

Tugas Mata Kuliah
IKI-83408T
Proteksi dan Keamanan Sistem Informasi



CHAPTER 2
Access Control Systems

LAPORAN

KELOMPOK 126:

<i>W. AGUS WINARTA</i>	<i>7204000411</i>
<i>AULIYA ILMAN FADLI</i>	<i>720400011X</i>
<i>ABDUL BASITH HIJAZY</i>	<i>7204000195</i>

MAGISTER TEKNOLOGI INFORMASI
UNIVERSITAS INDONESIA
JAKARTA - 2005

DAFTAR ISI

DAFTAR ISI	i
CHAPTER 2 Access Control Systems	1
1.1 Pendahuluan	1
1.1.1 Kerahasiaan	2
1.1.2 Integritas	2
1.1.3 Ketersediaan	5
1.2 Sekilas Info PT. Asuransi XXX	10
1.2.1 Visi	11
1.2.2 Misi	11
1.2.1 Aplikasi yang dimiliki	11
2.1 Dasar Kontrol Akses	16
2.1.1 Subjek dan Objek	19
2.1.2 Least Privilege	20
2.1.3 Controls	21
2.2 Teknik-teknik Kontrol Akses	21
2.2.1 Rancangan Kontrol Akses	21
2.3 Administration Access Control	25
2.3.1 Centralized Access Control	26
2.3.2 Decentralized Access Control	26
2.4 Accountability	27
2.5 Model-model Access Control	28
2.5.1 Model State Machine	28
Model Bell-LaPadula	29
Model Biba	30
Model Clark-Wilson	31
Model Noninterference	31
2.6 Metode-metode Identifikasi dan Otentikasi	33
2.6.1 Single Sign-On	34
2.6.2 Kerberos	34
2.7 Kepemilikan File dan Data	37
2.7.1 Pemilik Data	37
2.7.2 Pemelihara Data	37
2.7.3 Pemakai Data	37
2.8 Metode-metode Serangan	38
2.9 Ringkasan	43
2.10 Daftar Istilah	44
Daftar Acuan	49

CHAPTER 2

ACCESS CONTROL SYSTEMS

Setelah membaca suplemen bahan ajar ini diharapkan para pembaca bisa :

- Mengerti akan dasar-dasar dari kontrol akses
- Berdiskusi tentang teknik kontrol akses
- Memilih dan membandingkan model-model kontrol akses
- Mencari perbedaan dari berbagai macam teknik identifikasi dan otentifikasi
- Mengenali serangan-serangan yang umum dan menerapkan kontrol untuk pencegahannya

Bab ini menyajikan berbagai macam teknik dan metode untuk mengontrol akses dari user ke sumber daya sistem. Anda akan belajar pendekatan yang berbeda yang menyajikan bahwa hanya user yang mempunyai otorisasi yang akan bisa mengakses ke sumber daya yang dilindungi. Bab ini juga meliputi dasar-dasar dari kontrol akses, metode dan teknik yang umum yang dipakai untuk mengatur akses ke sumber daya dan serangan-serangan yang umum yang mungkin timbul dan menyerang sistem. Sebagai ilustrasi kami juga mengambil contoh penerapan di salah satu perusahaan asuransi di Indonesia, tempat penulis memberikan jasa pelayanan sistem informasi. Walaupun perusahaan yang diambil penulis bukan merupakan UKM, akan tetapi setidaknya hal ini akan dapat memberikan gambaran kepada pembaca tentang bagaimana teknik kontrol akses ini diterapkan pada sebuah perusahaan.

1.1 Pendahuluan

Seiring dengan perkembangan teknologi, mengelola keamanan komputer dan jaringan semakin lama menjadi pekerjaan yang semakin sulit dan menantang. Seorang yang bertanggung jawab terhadap keamanan harus dapat memastikan tiga hal utama dalam keamanan teknologi informasi, yaitu kerahasiaan(confidentiality), integritas(integrity), dan ketersediaan(availability).

1.1.1 Kerahasiaan

Lebih dikenal dengan istilah “confidentiality”, dapat diartikan sebagai perlindungan terhadap data dalam sistem informasi perusahaan, sehingga tidak dapat diakses oleh orang yang tidak berhak. Banyak yang beranggapan bahwa tipe perlindungan seperti ini hanya penting untuk kalangan militer dan pemerintahan, dimana mereka perlu merahasiakan rencana dan data penting. Akan tetapi kerahasiaan juga sangat penting bagi kalangan bisnis yang perlu melindungi rahasia dagang mereka dari kompetitor, atau untuk mencegah akses terhadap data-data yang dianggap sensitif oleh orang-orang yang tidak berhak didalam perusahaan (contohnya data personalia, medis, dan lainnya). Isu seputar privasi yang semakin diperhatikan akhir-akhir ini, telah memaksa badan pemerintahan dan perusahaan swasta sekalipun untuk menjaga kerahasiaan informasi secara lebih baik lagi, demi melindungi data-data pribadi yang disimpan dalam sistem informasi badan pemerintahan atau perusahaan swasta tersebut. Kerahasiaan harus terdefinisi dengan baik, dan prosedur untuk menjaga kerahasiaan informasi harus diterapkan secara berhati-hati, khususnya untuk komputer yang bersifat *standalone* atau tidak terhubung ke jaringan. Aspek penting dari kerahasiaan adalah pengidentifikasian atau otentikasi terhadap user. Identifikasi positif dari setiap user sangat penting untuk memastikan efektivitas dari kebijakan yang menentukan siapa saja yang berhak untuk mengakses data tertentu.

Ancaman terhadap kerahasiaan

Berikut ini adalah beberapa ancaman yang mungkin terjadi terhadap kerahasiaan data.

- **Hacker**

Seorang hacker adalah orang yang membobol pengendalian akses dalam sebuah sistem, dengan memanfaatkan kelemahan sistem tersebut. Selain itu banyak hacker yang sangat ahli dalam mengungkap password dan orang-orang yang berhak mengakses sistem, dimana orang-orang yang berhak mengakses sistem ini menggunakan password yang mudah ditebak atau terdaftar dalam kamus. Segala aktivitas hacker merupakan ancaman yang sangat serius terhadap kerahasiaan informasi dalam sistem informasi.

- **Masquerader**

Seorang masquerader adalah orang yang berhak mengakses sistem, tetapi telah memiliki password dari user lain sehingga dapat mengakses file yang tersedia untuk user lain tersebut. Hal ini berarti bahwa masquerader dapat menyalin file-file yang bersifat rahasia terhadap orang lain. Kegiatan “menyaru” ini sering terjadi dalam perusahaan yang memperkenankan user untuk saling berbagi password.

- **Aktivitas user yang tidak terotorisasi**

Tipe aktivitas ini terjadi saat user yang berhak untuk mengakses file-file yang sebenarnya tidak berhak untuk mereka akses. Kontrol akses yang lemah seringkali memungkinkan terjadinya akses yang tidak terotorisasi seperti ini, sehingga mengancam keamanan dari file-file yang bersifat rahasia.

- **Download file tanpa proteksi**

Melakukan download dapat mengancam kerahasiaan informasi apabila dalam prosesnya file dipindahkan dari tempat penyimpanan yang aman (dari server) ke personal komputer yang tidak terlindungi dengan baik, dalam rangka melakukan pemrosesan data secara lokal. Saat berada dalam personal komputer yang tidak terlindungi dengan baik, apabila tidak dijaga dengan baik maka informasi yang bersifat rahasia bisa diakses oleh orang-orang yang tidak berhak.

- **Local Area Network**

Khususnya untuk tipe LAN yang masih menggunakan topologi bus (masih menggunakan hub), maka ancaman terhadap kerahasiaan yang disebabkan oleh

aliran data yang dapat dilihat oleh setiap node dalam jaringan tersebut, tanpa memperdulikan apakah data dialamatkan ke node tersebut atau tidak. Hal ini menjadi penting, karena data-data dalam bentuk tidak terenkripsi bisa saja dilihat oleh orang-orang yang tidak berhak. Untuk hal ini, penting diperhatikan bahwa setiap informasi yang bersifat rahasia dan bukan untuk konsumsi umum harus dilindungi menggunakan enkripsi.

- **Trojan horse**

Program jahat ini dapat dilihat agar menyalin file-file rahasia ketempat yang tidak aman, tanpa diketahui oleh user yang berhak mengakses file tersebut. Saat dieksekusi untuk pertama kalinya, trojan horse menjadi resident dalam sistem user dan secara rutin melakukan aktivitas ilegalnya.

Model-model kerahasiaan

Model-model kerahasiaan digunakan untuk menjelaskan langkah apa saja yang perlu diambil untuk memastikan kerahasiaan informasi. selain itu, model-model tersebut juga merinci bagaimana cara menggunakan security tool untuk mencapai tingkat kerahasiaan yang diinginkan.

Model yang sering dipergunakan untuk menggambarkan proses penerapan sistem kerahasiaan informasi adalah model Bell-LaPadula. Model ini akan dibahas pada bagian-bagian berikut dalam bahan ajar ini. Model ini mendefinisikan hubungan antara obyek (contohnya : file, program, dan peralatan untuk menampung atau menerima informasi), dan subyek (contohnya : orang, proses, atau alat yang melakukan perpindahan informasi antar obyek). Hubungan diantara keduanya dijelaskan dalam istilah-istilah yang berhubungan dengan tingkat hak akses subyek dan tingkat sensitifitas dari obyek. Dalam istilah militer, hal ini dijelaskan sebagai security clearance dari subyek dan security classification dari obyek.

Subyek melakukan akses untuk membaca, menulis, atau membaca dan menulis informasi. model Bell-LaPadula menerapkan sebuah prinsip yang menentukan bahwa subyek memiliki hak tulis terhadap obyek yang berada ditingkat yang sama atau lebih rendah. Sedangkan hak baca / tulis hanya untuk obyek yang berada ditingkat yang sama dengan subyek. Prinsip ini untuk mencegah kemampuan untuk mencegah kemampuan untuk menulis informasi yang bersifat sangat rahasia kedalam file yang bersifat umum,

atau untuk mengungkapkan informasi yang sangat rahasia ke individu yang tingkat klasifikasinya lebih rendah. Karena tingkatan obyek mengindikasikan tingkat keamanan dari data yang dikandungnya, maka seluruh data dalam sebuah obyek harus berada ditingkat yang sama. Model seperti ini juga disebut sebagai flow model, karena memastikan bahwa informasi dalam tingkat keamanan tertentu hanya mengalir ke tingkat yang sama atau lebih tinggi. Tipe model lain yang juga umum digunakan adalah model kontrol akses, dimana mengorganisir sebuah sistem kedalam obyek (contohnya : resource yang ditangani), subyek (contohnya : proses dari interaksi yang terjadi) . sekumpulan aturan menentukan operasi apa yang dapat dilakukan terhadap sebuah obyek, dan oleh subyek yang mana. Model seperti ini memiliki manfaat tambahan, yaitu dapat memastikan integritas dan juga kerahasiaan informasi, sedangkan flow model hanya mendukung kerahasiaan.

