Makalah Keamanan Aplikasi
Semester V

Nama : Nirwansyah Ramdhani

NPM : 41155050160126

Teknik Informatika - B

Universitas Langlangbuana

KONSEP KEAMANAN INFORMASI

Keamanan informasi adalah seluruh prinsip-prinsip, standar-standar, dan mekanisme yang akan ditemui dengan tujuan fundamental ‘confidentiality’, ‘integrity’, dan ‘availability’ pada suatu informasi dan sumber pemroses informasi.

CIA memiliki tiga fokus utama tujuan, yaitu confidentiality, integrity, dan availability. Setiap komponen dalam CIA ini sangat berperan penting dalam kesempurnaan keamanan sistem informasi.

a. Confidentiality

   Pada konteks keamanan informasi, confidentiality memiliki arti bahwa sebuah informasi harus selalu dalam posisi yang tidak diketahui oleh masyarakat luas (rahasia) dan hanya orang-orang tertentu yang memiliki wewenang untuk mengakses informasi tersebut. Kita tahu bahwa informasi adalah sebuah kekuatan, dan di era informasi ini, akses menuju sebuah informasi menjadi lebih penting lagi.

   Akses tidak berwenang yang terjadi pada informasi yang rahasia (confidential) dapat memiliki konsekuensi yang sangat serius, tidak hanya pada aplikasi keamanan nasional, tapi juga berlaku pada industri/pabrik dan komersial.

Terdapat beberapa cara mekanisme proteksi ‘confidentiality’ untuk system informasi, antara lain adalah teknik kriptografi dan control akses. Maka ancaman-ancaman seperti malware, intruders, jaringan yang taka man, dan system administrasi yang lemah dapat diatasi.

b. Integrity

Integrity adalah kepercayaan, asal mula, kesempurnaan, dan kebenaran sebuah informasi sebagai bentuk pencegahan modifikasi pada suatu informasi yang tak berwenang atau yang tak pantas. Integrity yang dimaksud pada keamanan informasi tidak hanya pada informasi itu, namun juga integritas/kebenaran pada asal mula dimana informasi itu didapatkan.

Terdapat beberapa mekanisme proteksi pada ‘Integrity’, yang dibagi menjadi dalam 2 kelompok, yaitu mekanisme pencegahan, seperti control akses yang mencegah pemodifikasian informasi yang tak berwenang, selain itu ada teknik pendeteksian, dimana diadakan sebuah pendeteksian pemodifikasian informasi yang tak berwenan setelah mekanisme pencegahan gagal dilakukan. Ontrol yang menjaga ‘integrity’ termasuk prinsip antara lain privilege (hak), separation (pemisahan), dan rotation (perotasian) dalam pekerjaan.

c. Availability

Pada triad yang terakhir adalah availability pada informasi, atau keberadaan informasi itu sendiri. Apa yang terjadi, ketika dua triad awal, yaitu C-I berjalan, namun orang yang berwenang tidak bisa mengakses dan menggunakannya? Maka itu pun akan menjadi percuma. Maka tidak ada yang perlu enkripsi dan control akses yang luar biasa ribet/kompleks apabila informasi

yang dibuuhkan tidak bisa diakses oleh orang yang berwenang. Jadi, availability juga merupakan hal yang penting disamping confidentiality dan integrity.

Ancaman terhadap availability dikenal sebagai denial of service atau disingkat DoS. Musibah yang terjadi natural dan dibuat oleh manusia bisa mempengaruhi availabilitas. Maka, disaster recovery planning itu dibutuhkan untuk meminimalisir kehancuran/kehilangan data.

- Access Control

Access Control adalah suatu proses dimana user diberikan akses dan hak untuk melihat sistem, sumber atau informasi. Untuk keamanan komputer, access control meliputi otorisasi, otentikasi, dan audit dari suatu kesatuan untuk memperoleh akses. Access control memiliki subjek dan objek. User (manusia), adalah subjek yang mencoba untuk mendapatkan akses dari objek, Software. Dalam sistem komputer, daftar access control berisi perizinan dan data kemana user memberikan izin tersebut. Data yang telah memiliki izin hanya dapat dilihat oleh beberapa orang dan ini tentunya sudah dikontrol oleh access control.

