Tugas Mata Kuliah
Proteksi dan Keamanan Sistem Informasi (IKI-838408T)

Security Architecture and Models

Disusun Oleh:
Firdaus - 7204000462

Dosen:
Rahmat M. Samik-Ibrahim
Johny Moningka
Arrianto Mukti Wibowo

Magister Teknologi Informasi
Universitas Indonesia

Kelompok 125pagi

Firdaus – 7204000462

Security Architecture and Models

Daftar Isi

Daftar Gambar

1. Pendahuluan

Dua konsep yang perlu diketahui dalam keamanan sistem informasi adalah security model dan security policy. Security policy menegaskan beberapa tingkat point: bagaimana sebuah data diakses, sejumlah keamanan yang diperlukan, dan langkah-langkah apa saja yang harus dilakukan ketika kebutuhan ini tidak ditemukan. Security model mendukung security policy secara lebih mendalam. Jika security policy menegaskan " seluruh public web server harus ditempatkan kedalam DMZ", maka security model harus menspesifikkan "TCP port 80 dan 443 harus hanya boleh dilewati melalui firewall.

Didalam tulisan ini, penulis berusaha menjelaskan konsep-konsep Security Architecture and Models dengan penerapannya pada usaha kecil dan menengah. Adapaun langkah-langkah penjelasannya mengikuti kerangka buku "The CISSP® Prep Guide: Gold Edition" yang ditulis oleh Krutz, R.L dan Russel D. Vines. Topik-topik yang akan dibahas pada tulisan ini adalah:

Arsitektur Keamanan, pada bagian ini akan dijelaskan mengenai mekanisme keamanan pada sebuah sistem informasi. Untuk memahami mekanisme keamanan , terlebih dahulu akan dijelaskan sistematika sebuah komputer dalam menjalankan proses, dan mekanisme keamanan pada sebuah komputer. Dibagian ini juga akan dibahas mekanisme keamanan untuk sistem terdistribusi.

Assurance, bagian ini menjelaskan mengenai petunjuk utama dan standarisasi yang telah dikembangkan untuk mengevaluasi dan menerima aspek asuransi pada sebuah sistem. Bagian ini juga akan membahas kriteria evaluasi yang digunakan untuk menjadi mendukung petunjuk dasar dalam mengevaluasi produk vendor pada kriteria keamanan tertentu. Sedangkan metode resmi harus tersedia untuk meyakinkan bahwa pengamanan sistem informasi yang layak ditempatkan secara benar dan berjalan sesuai fungsinya masing-masing, untuk itu diperlukan akreditasi dan sertifikasi. CMM juga akan dibahas sebagai meningkatkan kualitas sebuah proses yang digunakan sebuah organisasi, maka kualitas produk dan pelayanan yang dihasilkan akan dapat dijamin.

Information Security Models, bagian ini akan menjelaskan teknik teknik keamanan sebuah informasi pada sebuah sistem. Model-model ini untuk memformalkan kebijakan-kebijakan yang telah dibuat. Model keamanan informasi ini dibagi dalam tiga kelompok menurut fungsinya, Access Control Models, Integrity Models, dan Information Flow Models.

Untuk memperdalam pemahaman tentang Security Architecture and Models, tulisan akan membahas penerapan teori yang sudah dijelaskan dengan ilustrasi penerapannya pada usaha kecil dan menengah.

2. Arsitektur Keamanan

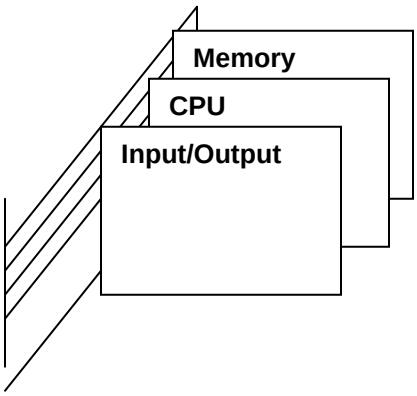
Arsitektur keamanan pada Sistem Informasi adalah hal yang sangat mendasar untuk menyelengarakan kebijakan keamanan Sistem Informasi suatu Organisasi. Oleh karena itu, hal ini sangat penting bagi para profesional keamanan untuk mengerti pokok-pokok arsitektur komputer, mekanisme proteksi, masalah distributed environment security, dan model-model formal yang menyediakan framework untuk kebijakan keamanan. Sebagai tambahan, para profesional harus mempunyai pengetahuan mengenai assurance evaluation, sertifikasi, dan petunjuk akreditasi dan standar. Pada bahasan ini akan dimuat topik mengenai:

- Organisasi komputer
- Komponen perangkat keras
- Komponen perangkat lunak / firmware
- Open systems
- Sistem terdistribusi
- Mekanisme proteksi
- Kriteria evaluasi
- Sertifikasi dan akreditasi
- Model Formal security
- Model Confidentiality
- Model infromation flow

2.1. Arsitektur Komputer

Istilah arsitektur komputer merujuk kepada organisasi dari elemen-elemen yang fundamental yang terkandung dalam komputer. Dari perspektif yang berbeda, arsitektur komputer merujuk pada pandangan bahwa seorang programer mempunyai sebuah sistem komputasi ketika dipandang melalui set instruksinya. Komponen perangkat keras utama dari sebuah komputer digital adalah Central Processing Unit (CPU), memory, dan perangkat input/output. Central Processing Unit dasar dari sebuah komputer digital yang ditijukan untuk keperluan umum terdiri dari Arithmetic Logic Unit (ALU), coontrol logic, satu atau lebih accumulator, multiple general-purpose registers, sebuah instruction register, sebuah program counter, dan beberapa on-chip local memory. Arithmetic Logic Unit melakukan operasi aritmatika dan operasi logikal dengan kalimat binnary sebuah komputer.

Sekumpulan konduktor yang disebut bus menghubungkan elemen-elemen komputer tersebut. Bus berjalan bersamaan dengan elemen-elemen komputer yang berbeda terhubung ke bus. Sebuah bus bisa di kelompokan ke dalam subunit, seperti address bus, data bus, dan control bus. diagram organisasi sebuah bus terlihat seperti gambar dibawah.



Gambar 1.1. Bus Pada Komputer

2.1.1. Memori

Beberapa tipe memori digunakan adalam sistem komputer digital. Berikut Prinsip dari tipe-tipe memori dan definisinya;

Cache memory. Adalah sebuah RAM kecepatan tinggi yang mempunyai ukuran memori yang relatif kecil (ketika dibandingkan dengan memori utama). Jenis memori ini memuat instruksi-instruksi dan data dari memori utama yang mempunyai kemungkinan diakses paling tinggi selama porsi eksekusi yang sedang berjalan dari sebuah program. Cache logic berusaha memprediksi instruksi dan data mana di dalam memori utama akan digunakan oleh program yang sedang berjalan. Lalu cache logic memindahkan instruksi dan data tersebut kedalam cache yang mempunyai kecepatan lebih tinggi untuk mengantisipasi kebutuhan CPU akan program dan data ini. Mendesain cache dengan benar dapat mengurangi acces time memori utama secara signifikan dan hal ini akan meningkatkan kecepatan eksekusi sebuah program.

Random Access Memory (RAM). Adalah memori yang lokasinya bisa secara langsung dialamatkan dan data yang disimpannya bisa di ubah. RAM bersifat volatile, data yang tersimpan akan hilang jika tegangannya dhilangkan. Dynamic RAM (DRAM) menyimpan infromasi pada parasitic capacitance yang hilang setelah masanya habis. Selain itu, data pada setiap bit RAM secara periodik harus di refresh. Proses refresh dilakukan dengan membaca dan menuliskan kembali setiap bit setiap beberapa milidetik. Sebaliknya, static RAM (SRAM) menggunkan penahan untuk menyimpan bit dan tidak memerlukan refresh. Tapi bagaimanapun kedua tipe RAM ini bersifat volatile.

RDRAM Memory (Rambus DRAM). Berbasis pada teknologi Rambus Signaling Level (RSL) yang diperkenalkan pada tahun 1992, perangkat RSL RDRAM menyediakan sistem dengan kpasitas memori 16MB sampai 2GB pada kecepatan sampani dengan 1066MHz. Kabal RDRAM

mencapai kecepatan tinggi dengan menggunkan kontrol dan alamat bus yang terpisah, protokol yang sangat efisien, pensinyalan yang rendah voltase, dan clocking yang akurat untuk meminimilkan ketidaksimetrisan antara clock dan garis data. Pada saat ini teknologi RSL mendekati kecepatan 1200MHz.

Programmable Logic Device (PLD). Adalah sirkuit yang terintegrasi dengan sebuah sambungan atau gerbang logic internal yang bisa diubah melalui proses pemrograman. Contoh dari sebuah PLD adalah Read Only Memory (ROM), sebuah perangkat Programbale Array Logic (PAL), Complex Programmable Logic Device (CPLD), dan Field Programmable Gate Array (FPGA). Pemrograman perangkat ini dilakukan dengan menggelembungkan koneksi fuse pada chip, menggunkan antifuse yang membuat sebuah koneksi ketika voltase tinggi diberikan pada sambungan, melalui mask programing ketika sebuah chip di buat, dan dengan menggunkan penghalang SRAM untuk mengubah sebuah transistor Metal Oxide Semiconductor (MOS) menjadi on atau off. teknologi baru dari perangkat ini adalah volatil.

Read Only Memory (ROM). Media penyimpanan yang tidak volatile dimana lokasinya bisa ditemukan secara lansung. Pada implementasi ROM standar, data tidk bisa diubah secara dinamis. Media penyimpanan non volatile menyimpan informasinya walaupun dia kehilangan power. Beberapa ROM di implementasikan dengan link fusible satu arah, dan isinya tidak bisa diubah. Tipe lain dari ROM (seperti ROM yang bisa dihapus, Programmable Read-Only Memories (EPROMs), Electrically Alterable Read Only Memories (EAROMs), Electrically Erasable Programmable Read Only Memories (EEPROMs), Flash memories, dan turunannya) bisa diubah dengan cara yang berbeda-beda, tapi hanya pada kecepatan yang relatif rendah jika dibandingkan dengan perangkat alat dan tulis pada sistem komputer yang normal. ROM digunakan untuk menjaga program dan data yang seharusnya tidak bisa diubah atau tidak terlalu sering diubah. Program disimpan kedalam perangkat ini yang direfer sebagai firmware.

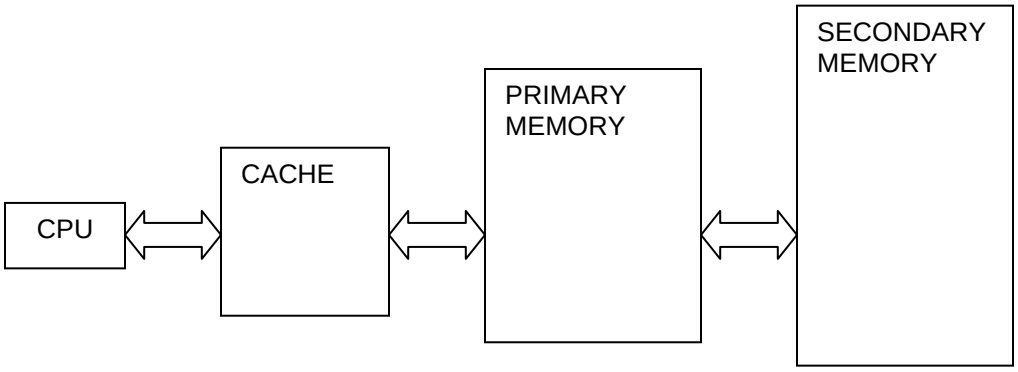
Real or primary memory. Memori yang secara langsung bisa dialamatkan oleh CPU dan digunkan untuk menyimpan instruksi dan data yang berhubungan dengan program yang sedang berjalan. Jenis memori ini biasanya adalah Random Access Memory (RAM) yang mempunyai kecepatan tinggi.

Secondary memory. Tipe memori ini adalah tipe memori yang lebih lambat (seperti magnetic disk) yang menyediakan penyimpanan yang tidak volatile.

Sequential memory. Memori dimana informasinya harus didapat dengan pencarian secara berurut (sequensial) dari awal tidak secara langsung mengakses ke lokasinya. Sebuah contoh dari sequential memory acces adalah membaca informasi dari sebuah tape magnetic.

Virtual memory. Tipe memori ini digunkan sebagai memori sekunder dalam sambungan dengan memori utama untuk menampilkan CPU dengan ruang pengalamatan yang jelas dari lokasi real memory.

