I. PRINSIP ACCESS CONTROL

Kontrol akses adalah komponen fundamental dari keamanan komputer, mencakup prinsip dan teknik yang bertujuan untuk mengatur dan mengelola akses ke sumber daya sesuai dengan kebijakan keamanan. Dua definisi kunci, seperti yang disediakan oleh NIST IR 7298 dan RFC 4949, memberikan pemahaman yang komprehensif tentang kontrol akses: NIST IR 7298: Kontrol akses didefinisikan sebagai proses memberikan atau menolak permintaan khusus untuk: Memperoleh dan menggunakan informasi serta layanan pemrosesan informasi terkait. Masuk ke fasilitas fisik tertentu. Definisi ini menekankan pengendalian akses baik ke informasi maupun fasilitas fisik, menekankan pentingnya melindungi data dan infrastruktur.

RFC 4949: Kontrol akses didefinisikan sebagai proses di mana penggunaan sumber daya sistem diatur sesuai dengan kebijakan keamanan dan hanya diizinkan oleh entitas yang diotorisasi (pengguna, program, proses, atau sistem lain) sesuai dengan kebijakan tersebut. Definisi ini memberikan pandangan yang lebih luas tentang kontrol akses dengan menekankan perannya dalam mengatur penggunaan sumber daya sistem berdasarkan kebijakan keamanan yang telah ditetapkan. Ini menegaskan bahwa akses hanya boleh diberikan kepada entitas yang diotorisasi sesuai dengan kebijakan yang ditetapkan.

Tujuan utama keamanan komputer adalah sebagai berikut:

1. Mencegah pengguna yang tidak diotorisasi mendapatkan akses ke sumber daya.
2. Mencegah pengguna yang sah mengakses sumber daya dengan cara yang tidak diotorisasi.
3. Memungkinkan pengguna yang sah mengakses sumber daya dengan cara yang diotorisasi.

Prinsip kontrol akses mencakup konsep-konsep kunci berikut:

1. Kebijakan Keamanan: Kontrol akses mengimplementasikan kebijakan keamanan yang mendefinisikan siapa atau apa (misalnya, proses) yang

diizinkan mengakses sumber daya sistem tertentu dan jenis akses yang diizinkan dalam setiap kasus.

2. Regulasi Akses: Kontrol akses mengatur akses ke sumber daya berdasarkan kebijakan keamanan yang telah ditetapkan. Ini menguatkan pembatasan dan izin untuk memastikan hanya entitas yang diotorisasi dapat mengakses sumber daya yang mereka butuhkan.

Dalam keamanan komputer, kontrol akses sangat penting untuk melindungi informasi sensitif, melindungi infrastruktur kritis, dan mempertahankan kerahasiaan, integritas, dan ketersediaan sumber daya. Ini merupakan dasar bagi bidang layanan keamanan yang lebih luas dalam sistem komputer, dan diimplementasikan melalui berbagai teknik dan mekanisme. Selain itu, manajemen kontrol akses melibatkan aspek seperti identitas, kredensial, dan atribut, yang membantu menentukan dan menegakkan izin akses, dan kerangka kerja kepercayaan diperkenalkan untuk meningkatkan postur keamanan sistem atau jaringan.

Konteks yang lebih luas dari kontrol akses, seperti yang digambarkan dalam Gambar 4.1, mencakup berbagai entitas dan fungsi yang sangat penting dalam kontrol akses yang efektif dalam konteks keamanan komputer. Entitas dan fungsi ini adalah:

- Autentikasi: Autentikasi melibatkan verifikasi kredensial pengguna atau entitas sistem lainnya untuk memastikan keabsahan mereka. Ini adalah proses untuk memastikan bahwa entitas yang mencoba mengakses sistem atau sumber daya adalah benar-benar mereka yang mereka klaim. Mekanisme autentikasi dapat mencakup pemeriksaan kata sandi, biometrik, kartu pintar, atau autentikasi multi-faktor untuk memverifikasi identitas pengguna.
- Otorisasi: Otorisasi adalah proses pemberian hak atau izin tertentu kepada entitas sistem, memungkinkan mereka untuk mengakses sumber daya sistem tertentu. Ini menentukan siapa yang dipercayai untuk mengakses sumber daya tertentu untuk tujuan tertentu. Mekanisme

otorisasi memastikan bahwa pengguna atau proses memiliki izin yang diperlukan untuk melakukan tindakan tertentu dalam sistem.

- Audit: Audit melibatkan melakukan tinjauan dan pemeriksaan independen atas catatan dan aktivitas sistem. Tujuan utamanya adalah untuk:
- Menguji kecukupan kontrol sistem. Memastikan kepatuhan terhadap kebijakan dan prosedur operasional yang telah ditetapkan
- Mendeteksi pelanggaran keamanan. Merekomendasikan perubahan dalam kontrol, kebijakan, dan prosedur berdasarkan temuan.

Mekanisme kontrol akses berperan sebagai perantara antara pengguna (atau proses yang beroperasi atas nama pengguna) dan berbagai sumber daya sistem, yang dapat mencakup aplikasi, sistem operasi, firewall, router, file, dan basis data. Untuk mengaktifkan akses, langkah-langkah berikut biasanya dilakukan:

- Autentikasi: Sistem mengautentikasi entitas (pengguna atau proses) yang mencari akses. Langkah ini mengonfirmasi identitas entitas dan memastikan bahwa mereka diotorisasi untuk mengakses sistem.
- Otorisasi: Setelah autentikasi berhasil, sistem melakukan otorisasi, menentukan tindakan atau sumber daya tertentu yang entitas yang telah diotentikasi diizinkan mengakses. Proses ini menerapkan hak akses dan izin berdasarkan kebijakan dan peraturan yang telah ditetapkan.

Tujuan keseluruhan dari konteks kontrol akses yang lebih luas ini adalah untuk menjaga keamanan sistem dengan memastikan bahwa hanya pengguna atau entitas yang diotorisasi yang dapat mengakses sumber daya, dan bahwa akses mereka terbatas pada apa yang diperlukan untuk tugas yang sah. Audit yang teratur membantu memastikan bahwa kontrol keamanan efektif, kebijakan diikuti, dan insiden keamanan atau pelanggaran segera terdeteksi dan ditangani.

Dalam konteks yang telah Anda deskripsikan, proses kontrol akses melibatkan beberapa langkah dan entitas untuk menentukan dan mengelola

akses ke sumber daya sistem. Berikut adalah poin-poin kunci dalam kutipan tersebut:

- Autentikasi Pengguna: Sistem pertama-tama mengautentikasi pengguna atau entitas yang mencari akses. Autentikasi memverifikasi identitas pengguna dan memastikan bahwa mereka diizinkan untuk mengakses sistem dalam kapasitas apa pun.
- Fungsi Kontrol Akses: Fungsi ini bertanggung jawab untuk menentukan apakah akses tertentu yang diminta oleh pengguna diizinkan. Fungsi kontrol akses berkonsultasi dengan basis data otorisasi yang dikelola oleh seorang administrator keamanan untuk membuat keputusan ini. Basis data otorisasi menentukan jenis akses ke berbagai sumber daya yang diizinkan untuk setiap pengguna.
- Audit: Fungsi audit memantau dan mencatat akses pengguna ke sumber daya sistem. Ini sangat penting untuk tujuan keamanan dan kepatuhan, karena melacak siapa yang mengakses sumber daya apa dan kapan.

