



# Keamanan Sistem Informasi-Chapter 1

Agung BP

| Week | Theme  |
|------|--|
| 1    | Pengantar Matakuliah KSI                                   |
| 2    | Aspek Keamanan dan Keamanan Program                        |
| 3    | Keamanan Sistem Operasi                                    |
| 4    | Standarisasi Keamanan Secara Global                        |
| 5    | Keamanan Jaringan Komputer                                 |
| 6    |  |
| 7    | Keamanan Database  |
| 8    | UTS  |
| 9    | Pencurian Identitas  |
| 10   | Framework Keamanan, ISO 270001/2                           |
| 11   | Pengaturan Keamanan  |
| 12   |  |
| 13   | Kriptografi Klasik (Chipper text/Vigenere Chiper & ROT-13) |
| 14   | Kriptografi Modern   |
| 15   | UAS  |

# Penilaian

---

- $NTS = (0.45 \times \text{Tugas}) + (0.55 \times \text{UTS})$
- $NAS = (0.45 \times \text{Tugas}) + (0.55 \times \text{UAS})$
- $NA = (NTS+NAS)/2$
- NTS= Nilai Tengah Semester
- NAS= Nilai Akhir Semester
- NA= Nilai Akhir / Nilai Total

# Information System Security Principles

---

- Pustaka:
  1. Cole, Dr. Eric . Krutz, Dr. Ronald and Conley, James W. 2005. Network Security Bible. Wiley Publishing, Inc:USA
  2. Peltier, Thomas R. Peltier, Justin. Blackley, John. 2005. Information Security Fundamentals. Auerbach Publications: Washington, D.C.
  3. Link referensi lainnya:

<https://sites.google.com/site/eindrajit/-5-publikasi-buku>



surat keterangan domisili



All

Images

Maps

Shopping

More

SafeSearch on

Your location: Semarang, Central Java - Learn more

Sort by: Relevance

### Price

- Up to IDR 20,000
- IDR 20,000 – IDR 50,000
- IDR 50,000 – IDR 250,000
- IDR 250,000 – IDR 600,000
- Over IDR 600,000

IDR Min - IDR Max

### Seller

Tokopedia

## See surat keterangan domisili

Sponsored



Jasa dan Persewian Pembuatan Domisili

- SURAT KEPERLUAN SURAT KETERANGAN DOMISILI



BIRO JASA TANGERANG

0838 - 0702 - 7123

@Bj.tng

JASA PEMBUATAN SURAT DOMISILI SEMUA WILAYAH



Surat Domisili -  
Surat Domisili

IDR 30,000.00  
Tokopedia

Surat Domisili

IDR 30,000.00  
Tokopedia

dokumen jadul  
surat keterangan  
penduduk tahun...

IDR 15,000.00 Us...  
Bukalapak

Hive Five - Surat  
Pengurusan Izin  
Umroh

IDR 230,000,000.00  
Blibli.com

surat domisili -  
Surat Domisili

IDR 135,000.00  
Blibli.com

Cara Mudah  
Mengurus Surat-  
Surat & Dokumen...

IDR 28,800.00  
Shopee



BUKU SURAT KET KEMATIAN  
Tidak Ada MerekLainnyaLainnya

OPRAH UNTUK



Paket Domisili (Vo) Pkp

Blangko Buku Surat Keterangan  
Sakit 1 Ply Tidak Ada Merek

IDR 39,000.00  
Shopee

Free delivery

Surat Keterangan Lahir

IDR 50,000.00  
Tokopedia

Free delivery

IDR 17,000.00  
Shopee

Free delivery

IDR 233,500.00  
Tokopedia

Free delivery



downdetector.id/masalah/indosat-ooredoo/surabaya/

Down**detector**!

Insights

Downdete

Pemadaman Indosat Ooredoo Surabaya yang dilaporkan dalam 24 jam terakhir



# Prinsip Dasar (buku 1)

---



Confidentiality  
(Kerahasiaan)

Availability  
(tersedia)

Integrity  
(Integritas/Utuh)



- 
- Prinsip-prinsip diatas tergantung dari pengaplikasiannya dan konteksnya ketika item mana yang didahulukan.

# Confidentiality (Kerahasiaan)

- Kerahasiaan berkaitan dengan mencegah ter-ekspos / kebocoran informasi yang bersifat sensitif.

# Integrity (Integritas/Utuh)

- Tiga tujuan dari menjaga integritas:
  1. Pencegahan modifikasi informasi oleh pengguna yang tidak sah.
  2. Pencegahan modifikasi informasi yang tidak sah baik disengaja ataupun tidak disengaja oleh pengguna yang berwenang.
  3. Menjaga konsistensi internal dan external.
    - a. internal: memastikan data internal tetap sesuai.
    - b. Eksternal: memastikan data yang tersimpan sudah sesuai dengan kenyataannya.

# Availability

---

- Ketersediaan menjamin bahwa pengguna resmi sistem memiliki akses yang tepat waktu dan mengakses tanpa gangguan ke informasi didalam sistem dan/atau ke jaringan.

# Other important terms related of CIA

---

- ◆ **Identification** — identitas pengguna yang diakui ketika masuk kedalam sistem,  
contoh: ID Login/Username.
- ◆ **Authentication** — verifikasi/pengecekan bahwa identitas yang digunakan oleh pengguna adalah valid. Seperti memasukkan username dan password, kemudian sistem melakukan pengecekan terhadap username dan password yang digunakan.

# Lanjutan.

---

- ◆ **Accountability** — menentukan tindakan dan perilaku pengguna ke dalam suatu sistem, dan tanggungjawab berada di tangan pengguna. Contoh: mencatat perilaku/kegiatan user ketika berada di dalam sistem.
- ◆ **Authorization** — pemberian hak akses kepada pengguna untuk dapat mengakses sumber daya.

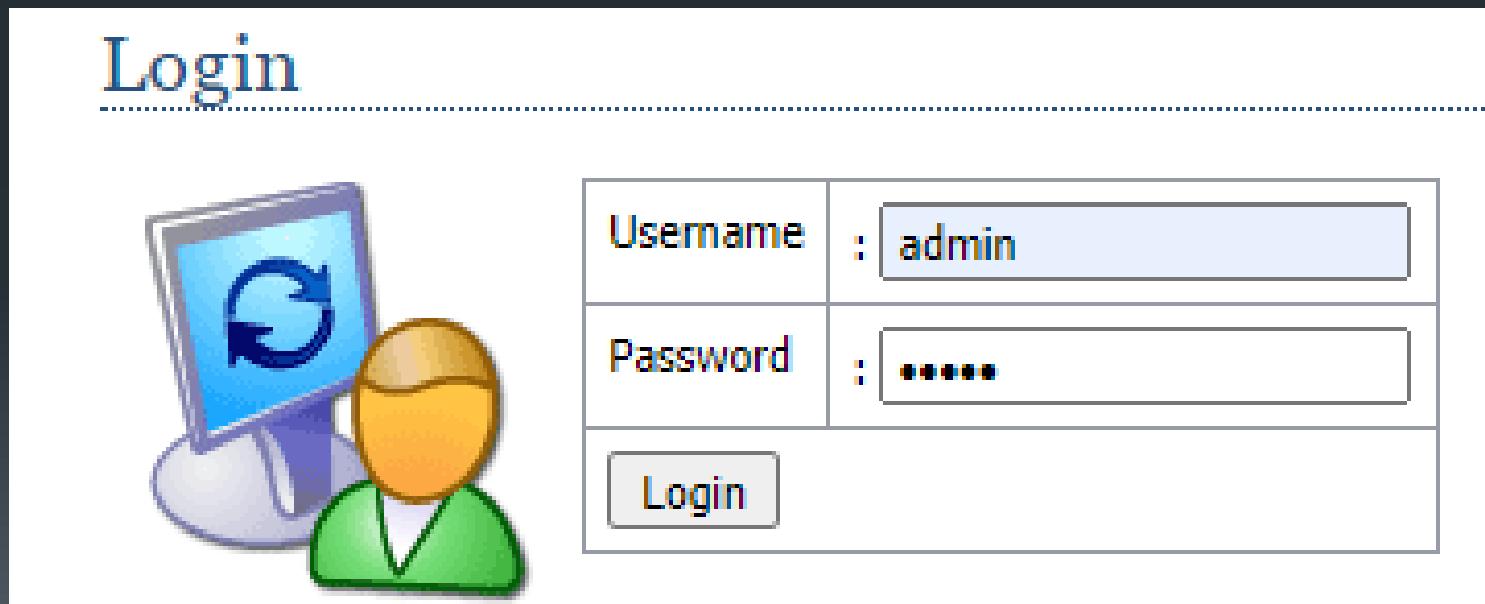
# Contoh dari IAAA

---

- IAAA= Identification, Authentication, Accountability, and Authorization.

# Identification

- Halaman Login,



# Authentication

- Table pengguna, inputan password dienkripsi

|   | username | password                         | nama_lengkap  | email           | no_telp     | level | blokir |
|---|----------|----------------------------------|---------------|-----------------|-------------|-------|--------|
| 1 | admin    | 21232f297a57a5a743894a0e4a801fc3 | Administrator | admin@detik.com | 08238923848 | admin | N      |
| * | (NULL)   | (NULL)                           | (NULL)        | (NULL)          | (NULL)      | user  | N      |

- Pengecekan/Authentication terkait username dan password dari pengguna.

```
<?php
include "../config/koneksi.php";
function antiinjection($data){
    $filter_sql = mysql_real_escape_string(stripslashes(strip_tags(htmlspecialchars($data,ENT_QUOTES))));
    return $filter_sql;
}

$username = antiinjection($_POST[username]);
$pass     = antiinjection(md5($_POST[password]));

$login=mysql_query("SELECT * FROM admins WHERE username='$username' AND password='$pass' AND blokir='N'");
$ketemu=mysql_num_rows($login);
```

# Accountability

|    | <b>id</b> | <b>user_u</b> | <b>nama</b> | <b>aktivitas</b>                 | <b>waktu</b>                |
|----|-----------|---------------|-------------|----------------------------------|-----------------------------|
|    | Filter    | Filter        | Filter      | Filter                           | Filter                      |
| 1  | 3         | agungtama     | agung       | Login                            | 02/05/2019 21:29:02         |
| 2  | 4         | agungtama     | agung       | Login                            | 02/05/2019 21:36:19         |
| 3  | 5         | agungtama     | agung       | Login                            | 02/05/2019 21:39:58         |
| 4  | 6         | agungtama     | agung       | Login                            | 02/05/2019 21:41:22         |
| 5  | 7         | agungtama     | agung       | Login                            | 02/05/2019 21:42:33         |
| 6  | 9         | agungtama     | agung       | Login                            | 02/05/2019 22:01:14         |
| 7  | 10        | agungtama     | agung       | Login                            | 02/05/2019 22:06:56         |
| 8  | 11        | agungtama     | agung       | Login                            | 02/05/2019 22:16:10         |
| 9  | 12        | agungtama     | agung       | Login                            | 02/05/2019 22:19:29         |
| 10 | 13        | agungtama     | agung       | Login                            | 02/05/2019 22:22:41         |
| 11 | 14        | admin         | admin       | Pendaftaran baru user domain ... | 2019-05-03 22:00:53.2182976 |

# Atau

- Kolom “adm” digunakan untuk mencatat siapa yang memasukkan data transaksi pembelian (no\_po=Nomer Purchase Order)

The screenshot shows a MySQL Workbench interface with the following details:

- Toolbar:** Includes tabs for Result, Messages, Table Data (selected), Objects, and History.
- Query Editor:** Shows a query with parameters: Show All, Or, Limit 0, 10000, and Refresh button.
- Table Data:** A table named "data\_transaksi" with the following schema:

|  | no_po        | tgl_po     | id_vendor | adm   | bayar |
|--|--------------|------------|-----------|-------|-------|
|  | PB0000000001 | 2015-03-29 | S1        | SUPER | Tunai |
|  | PB0000000002 | 2015-03-29 | S1        | SUPER | Tunai |
|  | PB0000000003 | 2015-03-29 | S1        | SUPER | Tunai |
|  | PB0000000004 | 2015-03-29 | S1        | SUPER | Tunai |
|  | PB0000000005 | 2015-03-29 | S1        | SUPER | Tunai |
|  | PB0000000006 | 2015-03-29 | S1        | SUPER | Tunai |
|  | PB0000000007 | 2015-03-29 | S1        | SUPER | Tunai |
|  | PB0000000008 | 2015-03-29 | S1        | SUPER | Tunai |

# Authorization

1 Result | 2 Messages | 3 Table Data | 4 Objects

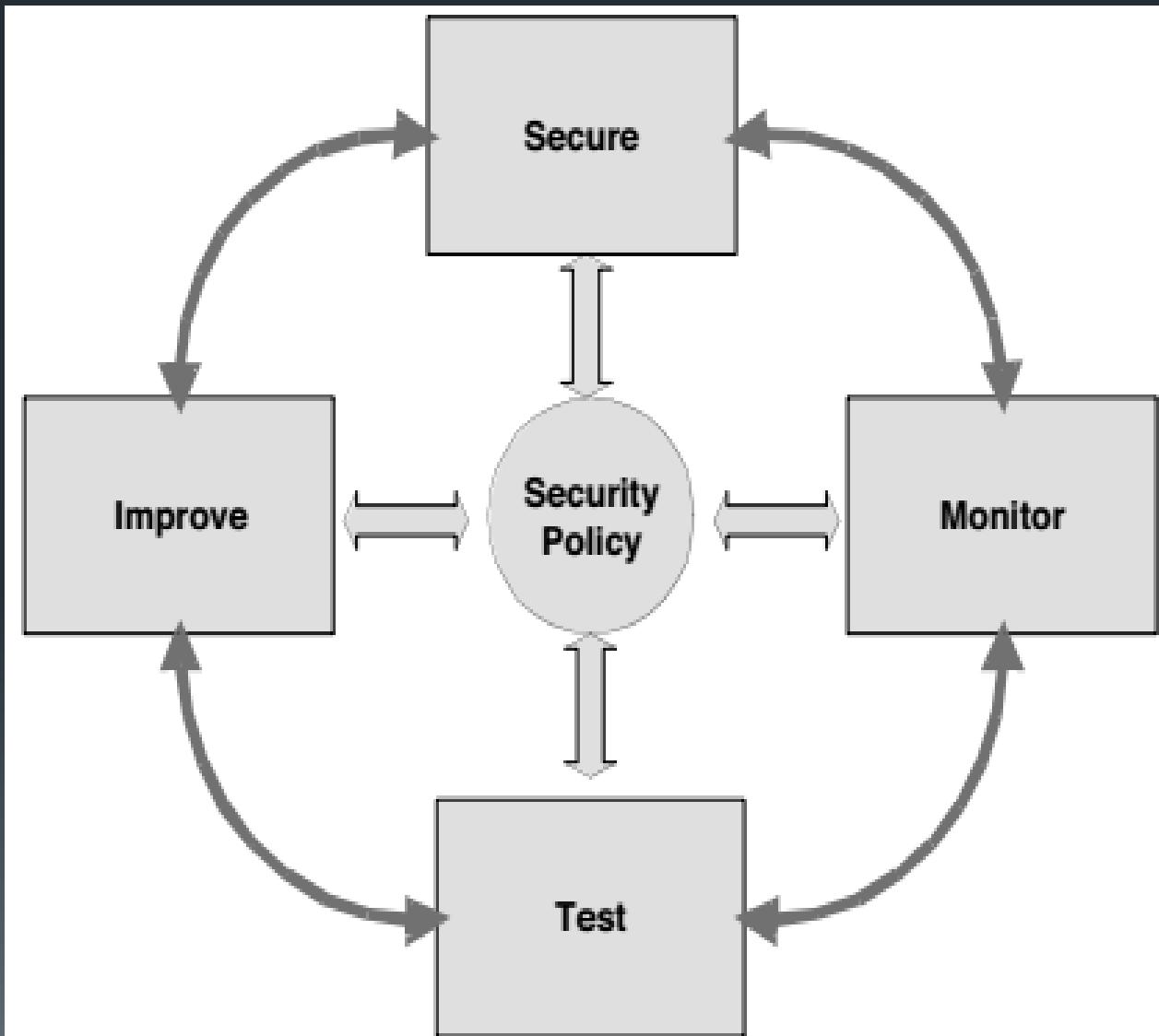
(Read Only)

|                          | Nama           | unit   | hak_akses     | status |
|--------------------------|----------------|--------|---------------|--------|
| <input type="checkbox"/> | Agata Christie | GUDANG | Gudang        | T      |
| <input type="checkbox"/> | Agata Christie | GUDANG | Hotel         | T      |
| <input type="checkbox"/> | Agung BP       | IT     | Front Office  | T      |
| <input type="checkbox"/> | Agung BP       | IT     | Administrator | T      |
| <input type="checkbox"/> | Joni Susilo    | KASIR  | Front Office  | T      |
| <input type="checkbox"/> | Joni Susilo    | KASIR  | Gudang        | T      |

|                          | kodeadm | nama   | alamat | telp   | password             | hakakses   |
|--------------------------|---------|--------|--------|--------|----------------------|------------|
| <input type="checkbox"/> | P00     | ADMIN  | -      | -      | c3VwZXI0ZG1pbm00c3Vr | SUPERADMIN |
| <input type="checkbox"/> | P01     | DONA   | -      | -      | IWJudQ==             | ADMIN      |
| <input type="checkbox"/> | P02     | YUNA   | -      | -      | dG9rb21lcmFo         | ADMIN      |
| *                        | (NULL)  | (NULL) | (NULL) | (NULL) | (NULL)               | (NULL)     |

# Security Wheel / Lingkaran Keamanan

- (buku 2)
- <https://flylib.com/books/en/1.224.1.57/1/>



# Absensi dan Posttest

berikut ini link digunakan untuk posttest dan absensi kehadiran matakuliah keamanan sistem informasi

Percobaan yang diperolehkan: 1

Kuis tidak akan tersedia sampai: Wednesday, 1 September 2021, 10:30 AM

Kuis ini akan ditutup pada Wednesday, 1 September 2021, 12:00 PM

Batas waktu: 10 min

[Tampilkan kuis sekarang](#)

# Jangan Lupa diisi atau update data elearning

21034010527 Tama Putra

▷ Perbesar semua

## ▽ Umum

NPM /NIP/NPT \*

21034010527

V

Nama Lengkap \*

Tama Putra

V

Alamat Email \*

[REDACTED]

V

Tampilan Email

Bolehkan hanya sesama peserta mata kuliah untuk melihat alamat email saya



Kota

Boyolali

Pilih negara

Indonesia



Zona waktu Asia/Jakarta

# **Keamanan Sistem Informasi**

**Agung BP**  
**Pertemuan 2**

1. Perlindungan terhadap virus komputer
2. Pengendalian program terhadap ancaman lainnya :
  - Security attack
  - Hacker
  - Cracker
  - Spyware
  - Spam

## Pembahasan

- Dari sudut pandang sebuah program atau programmer, bagaimana menilai keamanan aplikasi atau program atau komputer itu?

- Prinsip keamanan aplikasi/komputer sama dengan prinsip keamanan informasi, keamanan program diharapkan memberlakukan **kerahasiaan, integritas, dan ketersediaan** sama dengan prinsip keamanan informasi. (Pfleeger, C.P, 1997: chapter 3)

- Tahapan untuk mengevaluasi keamanan program (Joseph Migga, 2005:69) adalah
  1. Menentukan aset informasi yang perlu dilindungi.
  2. Mengevaluasi infrastruktur teknologi untuk menentukan apakah infrastruktur teknologi itu dapat melindungi aset perusahaan dan definisi kelemahan dan risiko terhadap aset-aset yang bersifat kritis.

3. Menggunakan praktik keamanan yang baik, membentuk sebuah organisasi perlindungan strategi yang luas dan merencanakan penanggulangan untuk risiko secara spesifik terhadap aset kritis.