Hirarki khas memori terlihat pada gambar



Gambar 1.2. Hirarki Memori Pada Komputer

Ada beberapa cara sebuah CPU mengalamatkan memori. Pilihan ini meyediakan fleksibilitas dan efisiensi ketika memprogram tipe-tipe berbeda dari aplikasi, seperti mencari melalui sebuah tabel atau memproses serangkaian data. Berikut adalah beberapa mode-mode pengalamatan yang biasa digunakan.

Register addressing. Pengalamatan register dalam sebuah CPU atau register dengan tujuan yang lain yang didesain pada memori primer.

Direct addressing. Pengalamatan sejumlah memori primer dengan menspesifikasikan alamat aktual dari lokasi memori. Alamat momori biasanya dibatasi oleh page memori yang sedang dieksekusi atau page zero.

Absolute addressing. Mengembangkan sebuah alamat memori dengan menambahkan isi dari alamat yang ditentukan didalam instruksi program kepada register indeks. Alamat yang efektif dan terkomputasi digunakan untuk mengakses likasi memori yang diinginkan. Jadi, jika sebuah register indeks bertambah atau berkurang, sejumlah lokasi memori bisa dikases.

Implied addressing. Digunakan jika operasi yang ada pada prosesor harus dilakukan, seperti membersihan sebuah bit yang dibawa yang diatur sebagai hasil dari operasi aritmatika. Karena operasi sedang dilakukan pada sebuah register internalyang dispesifikasikan dengan instruksi itu sendiri, meyediakan sebuah alamat tidak diperlukan.

Indirect addressing. Pengalamatan dimana lokasi alamat yang dispesifikasikan pada instruksi memuat alamat lokasi yang diinginkan yang sudah final.

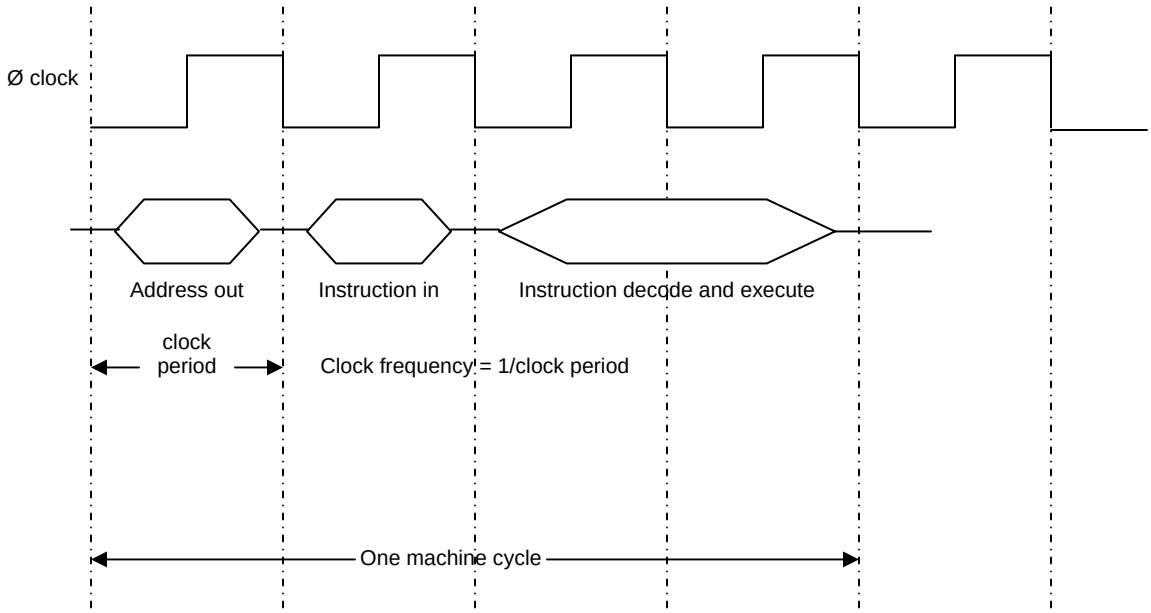
Sebuah definisi yanng berhubungan adalah definisi proteksi memori.

Memory protection. Mencegah sebuah program mengkases dan memodifikasi isi ruang memori yang dimiliki oleh program lain.
Proteksi memori dilakukan oleh sistem operasi atau oleh mekanisme perangkat keras.

2.1.2. Instruction Execution Cycle

Sebuah machine cycle standar terdiri dari dua fase: fetch dan execute. Pada fase fetch, CPU menampilkan alamat dari instruksi ke memori, dan dia menerima instruksi yang dilhasikan pada alamat tersebut. Lalu, selama fase eksekusi, instruksi didecode dan dieksekusi. Siklus ini dikontrol dan disinkronkan dengan sinyal clock CPU. Karena kebutuhan untuk me-refresh RAM dinamik, multiple clock signal yang dikenal sebagai multi-phase clock signal diperlukan . Static RAM tidak memerlukan refreshing dan menggunakan sinyal clock fase tunggal. Sebagai tambahan, beberapa instruksi memerlukan lebih dari satu siklus mesin untuk eksekusi, tergantung pada kompleksitasnya. Siklus mesin yang umum menunjukan clock fase tunggal bisa dilihat pada gambar 4. Pada contoh ini, empat perioda clock dibutuhkan untuk mengeksekusi sebuah instruksi tunggal.

Sebuah komputer bisa didalam sejumlah statemen yang berbeda selama operasinya. Ketika sebuah komputer mengeksekusi instruksi, situasi ini kadang-kadang disebut “run” atau “operating state”. Ketika program aplikasi sedang dieksekusi, mesin berada didalam statemen “application” atau “problem”, karena ini diharapkan menghitung solusi menjadi sebuah masalah. Untuk tujuan keamanan, pengguna hanya diizinkan untuk mengakses sebagian dari total set instruksi yang tersedia pada komputer pada statemen ini. Bagian ini dikenal sebagai instruksi “non-privileged”. Instruksi privileged dikesekusi oleh administrator sistem atau oleh individu yang telah diberikan izin untuk menggunkan instruksi-instruksi tersebut. Sebuah komputer dalam sebuah peernyataan s”supervisory” ketika dia mengeksekusi instruksi-instruksi privileged ini. Komputer bisa ada didalam statemen “wait”, sebagai contoh, jika komputer mengakses memori yang relatif lambat terhadap waktu siklus iinstruksi, dimana bisa mengakibatkan dia akan memperpanjang siklusnya.



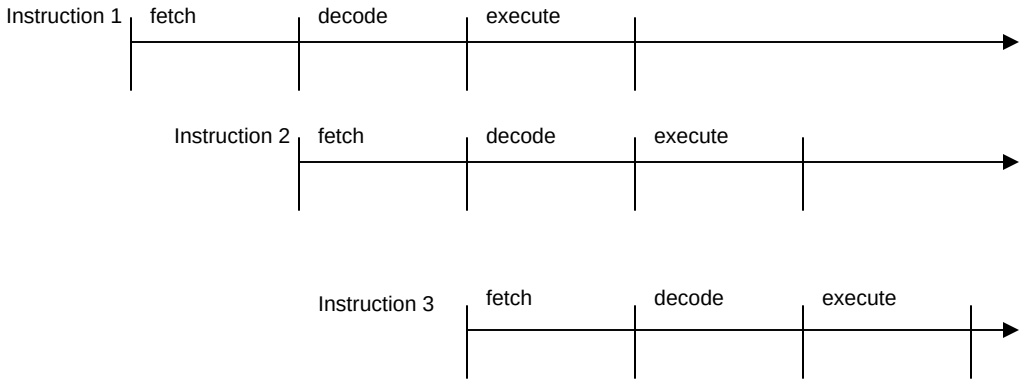
Gambar 1.3. A Typical Machine Cycle

Setelah memeriksa siklus mesin dasar, hal ini sangat nyata bahwa ada peluang untuk menambah kecepatan mendapatkan kembali dan mengeksekusi instruksi. Beberapa metode ini mencakup meng-overlap fetch dan mengeksekusi siklus, mengeksploitasi peluang untuk parallelism., mengantisipasi instruksi yang akan dieksekusi kemudian, fetching dan decoding instruksi lebih jauh, dan lain-lain. Desain komputer yang modern menggabungkan metode ini dan pendekatan kuncinya adalah menyediakan hal-hal berikut:

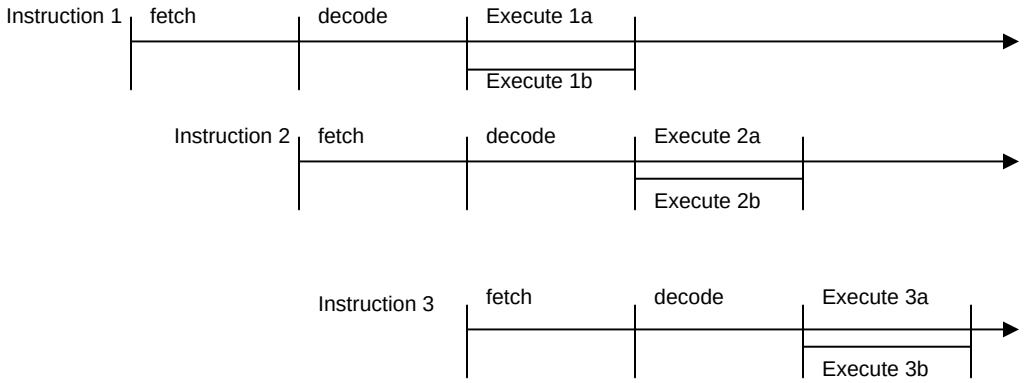
Pipelining. Meningkatkan kinerja komputer dengan meng-overlap langkah-langkah instruksi yang berbeda. Sebagai contoh, jika siklus instruksi dibagi menjadi tiga bagian kinstruksi –fetch, decode, dan eksekusi- bisa di-overlap (seperti terlihat pada gambar) untuk meningkatkan kecepatan eksekusi instruksi.

Complex Instruction Set Computer (CISC). Menggunakan instruksi yang melakukan banyak operasi per instruksi. Konsep ini didasarkan pada fakta bahwa pada teknologi sebelumnya, fetch instruksi adalah bagian terlama dari siklus. Oleh karena itu, dengan mengemas instruksi-instruksi dengan beberapa operasi, maka jumlah fetch bisa dikurangi.

Reduced Instruction Set computer (RISC). Menggunakan instruksi yang lebih simpel dan hanya memerlukan siklus clock yang sedikit untuk eksekusi. Pendekatan ini adalah hasil dari peningkatan pada kecepatan memori dan komponen prosesor lainnya, dimana memungkinkan bagian fetch siklus instruksi tidak menjadi lambat lagi dari pada bagian lain siklus. Pada kenyataannya, kehandalan dibatasi oleh waktu decoding dan eksekusi siklus instruksi.



Gambar 1.4. Instruction Pipelining



Gambar 1.5. Proses Very-Long Instruction Word (VLIW)

Scalar Processor. Sebuah prosesor yang mengeksekusi satu instruksi pada satu saat.

Superscalar Processor. Sebuah prosessor yang memungkinkan eksekusi yang bersamaan dari instruksi yang banyak pada tahap pipeline yang sama sebaik tahap pipeline yang lain.

Very-Long instruction Word (VLIW) Processor. Sebuah prosesor yang pada instruksi tungal menetapkan dan secara bersamaan mengeksekusi dua operasi didalam satu instruksi. Proses VLIW bisa terlihat pada gambar 5.

Multi-programing. Mengeksekusi dua atau lebih program secara simultan pada sebuah prosessor tunggal (CPU) dengan bertukar-tukar eksekusi sesama program.

Multi-tasking. Mengeksekusi dua atau lebih subprogram atau task pada saat yang bersamaan pada sebuah prosessor tunggal (CPU) dengan bertukar-tukar eksekusi sesama task.

Multi-processing. Mengeksekusi dua atau lebih program pada saat bersamaan pada banyak prosessor.