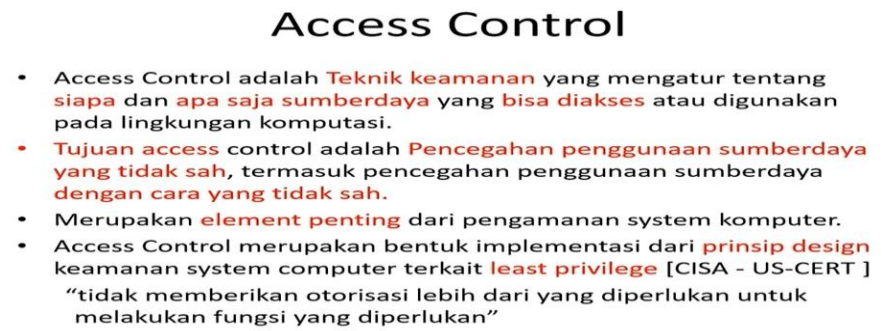
Dalam model yang disederhanakan seperti yang digambarkan dalam Gambar 4.1, fungsi kontrol akses disajikan sebagai modul logis tunggal. Namun, dalam praktiknya, beberapa komponen dapat bekerja secara kolaboratif untuk mengelola kontrol akses. Ini termasuk komponen kontrol akses asli dari sistem operasi, yang ada dalam semua sistem operasi dalam berbagai tingkat. Selain itu, paket keamanan tambahan dapat meningkatkan kemampuan kontrol akses asli dari sistem operasi, dan aplikasi atau utilitas khusus, seperti sistem manajemen basis data, mungkin memiliki fungsi kontrol akses mereka sendiri. Perangkat eksternal seperti firewall juga dapat menyediakan layanan kontrol akses.

Kebijakan kontrol akses mendikte jenis akses yang diizinkan, dalam keadaan apa, dan oleh siapa. Kutipan tersebut menjelaskan beberapa kategori kebijakan kontrol akses: Kontrol Akses Diskresioner (DAC): DAC mengontrol akses berdasarkan identitas pemohon dan aturan akses (otorisasi) yang menentukan apa yang diperbolehkan atau tidak diperbolehkan pemohon lakukan. Ini disebut "diskresioner" karena entitas mungkin memiliki hak

akses yang memungkinkannya, atas inisiatifnya sendiri, untuk memungkinkan entitas lain mengakses sumber daya tertentu. Kontrol Akses Wajib (MAC): MAC mengontrol akses dengan membandingkan label keamanan yang menunjukkan sensitivitas atau pentingnya sumber daya sistem dengan izin keamanan yang menunjukkan entitas sistem yang memenuhi syarat untuk mengakses sumber daya tertentu. Ini disebut "wajib" karena entitas dengan izin mungkin tidak, atas inisiatifnya sendiri, memungkinkan entitas lain mengakses sumber daya tersebut.

- Kontrol Akses Berbasis Peran (RBAC): RBAC mengontrol akses berdasarkan peran yang dimiliki pengguna dalam sistem dan aturan yang menentukan akses apa yang diizinkan untuk pengguna dalam peran tersebut.
- Kontrol Akses Berbasis Atribut (ABAC): ABAC mengontrol akses berdasarkan atribut pengguna, sumber daya yang akan diakses, dan kondisi lingkungan saat ini.

Keempat kebijakan kontrol akses ini tidak bersifat eksklusif, dan sistem dapat menggunakan satu atau lebih dari mereka secara bersamaan untuk mengelola berbagai jenis sumber daya sistem berdasarkan persyaratan khusus dan kebutuhan keamanan.



II. SUBJEK, OBJEK DAN HAK AKSES

Elemen-elemen dasar dari kontrol akses adalah subjek, objek, dan hak akses. Mari kita bahas konsep-konsep ini:

Subjek: Sebuah subjek adalah entitas yang mampu mengakses objek. Dalam banyak kasus, subjek setara dengan proses. Pengguna atau aplikasi apa pun mendapatkan akses ke objek melalui proses yang mewakili pengguna atau aplikasi tersebut. Proses tersebut mengambil atribut dari pengguna, termasuk hak akses. Biasanya, subjek bertanggung jawab atas tindakan yang mereka inisiasi, dan catatan audit dapat digunakan untuk mencatat asosiasi subjek dengan tindakan yang relevan dengan keamanan pada objek. Sistem kontrol akses biasanya mengklasifikasikan subjek menjadi tiga kelas, masing-masing dengan hak akses yang berbeda:

- Pemilik (Owner): Ini mungkin pencipta sumber daya, seperti file. Untuk sumber daya sistem, kepemilikan dapat dimiliki oleh seorang administrator sistem. Untuk sumber daya proyek, seorang administrator proyek atau pemimpin proyek dapat diberikan kepemilikan.
- Grup (Group): Selain hak yang diberikan kepada pemilik, sekelompok pengguna yang diberi nama juga dapat diberikan hak akses. Keanggotaan dalam grup tersebut sudah cukup untuk menggunakan hak akses ini. Pengguna dapat menjadi anggota beberapa grup dalam sebagian besar skema.
- Dunia (World): Hak akses paling sedikit diberikan kepada pengguna yang dapat mengakses sistem tetapi tidak termasuk dalam kategori pemilik dan grup untuk sumber daya tersebut.
- Objek: Sebuah objek adalah sumber daya yang diatur aksesnya. Biasanya, objek digunakan untuk menyimpan atau menerima informasi. Contoh-contohnya termasuk catatan, blok, file, direktori, kotak surat, pesan, dan program. Beberapa sistem kontrol akses juga dapat mencakup unit yang lebih kecil seperti bit, byte, atau bahkan komponen perangkat keras seperti prosesor, port komunikasi, dan node jaringan. Pemilihan dan jenis objek yang akan dilindungi oleh sistem kontrol akses tergantung pada lingkungan tertentu dan pertimbangan antara keamanan dan kompleksitas, beban pemrosesan, dan kemudahan penggunaan.

- Hak Akses: Hak akses menggambarkan cara seorang subjek dapat mengakses objek. Hak akses ini mendefinisikan tindakan apa yang diizinkan pada objek. Hak akses umum meliputi:

➢ Baca (Read): Ini memungkinkan pengguna untuk melihat informasi dalam sumber daya sistem, seperti membaca file, catatan yang dipilih, atau bidang dalam catatan. Hak baca juga mencakup kemampuan untuk menyalin atau mencetak informasi tersebut.

