

# 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

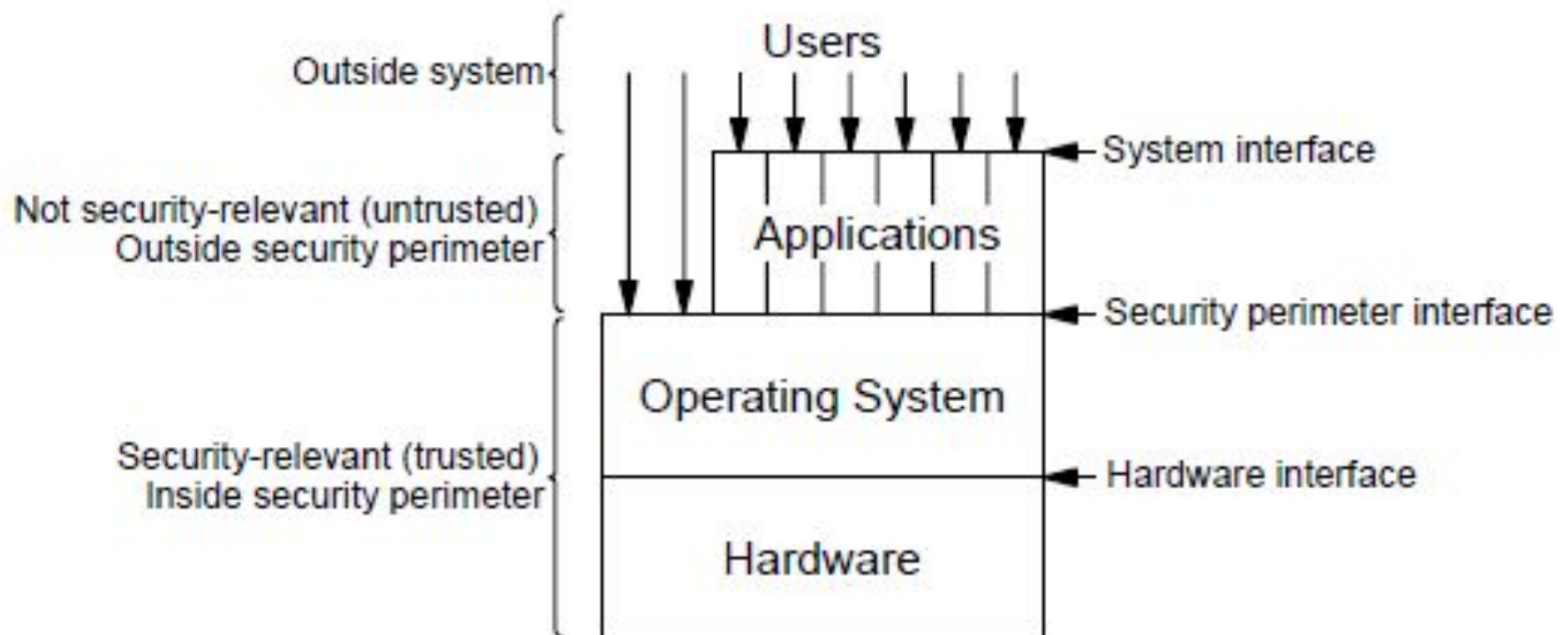
- 
- Sistem operasi mengambil peran yang lebih luas dalam konsep multiprogramming. Menyadari bahwa dua pengguna dapat interleave akses ke sumber daya sistem komputasi tunggal, peneliti mengembangkan konsep-konsep seperti penjadwalan, berbagi, dan penggunaan paralel.
  - Sistem operasi Multiprogrammed, 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

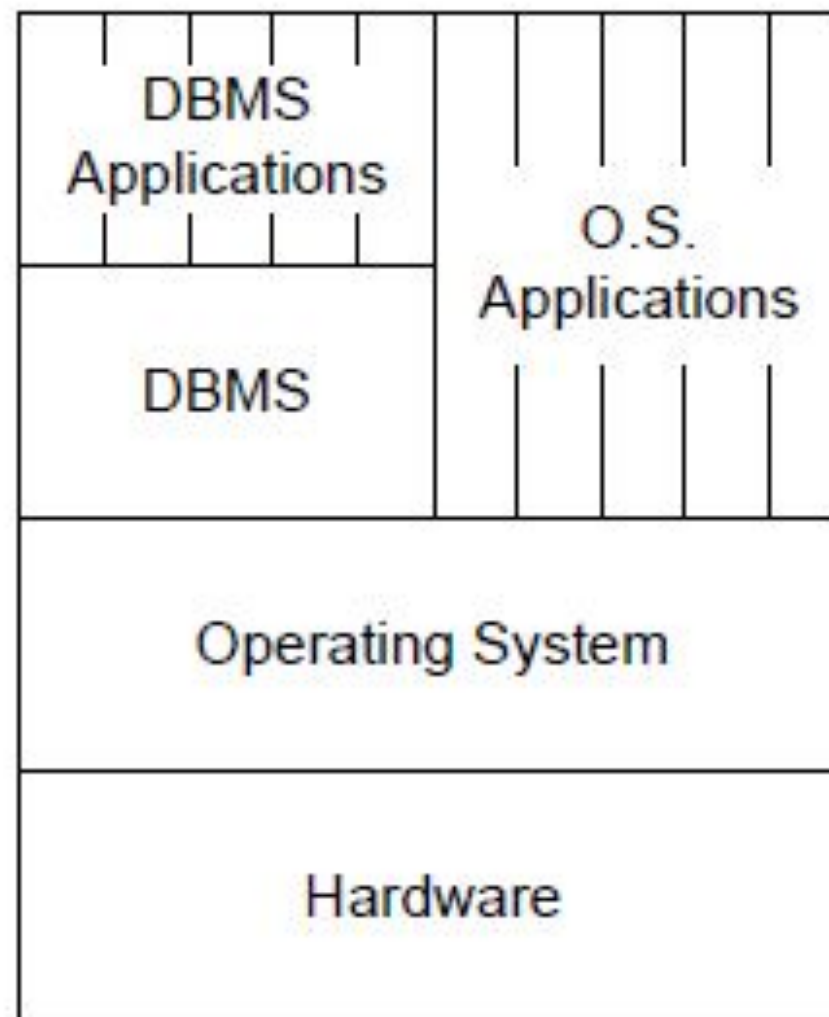
---

- 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.