- Tidak ada keamanan komputer atau jaringan atau aplikasi/sistem operasi anda yang akan sempurna 100%, karena hal itu tergantung dari pilihan mana dari elemen keamanan untuk menggunakan sepenuhnya, dan hal itu juga tergantung dari kebutuhan perusahaan yang memiliki sistem komputer atau jaringan.
- (Joseph Migga, 2005:69)

Username:

boyle02

Password:

whatever' or 1=1--

SQL Injection

# Element Keamanan

- Menurut Joseph Migga Kizza, element keamanan terdiri dari :
  1. Kebijakan Keamanan  
Rencana keamanan harus fokus pada orang-orang yang menggunakan sistem dengan membagi mereka menjadi dua kelompok, orang-orang di tim keamanan dan pengguna.

## **Element Keamanan**

## 2. The Access Control

Akses control ini dapat diartikan pengendalian atau memberikan wewenang terhadap orang-orang yang berhak dalam mengendalikan suatu sistem.

## 3. Strong Encryption Algorithms

## 4. Authentication Techniques

# Element Keamanan

- Banyak orang yang telah menaruh masa depan perusahaannya melalui e-commerce, ketika hal itu terjadi maka enkripsi data harus dan teknik otentikasi harus benar. Karena semakin banyak orang yang online untuk membeli dan menjual barang dagangan mereka, mereka membutuhkan algoritma yang kuat dan terpercaya, yang akan membuat transaksi tersebut aman.

## Element Keamanan

Beberapa teknik tentang pengamanan online yang ada saat ini adalah

- *Kerberos* adalah sebuah skema manajemen kunci yang mengotentikasi pelaku yang ingin berkomunikasi satu sama lainnya. Tugas server Kerberos adalah untuk menjamin identitas dengan mempertahankan database peserta, proses, server, orang, sistem, dan informasi lainnya.

## Element Keamanan

- *IPSec menyediakan kemampuan untuk menjamin keamanan data dalam jaringan komunikasi. Dengan mengenkripsi dan atau otentikasi semua lalu lintas pada tingkat jaringan Internet Protocol (IP). Hal ini membuat semua aplikasi internet termasuk client-server, e-mail, transfer file, dan akses Web yang aman.*

## **Element Keamanan**

- *SSL (secure socket layer)* adalah sistem enkripsi fleksibel yang beroperasi pada layer TCP / IP untuk mengotentikasi server dan klien terpilih/yang sudah diotentikasi. Sehingga dalam melakukan, akhirnya SSL akan memberikan kunci rahasia ke klien dan penggunaan server kemudian mengirim pesan terenkripsi.

## Element Keamanan

- S/Key adalah skema one-time password, setiap password yang digunakan dalam sistem ini digunakan hanya untuk satu otentikasi.
- ANSI X9.9 adalah standar perbankan AS untuk otentikasi transaksi keuangan. Algoritma Ini menggunakan otentikasi pesan yang disebut DES-MAC berdasarkan DES.

## Element Keamanan

- *ISO 8730* setara dengan ANSI X9.9
- *Indirect OTP* (one-time password) adalah suatu teknik otentikasi yang menghasilkan dan menggunakan password sekali dan kemudian membuangnya.

## Element Keamanan

## 5. Auditing

Tujuan audit adalah untuk menemukan masalah sebanyak mungkin dalam sistem sebelum penyusup menemukan kelemahan sistem anda. Anda bisa melakukan audit secara bebas, semakin sulit sistem anda ditembus maka akan semakin baik keamanan informasi.

# Element Keamanan

# Slide 2

---

Oleh :  
Agung Brastama Putra

# Pembahasan

---

- Aspek-Aspek Keamanan
- Keamanan Fisik

# Buku

---

- Salomon, David. 2010. Elements of Computer Security. Springer : Springer London Dordrecht Heidelberg New York.
- Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, Matt Bishop. 2010. Insider Threats in Cyber Security. Springer : Springer London Dordrecht Heidelberg New York.

# Aspek-Aspek Keamanan

---

- Masalah keamanan dari dalam atau internal amat sangat lebih berbahaya dibandingkan dengan ancaman dari luar.
- Karena orang dalam/internal mempunyai kemampuan mengakses “informasi” dari dalam tanpa tercurigai.

- 
- Dalam sebuah penelitian insider didefinisikan sebagai seseorang dengan akses, hak istimewa atau pengetahuan tentang layanan sistem informasi.
  - Contohnya :

- 
- Penyalahgunaan Hak Akses
  - Penggunaan komputer orang lain.
  - Penggunaan ID orang lain.

# Jadi orang dalam adalah

---

- Seseorang dengan sah meng-akses ke sumber daya.
- Seseorang yang sebagian atau sepenuhnya telah dipercaya.
- Individu yang telah atau memiliki hak akses ke sumber daya.

# Ancaman Orang Dalam

---

- Pengguna sistem yang dapat menyalahgunakan hak istimewa
- Seorang individu dengan akses resmi yang mungkin mencoba atau yang dapat bantuan dari luar, dalam melakukan penghapusan atau sabotase terhadap aset kritis secara tidak sah.

---

# Deteksi dan Mengurangi Ancaman

# Detection

---

- Data berlebihan,
- Data tidak valid,
- Kehilangan data.

# Mitigation

---

- Monitoring proses.
- Kebijakan jelas memainkan peran penting sehubungan dengan ancaman dari dalam, karena menentukan batas-batas antara boleh dan tidak boleh perilaku, baik pada tingkat teknis dan non-teknis.

- 
- Hak Akses tiap orang, bagian dan jabatan untuk memasuki sebuah sistem.
  - Diadakan Audit.

# Faktor dan Kepatuhan Manusia

---

- Terdapat banyak kesalahan tentang asumsi Faktor dan Kepatuhan Manusia, antara lain
  1. Ketika diadakan audit hanya berfokus untuk mencari-cari kesalahan dalam kebijakan.

- 
- 2. Monitoring dilakukan secara kelompok tertentu atau individu-individu tertentu yang mempunyai tingkah yang berbeda, dan tidak keseluruhan.
  - 3. Menanamkan budaya keamanan yang diinginkan oleh perusahaan.

# Seharusnya....

---

- 1) kebijakan perlu dibuat lebih mudah dikelola, dan
  - 2) diperlukan pengkajian ulang terhadap kebijakan-kebijakan yang berlebihan.
- Idealnya adalah kebijakan keamanan konsisten berkaitan dengan perilaku, dan sesuai dengan proses bisnis, dan nilai-nilai organisasi dan norma-norma.

---

# Keamanan Fisik

- 
- Lonjakan dalam listrik, sering disebabkan oleh petir, sehingga membuat komponen di komputer menjadi tidak stabil.
  - Solusi : Menggunakan uninterruptible power Supply (UPS).

- 
- Pertanyaanya bagaimana apabila power computer tiba-tiba mati????

- 
- Banyak di perusahaan data dapat dihapus jika terutama jika data sensitif dicuri atau rusak. Kerusakan dapat disengaja, ditimbulkan oleh seorang kriminal atau karyawan puas, atau disebabkan oleh api, kegagalan daya atau rusaknya pendingin udara.

- 
- Solusinya, kalau hal itu terjadi dalam rumah maka ditambahkan alarm dan untuk komputernya digunakan UPS.
  - Solusi untuk perusahaan/Entitas komersial, dengan pengendalian akses, dioperasikan kartu kunci, kamera keamanan, dan sistem otomatis api (menggunakan gas bukannya air jika mungkin).

- 
- Fasilitas yang menggunakan elektronik kunci dan kunci atau identifikasi fisik lainnya perangkat untuk membatasi akses ke daerah-daerah tertentu harus mempertimbangkan masalah berikut, dikenal sebagai piggybacking atau tailgating.

- 
- Medan magnet. Hard disk adalah media penyimpanan. Data yang disimpan dalam titik-titik magnetik yang kecil pada disk dan itu sangat sensitif terhadap medan magnet.

- 
- Keprihatinan terkait adalah listrik statis. Berjalan di atas karpet sering mengakibatkan listrik statis dikumpulkan di sepatu dan pakaian.
  - Daya listrik habis ketika menyentuh sebuah konduktor dan dapat merusak peralatan listrik yang halus.
  - Ruang komputer harus memiliki ubin lantai atau karpet setidaknya anti-statis

- 
- Hard copy. Media telah menggembarkan the paperless office untuk beberapa dekade, tetapi kita masih menggunakan kertas.



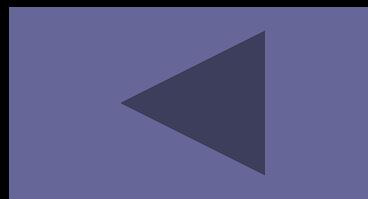
- 
- Memata-matai/Spyware. Spyware, ancaman penting, tetapi memata-matai juga dapat dilakukan dengan cara tradisional, oleh orang.
  - Data integrity



# DRP (Disaster Recovery Planning)

---

- Rencana pemulihan bencana adalah bagian penting dari setiap organisasi, apakah komersial, amal atau pemerintah.
- Rincian langkah-langkah yang diperlukan untuk cepat mengembalikan kemampuan teknis dan jasa setelah gangguan atau bencana.
- Ide dalam rencana tersebut adalah untuk meminimalkan dampak bencana di organisasi.
- DRP biasanya hanya disebut DRC (Disaster Recovery)



# Slide 3 – Keamanan Sistem Informasi

Agung Brastama Putra

# Pembahasan

---

- Keamanan Sistem Operasi
- File Protection Mechanisms in operating System

# Referensi Buku

**Charles P. Pfleeger - Security in Computing, Fourth Edition (Chapter 4)**

---

Morrie Gasser - Building A secure Computer System (Chapter 4)

- 
- Sistem operasi pertama digunakan untuk keperluan-keperluan sederhana, yang disebut eksekutif, yang dirancang untuk membantu programmer individu dan untuk memperlancar transisi dari satu pengguna lain

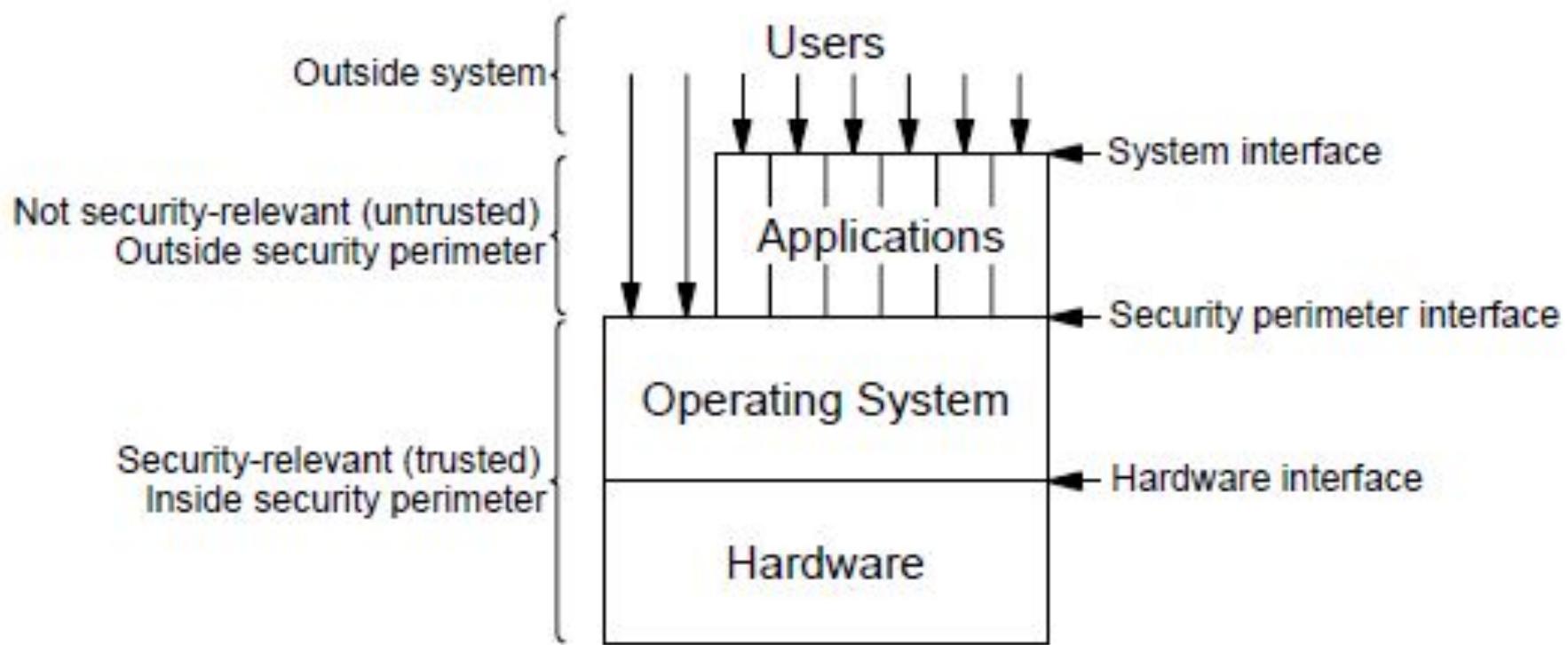
- 
- Sistem operasi mengambil peran yang lebih luas dalam konsep multiprogramming. Menyadari bahwa dua pengguna dapat interleave akses ke sumber daya sistem komputasi tunggal, peneliti mengembangkan konsep-konsep seperti penjadwalan, berbagi, dan penggunaan paralel.
  - Sistem operasi Multiprogrammed, juga digunakan untuk monitor, mengawasi setiap eksekusi program.
  - Monitor mengambil peran aktif, sedangkan eksekutif yang pasif. Artinya, seorang eksekutif tinggal di belakang layar, menunggu untuk dipanggil ke dalam pelayanan oleh pengguna yang meminta.

- 
- ◉ Namun monitor aktif menegaskan kontrol dari sistem komputasi dan memberikan sumber daya untuk pengguna hanya ketika permintaan konsisten dengan baik penggunaan umum sistem.
  - ◉ Demikian pula, eksekutif menunggu permintaan dan memberikan layanan.
  - ◉ Monitor mempertahankan kontrol atas semua sumber daya, memungkinkan atau menolak komputasi semua dan meminjamkan sumber daya untuk pengguna karena mereka membutuhkan mereka.

# ***Morrie Gasser - Building A secure Computer System (Chapter 4)***

---

# Sistem komputer secara general



# Keterangan Gambar

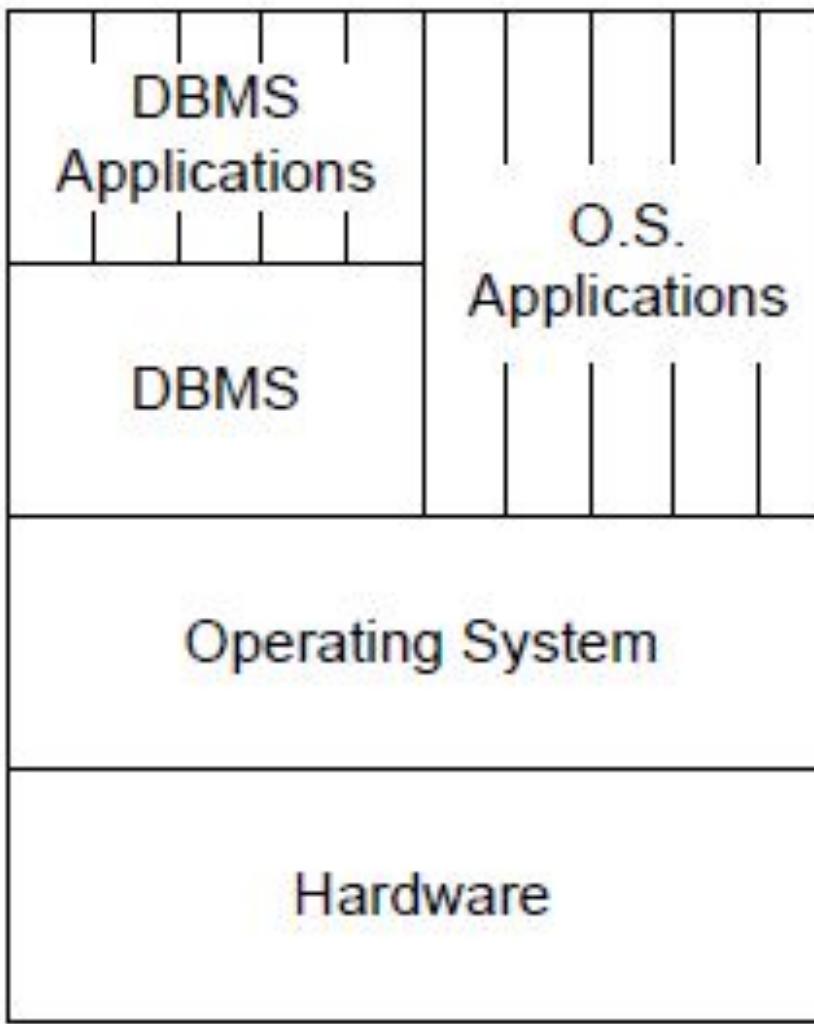
---

- Setiap lapisan harus tunduk pada aturan/cara mengakses yang diterapkan pada lapisan dibawahnya.
- Aplikasi mengakses sistem operasi melalui perimeter dengan cara panggilan sistem.
- Para pengguna berada di luar sistem.
- Mereka mengakses sistem melalui aplikasi atau, dapat berkomunikasi langsung dengan sistem operasi.

# Konsep Perbedaan hardware dan sistem operasi dalam paradigma lama

- Perbedaan antara perangkat keras dan sistem operasi adalah jelas:  
Sistem operasi ini diimplementasikan dengan bit dalam memori yang dapat dengan mudah diubah, dan hardware dilaksanakan dengan sirkuit yang bersifat tetap atau tidak dapat dipindahkan secara mudah.

- 
- Sekarang orang-orang lebih banyak mengenal dengan nama hardware dan software.
  - Dengan hardware yang merupakan perangkat keras contohnya RAM, Hardisk dll
  - Untuk software/perangkat lunak meliputi aplikasi-aplikasi



# ***THE REFERENCE MONITOR AND SECURITY KERNELS***

---

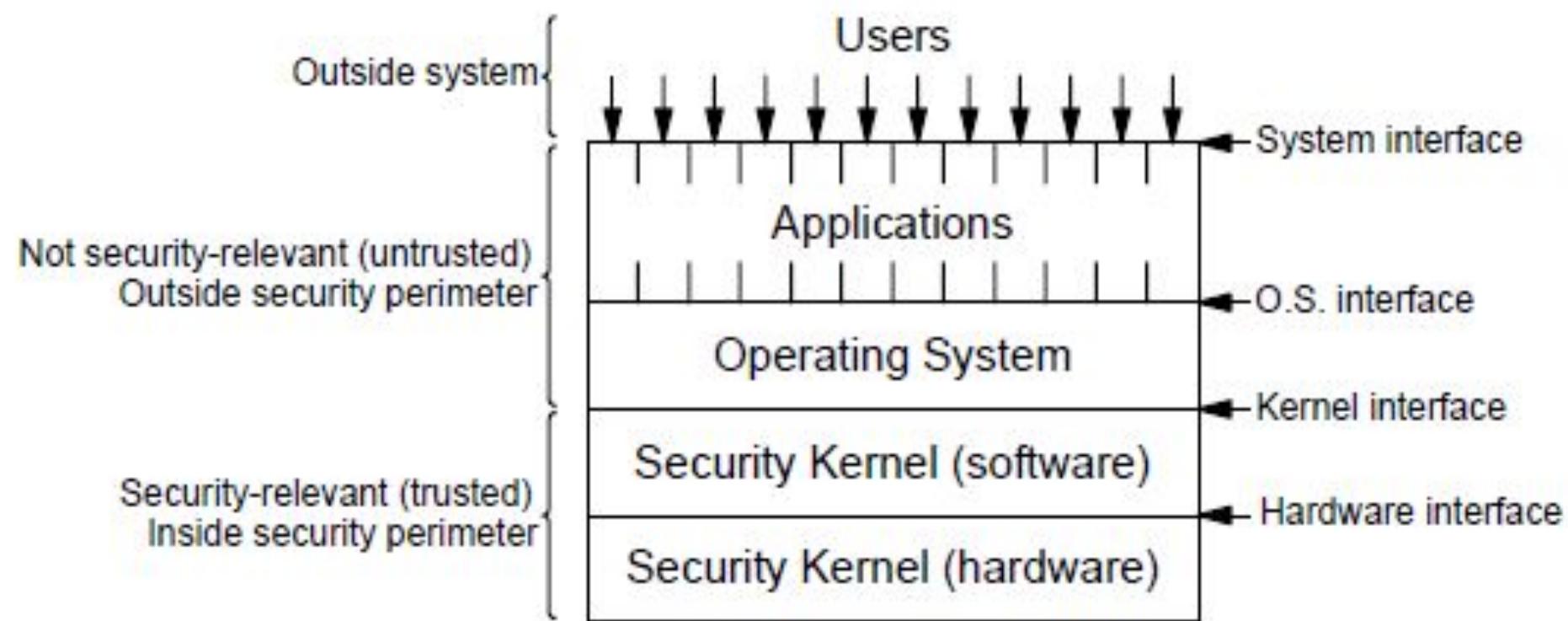
- 
- Keamanan dapat ditingkatkan dengan mengubah arsitektur fundamental.
  - Tetapi, untuk perlindungan secara maksimal pada akses informasi yang sangat sensitif, diperlukan strategi pembangunan yang ketat dan sistem arsitektur khusus.

