# KEAMANAN INFORMASI

## ACCESS CONTROL


**DISUSUN OLEH:**

( BACHTIAR PRAKOSO )

( 1310652051 )

**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2015**

# Access Control

**PENDAHULUAN**

Tujuan dari kontrol akses adalah untuk memungkinkan pengguna yang berwenang mengakses data yang sesuai dan menolak akses ke pengguna yang tidak sah. Kontrol akses melindungi terhadap ancaman seperti akses yang tidak sah, modifikasi yang tidak pantas data, dan hilangnya kerahasiaan. Sebelum kita bisa menjelaskan kontrol akses, kita harus mendefinisikan informasi landasan secu- konsep ritas. Konsep-konsep ini memberikan dasar yang di atasnya 10 domain Tubuh umum Pengetahuan dibangun.Kerahasiaan, integritas, dan ketersediaan Kerahasiaan, integritas, dan Ketersediaan adalah "triad CIA," konsep landasan keamanan informasi. Triad, yang ditunjukkan pada Gambar 1.1, membentuk tiga berkaki keamanan informasi bangku dibangun di atas. Urutan akronim dapat berubah (beberapa lebih "AIC," mungkin untuk menghindari hubungan dengan badan intelijen tertentu), tetapi konsep-konsep yang penting. Buku ini akan menggunakan "CIA" singkatan. **Kerahasiaan** : Kerahasiaan berusaha untuk mencegah pengungkapan yang tidak sah informasi: itu membuat rahasia data. Dengan kata lain, kerahasiaan berusaha untuk mencegah akses yang tidak sah read data. Contoh dari serangan kerahasiaan akan pencurian pribadi diidentifikasi Informasi (PII), seperti informasi kartu kredit.

Integritas berusaha untuk mencegah modifikasi yang tidak sah dari informasi. Dengan kata lain, integritas berusaha untuk mencegah akses tulis tidak sah ke data. Ada dua jenis integritas: integritas data dan integritas sistem. Integritas data berusaha untuk melindungi informasi terhadap modifikasi yang tidak sah; integritas sistem berusaha untuk melindungi sistem, seperti sistem operasi Windows server 2012, dari modifikasi yang tidak sah. Tersedianya

Ketersediaan memastikan bahwa informasi yang tersedia bila diperlukan. Sistem harus dapat digunakan (tersedia) untuk penggunaan bisnis normal. Contoh dari serangan terhadap ketersediaan akan menjadi (DoS) serangan Denial-of-Service, yang berusaha untuk menolak layanan (atauavailabil-ity) dari sistem.KerahasiaanPengungkapan, perubahan, dan perusakan Sebuah vailaIntegritasbility. CIA triad juga dapat dijelaskan oleh kebalikannya: Pengungkapan, Perubahan, dan Destruction (DAD). Pengungkapan adalah pengungkapan yang tidak sah informasi; perubahan adalah modifikasi yang tidak sah dari data, dan kehancuran adalah membuat sistem tidak tersedia. Sementara singkatan CIA kadang-kadang berubah, singkatan DAD adalah ditampilkan dalam urutan itu.Identitas dan otentikasi, otorisasi, dan akuntabilitas Istilah "AAA" sering digunakan, menggambarkan landasan konsep Authentication, Otorisasi, dan Akuntabilitas. Meninggalkan keluar dari AAA singkatan adalah Identifikasi, yang diperlukan sebelum tiga "A" dapat mengikuti.

## Pertahanan-mendalam

Pertahanan-mendalam (juga disebut pertahanan berlapis) berlaku beberapa perlindungan (juga disebut kontrol: tindakan yang diambil untuk mengurangi resiko) untuk melindungi aset.

Setiap keamanan tunggal control mungkin gagal; dengan mengerahkan beberapa kontrol, Anda meningkatkan kerahasiaan,integritas, dan ketersediaan data Anda.

**MODEL ACCESS CONTROL :**Sekarang kita telah meninjau konsep kontrol akses landasan, kita bisa mendiskusikan berbeda model kontrol akses: model utama adalah akses Discretionary Control (DAC), Wajib Access Control (MAC), dan akses nondiscretionary control. Kontrol akses discretionary Discretionary Access Control (DAC) memberikan pelajaran kontrol penuh dari benda-benda yang mereka miliki telah diberi akses ke, termasuk berbagi objek dengan mata pelajaran lain. Subyek diberdayakan dan mengendalikan data mereka. Sistem operasi standar UNIX dan Windows menggunakan DAC untuk sistem berkas: subjek dapat memberikan akses mata pelajaran lain untuk file mereka, mengubah atribut mereka, mengubah mereka, atau menghapusnya. Kontrol akses wajib.