2.1.3. Struktur Input/Output

Sebuah prosessor berkomunikasi dengan perangkat diluarnya melalui perangkat interface yang disebut input/output (I/O) interface adapters. Pada kebanyakan kasus, adapter ini adalah perangkat kompleks yang menyediakan data buffering dan timing dan interupt control. Adapter memiliki alamat pada bus komputer dan diseleksi oleh instruksi komputer. Jika adapter diberikan sebuah alamat pada ruang memori, lalu menempati alamat memori tertentu desain ini dikenal dengan memory mapped I/O. Keunggulan dari pendekatan ini adalah bahwa CPU tidak melihat perbedaan dalam insrtruksi untuk adapter I/O dan lokasi memori lainnya. Oleh karena itu, seluruh instruksi yang berhubungan dengan memori bisa digunakan untuk perangkat I/O. Demikian sebaliknya, dalam I/O yang terisolasi sebuah sinyal khusus pada sebuah bus mengindikasikan bahwa operasi I/O sedang dieksekusi. Sinyal ini membedakan sebuah alamat untuk sebuah perangkat I/O dari sebuah alamat ke memori. Sinyal dibangkitkat sebagai hasil eksekusi dari sedikit instruksi I/O yang telah diseleksi pada set instruksi komputer. Keunggulan dari sebuah I/O yang terisolasi adalah alamatnya tidak akan menggunakan alamat manapun yang mungkin dapat digunakan memori. Sedangkan kerugiannya adalah bahwa akses dan manipulasidata I/O terbatas pada sedikit instruksi I/O pada set instruksi prosessor. Memory-mapped dan I/O yang tersisolasi, kedua-duanya diistilahkan dengan programed I/O.

Dalam programed I/O, transfer data adalah sebuah fungsi dari kecepatan eksekusi instruksi yang memanipulasi data yang melewai sebuah CPU. Alternatif tercepat adalah akses memori secara langsung (DMA). Dengan DMA, data ditransfer secara langsung ke dan dari memori tanpa harus melewati sebuah CPU. DMA controller menyelesaikan transfer langsung ini dengan interval waktu antara eksekusi instruksi. Kecepatan transfer data dalam DMA terbatas terutama dibadningkan dengan waktu siklus memori. Jejak transfer data antara memori dan sebuah perangkat kadang-kadang disitilahkan dengan channel.

Alternatif lain untuk memindahkan data ke dalam dan keluar sebuah komputer adalah melalui penggunaan interupsi. Proses interupsi, adalah sinyak eksternal dari alur program normal dan servis yang diminta. Servis ini mungkin memuat membaca data atau merespon situasi darurat. Adapter menyediakan interface untuk menangani interupsi dan cara-cara untuk menetapkan prioritas diantara permintaan interupsi yang banyak. Ketika sebuah CPU menerima permintaan interupsi, ia akan menyimpan statemen informasi yang ada terkait dengan program yang sedang berjalan, dan ia akan melompat ke program yang lain yang melayani interupsi. Ketika layan interupsi selesai, CPU akan mengembalikan statemen dari program sebenarnya dan melanjutkan prosesnya kembali. Interupsi yang banyak bisa ditangani secara bersamaan dengan mengelompokan rutin layanan interupsi. Interupsi bisa di nonaktifkan atau ditutupi jika sebuah CPU mengeksekusi kode yang mempunyai prioritas tinggi dan tidak mungkin ada penundaan pada prosesnya.

2.1.4. Perangkat Lunak

CPU sebuah komputer didesain untuk mendukung eksekusi sebuah set instruksi yang berasosiasi dengan komputer tersebut. Set ini terdiri dari berbagai macam instruksi seperti ADD WITH CARRY, ROTATE BITS LEFT, MOVE DATA, dan JUMP TO LOCATION X. Setiap instruksi direpresentasikan sebagai kode biner dimana decoder instruksi dari CPU didesain untuk mengenali dan mengeksekusinya. Instruksi ini didefiniskian sebagai instruksi bahasa mesin. Kode stiap instruksi bahasa mesin berasosiasi dengan sebuah bahasa inggris yang mudah diingat untuk memudahkan orang-orang berkerja dengan kode-kode tersebut. Set instruksi dasar komputer yang mudah diingat ini disebut sebagai bahasa perakitan (assembly language) dimana bahasa ini spesifik terhadap komputer-komputer tertentu. Jadi, ada sebuah korespodensi satu-satu untuk setiap instruksi bahasa perakitan pada setiap isntruksi bahasa mesin. Sebagai contoh, pada sebuah kata instruksi 8 bit yang sederhana komputer, kode biner untuk instruksi bahasa mesin ADD WITH CARRY akan menjadi 10011101, dan korespodensi yang mudah diingat adalah ADC. Seorang programer yang menulis kode ini pada level bahasa mesin akan menulis kodenya menggunakan kata yang mudah diingat untuk setiaqp instruksinya. Lalu kode tersebut akan melewati program lain yang disebut assembler yang akan menjalankan transalsi satu ke satu kode bahasa perakitan ke kode bahasa mesin. Kode yang dihasilkan oleh assembler yang berjalan pada komputer disebut sorce code. Perangkat lunak assembler bisa berada pada komputer yang sedang diprogram dan ini disebut rsident assmebler. Jika assembler sedang berjalan pada komputer lain, assembler ini disebut cross assembler. Cross assembler bisa berjalan pada berbagai tipe dan model komputer. Sebuah disassembler berkebalikan fungsi dengan sebuah assembler dengan menterjemahkan bahasa mesin menjadi bahasa perekitan.

Jika sebuah kelompok statemen-statemen bahasa rakitan digunakan untuk melaksanakan satu fungsi spesifik, mereka dapat didefinisikan dengan assembler dengan sebuah nama yang disebut MAKRO. Kemudian, sebagai ganti menulis daftar statemen-statemen, MAKRO dapat dipanggil, menyebabkan assembler menyisipkan statemen-statemen yang sesuai.

Oleh karena keinginan untuk menulis perangkat lunak pada level yang lebih tinggi, statemen english-like, bahasa level tinggi digunakan. Pada bahasa ini, satu statemen biasanya memerlukan sejumlah instruksi bahasa mesin untuk implementasinya. Oleh karena itu, tidak seperti bahasa rakitan, ada hubungan satu ke banyak dari instruksi bahasa level tinggi ke instruksi bahasa mesin. Pascal, FORTRAN, BASIC, dan Java adalah contoh bahasa level tinggi. Bahasa level tinggi diterjemahkan ke instruksi bahasa mesin yang bersesuaian melalui baik sebuah program intepreter atau compiler. Sebuah interpreter beroperasi pada setiap statemen sumber bahasa level tinggi secara tersendiri dan menjalankan operasi yang sudah diindikasikan dengan cara mengeksekusi urutan instruksi bahsa mesin yang telah ditentukan. Oleh karena itu, instruksi-instruksi ini dieksekusi sesegera mungkin. Java dan BASIC adalah contoh dari bahasa interpreter. Secara kontras, sebuah compiler menterjemahkan seluruh program program perangkat lunak ke dalam perintah bahasa mesin yang bersesuaian. Instruksi ini lalu di muat kedalam memori komputer dan lalu dieksekusi sebagai sebuah paket program. FORTRAN adalah sebuah contoh dari sebuah bahasa compiler. Dari sudut pandang keamanan, sebuah program compiler tidak terlalu diinginkan dibandingkan

dengan sebuah interpreter karena kode yang membahayakan bisa menempati suatau tempat pada kode compiler, dan ini susah untuk dideteksi dalam program yang sangat besar.

Bahasa level tinggi dikelompokan dalam 4 kelompok generasi, dan mereka di beri nama sebagai Generation Language (GL). Berikut adalah daftar bahasa-bahasanya:

- 1 GL. Sebuah bahasa mesin komputer
- 2 GL. Sebuah bahasa perakitan
- 3 GL. FORTRAN, BASIC, PL/1, dan Bahasa C
- 4 GL. NATURAK, FOCUS, dan bahasa query database.
- 5 GL. Prolog, LISP, dan bahasa kecerdasan buatan lainnya yang memproses simbol atau menerapkan logika predikat.

Program (atau sekumpulan program) yang mengontrol sumber daya dan operasi komputer disebut sebagai Sistem Operasi (OS). Sistem operasi menjalankan manajemen proses, manajemen memori, manajemen file sistem, dan manajemen I/O. Windows XP, Windows 2000, Linux dan Unix adalah beberapa contoh sistem operasi.

Sistem operasi berkomunikasi dengan sistem I/O melalui sebuah controller. Controller adalah sebuah perangkat yang melayani sebagai interface kepada periferal dan menjalankan perangkat lunak tertentu untuk mengelola pertukaran infrormasi dan operasi dari sebuah disk drive.

Pada penerapannya di usaha kecil dan menengah, pemilihan sistem komputer dan sistem operasi mejadi isu yang ramai diperdebatkan. Dari sekian banyak perdebatan sistem operasi yang ada, Linux menjadi salah satu pilihan usaha kecil dan menengah.

Jika kita sudah menetapkan diri untuk menggunakan sistem komputer dalam membantu bisnis, maka langkah pertamanya adalah menentukan jenis komputer yang akan dipakai. Pemilihan komputer sebetulnya tidak terlalu sulit, karena dengan anggaran sekitar empat juta rupiah, kita sudah bisa mendapatkan server yang cukup tangguh, mampu menjalankan sistem tersebut dengan baik.

Intel Pentium 4 kecepatan 2,4 GHz, memori 256MB, hard disk 40GB sudah merupakan perangkat yang ideal yang bisa dipakai sebagai server. Kalau memang anggarannya terbatas, pilihan lainnya bisa menggunakan prosessor AMD atau Transmeta yang semakin lama semakin populer.

Berikutnya, kita harus menentukan sistem yang akan dipakai, apakah cukup menggunakan satu komputer, beberapa komputer sebagai sistem jaringan komputer, dikenal dengan nama Local Area Network (LAN), atau bahkan harus menerapkan Wide Area Network (WAN) jika letak gedungnya berjauhan satu sama lain.

Komputer yang kita beli tidak akan jalan sendiri tanpa sistem operasi, dan seperti kita ketahui, sistem operasi komputer yang paling banyak dipakai saat ini terdiri dari dua jenis, yaitu Microsoft Windows 2000 Server atau Linux. Kalau usaha kita dapat menyisihkan anggaran yang cukup, maka kita bisa membeli lisensi Microsoft Windows yang harganya bisa sampai ribuan dolar Amerika, sementara jika kita menggunakan Linux, kita tidak perlu membeli lisensi sistem operasinya, karena Linux merupakan sistem operasi yang bisa didapatkan dengan cuma-cuma.

Perdebatan dari kedua sistem ini tidak habis-habisnya, tetapi satu kenyataan bahwa pada akhirnya keduanya akan menuju ke satu titik, yaitu kepuasan pelanggan, dalam hal kemudahan dan kemampuan yang tinggi akan segala fungsinya.

Setelah semua infrastruktur kita sediakan, langkah berikutnya adalah menentukan pemakaian program aplikasi yang diinginkan. Pada saat ini, sudah lebih dari seratus produk program bisnis yang tersedia di pasaran dari yang nyaris diberikan cuma-cuma, sampai yang harga yang mencapai puluhan juta, semuanya tergantung pada kebutuhan kita.

Mahal-murahnya program yang akan dibeli tergantung dari fasilitas yang disediakan oleh pembuat programnya. Misalnya, ada program yang hanya bisa jalan di satu komputer, atau programnya bisa dihubungkan ke sistem bank, sehingga pemeriksaan buku bank menjadi lebih mudah

Ada pula sistem yang dibuat dalam standar internet, sehingga komputer kita bisa berhubungan dengan komputer lain yang berada di benua berbeda.

Dengan adanya jaringan internet, maka kebutuhan server untuk pelaku bisnis skala menengah ke bawah ini juga makin bertambah, yaitu dengan penambahan fungsi e-mail yang merupakan sarana terpenting dalam berkomunikasi dengan berbagai pihak, sudah tentu dengan tambahan fungsi; cepat dan murah.

2.1.5. Open and Closed Systems

Open system adalah sistem yang independen terhadap vendor yang mengeluarkan spesifikasi dan interface untuk memungkinkan operasi dengan produk dari pemasok lain. Salah satu keuntungan dari sebuah open system adalah dia menjadi objek review dan evaluasi oleh pihak ketiga yang independen. Biasanya, bentuk keamanan ini akan menyingkap kesalahan-kesalahan atau kerentanan pada sebuah produk.

Closed system menggunakan perangkat keras (dan / atau perangkat lunak) dari vendor tertentu ang biasanya tidak kompatibel dengan sistem atau komponen lain. Close systemadalah bukan subjek penilaian independen dan mungkin memiliki kerentanan yang tidak tiketahui atau tidak dikenal.