- 
- Pendekatan keamanan kernel adalah metode membangun sebuah sistem operasi yang menghindari masalah keamanan yang melekat dalam desain konvensional  
(Ames, Gasser, dan Schell 1983)

- 
- Kernel adalah suatu perangkat lunak yang menjadi bagian utama dari sebuah sistem operasi.
  - Tugasnya melayani bermacam program aplikasi untuk mengakses perangkat keras komputer secara aman.

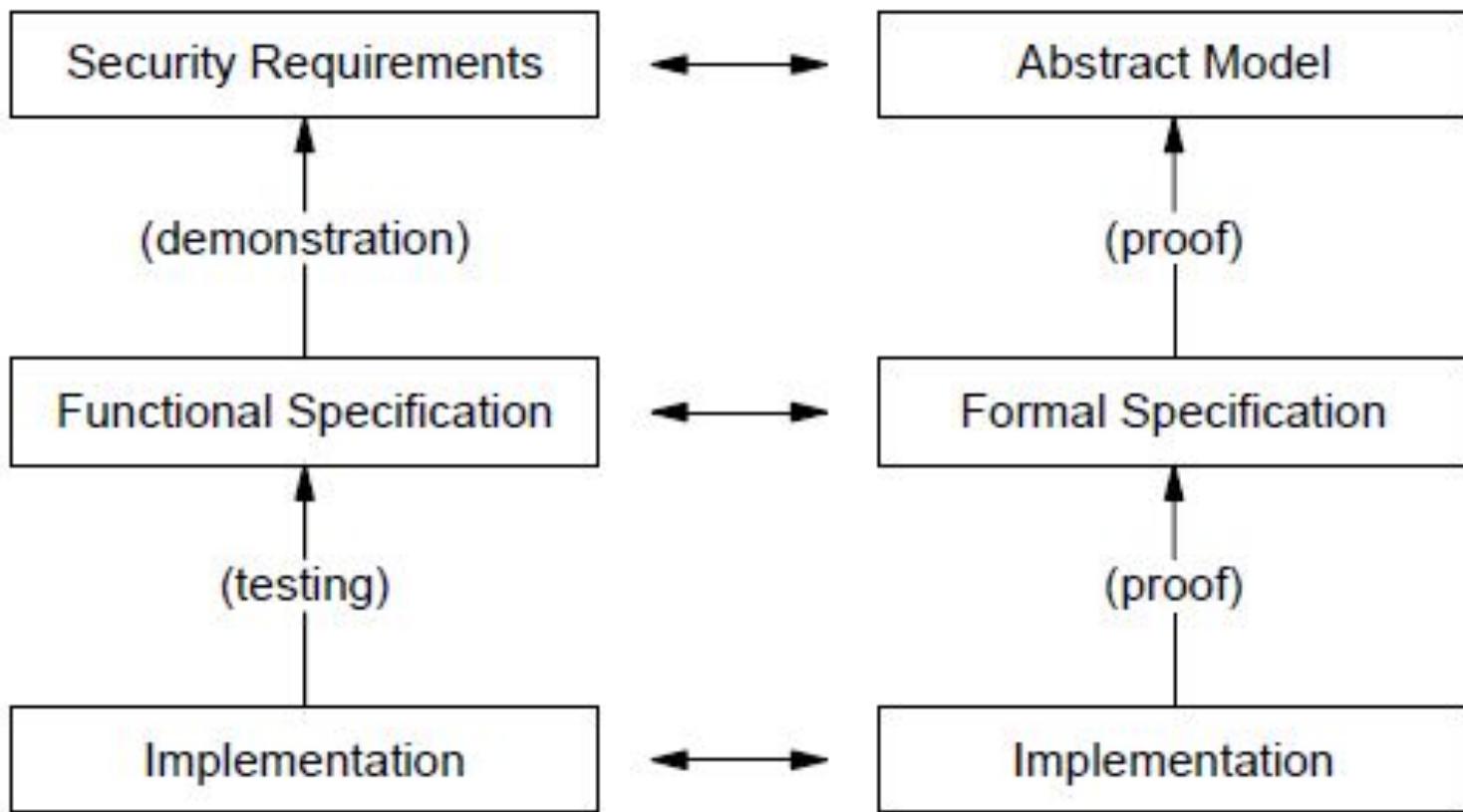
- 
- Karena akses terhadap perangkat keras terbatas, sedangkan ada lebih dari satu program yang harus dilayani dalam waktu yang bersamaan, maka kernel juga bertugas untuk mengatur kapan dan berapa lama suatu program dapat menggunakan satu bagian perangkat keras tersebut. Hal tersebut dinamakan sebagai **multiplexing**.

- 
- ◉ Kombinasi dari monitor hardware dan software merupakan cara yang efektif dalam menangani keamanan sistem operasi.
  - ◉ Keputusan Hak Akses ditentukan oleh kebijakan didasarkan pada sensifitas informasi/data.



# System Development Process for a Secure System

## Informal Development Path      Formal Development Path



- 
- Aspek keamanan dari proses pengembangan sistem yang ditunjukkan dalam dua jalur paralel.
  - Jalur informal konvensional, spesifikasi fungsional dan implementasi yang terbukti memenuhi persyaratan keamanan melalui langkah-langkah yang melibatkan korespondensi demonstrasi dan pengujian.
  - Jalur formal, dengan menggunakan teknik matematika, adalah digunakan untuk sistem di mana tingkat kemanan yang sangat tinggi dan menjamin mengenai kontrol keamanan yang diinginkan.

# **File Protection Mechanisms**

---

**Charles P. Pfleeger - Security in  
Computing, Fourth Edition**

# Skema Keamanan File

---

- **All None Protection :**
- Setiap pengguna dapat membaca, memodifikasi, atau menghapus file milik pengguna lain.

- 
- Administrator biasanya akan memproteksi file-file bersifat informasi yang sensitif, dengan cara password untuk dapat mengakses file (membaca, menulis, atau menghapus) dan memberikan kontrol penuh atas sistem untuk semua file.
  - Tapi di lain waktu password dikontrol hanya dapat menulis dan menghapus untuk user lain.

---

## ◎ Group Protection

## ◎ Individual Permissions

- Persistent Permission :
  - Kartu identitas
  - Finger Print
- Temporary Acquired Permission
  - Sistem Operasi Linux menerapkan 3 lapisan dalam pengaksesan file (Read, Write, Execute) dan dikelompokkan berdasarkan User, Group dan Other.

- 
- **Per-Object and Per-User Protection**
  - setiap pengguna harus menentukan setiap data yang akan diakses. Untuk pengguna baru perlu ditambahkan, hak-hak khusus yang dalam mengakses data sehingga file/data.
  - Jadi satu file bisa terdiri dari banyak user dengan hak akses sendiri-sendiri.

# Protection File in Linux

**drwxrwxrwx**

d = Directory

r = Read

w = Write

x = Execute

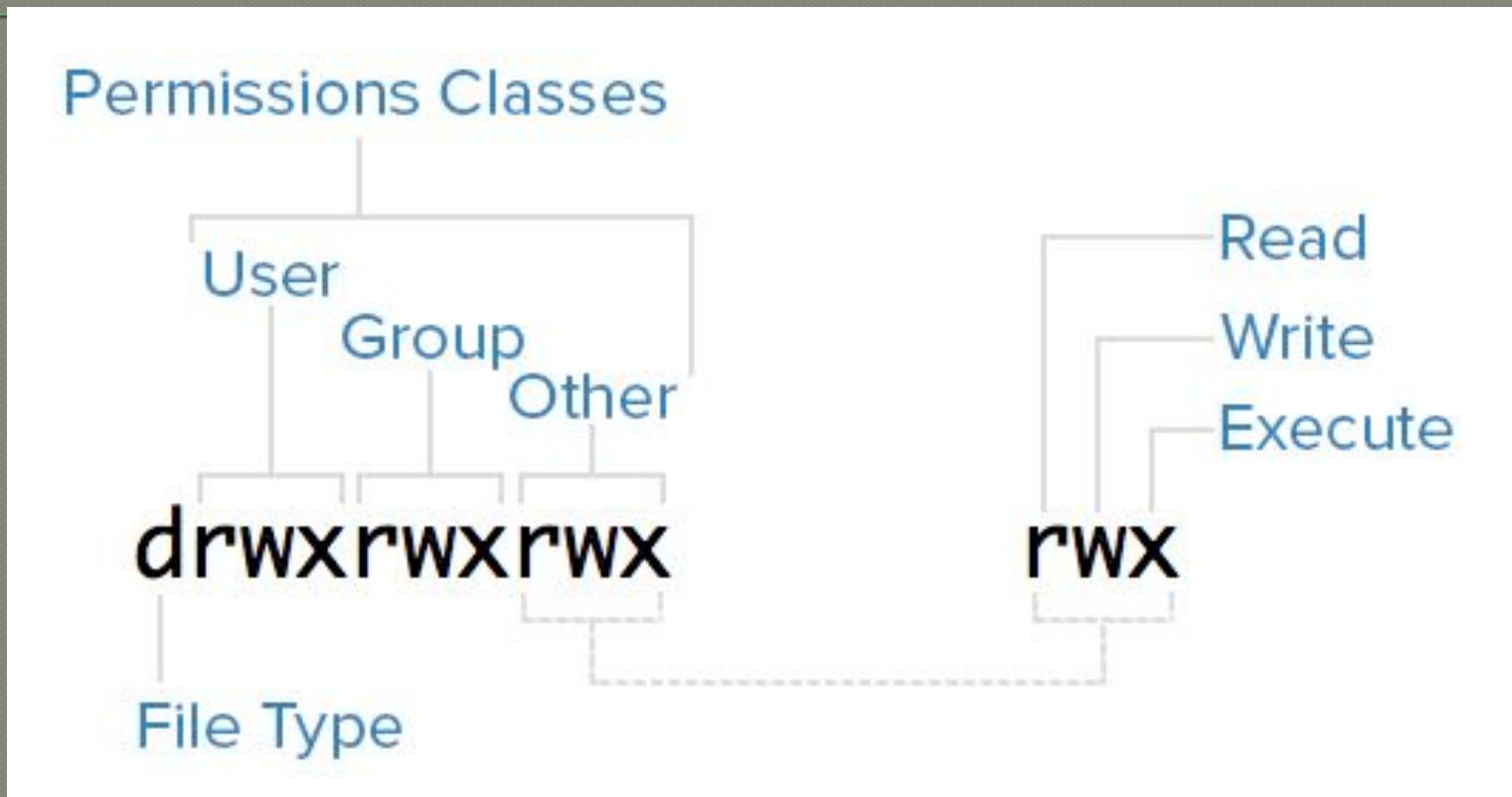
**chmod 777**

**rwx|rwx|rwx**

Owner|Group|Others

|   |     |     |
|---|-----|-----|
| 7 | rwx | 111 |
| 6 | rw- | 110 |
| 5 | r-x | 101 |
| 4 | r-- | 100 |
| 3 | -wx | 011 |
| 2 | -w- | 010 |
| 1 | --x | 001 |
| 0 | --- | 000 |

# Permission Linux



ref:

<https://linuxize.com/post/how-to-add-user-to-group-in-linux/#:~:text=Linux%20groups%20are%20organization%20units,they%20users%20within%20the%20group.>

# in Windows

User Accounts

Control Panel Home

Manage your credentials

Create a password reset disk

Configure advanced user profile properties

Change my environment variables

Make changes to your user account

Make changes to my account in PC settings

Lenovo Local Account Administrator

Change your account name

Change your account type

Manage another account

Change User Account Control settings

Search Control Panel

9:35 AM 2/21/2022

Computer Management

File Action View Help

Actions

Groups

New Group...

Refresh

Export List...

View >

Arrange Icons >

Line up Icons

Help

Creates a new local group.

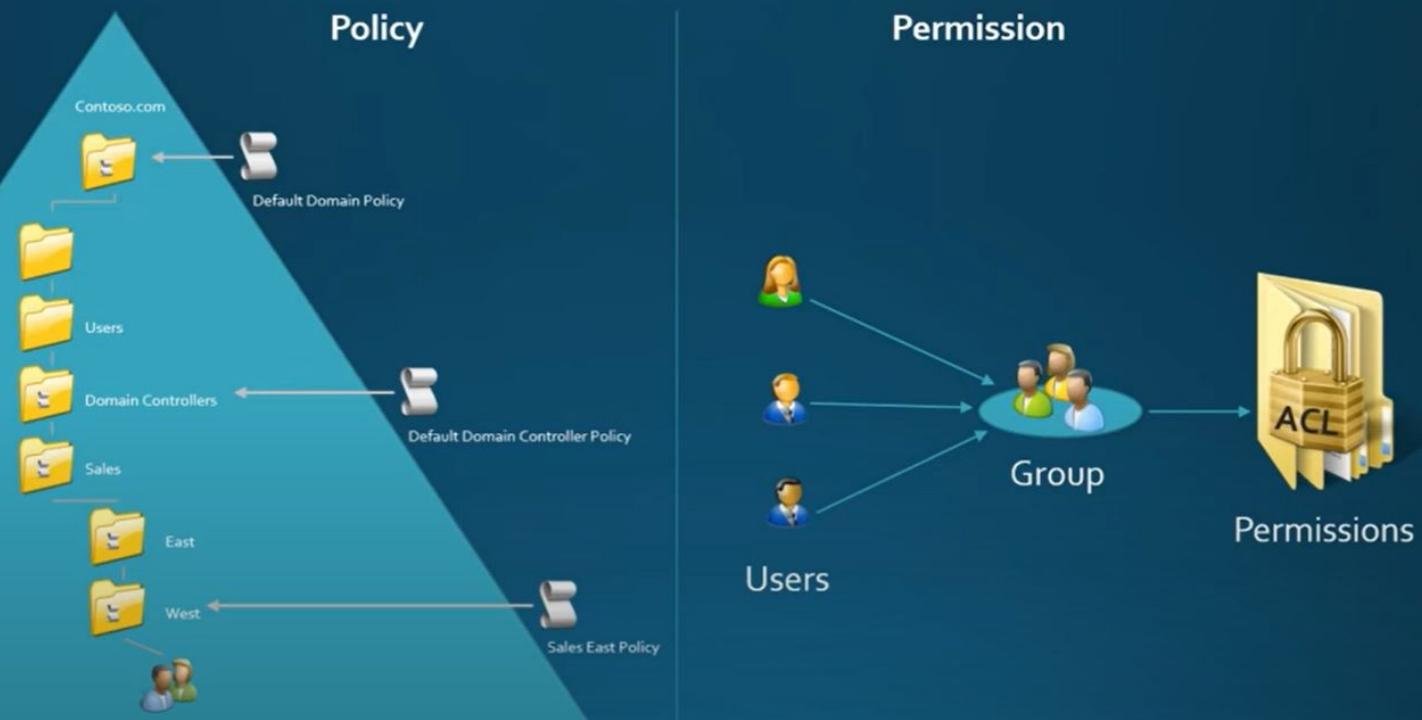
Name Description

- Access Control Assist... Members of this group can remot...
- Administrators Administrators have complete an...
- Backup Operators Backup Operators can override se...
- Cryptographic Operat... Members are authorized to perfor...
- Distributed COM Users Members are allowed to launch, a...
- Event Log Readers Members of this group can read e...
- Guests Guests have the same access as m...
- Hyper-V Administrators Members of this group have com...
- IIS\_IUSRS Built-in group used by Internet Inf...
- Network Configuratio... Members in this group can have s...
- Performance Log Users Members of this group may sche...
- Performance Monitor ... Members of this group can acces...
- Power Users Power Users are included for back...
- Remote Desktop Users Members in this group are grante...
- Remote Management... Members of this group can acces...
- Replicator Supports file replication in a dom...
- System Managed Acc... Members of this group are mana...
- Users Users are prevented from making ...
- \_vmware\_ VMware User Group