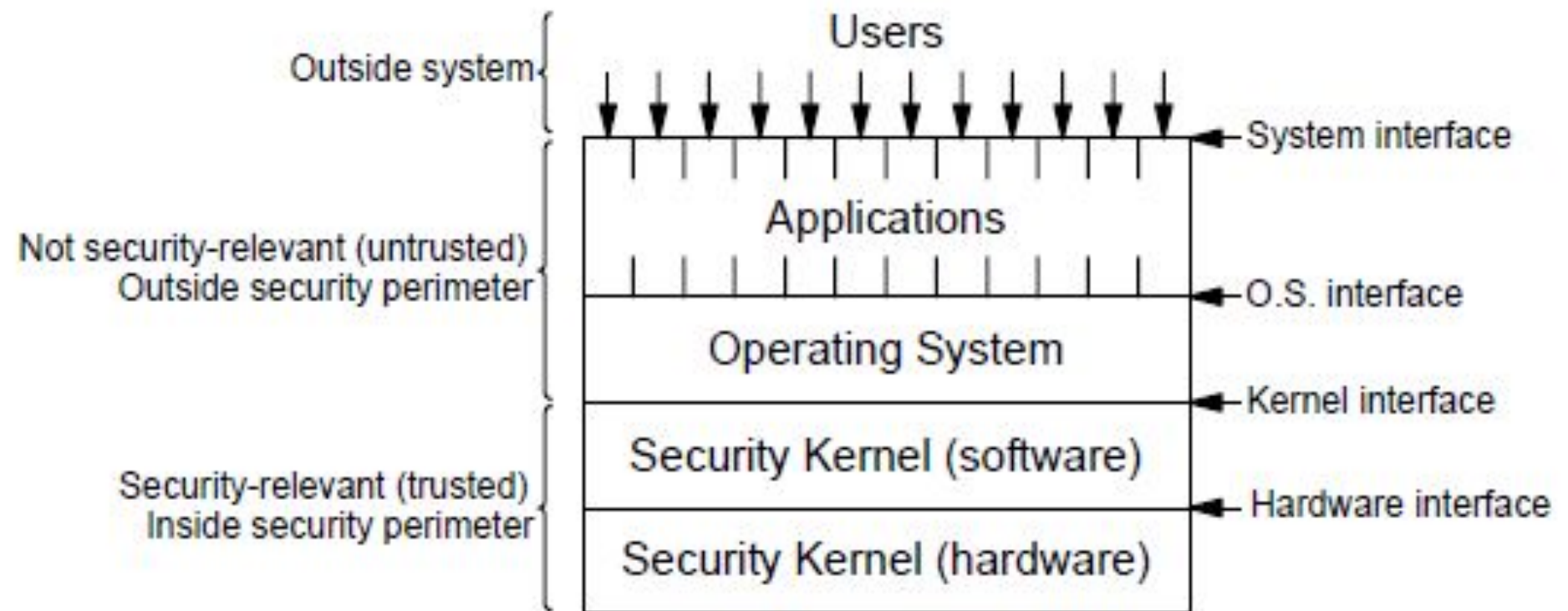
- 
- Pendekatan keamanan kernel adalah metode membangun sebuah sistem operasi yang menghindari masalah keamanan yang melekat dalam desain konvensional  
(Ames, Gasser, dan Schell 1983)

- 
- 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.



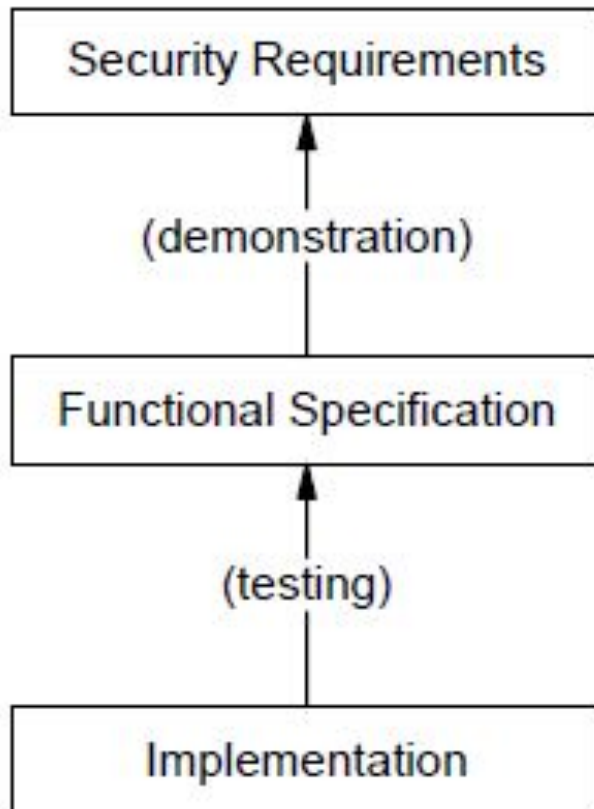
- 
- Karena akses terhadap perangkat keras terbatas, sedangkan ada lebih dari satu program yang harus dilayani dalam waktu yang bersamaan, maka kernel juga bertugas untuk mengatur kapan dan berapa lama suatu program dapat menggunakan satu bagian perangkat keras tersebut. Hal tersebut dinamakan sebagai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