Hal ini memungkinkan administrator untuk mengamankan informasi dan mengatur hak atas informasi apa saja yang boleh diakses, siapa yang bisa mengakses informasi tersebut, dan kapan informasi tersebut bisa diakses.

- Tantangan dalam Access Control
    - Berbagai macam tipe user membutuhkan level akses yang berbeda
    - Berbagai macam sumber memiliki klasifikasi level yang berbeda
    - Bermacam-macam data identitas harus disimpan di tipe user berbeda
    - Lingkungan perusahaan berubah secara kontinuitas

- Akses Kontrol
    - Authentication
      melakukan verifikasi bahwa pengguna atau entitas sistem tertentu adalah valid untuk melakukan akses terhadap sistem.
    - Authorization
      Pemberian hak atau izin terhadap entitas sistem untuk mengakses sumber daya sistem. Fungsi ini menentukan siapa yang dipercaya untuk melakukan aksi tertentu didalam sistem.

- Reverse Engineering
  atau bisa disebut back engineering, adalah proses di mana objek buatan manusia didekonstruksi untuk mengungkapkan desain, arsitektur, atau untuk mengekstraksi pengetahuan dari objek; mirip dengan penelitian ilmiah, satu-satunya perbedaan adalah bahwa penelitian ilmiah adalah tentang fenomena alam

KRIPTOGRAFI

Kriptografi (cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data .Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi.

Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan.

Pada prinsipnya, Kriptografi memiliki 4 komponen utama yaitu:

1. Plaintext, yaitu pesan yang dapat dibaca
2. Ciphertext, yaitu pesan acak yang tidka dapat dibaca
3. Key, yaitu kunci untuk melakukan teknik kriptografi
4. Algorithm, yaitu metode untuk melakukan enkrispi dan dekripsi

Kemudian, proses yang akan dibahas dalam artikel ini meliputi 2 proses dasar pada Kriptografi yaitu:

1. Enkripsi (Encryption)
2. Dekripsi (Decryption)

- Subtitusi
  Dalam kriptografi, sandi substitusi adalah jenis metode enkripsi dimana setiap satuan pada teks terang digantikan oleh teks tersandi dengan sistem yang teratur. Metode penyandian substitusi telah dipakai dari zaman dulu (kriptografi klasik) hingga kini (kriptografi modern).

Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan decrypt. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahanciphertext oleh orang yang tidak berhak.
Metode ini dilakukan dengan mengganti setiap huruf dari teks asli dengan huruf lain sebagai huruf sandi yang telah didefinisikan sebelumnya oleh algoritma kunci.

- Chesar Chiper
  Caesar Cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi. Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks. Teknik seperti ini disebut juga sebagai chiper abjad tunggal.

  Algoritma kriptografi Caesar Cipher sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama.

- One Tipe Pad
  Algoritma OTP merupakan algoritma berjenis symmetric key yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara stream cipher dimana cipher berasal dari hasil XOR antara bit plaintext dan bit key.

Sebagai tambahan, algoritma ini sering digunakan dalam proses enkripsi cookie (termasuk pemrosesan transaksi online menggunakan kartu kredit) karena prosesnya yang relatif mudah.

- Symmetric Key
  Symmetric dan Asymmetric kriptografi merupakan jenis algoritma kriptografi berdasarkan penggunaan kunci. Singkatnya, kriptografi symmetric menggunakan kunci yang sama untuk melakukan proses enkripsi dan dekripsi sedangkan kriptografi asymmetric menggunakan kunci yang berbeda untuk encrypt dan decrypt.

- Hash algorithms
  Hash function adalah suatu fungsi yang berguna untuk mengkompresi/memperkecil sebuah string yang panjang menjadi sebuah string yang lebih pendek. Dalam dunia kriptografi, hash function bukan merupakan suatu barang yang baru. Merupakan salah satu cabang dalam kriptografi, hash function memiliki daya tarik tersendiri dikarenakan cukup banyak aplikasi yang menggunakan hash function dalam penerapannya.