Ref: <https://www.youtube.com/watch?v=GD-jxhocJZU>

Objective 5.3 - Creating and Managing Groups and OUs on Windows Server 2012 R2

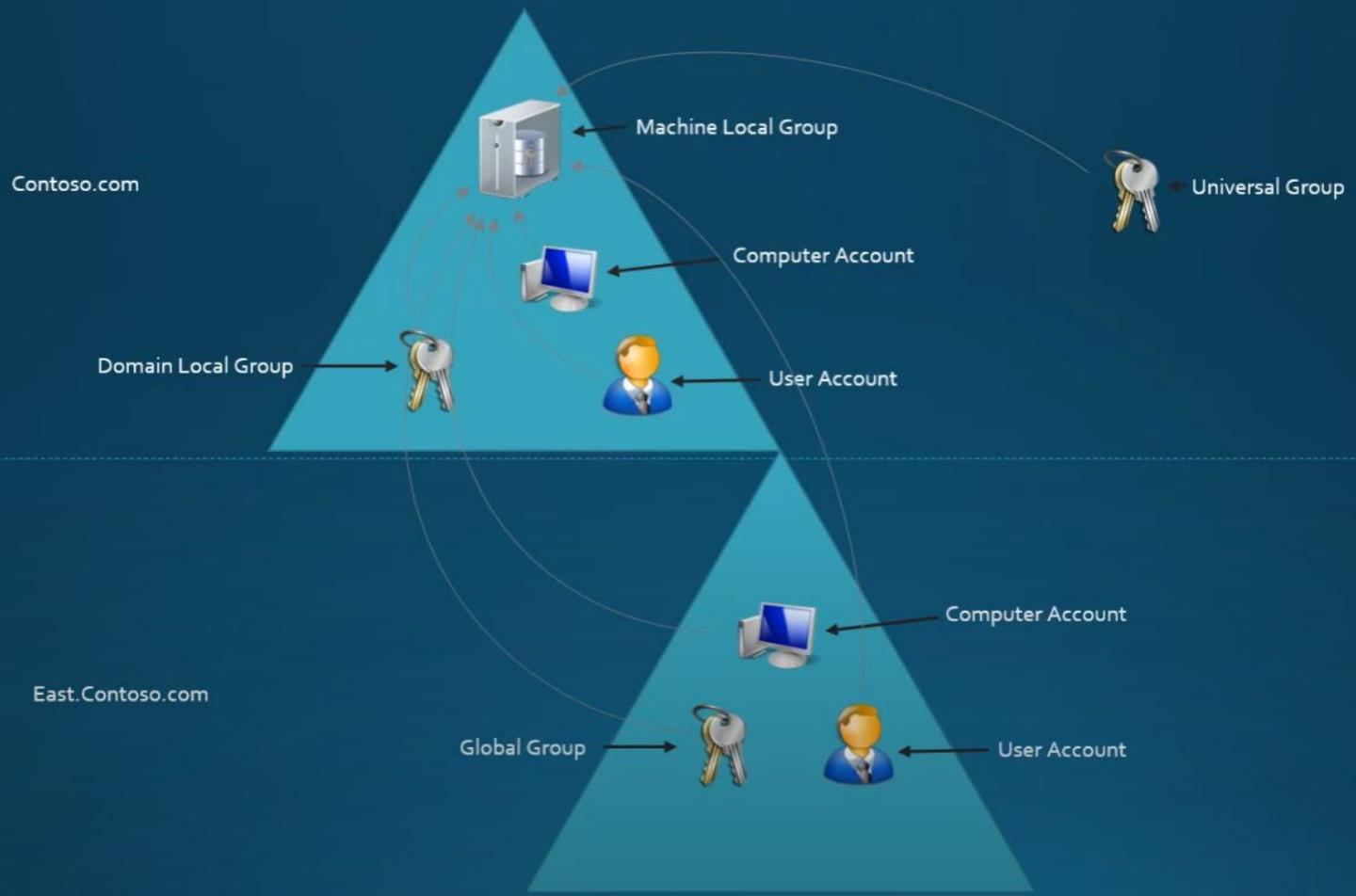
# Organizational Units vs. Groups



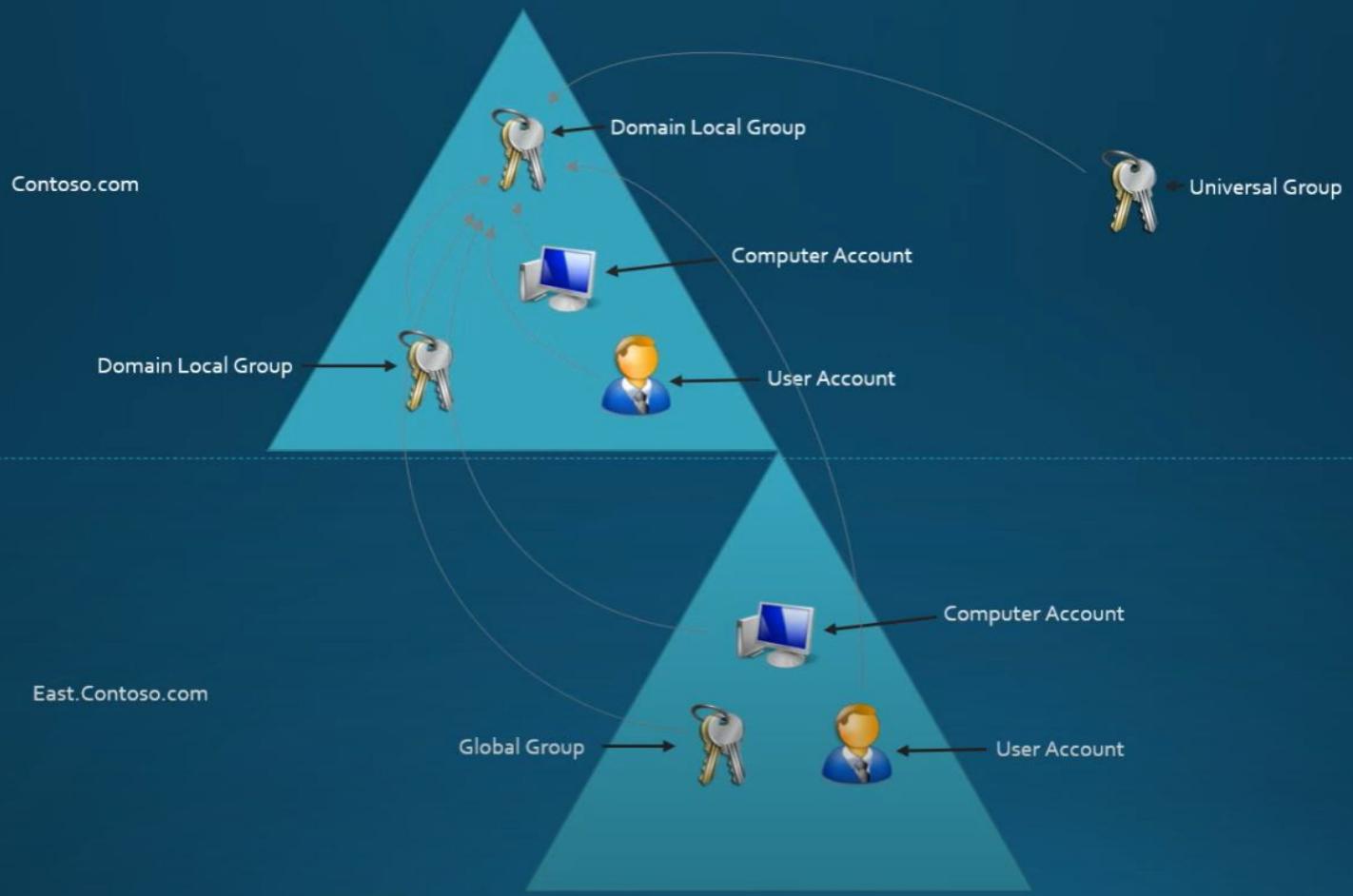
# Creating Groups

- GUI
  - ADUC – Active Directory Users and Computers
  - ADAC – Active Directory Administrative Center
- Command Line
  - DS Command
    - dsadd group <GroupDN>
  - PowerShell
    - New-ADGroup –Name <Group Name> -SamAccountName <SAM name> –GroupCategory Distribution|Security –GroupScope DomainLocal|Global|Universal –Path <distinguished name>