Akses wajib Control (MAC) adalah sistem-ditegakkan kontrol akses berdasarkan subjek clearance dan label objek. Subjek dan objek memiliki izin dan label, masing-masing, seperti rahasia, rahasia, dan rahasia. Sebuah subjek mungkin mengakses objek hanya jika izin subjek sama dengan atau lebih besar dari label objek. Subyek tidak dapat berbagi objek dengan mata pelajaran lain yang tidak memiliki izin yang tepat atau "menulis" objek untuk tingkat klasifikasi yang lebih rendah (seperti sejak rahasia untuk rahasia). Sistem MAC biasanya berfokus pada melestarikan kerahasiaan data. Kontrol akses nondiscretionary
Peran Berbasis Access Control (RBAC) mendefinisikan bagaimana informasi diakses pada sistem berdasarkan peran subjek. Peran A bisa menjadi perawat, administrator cadangan, bantuan teknisi meja, dll Subyek dikelompokkan menjadi peran dan peran masing-masing didefinisikan memiliki izin akses berdasarkan peran, bukan individu. **RBAC** adalah jenis kontrol akses nondiscretionary karena pengguna tidak memiliki kebijaksanaan mengenai kelompok benda mereka diizinkan untuk mengakses dan tidak mampu untuk mentransfer objek untuk mata pelajaran lainnya. Kontrol akses tugas berbasis model kontrol akses nondiscretionary lain, berkaitan dengan RBAC. Kontrol akses tugas berbasis didasarkan pada tugas masing-masing harus tunduk melakukan, seperti menulis resep, memulihkan data dari tape backup, atau membuka tiket help desk. Ia mencoba untuk memecahkan masalah yang sama yang RBAC memecahkan, fokus pada tugas-tugas tertentu, bukan peran. Akses kontrol berbasis aturan Sebuah sistem kontrol akses berbasis aturan menggunakan serangkaian aturan yang ditetapkan, pembatasan, dan filter untuk mengakses objek dalam suatu sistem. Aturan-aturan dalam bentuk "Jika / kemudian" pernyataan. Contoh dari perangkat kontrol akses berbasis aturan adalah proxy firewall yang memungkinkan pengguna untuk berselancar di Web dengan konten yang disetujui yang telah ditetapkan hanya (Jika pengguna berwenang untuk berselancar di Web dan situs pada daftar yang disetujui, kemudian memungkinkan akses). Situs lain dilarang dan aturan ini diberlakukan di seluruh semua dikonfirmasi pengguna. Kontrol akses terpusat Kontrol akses terpusat berkonsentrasi kontrol akses di satu titik logis untuk sistem atau organisasi. Alih-alih menggunakan database kontrol akses lokal, sistem mengotentikasi melalui server otentikasi pihak ketiga. Kontrol akses terpusat dapat digunakan untuk menyediakan Single Sign-On (SSO), di mana subjek dapat mengotentikasi sekali, dan kemudian mengakses beberapa sistem. Kontrol akses terpusat dapat terpusat menyediakan tiga "A" dari kontrol akses: Otentikasi, Otorisasi, dan Akuntabilitas.

Daftar kontrol akses Daftar kontrol akses (ACL) digunakan di seluruh banyak kebijakan keamanan IT, prosedur, dan teknologi. Daftar kontrol akses adalah daftar objek; setiap entri menggambarkan mata pelajaran yang dapat mengakses objek tersebut. Akses upaya subjek untuk obyek yang tidak memiliki entri yang cocok pada ACL akan ditolak. Akses pengadaan siklus hidup Setelah model kontrol akses yang tepat telah dipilih dan digunakan, akses penyediaan siklus hidup harus dijaga dan diamankan. Sementara banyak organisasi ikuti

praktik terbaik untuk mengeluarkan akses, banyak kekurangan proses formal untuk memastikan seumur hidup akses disimpan aman sebagai karyawan dan kontraktor bergerak dalam sebuah organisasi. IBM menjelaskan aturan siklus hidup identitas berikut:

•Password pemeriksaan kepatuhan kebijakan
•Memberitahukan pengguna untuk mengubah password mereka sebelum mereka berakhir
•Mengidentifikasi hidup perubahan siklus seperti rekening yang tidak aktif selama lebih dari 30hariberturut-turut
•Mengidentifikasi akun baru yang belum digunakan selama lebih dari 10 hari setelah penciptaan mereka.