Untuk usaha kecil dan menengah open system menjadi alternatif pilihan yang paling diminati. Masalah kesalahan-kesalahan dan kerentanan pada sistem terbuka bisa diketahui, hal ini menjadi nilai lebih bagi usaha kecil dan menengah karena keterbatasan sumber daya dan biaya yang mereka hadapi. Usaha kecil dan menengah tidak harus memlihara sistem yang mereka miliki sendiri. Mereka bisa mendapatkan informasi mengenai kerentanan dari system mereka dan mereka memperbaiki system tersebut dengan mudah tanpa biaya yang berlebih. Dengan semakin berkembangnya komunitas open system, maka dukungan terhadap system yang murah dan handal menjadi kenyataan bagi usaha kecil dan menengah.

2.2. Distributed Architecture

Migrasi komputasi dari model komputasi yang terpusat ke model client-server telah membentuk serangkaian masalah baru bagi profesional keamanan sistem informasi. Situasi ini juga telah menyatukan perkembangan PC desktop dan workstation.

Penangan keamanan arsitektur terdistribusi pada usaha kecil dan menengah menjadi perhatian yang cukup penting. Pada usaha kecil dan menengah, biasanya seorang user juga menjadi administrator sistem, programer dan operator sebuah desktop. hal ini menimbulkan kerentanan terhadap keamanan system, terutama data yang ada didalamnya.

Untuk mencegah kerentanan yang akan terjadi, usaha kecil dan menengah sebaiknya menerapkan mekanisme keamanan sebagai berikut:

- Menerapkan kebijakan penggunaan email dan download.
- Menerapkan kontrol akses, dan penggunaan password untuk mengakses komputer desktop.
- Sosialisasi tentang mekanisme keamanan dan pentingya keamanan sistem pada saat pertemuan.
- Penggunaan thin client mungkin bisa menjadi alternatif keamanan system.

2.3. Protection Mechanisms

Dalam sebuah sistem komputasi, proses yang beraneka ragam dapat berjalan secara bersamaan. Tiap proses memiliki kemampuan untuk mengakses lokasi meomori tertentu dan mengeksekusi bagian instruksi dalam tiap computer. Pelaksanaan dan kapasitas memori ini diperuntukkan pada setiap proses yang dikenal dengan daerah wewenang proteksi. Daerah wewenang/kekuasaan dapat diteruskan pada memori virtual, yang menambah ukuran nyata dari memori sesungguhnya dengan menggunakan kapasitas penyimpan disket. Maksud dari pembentukan daerah proteksi ini adalah untuk melindungi program-program yang ada dari segala bentuk modifikasi yang illegal atau pengaruh-pengarah buruk lainnya.

Para pakar keamanan harus paham bahwa TCB (Trusted Computing Base) merupakan total penggabungan dari mekanisme proteksi melalui sistem komputer yang meliputi perangkat keras, perangkat lunak maupun firmware yang diyakini dapat menekan ketentuan keamanan. Garis keliling keamanan itu merupakan batas yang memisahkan TCB dari peninggalan sisa sistem. Bagian yang legal harus slalu ada sehingga para pengguna system tersebut dapat mengakses TCB tanpa mengkompromikannya dengan proses lain atau pengguna lainnya. Sistem komputer yang benar merupakan satu-satunya yang menggunakan pengaturan penjaminan hardware dan software yang dibutuhkan agar kemampuannya dapat digunakan dalam keanekaragaman proses maupun penyampaian informasi yang sensitif dan teratur.

Sumber dapat dilindungi melalui abstraksi yang mendasar. Abstraksi melibatkan tampilan komponen sistem pada level tinggi dan menolak detail yang spesifik. Pendekatan ini meningkatkan kemampuan sistem untuk memahami sistem yang kompleks dan memfokuskan pada isu-isu dan berbagai kritikan. Dalam orientasi obyek program, sebagai contoh, metode (program) dan data yang dipaparkan dalam obyek sehingga dapat ditampilkan sebagai sebuah abstraksi. Konsep ini dikenal dengan penyamaran

informasi karena detil-detil obyek yang tersembunyi. Komunikasi melalui obyek ini membutuhkan tempat melalui pesan-pesan yang disampaikan pada objek yang ditegaskan melalui metode internal.

2.3.1. Rings

Satu perencanaan yang mendukung daerah wewenang proteksi merupakan kegunaan dari cincin proteksi. Cincin-cincin ini dikelompokkan pada daerah tersembunyi di tengah-tengah cincin dan pada ujung lokasi yang paling besar pada bagian cincin tersebut. Pendekatan ini ditunjukkan pada gambar 5.6.

Operating system security kernel biasanya terletak pada cincin dan memiliki akses pada seluruh daerah sistem. Security kernel disimpulkan sebagai hard ware, software, dan firmware pada dasar komputerisasi yang legal yang mengimplementasikan konsep layar referensi. Layar referensi adalah sebuah komponen sistem yang menekankan kontrol akses ke sebuah objek. Layar referensi merupakan sebuah mesin abstrak yang menjadi perantara seluruh akses pada sasarannya.

Security kernel harus :

- menjadi perantara semua akses
- terlindung dari segala bentuk modifikasi
- telah diverikasi dengan baik dan benar

dalam konsep cincin, wewenang akses berkurang apabila jumlah cincin bertambah. Karena proses legal kebanyakan terletak padar pusat cincin. Komponen sistem ditempatkan pada cincin yang layak sehubungan pada prinsip-prinsip tertentu. Proses hanya memiliki kegunaan minimum yang dibutuhkan untuk menjalankan fungsi-fungsinya.

Mekanisme proteksi cincin diimplementasikan dalam MIT’s MULTICs yang ditingkatkan untuk aplikasi aman melalui Honeywell Corporation. MULTICS awalnya ditargetkan untuk kegunaan media perangkat keras karena beberapa kegunaannya bisa diimplementasikan melalui perangkat keras yang didesain untuk menopang sebanyak 64 cincin, tapi dalam prakteknya, hanya delapan cincin yang bisa ditopang.

Berikut juga merupakan pendekatan-pendekatan kernel yang berkaitan pada proteksi :

- menggunakan perangkat keras yang terpisah yang menerangkan berlakunya masa seluruh refernsi dalam sistem tersebut
- mengimplementasikan layar mesin secara virtual, yang menetapkan jumlah dari mesin virtual yang terpisah dari bagian lainnya dimana sistem komputer dijalankan sesungguhnya. Mesin virtual ini meniru arsitektur dari wujud mesin yang sesungguhnya dalam pembentukan suatu lingkungan pengamanan bertingkat, dimana tiap mesin virtual dapat berjalan pada tingkat pengamanan yang berbeda.
- Menggunakan kernel pengamanan software yang beroperasi pada daerah kekuasaan proteksi perangkat kerasnya.

2.3.2. Security Labels

Label keamanan ditujukan pada suatu sumber untuk menunjukkan sebuah tipe pengelompokan atau perencanaan. Label ini dapat menunjukkan penanganan keamanan khusus, yang dapat digunakan untuk mengakses kontrol. Sekali label diberikan, maka label tersebut biasanya tidak dapat digantikan karena label-label ini merupakan mekanisme kontol akses yang efektif. Label yang ada harus dibandingkan, diuji dan dievaluasi terlebih dahulu melalui aturan pengamanan yang ada, karena dapat mendatangkan dampak buruk setelah proses berlangsung apabila tidak dievaluasi dulu.

2.3.3. Security Modes

Sebuah sistem informasi beroperasi dalam mode keamanan yang berbeda yang ditentukan oleh level klasifikasi sistem informasi dan penjelasan dari semua pengguna sistem. Bagaimanapun juga, tidak semua user memiliki kemampuan untuk mengetahui semua data. Mode bertingkat pada pengguna suport operasi yang memiliki perbedaan media pembersih dan data pada tingkat klasifikasi yang bertingkat.

Mode tambahan pada sistem operasi dapat dijelaskan sebagai berikut :

- dedikasi. Semua pengguna memiliki media pembersih atau semacam wewenang untuk mengetahui segala macam informasi yang diproses oleh sistem informasi; sistem yang bisa menangani level klasifikasi yang beraneka ragam
- compartmented. Semua user memiliki media pembersih untuk level tertinggi pada klasifikasi informasi, tapi mereka tidak memiliki wewenang yang diperlukan untuk mengetahui semua data yang dipegang sistem komputer.
- Terkendali. Merupakan tipe keamanan yang bertingkat dimana jumlah terbatas dari perangkat sistem yang ditempatkan secara legal dalam hubungannya pada tingkat informasi dapat diproses.
- Akses terbatas. Merupakan tipe akses sistem dimana hanya dapat digunakan user tertentu dan klasifikasi data maksimum tidak disusun, tetapi cukup sensitif.

Sebuah sistem informasi pada usaha kecil dan menengah sebaiknya menggunakan mode keamanan *multi-level mode of operation* karena pada usaha kecil dan menengah diperlukan keluesan terhadap informasi yang ada pada organisasi. Informasi harus mengalir dengan aman tanpa proses yang rumit, sesuai dengan sifat usaha kecil dan menengah yang harus cepat dan tangkas. Pada mode keamanan *multi-level mode of operation,* user memiliki level klasifikasi yanng berbeda. Penggunaan mode keamanan *system high mode of operation* pada usaha kecil dan menengah akan membuat komunikasi dan alur informasi pada organisasi menjadi rumit dan tidak tangkas. Karena setiap user terkesan sendiri-sendiri dalam berkerja dan dalam kepemilikan inforrmasi. Tapi penggunaan mode keamanan *multi-level mode of operation* ini bisa menjadi birokrasi yang rumit karena tingkatan-tingkatan yang ada, untuk itu diperlukan klasifikasi level yang pendek.

2.3.4. Additional Security Considerations

Vulnerabilitas pada arsitektur keamanan sistem dapat menghasilkan pelanggaran ketentuan keamanan sistem. Vulnerabilitas digambarkan sebagai berikut :

- Channel yang tersembunyi. Langkah komunikasi yang tidak disengaja diantara dua atau lebih subjek membagi secara umum, dimana mendukung pemindahan informasi menjadi semacam cara yang melanggar ketentuan keamanan sistem. Pemindahan biasanya membutuhkan tempat melalui area penyimpanan umum atau melalui akses menuju bagian tertentu yang dapat menggunakan chanel waktu untuk komunikasi yang tidak terencana.
- Kurangnya pemeriksaan parameter. Kegagalan mengecek ukuran stream input yang ditetapkan oleh parameter.
- Maintenance Hook. Mekasnisme perangkat keras maupun perangkat lunak diinstal untuk mengizinkan maintenance sistem dan untuk melewati perlindungan keamanan sistem.
- Time of Check to Time of Use (TOC/TOU) Attack. Perlawanan yang merusak perbedaan waktu kontrol keamanan dipasang dan waktu servis resmi digunakan.

2.3.5. Recovery Procedures

Pada saat komponen sebuah perangkat keras atau perangkat lunak dari suatu sistem yang diakui mengalami kegagalan atau gangguan, sangat penting diketahui bahwa gangguan tersebut tidak memiliki ketergantungan pada kelengkapan aturan keamanan pada sistem tersebut. Sebagai tambahan, prosedur recovery tidak memberikan perlawanan terhadap pelanggaran aturan ketentuan keamanan sistem. Jika sebuah sistem yang dimulai diperlukan, sistem tersebut harus dimulai dengan aman. Awal harus terjadi dalam mode pemelihaaran yang mengizinkan akses hanya dari pengguna yang dipercaya dari terminal yang diyakini juga. Mode ini mendukung penggunaan sistem dan keamanan.

Pada saat komputer atau komponen jaringan gagal namun komputer/jaringan tetap berfungsi, hal tersebut dikenal dengan system toleransi kesalahan. Dalam toleransi ksalahan beroperasi, sistem harus mampu mendeteksi bahwa kesalahan tersebut memang telah terjadi itu, dan sistem harus mampu untuk mengoreksi kesalahan atau operasi di sekitarnya. Dalam sistem perbaikan kesalahan ini, eksekusi program terbatas dan sistem terlindung dari pengaruh kompromi tertentu pada saat kegagalan hardware atau software terjadi dan terdeteksi. Komputer atau jaringan berlanjut pada fungsi dalam tingkat yang lebih rendah. Kegagalan akhir pada masa tertentu pada sistem lalu dihubungkan pada komponen duplikat back up dalam waktu nyata pada saat hardware atau software tejadi, dimana sistem mampu melanjutkan proses.

Prosedur pemulihan sistem pada usaha kecil menengah tidak menjadi suatu yang kritis. Pada saat system usaha kecil dan menengah mati atau gagal, system dapat direstart atau diperbaiki dengan mode default yang aman. System dapat diperbaiki oleh pihak yang diberi kewenangan langsung ke system yang bermasalah tanpa membutuhkan terminal khusus. Penggunaan backup system bisa sangat membantu untuk mengalihkan fungsi sistem agar bisa berjalan kembali.

