

NAMA: Agung Febri Ricandika

NIM: 1310651099

Kelas :B

Domain 1: Access Control

TUJUAN 1 UJIAN DALAM BAB INI

• Cornerstone Access Control Konsep • Access Control Model • Access Control Kategori Defensive dan Jenis • Metode Otentikasi • Access Control Teknologi • Menilai Access Control

PENGANTAR

Tujuan dari Acces Control adalah untuk memungkinkan pengguna berwenang mengakses data dan dapat melindungi ancaman akses data yang tidak sah.



FIGURE 1.1

The CIA triad.

Penjelasan gambar di atas

- Integrity untuk berusaha mencegah memodifikasi informasi atau data yang tidak sah. Integrity itu sendiri dibagi menjadi 2, Integrity data dan Integrity sistem .
- Availability untuk memastikan informasi yang diperlukan. Dan sistem harus dapat digunakan .
Contoh serangan terhadap Denial –of-Service (DOS).
- Confidentiality untuk menjaga informasi dari orang yg berhak mengakses, yang sifatnya data dataprivat, atau pencegahan bagi mereka yang tidak berkepentingan dengan pihak lain untuk keperluan tertentu

Dalam Access Control diperlukan Defense- in_depth yang di sebut juga pertahanan berlapis supaya lebih aman dalam menjaga data dan resiko tidak terlalu besar, dan sebaiknya harus menambahkan kerahasiaan atau kode pengaman , integritas.

Discretionary Acces Control (DAC) dimana User yang memutuskan untuk memprotek dan men share data melalui sistem computer untuk membatasi objek berdasarkan identitas atau kelompok yang bersangkutan.

Contoh ; Akses ke program aplikasi/ database, share resource.

Mandatory access controls (MAC) dimana sistem yang memutuskan bagaimana data diakses atau di share. atau melakukan operasi pada objek MAC user diklasifikasi berdasarkan level dan lebih aman dari pada DAC.

NAMA: Agung Febri Ricandika

NIM: 1310651099

Kelas :B

Contoh :

MAC akan mengantisipasi Pengaksesan terhadap File yang rahasia.

ACCESS CONTROL DEFENSIVE CATEGORIES AND TYPES

Di mana rangka ini untuk memahami dan menerapkan kontrol akses , dan memanfaatkan setiap kontrol yang dapat menambah keamanan. setiap jenis accessControl akan ditentukan pada sistem keamanan tersebut. Ada enam jenis kontrol akses :

• Pencegahan • Detektif • Korektif • Pemulihan • jera • Kompensasi

Type 1 authentication: something you know di butuhkan pengujian subjek dengan tantangan da respon dengan jawaban berpengatahuan.atau yang kita kenal dengan password atau PIN (Personal Identification Number , password nomor -based) . dan password atau PIN ini adalah pengaman yang mudah di bobol karna lemah.

Type 2 authentication: something you have di dalam ini pengguna harus memiliki tanda atau verivikasi yang pastinya aka dikonfirmasi oleh user.

Type 3 authentication: something you are adalah biometrik , yang menggunakan karakteristik fisik sebagai sarana identifikasi atau otentikasi, dapat digunakan untuk membangun sebuah identitas atau klaim identitas Contoh PEngenalan Wajah dan Pemindai Sidik jari.

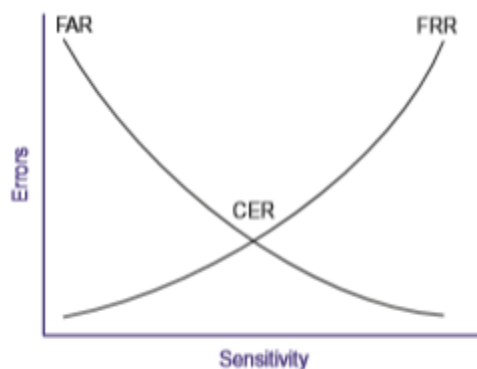


FIGURE 1.2

Crossover error rate.

Gambar diatas adalah grafik ke sensitifan sistem biometric

Types of biometric controls Ada sejumlah kontrol biometrik yang digunakan saat ini . Berikut ini adalah implementasi utama dan pro khusus mereka dan kontra yang berkaitan dengan keamanan kontrol akses .

Sidik jari

Sidik jari adalah yang paling banyak digunakan kontrol biometrik yang tersedia saat ini .

Banyak gedung perkantoran Pemerintah AS mengandalkan otentikasi sidik jari untuk akses fisik. Contohnya termasuk keyboard cerdas, yang mengharuskan pengguna untuk menyajikan sidik jari untuk membuka komputer screen saver

NAMA: Agung Febri Ricandika

NIM: 1310651099

Kelas :B

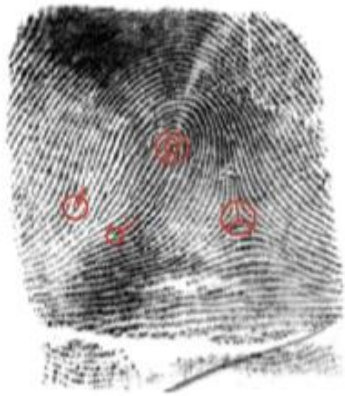


FIGURE 1.3

Fingerprint minutiae.¹⁰

EXAM WARNING

Scan sidik jari jarang digunakan karena risiko kesehatan . Alternatif harus dipertimbangkan untuk kontrol biometrik ini yang beresiko tinggi kalau di terus teruskan.

Memindai wajah

Pemindaian wajah (juga disebut pengenalan wajah) adalah proses pasif mengambil gambar wajah atau subjek dan membandingkan bahwa gambar ke daftar dalam database . dan keamanan ini bernilai tinggi karna wajah orang kan tidak sama.