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

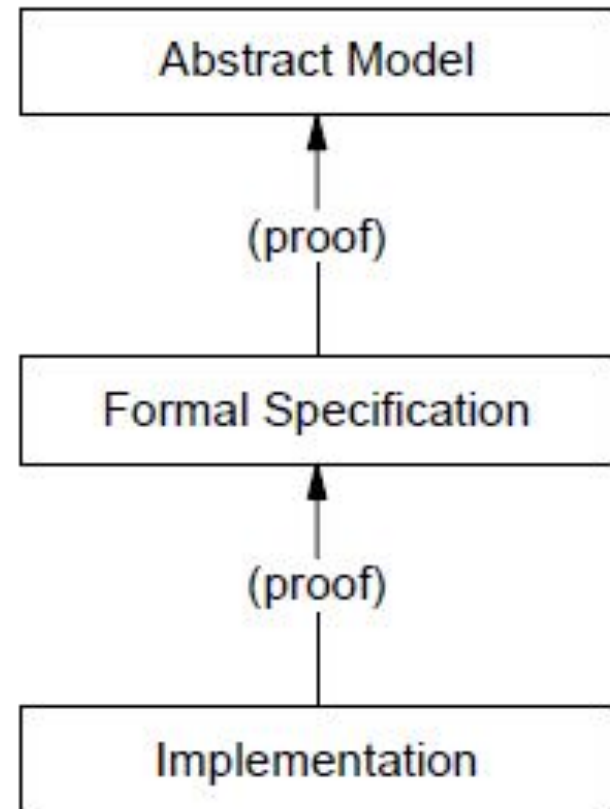


# System Development Process for a Secure System

## 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 keamanan 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

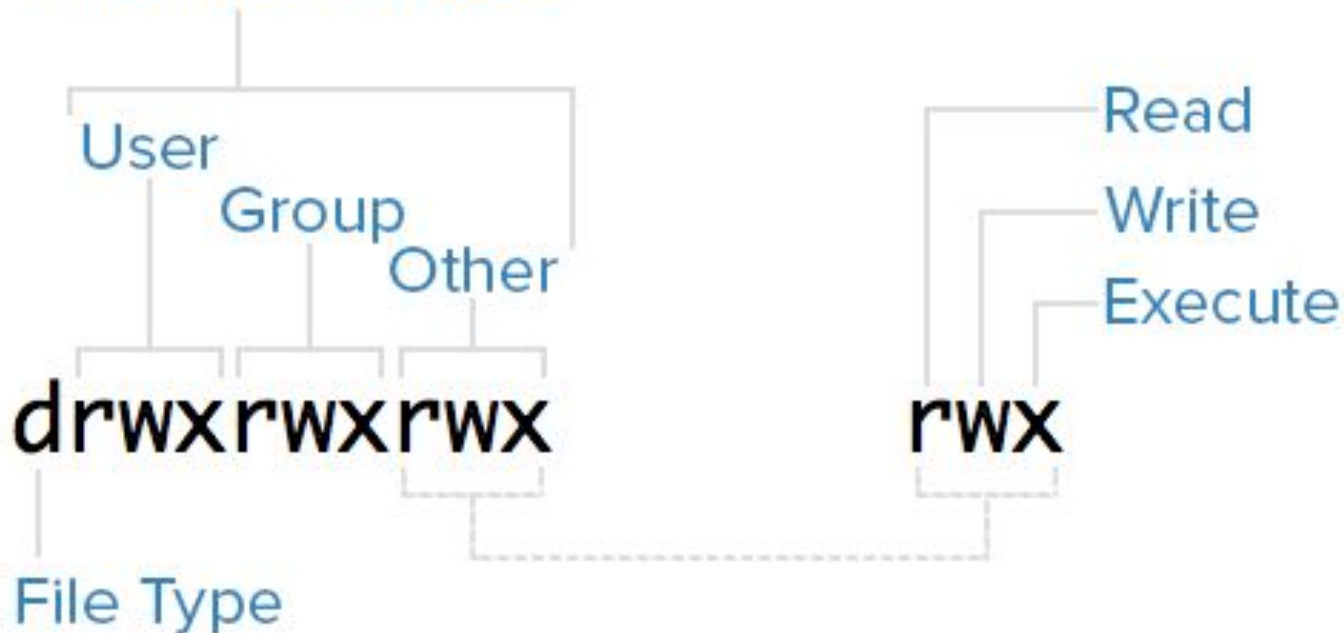
chmod 777

  
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

## Permissions Classes



ref:

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

# in Windows

User Accounts



Control Panel > All Control Panel Items > User Accounts



Search Control Panel



Control Panel Home

Manage your credentials  
Create a password reset disk

Configure advanced user  
profile properties  
Change my environment  
variables

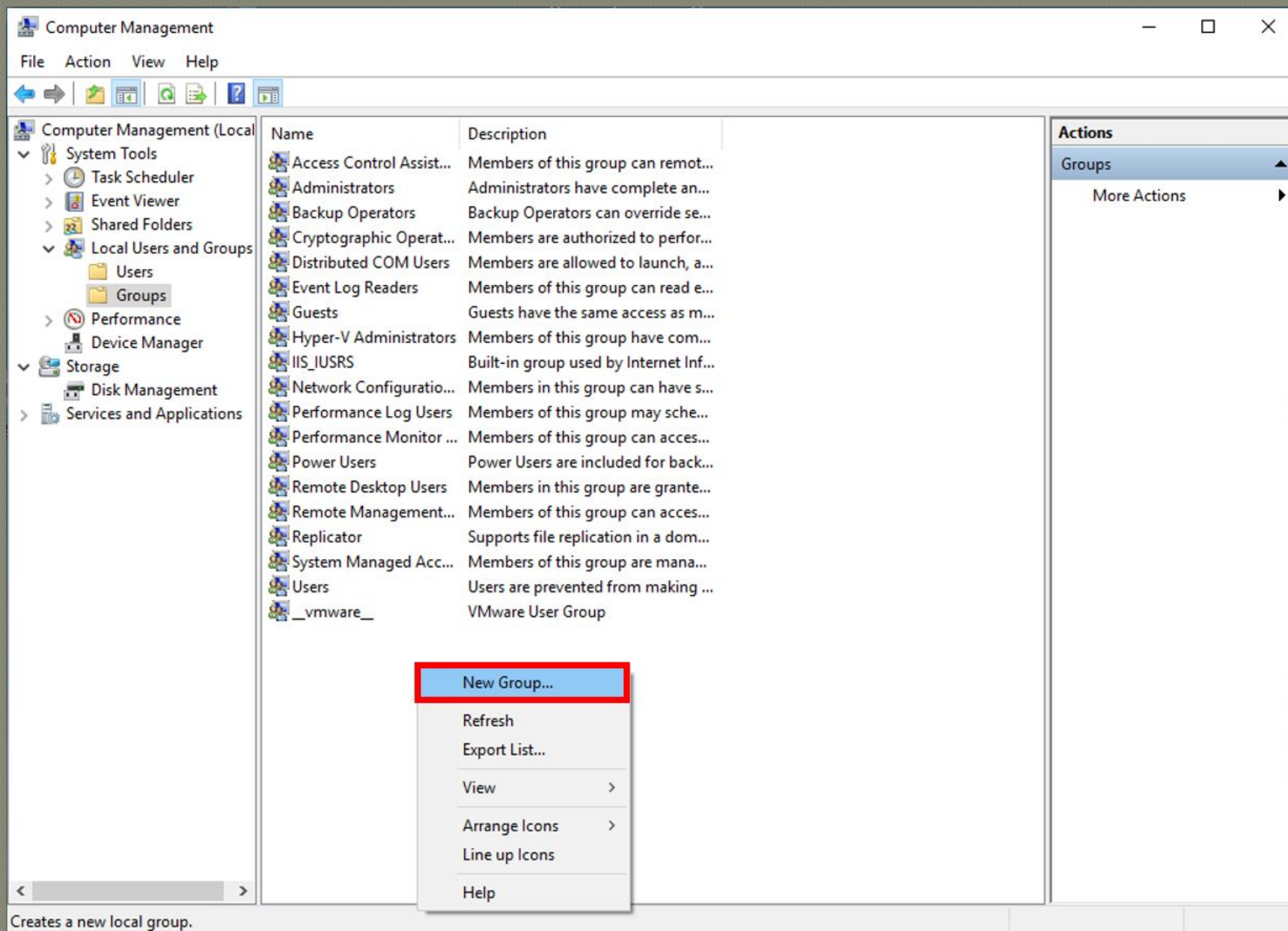
## Make changes to your user account

Make changes to my account in PC settings