Penerapan model-model kerahasiaan

Trusted system criteria yang dikembangkan oleh national computer security center dan dipublikasikan di dalam department of defense trusted computer system evaluation criteria(secara umum dikenal sebagai orange book), merupakan panduan terbaik dalam menerapkan model-model kerahasiaan yang sudah disebutkan sebelumnya. Sebagai tambahan National Computer Security Center sudah mengembangkan Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, yang merupakan aplikasi dari kriteria-kriteria dalam jaringan (secara umum dikenal sebagai Red Book).

1.1.2 Integritas

Integritas adalah perlindungan terhadap dalam sistem dari perubahan yang tidak terotorisasi, baik secara sengaja maupun secara tidak sengaja. Tantangan yang dihadapi setiap sistem keamanan informasi adalah untuk memastikan bahwa data terpelihara dalam keadaan yang sesuai dengan harapan dari user. Walau tidak dapat meningkatkan akurasi dari data yang dimasukan kedalam sistem oleh user, inisiatif keamanan informasi memastikan bahwa setiap perubahan memang benar-benar dikehendaki dan dilakukan secara benar.

Elemen tambahan dari integritas adalah kebutuhan untuk melindungi proses atau program yang digunakan untuk memanipulasi data dari modifikasi yang tidak terotorisasi. Saat paling penting dalam pemrosesan data dari kalangan komersial dan pemerintahan adalah memastikan integritas data untuk mencegah penipuan (fraud) dan kesalahan (error). Dengan demikian, sangat penting diperhatikan bahwa tidak ada user yang dapat mengubah data hingga menyebabkan hilangnya aset atau catatan keuangan, atau menyebabkan informasi yang dipakai untuk mengambil keputusan menjadi tidak *reliable*. Contoh dari sistem milik badan pemerintahan yang sangat mementingkan integritas adalah sistem pengendalian lalu lintas udara (air traffic control), sistem pengendalian persenjataan militer, dan sistem untuk mengelola kesejahteraan warga negara. Contoh untuk kalangan komersial adalah sistem pelaporan kredit, sistem pengendalian produksi, dan sistem penggajian.

Sama halnya dengan kebijaksanaan mengenai kerahasiaan, maka pengidentifikasian dan authentication terhadap user merupakan elemen kunci dari kebijaksanaan integritas data. Integritas bergantung kepada kontrol terhadap akses, dengan demikian sangat penting untuk mengidentifikasi setiap orang yang berusaha mengakses sistem secara positif dan unik.

Melindungi dari ancaman terhadap integritas

Seperti halnya kerahasiaan, integritas bisa dikacaukan oleh hacker, masquerader, aktivitas user yang tidak terotorisasi, download file tanpa proteksi, LAN, dan program-program terlarang. (contohnya : trojan horse dan virus), karena setiap ancaman tersebut memungkinkan terjadinya perubahan yang tidak terotorisasi terhadap data atau program. Sebagai contoh, user yang berhak mengakses sistem secara tidak sengaja maupun secara sengaja dapat merusak data dan program, apabila aktivitas mereka didalam sistem tidak dikendalikan secara baik.

Tiga prinsip dasar yang digunakan untuk menetapkan pengendalian integritas adalah :

- **Memberikan akses dalam kerangka need-to-know basis**

User seharusnya hanya diberikan akses terhadap file dan program yang mereka butuhkan untuk melakukan fungsi-fungsi pekerjaan mereka. Keleluasaan akses terhadap data produksi atau source code oleh user seharusnya diperketat menggunakan metode transaksi, dimana dapat memastikan bahwa user dapat mengubah data hanya dalam cara yang terkontrol dengan baik sehingga menjaga integritas data. Elemen umum dari metode transaksi ini adalah pencatatan modifikasi data dalam sebuah log, yang dapat diperiksa lebih lanjut untuk memastikan bahwa hanya perubahan yang diotorisasi dan benar saja yang dilakukan didalam sistem. Agar lebih efektif, metode transaksi ini harus memastikan bahwa data hanya dapat dimanipulasi menggunakan program-program tertentu saja. Program-program tersebut harus diawasi secara hati-hati, baik dalam pengembangan dan instalasinya, dan diterapkan pengendalian untuk mencegah modifikasi yang tidak terotorisasi. Karena user harus dapat bekerja secara efisien, hak akses harus diberikan secara bijaksana sehingga memungkinkan fleksibilitas operasional yang memadai. Akses berdasarkan *need-to-know basis* ini harus memungkinkan terjadinya kontrol maksimal dengan pembatasan seminimal mungkin terhadap user. Setiap inisiatif keamanan informasi harus menerapkan keseimbangan yang baik antara tingkat keamanan yang ideal dan produktivitas kerja.

- **Pemisahan tugas(separation of duties)**

Untuk memastikan di bahwa tidak satu orang karyawan pun yang mengendalikan sebuah transaksi dari awal sampai akhir, dua atau lebih orang harus bertanggung jawab untuk melakukannya. Contohnya adalah bahwa siapapun yang diperbolehkan untuk membuat sebuah transaksi tidak dapat dimanipulasi untuk kepentingan pribadi, kecuali seluruh orang yang terlibat didalamnya terlibat.

- **Rotasi tugas**

Penugasan suatu pekerjaan harus diubah-ubah secara periodik sehingga mempersulit user dalam berkolaborasi untuk mengendalikan sepenuhnya sebuah transaksi dan mengalihkannya untuk tujuan-tujuan terlarang. Prinsip ini sangat efektif saat digunakan bersamaan dengan prinsip pemisahan tugas. Masalah yang

timbul dalam melakukan rotasi dalam organisasi yang memiliki jumlah karyawan yang terbatas dan program pelatihan yang kurang memadai.

Model-model integritas

Model-modelintegritas ini digunakan untuk menjelaskan apa yang perlu dilakukan untuk menerapkan kebijaksanaan integritas informasi dalam organisasi. Ada tiga sasaran dari integritas yaitu :

- Mencegah user yang tidak berhak melakukan perubahan data atau program
- Mencegah user yang berhak melakukan perubahan yang tidak benar atau tidak terotorisasi
- Menjaga konsistensi data dan program secara internal dan eksternal

Langkah pertama dalam membuat model integritas untuk sebuah sistem adalah dengan mengidentifikasi dan menandai setiap bagian data yang integritasnya perlu dijaga. Kemudian ada dua prosedur yang dilakukan terhadap bagian data tersebut, pertama untuk memeriksa bahwa data valid. Berikutnya adalah proses untuk memeriksa apakah proses transformasi data atau transaksi valid, dimana kedua hal ini bisa mengubah data dari satu keadaan valid ke keadaan lainnya. Apabila dapat dipastikan bahwa hanya proses transformasi data tersebut yang dapat mengubah data, maka integritas data terjamin. Sistem untuk menjaga integritas data biasanya mengharuskan setiap proses transformasi dicatat, sebagai audit trail terhadap perubahan data. Aspek lain yang berpengaruh terhadap integritas data memiliki hubungan dengan sistem informasinya itu sendiri. Disini sistem informasi harus dapat bekerja secara konsisten dan dapat diandalkan, artinya harus melakukan apa yang diharapkan user.

1.1.3 Ketersediaan

Ketersediaan ini dapat diartikan sebagai kepastian bahwa sebuah sistem informasi dapat diakses oleh user yang berhak kapan saja sistem informasi tersebut dibutuhkan. Ada dua “pengganggu” ketersediaan yang sering dibicarakan, yaitu :

- **Denial Of Service**

Istilah ini biasanya dihubungkan dengan sebuah perbuatan yang mengunci layanan dari sistem informasi sehingga tidak bisa digunakan oleh user yang berhak. Contohnya adalah serangan worm yang memakan 90% kapasitas jaringan, sehingga server tidak bisa diakses oleh para user.

- **Hilangnya kemampuan pemrosesan data karena bencana alam atau perbuatan manusia**

Kehilangan ini mungkin lebih sering dihadapi, dan dapat ditanggulangi dengan membuat contingency plan yang dapat mengurangi waktu yang dibutuhkan untuk memulihkan kemampuan pemrosesan data saat terjadinya bencana. Contingency plan yang bisa melibatkan business resumption plan, pusat pemrosesan data alternatif, atau disaster recovery plan untuk memberikan panduan untuk menyediakan tempat pemrosesandata alternatif saat mengalami bencana, sehingga bisa memastikan ketersediaan sistem.

Masalah-masalah seputar urusan fisik, teknis dan administratif merupakan aspek penting dari inisiatif keamanan informasi untuk mengatasi isu ketersediaan. Masalah seputar urusan fisik termasuk kontrol terhadap akses demi mencegah orang yang tidak berhak untuk berhubungan langsung dengan data center, berbagai mekanisme pengendalian ancaman api dan air, hot site dan cold site yang akan digunakan sebagai tempat pemrosesan data alternatif, dan fasilitas penyimpanan backup media yang berjauhan dari data center utama. Masalah seputar urusan teknis termasuk mekanisme *fault-tolerance* (contohnya redundansi hardware, disk mirroring, dan application checkpoint restart), electronic vaulting (contohnya backup yang otomatis ke lokasi yang aman dan berjauhan dari data center utama), dan yang tidak kalah penting adalah kontrol akses dari sisi software untuk mencegah user yang tidak berhak mencoba mengganggu jalannya layanan data center. Masalah seputar urusan administratif termasuk kebijaksanaan kontrol akses, prosedur operasional, contingency plan, dan pelatihan user. Walau terlihat kurang penting, pelatihan yang memadai untuk para operator, programmer, dan petugas keamanan akan dapat membantu menghindari gangguan terhadap data center yang bisa menyebabkan hilangnya ketersediaan sistem informasi. Sebagai tambahan, ketersediaan sistem informasi bisa terhalangi apabila seorang petugas keamanan secara

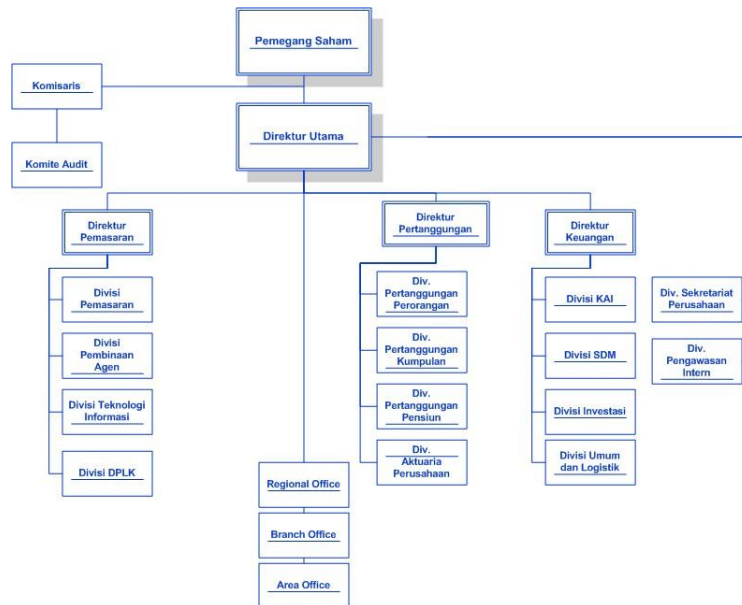
tidak sengaja mengunci database kontrol akses saat melakukan pemeliharaan rutin, sehingga mencegah user yang berhak untuk mengakses sistem dalam waktu yang cukup panjang.