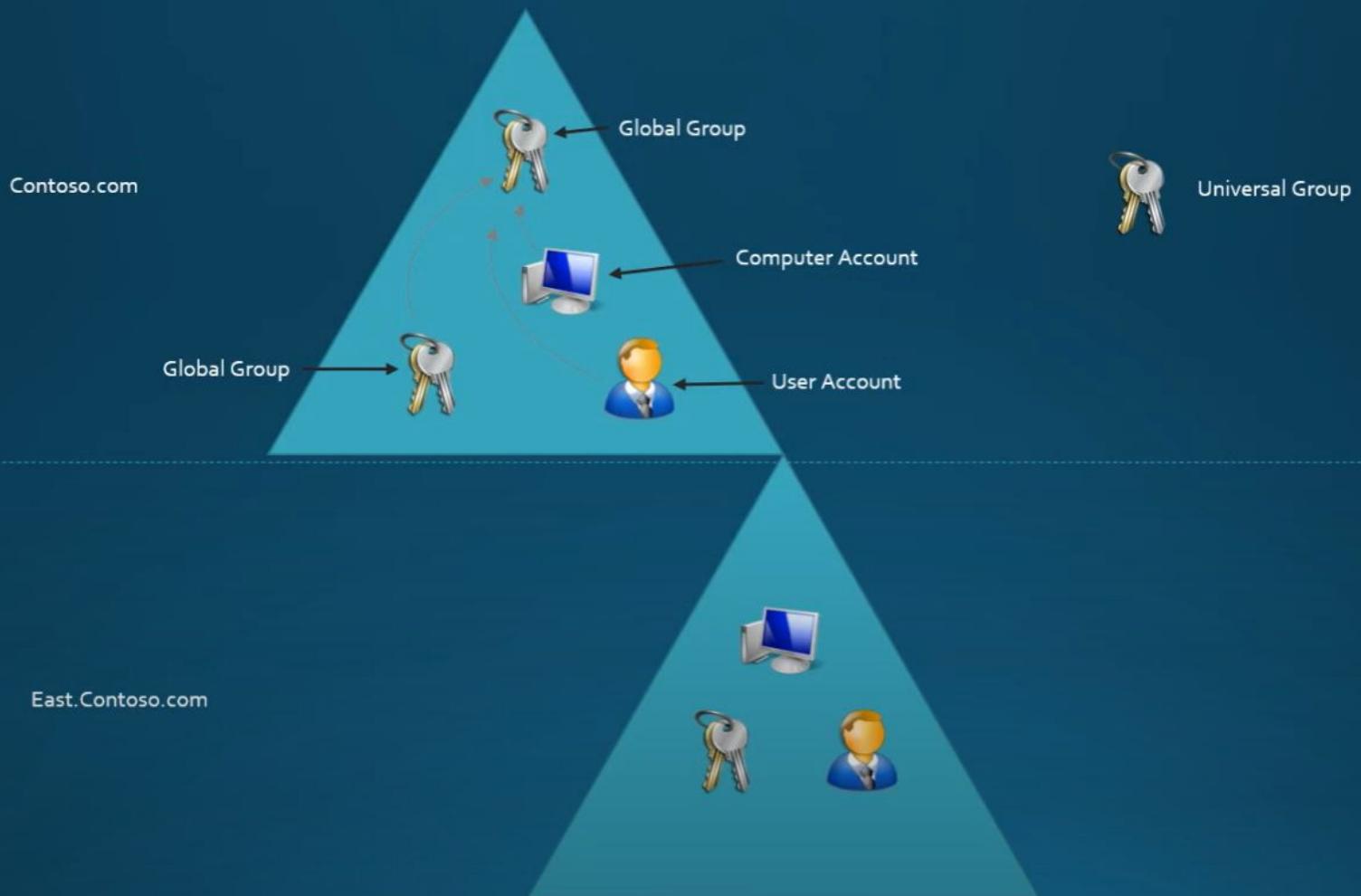
# Machine Local Groups



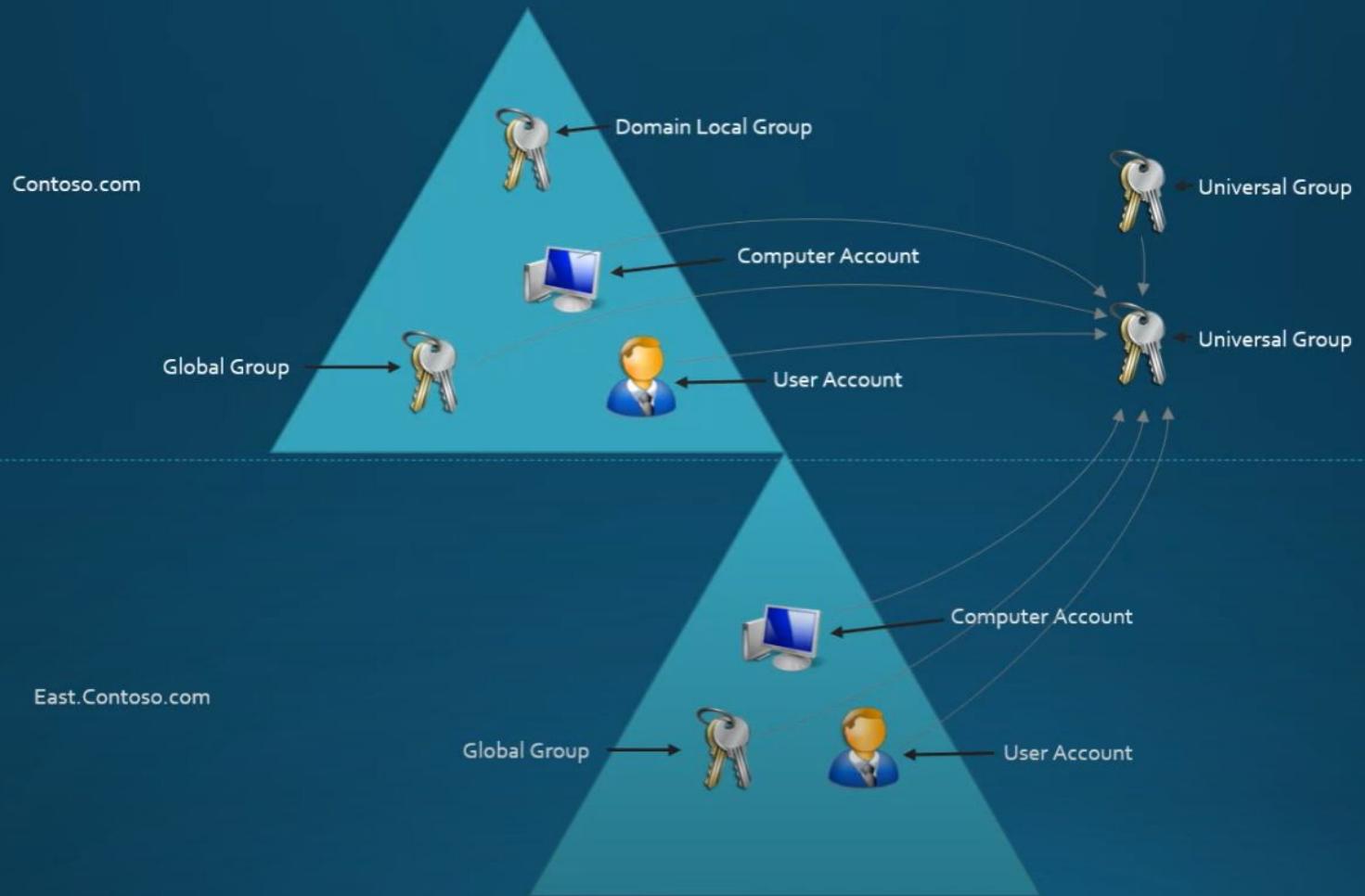
# Domain Local Groups



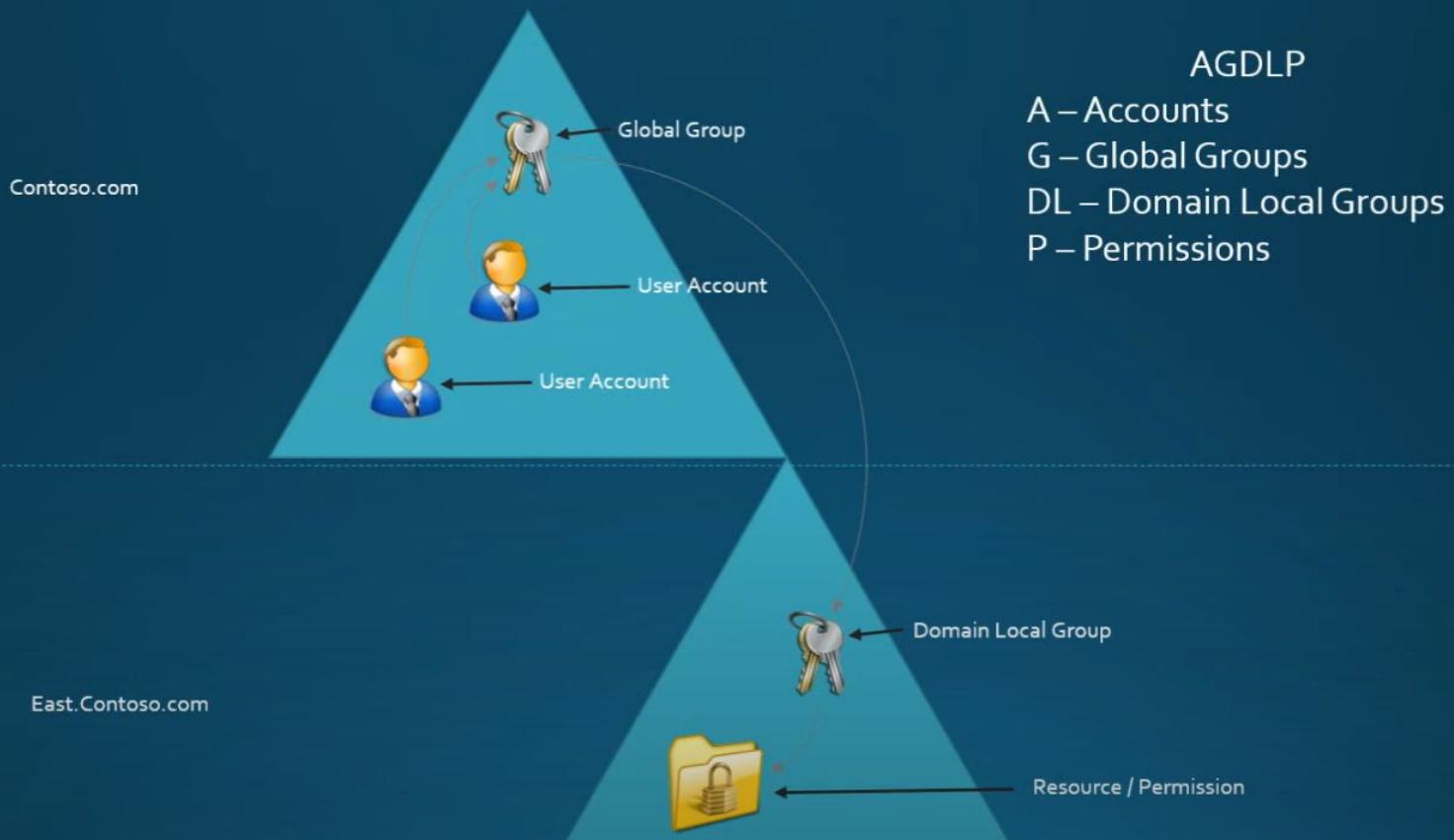
# Global Groups



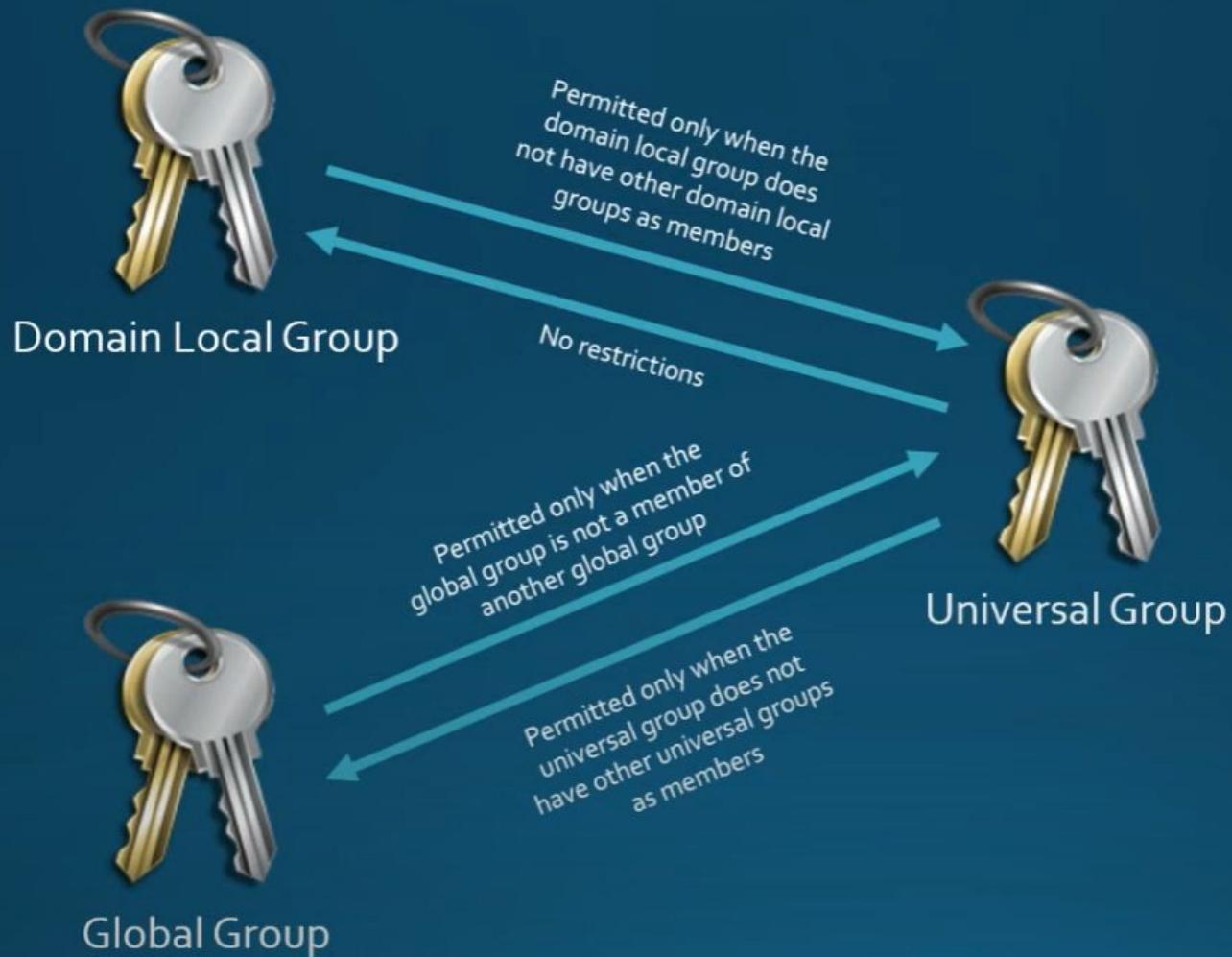
# Universal Groups



# Nesting Groups



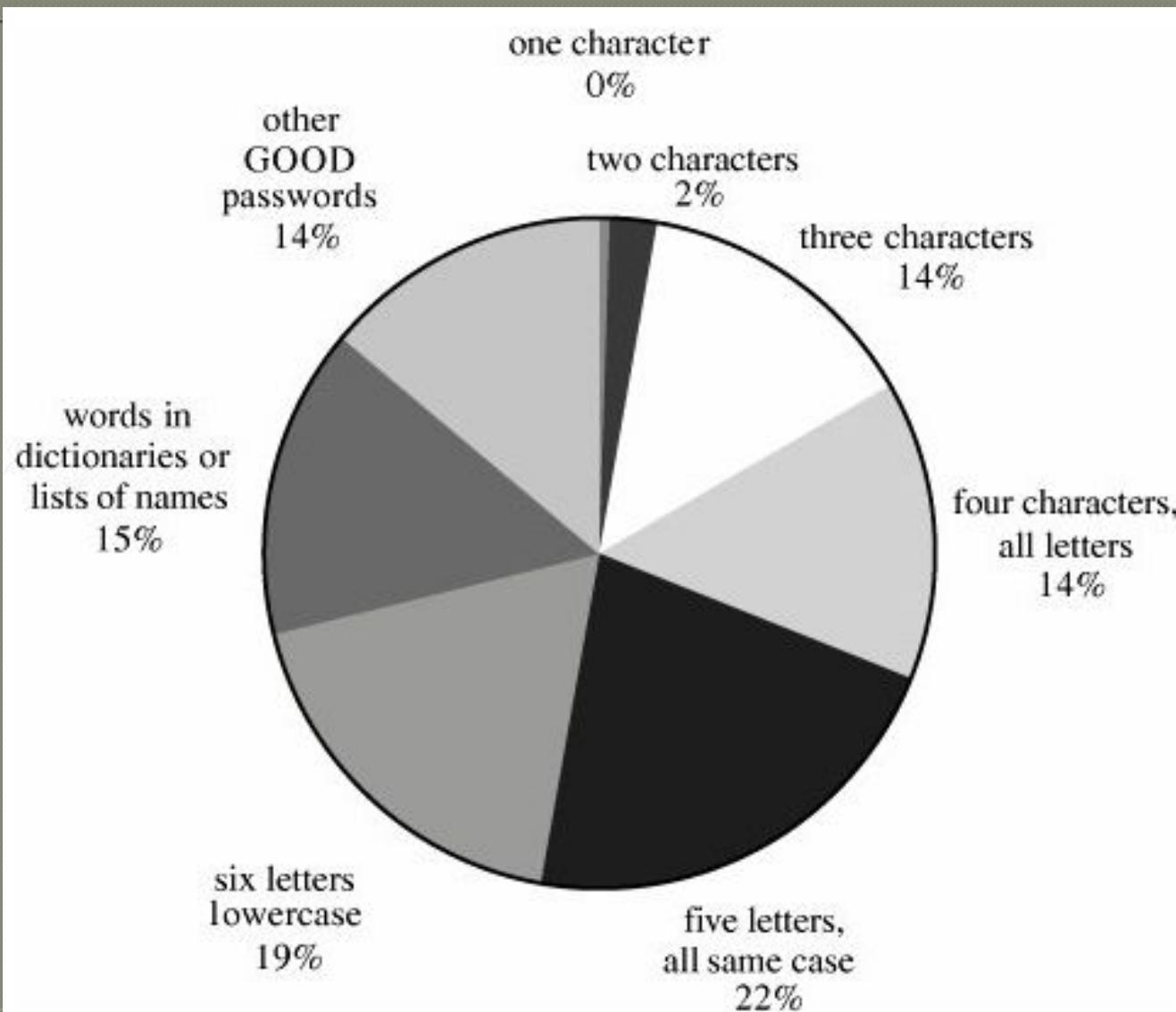
# Group Conversion



- 
- ④ Mekanisme otentikasi menggunakan salah satu dari tiga cara untuk mengkonfirmasi identitas pengguna, sebagai berikut :
    1. **Something the user knows** : Password, PIN, pass-phrases, contohnya nama orang tua, nomor telp, tgl lahir dll.
    2. **Something the user has** : Identity badges, physical keys, a driver's license, or a uniform are common examples of things people have that make them recognizable.

- 
3. **Something the user is :** These authenticators, called biometrics, are based on a physical characteristic of the user, such as a fingerprint, the pattern of a person's voice, or a face (picture).

# Users' Password Choices



# Information Security Standards, Regulations, and Compliance

Agung Brastama Putra

# Information Security Standart

- Keamanan informasi di dunia didasarkan pada standar keamanan.
- Standar-standar keamanan mengatur apa yang dianggap aman dan apa yang tidak.
- Selama mengelola lingkungan Anda, Anda pasti akan menemukan standar ini.
- Ini akan sangat bermanfaat bagi Anda jika Anda memahami standar ini, tahu siapa mengatur mereka, dan memahami mengapa mereka didirikan.

- Sebelum kita dapat membahas standar keamanan informasi, pertama kita harus pastikan bahwa anda tahu sedikit tentang organisasi yang menetapkan standar tersebut.
- Organisasi-organisasi yang umumnya menetapkan standar keamanan internasional di organisasi.
- Organisasi yang menetapkan standar keamanan informasi adalah ISO, IANA, NIST, dan IETF.

# ISO

- ISO = the International Organization for Standardization.
- ISO adalah salah satu yang terbesar di seluruh dunia standar organisasi.
- ISO memiliki kantor di seluruh dunia, tetapi markas pusatnya adalah berlokasi di Jenewa, Swiss.
- ISO menetapkan standar untuk informasi keamanan, serta industri lainnya.
- situs Web-nya di [www.iso.org](http://www.iso.org).

# NIST

- The NIST is the National Institute of Standards and Technology.
- Adalah badan pemerintah yang didirikan pada 1901.
- Badan ini bagian dari Amerika Serikat Departemen Perdagangan.
- NIST memiliki dua lokasi utama di Maryland dan Colorado.
- NIST menetapkan standar untuk semua bidang teknologi, bukan hanya teknologi informasi.
- situs Web-nya di [www.nist.org](http://www.nist.org).

# IETF

- The IETF is the Internet Engineering Task Force.
- IETF adalah Masyarakat internasional yang menetapkan standar untuk Internet.
- IETF dibagi dalam beberapa entitas yang disebut kelompok kerja.
- Setiap kelompok kerja memiliki topik tertentu atau teknologi yang bertanggung jawab.
- Setiap kelompok juga memiliki piagam yang berbeda. kelompok itu juga memiliki direksi.
- IETF memiliki keanggotaan terbuka, sehingga siapapun dapat bergabung dan menghadiri pertemuan-pertemuan reguler.
- Situs Web-nya di [www.ietf.org](http://www.ietf.org).

# IANA

- The IANA is the Internet Assigned Numbers Authority.
- IANA bertanggung jawab untuk alokasi alamat IP.
- IANA akan mendelegasikan administrasi kelompok alamat IP untuk pendaftaran lebih kecil.
- IANA juga bertanggung jawab untuk peraturan DNS.
- IANA menangani operasi dari DNS akar domain (. Com, net,.Org, dan sebagainya).
- situs Web-nya di [www.iana.org](http://www.iana.org).

# Security Standards and Certifications

# FIPS

- FIPS dikembangkan oleh pemerintah federal AS melalui NIST.
- FIPS lebih banyak dikenal adalah FIPS seri 140.
- FIPS 140 berfokus pada kriptografi.
- FIPS 140 menetapkan standar untuk perangkat keras kriptografi perangkat lunak dan modul.
- Kriptografi adalah bertanggung jawab menyediakan sertifikat untuk mereka agar algoritma kriptografi mereka mendapatkan sertifikat dengan standar FIPS 140.

- Lingkungan tertentu memerlukan penggunaan FIPS 140- bersertifikat algoritma. Jika hal ini terjadi, maka Anda harus memastikan bahwa algoritma yang digunakan di lingkungan anda juga mematuhi standar ini.
- Anda harus memeriksa dengan vendor perangkat lunak anda untuk memastikan bahwa aplikasi yang digunakan mematuhi standar FIPS 140.
- Selain itu, Sistem Microsoft memungkinkan Anda untuk membatasi penggunaan kriptografi hanya menggunakan algoritma standar FIPS 140.
- Anda dapat menggunakan Local Security Policy pada aplikasi Sistem Windows 7 untuk memaksa penggunaan FIPS 140 algoritma compliant.

| Local Security Policy  |        |                            |      |
|--|--------|----------------------------|------|
| File   | Action | View                       | Help |
| Security Settings  |        |                            |      |
| Account Policies   |        |                            |      |
| Local Policies   |        |                            |      |
| Audit Policy   |        |                            |      |
| User Rights Assignment   |        |                            |      |
| Security Options   |        |                            |      |
| Windows Firewall with Advanced Security  |        |                            |      |
| Network List Manager Policies  |        |                            |      |
| Public Key Policies  |        |                            |      |
| Software Restriction Policies  |        |                            |      |
| Application Control Policies   |        |                            |      |
| IP Security Policies on Local Computer   |        |                            |      |
| Advanced Audit Policy Configuration  |        |                            |      |
| Policy   |        | Security Setting           |      |
| Network security: Restrict NTLM: NTLM authentication in this domain  |        | Not Defined                |      |
| Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers                                   |        | Not Defined                |      |
| Recovery console: Allow automatic administrative logon   |        | Disabled                   |      |
| Recovery console: Allow floppy copy and access to all drives and all folders                               |        | Disabled                   |      |
| Shutdown: Allow system to be shut down without having to log on  |        | Enabled                    |      |
| Shutdown: Clear virtual memory pagefile  |        | Disabled                   |      |
| System cryptography: Force strong key protection for user keys stored on the computer                      |        | Not Defined                |      |
| System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing                    |        | Disabled                   |      |
| System objects: Require case insensitivity for non-Windows subsystems                                      |        | Enabled                    |      |
| System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)            |        | Enabled                    |      |
| System settings: Optional subsystems   |        | Posix                      |      |
| System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies            |        | Disabled                   |      |
| User Account Control: Admin Approval Mode for the Built-in Administrator account                           |        | Disabled                   |      |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop |        | Disabled                   |      |
| User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode           |        | Prompt for consent for ... |      |
| User Account Control: Behavior of the elevation prompt for standard users                                  |        | Prompt for credentials     |      |
| User Account Control: Detect application installations and prompt for elevation                            |        | Enabled                    |      |
| User Account Control: Only elevate executables that are signed and validated                               |        | Disabled                   |      |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations            |        | Enabled                    |      |
| User Account Control: Run all administrators in Admin Approval Mode  |        | Enabled                    |      |
| User Account Control: Switch to the secure desktop when prompting for elevation                            |        | Enabled                    |      |
| User Account Control: Virtualize file and registry write failures to per-user locations                    |        | Enabled                    |      |

# Kriteria Umum (Common Criteria) dan EAL

- Common Criteria adalah standar internasional untuk informasi keamanan sertifikasi.
- Karena Common Criteria adalah standar internasional dan bukan hanya standar di AS,
- di banyak organisasi lingkungan yang sesuai Kriteria umum adalah menggantikan kebutuhan compliant FIPS 140.

- Common Criteria menyediakan satu set rinci persyaratan untuk Sertifikasi.
- Sertifikasi Common Criteria diperoleh oleh vendor hardware dan software.
- Sertifikasi Common Criteria dilakukan untuk produk tertentu atau lingkungan tertentu dengan konfigurasi spesifik.
- Produk atau lingkungan yang disertifikasi disebut the Target of Evaluation (TOE).
- Sertifikasi TOE membutuhkan tiga komponen: Proteksi profil, Target Keamanan, dan Persyaratan Keamanan Fungsional.

- The Protection Profile adalah dokumen yang merinci secara aman implementasi perangkat atau jenis perangkat.
- beberapa produsen menggunakan Proteksi profil sebagai referensi ketika membuat jenis tertentu dari perangkat. Juga, Proteksi profil dapat memberi umpan balik ke Target Keamanan digunakan untuk sertifikasi.

- The Security Target adalah rincian konfigurasi keamanan TOE.
- Target Keamanan merupakan konfigurasi yang tepat untuk sertifikat.
- Vendor umumnya membuat The Security Target tersedia untuk pelanggan mereka.
- Dengan cara ini, pelanggan dapat mengkonfigurasi dengan cara yang mencerminkan konfigurasi Sertifikat.

- *Security Functional Requirements* adalah menyediakan fungsi sertifikat untuk produk.
- Common Criteria memiliki daftar fungsi standar yang dapat untuk produk.
- Fungsi-fungsi yang Anda inginkan termasuk dalam evaluasi harus terdaftar.
- Selama proses evaluasi Common Criteria, Anda juga harus menentukan tingkat jaminan. tingkat jaminan disebut Jaminan Evaluasi Level (EAL).
- EAL adalah indikator seberapa ketat pengujian tersebut. Ada tujuh tingkat EAL mungkin.
- 7 EAL adalah yang paling ketat.
- anda akses di situs <http://www.commoncriteriaprofile.org/>

# Regulations and Compliance

- sertifikasi peraturan dan kepatuhan yang berbeda dapat mempengaruhi lingkungan Anda.
- Beberapa peraturan mempengaruhi perusahaan di industri tertentu.
- Sangat penting bahwa Anda memahami peraturan dan sertifikasi kepatuhan mempengaruhi organisasi Anda.
- Aturan-aturan dan peraturan dapat secara dramatis mempengaruhi konfigurasi lingkungan Anda.

# PCI DSS

- PCI DSS is the Payment Card Industry Data Security Standard.
- PCI DSS standar didirikan oleh Dewan Kartu Pembayaran Standar Keamanan Industri.
- Standar PCI DSS mengatur sistem yang menyimpan dan memproses informasi kartu kredit.
- Tujuan adalah untuk membantu mencegah penipuan kartu kredit dan / atau pencurian.

- Standar PCI DSS memiliki 12 persyaratan yang dikelompokkan ke dalam enam Kategori

# Build and maintain a secure network

- Menginstal dan memelihara sebuah konfigurasi firewall untuk melindungi Data pemegang kartu
- Jangan gunakan vendor- default disediakan untuk password sistem dan parameter keamanan lainnya

# Protect cardholder data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open public networks

# Maintain a vulnerability management program

- Use and regularly update antivirus software or programs
- Develop and maintain secure systems and applications

# Implement strong access control measures

- Membatasi akses ke data pemegang kartu
- Menetapkan ID yang unik untuk setiap orang dengan akses komputer.
- Membatasi akses fisik ke data pemegang kartu

# Regularly monitor and test networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

# Maintain an information security policy

- Maintain a policy that addresses information security for employees and contractors

# Keuntungan

- Sertifikat TI dapat meningkatkan kredibilitas seorang profesional TI di mata pemberi kerja.

# Jenis Sertifikat

- Sertifikasi akademik (sebetulnya tidak tepat disebut sertifikasi) yang memberiakn gelar, Sarjana, Master dll
- Sertifikasi profesi. Yaitu suatu sertifikasi yang diberikan berdasarkan keahlian tertentu unutk profesi tertentu.

Sertifikasi profesional pada dasarnya memiliki 3 model, yaitu :

- Dikembangkan oleh Profesional Society, sebagai contoh British Computer Society (BCS), Australian Computer Society (ACS), South East Asian Regional Computer Confederation (SEARCC) etc

- Dikeluarkan oleh Komunitas suatu profesi, sebagai contoh Linux Profesional, SAGE (System Administration Guild), CISA(IS Auditing) [<http://www.isaca.org/>]

- Dikeluarkan oleh vendor sebagai contoh MCSE (by Microsoft), CCNA (Cisco), CNE (Netware), RHCE (Red Hat) etc. Biasanya skill yang dibutuhkan untuk memperoleh sertifikat ini sangat spesifik dan sangat berorientasi pada suatu produk dari vendor tersebut.

# Authentication, Authorization, and Accounting (AAA)

&

## Access Control

Agung Brastama Putra

- AAA merupakan singkatan yang diakui secara universal dalam keamanan informasi dunia.
- Masalahnya adalah bahwa banyak orang sering keliru tentang apa tiga A.
- 3 A adalah Otentikasi, Otorisasi, dan Akuntabel.
- Banyak orang berpikir 3 A adalah Otentikasi, Otorisasi, dan Access Control.
- Akses kontrol erat terkait dengan otentikasi dan otorisasi, tetapi bukan bagian dari triple A keamanan informasi.

# Authentication

- Sebelum Anda memberikan akses pengguna ke lingkungan Anda, pertama anda ingin pastikan, Anda tahu siapa pengguna yang masuk.
- Otentikasi digunakan untuk memverifikasi identitas pengguna.
- Otentikasi dapat dibagi menjadi dua komponen: identifikasi dan verifikasi.

# Pengertian Secara Harfiah

- Otentikasi adalah verifikasi apakah seseorang itu adalah orang yang berhak.
- Biasanya melibatkan username dan password, tapi dapat menyertakan metode lain yang menunjukkan identitas, seperti kartu pintar, sidik jari, dll.

- Jenis-Jenis Otentikasi
  1. Mutual Authentication
  2. Multifactor Authentication
  3. Claims-Based Authentication

# Mutual Authentication

- Umumnya, dalam sistem otentikasi, Anda dapat mempertimbangkan satu sistem klien dan sistem lain server. Biasanya, server mengotentikasi klien.
- Tapi bagaimana dengan server? Bagaimana klien yakin bahwa server yang dikatakannya itu?
- Jika identitas server tidak diverifikasi, maka mungkin server dapat dipalsukan.
- Kemudian, klien dapat mengirimkan mandat untuk sebuah entitas berbahaya.
- Di sinilah saling otentikasi masuk dalam skenario otentikasi bersama, baik klien dan server yang dikonfirmasi.

# Multifactor Authentication

- Ada tiga otentikasi faktor yang dapat digunakan: sesuatu yang Anda tahu, sesuatu anda miliki, dan sesuatu yang melekat dengan anda.
- Sesuatu yang Anda tahu akan menjadi password, ulang tahun atau beberapa informasi pribadi lainnya.
- Sesuatu yang anda miliki akan menjadi satu kali penggunaan token, kartu pintar atau beberapa artefak lain yang mungkin anda miliki di fisik Anda.
- Sesuatu yang melekat dengan anda akan menjadi identitas biometrik Anda, seperti sidik jari atau pola bicara

- Agar dianggap otentikasi multifaktor, maka harus menggunakan setidaknya dua dari tiga faktor yang disebutkan tadi.