Mengidentifikasi akun yang kandidat untuk dihapus karena mereka telah ditangguhkan selama lebih dari 30hari.
•Ketika kontrak berakhir, mengidentifikasi semua account milik mitra bisnisatau karyawan kontraktor dan mencabut hak akses mereka "Hak pengguna, akses review, dan audit yang
1 Akses agregasi terjadi sebagai pengguna individu memperoleh lebih banyak akses ke banyak sistem. Ini dapat terjadi secara sengaja, sebagai fungsi Single Sign-On (SSO). Hal ini juga dapat terjadi tidak sengaja: pengguna sering mendapatkan hak baru (juga disebut hak akses) karena mereka mengambil peran atau tugas baru. Hal ini dapat mengakibatkan otorisasi merayap: pengguna mendapatkan lebih banyakhak tanpa penumpahan yang lama. Kekuatan hak-hak ini dapat senyawa dari waktu ke waktu, mengalahkan kontrol seperti hak istimewa setidaknya dan pemisahan tugas. Hak pengguna harus secara rutin ditinjau dan diaudit. Proses harus dikembangkan yang mengurangi atau menghilangkan hak tua yang baru diberikan. Protokol kontrol akses dan kerangka kerja Kedua model sentralisasi dan desentralisasi dapat mendukung pengguna jauh otentikasi untuk sistem lokal. Sejumlah protokol dan kerangka kerja dapat digunakan untuk mendukung ini butuhkan, termasuk RADIUS, Diameter, TACACS / TACACSþ, PAP, dan CHAP.
RADIUS
Remote Authentication Dial-In Service Pengguna (RADIUS) protokol adalah pihak ketiga sistem otentikasi. RADIUS menggunakan User Datagram Protocol (UDP) port 1812 (Otentikasi) dan 1813 (akuntansi).RADIUS dianggap sebagai "AAA" sistem, yang terdiri dari tiga komponen: otentikasi, otorisasi, dan akuntansi. Ini mengotentikasi kredensial subjek terhadap database otentikasi. Ini kewenangan pengguna dengan memungkinkan pengguna tertentu ' akses ke objek data tertentu. Hal ini menyumbang setiap sesi data dengan menciptakan log entri untuk setiap koneksi RADIUS dibuat. Diameter Diameter adalah RADIUS 'penerus, dirancang untuk memberikan Authentication ditingkatkan, Otorisasi, dan Akuntansi (AAA) kerangka. RADIUS menyediakan terbatas akuntabilitas dan memiliki masalah dengan fleksibilitas, skalabilitas, kehandalan, dan keamanan.Diameter lebih fleksibel, yang memungkinkan dukungan bagi pengguna jarak jauh ponsel, misalnya. TACACS dan TACACS1 Terminal Access Controller Access Control System (TACACS) adalah terpusat sistem kontrol akses yang mengharuskan pengguna untuk mengirim ID dan statis (reusable) password untuk otentikasi. TACACS menggunakan port UDP 49 (dan mungkin juga menggunakan TCP). Reusable password memiliki kerentanan keamanan: ditingkatkan TACACSþ memberikan yang lebih baik proteksi password dengan memungkinkan otentikasi dua faktor yang kuat. TACACSþ tidak kompatibel dengan TACACS. TACACSþ menggunakan TCP Port 49 untuk otentikasi dengan TACACSþserver.

PAP dan CHAP Password Authentication Protocol (PAP) tidak aman: pengguna memasukkan password dan itu dikirim melalui jaringan "ACCESS CONTROL KATEGORI defensif DAN JENIS Untuk memahami dan

tepat menerapkan kontrol akses, pemahaman apa manfaat setiap kontrol dapat menambah keamanan sangat penting. Pada bagian ini, setiap jenis kontrol akses akan ditentukan atas dasar bagaimana menambah keamanan sistem. Ada enam jenis kontrol akses:

- Pencegah
- Detektif
- Perbaikan
- Pemulihan
- Pencegah
- Kompensasi.

**FAKTA CEPAT** Jenis kontrol akses ini dapat jatuh ke dalam salah satu dari tiga kategori: administrasi, teknis, atau fisik.