1.2 Sekilas Info PT. Asuransi XXX

Sebagai pelengkap dari pembahasan ini, kami akan menyertakan contoh penerapan tentang kontrol akses ini pada sebuah perusahaan Asuransi XXX, sebagai bahan pengetahuan seberapa jauh penerapan terhadap proteksi keamanan yang akan disajikan dalam pembahasan bahan ajar berikut ini.

PT. Asuransi XXX adalah sebuah badan usaha milik negara (BUMN) yang bergerak dibidang Asuransi Jiwa. PT. Asuransi XXX terdiri dari Kantor Pusat, Kantor Wilayah (Regional Office) sebanyak 17 kantor, Kantor Cabang (Branch Office) sebanyak 70 kantor, Area Office (AO) dan UDA yang tersebar di seluruh wilayah Indonesia.

Berikut ini adalah struktur organisasi dari perusahaan tersebut.



Gambar 2.1 Struktur Organisasi PT. Asuransi XXX

1.2.1 Visi

Menjadi Perusahaan Asuransi yang Terpercaya dan Terdepan Dalam Prestasi.

1.2.2 Misi

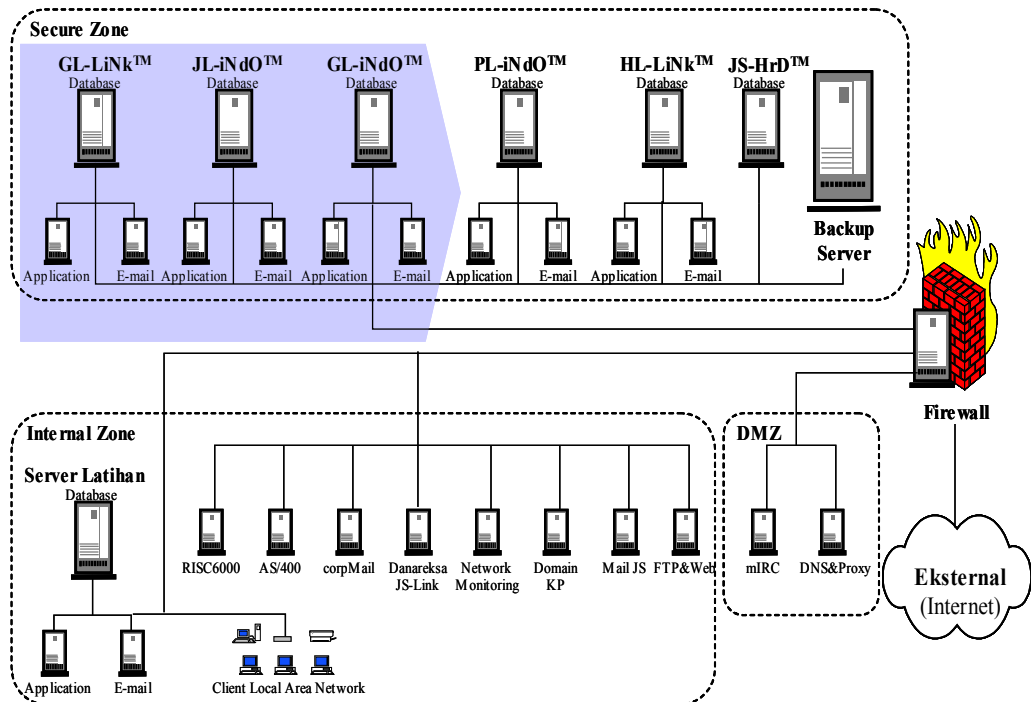
Memberikan jasa perlindungan keuangan yang berkualitas dan berorientasi kepada kepuasan pemegang polis melalui pengelolaan data secara professional.

1.2.3 Aplikasi yang dimiliki

Berdasarkan hasil pengamatan kami, diketahui bahwa PT. Asuransi XXX sampai dengan saat ini memiliki 4 aplikasi baru yang sudah dibangun untuk menunjang bisnis utama, yaitu JL-INDO, GL-INDO dan PL-INDO dan GL-LINK menggantikan aplikasi yang lama. Namun baru aplikasi JL-INDO yang sudah dipakai untuk operasional karena tiga aplikasi yang lainnya masih dalam tahap migrasi data dan penyempurnaan.

Berikut adalah gambar aplikasi *on-line* yang sudah dimiliki oleh PT. Asuransi XXX.

On-Line Application Yang Sudah Ada



Gambar 1.2: Sistem Online yang sudah ada

Berikut adalah penjelasan singkat mengenai aplikasi-aplikasi yang sudah dibangun:

JL-INDO

JL-INDO merupakan aplikasi yang dipakai untuk mendukung bisnis pertanggung jawaban perorangan. Bisnis ini merupakan bisnis yang paling banyak memberikan pemasukan premi dibanding bisnis-bisnis yang lainnya. Operasional dari aplikasi ini dilakukan di *Branch-Office* dan *Regional-Office*. Ada 2 tipe aplikasi yaitu *web-based* dan *client-server* dengan konsep *3-tier transact pattern*. Aplikasi web dipergunakan di *branch-office* untuk entry surat permintaan asuransi jiwa (spaj), pembayaran premi, pembayaran klaim, komisi dan lain sebagainya. Aplikasi *client-server* dipakai di *regional office* dan *head office* untuk setup produk baru, akseptasi, pencetakan polis, pencetakan kuitansi, *billing-booking* dan lain-lain. *Application-Server*, *Web-Server* dan *Database Server* tersentralisasi di *head-office*.

Secara garis besar aplikasi JL-INDO ini bisa kami identifikasi sebagai berikut :

Database	: ORACLE 9i
Application Server	: Sybase EAServer 5.1
Web Server	: Apache
Development Tools	: Power Builder 8, PHP
Operating System	:
Database	: AIX 5L
Application Server	: Windows Server 2003
Web Server	: Redhat Linux

GL-INDO

GL-INDO merupakan aplikasi yang dipakai untuk mendukung bisnis Pertanggungjawaban Kumpulan. Operasional berada di *Branch-Office* dan *Regional-Office*. Ada 2 tipe aplikasi yaitu *web-based* dan *client-server* dengan konsep *3-tier transact pattern*. Aplikasi web dipergunakan di *branch-office* dan *regional office* hanya untuk informasi harian atau informasi kepersertaan. Tidak ada transaksi yang dilakukan melalui aplikasi tersebut. Aplikasi *client-server* dipakai di *regional office* dan *head office* untuk administrasi produk, *new business*, pemeliharaan polis, cetak penawaran, klaim dan sebagainya. Karena jumlah peserta dari setiap perusahaan sangat besar, maka pada aplikasi ini juga dilengkapi dengan fasilitas upload data peserta, yang akan memudahkan pihak customer untuk mendaftarkan karyawannya menjadi peserta dari program ini.

Secara garis besar aplikasi GL-INDO ini bisa kami identifikasi sebagai berikut :

Database	: ORACLE 9i
Application Server	: Sysbase EAServer 5.1
Web Server	: Apache
Development Tools	: Power Builder 8, PHP
Operating System	:
Database	: AIX 5L
Application Server	: Windows Server 2003
Web Server	: Redhat Linux

PL-INDO

PL-INDO merupakan aplikasi yang dipakai untuk mendukung bisnis Pertanggungjawaban Pensiun. Sampai saat ini, operasional pertanggungjawaban pensiun baru sampai pada tingkat *regional-office* , namun kedepan akan dikembangkan sampai ke tingkat *branch office*. Aplikasi web

dipergunakan di branch-office dan regional office hanya untuk informasi harian. Aplikasi *client-server* dipakai di *regional office* dan *head office* untuk administrasi produk, *new business*, pemeliharaan polis, cetak penawaran, klaim dan sebagainya. Proses yang dilakukan mirip dengan aplikasi GL-INDO, tetapi aplikasi PL-INDO lebih banyak benefit yang harus disetup. Karena masing-masing perusahaan terkadang memiliki permintaan yang berbeda terhadap *benefit* yang ingin di *cover*, menyebabkan sistem harus bisa menyediakan fasilitas customisasi terhadap produk yang sesuai dengan keinginan customer tanpa harus mengubah *source code* dari program. Aplikasi ini termasuk kedalam *3-tier transact pattern*.

Secara garis besar aplikasi PL-INDO ini bisa kami identifikasi sebagai berikut :

Database	: ORACLE 9i
Application Server	: Sysbase EAServer 5.1
Web Server	: Apache
Development Tools	: Power Builder 8, PHP
Operating System	:
Database	: AIX 5L
Application Server	: Windows Server 2003
Web Server	: Redhat Linux

GL-LINK

GL-LINK merupakan aplikasi yang dimiliki oleh Divisi Keuangan, Akuntansi dan Investasi PT. Asuransi XXX. Aplikasi ini dipakai untuk mencatat semua transaksi keuangan yang terjadi baik untuk 3 bisnis utama maupun biaya-biaya *overhead* yang timbul akibat operasional perusahaan. Semua transaksi yang terjadi akan bermuara pada GL-LINK. Ada 2 tipe aplikasi yaitu *web-based* dan *client-server* dengan konsep *3-tier transact pattern*. Aplikasi web dipergunakan di branch-office untuk melakukan entry transaksi harian. Aplikasi *client-server* dipakai di *regional office* dan *head office* untuk entry transaksi harian, konsolidasi,

posting dan juga pencetakan laporan. Semua transaksi yang berasal dari aplikasi bisnis utama (JL-INDO, GL-INDO, PL-INDO) akan secara langsung di generate jurnalnya dan masuk kedalam database GL-LINK sehingga tidak perlu lagi ada *double entry* yang akan memperkecil kemungkinan terjadinya kesalahan entry data.

Secara garis besar aplikasi GL-LINK ini bisa kami identifikasi sebagai berikut :

Database : ORACLE 9i
Application Server : Sysbase EAServer 5.1
Web Server : Apache
Development Tools : Power Builder 8, PHP
Operating System :

Database : AIX 5L
Application Server : Windows Server 2003
Web Server : Redhat Linux

JS-HRD

JS-HRD merupakan aplikasi yang dimiliki oleh divisi sumber daya manusia. Aplikasi ini dipergunakan untuk menyimpan data karyawan, pencatatan kehadiran, pemberian tunjangan, administrasi lembur, pelatihan, penilaian karyawan, pengaturan cuti, *performance appraisal* dan sebagainya. Database yang dipakai adalah SQL Server, dengan bahasa pemrograman menggunakan Visual Basic. Aplikasi ini termasuk kedalam *2-tier transact pattern*.