# Claims-Based Authentication

- Berbasis Klaim otentikasi adalah metode untuk menyediakan cross-platform otentikasi dan single sign-on.
- Seorang pengguna untuk mengotentikasi satu penyedia otentikasi, dan identitas nya kemudian dibawa ke sebuah aplikasi atau layanan yang mungkin menggunakan otentikasi penyedia yang berbeda.

- Contohnya
- Aplikasi yang melakukan verifikasi keaslian produknya menggunakan Token/donggel, apabila tidak ada token maka aplikasi tersebut tidak bisa dipakai.



Compatible with:  
USB B type and Parallel port (IEEE 1284 Port).

[www.sjtweb.net](http://www.sjtweb.net)



# *Advanced Authentication Types*

- Berikut ini adalah beberapa metode otentifikasi

# PAP

- PAP Password Authentication Protokol. sebelum otentikasi terjadi, PAP menggunakan hubungan untuk membuat sambungan antara klien dan server.
- Setelah koneksi telah ditetapkan, username dan password kemudian dikirim melalui koneksi dalam bentuk teks.
- Transmisi ini jelas teks username dan password adalah salah satu alasan mengapa PAP dianggap oleh sebagian besar menjadi sebuah protokol tidak aman.
- password ditransmisikan dalam bentuk teks dapat dicuri menggunakan sniffer jaringan dasar.
- Jadi Anda harus berhati-hati jika Anda memilih untuk menggunakan PAP di lingkungan Anda.

# CHAP

- CHAP is the Challenge Handshake Authentication Protocol
- CHAP dianggap lebih aman daripada PAP.
- CHAP menggunakan three-way sebuah hubungan saat membuat koneksi.
- Setelah link dibentuk, server akan mengirim tantangan kembali ke klien.
- Klien kemudian merespon dengan nilai hash. Server akan kemudian memeriksa nilai ini terhadap nilai yang dihitung dengan menggunakan hash. Jika nilai adalah sama, maka sambungan dibuat.
- Karena nilai hash yang dikirim bukan yang sebenarnya password, proses koneksi dianggap lebih aman.

# EAP

- EAP is the Extensible Authentication Protocol
- EAP digunakan dalam dial-up, point-to-point, dan koneksi LAN.
- Bagaimanapun EAP, sebagian besar adalah terlihat saat ini pada sambungan LAN nirkabel. EAP lebih dari sekedar sebuah protokol, melainkan lebih dari kerangka kerja.
- Kerangka EAP terdiri dari beberapa metode otentikasi.
- Beberapa yang paling sering digunakan adalah EAP-TLS, PEAP, dan LEAP.

# LDAP

- LDAP is the Lightweight Directory Access Protocol.
- Ada beberapa kesalahpahaman ketika membahas LDAP dalam konteks otentikasi.
- LDAP sebenarnya adalah protokol yang digunakan untuk query direktori.
- Ketika LDAP digunakan untuk otentikasi, apa yang sebenarnya terjadi adalah bahwa LDAP digunakan untuk mengakses direktori di mana kepercayaan pengguna disimpan.

- Aplikasi atau sistem yang otentik kemudian akan melakukan yang sebenarnya otentikasi.
- Kadang-kadang, ada kekhawatiran atas keamanan menggunakan LDAP untuk komunikasi dengan direktori.
- Untuk mengatasi masalah ini, Anda dapat menggunakan LDAP melalui SSL atau LDAPS.
- Dengan LDAPS, LDAP komunikasi ke direktori dienkripsi menggunakan SSL.
- Dengan LDAPS, Anda harus memastikan struktur sertifikat tidak di tempat.

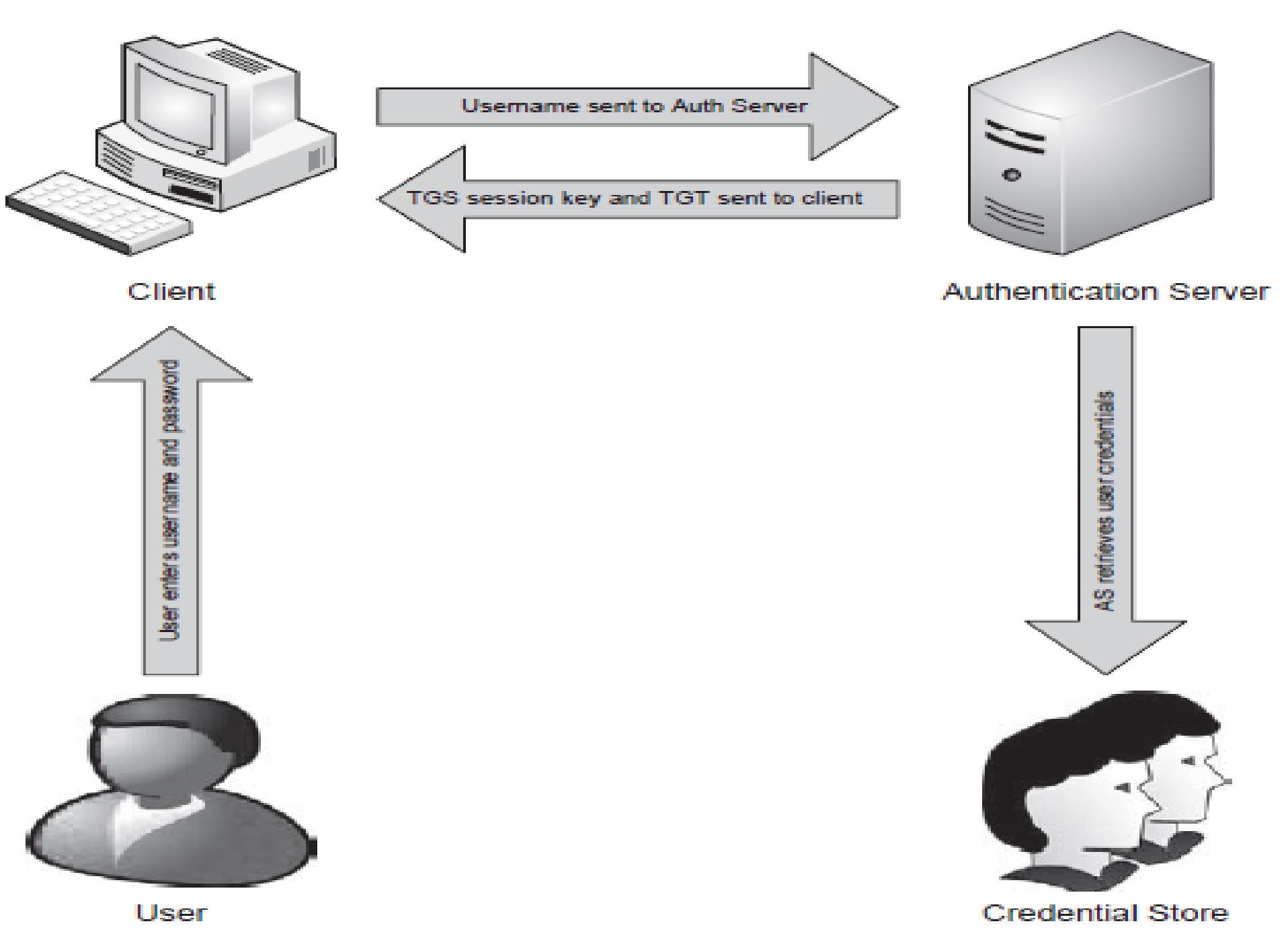
# Karberos

- Kerberos adalah sistem otentikasi tiket berbasis.
- Hal ini didasarkan pada penggunaan kunci simetrik.
- Kerberos menggunakan tiket untuk menyediakan otentikasi ke sumber daya, bukan password.
- tiket ini membantu menyelesaikan ancaman mencuri password melalui jaringan sniffing. Untuk membantu menyediakan lingkungan yang aman, Kerberos menggunakan saling otentikasi.
- Dalam Otentikasi Reksa, baik server dan klien harus disahkan. Ini membantu mencegah serangan menengah dan spoofing.
- Komponen utama dalam sistem Kerberos adalah Kunci Distribusi Center, Layanan Tiket-Pemberian, dan tiket-Pemberian tiket.

- Key Distribution Center : The Key Distribution Center (KDC) adalah pusat dari proses Kerberos.
- KDC ini memiliki database tombol yang digunakan dalam proses otentikasi. KDC ini terdiri dari dua utama bagian: Layanan Otentikasi dan Tiket Layanan

- Layanan Otentikasi adalah apa mengotentikasi klien.
- Layanan Pemberian-Tiket adalah apa yang menyediakan tiket dan Pemberian-Tiket ke sistem klien. Pemberian-Tiket berisi ID klien, alamat jaringan klien, masa berlaku tiket, dan Pemberian-Tiket kunci Session Server

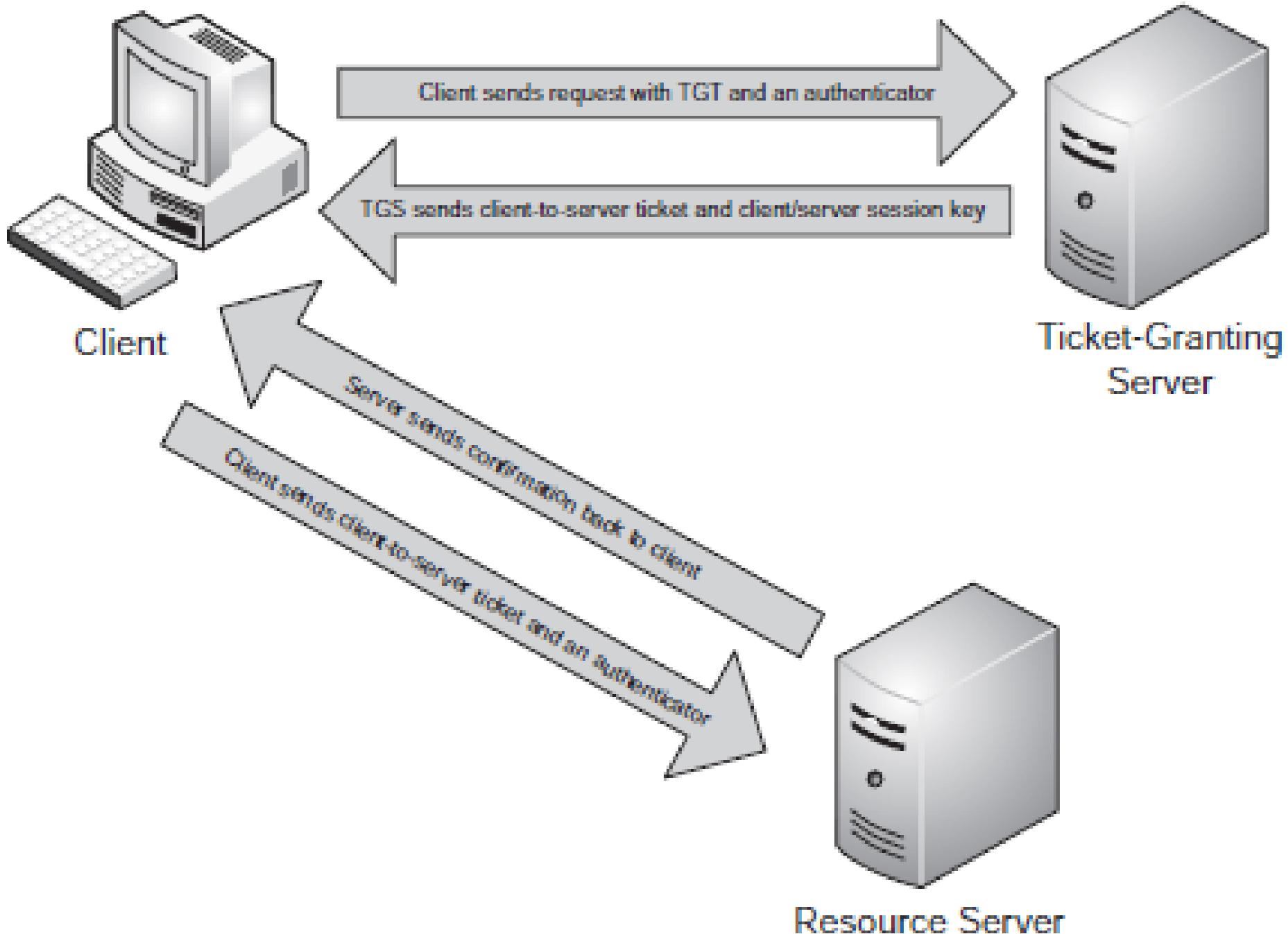
- Langkah-langkah berikut menguraikan proses Otentikasi Kerberos,
  1. Pengguna memasukkan nama pengguna nya dan password di sistem klien.
  2. Klien menggunakan hash satu arah untuk menutupi password. hash ini satu arah dianggap sebagai rahasia klien.



- 3. Klien mengirimkan username ke Server Authentication.
- 4. Server Otentikasi mengambil password pengguna dari penyimpanan credential dan membuat hash satu arah.
- 5. Server Otentikasi memeriksa untuk memastikan bahwa klien adalah disetujui database klien.
- 6. Jika klien disetujui, Authentication Server akan mengirimkan kembali kunci Pemberian-Tiket Session Server dan Pemberian-Tiket.
- 7. Klien kemudian dikonfirmasi ke server Pemberian-Tiket .

# Langkah-langkah berikut menguraikan proses Kerberos permintaan sumber daya

1. Client mengirimkan permintaan ke Layanan Pemberian-Tiket. permintaan itu berisi Tiket Pemberian-Tiket dan authenticator sebuah dienkripsi menggunakan kunci Pemberian-Tiket Session Server.
2. Layanan Tiket-Pemberian mengirimkan tiket klien-ke-server dan kunci session klien/server.
3. Klien mengirimkan tiket klien-ke-server dan authenticator baru ke server di mana sumber daya berada.
4. Server kemudian mengirimkan pesan konfirmasi kembali ke klien.
5. Klien menegaskan server dan mulai mengirim permintaan.



- Kerberos pada Windows Sistem: Kerberos adalah sangat umum di lingkungan windows.
- In fact, Windows 2000 and later use Kerberos as the default method of authentication

# Authorization

- Otorisasi adalah proses menentukan apa yang pengguna perbolehkan.
- kebijakan keamanan menentukan pengguna sumber daya apa di lingkungan Anda yang diijinkan untuk diakses.
- Anda harus juga menentukan apa setiap user yang diperbolehkan untuk dilakukan dengan sumber daya tersebut.

Kebijakan keamanan akan diimplementasikan menggunakan otorisasi sistem Anda dan diteruskan menggunakan akses sistem kontrol Anda.

- ada dua konsep untuk memastikan lingkungan Anda aman :
  1. *Principle of Least Privilege*
  2. *Principle of Separation of Duties*

# *Principle of Least Privilege*

- Prinsip ini setidaknya mengacu pada konsep memberikan mengguna hak minimal yang dibutuhkan untuk melakukan fungsi pekerjaannya.
- Hal ini membantu mencegah pengguna dari sengaja atau tidak sengaja melakukan hal-hal mereka tidak seharusnya.
- Sebagai contoh, Claudine di Departemen akuntansi tidak harus diberi wewenang untuk melakukan fungsi dalam sistem pengiriman

# *Principle of Separation of Duties*

- Mungkin ada tugas penting atau proses dalam organisasi Anda, bahwa Anda ingin mengambil tindakan ekstra untuk melindungi terhadap penipuan atau kejahatan lainnya.
- Sebuah pemisahan tugas dapat membantu Anda melindungi tugas atau proses.
- Anda mulai dengan memecah proses menjadi tugas yang lebih kecil atau proses.
- Anda kemudian mengotorisasi orang yang berbeda untuk melakukan tugas-tugas yang lebih kecil atau proses.

# Accounting

- Accounting adalah proses melacak siapa yang mengakses sumber daya yang di lingkungan Anda.
- Informasi ini dapat digunakan untuk beberapa tujuan. Anda dapat menggunakannya untuk melacak dan memverifikasi masalah keamanan

# Product AAA

- RADIUS

# RADIUS

- RADIUS is the Remote Authentication Dial-In User Service.
- RADIUS adalah salah satu protokol AAA tertua.
- Awalnya, RADIUS hanya digunakan dalam sistem akses remote.
- Penggunaan RADIUS diperluas untuk mencakup aplikasi dan perangkat jaringan.
- Popularitas RADIUS 'berasal dari fakta bahwa standar protokol itu yang dapat digunakan pada berbagai macam perangkat dan sistem.

- Pengaturan suatu RADIUS membutuhkan klien RADIUS, server RADIUS, dan protokol RADIUS.
- Klien RADIUS umumnya ada di perangkat di tempat usaha koneksi yang dibuat. bahwa perangkat pada gilirannya membuat panggilan ke server RADIUS.
- RADIUS menggunakan UDP untuk komunikasi

# TACACS+

- TACACS is the Terminal Access Controller Access control System.
- TACACS adalah standar otentikasi remote. TACACS digunakan untuk dial-in dan akses jaringan.
- Para TACACS asli standar banyak digunakan di sistem UNIX.
- Protokol asli TACACS hampir tidak digunakan lagi. Ini telah digantikan oleh TACACS + dan RADIUS.

- TACACS + adalah ekstensi milik dari standar TACACS dikembangkan oleh Cisco.
- TACACS + yang digunakan oleh Cisco untuk otentikasi pengguna untuk perangkat jaringan seperti switch, router, dan jaringan akses server.
- Tidak seperti namanya, TACACS + sangat berbeda dari standar asli TACACS.
- Bahkan, bahkan mereka tidak kompatibel satu sama lain.

- TACACS dianggap upgrade terbaru dari RADIUS.
- TACACS + menggunakan TCP untuk komunikasi. TCP dianggap lebih dapat diandalkan dibandingkan UDP, UDP adalah apa yang RADIUS gunakan.

# Diameter

- Diameter dianggap sebagai penerus protokol RADIUS.
- Dalam geometri, diameter lingkaran adalah dua kali panjang jari-jari lingkaran.
- Meskipun Diameter dianggap sebagai upgrade dari RADIUS, penting untuk dicatat bahwa RADIUS dan Diameter tidak langsung kompatibel.

- Diameter meliputi upgrade selama bertahun-protokol RADIUS.
- Diameter, seperti TACACS, menggunakan TCP untuk komunikasi, sebagai lawan dengan UDP.
- Diameter juga mendukung IPSec dan TLS. Ini mencakup kemampuan negosiasi dan error.
- Diameter juga mencakup lebih atribut-nilai pasangan.

# Access Control

- akses kontrol sistem umumnya apa yang digunakan untuk melakukan otorisasi kebijakan anda.

# Access Control Models

- *Mandatory Access Control (MAC)*
- *Discretionary Access Control (DAC)*
- *Role-Based Access Control (RBAC)*

# *Mandatory Access Control (MAC)*

- Mandatory Access Control didasarkan pada model hirarkis.
- hirarki itu didasarkan pada tingkat keamanan.
- Semua pengguna ditugaskan keamanan atau izin tingkat.
- Semua obyek ditugaskan keamanan. Pengguna dapat mengakses sumber daya hanya yang sesuai dengan keamanan sama dengan atau lebih rendah dari mereka dalam hirarki tingkat.

# *Discretionary Access Control (DAC)*

- Discretionary Access Control is based on Access Control Lists (ACLs).
- Daftar pengguna ACL mana yang memiliki akses ke sebuah obyek dan apa dapat mereka lakukan dengan objek.
- ACL akan mendaftar pengguna dan perizinan.
- Anda dapat memberikan hak akses khusus atau menolak perizinan.