3. Assurance

Assurance secara sederhana didefinisikan sebagai tingkat kepercayaan dalam kepuasan atas kebutuhan mengenai jaminan rasa keamanan. Sesi berikut menjelaskan mengenai petunjuk utama dan standarisasi yang telah dikembangkan untuk mengevaluasi dan menerima aspek asuransi pada sebuah sistem.

3.1. Evaluation Criteria

Pada tahun 1985, TCSEC (Trusted Computer System Evaluation Criteria) telah dibangunan oleh NCSC (National Computer Security Center) untuk mendukung petunjuk dasar dalam mengevaluasi produk vendor pada kriteria keamanan tertentu.

TCSEC meliputi hal-hal sebagai berikut :

- sebuah dasar untuk menetapkan kebutuhan keamanan dalam spsifikasi tambahan.
- sebuah standar servis keamanan yang akan didukung melalui vendor untuk kelas yang berbeda pada kelengkapan keamanan.
- Sebuah maksud untuk mengukur tingkat kepercayaan pada sistem informasi.

Dokumen TCSEC, disebut dengan Orange Book karena warnanya, merupakan bagian dari petunjuk yang mana sampulnya berwarna warni dan dikenal dengan Seri Pelangi. Seri pelangi ditutupi oleh detil seperti yang tertera pada Appendix B. Dalam Buku Orange, objek kontrol dasar meliputi atuan keamanan, asuransi dan penjelasan akutanbilitas. TSCEC menempati posisi tertentu tapi tidak menutupi integritasnya. Fungsi (kontrol keamanan yang ditawarkan) dan asuransi (tingkatan dimana kontrol keamanan difungsikan seperti yang diharapkan) tidak terpisah dalam TCSEC sebagaimana tertera dalam kriteria evaluasi yang terbentuk nantinya. Orange Book menjelaskan mengenai kelas hirarki pada keamanan melalui huruf D sampai A sebagai berikut :

- D. Proteksi minim
- C. Proteksi keputusan (C1 dan C2)
- B. Proteksi mandatori (B1, B2 dan B3)
- Proteksi yang telah diverikasi, metode formil (A1)

DoD TNI (Trusted Network Interpretion) dijelaskan pada Buku Orange.,ditempatkan pada sistem jaringan komunikasi dan komputer yang telah diakui, dikenal dengan Buku Merah. TDI bertempat pada sistem manajemen data base yang terpercaya.

ITSEC (European Information Technology Security Evaluation Criteria) menempatkannya pada isu SIA. Produk atau sistem yang dievaluasi melalui ITSC dijelaskan sebagai target evaluasi (TOE). TOE harus memiliki target keamanan, yang meliputi mekanisme pemaksaan keamanan dan aturan keamanan sistem.

ITSEC secara terpisah mengevaluasi fungsi dan asuransi, yang meliputi 10 kelas fungsi (F), 8 level asuransi (Q), tujuh level kebenaran (E) dan delapan fungsi dasar keamanan pada kriteria yang telah ada. Juga menjelaskan 2 jenis asuransi. Yang pertama adalah kebenaran implementasi fungsi keamanan dan yang kedua adalah efektivitas TOE pada saat operasi.

Rating ITSEC terdapat pada form F-X, E, dimanan fungsi dan asuransi termasuk di dalamnya. Rating ITSEC bila disamakan dengan TCSEC adalah sebagai berikut :

F-C1, E1 = C1

F-C2, E2 = C2

F-B1, E3 = B1

F-B2, E4 = B2

F-B3, E5 = B3

F-B3, E36 = A1

Kelas lain pada ITSEC menempati posisi integritas tinggi dan kemampuan tinggi. TCSEC, ITSEC, dan CTCPEC telah dikembangkan ke dalam sebuah kriteria yang iknal dengan Common Criteria. Kriteria ini menjelaskan mengenai sebuah profil proteksi (PP), dimana implementasi pada spesifikasi tersendiri pada perlengkapan kemanan yang dibutuhkan dan proteksi pada sebuah produk bisa dibangun. Terminologi untuk kriteria umum pada tingkat pemeriksaan produk yang akan dites adalah EAL (Evaluation Assurance Level). Batasan EAL dari EA1 (testing fungsional) sampai EA7 (testing detil dan verifikasi desain formil).

Kriteria TOE berkaitan dengan produk yang akan diuji. Target keamanan (ST) tertera pada klaim keamanan untuk produk keamanan IT yang khusus. Juga, kriteria ini menjelaskan mengenai pengelompokan komponen keamanan sebagai sebuah kemasan. Fungsi pada kriteria ini ditujukan pada keperluan kelengkapan keamanan yang berfungsi baik, dimengerti dan sesuai standar yang berlaku untuk sistem IT. Kelengkapan ini disusun sedemikian rupa pada kesatuan TCB meliputi kontrol fisik dan logis, startup dan recovery, mediasi referensi, privileged states. Kriteria umum didiskusikan pada Appendi G. Seperti halnya TCSE dan ITSEC, rating pada Common Criteria juga hirarkis.

3.2. Certification and Accreditation

Di banyak lingkungan, metode resmi harus tersedia untuk meyakinkan bahwa pengamanan sistem informasi yang layak ditempatkan secara benar dan berjalan sesuai fungsinya masing-masing. Tambahan, pemegang wewenang harus bertanggung jawab untuk meletakkan sistema ke dalam operasi. Fungsi-fungsi berikut ini diketahui sebagai sertifikat dan akreditasi.

Sertifikat.

Evaluasi menyeluruh pada fitur pengamanan teknis dan non teknis dari sistem informasi dan pengamanan lain, yang terbentuk dalam penopang proses akreditasi untuk membentuk penambahan untuk desain khusus dan implementasi yang dibutuhkan kelengkapannya.

Akreditasi

Deklarasi resmi melalui DAA (Designated Approving Authority) dimana sistem informasi yang diyakini untuk beroperasi dalam mode keamanan khusus dengan menggunakan pengamanan pada batas resiko yang masih dapat diterima.

Sertifikat dan akreditasi pada sebuah sistem harus diperiksa melalui periode waktu yang telah ditentukan atau pada saat terjadi perubahan pada sistem dan atau lingkungannya. Kemudian, sertifikasi dan akreditasi ulang mutlak diperlukan.

untuk mendukung petunjuk dasar dalam mengevaluasi produk vendor pada kriteria keamanan tertentu Standarisasi Sertifikat dan akreditasi milik badan pertahanan dan pemerintah Amerika Serikat telah dikembangkan melalaui evaluasi sistem informasi. Standar tersebut adalah DITSCAP (Defense Information Technology Security Certification dan Accreditation Process) serta NIACAP (National Iformation Assurance Certification and Accreditation Process).

3.2.1.1. DITSCAP

DITSCAP menetapkan sebuah proses standar, satu set kegiatan, deskripsi pekerjaan umum adan struktur manajemen untuk menjelaskan dan mengakui sisem IT yang akan memelihara postur keamanan yang dibutuhkan. Proses ini direncanakan untuk menjelaskan bahwa sistem IT membutuhkan kelengkapan akreditasi dan bahwa sistem akan mengutamakan wujud keamanan yang diyakini sepanjang masa sistem tersebut. Berikut 4 tahap menuju DITCAP.

Fase 1. Definisi. Fase 1 memfokuskan pada pemahaman mengenai misi, lingkungan dan bentuk arsitektur agar dapat menentukan keperluan keamanan dan batasan usaha yang diperlukan utnuk mencapai pengakuan.

Fase 2. Verifikasi. Fase 2 memeriksa pengembangan atau pelaksanaan sistem yang dimodifikasi melalui informasi yang telah disepakati bersama dalam System Security Authorization Agreement (SSAA). Sasarannya adalah untuk menggunakan SSAA untuk membenuk sebuah pengembangan atas kesepakatan pada batas keamanan yang dipelukan seblum pengembangan sistem dimulai atau berubah menjadi sistem yang terbentuk sebelumnya. Setelah tahap akreditasi, SSAA menjadi landasan utama dalam dokumen konfigurasi keamanan.

Fase 3. Validasi. Fase 3 menerangkan berapa lama pelaksanaan sistem terintegrasi secara sempurna melalui informasi yang dimulai dalam SSAA.

Fase 4. Post Accreditation. Fase 4 meliputi kegiatan yang diperlukan untuk melanjutkan operasi dalam sistem IT yang telah diakui dalam lingkungan komputerisasi dan untuk menempatkan perubahan selama sistem tersebut berlangsung.

3.2.1.2. NIACAP

NIACAP membentuk standar nasional minimum untuk menjelaskan dan mengakui adanya sistem keamanan nasional. Proses ini memberi sebuah standar untuk aktivitas, pekerjaan umum dan struktur manajemen dalam menjelaskan dan mengakui keberadaan sisterm yang memberikan penjaminan informasi

dan postur keamanan pada sebuah sistem. NIACAP dirancang untuk menerangkan bahwa sistm informasi membtuhkan adanya pengakuan dalam bentuk dokumentasi yang diperlukan dan akan berlanjut terus dalam menentukan postur keamanan yang terakreditasi sepanjang umur sistem itu.

Berikut tiga tipe akreditasi NIACAP :

- Site Accreditation. Mengevaluasi aplikasi dan sitem pada lokasi secara spesifik
- Type Accreditation. Mengevaluasi sebuah aplikasi atau sistem yang didistribusikan pada sejumlah lokasi yang berbeda.
- System Accreditation. Mengevaluasi aplikasi utama atau penopang umum pada sistem.

NIACAP disusun berdasarkan 4 fase : Definisi, Verifikasi, Validasi dan Akreditasi Akhir. 4 hal tersebut diperlukan untuk mencapai DITSCAP. Saat ini, CIAP (Commercial Information Security Analysis Process (CIAP) dikembangkan untuk evaluasi sistem komersial dengan menggunakan metodologi NIACAP.

3.3. The Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CCM didasari oleh premis bahwa jika anda dapat menjamin kualitas sebuah proses yang digunakan sebuah organisasi, maka anda dapat menjamin kualitas produk dan pelayanan yang dihasilkan pada proses tersebut. Hal tersebut telah dikembangkan melalui konsorsium pemerintah dan pakar industri dan saat ini berada di bawah naungan ISSEA (International Systems Security Engeineering Association) pada situs www.issea.org. SSE-CCM merupakan :

menjelaskan karakteristik proses dari security engineering untuk mendapatkan hasil yang baik.

- Melakukan praktek terbaik dalam industri
- Mendapatkan pelatihan dan kemampuan berimprovisasi
- Memberi ukuran pertumbuhan dalam kemampuan melakukan proses

Bagian SSE-CCM ditempatkan pada areal keamanan sebagai berikut :

- Keamanan operasi
- Kemanan informasi
- Keamanan jaringan
- Keamanan fisik
- Keamanan personil
- Keamanan adiministratif
- Keamanan komunikasi
- Keamanan pemancar
- Keamanan komputer

Metodologi dan sistem pengukuran SSE-CMM memberikan referensi dalam membandingkan engineering pengamanan sistem yang telah ada praktek terbaik melalui elemen tersebtu yang dijelaskan dalam model. Hal ini disimpulkan dalam 2 dimensi yang digunakan untuk mengukur kemampuan suatu

organisasi untuk melakukan aktivitas tertentu. Dimensi-dimensi ini terdiri atas daerah kekuasaan dan kemampuan.

Khusus untuk dimensi domain, SSE-CMM menetapkan 11 security engineering Pas dan 11 Pas yang terorganisir dan berkaitan dengan proyek, pada setiap BPs yang ada. BPs merupakan karakteristik utama yang harus tetap ada dalam proses pengmanan sebelum organisasi dapat menuntut kepuasan dalam PA yang telah diberikan. 22 PA dan hubungannya dengan BP diakui sebagai praktik terbaik dalam engineering security system. PA terdiri atas :

Security Engineering

- PA01 kontrol keamanan administer
- PA02 menaksir dampak yang ditimbulkan
- PA03 Menaksir resiko keamanan
- PA04 menaksir kecurangan
- PA05 menaksir vulnerabilitas
- PA06 membangun argumen penjaminan
- PA07 koordinasi keamanan
- PA08 monitor postur keamanan
- PA09 membei input keamanan
- PA10 menetapkan kebutuhan keamanan
- PA11 pemeriksaan dan menentukan umur keamanan

Project dan Organizational Practices

- PA12. Menentukan kualitas
- PA13 Mengatur konfigurasi
- PA14 Mengatur resiko proyek
- PA15 Monitor dan kontrol usaha teknis
- PA16 Perencanaan Usaha teknis
- PA17 menjelaskan proses engineering sistem organisasi
- PA18 Improvisasi proses egineering sistem organisasi
- PA19 Mengatur Evaluasi batas produk
- PA20 mengatur lingkungan pendukung engineering sistem
- PA21 memberi skil dan pengetahuan
- PA22 Koordinasi dengan suplier.