2.1 Dasar kontrol akses

Kontrol akses adalah kumpulan dari metode dan komponen yang dipergunakan untuk melindungi asset informasi. merkipun informasi harus dapat diakses oleh setiap orang maka diperlukan perlindungan terhadap informasi lainnya. Kontrol akses

mendukung baik kerahasiaan dan integritas dari sebuah sistem yang aman. Kerahasiaan melindungi informasi dari orang yang tidak berhak. Anda akan menggunakan kontrol akses untuk memastikan hanya orang2 yang berhak saja yang dapat melihat informasi. integrity property melindungi informasi terhadap perubahan dari orang yang tidak berhak. Kontrol akses memberikan kemampuan untuk mendikte mana informasi yang bisa dilihat atau dimodifikasi oleh user.

Sebelumnya, anda bisa membicarakan implementasi tentang kebijakan kontrol akses. Pertama-tama anda harus membuat perencanaan. Berikut ini adalah beberapa pertanyaan yang harus dijawab:

Bagaimana caranya membedakan mana informasi yang rahasia atau tidak

Metode apakah yang harus kita ambil untuk mengidentifikasi user yang meminta akses ke informasi yang rahasia

Apa cara terbaik untuk memastikan bahwa memang user yang berhak yang akan mengakses informasi yang rahasia.

Sebagai contoh penerapan kontrol akses pada perusahaan Asuransi XXX, untuk mengamankan database SDM nya terhadap akses dari orang-orang yang tidak berhak adalah sebagai berikut. Database tersebut menggunakan SQL Server. Maka perlu ditinjau keamanan diseperti SQL Server. Tinjauan keamanan di SQL Server akan mencakup dua hal, yaitu pengamanan di SQL Server sendiri dan aplikasi yang mengakses SQL Server.

Ada beberapa alasan mengapa PT. Asuransi XXX perlu mengamankan *database* yaitu :

- Untuk Memproteksi informasi penting yang tersimpan dalam *database*. Contoh yang bagus misalnya informasi gaji yang tersimpan dalam tabel pegawai. *Management* dan *accounting* sering menggunakan informasi ini , meskipun umumnya hal ini disampaikan kepada umum(*published*) ke seluruh perusahaan.
- Untuk memproteksi objek *database access* dari usaha perubahan. Perubahan yang tidak berhak pada *database* dapat menyebabkan kerusakan atau tidak berfungsi.
- Untuk memproteksi kekayaan intelektual dari desain *database* dan kode dalam aplikasi.

Untuk men-set keamanan untuk *network databases* dimana terletak sumber data anda, langkah pertama adalah berpikir tentang apakah tipe keamanan yang anda perlukan. Anda perlu mempertimbangkan jawaban dari pertanyaan di bawah ini:

- Kelompok mana yang perlu mengakses *database*?
- Informasi penting yang harus dibatasi dari kelompok tertentu?
- Bagaimanakah *set up network* dan *file system* menangani kerahasiaan file?

Jawaban atas dua pertanyaan pertama membantu anda mengorganisir *user groups* dan men-set ijin akses *database*, sementara pertanyaan lainnya menentukan bagaimana mengkonfigurasi *file system*nya. Berikut akan diberikan beberapa contoh pengamanan yang bisa dilakukan yang berhubungan dengan kontrol akses ke dalam database.

Keamanan SQL Server

Beberapa hal yang perlu dilakukan sehubungan dengan keamanan SQL Server sebagian besar berhubungan dengan kontrol akses.

1. Lakukan scanning keamanan jaringan anda dengan tool security

Tool seperti Microsoft Baseline Security Analyzer merupakan salah satu tool yang melakukan scanning terhadap network dan server untuk mendeteksi celah keamanan yang ada di dalam sistem.

2. Lakukan Service pack SQL Server yang up-to-date
3. Membatasi hak akses account yang ada

Lakukan setting domain user account untuk menjalankan service MSSQL server dan SQL Agent. Domain user account tersebut hendaknya diberi hak/privilege sebagai user biasa, bukan berada dalam grup administrator. Peralnya, resiko keamanan SQL Server akan meningkat apabila setting privilege domain user account melebihi setting minimal yang dibutuhkan oleh service tersebut. Bila service SQL Agent tidak diperlukan, setting saja menjadi manual atau di disable saja.

4. Gunakan Otentikasi berbasis Windows

Otentikasi SQL server terdiri atas dua jenis yaitu Windows Authentication dan SQL server Mix Authentication. Windows authentication menjamin keamanan yang lebih karena user tidak perlu memasukan user id dan password ke dalam aplikasi yang terhubung dengan SQL Server. Selain itu, Windows Authentication memperkecil peluang masuknya hacker lewat internet dengan melakukan setting akses hanya untuk domain account.

5. Blok dengan firewallll untuk port yang menjadi target serangan worm Slammer
6. Gunakan password sa yang sulit ditebak

Kompleksitas password untuk login sa menentukan tingkat kerentanan keamanan SQL Server. Jika password tersebut mudah ditebak baik secara manual maupun lewat brute-force dictionary searching, maka penyusuf akan dengan mudah mengambil alih sistem SQL Server.

7. Tetapkan ajses keamanan secara fisik

Keamanan SQL server kurang lengkap bila tidak dibarengi dengan akses fisik secara terkendali ke sistem SQL Server. Audit terhadap akses fisik SQL Server perlu dilakukan secara berkelanjutan dan konsisten.

Keamanan Akses aplikasi ke SQL Server

- Isu utama mengenai keamanan aplikasi yang akan mengakses SQL Server adalah isu mengenai SQL Injection. Pencegahan terhadap SQL Injection ini perlu dilakukan lewat aplikasi itu sendiri. Beberapa langkah yang bisa dilakukan untuk menghindari serangan jenis ini adalah :
 - Validasi tanda baca tunggal (‘)
 - Hindari penggunaan dynamic SQL
 - Lakukan validasi input
 - Terapkan prinsip hak akses (privilege) seminimal mungkin.

Disamping keamanan terhadap database SDM, PT Asuransi XXX juga sudah melakukan kontrol akses terhadap data-data yang lain seperti data Pertanggung Perorangan, Pertanggung Kumpulan maupun Pertanggung Pensiun. Kontrol

akses pada ketiga sistem ini dilakukan baik didalam databasenya sendiri maupun dari aplikasi yang dibangun. Sebagai contoh, setiap user yang akan memakai aplikasi diberikan hak akses yang berbeda yang disesuaikan dengan hak dan tanggung jawabnya dalam organisasi. Disamping itu dari database nya sendiri sudah mengatur mengenai pemberian *roles* tertentu untuk orang atau user tertentu dan apa yang bisa dilakukan. Dalam sistem operasi yang dipakai juga dilakukan sama. Ada seseorang administrator yang khusus mengetahui dan bertanggung jawab terhadap keamanan mesin tersebut. Jadi bisa dikatakan database merupakan asset yang sangat perlu diamankan diantaranya menggunakan password dan menentukan akses kontrol. Hal itu tentu saja sangat tidak cukup mengamankan data, komponen lain tentu saja harus saling melengkapi mulai dari kebijakan manajemen untuk menentukan anggaran bagi keamanan data, kesadaran akan pentingnya keamanan data , sumber daya manusia termasuk administor yang mumpuni serta terus meng-*update* pengetahuannya. Ancaman terhadap keamanan data dapat datang dari mana saja, levelnya beragam misalnya, level fisik, sistem operasinya maupun dari level aplikasi

2.1.1 Subyek dan Obyek

Kontrol akses adalah semua yang mengatur tentang proses pengontrolan akses. Pertama-tama kita akan mendefinisikan beberapa pengertian. Sebuah entitas yang meminta akses ke sebuah sumberdaya disebut sebagai akses dari subjek. Sebuah subjek merupakan entitas yang aktif karena dia menginisiasi sebuah permintaan akses. Sebuah sumber daya yang akan diakses oleh subyek disebut sebagai objek dari akses. Objek dari akses merupakan bagian yang pasif dari akses karena subjek melakukan aksei terhadap obyek tersebut. Jadi tujuan dari kebijakan kontrol akses adalah mengijinkan hanya subyek yang mempunyai otorisasi yang bisa mengakses obyek yang sudah diijinkan untuk diakses. Hal ini mungkin juga ada subjek yang sudah mempunyai otorisasi tapi tidak melalukan akses terhadap spesifik obyek tertentu.

2.1.2 Least Privilege

Organisasi-organisasi menggunakan beberapa kebijakan dalam menerapkan peraturan kontrol akses. Filosofi yang paling tidak aman (paling berbahaya) adalah

memberikan hak akses kepada setiap orang secara default. Memang kelihatannya mudah akan tetapi hal ini mudah juga untuk di bobol. Jadi pada metode ini, kita harus memastikan bahwa semua akses harus dibatasi, administrasi yang buruk bisa menyebabkan lubang kemanan. Filosofi dari least privilege adalah sebuah subject hanya diberikan hak sesuai dengan keperluannya tidak lebih. Least privilege membantu menghindari authorization creep, yaitu sebuah kondisi dimana sebuah subject memiliki hak akses lebih dari apa sebenarnya dibutuhkan. Pada asuransi XXX ini, mereka memberikan hak tertentu kepada user yang memang memiliki tanggung jawab untuk menjaga semua operasi yang melibatkan database berjalan lancar tanpa gangguan. Sehingga orang tersebut diberikan userid dan password yang bisa dipakai untuk melakukan monitor terhadap beberapa server untuk keperluan operasional.

2.1.3 Controls

Kontrol adalah sebuah mekanisme yang mengatur mana yang berhak dan tidak berhak melakukan akses terhadap sebuah object. Kontrol bisa menjadi penjaga keamanan informasi dari serangan. Berikut adalah katagori kontrol yang umum.

Control Category	Description	Example
Administrative	Prosedur dan kebijakan yang di desain untuk mewujudkan peraturan keamanan	Hiring practices Usage monitoring and accounting Security awareness training
Logical(Technical Control)	Pembatasan akses terhadap object dengan menggunakan software atau hardware	User identification atau authentication Encryption Segregated network architecture
Physical	Physical acces to	Fences

	hardware limited	Walls Locked Door
--	------------------	----------------------

Tabel 2.1 Kategori Kontrol Umum

2.2 Teknik-teknik Kontrol Akses

Anda harus memilih teknik kontrol akses yang cocok terhadap organisasi agar bisa memberikan tingkat keamanan yang paling maksimum. Beberapa teknik yang biasa digunakan.

2.2.1 Rancangan Kontrol Akses

Rancangan Kontrol Akses mendefinisikan peraturan terhadap user dalam melakukan akses terhadap file atau device. Berikut adalah 3 desain kontrol akses yang umum dipergunakan.

Mandatory Access Control

Mandatory access control yaitu memberikan sebuah label keamanan terhadap semua subjects dan object.