Terdapat 2 bagian dari akses kontrol, yaitu :

- Authentication/Otentikasi:
  - Apakah kamu adalah orang yg kamu akui ?
  - Tentukan apakah akses dibolehkan atau tidak
  - Cek mesin atau orang
  - Atau memang mau mesin ke mesin
- Authorization/Otorisasi:
  - Apakah kamu dibolehkan melakukan itu ?
  - Apabila boleh akses, apa yg boleh kamu lakukan ?
  - Jaga batasan apa2 saja yg boleh

Perbandingan Key & Passwords

- **Crypto keys**
- 64 bits
- Jadi ada 2^{64} keys
- Key adalah random
- Pembajak perlu mencoba sebanyak 2^{63} password

- **Passwords**
- 8 characters, (ada 256 karakter di keyboard)
- Jadi ada $256^8 = 2^{64}$ password
- Pengguna umumnya tdk membuat password secara random
- Pembajak perlu mencoba sebanyak 2^{63} password

Perbandingan Password yang Bagus & Tidak Bagus

- Passwords jelek
  - frank
  - Fido
  - Password
  - incorrect
  - Pikachu
  - 102560
  - AustinStamp
- Baguskah pswd ini?
  - jfIej,43j-EmmL+y
  - 09864376537263
  - P0kem0N
  - FSa7Yago
  - OnceuP0nAt1m8
  - PokeGCTall150

Penyerangan terhadap password

- Umumnya attack
  - Target ke akun tertentu
  - Target berbagai ke akun yg ada di sistem
  - Target ke berbagai akun di berbagai sistem
  - Target utk melumpuhkan denial of service (DoS)
- Pelaku attack
  - Outsider > normal user > administrator

- Biometrik

  Aplikasi teknologi biometrik bisa dicontohkan seperti ketika Anda memberikan tanda masuk ke kantor atau akses ke komputer menggunakan pemindai sidik jari; mengambil uang dari mesin kas yang dapat memindai mata Anda untuk mengenali bahwa Anda-lah pemilik sah uang itu; mengidentifikasi diri Anda pada bank melalui telepon dengan memakai pengenal suara (voice recognition); dan check in untuk penerbangan hanya dengan melewati sebuah kamera di

bandara yang mengenali Anda sebagai penumpang berlangganan.

Contoh lainnya dari biometrik adalah :

- Sidik jari
- Tanda tangan
- Pengenal wajah
- Pengenal suara
- Suara/gaya langkah
- “Bau badan” (odor recognition)

Cookie Website

Cookie adalah informasi berukuran kecil yang disimpan suatu situs web di komputer pengguna, dan digunakan setiap kali pengguna mengunjungi situs web tersebut. Biasanya ini dilakukan untuk memudahkan pengguna, seperti "mengingat" pengguna setiap kali ia mengunjungi situs web tersebut.

Penggunaan cookie di internet adalah hal standar. Meski sebagian besar browser web otomatis menerima cookie (yaitu, mengizinkan situs web menyimpan cookie di komputer Anda), semua browser web memiliki opsi untuk menerima atau menolak cookie. Lihat Pernyataan Privasi kami untuk informasi selengkapnya tentang bagaimana cookie digunakan di situs ini.

1. Lampson’s
    a. ACL (Access Control List)

ACL (Access Control List) merupakan metode selektivitas terhadap packet data yang akan dikirimkan pada alamat yang dituju. Secara sederhana ACL dapat kita ilustrasikan seperti halnya sebuah standard keamanan. Hanya packet yang memiliki kriteria yang sesuai dengan aturan yang diperbolehkan melewati gerbang keamanan, dan bagi packet yang tidak memiliki kriiteria yang sesuai dengan aturan yang diterapkan, maka paket tersebut akan ditolak. ACL dapat berisi daftar IP address, MAC Address, subnet, atau port yang diperbolehkan maupun ditolak untuk melewati jaringan.

Jenis-jenis ACL

<u>Standard ACL</u>

Standard ACL merupakan jenis ACL yang paling sederhana. Standard ACL hanya melakukan filtering pada alamat sumber (Source) dari paket yang dikirimkan. Alamat sumber yang dimaksud dapat berupa alamat sumber dari jaringan (Network Address) atau alamat sumber dari host. Standard ACL dapat diimplementasikan pada proses filtering protocol TCP, UDP atau pada nomor port yang digunakan. Meskipun demikian, Standard ACL hanya mampu mengijinkan atau menolak paket berdasarkan alamat sumbernya saja. Berikut ini adalah contoh konfigurasi dari Standard ACL.