➢ Tulis (Write): Pengguna dengan hak menulis dapat menambahkan, mengubah, atau menghapus data dalam sumber daya sistem, yang mencakup baik membaca maupun mengubah data dalam sumber daya tersebut.

➢ Jalankan (Execute): Hak menjalankan memungkinkan pengguna menjalankan program-program tertentu atau mengeksekusi tindakan-tindakan khusus.

➢ Hapus (Delete): Pengguna dengan hak menghapus dapat menghapus sumber daya sistem tertentu, seperti file atau catatan.

➢ Buat (Create): Hak ini memungkinkan pengguna untuk membuat file, catatan, atau bidang baru dalam sumber daya.

➢ Cari (Search): Pengguna dengan hak mencari dapat mencantumkan file dalam direktori atau melakukan tindakan pencarian lainnya dalam direktori.

Mekanisme kontrol akses menggunakan elemen-elemen ini untuk menentukan dan memberlakukan siapa yang dapat melakukan apa terkait dengan berbagai sumber daya dalam sistem komputer. Kombinasi subjek, objek, dan hak akses membentuk dasar dari kebijakan kontrol akses dan konfigurasi keamanan.

III. ROLEBASED ACCESS CONTROL

Control Akses Discretionary (DAC) adalah sebuah skema di mana suatu entitas diberikan hak akses yang memungkinkannya, atas kebijakannya sendiri, untuk memberi entitas lain akses ke suatu sumber daya. Pendekatan umum dalam DAC, yang digunakan dalam sistem operasi dan sistem

manajemen database, menggunakan matriks akses, sebuah konsep yang awalnya dirumuskan oleh Lampson dan selanjutnya disempurnakan oleh yang lain.

Matriks akses adalah struktur dua dimensi di mana satu dimensinya terdiri dari subjek yang teridentifikasi, seperti pengguna individu atau kelompok pengguna, dan dimensi lainnya mencantumkan objek yang dapat diakses. Objek dapat berkisar dari bidang data yang sangat halus hingga pengelompokan yang lebih agregat seperti catatan, file, atau bahkan basis data keseluruhan. Setiap entri dalam matriks menentukan hak akses subjek tertentu untuk suatu objek tertentu.

Berikut adalah poin-poin kunci mengenai DAC dan matriks akses:

1. Matriks yang Rendah: Dalam praktiknya, matriks akses seringkali merupakan matriks yang jarang terisi, yang berarti tidak setiap kombinasi subjek dan objek memiliki entri. Untuk memudahkan pengelolaan, matriks ini biasanya didekomposisi dalam salah satu dari dua cara.
2. Dekomposisi berdasarkan Kolom (ACLs): Matriks dapat didekomposisi berdasarkan kolom untuk membuat Daftar Kontrol Akses (ACLs). Untuk setiap objek, ACL mencantumkan pengguna dan hak akses yang diperbolehkannya. ACL dapat mencakup entri default atau publik, yang memungkinkan pengguna yang tidak secara eksplisit terdaftar memiliki seperangkat hak akses default, yang seharusnya mengikuti prinsip hak paling rendah. Entri dalam ACL dapat mencakup pengguna individu dan kelompok pengguna.
3. Dekomposisi berdasarkan Baris (Tiket Kemampuan): Dekomposisi berdasarkan baris menghasilkan tiket kemampuan. Setiap tiket menentukan objek yang diotorisasi dan operasi yang diperbolehkannya untuk pengguna tertentu. Pengguna dapat memiliki beberapa tiket dan diotorisasi untuk meminjamkan atau memberikannya kepada orang lain. Tiket kemampuan kurang nyaman untuk menentukan hak akses pengguna tertentu, karena mereka memberikan informasi untuk setiap sumber daya, yang membuatnya lebih aman. Melindungi integritas tiket

kemampuan sangat penting, dan biasanya dilakukan oleh sistem operasi. Salah satu cara untuk memastikan integritas tiket adalah dengan membuat sistem operasi menyimpan semua tiket dalam area memori yang aman dan tidak dapat diakses oleh pengguna. Alternatif lain adalah menyertakan token yang tidak dapat dipalsukan dalam kemampuan. Ini bisa berupa kata sandi acak besar atau kode otentikasi pesan kriptografis. Nilai ini diverifikasi oleh sumber daya yang relevan setiap kali akses diminta. Bentuk tiket kemampuan ini cocok digunakan dalam lingkungan terdistribusi, di mana keamanan konten tiket tidak dapat dijamin.

Secara ringkas, DAC memungkinkan entitas untuk memiliki kebebasan dalam memberikan hak akses, dan matriks akses adalah konsep dasar dalam DAC, di mana subjek dan objek dikelola untuk menentukan dan memberlakukan kontrol akses. Penggunaan ACL dan tiket kemampuan menyediakan metode yang fleksibel dan aman untuk mengendalikan akses ke sumber daya.

IV. ATTRIBUTE BASED ACCESS CONTROL

Attribute-Based Access Control (ABAC) adalah model kontrol akses modern yang memberikan kendali yang sangat rinci terhadap akses ke sumber daya berdasarkan atribut yang terkait dengan subjek (pengguna, aplikasi, perangkat), objek (sumber daya), dan lingkungan di mana permintaan akses terjadi. Pendekatan ini menawarkan fleksibilitas dan kekuatan ekspresif, memungkinkan kebijakan akses yang kompleks. Elemen kunci dari model ABAC mencakup:

1. Atribut: Atribut adalah karakteristik atau properti yang terkait dengan subjek, objek, dan lingkungan. Mereka telah ditentukan sebelumnya dan ditetapkan oleh otoritas. Biasanya, atribut terdiri dari tiga komponen:
   - Kelas: Mendeskripsikan jenis atau kategori informasi yang terkait dengan atribut.
   - Nama: Memberikan label yang dapat dibaca oleh manusia untuk atribut tersebut.

- Nilai: Mewakili nilai spesifik atau contoh dari atribut tersebut.

Ada tiga jenis atribut dalam model ABAC:

- Atribut Subjek:

  Atribut ini menggambarkan karakteristik entitas aktif seperti pengguna, aplikasi, proses, atau perangkat. Mereka mendefinisikan identitas dan karakteristik subjek.

  Contoh atribut subjek mencakup pengenal subjek, nama, organisasi, jabatan, dan peran subjek.

- Atribut Objek:

  Atribut objek berkaitan dengan entitas pasif, juga dikenal sebagai sumber daya. Ini bisa berbagai entitas terkait sistem informasi seperti file, catatan, tabel, proses, program, jaringan, dan domain. Contoh atribut objek untuk dokumen Microsoft Word misalnya bisa mencakup judul, subjek, tanggal, dan penulis. Atribut objek seringkali dapat diperoleh dari metadata objek, dan mereka sangat penting untuk pengambilan keputusan kontrol akses.