Classification	Description	
Unclassified	Data tidak sensitive atau classified	
Sensitive but unclassified (SBU)	Data bisa menyebabkan kerugian jika tidak dicuri	
Confidential	Data hanya untuk kalangan internal	
Secret	Data yang bisa menyebabkan kerusakan serius pada keamanan nasional	
Top Secret	Data yang bisa menyebabkan kerusakan	

	yang parah pada keamanan nasional	
--	-----------------------------------	--

Tabel 2.2 Military Data Classification

Classification	Description	
Public	Data tidak di lindungi dimanapun	
Sensitive	Informasi bisa berpengaruh terhadap bisnis dan kepercayaan public jika tidak dilindungi dengan baik	
Private	Informasi personal yang bisa berakibat negatif terhadap seseorang jika bocor	
Confidential	Informasi perusahaan yang bisa berakibat negatif terhadap organisasi jika bocor	

Tabel 2.3 Klasifikasi Data Komersil

Satu lagi metode implementasi yang umum dipakai adalah rule-based access control. Pada metode ini semua akses diberikan melalui referensi security clearance dari subject dan security label dari object. Kemudian peraturan menentukan mana dari permintaan akses tersebut yang di berikan dan mana yang ditolak. Need to know property mengindikasikan sebuah subject memerlukan akses kepada object untuk menyelesaikan kegiatan.

Directional Access Control

Directional Access Control mempergunakan identitas dari subject untuk menentukan apakah permintaan akses tersebut akan dipenuhi atau di tolak. Acces control ini di desain kurang aman daripada mandatory access control tetapi merupakan desain yang paling umum dipergunakan pada berbagai sistem operasi. Metode ini lebih mudah

di implementasikan dan lebih fleksibel. Setiap object memiliki permissions, yang menentukan user atau group yang bisa melakukan akses terhadap object.

Directional access control termasuk Identity-based access control dan access control list. Identity-based access control membuat keputusan untuk akses terhadap akses berdasarkan userid atau keanggotaan group dari user yang bersangkutan. Pemilik dari object yang menentukan user atau group yang mana yang bisa melakukan akses terhadap object. Kebanyakan sistem operasi memberikan hak akses read, write and execute permissions. Untuk membuat administrasi menjadi lebih mudah maka Access Control Lists(ACLs) mengizinkan groups dari objects, atau groups dari subjects untuk dikontrol bersama-sama. Access Control Lists dapat memberikan hak akses terhadap group dari subject atau memberikan hak kepada akses group dari subjects kepada object tertentu.

Nondiscretionary Access Control

Ini merupakan desain kontrol akses yang ketiga. biasanya menggunakan role dari subjects atau kegiatan yang di assigned kepada sebuah subject, untuk menerima atau menolak akses. Nondiscretionary access control disebut juga roled-based acces control atau task base access control. Tipe kontrol akses ini cocok dipakai pada kasus high turnover atau reassginments. Ketika security di asosiasikan kedalam sebuah role atau task, mengganti orang yang mengerjakan tugas membuat security administration lebih mudah.

Lattice-based access control adalah salah satu variasi dari desain nondiscretionary access control. Disamping mengasosiasikan beberapa kontrol akses dengan task atau role yang spesifik, masing-masing hubungan antara subject dan object memiliki beberapa pasang batasan. Batasan akses ini yang mendefinisikan peraturan dan kondisi yang mengizinkan mengakses sebuah object. Pada kebanyakan kasus, batas akses mendefinisikan batas atas dan batas bawah yang menyatakan klasifikasi dari keamanan dan label.

2.3 Access Control Administration

Langkah berikutnya dari organisasi setelah melakukan desain terhadap kontrol akses adalah menentukan access control administration. Access control administration bisa di implementasikan baik centralized atau decentralized. Pilihan terbaik dalam melakukan administrasi tergantung dari kebutuhan dari organisasi dan sensitivitas informasi yang disimpan dalam sistem komputer.

2.3.1 Centralized Access Control

Centralized access control administration memerlukan sebuah pusat keamanan yang bisa menentukan apakah sebuah permintaan akan disetujui atau ditolak. Pendekatan ini sangat mudah karena object hanya di pelihara pada lokasi yang tunggal. Salah satu kelemahannya adalah central access control bisa menjadi single point of failure. Jika central access control rusak, maka semua object tidak akan bisa diakses. Dampak negatif yang lainnya adalah dalam masalah performance, jika sistem tidak bisa memenuhi semua permintaan dari user. Anda dapat memilih beberapa paket yang biasa dipakai dalam mengimplementasikan administrasi terhadap kontrol akses.

Remote Authentication Dial-In User Service(RADIUS) menyediakan kontrol akses kepada user yang melakukan dial-in. user di validasi berdasarkan list dari user yang ada di RADIUS server. Anda bisa melakukan hang-up dan memanggil user kembali melalui nomor telepon yang ada di server. Contoh lain dari Centralized Access Control for Dial-In User adalah Challenge Handshake Authentication Protocol(CHAP). CHAP menampilkan tantangan ketika user meminta akses. Jika user merespon tantangan tersebut dengan benar maka user tersebut akan diberikan hak CHAP mengembangkan keamanannya dengan melakukan enkripsi selama pertukaran pesan.

Centralized Access Control untuk aplikasi network bisa menggunakan TACACS(Terminal Access Controller Access Control System). TACACS menyediakan services umum untuk melakukan Authentication dan Authorization.

2.3.2 Decentralized Access Control

Decentralized Access Control meletakkan tanggung jawab dari lebih dekat terhadap object. Pendekatan ini memerlukan lebih banyak administrasi daripada centralized access control karena sebuah object mungkin saja memerlukan sangat aman pada lokasi tertentu. Tapi hal ini bisa lebih stabil karena tidak ada Single Point Of Failure. Decentralized Access Control biasanya diimplementasikan memakai **security domain**. Security domain adalah bagian sebuah kepercayaan, atau koleksi dari object dan subject, yang mendefinisikan access rule dan permissions. Subject harus termasuk dalam domain tersebut. Pendekatan ini bisa memudahkan untuk mengeluarkan subject yang dicurigai, tetapi bisa membuat administrasi secara umum lebih sulit karena berbagai macam variasi dari peraturan keamanan.

2.4 Accountability

Sistem audit membantu administrasi dengan membuat log dari aktifitas. Log aktifitas ini memudahkan administrator sistem untuk memonitor siapa saja yang memakai sistem dan apa yang dilakukannya. Log dari sistem yang diperoleh selama monitoring bisa dipergunakan untuk :

- Mengidentifikasi aktifitas yang tidak biasa

- Dokumen yang dipakai untuk kemungkinan aksi berikutnya.

- Menggunakan informasi untuk menentukan aksi yang tidak sepatutnya dimasa yang akan datang

- Memastikan bahwa user yang ada sudah di lindungi oleh kebijakan keamanan yang ada sekarang.

Penggunaan koleksi informasi dengan auditing memberi keyakinan bahwa masing-masing user memang berhak mengakses sistem informasi. Dengan auditing semua aktifitas bisa terekam dan bisa di lacak termasuk user yang melakukannya. Administrator

juga harus mengeluarkan effort untuk menjamin kerahasiaan dan integritas dari log yang sensitif.

Administrator bisa menentukan event mana saja yang perlu di audit. Salah satu metode yang umum dipakai untuk membatasi kapasitas dari log adalah dengan menggunakan **clipping levels**, yang akan membatasi tidak diperlukannya log dari aktifitas kecuali kalau ada suatu kejadian. Sebagai contoh, kita bisa menentukan clipping level dari kegagalan login sampai 3 kali. Jika user gagal melakukan login sampai 2 atau 3 kali, tidak ada auditing informasi yang akan dilakukan. Ketika login yang ketiga gagal, maka login ketiga dan kejadian selanjutnya dicatat. Hal ini akan memudahkan administrator untuk memisahkan data dan melihat hanya terhadap data yang mengalami keanehan.

2.5 Access Control Models

Access Control Models sangat berfungsi dalam menentukan jenis kontrol akses yang diperlukan dalam mendukung kebijakan keamanan. Model akses kontrol ini menyediakan view konseptual dari kebijakan keamanan. Hal ini akan memungkinkan kita untuk melakukan pemetaan antara tujuan dan petunjuk dari kebijakan keamanan anda terhadap event yang spesifik. Proses dari pemetaan ini memungkinkan terbentuknya definisi formal dan spesifikasi yang diperlukan dalam melakukan kontrol terhadap keamanan. Singkatnya, access control model memungkinkan untuk memilah kebijakan keamanan yang kompleks menjadi langkah –langkah keamanan yang lebih sederhana dan terkontrol. Beberapa model yang berbeda sudah dibangun sampai dengan tahun ini. Kita akan membahas beberapa model yang dianggap unik pada bagian-bagian selanjutnya. Kebanyakan penerapan kebijakan keamanan melakukan kombinasi dari beberapa access control models.

2.5.1 State Machine Model

State Machine model adalah kumpulan dari defined instances, yang disebut state, dan sebuah transisi yang spesifik yang diijinkan untuk melakukan modifikasi terhadap object dari satu state ke state berikutnya. State machine sering dipakai untuk real-life entities ketika state yang spesifik dan transisinya ada dan dimengerti. Ketika sebuah subject meminta untuk membaca sebuah object, harus ada sebuah transisi yang mengijinkan untuk merubah sebuah object yang closed menjadi open object. Gambar 2.1 menunjukkan diagram dari state machine yang sederhana. State direpresentasikan oleh lingkaran, dan transisinya direpresentasikan oleh anak panah.

Model Bell-LaPadula

Bell-LaPadula dibangun pada tahun 1970an untuk membantu pemahaman yang lebih baik dan mengimplementasikan kontrol kerahasiaan. Angkatan bersenjata Amerika Serikat sangat tertarik dalam memproteksi data yang terklasifikasi sementara membiarkan peningkatan jumlah akses terhadap mesin yang menyimpan data rahasia. Karena angkatan bersenjata sangat tertarik dengan kerahasiaan data, model ini bekerja baik dalam organisasi yang fokus utamanya tertuju pada kontrol kerahasiaan. Model Bell-LaPadula adalah model state machine yang membuat daftar kontrol akses dan label keamanan untuk mengimplementasikan keamanan objek.

Model ini menggunakan dua properti dasar untuk mengevaluasi permintaan akses. Tabel 2.4 memperlihatkan properti-properti dasar dan istilah umumnya.

Properti-properti tersebut terlihat membingungkan pada awalnya, namun perhatikan apa yang dinyatakan oleh masing-masing properti tersebut. Perlu diingat bahwa kerahasiaan merupakan fokus utamanya. Aturan keamanan sederhana melindungi keterungkapan informasi oleh subjek yang tidak memiliki otoritas. Properti **-property* melindungi data sensitif atau rahasia terhadap kemungkinan disimpan dalam objek yang memiliki tingkat keamanan yang lebih rendah. Jika hal tersebut terjadi, seseorang dapat mencuplik sebuah paragraf dari dokumen sangat rahasia ke dalam dokumen yang diklasifikasikan sebagai dokumen publik. Penyalinan semacam ini akan mengungkapkan informasi rahasia kepada

setiap orang yang hanya dapat melihat dokumen publik. Hal ini jelas melanggar kerahasiaan dari informasi yang tersalin ke dalam dokumen publik.