1. Administrasi (juga disebut directive) kontrol dilaksanakan dengan menciptakan dan mengikuti kebijakan organisasi, prosedur, atau peraturan. Pelatihan pengguna dan kesadaran juga jatuh ke dalam kategoriini.
2. kontrol Teknis diimplementasikan menggunakan perangkat lunak, perangkat keras, atau firmware yang membatasi Akses logis pada sistem teknologi informasi. Contohnya termasuk firewall, router, dan enkripsi.
3. kontrol fisik diimplementasikan dengan perangkat fisik, seperti kunci, pagar, gerbang, dan penjaga keamanan. Pencegah Kontrol preventif mencegah tindakan dari terjadi. Ini berlaku pembatasan untuk apa Potensi pengguna, baik resmi atau tidak sah, dapat dilakukan. Contoh Domain 1: Access Control ,Kontrol pencegahan administrasi adalah skrining obat pra kerja. Hal ini dirancang untuk mencegah organisasi dari mempekerjakan seorang karyawan yang menggunakan obat-obatan terlarang.DetektifKontrol detektif adalah kontrol yang siaga selama atau setelah serangan yang berhasil. Intrusisistem deteksi sinyal setelah serangan sukses, kamera televisi sirkuit tertutup(CCTV) yang penjaga waspada terhadap penyusup, dan sistem bangunan alarm yang dipicuoleh penyusup merupakan contoh dari kontrol detektif. PerbaikanKontrol korektif bekerja dengan "memperbaiki" sistem atau proses rusak. The korektif kontrol akses biasanya bekerja bergandengan tangan dengan kontrol akses detektif. Anti Virus perangkat lunak memiliki kedua komponen. Pertama, perangkat lunak antivirus menjalankan scan dan kegunaan file definisi untuk mendeteksi apakah ada software yang cocok daftar virus tersebut. Jika mendeteksi virus, kontrol korektif mengambil alih, menempatkan perangkat lunak yang mencurigakan dikarantina, atau menghapusnya dari sistem.Pemulihan Setelah insiden keamanan telah terjadi, kontrol pemulihan mungkin perlu diambil dalam memesan untuk mengembalikan fungsi dari sistem dan organisasi. Pemulihan berarti bahwa sistem harus pulih: diinstal ulang dari OS Media atau gambar, data dikembalikan dari backup, dll

Pencegah Kontrol jera mencegah pengguna dari melakukan tindakan pada sistem. Contohnya termasuk "Waspadalah terhadap anjing" tanda: pencuri menghadapi dua bangunan, satu dengan anjing penjaga dan satu tanpa, lebih mungkin untuk menyerang bangunan tanpa anjing penjaga. Denda besar untuk ngebut adalah pencegah untuk driver untuk tidak mempercepat. Sebuah kebijakan sanksi yang membuat pengguna memahami bahwa

mereka akan dipecat jika mereka tertangkap situs Web berselancar terlarang atau ilegal adalah pencegahan. Kompensasi Sebuah kontrol kompensasi adalah kontrol keamanan tambahan dimasukkan ke dalam tempat untuk mengkompensasi kelemahan dalam kontrol lainnya.

**METODEAUTHENTIKASI**

Sebuah konsep kunci untuk melaksanakan jenis kontrol akses mengendalikan tepat otentikasi subyek dalam sistem IT. Subjek A pertama mengidentifikasi dirinya atau dirinya; Identifikasi ini tidak bisa dipercaya. Subjek kemudian mengotentikasi dengan menyediakan jaminan bahwa identitas diklaim berlaku. Satu set credential adalah istilah yang digunakan untuk kombinasi keduanya identifikasi dan otentikasi pengguna. Access Control Sandi hash dan password cracking Dalam kebanyakan kasus, password teks yang jelas tidak disimpan dalam sistem IT; hanya output hash dari mereka password yang disimpan. Hashing adalah enkripsi satu arah menggunakan algoritma dan tidak ada tombol. Ketika pengguna mencoba untuk login, password mereka ketik adalahhash, dan hash yang dibandingkan terhadap hash yang disimpan pada sistem. Hash Fungsi tidak dapat dibalik: tidak mungkin untuk membalikkan algoritma dan menghasilkan password dari hash. Sementara hash tidak dapat terbalik, penyerang dapat menjalankan algoritma hash maju berkali-kali, memilih berbagai password mungkin dan membandingkan output untuk hash yang diinginkan, berharap menemukan kecocokan (dan untuk mendapatkan yang asli password). Ini disebut password cracking. Serangan kamus Sebuah serangan kamus menggunakan daftar kata: daftar standar dari kata-kata, dan kemudian berjalan masing-masing kata melalui algoritma hash. Jika perangkat lunak retak sesuai dengan output dari Serangan keluaran kamus hash password, penyerang akan dapat mengidentifikasi password asli.Serangan Hybrid Sebuah serangan hybrid menambahkan, prepends, atau perubahan karakter dalam kata-kata dari kamus sebelum hashing, untuk mencoba celah tercepat password yang kompleks. Sebagai contoh, sebuah Penyerang mungkin memiliki kamus administrator sistem potensial password tetapi juga menggantikan setiap huruf "o" dengan angka "0"Serangan brute-force Serangan brute-force mengambil lebih banyak waktu tetapi lebih efektif. Penyerang menghitung output hash untuk setiap password mungkin. Hanya beberapa tahun yang lalu, kecepatan komputer dasar masih cukup lambat untuk membuat tugas yang menakutkan. Namun, dengan kemajuan dalam Kecepatan CPU dan komputasi paralel, waktu yang diperlukan untuk brute-force password yang kompleks telah jauh berkurang. Tabel pelangi Sebuah meja pelangi adalah kompilasi precomputed dari plainteks dan cipherteks yang cocok (Biasanya password dan hash cocok mereka). Tabel pelangi sangat mempercepat banyak jenis password cracking serangan, sering mengambil menit untuk memecahkan mana lain metode (seperti kamus, hibrida, dan password brute force retak upaya) mungkin memakan waktu lebih lama. Meskipun tabel pelangi bertindak sebagai database, mereka lebih kompleks di bawah tenda, mengandalkan waktu / memori trade-off untuk mewakili dan memulihkan password dan hash. Kebanyakan tabel pelangi dapat memecahkan sebagian besar, tapi tidak semua, mungkin hash.GaramSebuah garam memungkinkan satu password untuk hash beberapa cara. Beberapa sistem (seperti yang modern Sistem UNIX / Linux) menggabungkan garam dengan password