Change your account name  
Change your account type

Manage another account  
Change User Account Control settings

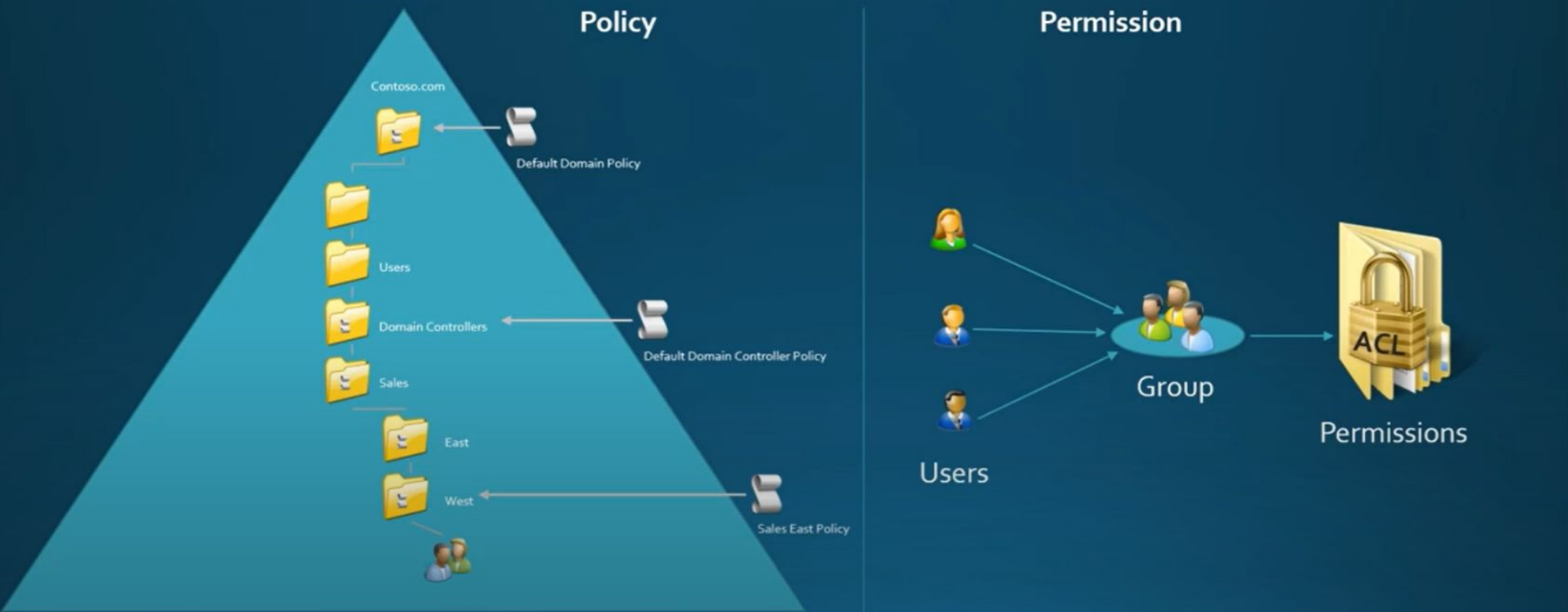




Ref: <https://www.youtube.com/watch?v=GD-jxhocJZU>

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

# Organizational Units vs. Groups



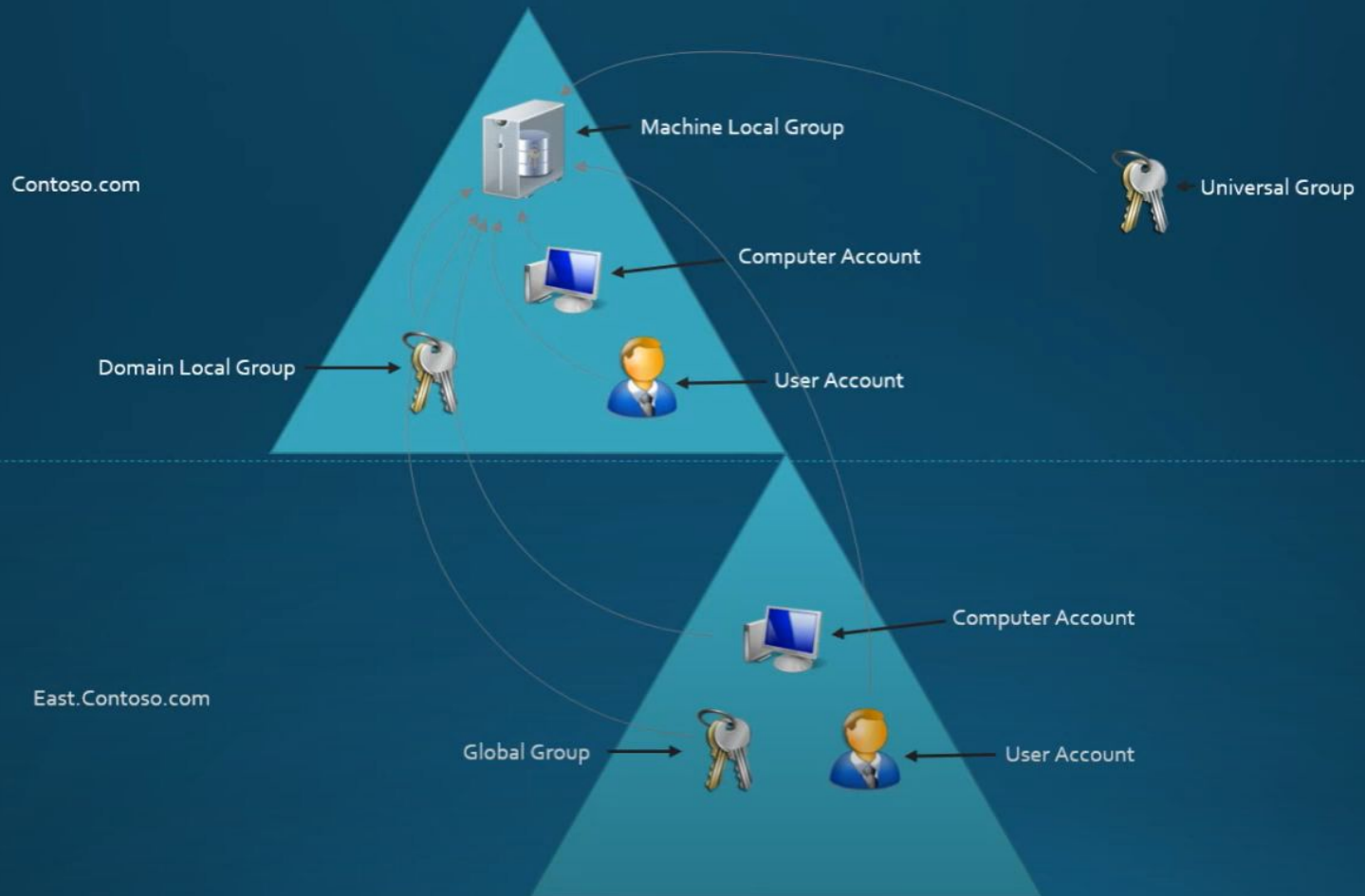