Property	Common Name	Description
Simple security rule	No read up	A subject of a given security clearance cannot read data from a higher security level.
*-property (star property)	No write down	A subject of a given security clearance cannot write to an object at a lower security level.

Tabel 2.4 Properti-properti Bell-LaPadula

Model Biba

Model Biba dibangun setelah model Bell-LaPadula untuk mengatasi masalah integritas data. Model Biba juga dibangun berbasis model state machine dan mendefinisikan state dan transisi yang berfokus pada integritas data, bukan kerahasiaan. Model Biba dengan cepat menjadi populer dalam dunia bisnis karena fokus utamanya adalah untuk menjamin bahwa objek yang tidak memiliki otoritas tidak dapat melakukan perubahan terhadap objek.

Mirip dengan model Bell-LaPadula, Model Biba menggunakan dua properti dasar untuk mengevaluasi permintaan akses. Tabel 2.5 memperlihatkan properti-properti dasar Biba dan istilah umumnya.

Property	Common Name	Description
Simple integrity property	No read down	A subject cannot read an object of a lower integrity level.
*-property (star property)	No write up	A subject cannot write to an object of a higher integrity level.

Tabel 2.5 Properti-properti Biba

Model Clark-Wilson

Model Clark-Wilson dibangun setelah model Biba. Tidak seperti model Bell-LaPadula dan Biba, model Clark-Wilson tidak berbasis pada model state machine; model ini menggunakan pendekatan yang berbeda untuk menjamin integritas data. Model Clark-Wilson tidak melakukan pemberian akses suatu subjek terhadap objek, melainkan memblokir semua akses terhadap sejumlah kecil program akses yang dikontrol secara ketat. Pendekatan ini berhasil dalam aplikasi komersial dimana integritas data seringkali lebih penting daripada kerahasiaan data secara keseluruhan.

Model Clark-Wilson menetapkan beberapa istilah yang perlu dipahami untuk mengikuti alur akses model:

Constrained data item (CDI): semua bagian data yang dilindungi oleh model

Unconstrained data item (UDI): Data yang tidak dilindungi oleh model (contoh, input atau output data)

Integrity verification procedure (IVP): prosedur yang menguji integritas dari suatu bagian data

Transformation Procedure (TP): Setiap prosedur yang membuat perubahan yang sah terhadap suatu bagian data.

Model Clark-Wilson menjamin semua *unconstrained data* disahkan oleh IVP, dan kemudian dimasukkan ke dalam sistem oleh TP. Semua modifikasi selanjutnya disahkan

terlebih dahulu oleh IVP, dan kemudian perubahan dilakukan oleh TP. Tentunya IVP dan TP tidak dipanggil sebelum subjek telah terotentikasi dengan benar dan diperbolehkan untuk mengakses objek sesuai permintaan.

Model Noninterference

Model kontrol akses yang terakhir adalah seringkali suatu pelengkap bagi model lainnya. Model Noninterference menjamin bahwa perubahan pada suatu tingkat keamanan tidak mengorbankan level keamanan lainnya dan mempengaruhi suatu objek dalam konteks yang lain. Sebagai contoh, apa yang terjadi bila dokumen rahasia yang telah disertakan dalam dokumen publik disimpan? Bahaya dalam kasus ini sangat jelas: Terdapat resiko keterungkapan data rahasia ketika informasi tersebut disalin ke dalam dokumen publik. Dasar pemikiran dari model noninterference adalah bahwa setiap tingkatan keamanan memiliki perbedaan dan perubahan tidak akan berpengaruh terhadap tingkatan lain. Jaminan ini mempersempit cakupan suatu perubahan dan mengurangi kemungkinan bahwa suatu perubahan memiliki efek samping yang tidak disengaja. Dengan menutup kemungkinan modifikasi terhadap tingkatan keamanan tertentu, model ini dapat memelihara integritas dan kerahasiaan data.

2.6 Metode-metode Identifikasi dan Otentikasi

Elemen *user interface* yang pertama kali ditemui kebanyakan subjek ketika mengakses sistem informasi adalah identifikasi dan otentikasi. Tahap identifikasi memperkenalkan subjek mengklaim sebagai entitas tertentu dengan menunjukkan bukti-bukti identitas. Bukti-bukti tersebut dapat sesederhana *user ID* atau nomer PIN, atau yang lebih kompleks seperti atribut fisik. Setelah subjek mengklaim suatu identitas, sistem memvalidasi apakah user tersebut terdaftar dalam *user database* dan membuktikan bahwa subjek tersebut adalah benar-benar sebagai entitas yang diklaimnya. Tahap otentikasi meminta subjek menunjukkan informasi tambahan yang berkesesuaian dengan informasi

tentang subjek tersebut yang telah disimpan. Dua tahap ini sering disebut dengan otentikasi dua faktor, yang memberikan proteksi terhadap subjek yang tidak memiliki otoritas untuk mengakses sistem. Setelah subjek diotentikasi, sistem kontrol akses mengevaluasi hak dan izin subjek untuk mengabulkan atau menolak permintaan akses terhadap objek. Tahap ini disebut dengan tahap otorisasi.

Ada tiga kategori/tipe umum dari informasi otentikasi. Pratek pengamanan yang baik biasanya membuat tahap identifikasi dan otentikasinya memerlukan input setidaknya dari dua tipe berbeda. Tiga tipe umum data otentikasi dijelaskan dalam Tabel 2.6.

Authentication Type	Description	Examples
Type 1	What you know	Password, passphrase, PIN, lock combination
Type 2	What you have	Smart card, token device
Type 3	What you are	Biometrics—fingerprint, palm print, retina/iris pattern, voice pattern

Tabel 2.6. Tipe-tipe otentikasi

Tipe otentikasi yang paling umum dan paling mudah untuk di implementasikan adalah otentikasi tipe 1. Yang dilakukan adalah meminta subjek membuat *password*, *passphrase*, atau nomer PIN. Alternatif lain adalah menyediakannya untuk user. Kesulitan dalam otentikasi tipe 1 adalah perlunya mendorong subjek untuk membuat frase yang sangat sulit diterka oleh orang lain, namun tidak terlalu rumit sehingga sulit untuk diingat. Password (frase atau PIN) yang sulit diingat akan mengurangi nilai dari password itu sendiri. Hal tersebut dapat terjadi bila administrator terlalu sering memerlukan penggantian password sehingga user kesulitan untuk mengingat password terbaru. Jadi, yang disarankan adalah menjaga password secara rahasia dan aman. Aturan-aturan berikut ini adalah petunjuk yang baik untuk membuat password yang aman:

- Password setidaknya memiliki panjang 6 karakter.
- Password setidaknya mengandung sebuah angka atau karakter tanda baca.
- Tidak menggunakan kosakata atau kombinasi kosakata.
- Tidak menggunakan data pribadi, seperti tanggal kelahiran, nama anggota keluarga atau binatang peliharaan, atau lagu atau hobi favorit.
- Tidak sesekali menuliskan password.
- Membuat password yang mudah diingat tetapi sulit diterka.

Data otentikasi tipe 2 lebih rumit untuk dilakukan karena subjek perlu membawa suatu alat atau sejenisnya. Alat tersebut umumnya perangkat elektronik yang menghasilkan suatu nilai yang bersifat sensitif terhadap waktu atau suatu jawaban untuk diinput. Meskipun otentikasi tipe 2 lebih rumit, tipe ini hampir selalu lebih aman dibandingkan dengan otentikasi tipe 1.

Otentikasi tipe 3, atau *biometrics* adalah yang paling canggih. Biometric menggambarkan pendeteksian dan pengklasifikasian dari atribut fisik. Terdapat banyak teknik biometric yang berbeda, diantaranya:

- Pembacaan sidik jari/telapak tangan
- Geometri tangan
- Pembacaan retina/iris
- Pengenalan suara
- Dinamika tanda tangan

Karena kerumitannya, biometric adalah tipe otentikasi yang paling mahal untuk diimplementasikan. Tipe ini juga lebih sulit untuk dipelihara karena sifat ketidaksempurnaan dari analisis biometric. Dianjurkan untuk berhati-hati beberapa masalah-masalah utama dari eror-eror biometric. Pertama, sistem mungkin menolak subjek yang

memiliki otoritas. Ukuran kesalahan semacam ini disebut dengan *false rejection rate* (FRR). Di sisi lain, sistem biometric mungkin menerima subjek yang salah. Ukuran kesalahan semacam ini disebut dengan *false acceptance rate* (FAR). Yang menjadi masalah adalah ketika sensitifitas sistem biometric diatur untuk menurunkan FRR, maka FAR meningkat. Begitu juga berlaku sebaliknya. Posisi pengaturan yang terbaik adalah bila nilai FRR dan FAR seimbang, ini terjadi pada *crossover error rate* (CER).

2.6.1 Single Sign-On

Semakin banyak informasi, atau faktor, yang diminta dari subjek, semakin menjamin bahwa subjek adalah benar-benar entitas yang diklaimnya. Oleh karenanya, otentikasi dua faktor lebih aman dari otentikasi faktor tunggal. Masalah yang timbul adalah bila subjek ingin mengakses beberapa sumber daya pada sistem yang berbeda, subjek tersebut mungkin diminta untuk memberikan informasi identifikasi dan otentikasi pada masing-masing sistem yang berbeda. Hal semacam ini dengan cepat menjadi sesuatu yang membosankan. Sistem *Single Sign-On* (SSO) menghindari *login* ganda dengan cara mengidentifikasi subjek secara ketat dan memperkenankan informasi otentikasi untuk digunakan dalam sistem atau kelompok sistem yang terpercaya. *User* lebih menyukai SSO, namun administrator memiliki banyak tugas tambahan yang harus dilakukan. Perlu perhatian ekstra untuk menjamin bukti-bukti otentikasi tidak tersebar dan tidak disadap ketika melintasi jaringan. Beberapa sistem SSO yang baik kini telah digunakan. Tidak penting untuk memahami setiap sistem SSO secara detail. Konsep-konsep penting dan kesulitan-kesulitannya cukup umum bagi semua produk SSO. Berikut adalah salah satu produk SSO, Kerberos, yang akan dikaji bagaimana sistem ini bekerja.

2.6.2 Kerberos

Sistem Kerberos berasal dari Athena, proyek Massachusetts Institute of Technology (MIT). Kerberos memberikan proteksi baik terhadap otentikasi dan pesan. Kerberos menggunakan kriptografi kunci simetris (kedua sisi memiliki kunci yang sama)

untuk meng-enkripsi pesan. Fitur dari enkripsi memberikan keamanan bersifat *end-to-end*, yang berarti bahwa mesin yang berada di antara mesin asal dan target tidak dapat melihat isi dari pesan. Kerberos berkembang populer untuk digunakan dalam sistem yang terdistribusi. Walaupun dapat bekerja baik dalam lingkungan yang terdistribusi, kerberos sendiri menggunakan server tersentralisasi untuk menyimpan kunci-munci kriptografi.

