Acces Control

Integritas

Integritas berusaha untuk mencegah modifikasi tidak sah dari informasi.Dalam kata lain, integritas berusaha untuk mencegah tidak sah untuk menulis akses data

ketersediaan

Memastikan ketersediaan informasi yang tersedia saat dibutuhkan .Sistem harus dapat digunakan atau tersedia untuk penggunaan bisnis normal .Contoh serangan terhadap denial-of-service ketersediaan, yang berusaha untuk menyangkal (atau ketersediaan layanan dari sebuah sistem

Pengungkapan perubahan dan kehancuran

Cia juga dapat dijelaskan oleh triad sebaliknya ialah pengungkapan , perubahan , dan kehancuran ( ) ayah .Pengungkapan yang tidak sah adalah pengungkapan informasi; perubahan adalah modifikasi dari data yang tidak sah , dan kehancuran yang membuat sistem yang tidak tersedia .Kadang-kadang perubahan sementara yang merupakan singkatan dari cia , merupakan singkatan dari sang ayah yang disajikan dalam rangka

Identitas dan pengesahan

Identitas adalah suatu klaim: jika nama anda adalah orang x , anda memperkenalkan diri dengan mengatakan aku x orang . identitas sendiri masih kurang karena tidak ada bukti .Anda juga bisa memperkenalkan diri dengan mengatakan aku orang y . membuktikan klaim identitas yang disebut otentikasi: anda mengotentikasi klaim identitas , biasanya dengan menyediakan bagian dari informasi atau sebuah objek yang hanya kau yang dimiliki , seperti mendapatkan password atau paspor anda .

Otorisasi

Otorisasi menggambarkan tindakan yang dapat anda lakukan di sistem anda tidak pernah diketahui dan dibuktikan .Tindakan meliputi dapat membaca , menulis , atau pelaksana program atau berkas

Akuntabilitas pengguna

Akuntabilitas pengguna memegang bertanggung jawab untuk tindakan mereka.Ini biasanya dicapai oleh penebangan dan menganalisis data audit.Menegakkan akuntabilitas membantu menjaga jujur orang jujur. untuk beberapa pengguna mengetahui bahwa data login adalah tidak cukup untuk memberikan akuntabilitas: mereka harus tahu bahwa data adalah login dan diaudit dan sanksi yang mungkin hasil dari pelanggaran kebijakan.

Nonrepudiation

berarti pengguna tidak dapat menyangkal atau menolak) setelah dilakukan transaksi .Ini menggabungkan otentikasi dan integritas ialah nonrepudiation authenticates identitas pengguna yang melakukan transaksi dan menjamin integritas transaksi itu .Anda harus memiliki integritas dan kedua pengesahan telah membuktikan nonrepudiation: anda menandatangani kontrak untuk membeli sebuah mobil (mengotentikasi identitas anda sebagai pembeli) tidak ada gunanya jika mobil dealer dapat mengubah harga dua puluh ribu dolar dari 40 ribu dolar untuk (melanggar integritas kontrak) .

hak pengguna

Berarti yang paling sedikit hak pengguna diberi jumlah minimum dari (akses diperlukan sk) melakukan tugasnya , tetapi tidak ada lagi .Paling tidak hak istimewa yang ada dilakukan untuk kelompok dari objek .Harus mengetahui lebih sedikit pun dari granular hak pengguna: kebutuhan harus supaya ia mengetahui bahwa bagian kecil dari catatan yang spesifik informasi sebelum mengaksesnya

Subyek dan obyek

Subjek adalah sebuah entitas aktif di sebuah sistem data .Contoh dari sebagian besar mata pelajaran yang melibatkan orang yang mengakses file data .Akan tetapi , menjalankan program komputer adalah mata pelajaran juga .Objek adalah setiap data yang pasif dalam sistem .Objek dapat bervariasi dari database ke file teks .Hal yang penting untuk diingat mengenai bahwa mereka adalah obyek yang pasif dalam sistem .Mereka tidak memanipulasi benda-benda lain

Model akses control

Sekarang bahwa kita memiliki kontrol akses konsep batu pertama ditinjau ulang , kita dapat membahas akses kontrol yang berbeda yakni model model yang utama dengan akses kontrol ( ) dac , akses kontrol (mac) wajib , dan akses kontrol nondiscretionary

Kebebasan akses kontrol

Kebebasan akses kontrol (dac) memberikan kontrol penuh pelajaran bagi mereka, telah diberikan izin untuk berbagi dengan objek lainnya seperti mata pelajaran.Mereka rakyat yang terberdayakan dan mengontrol informasi.Suatu sistem operasi unix dan digunakan untuk jendela dac berkas bidang lainnya: sistem-sistem yang memberikan akses ke file, mereka subyek mereka mulai berubah. Mengubah mereka, atau melihat mereka.