# Creating Groups

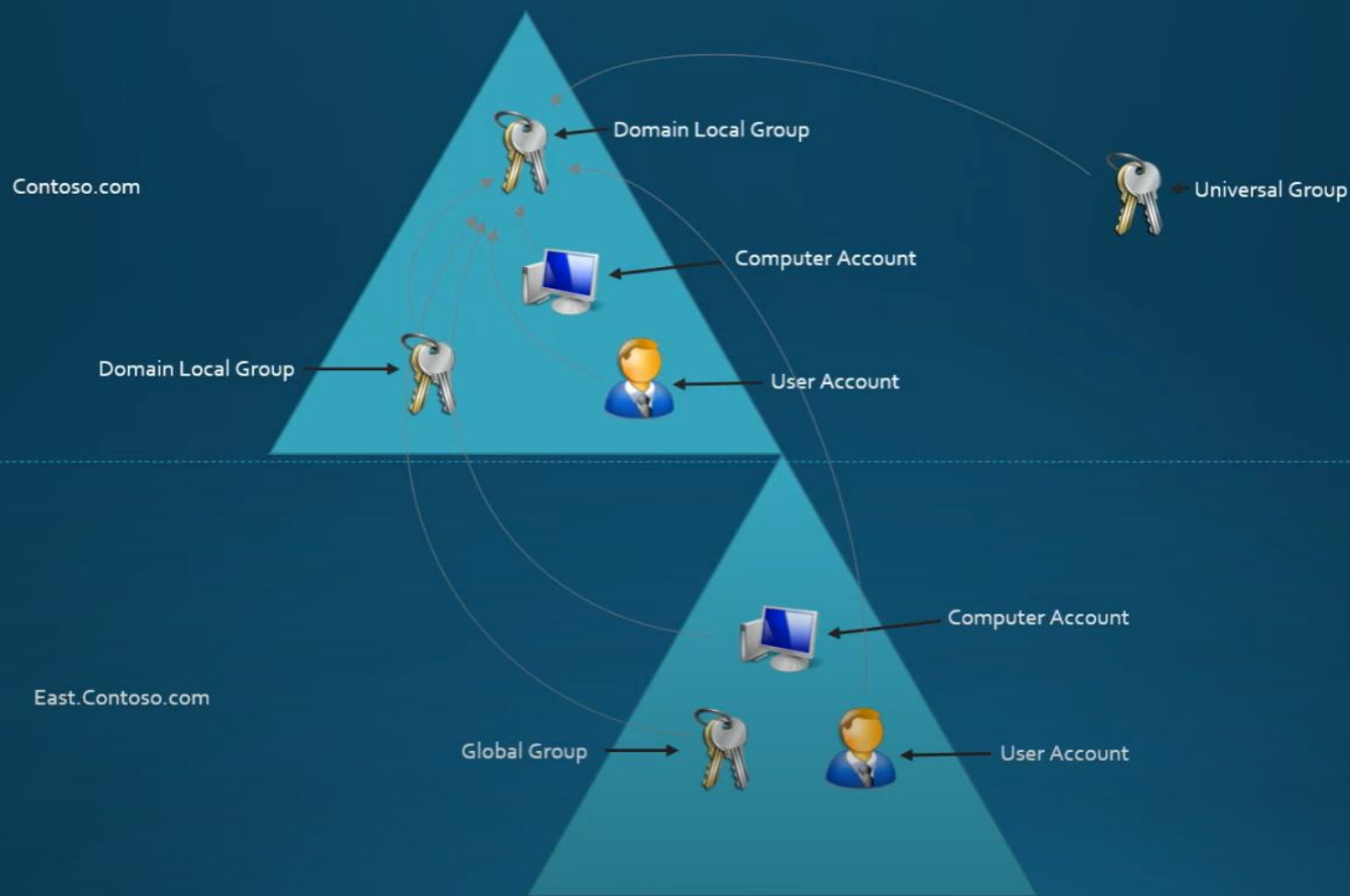
- GUI
  - ADUC – Active Directory Users and Computers
  - ADAC – Active Directory Administrative Center
- Command Line
  - DS Command
    - dsadd group <GroupDN>
  - PowerShell
    - New-ADGroup -Name <Group Name> -SamAccountName <SAM name> -GroupCategory Distribution|Security -GroupScope DomainLocal|Global|Universal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