sebelum hashing: "The desainer dari sistem operasi UNIX meningkat pada metode ini dengan menggunakan random. Nilai disebut 'garam. "Nilai garam memastikan bahwa password yang sama akan mengenkripsi berbeda bila digunakan oleh pengguna yang berbeda. Metode ini menawarkan keuntungan yang penyerang harus mengenkripsi kata yang sama beberapa kali (sekali untuk setiap garam atau pengguna) untuk mount-sandi menebak sukses serangan. "
4 Hal ini membuat tabel pelangi jauh lebih efektif (jika tidak benar-benar tidak efektif) untuk sistem yang menggunakan garam. Alih-alih menyusun meja satu pelangi untuk sistem yang tidak tidak menggunakan garam (seperti Microsoft LAN hash Manager), ribuan, jutaan, miliaran, atau tabel pelangi lebih akan diperlukan untuk sistem yang menggunakan garam, tergantung pada panjang garam. Ketik 2 otentikasi: sesuatu yang harus Tipe 2 otentikasi (sesuatu yang harus) mengharuskan pengguna memiliki sesuatu, seperti token, yang membuktikan mereka adalah pengguna dikonfirmasi. Token adalah sebuah objek yang membantu membuktikan klaim identitas. Token dinamis sinkron Token dinamis sinkron menggunakan waktu atau counter untuk menyinkronkan tanda ditampilkan kode dengan kode diharapkan oleh server otentikasi: kode disinkronisasi. Token dinamis sinkron berbasis waktu menampilkan kode tanda dinamis yang sering berubah, seperti setiap 60 detik. Kode dinamis hanya baik selama jendela. Server otentikasi tahu nomor urut masing-masing berwenang tanda, pengguna hal ini terkait dengan, dan waktu. Hal ini dapat memprediksi kode dinamis pada setiap token menggunakan tiga potongan informasi. Token dinamis sinkron berbasis kontra menggunakan counter sederhana: otentikasi Server mengharapkan kode token 1, dan token pengguna menampilkan cara yang sama. Setelah digunakan, token menampilkan token kedua, dan server juga mengharapkan tanda # 2. Asynchronous tanda dinamis Asynchronous token dinamis tidak disinkronkan dengan server pusat. Paling Berbagai umum adalah token tantangan-respon. Tantangan-respon otentikasi tanda sistem menghasilkan tantangan atau masukan untuk perangkat tanda. Kemudian pengguna secara manual memasukkan informasi ke dalam perangkat bersama dengan PIN mereka, dan perangkat menghasilkan output. Output ini kemudian dikirim ke sistem. Ketik 3 otentikasi: sesuatu yang Anda Tipe 3 otentikasi (sesuatu yang Anda) adalah biometrik, yang menggunakan karakteristik fisik sebagai sarana identifikasi atau otentikasi. Biometrics dapat digunakan untuk membentuk identitas atau untuk otentikasi (membuktikan klaim identitas). Sebagai contoh, sebuah Bandara sistem pengenalan wajah dapat digunakan untuk menentukan identitas suatu diketahui teroris, dan pemindai sidik jari dapat digunakan untuk otentikasi identitas subjek (Yang membuat klaim identitas dan kemudian gesekan atau jarinya untuk membuktikannya).