- Atribut Lingkungan:

  Atribut ini menggambarkan konteks atau lingkungan operasional, teknis, dan situasional di mana akses informasi terjadi. Contoh atribut lingkungan mencakup tanggal dan waktu saat ini, status aktivitas virus/hacker saat ini, dan tingkat keamanan jaringan (misalnya, Internet atau intranet). Meskipun atribut subjek dan objek lebih sering digunakan, atribut lingkungan dapat relevan dalam skenario kontrol akses yang spesifik.

Model Kebijakan: Model kebijakan dalam ABAC mendefinisikan aturan dan kondisi yang menentukan izin akses. Ini menentukan bagaimana atribut digunakan untuk membuat keputusan kontrol akses. Kebijakan dalam ABAC dapat sangat fleksibel dan dapat mengungkapkan kondisi kompleks yang melibatkan atribut subjek, objek, dan lingkungan. Kebijakan tersebut biasanya didasarkan pada logika Boolean, memungkinkan pembuatan aturan kontrol akses yang canggih.

Model Arsitektur: Model arsitektur adalah implementasi praktis dari kebijakan kontrol akses yang ditentukan dalam model kebijakan. Ini menjelaskan bagaimana sistem kontrol akses menerapkan kebijakan yang telah ditentukan, memastikan bahwa permintaan akses dievaluasi sesuai dengan kondisi atribut yang telah ditentukan. Dalam praktiknya, mekanisme penegakan kontrol akses dapat bervariasi, termasuk titik keputusan kebijakan, titik penegakan kebijakan, dan server otorisasi.

ABAC khususnya cocok untuk skenario di mana kendali yang sangat rinci terhadap akses ke sumber daya diperlukan, seperti dalam layanan web, komputasi awan, dan lingkungan lain dengan persyaratan akses yang kompleks. Meskipun dampak kinerja dari evaluasi kebijakan akses berbasis atribut dapat menjadi kekhawatiran, hal ini seringkali kurang terasa dalam konteks di mana sudah ada biaya kinerja yang relatif tinggi terkait dengan permintaan akses. Sebagai hasilnya, ABAC telah diterapkan dalam berbagai domain aplikasi, khususnya yang membutuhkan kemampuan kontrol akses canggih.

V. ACCESS MANAGEMENT, IDENTITY DAN CREDENSIAL

Manajemen Identitas, Kredensial, dan Akses (Identity, Credential, and Access Management - ICAM) adalah pendekatan komprehensif untuk mengelola dan menerapkan identitas digital (dan atribut terkait), kredensial, dan kontrol akses. ICAM telah dikembangkan oleh pemerintah Amerika Serikat, tetapi dapat diterapkan tidak hanya oleh lembaga pemerintah, tetapi juga oleh perusahaan yang mencari pendekatan bersatu dalam mengendalikan akses. ICAM dirancang untuk:

Membuat representasi identitas digital yang dapat dipercaya dari individu dan apa yang disebut dalam dokumen ICAM sebagai entitas non-person (NPE). NPE mencakup proses, aplikasi, dan perangkat otomatis yang mencari akses ke sumber daya. Mengikat identitas tersebut ke kredensial yang dapat berfungsi sebagai pengganti individu atau NPE dalam transaksi akses. Kredensial adalah objek atau struktur data yang secara sah mengikat identitas

(dan secara opsional, atribut tambahan) ke token yang dimiliki dan dikendalikan oleh pelanggan. Menggunakan kredensial untuk memberikan akses yang diotorisasi ke sumber daya lembaga.

1. Manajemen Identitas

   Manajemen identitas berurusan dengan menetapkan atribut pada identitas digital dan menghubungkan identitas digital tersebut dengan individu atau NPE. Tujuannya adalah untuk membangun identitas digital yang dapat dipercaya yang independen dari aplikasi atau konteks tertentu. Pendekatan tradisional, dan masih paling umum, untuk kontrol akses pada aplikasi dan program adalah dengan membuat representasi digital identitas untuk penggunaan khusus aplikasi atau program tertentu. Sebagai hasilnya, pemeliharaan dan perlindungan identitas itu sendiri diperlakukan sebagai sesuatu yang sekunder dibandingkan dengan misi yang terkait dengan aplikasi. Selain itu, terdapat tumpang tindih yang signifikan dalam upaya untuk membentuk identitas khusus aplikasi ini.

   Berbeda dengan akun yang digunakan untuk masuk ke jaringan, sistem, atau aplikasi, catatan identitas lembaga tidak terkait dengan jabatan, tugas pekerjaan, lokasi, atau apakah akses diperlukan ke sistem tertentu. Hal-hal tersebut mungkin menjadi atribut yang terkait dengan catatan identitas lembaga, dan juga dapat menjadi bagian dari apa yang secara unik mengidentifikasi individu dalam aplikasi tertentu. Keputusan kontrol akses akan didasarkan pada konteks dan atribut yang relevan dari pengguna, bukan hanya identitas mereka. Konsep identitas lembaga adalah bahwa individu akan memiliki representasi digital tunggal dari diri mereka sendiri yang dapat dimanfaatkan di berbagai departemen dan lembaga untuk berbagai tujuan, termasuk kontrol akses.

2. Manajemen Kredensial

   Seperti yang disebutkan, kredensial adalah objek atau struktur data yang secara sah mengikat identitas (dan secara opsional, atribut tambahan) ke

token yang dimiliki dan dikendalikan oleh pelanggan. Contoh kredensial termasuk kartu pintar, kunci kriptografi pribadi/publik, dan sertifikat digital. Manajemen kredensial adalah pengelolaan siklus hidup kredensial. Manajemen kredensial mencakup lima komponen logis berikut:

- Individu yang berwenang mensponsori individu atau entitas untuk mendapatkan kredensial agar bisa mengakses sumber daya. Misalnya, seorang supervisor departemen mensponsori seorang karyawan departemen. Individu yang disponsori mendaftar untuk kredensial, yang merupakan proses yang biasanya mencakup pembuktian identitas dan pengambilan data biografi dan biometrik. Langkah ini juga dapat melibatkan penyatuan data atribut yang otoritatif, yang dikelola oleh komponen manajemen identitas.
- Kredensial diproduksi. Bergantung pada jenis kredensial, produksi dapat melibatkan enkripsi, penggunaan tanda tangan digital, produksi kartu pintar, atau fungsi lainnya. Kredensial diberikan kepada individu atau NPE.

Akhirnya, kredensial harus dikelola selama siklus hidupnya, yang mungkin mencakup pencabutan, penerbitan ulang/penggantian, pendaftaran ulang, masa berlaku habis, pengaturan ulang nomor identifikasi pribadi (PIN), penangguhan, atau pemulihan.