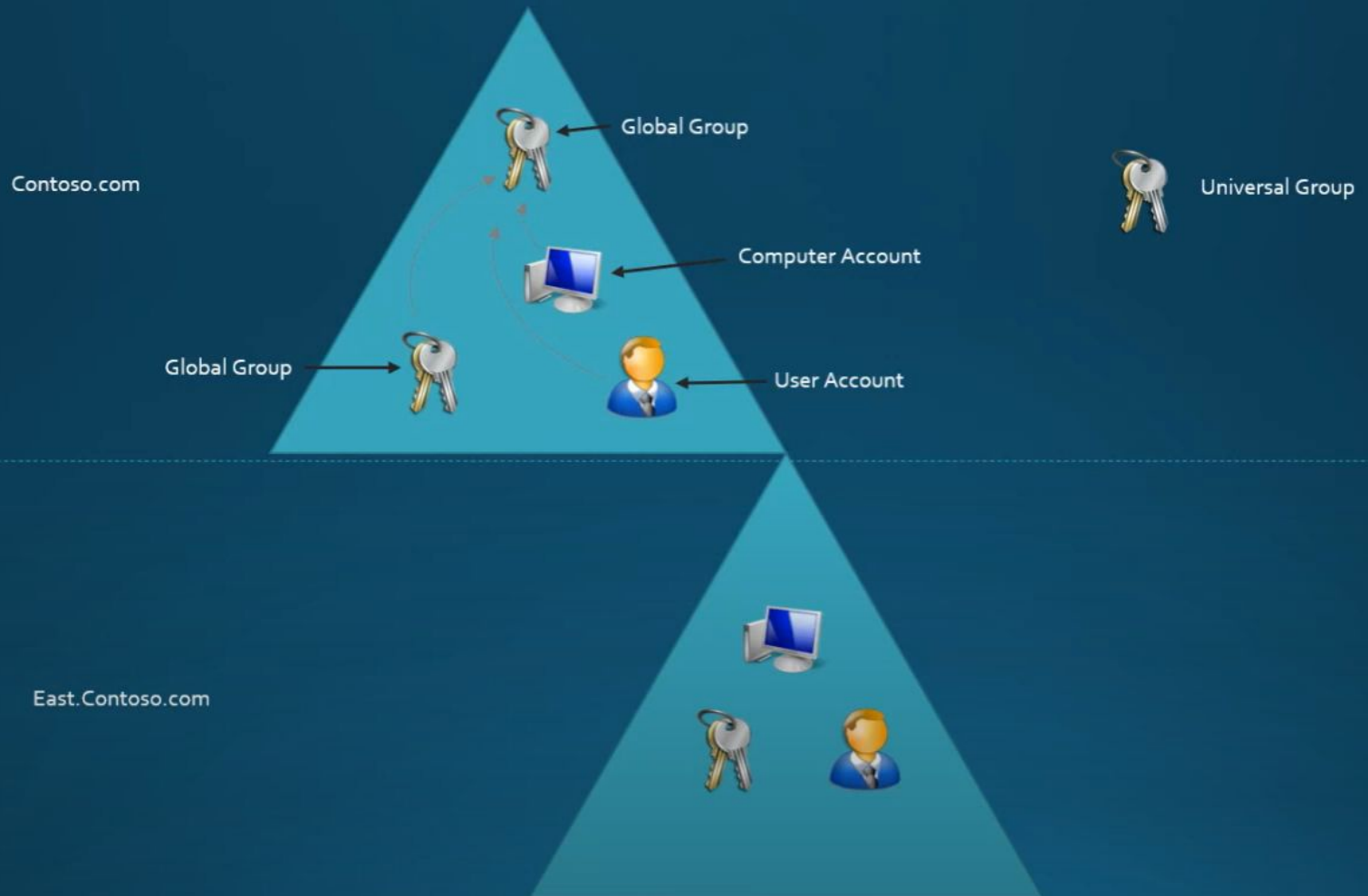
# Machine Local Groups



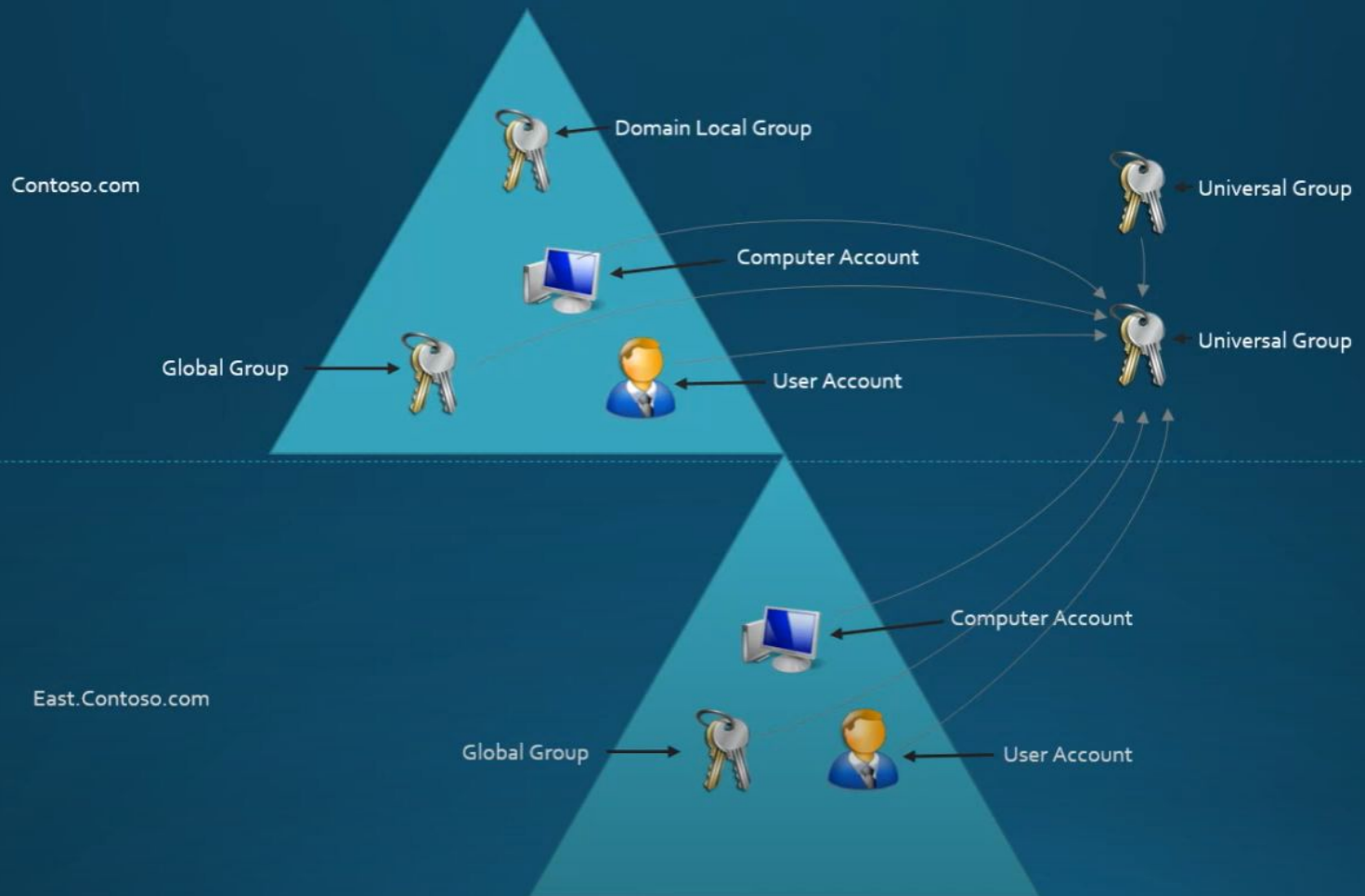
# Domain Local Groups



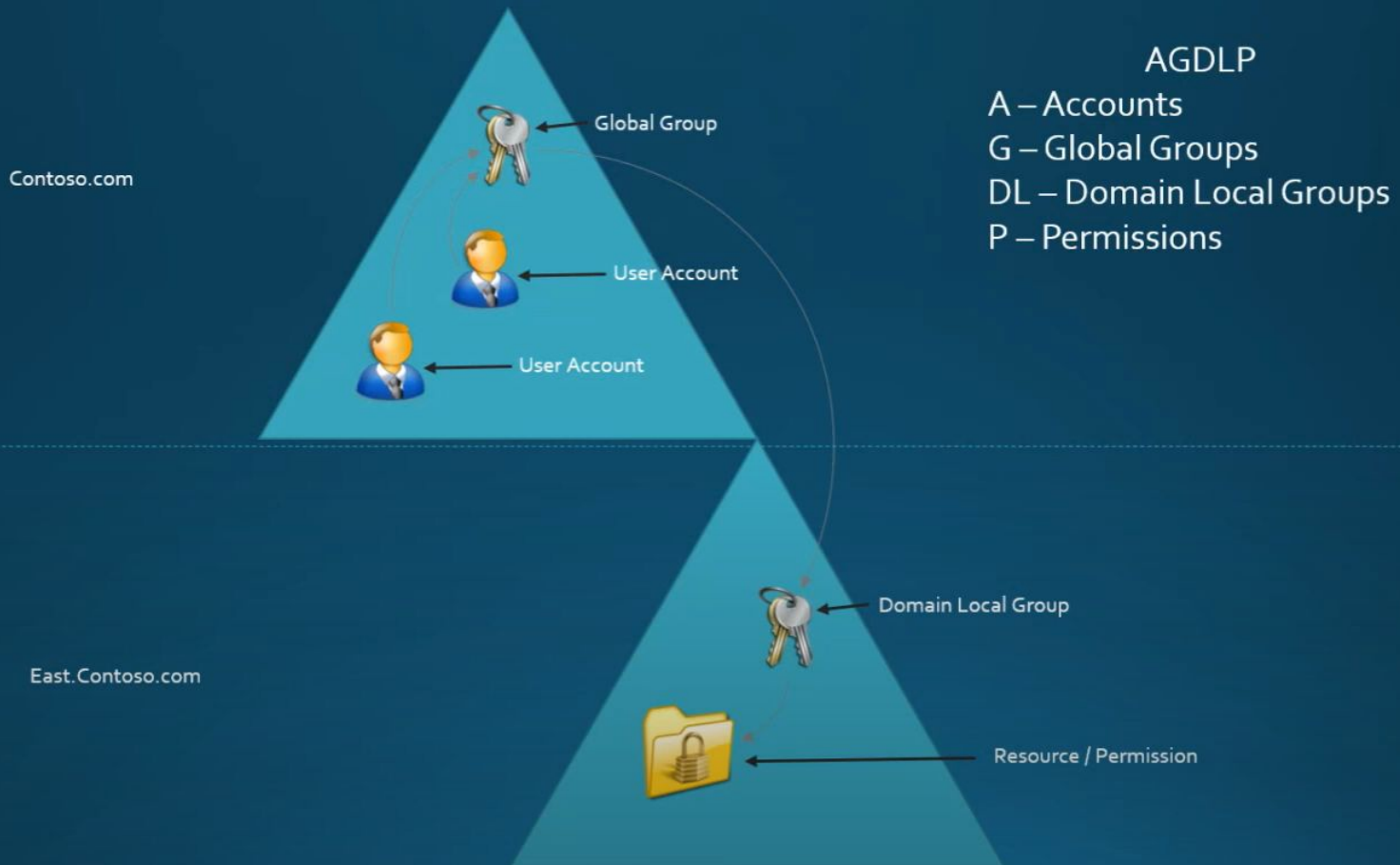