Kerberos mencakup sebuah repositori data dan proses otentikasi. *Key Distribution Center* (KDC) berada di pusat dari Kerberos. KDC menyimpan semua kunci kriptografi dari subjek dan objek. KDC memiliki peran untuk memelihara dan mendistribusikan kunci-kunci tersebut, juga menyediakan layanan otentikasi (AS, *Authentication Service*). Ketika KDC menerima permintaan akses terhadap suatu objek, KDC memanggil AS untuk melakukan otentikasi terhadap subjek dan permintaannya. Bila permintaan subjek diotentikasi, AS membuat tiket akses yang berisi kunci bagi subjek dan objek kemudian mendistribusikan kunci tersebut ke subjek dan objek. Berikut adalah langkah-langkah dasar dalam siklus permintaan akses Kerberos:

1. Subjek melakukan permintaan akses terhadap suatu objek. Software Kerberos subjek meminta user ID, dan mengirim user ID tersebut bersama permintaan subjek ke KDC.
2. KDC memanggil AS untuk melakukan otentikasi terhadap subjek dan objek.
3. Jika otentikasi diberikan, KDC mengirimkan sebuah kunci sesi yang ter-enkripsi ke mesin subjek dan objek.
4. Software Kerberos klien subjek meminta password subjek dan menggunakannya, bersama dengan kunci rahasia subjek, untuk men-dekripsi kunci sesi.
5. Kemudian subjek mengirim permintaan akses bersama dengan kunci sesi ke objek.
6. Objek men-dekripsi kunci sesi yang diterima dari KDC dan membandingkannya dengan kunci sesi yang diterimanya bersamam permintaan akses.
7. Jika kedua kunci sesi bersesuaian, akses dikabulkan.

Sifat tersentralisasi dan KDC menampakkan satu dari kelemahan utama Kerberos: KDC merupakan titik tunggal kegagalan. Kegagalan KDC berarti kegagalan akses objek. KDC juga dapat menjadi *bottleneck* kinerja bagi mesin berbeban besar. Juga, terdapat sedikit

peluang saat kunci sesi berada dalam mesin klien. Terbuka kemungkinan bagi penyusup untuk menanngkap kunci ini dan mendapatkan akses terhadap sumber daya tanpa terotorisasi. Meskipun meiliki beberapa kekurangan, Kerberos merupakan contoh yang baik dari sistem SSO dan telah mendapat sambutan luas.

2.7 Kepemilikan File dan Data

File dan data dapat mengandung informasi penting dan berharga. Informasi penting ini perlu menjadi fokus dari usaha pengamanan. Tetapi siapakah yang bertanggung jawab terhadap penjaminan keamanan dari informasi suatu organisasi? Pertanyaan ini terjawab dengan menetapkan tanggung jawab berlapis atas setiap informasi penting. Setiap file, atau elemen data, perlu menetapkan sekurang-kurangnya tiga pihak yang bertanggung jawab. Tiga lapis tanggung jawab tersebut mewakili prasyarat dan tindakan berbeda untuk masing-masing kelompok. Lapisan-lapisan yang paling umum adalah *data owner* (pemilik data), *data custodian* (pemelihara data), dan *data user* (pengguna data). Masing-masing lapisan memiliki peranan tertentu untuk mendukung kebijakan keamanan organisasi.

2.7.1 Pemilik Data

Pemilik data memikul tanggung jawab terbesar terhadap proteksi dari data. Pemilik data umumnya adalah anggota manajemen dan berperan sebagai wakil dari organisasi dalam tugas ini. Ia adalah pemilik yang menentukan tingkat klasifikasi data dan mendelegasikan tanggung jawab pemeliharaan sehari-hari kepada pemelihara data. Jika terdapat pelanggaran keamanan, maka pemilik data-lah yang memikul beban berat dari setiap masalah kelalaian.

2.7.2 Pemelihara Data

Pemilik data menugaskan pemelihara data untuk melaksanakan kebijakan keamanan sesuai dengan klasifikasi data oleh pemilik data. Pemelihara sering kali merupakan staff departemen TI dan mengikuti prosedur tertentu untuk mengamankan dan melindungi data yang ditugaskan. Ini termasuk menerapkan dan merawat kontrol yang sepatutnya, melakukan backup dan memvalidasi integritas data.

2.7.3 Pemakai Data

Akhirnya, pemakai data adalah salah satu yang mengakses data setiap harinya. Mereka dibebankan tanggung jawab untuk mengikuti kebijakan keamanan sewaktu mengakses data. Anda harus berharap untuk melihat lebih banyak prosedur formal yang terkait dengan data penting, dan pemakai dapat diandalkan atas penggunaan data dan mendukung prosedur tersebut. Sebagai tambahan pada komitmen untuk mengikuti prosedur keamanan, pemakai harus menyadari betapa pentingnya prosedur keamanan kepada kesehatan organisasi. Seringkali, pemakai mengambil jalan pintas untuk melewati kontrol keamanan karena kurangnya pemahaman mereka terhadap pentingnya kontrol. Staff keamanan harus secara terus menerus menjaga pemakai data agar menyadari kebutuhan akan keamanan, termasuk kebijakan keamanan dan prosedur.

2.8 Metode yang berkaitan dengan penyerangan

Tujuan utama untuk menerapkan kontrol akses adalah untuk mencegah akses yang tidak berhak ke objek yang sensitif. Tujuan utama penyerang adalah untuk mengakses objek tersebut. Beberapa tipe serangan berkaitan dengan kontrol akses. Paling banyak serangan yang diarahkan ke kontrol akses didesain untuk merintangi atau melewati kontrol dan memperbolehkan akses ke objek yang dilarang. Salah satu cara untuk memutuskan kontrol yang mana yang akan diletakkan adalah dengan memahami sifat dari serangan yang akan dihentikan. Berikut adalah serangan yang umum terhadap kontrol akses.

Brute Force Attack

Brute Force Attack merupakan serangan yang tidak mutakhir tetapi dapat menjadi efektif. Tujuan dari serangan ini adalah mencoba beberapa kombinasi karakter yang memenuhi otentikasi tipe 1. Seringkali disebut menebak *password*, sebuah program mengirim beberapa *login* percobaan, masing-masingnya dengan *password* yang sedikit berbeda. Harapannya adalah program akan menemukan *password* sebelum orang menyadari bahwa serangan sedang berlangsung. Salah satu variasi *brute force attack* adalah *war dialing*, yaitu program yang memanggil nomor telepon dan mendengarkan jawaban dari *modem*. Sewaktu program menemukan *modem*, nomor tersebut disimpan untuk penyerangan kemudian. Serangan ini dinamakan *brute force attack* karena mereka mencoba sejumlah besar kemungkinan untuk menemukan *password* atau nomor akses. Pertahanan terbaik adalah serangan terbaik. Cara yang baik untuk melindungi sistem dari *brute force attack* adalah dengan melakukannya sendiri. Merupakan ide yang baik untuk menjalankan program *password* atau *war dialing* kepada sistem sendiri secara periodik. Sekali tidaklah cukup. Setiap kali pemakai lelah akan *password* atau menemukan bahwa semakin sulit mengakses internet, akan semakin mudah ditemukan *password* yang mudah ditebak. Lakukan *brute force attack* secara periodik untuk menemukan pemakai yang mengambil jalan pintas.

Sebagai tambahan atas serangan sendiri, atur level sistem monitor untuk memberi tahu ketika aktifitas yang tidak umum sedang terjadi. Ide bagus juga untuk mengatur level penguncian ke tingkat yang agresif sehingga *account* terkunci setelah beberapa kegagalan *login*. Hal ini akan merepotkan bagi pemakai yang melupakan *password*-nya, tetapi hal ini menyediakan pertahanan yang baik terhadap *brute force attack*.

Dictionary Attack

Dictionary attack sebenarnya merupakan turunan dari *brute force attack*. Sebagai ganti dari mencoba semua kombinasi *password*, *dictionary attack* mencoba untuk memenuhi permintaan *password* dengan memberikan *password* umum dari sebuah daftar atau kamus. Banyak daftar dari *password* yang umum digunakan mudah untuk dicari. Meskipun mereka membuat sumber yang bagus untuk *dictionary attack*, mereka juga menyediakan contoh *password* yang dihindari. Pada kenyataannya, salah satu cara terbaik untuk mencegah *dictionary attack* adalah dengan kebijakan *password* yang ketat. Kebijakan *password* memberitahu pemakai bagaimana membuat *password* dan jenis-jenis *password* yang harus dihindari. Jalankan *dictionary attack* secara periodik. Serangan ini tidak segenyar *brute force attack* dan memberikan gambaran siapa yang mematuhi kebijakan *password*. Hindari pemberitahuan *password* dengan tidak pernah mengirimkan *password* sebagai teks. Hindari menggunakan HTTP atau Telnet. Gunakan HTTPS.

Spoofing Attack

Tipe lain dari serangan kontrol akses adalah *login spoofing*. Seorang penyerang meletakkan program *login* palsu yang meminta kepada pemakai, *user ID* dan *password*. Tampilannya seperti *login* normal, sehingga pemakai memberikan informasi yang diminta. Alih-alih memasukkan pemakai ke dalam sistem, program tersebut menyimpan informasi dan menampilkan pemberitahuan bahwa *login* gagal.

Pertahanan terbaik melawan serangan jenis ini adalah membangun jalur yang terpercaya antara pemakai dan *server* ketika memungkinkan. Lakukan percobaan untuk meminimalkan peluang bagi penyerang untuk masuk antara pemakai dan *server*. Didalam lingkungan dimana keamanan menjadi sangat penting, pemakai harus dengan hati-hati mempelajari semua percobaan *login* yang gagal dan memastikan kegagalan tersimpan dan dilaporkan.

Trojan horse

Trojan horse adalah cara yang sering digunakan penyusuf untuk menjebak user agar menginstall program yang membuka pintu belakang di sistem yang digunakan, sehingga penyusup tersebut dapat dengan mudah mengakses komputer milik user tanpa sepengetahuan pemiliknya. Kemudian, penyusup tersebut bisa melakukan perubahan konfigurasi sistem atau menularkan virus ke komputer tersebut.

Back door dan remote administration program

Di komputer yang menggunakan *operating system*, pada umumnya penyusup menggunakan tiga tool, back Orificem Netbus, dan SubSeven untuk mendapatkan akses ke komputer secara remote. Setelah diinstall, back door atau remote administration program ini memungkinkan orang lain untuk mengakses dan mengendalikan komputer tersebut. Platform komputer lainnya mungkin juga memiliki kelemahan terhadap model

serangan seperti ini, sehingga user harus selalu memantau laporan-laporan mengenai vulnerability dari sistem yang digunakan.

Denial-of-service

Ini adalah tipe serangan yang menyebabkan komputer crash atau menjadi sangat sibuk memproses data, sehingga user tidak mempergunakannya. Umumnya, serangan seperti ini bisa diatasi dengan menginstall patch terakhir dari sistem yang digunakan.

Windows networking share yang tidak terlindungi

Penyusup dapat mengeksploitasi Windows networking share yang tidak terlindungi, menggunakan cara-cara yang terotomatisasi untuk meletakkan tool di sejumlah besar komputer berbasis windows yang terhubung ke internet. Komputer yang sudah disusupi ini tidak hanya menyebabkan masalah bagi pemilik komputer tersebut, akan tetapi menjadi ancaman bagi komputer lainnya di internet.