GP digolongkan dalam tingkat kematangan dan dikelompokkan dalam suatu bentuk dan perbedaan diantara lima level kematangan engineering keamanan. Atribut tersebut antara lain sbb :

- Level 1

  1.1 BP terbentuk

- Level 2
  2.1. performance perencanaan
  2.2. perfomance disiplin
  2.3. verifikasi performance
  2.4. tracking performance
- Level 3
  3.1. Menjelaskan sebuah proses standar
  3.2. Membentuk proses yang jelas
  3.3. menghubungkan setiap proses
- Level 4
  4.1. membangun hasil mutu yang terukur
  4.2. secara obyektif mengatur performance
- Level 5
  5.1. mengembangkan kemampuan organisasi
  5.2 mengembangkan efektifitas proses

Penjelasan atas kelima level diatas adalah sebagai berikut :

- Level 1, " terbentuk tak resmi, " fokus pada organisasi atau proyek yang melakukan suatu proses yang melibatkan BP. Pernyataan khusus untuk level ini adalah. "Anda harus melakukannya sebelum anda bisa mengaturnya".
- Level 2, Terencana dan Terlatih, fokus pada definisi level-proyek, perencanaan dan isu-isu performance. Pernyataan yang sesuai untuk karakter level ini, "Pahami apa yang terjadi pada suatu proyek sebelum menjelaskan proses yang lebih mendalam.
- Level 3, Ditegaskan dengan baik, fokus pada bidang pekerjaan dari proses yang dijelaskan pada level organisasi. Pernyataan yang sesuai untuk level ini adalah :Gunakan yang terbaik apa yang telah anda pelajari dari proyek-proyek anda untuk menghailkasn proses yang lebih baik.
- Level 4, "terkendali secara kuantitaitf", fokus pada pengukuran yang diikat pada hasil bisnis pada suatu organisasi. Meskipun penting untuk memulai penngumpulan dan menggunakan ukuran poyek mendasar sejak awal, pengukuran dan penggunaan data yang tidak diharapkan sampai level yang lebih tinggi telah tercapai. Pernyataan khusus pada level ini " Anda tak dapat mengukur sesuatu sampai anda tahu sesuatu itu apa dan "pengaturan dengan pengukuran hanya berarti pada saat anda mengukur hal-hal yang benar".
- Level 5, "Improvisasi yang berlanjut", mencapai pengaruh kekuatan dari keseluruhan kemajuan praktek manajemen yang terlihat pda level-level sebelumnya yang menekankan daya kultural yang akan menopang hasil yang diperoleh. Sebuah pernyataan yang memberikan makna khusus pada level ini adalah "sebuah budaya pengembangan yang berkesinambungan membutuhkan sebuah pondasi praktek manajemen, proses yang jelas dan hasil yang terukur".

Menegaskan fakta bahwa solusi CMM bisa diterapkan secara efektif pada usaha kecil dan menengah sebaik penerapannya pada perusahaan besar, Commodere Vavin Chandra[4] mengatakan bahwa "konsep dasar dari solusi CMM secara aktual bisa diterapkan kepada seluruh organisasi, aplikasi atau kontek bisnis".

CMM bisa diterapkan pada usaha kecil dan menengah . yang menjadi pertanyaan, bagaimana menggunakan CMM secara efektif untuk mengkombinasikan realita bisnis dengan proses perangkat lunak yang well-defined?. CMM adalah sebuah set petunjuk yang bisa membantu sebuah perusahaan mengelola resiko dan juga untuk merencanakan dan mengelola bisnis dengan cara yang efektif. Komponen utama dari MM adalah level maturity, key process area dan goal.

CMM bisa diterapkan pada seluruh organisasi yang terlibat dalam pengembangan pereangkat lunak. Bagaimanapun, mengerjakan suatu proses memerlukan sebuah analisa dan pengawasan yang berkelanjutan dan implementasi dari proses pengukuran koreksi. Hal ini bisa menjadi sebuah tantangan untuk sebuah perusahaan yang tidak menggunakan CMM, terutama pada area usaha kecil dan menengah.

Salah satu kesalahan terbesar yang terjadi pada usaha kecil dan menengah yang menggunakan CMM hanya mempunyai tujuan bertahan di pasar. Dari pada berfokus pada hasil akhir, sebaiknya usaha kecil dan menengah bersegera memenuhi tenggat akhir proyek.

Dengan tekanan untuk memuaskan konsumen, usaha kecil dan menengah sebaiknya sering membuang kesalahan pada saat peredaman proyek sebagai sesuatu yang bisa di respon nanti. Usaha kecil dan menengah perlu mengingat bahwa perusahaan besar menhadapi permasalah yang sama dengan usaha kecil dan mengengah (perusahaan besar ini juga memiliki masalah dengan proyek yangtertunda, informasi yang tidak terdokumentasi, manajer yang tidak berpengalaman, kurangnya latihan, kurangnya alokasi sumberdaya, dan lain-lain. Perencanaan, kontak konsumen, menyampaikan komitmen dan mengelola resiko adalah masalah yang berhubungan dengan setiap bisnis. CMM juga bisa digunakan sebagai alat yang sangat berguna sebagai panduan peningkatan proses, dan ini adalah konsep dasar yang secara aktual bisa diterapkan kepada seluruh organisasi, terutama usaha kecil dam menengah.

CMM menyediakan petunjuk untuk manajemen yang baik dan penerapan rekayasa, dengan penekanan yang kuat pada menajemen, komunikasi, dan koordinasi untuk pengembangan dan perawatan dari proses perangkat lunak. Pengguna CMM harus mempertimbangkan perengkat lunak sebagai buku petunjuk dan bukan sebagai diktat, dan melihat pada penggabungan pencapaian sukses antara proses perangkat lunak dan tujuan bisnis.

Ada beberapa kasus yang kurang baik, dimana kurangya kemampuan rekayasa yang baik dan penerapan manajemen menghadapi sebuah masalah. Hal ini menjadi kenyataan pada kasus seoarang tenaga teknis yang baik yang dipromosikan untuk posisi manajerial, tanpa bekal pengalaman manajamen atau pelatihan yang cukup.

Tapi perubahan terjadi hanya ketika ada ketidakpuasan dengan status quo yang ada dan ketika manajer dan staff berkeinginan melakukan sesuatu secara berbeda. Hal ini benar-benar terjadi pada usaha kecil dan menengah.

Dari pengalaman yang ada, tujuan utama dari solusi CMM adalah untuk menyediakan rekayasa perangkat lunak yang baik dan penerapan manajemen untuk setiap proyek pada setiap lingkungan. Hal ini sangat mudah diterapkan untuk perusahaan besar, proyek virtual, proyek yang tersebar secara geografis, organisasi pelayanan perangkat lunak dan usaha kecil dan menengah. Pada usaha kecil dan menengah di India, mereka memulai dari awal dengan mengidentifikasikan area yang mereka perlukan mejadi fokus untuk meningkatkan proses perangkat lunak. Hal ini secara gradual membawa mereka kepada langkah kedua (dimana mereka perlu fokus pada perencanaan dan manajemen proyek), kemudian diikuti oleh tahap kedua.

Menjawab pertanyaan, apakah CMM bisa diterapkan pada segemen usaha kecil dan menengah? Jawabannya adalah bisa, CMM bisa digunakan pada segmen usaha kecil dan menengah atau bahkan pada proyek yang kecil. Sebagai kesimpulan, sebaiknya CMM fokus pada mengidektifikasi masalah yang berhubungan, melembagakan kegiatan initi seperti perencanaan, pelatihan dan lain-lain pada perusahaan dan mengkombinasikan peningkatan proses perangakat lunak dengan tujuan bisnis.

4. Information Security Models

Bentuk-bentuk yang digunakan dalam informasi keamanan memformalisasikan “Keamanan kebijakan”. Bentuk-bentuk keamanan ini bersifat abstrak atau intuisi dan melengkapi kerangka kerjanya untuk memahami konsep-konsep dasar. Pada bagian ini ada 3 bentuk yang akan dijelaskan, yaitu: Model kontrol akses, Model Integritas dan Modul Arus Informasi.

4.1. Access Control Models

Proses kontrol akses dapat dirangkai ke dalam bentuk yang membatasi ruang lingkup dasar dan perbedaan yang tampak pada model ini. Bentuk dari kontrol akses ini adalah akses matriks, model “Take-Grant”, Model “Bell-LaPadula”, dan model “State Machine” .

4.1.1. The Access Matrix

Akses Matriks merupakan tindakan akses yang benar dirangkai dari subjek ke objek. Akses yang benar yaitu tipe data yang dapat membaca, menulis dan mengerjakan. Subjek merupakan kesatuan yang aktif untuk melakukan pencarian sumber atau objek yang benar. Subjek dapat berupa orang, program atau proses. Objek merupakan kesatuan yang pasif, seperti file atau tempat penyimpanan data. Dalam beberapa hal ini, satu sisi berupa subjek dalam konteks dan objek dalam konteks yang lainnya. Bentuk matriks kontrol akses ditunjukkan dalam gambar 3.1.

Subjek/Objek	Data Masukan	Data Gaji	Proses Pengambilan	Sprint server A
Joe	Baca	Baca/Tulis	Bekerja	Tulis
Jane	Baca/Tulis	Baca	Tidak ada	Tulis
Proses Pengecekan	Baca	Baca	Bekerja	Tidak ada
Program Biaya	Baca/Tulis	Baca/Tulis	Panggil	Tulis

Gambar 3.1. Contoh Matriks Akses

Kolom matriks akses disebut “Access Control Lists (ACLs)”, dan disebut “Capability Lists”. Bentuk matriks akses ini mendukung kontrol akses sepenuhnya karena matriks ini merupakan individu yang memiliki kendali sepenuhnya. Dalam matriks kontrol akses kemampuan subjek dibatasi oleh 3 macam bentuk (objek, posisi dan pengacakan). Jadi 3 bentuk yang membatasi ini posisi di mana subjek harus merupakan objek sepanjang pengacakan nomor berlangsung yang biasanya mencegah terjadinya proses pengulangan . Ketika bentuk batasan ini sama halnya dengan “Karberos Tickets” yang dibahas pada bab sebelumnya “Sistem Kontrol Akses”.

Masalah yang paling penting dalam proteksi file adalah membuat akses yang yang bergantung pada identitas user yang mengakses berkas. Implementasi yang umum untuk menerapkan akses yang bergantung pada identitas sebuah file atau objek adalah Access Control List (ACL). ACL menspesifikasikan nama user dan tipe akses yang mana yang dizinkan untuk setiap user. Akan tetapi, terdapat kelemahan jika mengimplementasikan ACL untuk proteksi berkas:

1. Harus melist satu persatu user terhadap tipe akses yang diizinkan terhadap berkas.
2. Manajemen ruang kosong pada memori akan lebih susah.

Kelemahan ACL dapat diatasi dengan cara mengklasifikasikan user menjadi tiga, yaitu:

1. Owner, user yang membuat file/ objek tersebut.
2. Group, sekumpulan user yang berbagi file/ objek yang membutuhkan akses yang sama terhadap sebuah file/objek.
3. Universe, semua user pada sistem tersebut. Penulisannya adalah file/objek (owner, group, right).

Sebagai contoh, ada empat user (A, B , C, dan D) yang masing-masing termasuk dalam group system, staff, dan student.

File0 (A,*, RWX)

File1 (A, system, RWX)

File2 (A, *, RW-) (B, staff, R--) (D , *, RW-)

File3 (*, student, R--)

File4 (C,*,---) (*, student, R--)

File0 dapat dibaca, dieksekusi dan ditulis oleh user A pada semua group yang ada. File1 dapat dibaca, dieksekusi dan ditulis oleh user A pada group system. File2 dapat dibaca dan ditulis oleh user A dan D pada semua group, dibaca oleh user B pada group staff. File3 dapat dibaca oleh semua member dari group student. File4 memiliki keistimewaan yaitu ia mengatakan bahwa user C di setiap group tidak memiliki akses apapun, tetapi semua member group student dapat membacanya, dengan mengunakan ACL memungkinkan menjelaskan spesifik user, group yang mengakses sebuah file atau objek[3].