3. Manajemen Akses

Komponen manajemen akses menangani manajemen dan pengendalian cara entitas diberi akses ke sumber daya. Ini mencakup akses logis dan fisik, dan bisa menjadi bagian internal dari sistem atau elemen eksternal. Tujuan manajemen akses adalah memastikan bahwa verifikasi identitas yang tepat dilakukan ketika individu mencoba mengakses gedung, sistem komputer, atau data yang sensitif terhadap keamanan. Fungsi kontrol akses menggunakan kredensial yang disajikan oleh mereka yang meminta akses dan identitas digital pihak yang meminta. Tiga elemen dukungan diperlukan untuk fasilitas kontrol akses di seluruh perusahaan:

4. Manajemen sumber daya: Elemen ini berkaitan dengan menentukan aturan untuk sumber daya yang memerlukan kontrol akses. Aturan tersebut akan mencakup persyaratan kredensial dan atribut pengguna, atribut sumber daya, dan kondisi lingkungan yang diperlukan untuk mengakses sumber daya tertentu untuk fungsi tertentu.
5. Manajemen hak istimewa: Elemen ini berkaitan dengan menetapkan dan memelihara atribut hak istimewa yang merupakan profil akses individu. Atribut ini mewakili fitur individu yang dapat digunakan sebagai dasar untuk menentukan keputusan akses ke sumber daya fisik dan logis. Hak istimewa dianggap sebagai atribut yang dapat dihubungkan ke identitas digital.
6. Manajemen kebijakan: Elemen ini mengatur apa yang diperbolehkan dan tidak diperbolehkan dalam transaksi akses. Dengan kata lain, diberikan identitas dan atribut pengguna, atribut sumber daya atau objek, dan kondisi lingkungan.

VI. TRUST FRAME WORK

Kerangka Kepercayaan (Trust Frameworks) adalah konsep yang terkait dengan kepercayaan, identitas, dan atribut yang telah menjadi perhatian inti bisnis internet, penyedia layanan jaringan, dan perusahaan besar. Perhatian ini dapat terlihat jelas dalam pengaturan e-commerce. Untuk efisiensi, privasi, dan kesederhanaan hukum, pihak yang terlibat dalam transaksi umumnya menerapkan prinsip "perlu tahu": Apa yang Anda perlu ketahui tentang seseorang untuk berurusan dengan mereka? Jawabannya bervariasi dari kasus ke kasus, dan mencakup atribut seperti nomor registrasi profesional atau lisensi, organisasi dan departemen, ID staf, tingkat keamanan, nomor referensi pelanggan, nomor kartu kredit, pengenal kesehatan unik, alergi, golongan darah, nomor kartu sosial, alamat, status kewarganegaraan, penanganan jaringan sosial, nama samaran, dan sebagainya. Atribut individu yang harus diketahui dan diverifikasi untuk mengizinkan suatu transaksi tergantung pada konteks.

Perhatian yang sama terhadap atribut semakin penting untuk semua jenis situasi pengendalian akses, bukan hanya dalam konteks bisnis elektronik. Sebagai contoh, sebuah perusahaan mungkin perlu memberikan akses ke sumber daya bagi pelanggan, pengguna, pemasok, dan mitra. Bergantung pada konteks, akses akan ditentukan bukan hanya berdasarkan identitas, tetapi juga berdasarkan atribut permintaan dan sumber daya.

1. Pendekatan Pertukaran Identitas Tradisional

   Transaksi online atau jaringan yang melibatkan pihak dari berbagai organisasi, atau antara organisasi dan pengguna individu seperti pelanggan online, umumnya memerlukan pertukaran informasi identitas. Informasi ini dapat mencakup sejumlah atribut terkait selain dari nama atau identifier numerik sederhana. Baik pihak yang mengungkapkan informasi maupun pihak yang menerima informasi perlu memiliki tingkat kepercayaan terhadap isu-isu keamanan dan privasi terkait informasi tersebut. Gambar 4.13a menunjukkan teknik tradisional untuk pertukaran informasi identitas. Ini melibatkan pengguna mengembangkan pengaturan dengan penyedia layanan identitas untuk memperoleh identitas digital dan kredensial, serta pengaturan dengan pihak yang memberikan layanan dan aplikasi pengguna akhir dan bersedia mengandalkan informasi identitas dan kredensial yang dihasilkan oleh penyedia layanan identitas.

2. Kerangka Kepercayaan Identitas Terbuka

   Tanpa adanya standar universal dan kerangka kerja, pengaturan seperti yang ditunjukkan pada Gambar 4.13a harus direplikasi dalam berbagai konteks. Pendekatan yang lebih baik adalah mengembangkan pendekatan terbuka dan terstandarisasi untuk pertukaran identitas dan atribut yang dapat dipercaya. Di sisa bagian dari bagian ini, kita akan mengkaji pendekatan semacam ini yang semakin diterima. Sayangnya, topik ini penuh dengan singkatan, sehingga lebih baik dimulai dengan definisi yang paling penting:

   - OpenID: Ini adalah standar terbuka yang memungkinkan pengguna diotentikasi oleh situs yang bekerja sama (dikenal sebagai Pihak yang

Bergantung) menggunakan layanan pihak ketiga, menghilangkan kebutuhan bagi pemilik situs web untuk menyediakan sistem mereka sendiri dan memungkinkan pengguna untuk mengkonsolidasikan identitas digital mereka. Pengguna dapat membuat akun dengan penyedia identitas OpenID pilihan mereka, dan kemudian menggunakan akun tersebut sebagai dasar untuk masuk ke situs web yang menerima otentikasi OpenID.

- OIDF: OpenID Foundation adalah organisasi nirlaba internasional dari individu dan perusahaan yang berkomitmen untuk mengaktifkan, mempromosikan, dan melindungi teknologi OpenID. OIDF membantu komunitas dengan menyediakan infrastruktur yang diperlukan dan membantu dalam mempromosikan dan mendukung adopsi OpenID yang lebih luas.
- ICF: Information Card Foundation adalah komunitas nirlaba dari perusahaan dan individu yang bekerja sama untuk mengembangkan ekosistem Kartu Informasi. Kartu Informasi adalah identitas digital pribadi yang dapat digunakan oleh orang secara online dan merupakan komponen utama dalam metasistem identitas. Secara visual, setiap Kartu Informasi memiliki gambar berbentuk kartu dan nama kartu yang terkait dengannya yang memungkinkan orang mengorganisir identitas digital mereka dan dengan mudah memilih yang ingin mereka gunakan untuk interaksi tertentu.
- OITF: Kerangka Kepercayaan Identitas Terbuka adalah spesifikasi standar dari kerangka kepercayaan untuk pertukaran identitas dan atribut, yang dikembangkan bersama oleh OIDF dan ICF.
- OIX: Open Identity Exchange Corporation adalah penyedia kerangka kepercayaan sertifikasi independen, netral, internasional yang sesuai dengan model Kerangka Kepercayaan Identitas Terbuka.
- AXN: Jaringan Pertukaran Atribut (AXN) adalah gerbang internet skala besar untuk penyedia layanan identitas dan pihak yang bergantung untuk mengakses atribut identitas online yang dinyatakan