# *Role-Based Access Control (RBAC)*

- Access Control Sistem Berbasis Peran didasarkan pada peran pengguna dan tanggung jawab.
- Pengguna tidak diberikan akses ke sistem; peran itu.
- Dalam sistem RBAC, peran yang dikelola secara terpusat oleh administrator.
- Administrator menentukan peran apa yang ada dalam perusahaan mereka dan kemudian peta peran untuk fungsi pekerjaan dan tugas.

# Keamanan Sistem Informasi

Agung Brastama Putra

# Pembahasan

- Cracker
- Virus computer
- Spyware
- Spam

# Cracker

- Cracker adalah sebutan untuk mereka yang masuk ke sistem orang lain dan cracker lebih bersifat destruktif.
- biasanya di jaringan komputer, mem-bypass password atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-deface (mengubah halaman muka web) milik orang lain bahkan hingga men-delete data orang lain, mencuri data dan umumnya melakukan cracking untuk keuntungan sendiri, maksud jahat, atau karena sebab lainnya karena ada tantangan.

- Beberapa proses pembobolan dilakukan untuk menunjukan kelemahan keamanan sistem

# Virus computer

- **Virus komputer** merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain.
- Virus komputer dapat dianalogikan dengan virus biologis yang menyebar dengan cara menyisipkan dirinya sendiri ke sel makhluk hidup.

- Virus komputer dapat merusak (misalnya dengan merusak data pada dokumen), membuat pengguna komputer merasa terganggu, maupun tidak menimbulkan efek sama sekali.

## a. Worm

Worm adalah lubang keamanan atau celah kelemahan pada komputer kita yang memungkinkan komputer kita terinfeksi virus tanpa harus eksekusi suatu file yang umumnya terjadi pada jaringan.

## b. Trojan

Trojan adalah sebuah program yang memungkinkan komputer kita dikontrol orang lain melalui jaringan atau internet.

## c. Spyware

Spyware adalah aplikasi yang membocorkan data informasi kebiasaan atau perilaku pengguna dalam menggunakan komputer ke pihak luar tanpa kita sadari. Biasanya digunakan oleh pihak pemasang iklan

# Tanda-Tanda Komputer Terinfeksi Virus Komputer

- Komputer berjalan lambat dari normal
- Sering keluar pesan eror atau aneh-aneh
- Perubahan tampilan pada komputer
- Media penyimpanan seperti disket, flashdisk, dan sebagainya langsung mengkopi file aneh tanpa kita kopi ketika kita hubungkan ke komputer.
- Komputer suka restart sendiri atau crash ketika sedang berjalan.
- Suka muncul pesan atau tulisan aneh
- Komputer hang atau berhenti merespon kita.
- Harddisk tidak bisa diakses

- Printer dan perangkat lain tidak dapat dipakai walaupun tidak ada masalah hardware dan software driver.
- Sering ada menu atau kotak dialog yang error atau rusak.
- Hilangnya beberapa fungsi dasar komputer.
- Komputer berusaha menghubungkan diri dengan internet atau jaringan tanpa kita suruh.
- File yang kita simpan di komputer atau media penyimpanan hilang begitu saja atau disembunyikan virus

# bentuk media penyebaran virus komputer

- Media Penyimpanan
- Jaringan lan, wan, man, internet dan lain sebagainya.
- File attachment atau file lampiran pada email atau pesan elektronik lainnya.
- File software (piranti lunak) yang ditunggangi virus komputer

# Spyware

- Spyware adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada salah satu bentuk perangkat lunak mencurigakan (*malicious software/malware*) yang menginstalasikan dirinya sendiri ke dalam sebuah sistem untuk mencuri data milik pengguna

- *Spyware merupakan turunan dari adware, yang memantau kebiasaan pengguna dalam melakukan penjelajahan Internet untuk mendatangkan "segudang iklan" kepada pengguna*

- Spyware menjadi berbahaya karena saat ini Spyware tidak hanya sebagai pengirim info tersembunyi saja.
- tapi juga menginstall (memasang) semacam program khusus (sering disebut '*trojan*') yang pada akhirnya si pemilik Spyware bisa memata-matai segala aktivitas yang kita lakukan di internet tanpa sepengetahuan kita

# Kerugian

- Pencurian Data
- Tambahan Biaya Pemakaian Internet

# Website Ber-Spyware pada umumnya

- Pada umumnya, website yang memberikan spyware adalah website yang memberikan layanan gratis ataupun website yang menjual produk. Contohnya adalah Grisoft, Ziddu, blog-blog pribadi yang menginginkan penghasilan lebih dari iklannya, seperti dari Google Adsense, Formula bisnis, Kumpul Blogger, kliksay, dkk.
- Pada dasarnya, Spyware tersebut diiringi dengan PopUp Windows, yang tentunya selain memakan Bandwith lebih, juga membuat loading Internet anda semakin lambat

# Contoh Program Spyware dan Adware

- Windows Live Messenger

# Adware

- Adware adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada sebuah jenis perangkat lunak mencurigakan (malicious software/malware) yang menginstalasikan dirinya sendiri tanpa sepengetahuan pengguna dan menampilkan iklan-iklan ketika pengguna berselancar di Internet.

# Perbedaan Adware, Malware, Spyware

- Adware
- Adware adalah bentuk lain dari malware dan persis seperti namanya, perangkat lunak dengan tujuan promosi atau iklan. Adware biasanya terdapat didalam software freeware yang kita download.
- Meskipun beberapa program memberikan pilihan untuk tidak menginstal adware ekstra, banyak sekali software gratis menambahkan adware didalamnya tanpa sepengertahan kita

## ■ Malware

■ Malware adalah perangkat lunak yang bertujuan memberikan masalah pada komputer dengan cara membatasi, mengubah dan memberhentikan kinerja komputer. Dengan tujuan umum untuk proses download dan installasi tersembunyi yang membingungkan

- Malware sendiri biasa didapati karena download internet, link email dan lampiran, jejaring sosial, game online, chatroom dari website berbahaya dsb.

## ■ Indikasi Malware

Beberapa faktor sehingga dapat disimpulkan bahwa telah terinstall malware pada komputer kita adalah :

- Browser homepage terus berubah.
- Iklan pop-up muncul setelah browser ditutup.
- Muncul ikon aneh pada desktop.
- Lampu komputer berkedip (mengartikan komputer dalam proses mengolah informasi) pada waktu yang tidak biasa atau tak terduga. Hal ini sulit untuk diamati dengan broadband karena tidak ada perbedaan visual antara data yang masuk dan keluar.
- Pengaturan browser berubah, termasuk default web saat awal browser dibuka.
- File upload atau download terjadi tanpa izin pengguna

- Spyware
- Spyware adalah jenis program yang menyerang komputer dengan memata-matai komputer.
- spyware dan malware memiliki kesamaan yaitu kemampuan untuk mengumpulkan dan mendistribusikan informasi pribadi tanpa izin Anda

- Spyware dan malware adalah metode yang mungkin untuk pencurian identitas sejak pemilik atau pengguna komputer tidak tahu tentang atau tidak memberikan izin mereka untuk instalasi dan penggunaan program tersembunyi atau file

# Menghindari Malware, Adware dan Spyware

- Tidak membuka email atau lampiran email dari pengirim yang tidak dikenal.
  - Block atau tidak mengklik jendela pop-up yang mencurigakan.
  - Jangan membuka file yang tergolong terkait dengan malware seperti .bat, .com, .exe, .pif, .txt.vbs, .htm.exe atau .vbs
  - Tidak download dan menginstall aplikasi selain dari sumber terpercaya.
  - Hindari penipuan berupa phising.
  - Gunakan update software anti-virus dan anti-spyware secara teratur

# PHISING

- *Phising* , adalah tindakan memperoleh informasi pribadi seperti User ID, PIN, nomor rekening bank, nomor kartu kredit Anda secara tidak sah.

# Bagaimana phishing dilakukan?

- Penggunaan alamat *e-mail* palsu dan grafik untuk menyesatkan Nasabah sehingga Nasabah terpancing menerima keabsahan *e-mail* atau *web sites*. Agar tampak meyakinkan, pelaku juga seringkali memanfaatkan logo atau merk dagang milik lembaga resmi, seperti; bank atau penerbit kartu kredit

- Membuat situs palsu yang sama persis dengan situs resmi. atau . pelaku *phishing* mengirimkan *e-mail* yang berisikan *link* ke situs palsu tersebut.
- Membuat *hyperlink* ke *web-site* palsu atau menyediakan form isian yang ditempelkan pada *e-mail* yang dikirim

# SPAM

- *Spam* atau bisa juga berbentuk *junk mail* adalah penyalahgunaan sistem pesan elektronik (termasuk media penyiaran dan sistem pengiriman digital) untuk mengirim berita iklan dan keperluan lainnya secara massal.
- Umumnya, *spam* menampilkan berita secara bertubi-tubi tanpa diminta dan sering kali tidak dikehendaki oleh penerimanya.

- Bentuk *spam* yang dikenal secara umum meliputi : *spam surat elektronik*, *spam pesan instan*, *spam Usenet newsgroup*, *spam mesin pencari informasi web (web search engine spam)*, *spam blog*, *spam wiki*, *spam iklan baris daring*, *spam jejaring sosial*

Agung Brastama Putra

Slide 5

# Pembahasan

- Virus computer

# Virus Computer

- Virus komputer adalah program komputer yang disembunyikan di dalam program lain di komputer atau di disk drive, yang mencoba untuk menyebarkan dirinya ke komputer lain, dan sering mencakup beberapa fungsi yang merusak (payload).

# Virus, predator or prey

- Virus komputer umumnya terdiri dari dua model yaitu menyebar dan merusak.
- Untraceability adalah fitur utama yang membedakan virus dari ancaman keamanan lainnya.

- Pengguna komputer dan pandangan umum virus sebagai predator yang menyerang komputer dan memangsa data mereka, tetapi virus komputer memiliki pandangan sangat yang berbeda pada situasi yang sama dan menganggap dirinya sebagai mangsa.

- Virus adalah dirancang dan dilaksanakan tidak hanya untuk menyerang, tetapi juga untuk bertahan hidup.
- kelangsungan hidup tergantung pada reproduksi cepat dan untuk menghindari deteksi.
- Kebanyakan virus yang mudah untuk mendeteksi dan menghapus.

# Alasan Pembuatan Virus

- Niat
- Aggression
- Membenci Sesuatu/kebijakan tertentu
- Mampu Membuat
- Hobi dan experiment
- Pengakuan terhadap komunitas pembuat virus
- Sensasi dan Memacu adrenalin
- Menikmati Ketenaran
- Prustasi terhadap sesuatu

- Alasan Politik
- Ketidakadilan Sosial
- Membiarakan Orang lain melakukan pekerjaan yang kotor.
- Hanya untuk belajar.

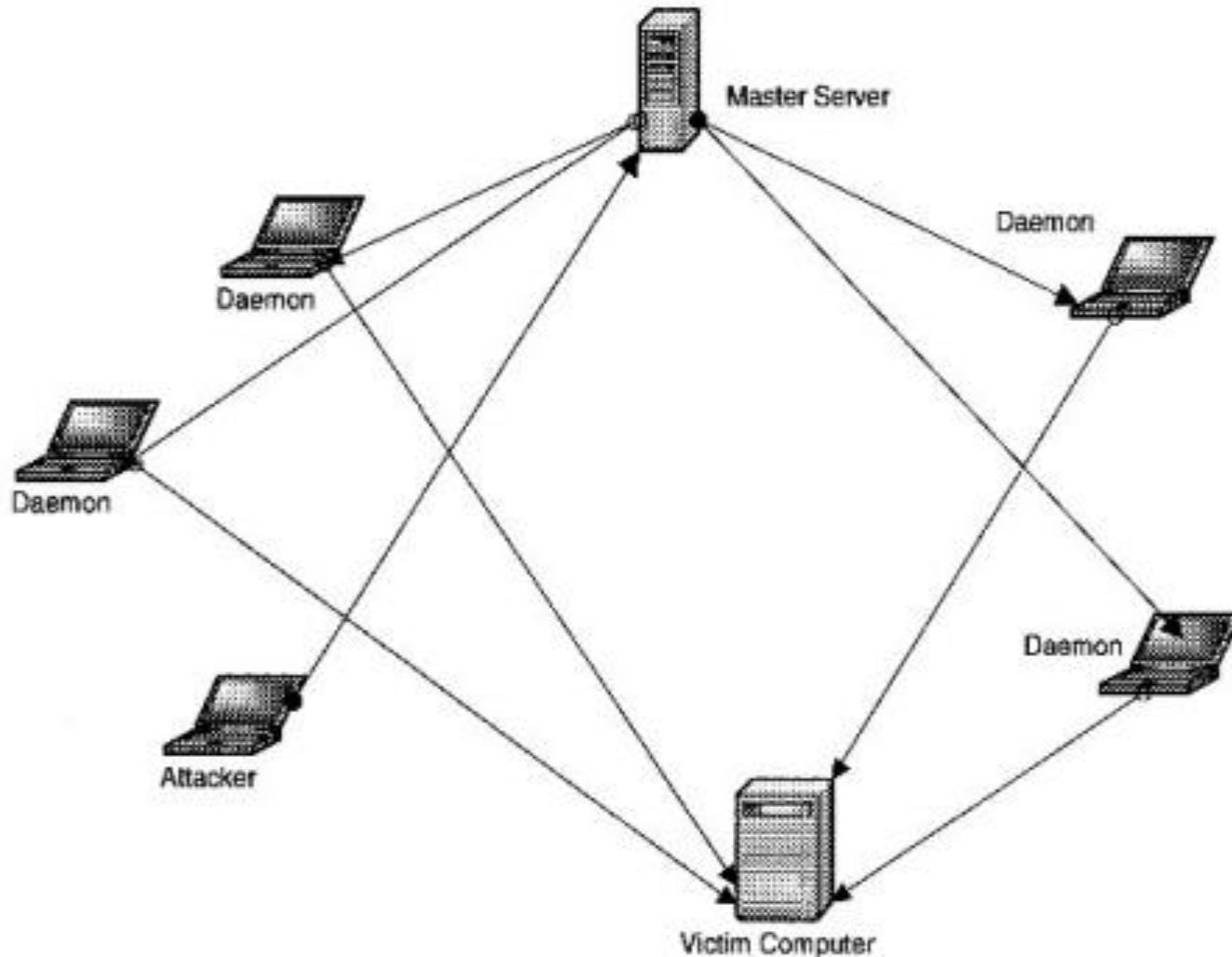


Figure 3.2 The Working of a DDOS Attack

# Slide 6

# Keamanan Sistem Informasi

---

Agung Brastama Putra

# Pembahasan

---

- OSI Layer & TCP/IP Layer
- Enkapkulasi dan Dekapkulasi

# Buku

---

- Larry L. Peterson & Bruce S. Davie.  
2007. Computer networks a system approach edition 4. Morgan Kaufmann Publishers is an imprint of Elsevier.
- Martin P. Clark. 2003. Data Networks, IP and the Internet. WILEY

# Layering and Protocols

---

- Ide abstraksi nya adalah untuk menentukan model pemersatu yang dapat menangkap beberapa aspek penting dari sistem, model ini merangkum dalam suatu objek yang menyediakan antarmuka yang dapat dimanipulasi oleh komponen lain dari sistem, dan menyembunyikan rincian tentang bagaimana objek tersebut dilaksanakan dari pengguna objek

- 
- Abstraksi bisa dikatakan perwakilan dari layering.
  - Ide Umum nya adalah bahwa Anda mulai dengan layanan yang ditawarkan oleh hardware yang mendasarinya, dan kemudian menambahkan serangkaian lapisan, masing-masing memberikan layanan tingkat lebih tinggi (lebih abstrak)

- 
- Layanan yang disediakan pada lapisan tinggi yang diimplementasikan sebagai layanan yang disediakan oleh lapisan rendah

# Contoh Model

---

APPLICATION PROGRAM

CHANNEL PROSES KE CHANNEL PROSES

KONEKSI HOST-TO-HOST (H2H)

HARDWARE

# Keuntungan Model Layering

---

- Pertama :
- Pengelolaan dalam jaringan lebih mudah.
- Model ini dapat menerapkan beberapa lapisan, yang masing-masing memecahkan salah satu bagian dari masalah.

- 
- Kedua :
  - menyediakan lebih modular desain.
  - Jika memutuskan bahwa ingin menambahkan beberapa layanan baru, mungkin hanya perlu memodifikasi fungsi pada satu lapisan, menggunakan kembali fungsi yang disediakan pada semua lapisan yang lain.

# Contoh Layer di dalam Layer

---

APPLICATION PROGRAM

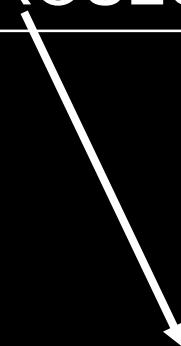
CHANNEL PROSES KE CHANNEL PROSES

KONEKSI HOST-TO-HOST (H2H)

HARDWARE

REQUEST/REPLY  
CHANNEL

MESSAGE STREAM  
CHANNEL



# Maka.....

---

APPLICATION PROGRAM

REQUEST/REPLY  
CHANNEL

MESSAGE STREAM  
CHANNEL

KONEKSI HOST-TO-HOST (H2H)

HARDWARE

# Protocol

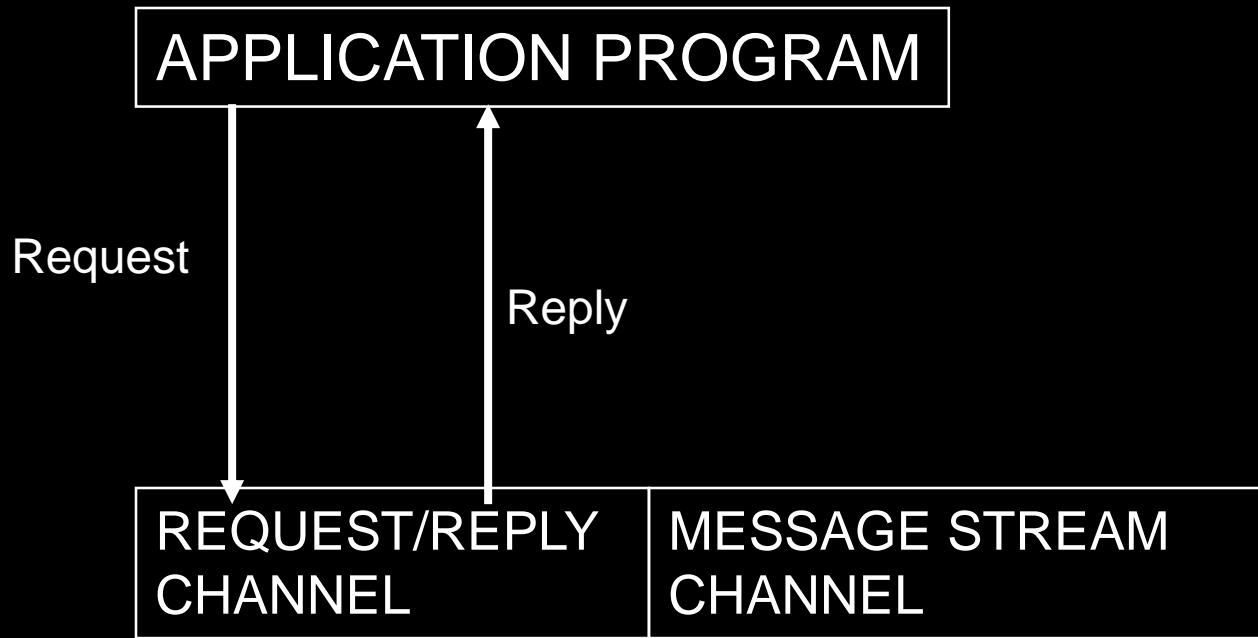
---

- obyek-obyek abstrak yang membentuk lapisan sistem jaringan disebut protokol
- adalah, menyediakan sebuah protokol komunikasi layanan objek bahwa tingkat yang lebih tinggi (seperti proses-proses aplikasi, atau mungkin tingkat yang lebih tinggi protokol) menggunakan untuk bertukar pesan

