang user mengakses suatu resource lebih dari 100 kali dalam sehari. Sistem ini mencatat setiap langkah dari user dan memblokir segala yang diakses user jika ia mengakses lebih dari 100 kali.

Setiap pendekatan yang dipaparkan diatas dapat dikombinasikan dan diterapkan pada resource-resource yang berbeda. Hal ini disesuaikan dengan kebijakan perusahaan dan pertimbangan keamanan yang telah dibuat sebelumnya.

## **V. Kesimpulan**

Identity management merupakan salah satu cara meningkatkan keamanan jaringan. Dengan penetapan kebijakan yang tepat dan penerapan aspek-aspek fungsional identity management (autentifikasi, password management, provisioning, dan access control) yang baik tidak hanya keamanan yang diperoleh, namun efisiensi kerja dan

produktivitas juga meningkat. Identity management membuat infrastruktur jaringan dalam mengelola identitas user dalam jumlah besar menjadi lebih fleksibel.

## Referensi:

- [1] “*Trust and Identity Management, Solution Overview*,” Cisco System Inc, 2004.
- [2] Archie Reed, “*The Definitive Guide to Identity Management*,” realtimepublishers.com, 2002.
- [3] Budi Rahardjo, “*Perkembangan E-commerce: Peluang dan Permasalahan*,” PPAU Mikroelektronika ITB, UPT PIKSI, 2000.
- [4] “*Getting a Grip on Access Control Term*,” Camelot Information Technologies Ltd, 2001. <http://www.camelot.com>
- [5] Julie Bort, “*Identity Management Begins with The Humble Password*,” in NetworkWorldFusion, 2002. <http://www.nwfusion.com>
- [6] “*Identity Management Concept, Secure and Trusted Practices*.” Northwestern University, 2004.
- [7] Julia Widjaja, “*Mengamankan Bisnis dari Serangan Hacker*,” Harian Sinar Harapan, 2003.
- [8] Artikel: “*IBM Raih Posisi I Pasar Software Keamanan 3A*,” infokomputer.com, 2003
- [9] Computer Associates Indonesia, <http://www.ca.co.id>