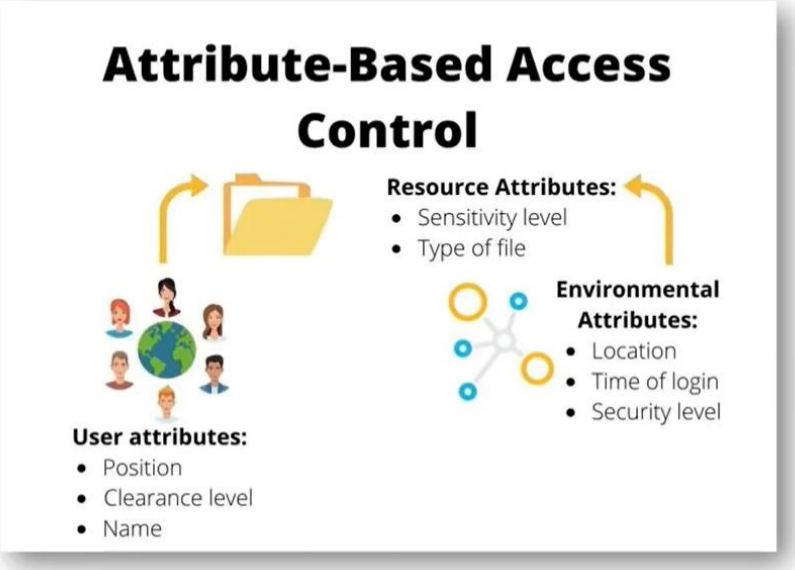
oleh pengguna, yang diizinkan, dan diverifikasi dalam jumlah besar dengan biaya terjangkau.

Dalam sistem identitas digital, kerangka kepercayaan berfungsi sebagai program sertifikasi. Ini memungkinkan pihak yang menerima kredensial identitas digital (disebut sebagai pihak yang bergantung) untuk percaya pada identitas, keamanan, dan kebijakan privasi pihak yang mengeluarkan kredensial tersebut (disebut sebagai penyedia layanan identitas) dan sebaliknya. Secara lebih formal, OIX mendefinisikan kerangka kepercayaan sebagai seperangkat komitmen yang dapat diverifikasi dari masing-masing pihak dalam transaksi kepada pihak lawan mereka. Komitmen ini mencakup kontrol (termasuk kewajiban regulasi dan kontraktual) untuk membantu memastikan komitmen dijalankan dan solusi untuk ketidakpatuhan terhadap komitmen tersebut.

Kebijakan Access Control

- **Discretionary** access control (DAC): kebijakan yang mengizinkan entitas tertentu (orang, proses, perangkat) untuk mengontrol akses entitas lain untuk mengakses sumberdaya system sesuai dengan izin (access rules) yang di berikan.
- **Mandatory** access control (MAC): menetapkan label atau klasifikasi keamanan ke sumberdaya sistem dan mengizinkan akses hanya ke entitas (orang, proses, perangkat) dengan tingkat otorisasi atau izin yang berbeda. Kontrol ini umumnya di tetapkan oleh sistem operasi atau security kernel.
- **Role-based** access control (RBAC): identifikasi, otentikasi, dan otorisasi individu berdasarkan jabatan pekerjaan mereka dalam suatu organisasi.
- **Attribute-based** access control: juga di kenal sebagai Policy – Based. Hak akses di berikan melalui penggunaan kebijakan yang menggabungkan attribute Bersama.

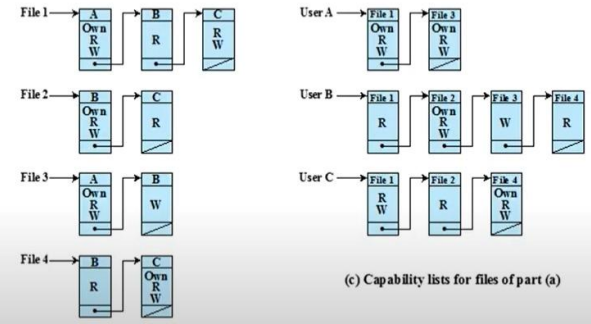
Kebijakan Access Control



Access Control Requirement

- **Reliable input**: melalui mekanisme autentikasi
- **Fine and coarse specifications**: membagi hak akses ke berbagai tingkatan akses.
- **Least privilege**: minimum authorisasi untuk melaksanakan tugasnya
- **Separation of duty**: individu yang berbeda memiliki langkah-langkah yang berbeda.
- **Open and closed policies**: mengakses secara khusus diizinkan atau izinkan semua akses kecuali yang di larang.
- **Administrative policies**: siapa yang dapat menambahkan, menghapus, dan memodifikasi rules.

Access Matrix and Data Structure



(b) Access control lists for files of part (a)

(c) Capability lists for files of part (a)

Types of attributes

Subject attributes

Object attributes

Environment attributes

Object attribute

—

- Objek (atau resource) adalah informasi terkait system yang memuat atau menerima informasi dari subjek.
- Objek memiliki atribut yang dapat dapat di tingkatkan untuk membuat keputusan akses control.
  - Judul
  - Penulis
  - Tangga

Subject attributes

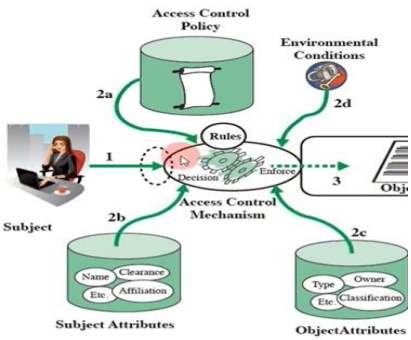
- Subject adalah entitas aktif yang menyebabkan informasi mengalir ke antar objek atau actor yang mengubah state dari system
- Attributes mendefinisikan identitas dan karakteristik dari subjek
  - Nama
  - Organisasi
  - Nama pekerjaan

Environment attributes

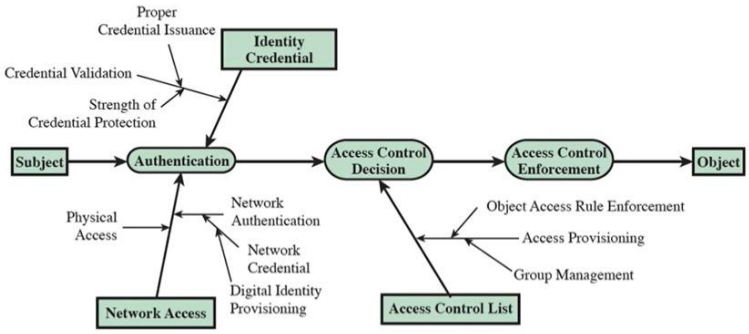
- Mendeskripsikan lingkungan atau konteks operasional, teknis, dan bahkan situasional tempat akses informasi terjadi.
  - Tanggal aktual
  - Aktivitas virus / hacker teraktual
  - Level keamanan jaringan
  - *Tidak berasosiasi dengan subjek maupun objek*
- Attribut ini paling sering diabaikan pada banyak kebanyakan kebijakan access control.

Sample ABAC scenario

1. Subject request akses ke objek
2. Access Control diatur oleh sekumpulan rules (2a) : menilai attribute dari subjek (2b) objek, dan (2c) environment.
3. Access Control memberikan akses subjek ke objek jika diizinkan.