Access ControlBiometrik pendaftaran dan throughputPendaftaran menjelaskan proses pendaftaran dengan sistem biometrik: menciptakan account untuk pertama kalinya. Pengguna biasanya memberikan nama mereka (identitas), password atau PIN, dan kemudian memberikan informasi biometrik, seperti sidik jari pada menggesekkan pembaca sidik jari atau setelah sebuah foto yang diambil dari iris mereka. Pendaftaran adalah sekali pakai yang proses yang harus mengambil 2 menit atau kurang. Throughput yang menjelaskan proses otentikasi ke sistem biometrik. Ini adalah juga disebut waktu respon sistem biometrik. Sebuah throughput yang khas adalah 6-10 detik. Akurasi sistem biometrik Keakuratan sistem biometrik harus dipertimbangkan sebelum menerapkan biometrik program pengendalian. Tiga metrik yang digunakan untuk menilai akurasi biometrik: yang Salah Tolak Rate (FRR), yang Salah Terima Rate (FAR), dan Crossover Error Rate

(CER).Salah tingkat menolak Penolakan palsu terjadi ketika subjek yang berwenang ditolak oleh sistem biometrik Tanpa otoritas. Penolakan palsu juga disebut Tipe I kesalahan. Penolakan palsu menyebabkan frustrasi dari pengguna yang berwenang, pengurangan pekerjaan karena kondisi akses yang buruk, dan pengeluaran sumber daya untuk memvalidasi ulang pengguna yang berwenang. Salah menerima tingkat Sebuah penerimaan palsu terjadi ketika subjek tidak sah diterima sebagai valid. Jika kontrol biometrik organisasi memproduksi banyak penolakan palsu, kontrol secara keseluruhan mungkin harus menurunkan akurasi sistem dengan mengurangi jumlah data yang dikumpulkan ketika otentikasi subyek. Ketika titik data diturunkan, organisasi risiko kenaikan tingkat penerimaan palsu. Organisasi risiko pengguna mendapatkan akses tidak sah. Jenis kesalahan juga disebut kesalahan Tipe II. Rate menggambarkan akurasi keseluruhan biometrik sistem. bagai sensitivitas sistem biometrik meningkat, FRRS akan naik dan Fars akan drop. Sebaliknya, sebagai sensitivitas diturunkan, FRRS akan turun dan Fars akan naik. Gambar 1.2 menunjukkan grafik yang menggambarkan FAR versus FRR. CER adalah persimpangan kedua garis dari grafik seperti yang ditunjukkan pada Gambar 1.2, berdasarkan ISACA Biometrik Audit Panduan, G36.Jenis kontrol biometrik. Ada sejumlah kontrol biometrik yang digunakan saat ini. Berikut ini adalah implementasi utama dan pro khusus mereka dan kontra terkait dengan mengakses kontrol keamanan. Sidik jari Sidik jari adalah yang paling banyak digunakan kontrol biometrik yang tersedia saat ini. Smartcard dapat membawa informasi sidik jari. Banyak gedung perkantoran Pemerintah AS mengandalkan otentikasi sidik jari untuk akses fisik ke fasilitas. Contohnya termasuk cerdas keyboard, yang mengharuskan pengguna untuk menyajikan sidik jari untuk membuka komputer screen saver. Data yang digunakan untuk menyimpan sidik jari setiap orang harus dari ukuran yang cukup kecil yang akan digunakan untuk otentikasi. Data ini adalah representasi matematis dari sidik jari hal-hal kecil, rincian spesifik dari pegunungan gesekan jari, yang meliputi uliran, pegunungan, bifurkasi, dan lain-lain. Gambar 1.3 menunjukkan hal-hal kecil jenis (dari kiri) bifurkasi, ridge ending, inti, dan delta.Pemindaian retinaFARFRR Kesalahaniris scan.

**Scan iris** adalah kontrol biometrik pasif. Sebuah kamera mengambil gambar dari iris (yang berwarna porsi mata) dan kemudian membandingkan foto dalam database otentikasi. Ini juga bekerja melalui lensa kontak dan kacamata. Setiap orang dua iris adalah iris unik, bahkan kembar '. Manfaat iris scan termasuk akurasi tinggi, scan- pasif ning (yang dapat dicapai tanpa sepengetahuan subyek), dan tidak ada pertukaran cairan tubuh. geometri tangan Di tangan geometri kontrol biometrik, pengukuran diambil dari titik-titik tertentu pada tangan subjek: "Perangkat menggunakan konsep yang sederhana untuk mengukur dan merekam panjang, lebar, ketebalan, dan luas permukaan tangan individu sementara dipandupadapiring."

Perangkat geometri tangan yang cukup sederhana dan dapat menyimpan informasi dalam waktu sebagai 9 byte.Dinamika Keyboard Dinamika Keyboard mengacu pada seberapa keras seseorang menekan setiap tombol dan irama oleh yang tombol yang ditekan. Anehnya, jenis kontrol akses murah untuk menerapkan dan bisa efektif. Sebagai orang belajar bagaimana untuk mengetik dan menggunakan komputer keyboard, mereka mengembangkan kebiasaan tertentu yang sulit untuk meniru, meskipun bukan tidak mungkin. Signature dinamis Tanda tangan dinamis mengukur proses dimana seseorang sign namanya. Proses ini mirip dengan dinamika keyboard, kecuali bahwa metode ini mengukur tulisan tangan dari subyek sementara mereka menandatangani nama mereka. Mengukur waktu,

tekanan,loop di tanda tangan, dan awal dan akhir poin semua bantuan untuk memastikan pengguna otentik.