Router(config)#access-list list list [nomor daftar akses IP standar] [permit / deny] [IP address] [wildcard mask]

Pada konfigurasi di atas, nomor daftar akses IP adalah 1 – 99, kemudian permit / deny adalah sebuah parameter untuk mengizinkan atau menolak hak akses. IP address diisi dengan alamat pengirim atau alamat asal, kemudian wildcard mask adalah untuk menentukan jarak dari suatu subnet.

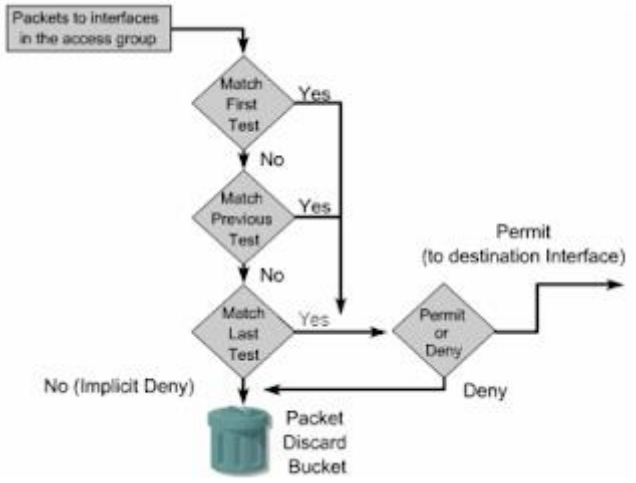
<u>Extended ACL</u>

Extended ACL merupakan jenis ACL yang mampu memberikan tingkat keamanan yang lebih baik ketimbang Standard ACL. Extended ACL mampu melakukan filtering pada alamat sumber (source) dan alamat tujuan (destination). Selain itu extended ACL memberikan keleluasaan kepada admin jaringan dalam melakukan proses filtering dengan tujuan yang lebih spesifik.

Router(config)#access-list [nomor daftar akses IP extended] [permit atau deny] [protokol] [source address] [wildcard mask] [destination address] [wildcard mask] [operator] [informasi port]

Pada konfigurasi diatas, nomor daftar akses IP extended adalah 100 – 199, kemudian sama dengan standart ACL permit atau deny adalah sebuah parameter untuk mengizinkan atau menolak hak akses. Protokol dapat diisi dengan TCP, UDP, dsb. Destination address diisi dengan alamat yang akan dituju, wildcard mask untuk menentukan jarak subnet.

Cara Kerja ACL



Keputusan dibuat berdasarkan pernyataan/statement cocok dalam daftar akses dan kemudian menerima atau menolak sesuai apa yang

didefinisikan di daftar pernyataan. Perintah dalam pernyataan ACL adalah sangat penting, kalau ditemukan pernyataan yang cocok dengan daftar akses, maka router akan melakukan perintah menerima atau menolak akses.

Pada saat frame masuk ke interface, router memeriksa apakah alamat layer 2 cocok atau apakah frame broadcast. Jikaalamat frame diterima, maka informasi frame ditandai dan router memeriksa ACL pada interface inbound.

Jika ada ACL, paket diperiksa lagi sesuai dengan daftar akses. Jika paket cocok dengan pernyataan, paket akan diterima atau ditolak. Jika paket diterima di interface, ia akan diperiksa sesuai dengan table routing untuk menentukan interface tujuan dan di-switch keinterface itu. Selanjutnya router memeriksa apakah interface tujuan mempunyaiACL. Jika ya, paket diperiksa sesuai dengan daftar akses. Jika paketcocok dengan daftar akses, ia akan diterima atau ditolak. Tapi jika tidak ada ACL paket diterima dan paketdienkapsulasi di layer 2 dan di-forwardkeluar interface device berikutnya.

b. C-List (Capability List)

Salah satu cara untuk mempartisi matriks adalah dengan row. Dengan demikian kita memiliki semua hak akses dari satu pengguna bersama. Ini disimpan dalam struktur data yang disebut Capability List, yang mencantumkan semua hak akses atau kemampuan yang dimiliki pengguna. Berikut ini adalah Capability List contoh :

Fred --> /dev/console(RW)--> fred/prog.c(RW)--> fred/letter(RW) --> /usr/ucb/vi(X) Jane --> /dev/console(RW)--> fred/prog.c(R)--> fred/letter() --> /usr/ucb/vi(X)
Ketika suatu proses mencoba untuk mendapatkan akses ke suatu objek, sistem operasi dapat memeriksa Capability List yang tepat.