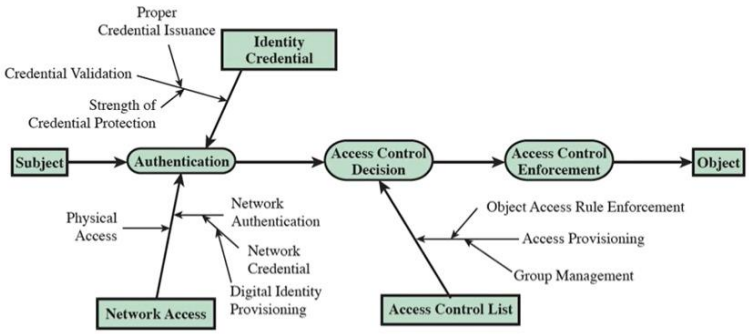


Access Control List vs AttrBasedAC trust relationships



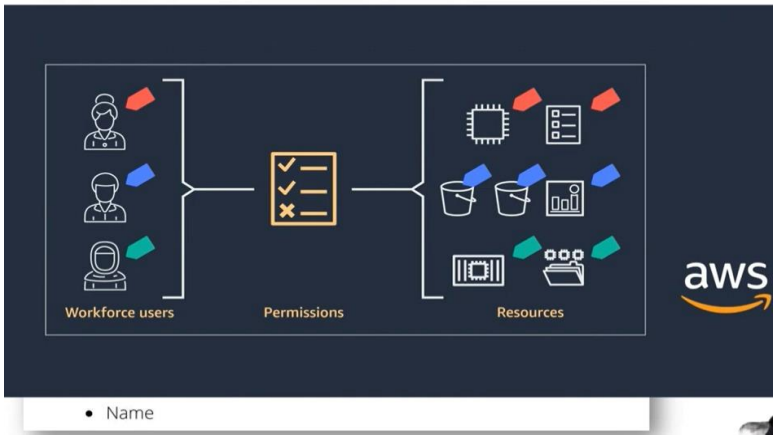
Access Control List

Access Control List vs AttrBasedAC trust relationships

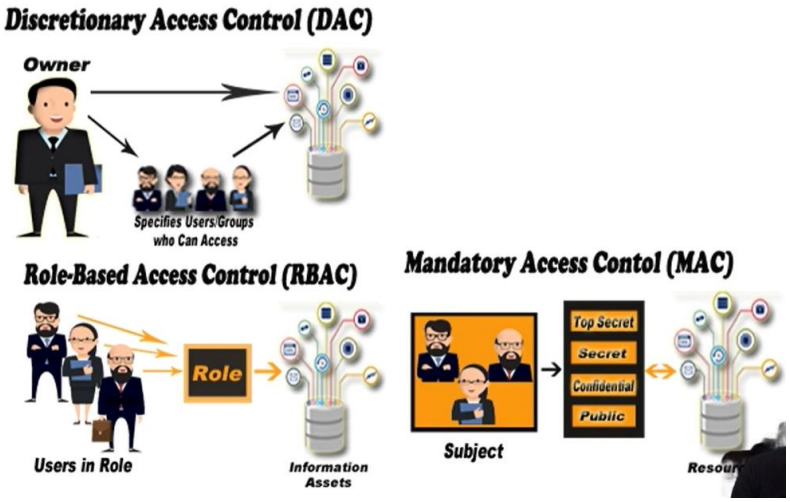


Access Control List

Kebijakan Access Control



Kebijakan Access Control



Access Control Element

- **Subject:** entity that can access objects
  - a process representing user/application
  - often have 3 classes: **owner**, **group**, **world**
- **Object:** access controlled resource
  - e.g. files, directories, records, programs etc
  - number/type depend on environment
- **Access right:** way in which subject accesses an object
  - e.g. read, write, execute, delete, create, search

Discretionary Access Control

- Sering digambarkan menggunakan access matrix
  - Mencantumkan subjek dalam dimensi pertama (baris)
  - Mencantumkan objek dalam dimensi lainnya (kolom)
  - Setiap entry menentukan hak akses dari subjek tertentu untuk objek tersebut.
- Access matrix selalu tersebar.
- Dapat diuraikan dalam bentuk baris atau kolom

Access Matrix

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

Protection Domain

- Protection domain merupakan **sekumpulan objek** terikat bersamaan dengan **hak akses ke objek tersebut.**
- Pada contoh access matrix setiap baris mendefinisikan sebuah protection domain. Setiap pengguna berasosiasi dengan sebuah protection domain
- Setiap proses yang dipicu oleh user terhadap object memiliki hak akses yang didefinisikan oleh protection domain object tersebut.
- Pengguna dapat menciptakan proses baru yang memiliki sebagian dari hak akses pengguna. Hal ini mendefinisikan sebuah sebuah protection domain baru. Dengan begini pengguna dapat menentukan protection domain khusus untuk program yang mencurigakan.
- Asosiasi antara proses dan protection domain dapat berlangsung secara statis maupun dinamis.
- Pada mode pengguna sebagian arena memory atau instruksi mungkin tidak akan bisa diakses.
- Pada mode kernel instruksi istimewa dapat dijalankan dan area memory yang dilindungi dapat diakses.

Access Control Structures

- Access control lists (decomposed by column)
- Capability tickets (decomposed by row)

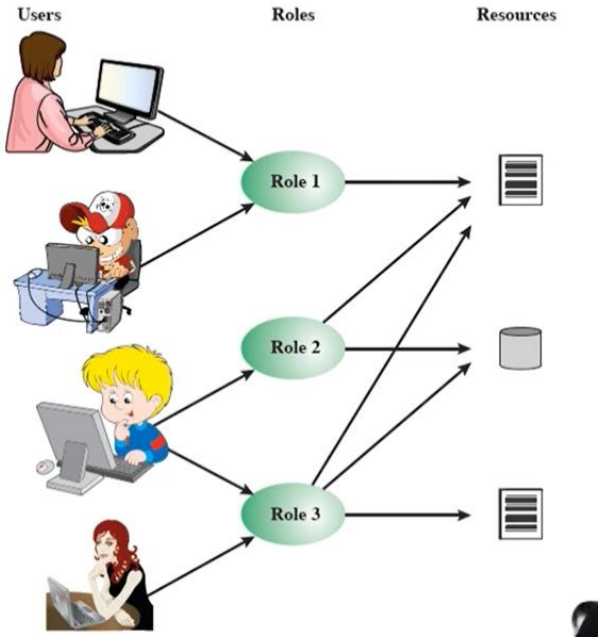
	Patient medical record	Patient's e-health terminal	Home network central station	e-prescription	Location Information Centre	Health Directory System	Invoice / Receipt
Patient	Read()	Access()	Read()	Read()			Sign()
Doctor	Modify() Store()	Access()	Access()	Create() Send()	Access()		Sign()
ERC	Read() Store()	Access()	Access()		Access()	Browse() Modify()	
Social worker				Read()		Browse()	Sign()
Pharmacist				Read()		Browse() Modify()	Sign()
Electrician			Access()				