# Global Groups



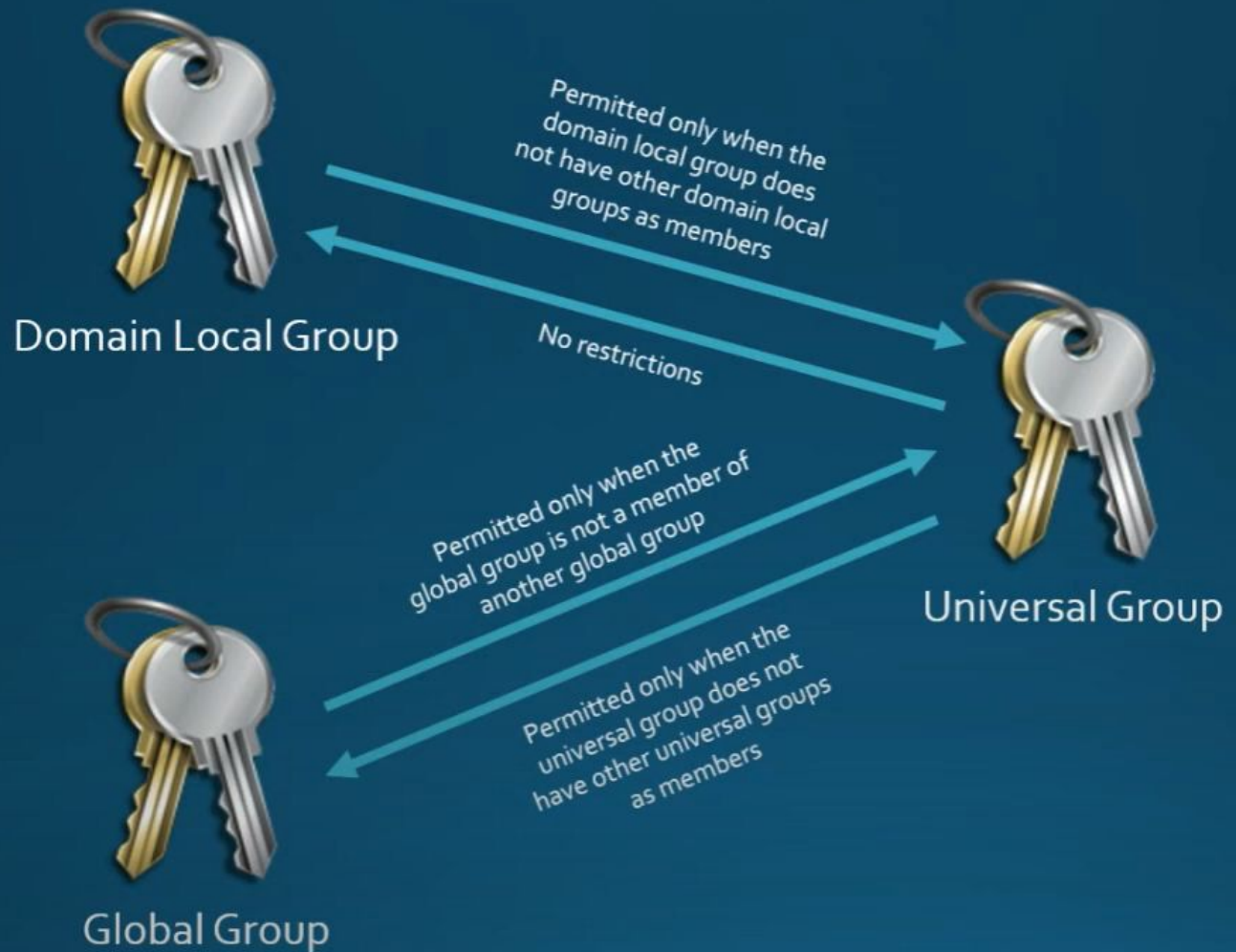
# Universal Groups



# Nesting Groups



# Group Conversion





- 
- 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