Access Control TECHNOLOGIES ACCESS CONTROL Ada beberapa teknologi yang digunakan untuk pelaksanaan kontrol akses. Karena setiap teknologi disajikan, penting untuk mengidentifikasi apa yang unik tentang masing-masing solusi teknis. Single sign-on Sign-On tunggal (SSO) memungkinkan beberapa sistem untuk menggunakan server otentikasi pusat (AS). Hal ini memungkinkan pengguna untuk mengotentikasi sekali dan kemudian mengakses beberapa, sistem yang berbeda.
Hal ini juga memungkinkan administrator keamanan untuk menambah, mengubah, atau mencabut hak pengguna pada satu sistem pusat. Kerugian utama untuk SSO itu memungkinkan penyerang untuk mendapatkan akses ke beberapa sumber setelah mengorbankan salah satu metode otentikasi, seperti password. SSO harus selalu digunakan dengan otentikasi multifaktor untuk alasan ini.
Manajemen identitas federasi Federated Identity Management (FIdM) berlaku Single Sign-On pada lebih luas skala: mulai dari lintas organisasi untuk skala Internet. Kadang-kadang hanya disebut Identity Management (IDM). FIdM dapat menggunakan OpenID atau SAML (Security Association Markup Language).Menurut EDUCAUSE, "manajemen Identitas mengacu pada kebijakan, proses, dan teknologi yang membangun identitas pengguna dan menegakkan aturan tentang akses kesumberdaya.

**KERBEROS**

Kerberos adalah layanan otentikasi pihak ketiga yang dapat digunakan untuk mendukung Single Sign-On. Kerberos (http://www.kerberos.org/) adalah nama yang threeheaded anjing yang dijaga pintu masuk ke Hades (juga disebut Cerberus) di Yunani mitologi. Kerberos menggunakan enkripsi simetris dan memberikan saling otentikasi kedua klien dan server. Ini melindungi terhadap jaringan mengendus dan ulangan serangan. Sekarang versi Kerberos adalah versi 5, dijelaskan oleh RFC 4120 (http://www.ietf.org/ RFC / rfc4120.txt).FAKTA CEPAT Kerberos memiliki komponen-komponen berikut:

- Principal: Client (user) atau layanan
- Realm: Sebuah jaringan Kerberos logis
- Tiket: Data yang mengotentikasi identitas kepala sekolah
- Kredensial: A tiket dan kunci layanan
- KDC: Key Distribution Center, yang mengotentikasi kepala sekolah
- TGS: Layanan Tiket-Pemberian
- TGT: Tiket-Pemberian Tiket
- C / S: Client / Server, tentang komunikasi antara dua

SESAME

SESAME adalah Sistem Eropa Aman untuk Aplikasi di lingkungan multivendor, sistem single sign-on yang mendukung lingkungan yang heterogen.
SESAME dapat dianggap sebagai sekuel dari jenis untuk Kerberos, "SESAME menambah Kerberos: heterogenitas, fitur kontrol akses yang canggih, skalabilitas sistem kunci publik, pengelolaan yang lebih baik, audit dan delegasi. "
Dari mereka perbaikan, penambahan kunci publik (asimetris) enkripsi adalah yang paling menarik. Ini alamat salah satu kelemahan terbesar dalam Kerberos: plaintext

penyimpanan kunci simetris.
SESAME menggunakan Privilege Atribut Sertifikat (PAC) di tempat Kerberos '
tiket. Informasi lebih lanjut tentang SESAME tersedia di https: //www.cosic.esat.
kuleuven.be/sesame/.
MENILAI ACCESS CONTROL
Sejumlah proses yang ada untuk menilai efektivitas pengendalian akses. Tes dengan
lingkup sempit meliputi tes penetrasi, penilaian kerentanan, dan keamanan
audit. Sebuah penilaian keamanan adalah tes yang lebih luas yang mungkin termasuk tes sempit, seperti sebagai tes penetrasi, sebagai subbagian.
Pengujian penetrasi
Sebuah tester penetrasi adalah hacker topi putih yang menerima otorisasi untuk mencoba
masuk ke perimeter fisik atau elektronik organisasi (dan kadang-kadang keduanya).
Tes penetrasi (disebut "tes pena" untuk pendek) dirancang untuk menentukan apakah
9 18 BAB 1 Domain 1: Access Control
black hat hacker bisa melakukan hal yang sama. Mereka adalah sempit, tetapi sering berguna, tes, terutama
jika tester penetrasi berhasil.
Tes penetrasi dapat mencakup tes berikut:

- Jaringan (Internet)
- Jaringan (internal atau DMZ)
- Panggilan perang
- Wireless
- Fisik (upaya untuk mendapatkan masuk ke pusat atau ruang)
- Wireless

Serangan jaringan dapat memanfaatkan serangan client-side, serangan server-side, atau aplikasi Web serangan. Lihat Bab 6, "Domain 6: Arsitektur Keamanan dan Desain" untuk
informasi lebih lanjut tentang serangan ini. Panggilan perang menggunakan modem dial serangkaian telepon
nomor, mencari nada pembawa modem penjawab (tester penetrasi kemudian
mencoba untuk mengakses sistem penjawab); Nama ini berasal dari tahun 1983 film
WarGames.
Rekayasa sosial menggunakan pikiran manusia untuk melewati kontrol keamanan. Social engineering dapat digunakan dalam kombinasi dengan berbagai jenis serangan, terutama clientside
serangan atau tes fisik. Contoh dari serangan rekayasa sosial dikombinasikan
dengan serangan sisi klien e-mail malware dengan baris subjek "Kategori 5 Badai
adalah untuk memukul Florida! "

Sebuah tes nol pengetahuan adalah "buta"; tester penetrasi dimulai tanpa eksternal atau terpercaya informasi dan memulai serangan dengan informasi publik saja. Sebuah uji penuh pengetahuan menyediakan informasi internal untuk tester penetrasi, termasuk diagram jaringan, kebijakan dan prosedur, dan kadang-kadang laporan dari sebelumnya penguji penetrasi. Tes parsial pengetahuan dalam antara nol dan pengetahuan penuh: tester penetrasi menerima beberapa informasi yang terpercaya terbatas.

Pengujian kerentanan

Kerentanan pemindaian (juga disebut pengujian kerentanan) scan jaringan atau sistem untuk daftar kerentanan yang telah ditetapkan seperti sistem misconfiguration, usang perangkat lunak, atau kurangnya patch. Sebuah alat pengujian kerentanan seperti Nessus (http: // www.nessus.org) atau OpenVAS (http://www.openvas.org) dapat digunakan untuk mengidentifikasi kerentanan.

Audit keamanan

Sebuah audit keamanan adalah tes terhadap standar diterbitkan. Organisasi dapat diaudit untuk PCI-DSS (Industri Kartu Pembayaran Standar Keamanan Data) kepatuhan, misalnya. PCI-DSS mencakup banyak kontrol yang diperlukan, seperti firewall, kontrol akses tertentu model, dan enkripsi nirkabel. Seorang auditor kemudian memverifikasi situs atau organisasi memenuhi standar diterbitkan.

## PENILAIAN KEAMANAN

Penilaian keamanan adalah pendekatan holistik untuk menilai efektivitas akses control. Alih-alih mencari sempit di tes penetrasi atau penilaian kerentanan, penilaian keamanan memiliki lingkup yang lebih luas. IKHTISAR TUJUAN UJIAN Jika orang berpikir tentang analogi benteng untuk keamanan, kontrol akses akan parit dan dinding benteng. Kontrol akses memastikan bahwa mekanisme perlindungan perbatasan, di kedua sudut pandang logis dan fisik, dijamin. Tujuan dari kontrol akses adalah untuk memungkinkan pengguna berwenang akses ke data yang sesuai dan menolak akses ke users- tidak sah ini juga dikenal sebagai membatasi akses subyek ke obyek. Meskipun tugas ini adalah kompleks dan terlibat satu, adalah mungkin untuk menerapkan program kontrol akses yang kuat tanpa membebani pengguna yang bergantung pada akses ke sistem. Melindungi triad CIA adalah aspek kunci lain untuk menerapkan kontrol akses. Menjaga kerahasiaan, integritas, dan ketersediaan adalah sangat penting. Menjaga keamanan selama CIA dari sistem berarti memberlakukan prosedur khusus untuk akses data. Prosedur ini akan berubah tergantung pada fungsi yang pengguna membutuhkan dan sensitivitas data yang tersimpan pada sistem. TOP LIMA PERTANYAAN terberat Pertanyaan 1 dan 2 didasarkan pada skenario ini: Perusahaan Anda telah menyewa sebuah perusahaan pihak ketiga untuk melakukan tes penetrasi. CIO Anda ingin tahu apakah eksploitasi sistem bisnis penting adalah mungkin. Dua persyaratan perusahaan memiliki adalah:

•Tes akan dilakukan pada, jaringan bisnis fungsional hidup. Inijaringan harus fungsional agar bisnis berjalan dan tidak dapat ditutup,bahkan untuk evaluasi.

•Perusahaan ngin yang paling mendalam tes mungkin.