Kontrol akses didasarkan pada hukum

Sistem kontrol akses didasarkan pada hukum yang menggunakan serangkaian peraturan yang telah ditetapkan , pembatasan , dan filter untuk mengakses objek dalam sebuah sistem .Aturan-aturan yang di bentuk jika tahun lalu pernyataan .Contoh dari peralatan kendali akses yang didasarkan pada hukum adalah sebuah firewall proxy yang memungkinkan pengguna untuk menjelajahi internet dengan konten telah ditetapkan sebelumnya hanya berupa jika pengguna yang berkepentingan untuk menjelajah internet dan situs yang ada di daftar disetujui , kemudian memungkinkan akses) .Situs lain yang dilarang dan diberlakukan aturan ini diberlakukan di semua pengguna dibuktikan keasliannya .

Daftar akses kontrol

Daftar akses kontrol (acl) yang digunakan dalam banyak kebijakan keamanan itu. Prosedur. Dan teknologi.Sebuah akses kontrol yang ada dalam daftar adalah daftar; catatan yang menjelaskan subjek masing-masing yang mungkin keberatan yang masuk.Orang yang masuk ke sebuah usaha oleh sebuah benda yang tidak memiliki acl menyamai catatan di akan ditolak

Mengakses sistem pengadaan

Akses kontrol yang tepat sekali model yang telah dipilih dan menyebar , pengadaan akses lifecycle yang harus dikembangkan dan aman .Sementara banyak lembaga untuk menerbitkan mengikuti best practice di akses , tidak banyak proses formal seumur hidup untuk menjamin akses aman disimpan sebagai karyawan dan kontraktor bergerak dalam sebuah organisasi

Akses kontrol dan kerangka protokol

Kedua model desentralisasi sentralistik dan dapat mendukung otentikasi para pengguna sistem ke daerah terpencil .Beberapa protokol dan klasik dapat digunakan untuk mendukung kebutuhan ini , termasuk jari-jari , diameter , tacacs tacacs tahun , pap , dan anak

Jarak

Remote dial-in otentikasi pengguna layanan ( ) jari-jari adalah sebuah sistem protokol otentikasi dari pihak ketiga .Menggunakan jari-jari pengguna datagram (protokol otentikasi (port udp) tahun 1812 dan 1813 (akuntansi) .Jari-jari adalah dianggap sebagai aaa sistem , yang terdiri dari tiga komponen yaitu otentikasi , otorisasi , dan akuntansi .Itu authenticates subjek s otentikasi kepercayaan terhadap sebuah database .Pengguna kewenangan ini dengan memungkinkan pengguna tertentu khusus untuk akses data objects .Data rekening itu untuk setiap sesi dengan menciptakan sebuah entri log untuk setiap jarak koneksi yang dibuat

Diameter

diameternya sekitar jari-jari; pengganti dirancang untuk memberikan lebih, untuk otentikasi otorisasi, (akuntansi) dan aaa kerangka.Memiliki radius memberikan sedikit masalah dengan akuntabilitas dan lentur. Skalabilitas. Bisa diandalkan, dan keamanan.Diameter lebih fleksibel, pemberian bantuan kepada pengguna mobile terpencil, sebagai contoh.

pap and chap

Kata kunci protokol otentikasi (pap) adalah tidak aman: pengguna memasuki sebuah password dan itu dikirim di seluruh network in jelas teks .Saat menerima oleh pap server , hal ini dibuktikan keasliannya dan divalidasi .Mengendus jaringan mei mengungkapkan nilai plaintext password

Akses kelompok kontrol dan membuat jenis

Dalam rangka untuk memahami dengan tepat dan menjalankan kontrol akses , memahami apa keuntungan dan kontrol dapat menambah keamanan penting .Pada bagian ini , setiap jenis kontrol akses yang akan ditentukan atas dasar itu menambah keamanan sistem .

Ada enam jenis akses kontrol:

- pencegahan
- detektif
- perbaikan
- pemulihan
- jera
- kompensasi