Pengaturan ini memiliki beberapa kelemahan:

Jika setiap capability list memiliki entri untuk semua objek, banyak entri akan menunjukkan bahwa tidak ada akses yang diizinkan. Sebagai contoh, sebagian besar file pribadi Fred dapat dilindungi dari Jane. Pemborosan ruang ini dapat dihilangkan dengan hanya mencantumkan objek-objek yang dapat diakses pengguna.

Kumpulan objek yang dapat diakses oleh satu pengguna, khususnya pengguna istimewa, mungkin sangat besar. Ini bisa mahal untuk mencari capability list untuk pengguna seperti itu, kecuali kita menggunakan pengalamatan berbasis kemampuan, yang disajikan kemudian ketika kita mendiskusikan kemampuan secara lebih rinci. capability list harus dibuat untuk pengguna baru.

2. MLS
    a. BLP (Bell La Padulla)

The Bell-LaPadula Model (disingkat BLP) adalah model state machine digunakan untuk menegakkan akses kontrol dalam aplikasi pemerintah dan militer. Ini dikembangkan oleh David Elliott Bell dan Leonard J. LaPadula, setelah bimbingan yang kuat dari Roger R. Schell untuk meresmikan US Department of Pertahanan (DoD) keamanan bertingkat (MLS) kebijakan. Model ini adalah model transisi state formal kebijakan keamanan komputer yang menggambarkan seperangkat aturan kontrol akses yang menggunakan label keamanan pada objek dan izin untuk mata pelajaran. Label keamanan berkisar dari yang paling sensitif (misalnya "Top Secret"), sampai ke paling sensitif (misalnya, "Unclassified" atau "Public"). Model Bell-LaPadula adalah contoh dari sebuah model di mana tidak ada perbedaan yang jelas perlindungan dan keamanan.

Fitur

Model Bell-LaPadula berfokus pada kerahasiaan data dan akses dikendalikan untuk diklasifikasikan informasi, berbeda dengan Model Biba Integritas yang menggambarkan aturan untuk perlindungan data integritas. Dalam model formal, entitas dalam suatu sistem informasi dibagi menjadi subyek dan benda. Gagasan tentang "negara aman" didefinisikan, dan terbukti bahwa setiap negara yang diawetkan transisi keamanan dengan bergerak dari negara yang aman untuk mengamankan negara, sehingga induktif membuktikan bahwa system memenuhi tujuan keamanan model. Model Bell-LaPadula dibangun

pada konsep mesin negara dengan satu set negara diijinkan dalam sistem jaringan komputer.

Transisi dari satu negara ke negara lain didefinisikan oleh fungsi transisi. Sebuah sistem negara didefinisikan sebagai "aman" jika satu-satunya mode akses yang diizinkan subyek ke obyek yang sesuai dengan kebijakan keamanan. Untuk menentukan apakah mode akses tertentu diperbolehkan, clearance subjek dibandingkan dengan klasifikasi objek (lebih tepatnya, untuk kombinasi klasifikasi dan set kompartemen, membuat tingkat keamanan) untuk menentukan apakah subjek berwenang untuk mode akses tertentu. Skema izin / klasifikasi dinyatakan dalam kisi. Model ini mendefinisikan dua kendali akses mandatory (MAC) aturan dan satu kontrol akses discretionary (DAC) aturan dengan tiga sifat keamanan:

1. The Property Security Simple - subjek pada tingkat keamanan yang diberikan mungkin tidak membaca suatu objek pada tingkat keamanan yang lebih tinggi (ada read-up).
2. The *-properti (baca "bintang"-property) - subjek pada tingkat keamanan yang diberikan tidak harus menulis ke benda pada tingkat keamanan yang lebih rendah (tidak ada write-down). The *-properti juga dikenal sebagai Properti kurungan.
3. The Discretionary Keamanan Properti - penggunaan matriks akses untuk menentukan kebijaksanaan kontrol akses. Transfer

informasi dari dokumen-sensitivitas tinggi terhadap dokumen-sensitivitas yang lebih rendah mungkin terjadi dalam model Bell-LaPadula melalui konsep pelajaran dipercaya. Subyek Trusted tidak dibatasi oleh *-property. Subyek Untrusted berada. Subyek Trusted harus terbukti dipercaya berkaitan dengan kebijakan keamanan. Model keamanan ini diarahkan kontrol akses dan ditandai dengan kalimat: "tidak membaca, tidak menulis." Bandingkan model Biba, Clark- Model Wilson dan model Wall Chinese.

Keterbatasan

· Hanya alamat kerahasiaan, kontrol menulis (salah satu bentuk integritas), *-property dan kontrol akses discretionary
· Covert channels yang disebutkan tetapi tidak ditangani secara komprehensif
· Prinsip ketenangan membatasi penerapannya ke sistem di mana tingkat keamanan yang tidak berubah

b. Biba

Model Biba yang dikembangkan oleh Kenneth J. Biba pada tahun 1975, adalah sistem peralihan status formal dari kebijakan keamanan komputer yang menggambarkan serangkaian aturan kontrol akses yang dirancang untuk memastikan integritas data. Data dan subjek

dikelompokkan ke dalam level integritas yang teratur. Model dirancang agar subjek tidak merusak data dalam tingkat yang lebih tinggi dari subjek, atau rusak karena data dari tingkat yang lebih rendah daripada subjek.

Secara umum model dikembangkan untuk menunjukkan integritas sebagai prinsip inti, yang merupakan kebalikan langsung model Bell-LaPadula.

Secara umum, pelestarian integritas data memiliki tiga sasaran:

- Mencegah modifikasi data oleh pihak yang tidak berwenang
- Mencegah modifikasi data yang tidak sah oleh pihak yang berwenang
- Menjaga konsistensi internal dan eksternal (yaitu data mencerminkan dunia nyata)

Model keamanan ini diarahkan pada integritas data dan ditandai dengan frasa: "baca, tulis". Ini berbeda dengan model Bell-LaPadula yang dicirikan oleh frasa "read kebawah, write keatas".

Dalam model Biba, pengguna hanya dapat membuat konten pada atau di bawah tingkat integritas mereka sendiri (seorang biksu dapat menulis buku doa yang dapat dibaca oleh orang biasa, tetapi tidak dapat dibaca oleh seorang imam besar). Sebaliknya, pengguna hanya dapat melihat konten pada atau di atas tingkat integritas mereka

sendiri (seorang biksu dapat membaca buku yang ditulis oleh imam besar, tetapi mungkin tidak membaca pamflet yang ditulis oleh orang biasa yang rendah hati). Analogi lain yang harus dipertimbangkan adalah rantai komando militer. Seorang Jendral boleh menulis perintah kepada seorang Kolonel, yang dapat mengeluarkan perintah ini kepada seorang Mayor. Dengan cara ini, perintah asli Jenderal tetap utuh dan misi militer dilindungi (dengan demikian, "read up" integritas). Sebaliknya, seorang Pribadi tidak akan pernah dapat memberikan perintah kepada Sersan-nya, yang mungkin tidak pernah memberikan perintah kepada seorang Letnan, juga melindungi integritas misi ("write down").

Model Biba mendefinisikan seperangkat aturan keamanan, dua yang pertama mirip dengan model Bell-LaPadula. Dua aturan pertama ini adalah kebalikan dari aturan Bell-LaPadula:

- Properti Integritas Sederhana menyatakan bahwa subjek pada tingkat integritas tertentu tidak boleh membaca data pada tingkat integritas yang lebih rendah (dibaca).
- Properti Integritas * (bintang) menyatakan bahwa subjek pada tingkat integritas tertentu tidak boleh menulis data pada tingkat integritas yang lebih tinggi (tulis).