Kebanyakan sistem informasi bagi usaha kecil dan menengah dibangun dengan asumsi tidak terdapat keamanan komputer yang akan diterapkan. Kebutuhan tersebut cukup hingga kemajuan teknologi jaringan umumnya dan internet pada khususnya dan peningkatan penggunan koneksi yang terus tersambung seperti xDSL dan model kabel. Koneksi ke internet yang selalu tersambungkan ini berarti komputer dapat diketahui dengan mudah oleh hacker, karena keberadaan komputer relatif lebih mudah diprediksi dan alamat IP yang stabil-yang berarti baik alamat IP yang statis atau bentuk pool kecil alamat yang berdekatan. Jika alamat IP koneksi komputer pengguna ke internet statis, komputer tersebut cukup ditemukan satu kali saja; jika alamat IP koneksi komputer pengguna ke internet diberikan secara dinamis, hacker harus mencari tiap kali ingin mengetahui lokasi komputer tersebut tetapi sering kali pencarian tersebut hanya pada sejumlah kecil alamat dari koleksi alamat yang telah diketahui. Begitu sebuah komputer telah ditemukan alamatnya, cracker atau hacker dapat mulai mencari informasi atau menyerang

komputer pengguna tersebut. Hal inilah yang menjelaskan mengapa saat pengguna komputer lebih sering terhubung ke internet, kebutuhan keamanan pengguna komputer tersebut juga meningkat.

Satu cara utama untuk memperoleh keamanan komputer adalah mengijinkan atau membatasi akses ke file atau directory atau sumber daya komputasi yang dipergunakan pengguna komputer pada suatu komputer. Dengan pembatasan akses tersebut, administrator komputer dapat mengetahui siapa yang atau yang tidak melakukan suatu aktifitas pada sistem yang diaturnya. Hal yang lebih penting, administrator dapat mengendalikan siapa saja yang melakukan aktifitas tertentu.

Suatu usaha kecil menengah bisa memiliki roles acces controll sesuai kebutuhannya, tapi sebaiknya pengelompokan izinnya unik. Dan tidak ketinggalan pula, bahwa terlalu banyak role berarti memerlukan perawatan struktur keamanan yang lebih.

Untuk pemilihan sistem operasi pada usaha kecil dan menengah, sebaiknya menggunakan sistem operasi yang memiliki setting default sistem keamanan yang cukup. Hindari penggunaan windows9x dan windows ME, karena sistem operasi tersebut memiliki kemampuan yang terbatas dalam mengontrol dan mengelola pengguna[2].

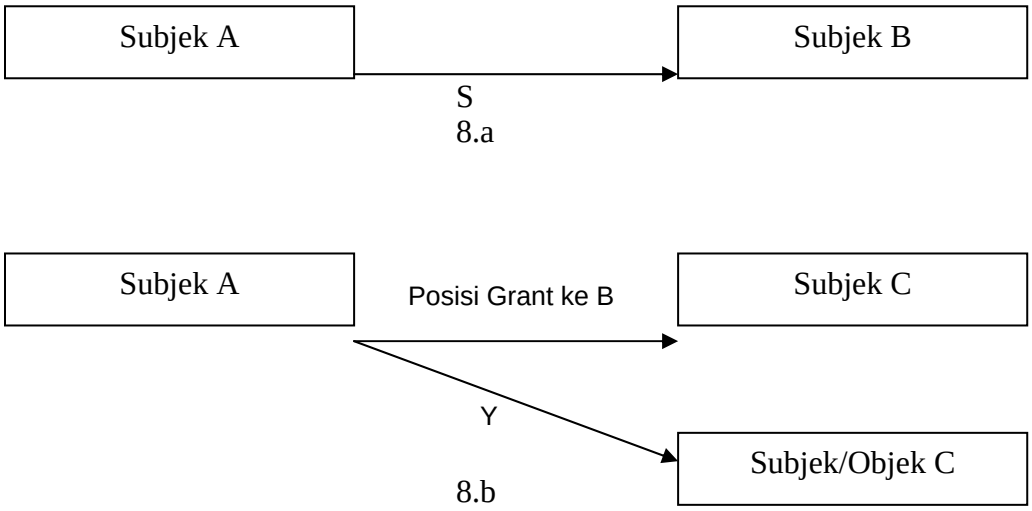
4.1.2. Take-Grant Model

Bentuk “Take-Grant” menggunakan petunjuk grafik untuk posisi yang lebih spesifik bahwa subjek dapat mentransfer objek dan sebuah subjek dapat diambil dari subjek lainnya. Contoh: Asumsikan bahwa Subjek A menduduki posisi yang mencakup posisi “Grant” yang ditujukan ke objek B. Kejadian ini digambarkan dalam gambar 3.2.a. Kemudian asumsikan bahwa subjek A dapat mentransfer posisi “Grant” untuk objek B ke ojek C, dan subjek A menempati posisi yang lain (Y) ke objek D. Dalam beberapa hal ini objek D berlaku sebagai sebuah objek dan objek lainnya berlaku sebagai subjek. Kemudian seperti yang ditunjukkan oleh panah tebal dalam gambar 3.2.b, subjek C menempati posisi “Y” ke subjek/objek D, karena subjek A melewati posisi “Grant” ke subjek C.

“Take Capability” bekerja dalam bentuk khusus seperti gambar “Grant”.

4.1.3. Bell-LaPadula Model

Bentuk Bell-LaPadulla dikembangkan untuk memformalkan kebijakan keamanan multi level Departemen Keamanan Amerika Serikat. Label DoD merupakan klasifikasi keamanan pada tingkatan yang berbeda. Seperti pada pembahasan sebelumnya, tingkatan ini terdiri dari “UnClasisfied”, “Confidential”, “Secret” dan “Top Secret” dari sensitivitas yang paling kecil ke sensitivitas yang paling besar.



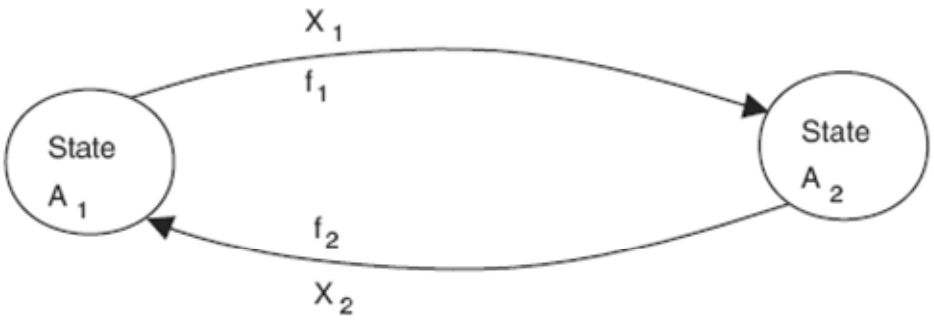
Gambar 3.2. Model Take-Grant

Individual yang menerima penjelasan “Confidential, “Secret”, atau “top Secret” dapat mengakses material pada klasifikasi tingkatan tersebut atau di bawahnya. Syarat tambahan, bagaimanapun juga individual harus memiliki pengetahuan mengenai material tersebut. Jadi seorang individual menjelaskan “Secret” hanya dapat mengakses label data “secret” yang penting bagi individual guna menampilkan fungsi tugas pekerjaan. Bentuk Bell-LaPadulla setuju dengan penggolongan material. Bentuk Bell-LaPadulla tidak dialamatkan secara lengkap atau sempurna.

Model Bell-LaPadulla dengan konsep “State Machine”, konsep ini membatasi rangkaian kondisi yang diizinkan (Ai) dalam sistem. Perpindahan dari satu tempat ke tempat lainnya di atas penerima input (Xi) yang dibatasi oleh fungsi transisi (fk). Kenyataan model ini menjamin bahwa posisi awal merupakan kepastian dan bahwa transisi selalu berhasil. Perpindahan (transisi) antara 2 tempat digambarkan dalam gambar 3.3

Bentuk Bell-LaPadulla membatasi posisi yang telah ditetapkan melalui 3 unsur multi level yang pertama 2 unsur penerapan kontrol akses dan yang ketiga, 1 unsur yang diizinkan kontrol akses. Unsur-unsur dijelaskan sebagai berikut:

1. Unsur keamanan yang sederhana (unsur ss) menyatakan pembacaan informasi oleh subjek pada tingkatan sensitivitas yang lebih rendah dari objek tingkatan sensitivitas yang lebih tinggi yang tidak diizinkan (tidak terbaca).



Gambar 3.3. Perpindahan Posisi Dibatasi Oleh Fungsi F Dan Input X.

2. Unsur keamanan bintang (*), menyatakan penulisan informasi dengan subjek pada tingkatan sensitivitas yang lebih tinggi ke objek tingkatan yang lebih rendah tidak diizinkan tidak terbaca).
3. Unsur keamanan polisi. Menggunakan matriks akses untuk mengenal kode akses kontrol.

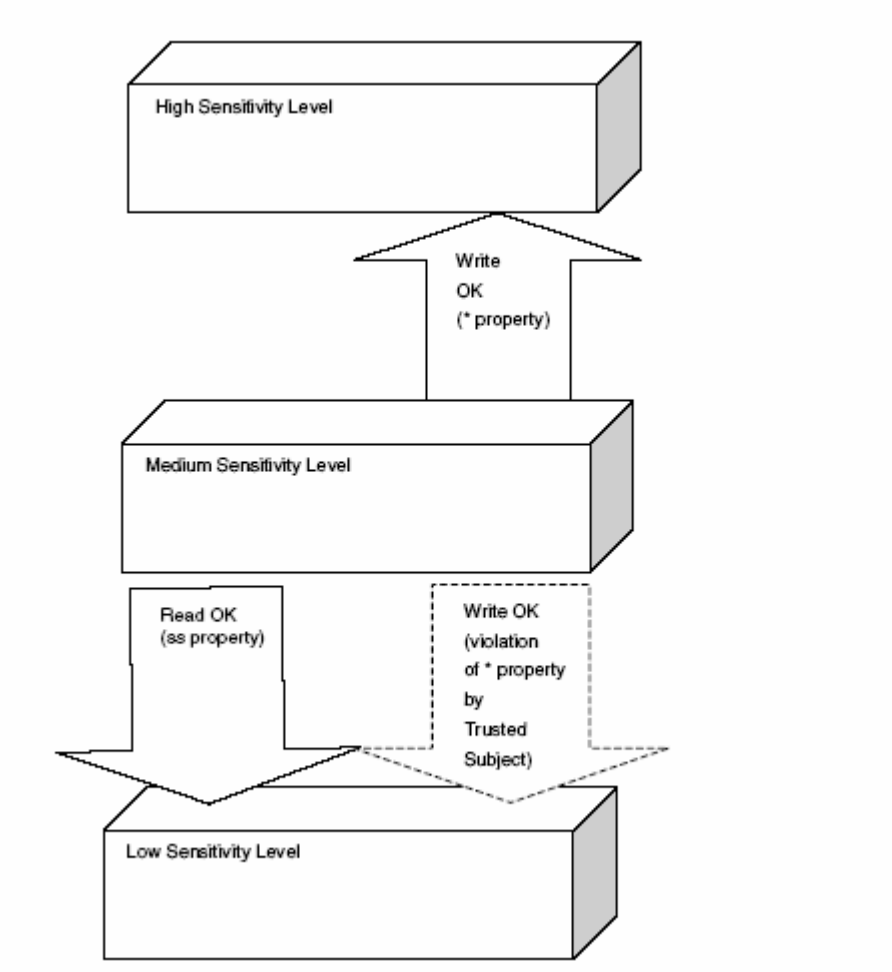
Kecepatan unsur bintang (*) terlalu terbatas dan menambah data yang disyaratkan. Misalnya unsur ini dapat memindahkan paragraf yang sensitivitasnya lebih rendah dalam dokumen yang lebih tinggi ke dokumen yang sensitivitasnya lebih rendah. Transfer informasi diizinkan oleh bentuk Bell-LaPadulla melalui subjek yang dipercaya (trusted subject). Trusted Subject dapat melanggar unsur bintang (*), namun sekarang tidak bisa lagi. Konsep ini digambarkan dalam gambar 5.10.

Dalam beberapa contoh, sebuah unsur yang disebut unsur yang keras ketetapannya. Unsur ini menetapkan bahwa pembacaan dan penulisan yang diizinkan pada tingkatan sensitivitas tertentu tetapi tidak juga untuk tingkatan sensitivitas yang lebih tinggi atau lebih rendah.