Role Based Access Control

Access based on 'role', not identity

Many-to-many relationship between users and roles

Roles often static



General RBAC Variation

4 Model RBAC

- RBAC0: Minimum functionality
- RBAC1: RBAC0 plus role (permission) inheritance
- RBAC2: RBAC0 plus constraints (restrictions)
- RBAC3: RBAC0 plus all of the above

RBAC0 entities

- **User**: an individual (with UID) with access to system
- **Role**: a named job function (tells authority level)
- **Permission**: equivalent to access rights
- **Session**: a mapping between a user and set of roles to which a user is assigned

Constraints

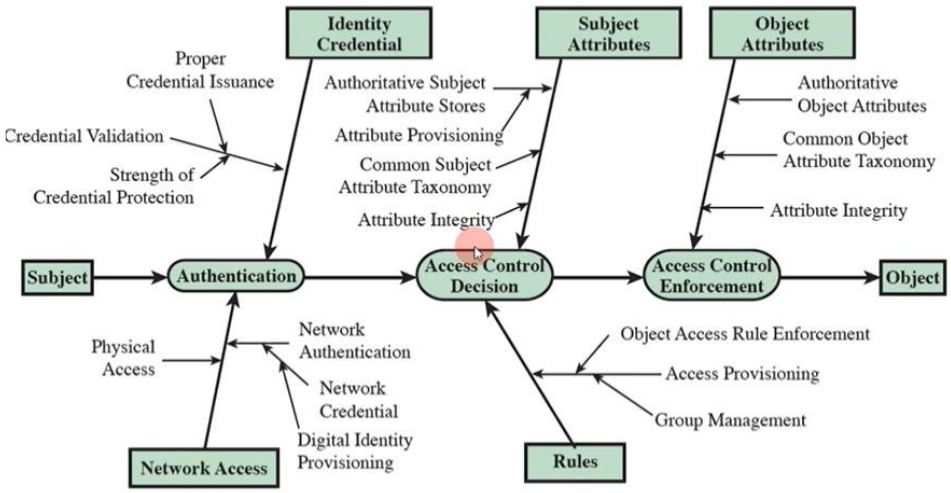
Sebuah kondisi (batasan) pada sebuah role atau antar role.

- **Mutually exclusive**
  - Pengguna hanya dapat ditetapkan ke salah satu role dari sekumpulan role.
  - Izin apapun hanya dapat di berikan untuk satu peran.
- **Cardinality**: tetapkan jumlah maksimum pengguna dengan peran tertentu (e.g., role untuk staff pemasaran)
- **Prerequisite role**: pengguna hanya dapat ditetapkan ke role tertentu setelah sebelumnya pernah mendapatkan role tertentu.

Attribute-based access control

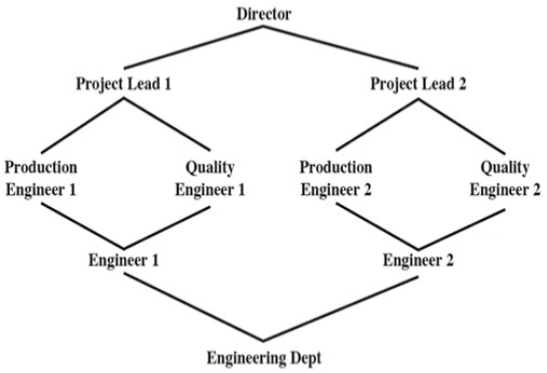
- Teknik yang termasuk baru
- Tentukan otorisasi yang mengekspresikan kondisi pada property sumberdaya dan subjek
  - Setiap sumbedaya memiliki attribut
  - Sebuah rule tunggal menyatakan kepemilikan untuk creatornya.
- Kekuatan : fleksibilitas
- Model yang umum digunakan pada **layanan cloud**.

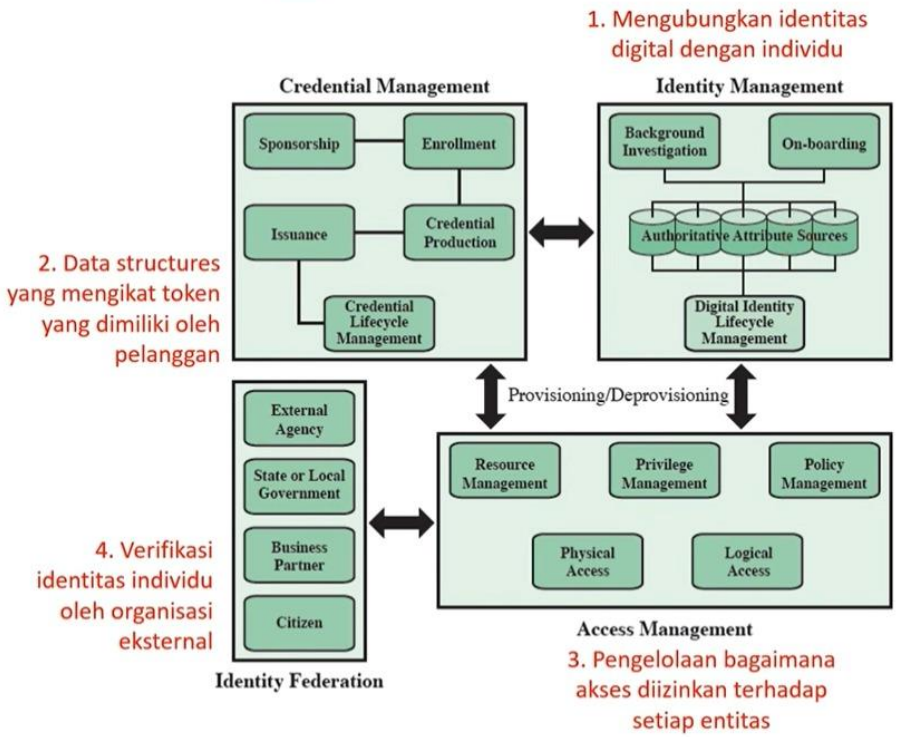
Access Control List vs AttrBasedAC trust relationships



Example of role hierarchy

- Director memiliki semua privileges
- Setiap role mewarisi semua privileges dari roles dibawahnya
- A role dapat di inherit dari beberapa role
- Privileges tambahan dapat ditugaskan kepada role tertentu





Identity, Credential, and Access Management (ICAM)

—

- Pendekatan yang kompherensif untuk mengelola dan menerapkan identitas digital, kredensial, dan access control.
- Dibuat oleh pemerintah Amerika
- Di desain untuk membuat representasi identitas digital yang terpercaya dari masing-masing individu dan entitas selain manusia.
- Kredensial berbentuk objek atau struktur data yang secara otoritatif mengikat identitas ke token yang dimiliki dan di kendalikan oleh pelanggan.
- Gunakan kredensial untuk menyediakan akses resmi ke sumberdaya agensi.