- Invocation Property menyatakan bahwa proses dari bawah tidak dapat meminta akses yang lebih tinggi; hanya dengan subjek pada tingkat yang sama atau lebih rendah.

3. Compartment

Compartment adalah nama yang dikaitkan dengan peran. Anda menetapkan bahwa peran adalah bagian dari compartment dengan menambahkan nama compartment ke setiap peran dalam compartment. Ketika peran dikompartasikan, nama compartment digunakan sebagai pemeriksaan tambahan saat menentukan otoritas pengguna untuk mengakses atau membuat dokumen dalam basis data. compartment tidak berpengaruh pada pelaksanaan hak istimewa. Tanpa keamanan compartment, perizinan diperiksa menggunakan OR semantik.

Misalnya, jika dokumen telah membaca izin untuk peran1 dan membaca izin untuk peran2, pengguna yang memiliki peran1 atau peran2 dapat membaca dokumen itu. Jika peran tersebut memiliki compartment berbeda yang terkait dengannya (misalnya, compartment1 dan compartment2, lain - lain), maka izin diperiksa menggunakan DAN semantik untuk setiap compartment, serta semantik OR untuk setiap peran non-dikompresi. Untuk mengakses dokumen jika role1 dan role2 berada dalam compartment yang berbeda, pengguna harus memiliki role1 dan role2 untuk mengakses

dokumen, serta peran non-compartmented yang memiliki izin yang sesuai pada dokumen.

Jika ada izin pada dokumen yang memiliki compartment, maka pengguna harus memiliki compartment itu untuk mengakses salah satu kemampuan, bahkan jika kemampuannya bukan dengan compartment.

Akses ke dokumen memerlukan izin di setiap compartment yang ada izin pada dokumen, terlepas dari kemampuan izin. Jadi jika ada izin baca untuk peran dalam compartment1, harus ada izin pembaruan untuk beberapa peran dalam compartment1 (tetapi tidak harus peran yang sama). Jika Anda mencoba menambahkan membaca, menyisipkan, pembaruan node, atau mengeksekusi izin yang merujuk peran yang dikompartasikan ke dokumen yang tidak ada izin pembaruan dengan compartment yang sesuai.

4. Covert Channel

Covert Channel adalah jenis serangan yang menciptakan kemampuan untuk mentransfer objek informasi antara proses yang tidak seharusnya diizinkan untuk berkomunikasi dengan kebijakan keamanan komputer. Istilah, berasal pada tahun 1973 oleh Lampson, didefinisikan sebagai saluran "tidak dimaksudkan untuk transfer informasi sama sekali, seperti efek program layanan pada beban

sistem," untuk membedakannya dari saluran yang sah yang mengalami kontrol akses oleh COMPUSEC.

Karakteristik

Covert Channel disebut demikian karena tersembunyi dari mekanisme kontrol akses sistem operasi yang aman karena tidak menggunakan mekanisme transfer data yang sah dari sistem komputer (biasanya, baca dan tulis), dan karena itu tidak dapat dideteksi atau dikendalikan oleh mekanisme keamanan yang mendasari sistem operasi yang aman. Saluran terselubung sangat sulit untuk dipasang di sistem nyata, dan sering dapat dideteksi dengan memantau kinerja sistem. Selain itu, mereka menderita rasio signal-to-noise rendah dan tingkat data yang rendah (biasanya, pada urutan beberapa bit per detik). Mereka juga dapat dihapus secara manual dengan jaminan tingkat tinggi dari sistem yang aman dengan strategi analisis covert channel yang mapan.

Covert channel berbeda dari, dan sering disalahartikan dengan, eksploitasi saluran yang sah yang menyerang sistem pseudo-secure dengan jaminan rendah menggunakan skema seperti steganografi atau bahkan skema yang kurang canggih untuk menyamarkan objek terlarang di dalam objek informasi yang sah. Penyalahgunaan saluran yang sah oleh steganografi secara khusus bukan bentuk Covert channel.