Model ini membatasi permintaan sistem. Permintaan dibuat saat sistem dalam posisi v1; sebuah keputusan (d) dibuat di atas perminaan, dan sistem mengubah posisi v2(R,d,v1,v2) yang mewakili jenis model ini. Kadang-kadang kecepatan model (bentuk) ini memastikan bahwa ada perpindahan dari satu tempat (posisi) ke tempat yang lain.

Model kerja Bell-LaPadulla berdasarkan pada akses matriks. Sistem keamanan polisi membatasi pengendalian khusus ke sumber sistem. Pengendalian berhubungan dengan bagaimana posisi mengakses yang dibatasi dan bagaimana mereka mengevaluasi (mengecek). Beberapa pencapaian sistem kerja berdasarkan ketergantungan konteks dan kontrol akses ketergantungan isi. Ketergantungan isi mengontrol membuat keputusan akses berdasarkan data yang ada dalam objek, sebaliknya kontrol ketergantungan konteks menggunakan subjek atau atribut objek ataupun karakteristik sistem untuk membuat keputusan. Contoh beberapa karakteristik termasuk aturan kerja, akses-akses awal, dan pembuatan file tanggal dan waktu.

Karena banyak bentuknya, model Bell-LaPadulla memiliki kelemahan. Berikut ini salah satu kelemahannya yang besar adalah:



Gambar 3.4. Biba Model Axioms

- Model ini memungkinkan atau mengizinkan atau mempertimbangkan jalur perubahan informasi yang normal dan tidak memperbolehkan jalur yang tersembunyi atau rahasia
- Model ini tidak sejalan dengan sistem modern yang menggunakan pembagian arsip dan banyak pengelola (data)
- Model ini tidak secara gamblang atau tegas membatasi apa yang diinginkan dengan sebuah perubahan keadaan yang tertutup
- Model ini berdasarkan pada kebijakan pengamanan bertingkat atau berjenjang dan tidak memperbolehkan model jenis kebijakan lain yang mungkin digunakan oleh sebuah organisasi.

4.2. Integrity Models

Pada banyak organisasi baik pemerintahan maupun bisnis keterbukaan data adalah penting atau lebih penting dari pada kerahasiaan pada penerapan / aplikasi tertentu. Jadi model keterpaduan resmi

dikembangkan, singkatnya model keterpaduan di kembangkan sebagai suatu perbandingan atas model kerahasiaan Bell-LaPadulla dan kemudian menjadi lebih mampu untuk menghadapi keperluan meningkatnya syarat penambahan keterpaduan.

4.2.1. The Biba Integrity Model

Keterpaduan ini biasanya dicirikan dengan 3 tujuan berikut :

1. Data dilindungi dari perubahan yang dibuat oleh para pengguna yang tidak berhak.
2. Data dilindungi dari modifikasi atau perubahan yang tidak di perkenankan oleh pengguna yang berhak.
3. Data ini pada bagian dalam dan bagian luar saling bersesuaian data yang didapat. Pada sumber data harus seimbang pada bagian dalam dan sesuai dengan bagian luar, situasi dunia nyata.

Untuk menuju sasaran keterpaduan pertama, model biba dikembangkan pada tahun 1977 sebagai perbandingan keterbukaan atas model kerahasiaan Bell-LaPadulla. Model biba berdasarkan pola-pola dan menggunakan hubungan kurang dari atau sama dengan. Pola-pola struktur ini diartikan sebagai kumpulan perintah terpisah dengan Least Upper Bound (LUB) : (batas yang lebih tinggi dari terendah) dan Greatest Lower Bound (GLB) : (batas yang lebih rendah dari yang tertinggi). Pola-pola ini mewakili sekumpulan tingkat keterpaduan dari suatu hubungan perintah yang termasuk dalam tingkatan tersebut.

Mirip dengan model klasifikasi tingkat perbedaan kepekaan Bell-LaPadulla model biba menggabungkan objek ke dalam tingkat perbedaan keterbukaan. Model ini menggolongkan 3 aksioma (ketetapan) keterpaduan :

1. Aksioma (ketetapan) keterbukaan sederhana.
   Menetapkan bahwa subjek pada sebuah tingkat keterpaduan tidak diperbolehkan untuk meneliti sebuah objek pada tingkat keterbukaan yang lebih rendah (tidak melihat ke bawah)
2. The * (star) Integrity Axiom.
   Menetapkan bahwa sebuah objek pada suatu tingkat keterbukaan tidak diperbolehkan untuk mengubah suatu objek dari tingkat keterpaduan yang lebih tinggi.
3. Sebuah subjek dari level pertama keterpaduan tidak dapat meminta sebuah objek atas level / tingkatan keterpaduan yang lebih tinggi

4.2.2. The Clark-Wilson Integrity Model

Model pendekatan metode Clack - Wilson (1987) telah dikembangkan sebagai suatu kerangka kerja yang digunakan pada dunia nyata di lingkungan perniagaan / bisnis. Model ini merujuk pada 3 sasaran keterbukaan dan menegaskan syarat-syarat sebagai berikut :

- Constrained Data Item (CDI) => bagian data yang mendesak
  Sebuah data pokok yang mempunyai keterpaduan sebagai sesuatu yang dipelihara
- Integrity Verification Prosedure (IVP) => Prosedur Pemeriksaan Keterpaduan
  Memperkuat semua hal tentang CDI yang merupakan sesuatu yang benar dari suatu wujud keterpaduan

- Transformation Procedure (TP) => Prosedur Transformasi

  Manipulasi dari CDls yang telah selesai yang merupakan suatu transaksi yang berbentuk baik. Yang mana telah ada perubahan CDI dari satu wujud keterbukaan ke wujud keterpaduan yang lainnya.

- Uncostrained Data Item => Sistem (bagian) yang tidak mendesak

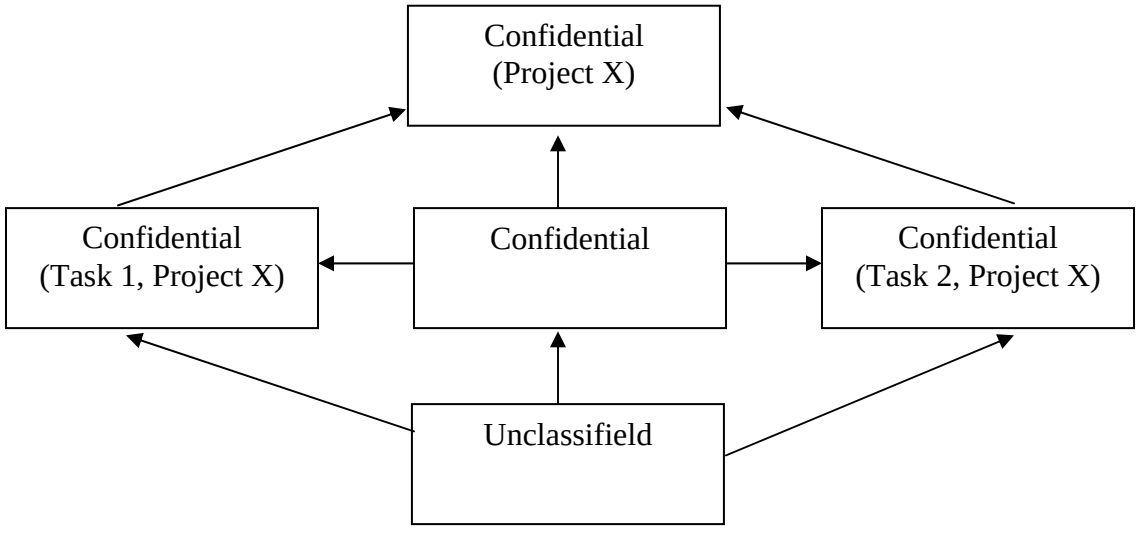
  Bagian data ini terletak di bagian luar dari tempat kontrol (pengawasan_ dari contoh lingkungan, sebagai contoh masukan informasi.

Model Clack – Wilson membutuhkan penamaan keterpaduan untuk memutuskan tingkatan keterpaduan dari sebuah bagian data untuk membuktikan bahwa keterpaduan ini telah terpelihara setelah menggunakan aplikasi dari suatu TP (Transformation Procedure). Model ini telah memasukkan mekanisme dalam menjalankan data dari luar kemantapan dalam mengambil tindakan, pemisahan dari kewajiban dan keterpaduan kebijaksanaan oleh pemberi perintah.

4.3. Information Flow Models

Suatu model aliran informasi yang berdasarkan atas wujud mesin, dan aliran ini terdiri dari suatu objek, wujud peralihan dan pola-pola (kebijakan mengalir) keadaan. Pada keadaan seperti sekarang ini, objek juga bias mewakili penggunaannya, sebuah informasi yang memaksa untuk mengikuti aliran dalam suatu pengawasan yang harus memiliki surat izin oleh kebijakan keamanan. Sebagai contoh ditunjukkan pada gambar 3.5.

Dalam gambar 3.5 Aliran informasi dari sesuatu yang tidak digolongkan menjadi suatu rahasia di dalam tugas di proyek x dan kombinasi tugas di proyek x. Informasi ini dapat mengikuti aliran informasi di dalam satu aturan.



Gambar. 3.5. Model Alir Informasi

4.3.1. Non-Interference Model

Model ini menceritakan tentang model aliran informasi dengan larangan yang terdapat pada aliran informasi. Pada dasarnya prinsip model ini adalah merupakan sebuah grup yang terdiri dari para pengguna (A). Seorang yang menggunakan Perintah (C). Jangan mencampuri urusan para pengguna (B), seseorang yang menggunakan perintah (D). Konsep ini ditulis sebagai A,C :| B,D Perintah untuk menyatakan kembali peraturan ini. Tindakan yang dilakukan oleh grup A yang menggunakan perintah C tidak dapat dilihat oleh para pengguna grup B yang menggunakan perintah D.

4.3.2. Composition Theories

Pada beberapa aplikasi, sistem ini dibangun oleh kombinasi sistem-sistem yang kecil. Sebuah situasi yang menarik perhatian untuk menanggap apakah keamanan suatu komponen sistem telah mampu terpelihara ketika mereka akan mengkombinasikan ke dalam sebuah entitas formulir yang besar.

Jhon Mc Clean mempelajari tentang persoalan ini pada tahun 1994 (MCLean. J). “Teori keseluruhan tentang suatu komposisi yang digunakan untuk menetapkan jejak tertutup di bawah fungsi untuk disisipkan di antaranya”. Dimulai pada tahun 1994 IEEE kumpulan karangan penelitian tentang keamanan dan kerahasiaan IEEE Press, 1994)”

Dia mendefenisikan 2 buah gagasan komposional : yaitu dari dalam dan luar. Berikut ini adalah beberapa tipe gagasan yang berasal dari luar.

- Cascading, Suatu sistem masukan yang mendapatkan dari keluaran dari sistem yang lainnya.
- Feedback, Satu sistem yang memberikan masukan kepada sistem kedua, yang merupakan putaran arus balik yang berasal dari masukan pada sistem yang pertama.
- Hookup, Sebuah sistem yang merupakan kombinasi dengan sistem lainnya sebaik dengan entitas yang berasal dari luar.

Gagasan komposisi internal (dari dalam) adalah suatu titik potong, perpaduan dan perbedaan. Keseluruhan kesimpulan dari pelajaran ini adalah tentang keamanan kepemilikan dari suatu sistem yang kecil di mana telah terpelihara di bawah suatu komposisi (di beberapa instansi). Dalam gagasan cascading sebelumnya telah juga terdapat suatu subjek yang berasal dari variabel sistem yang berasal dari gagasan yang lainnya.

Daftar Pustaka

1. Krutz, R.L and Russel D. Vines, "*The CISSP® Prep Guide: Gold Edition*", John Wiley Publising, Inc., 2003.
2. Shea, B., "*Have You Locked the Castle Gate?: Home and Small Business Computer Security*", Pearson, 2002.
3. Masyarakat Digital Gotong Royong, "*Pengantar Sistem Operasi Komputer*" ,Bab 39 SISTEM *BERKAS* JARINGAN, http://bebas.vlsm.org/v06/Kuliah/SistemOperasi/BUKU/SistemOperasi/ch39s13.html, diakses 8 Desember 2005.
4. Chandra, V, Commodere "*Quest for excellence in CMM*" http://www.expresscomputeronline.com/20030324/opinion3.shtml, diakses 8 Desember 2005