# Contohnya....

---

## ■ Komunikasi antara

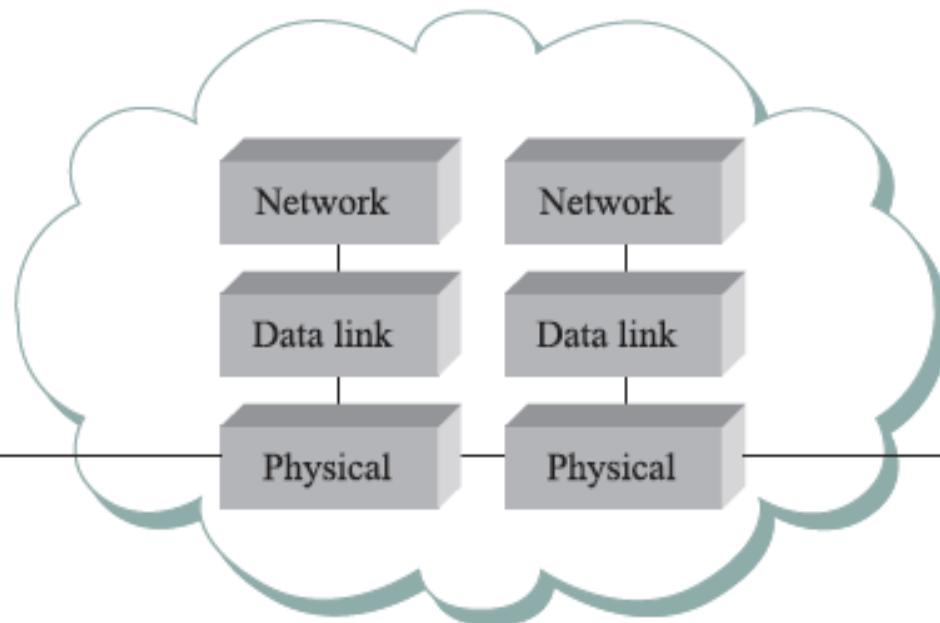
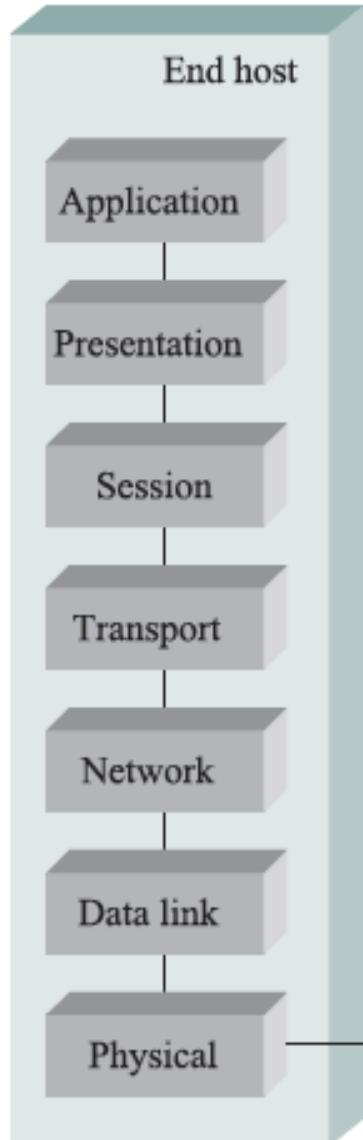


# OSI Architecture

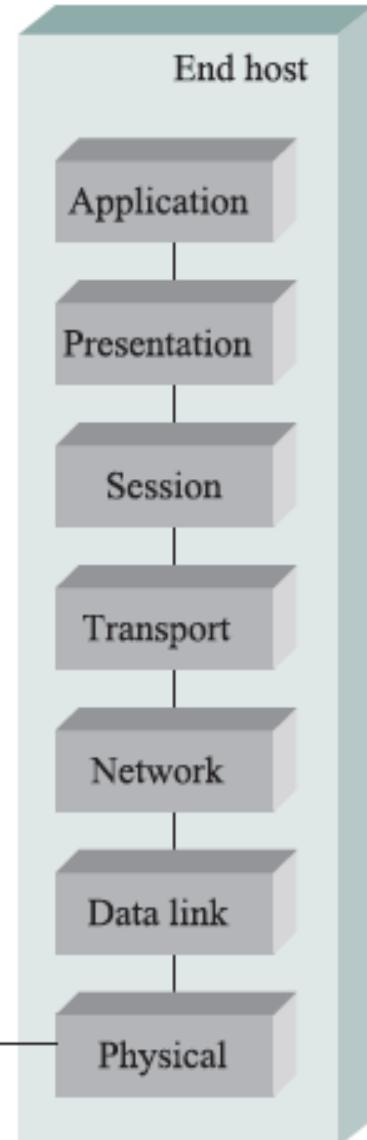
---

- ISO adalah salah satu organisasi pertama untuk menetapkan secara formal cara yang umum untuk menghubungkan tiap-tiap komputer
- Their architecture, called the *Open Systems Interconnection (OSI)*

- 
- Model ini ditujukan untuk interkoneksi Open System
  - Open System diartikan suatu sistem terbuka untuk berkomunikasi dengan sistem-sistem lain yang berbeda arsitektur maupun sistem operasi



One or more nodes  
within the network



# Model OSI

---

- Model OSI dibagi menjadi
  1. Application layer
  2. Presentation layer
  3. Session layer
  4. Transport layer
  5. Network layer
  6. Data Link layer
  7. Physical layer

# TCP/IP

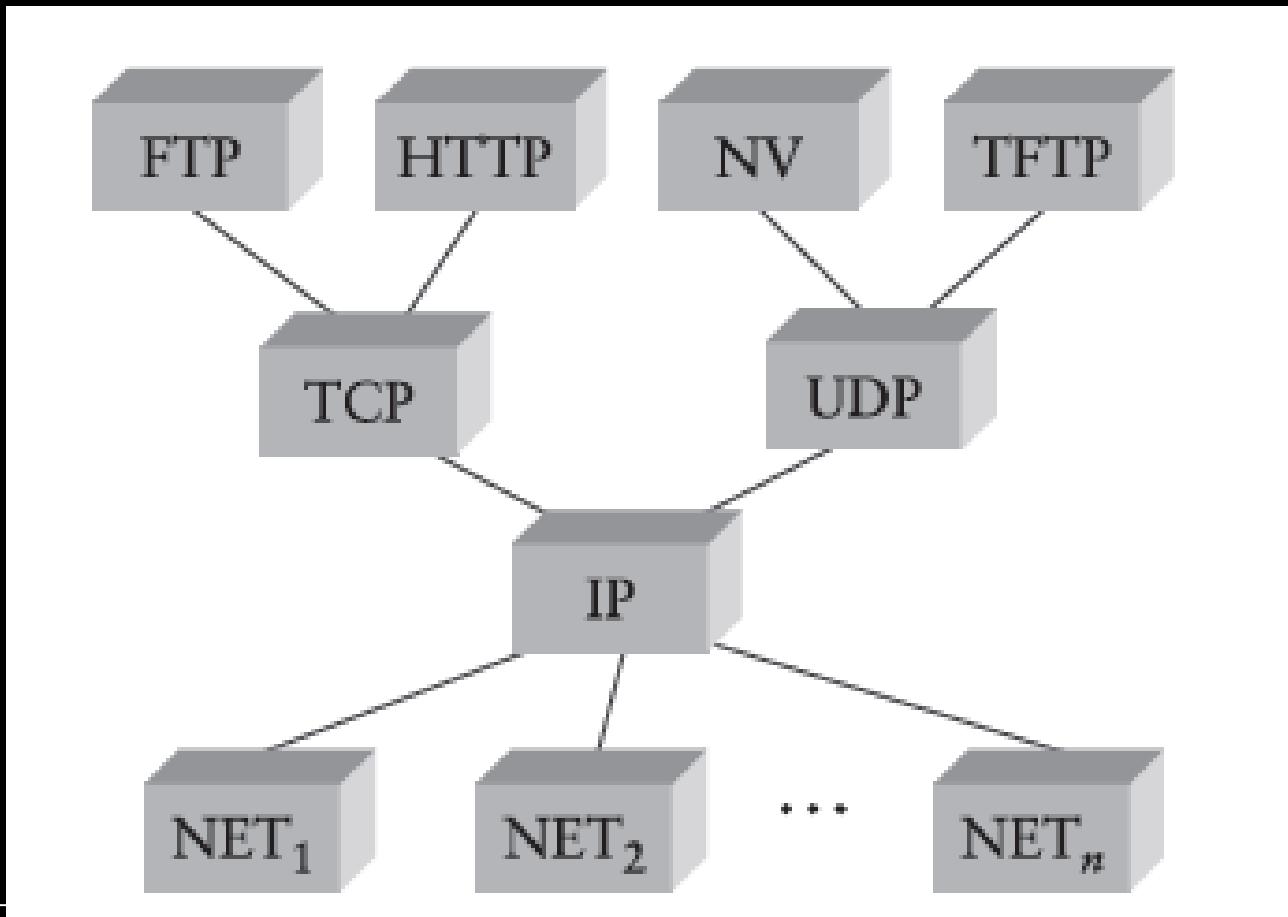
---

- Arsitektur Internet, yang kadang-kadang juga disebut arsitektur TCP/IP.
- TCP/IP adalah singkatan dari Transmission Control Protocol/Internet Protocol

- 
- TCP bertugas menerima pesan elektronik dengan panjang sembarang dan membaginya ke dalam bagian2 berukuran 64 kb.
  - IP bertugas sebagai memeriksa ketepatan bagian2 pengalamatan ke sasaran yang dituju dan memastikan apakah bagian-bagian tersebut sudah dikirim sesuai dengan urutan yang benar.

# Arsitektur Internet

---



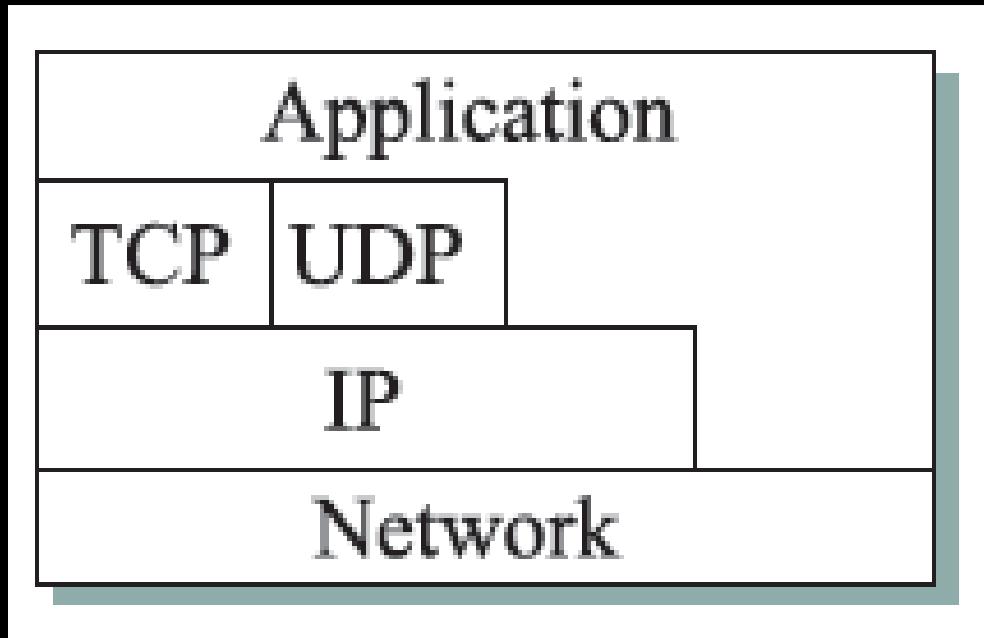
# Model TCP/IP

---

1. Application
2. Transport
3. Internet
4. Network Access

# TCP/IP

---



# Enkapsulasi dan Dekapsulasi

---

- Enkapsulasi adalah sebuah proses menambahkan header dan trailer atau melakukan pemaketan pada sebuah data. Dengan enkapsulasi data menjadi memiliki identitas

- 
- Sedangkan Dekapsulasi adalah Proses pemisahan header IP terluar pada paket yang datang, sehingga datagram yang ditumpangkan itu dapat diakses dan dapat dikirimkan ke tujuan yang sebenarnya. Dekapsulasi merupakan kebalikan dari enkapsulasi

# Pertanyaan

---

- Apa itu Enkapsulasi dan Dekapsulasi ?
- Apa yang dapat anda simpulkan dari OSI dan TCP/IP ?????
- Apa yg dapat anda simpulkan mengenai Layer dan protokol?

# Pertemuan Ke 7

Agung BP

- Integrity for databases: record integrity, data correctness, update integrity
- Security for databases: access control, inference, and aggregation
- Multilevel secure databases: partitioned, cryptographically sealed, filtered
- Security in data mining applications

## Pembahasan

- Charles P. Pfleeger & Shari Lawrence Pfleeger, Security in Computing, 4<sup>th</sup> Ed., Pearson Education, 2007
- Chapter 6

## PUSTAKA

- Database adalah kumpulan data dan seperangkat aturan yang mengatur tentang data dengan menetapkan hubungan tertentu antara data.
- User/pengguna menggambarkannya data berupa *logical format*.
- *Physical Format* tidak selalu mendapatkan perhatian secara serius oleh pengguna/user.

## Konsep Database



# Logical Format Database

Share with ▾ Burn New folder

| Name       | Date modified    | Type        | Size |
|------------|------------------|-------------|------|
| cdcol      | 15/02/2013 19:24 | File folder |      |
| cucimobil  | 25/04/2013 0:18  | File folder |      |
| database1  | 03/03/2013 1:38  | File folder |      |
| dbmurah    | 04/04/2013 13:56 | File folder |      |
| dd3        | 01/04/2013 11:16 | File folder |      |
| latihan    | 06/03/2013 12:20 | File folder |      |
| mysql      | 15/02/2013 19:24 | File folder |      |
| percobaan  | 01/04/2013 23:35 | File folder |      |
| phpmyadmin | 15/02/2013 19:24 | File folder |      |
| pssi       | 01/04/2013 11:20 | File folder |      |
| tes123     | 02/05/2013 1:42  | File folder |      |
| test       | 15/02/2013 19:24 | File folder |      |
| webauth    | 15/02/2013 19:24 | File folder |      |

# Physical Format

- DBA (Database Administrator) adalah seseorang yang memberikan aturan kepada pengguna untuk mengelola, mengatur dan memantau data di database.
- Contoh Sintak memberi Grant User di Oracle:
- **create user** alfredo identified by alfredos\_secret;
- **create user** alfredo identified externally;
- **create user** alfredo identified globally as 'external\_name';

- create user alfredo identified by  
alfredos\_secret **default tablespace**  
**ts\_users temporary tablespace**  
**ts\_temp;**
- Atau
- create user alfredo identified by passw0rd  
**account lock;**
- grant connect to alfredo;

Lanjt.

- **grant** system privilege to username;
- **grant** system privilege\_1,  
system\_privileges\_2, ..,system\_privileges\_n  
to username;
- **grant** system privilege\_1 to username with  
admin option;
- **grant** object privilege to username;
- **grant** object privilege to username with  
grant option;
- **grant** object privilege to username with  
hierarchy option;

- The user interacts with the database through a program called a **database manager or a database management system (DBMS)**, informally known as a **front end**

- Record – contain one related group of data
- Each record contains **fields or elements.**
- The logical structure of a database is called a **schema**
- A particular user may have access to only part of the database, ini disebut dengan **Subschema**

## Komponen

|         |                |          |    |       |
|---------|----------------|----------|----|-------|
| ADAMS   | 212 Market St. | Columbus | OH | 43210 |
| BENCHLY | 501 Union St.  | Chicago  | IL | 60603 |
| CARTER  | 411 Elm St.    | Columbus | OH | 43210 |

```
graph LR; A[Main Table] --> B[Child Table]; A --> C[Separate Table]
```

|         |          |
|---------|----------|
| ADAMS   | Charles  |
| ADAMS   | Edward   |
| BENCHLY | Zeke     |
| CARTER  | Marcie   |
| CARTER  | Beth     |
| CARTER  | Ben      |
| CARTER  | Lisabeth |
| CARTER  | Mary     |

|       |     |
|-------|-----|
| 43210 | CMH |
| 60603 | ORD |

## Related Parts of a Database

## Schema of Database

| Name    | First     | Address        | City     | State | Zip   | Airport |
|---------|-----------|----------------|----------|-------|-------|---------|
| Adams   | Charles   | 212 Market St. | Columbus | OH    | 43210 | CMH     |
| Adams   | Edward    | 212 Market St. | Columbus | OH    | 43210 | CMH     |
| Benchly | Zeke      | 501 Union St.  | Chicago  | IL    | 60603 | ORD     |
| Carter  | Marlene   | 411 Elm St.    | Columbus | OH    | 43210 | CMH     |
| Carter  | Beth      | 411 Elm St.    | Columbus | OH    | 43210 | CMH     |
| Carter  | Ben       | 411 Elm St.    | Columbus | OH    | 43210 | CMH     |
| Carter  | Elisabeth | 411 Elm St.    | Columbus | OH    | 43210 | CMH     |
| Carter  | Mary      | 411 Elm St.    | Columbus | OH    | 43210 | CMH     |

- The name of each column is called an **attribute of the database**
- A **relation** is a set of columns.

- Users interact with database managers through commands to the DBMS that retrieve, modify, add, or delete fields and records of the database.
- Command is called **query**.

- Other, more complex, selection criteria are possible, with logical operators such as **and** ( $\wedge$ ) and **or** ( $\vee$ ), and comparisons such as **less** ( $<$ )

# **Advantage of Using Databases vs file**

- A database is a single collection of data, stored and maintained at one central location, to which many people may have access as needed.
- The users are unaware of the physical arrangements; the unified logical arrangement is all they see.

**With a database we can....**

- **Shared access** – users use one common, centralized set of data
- **Minimal redundancy.** users do not have to collect and maintain their own sets of data
- **Data consistency.** change to a data value affects all users of the data value.
- **Data integrity.** data values are protected against accidental or malicious undesirable changes
- **Controlled access.** only authorized users are allowed to view or to modify data values

- ***Physical database integrity.***
- ***Logical database integrity.***
- ***Element integrity.***
- ***Auditability.***
- ***Access control.***
- ***User authentication.***
- ***Availability.***

## Security Requirements

- Two situations can affect the integrity of a database:
- when the whole database is damaged or corrupt.
- when individual data items are unreadable.

## **Integrity of the Database**

- Integrity of the database as a whole is the responsibility of :
  - The DBMS
  - The operating system
  - The (human) computing system manager.

- **Separation**
  - **Partitioning**
  - **Encryption**
  - **Integrity Lock**

**Proposals for Multilevel Security**

- A user identifies himself or herself to the front end; the front end authenticates the user's identity.
- The user issues a query to the front end.
- The front end verifies the user's authorization to data
- The front end issues a query to the database manager

## Trusted Front End

- The database manager performs I/O access, interacting with low level access control to achieve access to actual data.
- The database manager returns the result of the query to the trusted front end.
- The front end analyzes the sensitivity levels of the data items in the result and selects those items consistent with the user's security level.

- The front end transmits selected data to the untrusted front end formatting.
- The untrusted front end transmits formatted data to the user.

# **Summary of Database Security**

- Address three aspects of security for database management systems:
- Masalah keutuhan dan kerahasiaan database secara spesifik
  - Kerahasiaan tanggung jawab dari user.
  - Keutuhan seluruh database dan table tanggung jawab dari DBMS dan DBA.

- Permasalahan Data di database.
- Permasalahan bisa terletak pada user dan tingkat sensitivitas data pada tiap-tiap database atau bahkan tiap-tiap table.