Covert channel dapat menerobos melalui sistem operasi yang aman dan memerlukan tindakan khusus untuk mengendalikan. Analisis Covert channel adalah satu-satunya cara yang terbukti untuk mengendalikan Covert channel. Sebaliknya, sistem operasi yang aman dapat dengan mudah mencegah penyalahgunaan saluran yang sah, jadi membedakan keduanya adalah penting. Analisis saluran yang sah untuk objek-objek tersembunyi sering disalahpahami sebagai satu-satunya cara yang berhasil untuk penyalahgunaan saluran yang sah. Karena jumlah ini untuk analisis sejumlah besar perangkat lunak, itu ditunjukkan pada awal tahun 1972 menjadi tidak praktis. Tanpa diberitahu tentang hal ini, ada pula yang disesatkan untuk percaya bahwa analisis akan "mengelola risiko" dari saluran yang sah ini.

Mengidentifikasi saluran rahasia

Hal-hal biasa, seperti keberadaan file atau waktu yang digunakan untuk komputasi, telah menjadi media di mana Covert channel berkomunikasi. Covert channel tidak mudah ditemukan karena media ini sangat banyak dan sering digunakan.

Dua teknik yang relatif lama tetap menjadi standar untuk menemukan Covert channel yang potensial. Satu bekerja dengan menganalisis sumber daya sistem dan pekerjaan lain di tingkat kode sumber.

Malware (Malicious Software) adalah suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer. Malware dapat menginfeksi banyak komputer dengan masuk melalui email, download internet, atau program yang terinfeksi.

Malware bisa menyebabkan kerusakan pada sistem komputer dan memungkinkan juga terjadi pencurian data / informasi. Hal yang pada umumnya terjadi penyebab malware adalah mendownload software dari tempat ilegal yang disisipan malware. Malware mencakup virus, worm, trojan horse, sebagian besar rootkit, spyware, adware yang tidak jujur, serta software-software lain yang berbahaya dan tidak diinginkan oleh pengguna PC.

Cara Kerja Malware / Virus Komputer

Virus komputer umumnya dapat merusak perangkat lunak komputer dan tidak dapat secara langsung merusak perangkat keras komputer tetapi dapat mengakibatkan kerusakan dengan cara memuat program yang memaksa over process ke perangkat tertentu. Efek negatif virus komputer adalah memperbanyak dirinya sendiri, yang membuat sumber daya pada komputer (seperti penggunaan memori) menjadi berkurang secara signifikan. Hampir 95% virus komputer berbasis sistem operasi Windows. Sisanya menyerang Linux/GNU, Mac, FreeBSD, OS/2 IBM, dan Sun Operating System. Virus yang ganas akan merusak perangkat keras.

Contoh malwarenya adalah seperti dibawah ini :

- Brain virus (1986)
- Morris worm (1988)
- Code Red (2001)
- SQL Slammer (2004)
- Stuxnet (2010)
- Botnets (currently fashionable malware)
- Future of malware?

Morris Worm

Morris Worm adalah salah satu malware pertama yang menghebohkan dunia. Nama malware ini diambil dari nama pembuatnya Robert Morris, pada saat itu adalah mahasiswa di Cornell University. Malware ini mulai dipublish tanggal 2 november 1988. Malware ini berhasil menginfeksi lebih dari 6000 komputer, padahal saat itu baru sekitar 60000 komputer yang terhubung internet. Jadi malware ini menginfeksi sekitar 10% komputer dunia pada saat itu.

Cara Mendeteksi Malware

Terdapat 3 cara untuk mendeteksi malware, yaitu :

- Signature detection
- Change detection
- Anomaly detection

FUTURE MALWARE

Beberapa tahun dari sekarang sebenarnya sudah dapat dipastikan bahwa akan semakin banyak virus-virus baru lahir. Entah itu yang ganas, biasa, atau ‘ramah’. Sementara itu, semua pakar sepakat bahwa virus-virus komputer yang lama atau klasik tidak akan mengalami kematian, hal ini wajar dan memang sangat sesuai dengan sifat-sifat virus biologis pada kenyataannya. Patut diingat oleh semua pengguna komputer di atas planet bumi bahwa tidak akan ada istilah

‘mati’ untuk program komputer, dan virus komputer itu pun sejatinya merupakan sebuah program komputer yang akan ‘hidup’ atau bergerak sesuai dengan kode penyusun (source code) yang telah dibuat oleh sang penciptanya.