Packet Snifing

Packet sniffer adalah program yang menangkap informasi dari paket data yang lalu lalang di jaringan. Informasi yang bisa didapatkan contohnya adalah identitas user, password, dan informasi lainnya yang bersifat rahasia dalam bentuk cleartext. Dengan ratusan sampai ribuan password yang ditangkap menggunakan paket sniffer, penyusup bisa saja melakukan penyerangan besar-besaran terhadap suatu sistem. Berbeda dengan tipe koneksi DSL dan dial-up tradisional, koneksi yang menggunakan kabel modem memiliki resiko yang lebih tinggi terhadap paket sniffer, karena satu kelompok koneksi kabel modem manapun akan dapat menangkap paket data yang dikirimkan ke kabel modem lainnya dalam kelompok yang sama.

Pencurian identitas

Informasi yang disimpan dalam sebuah home computer bisa menjadi sumber informasi pribadi yang mencukupi bagi para hacker untuk mendaftarkan kartu kredit atau identitas lainnya, dengan mengatasnamakan korban tersebut.

Tunelling

Saat karyawan bekerja di rumah dan mengirimkan file ke sebuah komputer di kantor, ada potensi bahwa seseorang dapat mengakses home computer tersebut dan menyusupkan file rahasia didalam sebuah dokumen yang nantinya disimpan di dalam sistem milik perusahaan.

Zombie

Ini adalah program yang mencari sistem yang terhubung ke internet, tetapi tidak terlindungi dengan baik, kemudian mengambil alih tanpa sepengetahuan user dan menggunakannya untuk tujuan jahat.

Spyware

Program yang terlihat “baik-baik”(contohnya program P2P agent yang digunakan untuk saling bertukar file secara peer-to-peer) bisa saja menyembunyikan program yang mengumpulkan informasi mengenai sistem dan kegiatan user, kemudian mengirimka informasi tersebut ke pihak ketiga tanpa diketahui oleh user dari komputer tersebut.

Virus yang disebarkan melalui email

Virus dan tipe program jahat lainnya seringkali disebarkan sebagai attachment di dalam pesan email. Sebelum membuka attachment apa pun, user harus mengetahui sumber dari attachment tersebut . Tidak cukup dengan sekedar mengetahui bahwa email berasal dari alamat yang sudah kita kenal. Sebagai contoh, virus Melissa menyebar dengan mudah karena pesan email yang menyebarkannya terkesan berasal dari alamat yang dikenal korban.

2.9. Ringkasan

- Kontrol akses mendukung kerahasiaan data dan integritas data.
- Filosofi *privilege* yang terendah menyatakan bahwa subjek harus diberikan hanya izin yang diperlukan untuk menyelesaikan tugas yang dibutuhkan dan tidak lebih.
- Kontrol adalah perintang potensial yang diletakkan ditempat yang melindungi informasi.
- Kontrol akses yang wajib, juga disebut kontrol akses berdasarkan aturan, menggunakan label keamanan untuk memberikan atau menolak permintaan akses.
- Organisasi komersial dan militer mempunyai persamaan tetapi klasifikasi data yang jelas.
- *Discretionary* kontrol akses, disebut juga kontrol akses berdasarkan identitas, menggunakan identitas subjek untuk memberikan atau menolak permintaan akses.
- *Nondiscretionary* kontrol akses, disebut juga kontrol akses berdasarkan pada peran atau tugas, menggunakan peran atau tugas pemakai untuk memberikan atau menolak permintaan akses.
- Kontrol akses dapat disentralisasi, seperti RADIUS, CHAP dan TACACS atau desentralisasi.
- Semua pemakai dari sistem informasi yang aman, akan dimonitor untuk memastikan bahwa mereka dapat diandalkan untuk semua aksinya.
- Beberapa model kontrol akses teoritis membantu untuk memvisualisasikan objek akses.
- Model Bell-LaPadula adalah model *state machine* yang mendukung kerahasiaan data.
- Model Biba juga model *state machine* yang mendukung integritas data.
- Model Clark-Wilson mendukung integritas data dengan membatasi prosedur yang dapat merubah data.

-
- Model non interfensi memastikan bahwa perubahan pada suatu level keamanan tidak mempunyai dampak ke data di level yang lain.
 - Otentikasi adalah proses untuk memvalidasi bahwa subjek adalah benar adanya.
 - Otentikasi tipe 1 adalah sesuatu yang diketahui, otentikasi tipe 2 adalah sesuatu yang dimiliki dan otentikasi tipe 3 adalah diri sendiri.
 - Pemilik data, pemelihara dan pemakai masing-masing memiliki tanggung jawab untuk merawat keamanan data.

2.10. Daftar Istilah

Access Control List (ACL): 1. Daftar yang digunakan untuk memberikan subjek akses ke sekelompok objek atau memberikan kelompok subjek akses ke objek tertentu. 2. Daftar sumber daya dan pemakai dan kelompok yang diperbolehkan untuk mengaksesnya.

Authentication: subjek memberikan verifikasi bahwa dia adalah benar.

Authentication service (AS): sebuah proses dalam Kerberos KDC yang melakukan otentikasi terhadap subjek dan permintaannya.

Authorization creep: sebuah kondisi dimana subjek mendapatkan akses ke lebih banyak objek diluar keadaan semula.

Bell-LaPadula model: sebuah model kontrol akses dikembangkan di tahun 1970an untuk membantu pemahaman yang lebih baik dan implementasi kontrol kerahasiaan data.

Biba model: sebuah model kontrol akses yang dikembangkan setelah model Bell-LaPadula untuk menyelesaikan masalah integritas data.

Biometrics: pendeteksian dan pengelompokan atribut fisik.

Brute force attack: sebuah serangan kontrol akses yang mencoba semua kemungkinan kombinasi *password*.

Centralized access control administration: semua permintaan akses melalui sebuah otoritas pusat yang memberikan atau menolak permintaan.

Challenge Handshake Authentication Protocol (CHAP): sebuah sistem kontrol akses terpusat yang menyediakan kontrol akses untuk pemakai *dial-in*.

Clark-Wilson model: sebuah model akses kontrol yang mengacu pada integritas data dengan melarang semua akses ke sejumlah program akses yang dikontrol secara ketat.

Clipping levels: ambang untuk aktifitas yang memicu suatu aktifitas ketika dilampaui.

Constrained data item (CDI): semua data yang diproteksi menggunakan model Clark-Wilson.

Control: rintangan potensial yang melindungi informasi dari akses yang tidak berhak.

Crossover error rate (CER): titik dimana $FRR = FAR$.

Data custodian: umumnya, orang TI yang ditugaskan oleh pemilik data untuk melaksanakan kebijakan keamanan sesuai pengelompokan data yang diatur oleh pemilik.

Data owner: anggota manajemen yang menerima tanggung jawab untuk melindungi data.

Data user: pemakai sistem yang mengakses data untuk keperluan sehari-hari.

Decentralized access control: meletakkan tanggung jawab kontrol diakses di dekat objek.

Dictionary attack: sebuah serangan kontrol akses yang mencoba *password* dari kumpulan *password* yang umum digunakan.

Discretionary access control: keputusan akses objek yang berdasarkan pada identitas dari subjek yang meminta akses.

False acceptance rate (FAR): suatu tingkat dimana subjek yang tidak valid diterima.

False rejection rate (FRR): suatu tingkat dimana subjek yang valid ditolak.

Identification: 1. Fase dimana subjek diharuskan menjadi identitas yang spesifik. 2. Proses verifikasi identitas subjek.

Identity-bases access control: keputusan akses objek yang berdasarkan pada *user ID* atau sekelompok user.

Integrity verification procedure (IVP): sebuah prosedur yang memverifikasi integritas data.

Kerberos: sistem SSO yang populer yang menyediakan otentikasi dan perlindungan pesan.

Key Distribution Center (KDC): layanan jaringan dan penyimpanan data yang menyimpan semua kunci kriptografi untuk subjek dan objek didalam sistem Kerberos.

Lattice-based access control: variasi dari model kontrol akses *nondiscretionary* yang membentuk setiap keterkaitan antara subjek dan objek dengan batasan akses.

Least privilege: sebuah filosofi dimana subjek hanya diberikan izin yang dibutuhkan untuk menyelesaikan suatu tugas dan tidak lebih.

Login spoofing: serangan kontrol akses yang menggantikan layar login asli dengan layar login dari penyerang

Mandatory access control: mekanisme kontrol akses yang memberikan label keamanan ke setiap subjek dan objek.

Need to know: kondisi dimana subjek memerlukan akses ke suatu objek untuk menyelesaikan tugas.

Nondiscretionary access control: menggunakan peran subjek atau tugas yang diberikan kepada subjek untuk memberikan atau menolak akses ke objek.

Noninterference model: model kontrol akses yang memastikan bahwa perubahan di suatu level keamanan tidak mempengaruhi level keamanan yang lain.

Object: sumber daya dimana subjek mencoba mengakses.

Remote Authentication Dial-In User Service (RADIUS): sistem kontrol akses yang terpusat yang menyediakan kontrol akses bagi pemakai *dial-in*.

Role-based access control: metode kontrol akses *nondiscretionary* yang menggunakan peran subjek untuk memberikan atau menolak akses ke objek.

Rule-based access control: semua hak akses diputuskan dengan mengacu hak akses dari subjek dan label keamanan dari objek.

Security domain: kumpulan subjek dan objek dengan aturan akses atau izin.

Security label: tingkat sensitifitas yang diberikan.

Single sign-on (SSO): sistem yang menghindari *login* secara berulang kali dengan mengidentifikasi subjek dan memperbolehkan informasi otentik untuk digunakan dalam sistem yang dipercaya atau kelompok sistem.

Subject: entitas yang melakukan permintaan akses ke sumber daya.

Task-based access control: metode kontrol akses *nondiscretionary* yang menggunakan tugas subjek yang memberikan atau menolak akses ke objek.

Terminal access controller access control system (TACACS): sistem kontrol akses terpusat yang menyediakan kontrol akses bagi pemakai jaringan.

Ticket: pesan otentikasi Kerberos yang mengandung kunci bagi subjek dan objek.

Transformation procedure (TP): prosedur yang membuat otorisasi perubahan pada data.

Two-factor authentication: proses yang menyediakan dua buah informasi untuk diotentikasi.

Unconstrained data item (UDI): semua data yang tidak dilindungi oleh model Clark-Wilson.

War dialing: otomatisasi menghubungi beberapa nomor telepon untuk mencari *modem*.

Daftar Acuan

Ronald L. Krutz & Russel Dean Vines ,2004, The CISSP Prep. Guide, Wiley Publishing, Canada.

Chapple, Access Control Methodologies.

***Clint Covington , “Creating Secure Data Access Pages” Microsoft Corporation,1999.
<http://www.msdn.microsoft.com/>***

SDA Asia Magazines, Vol. 9, 2005.