Cyber Security 0010

RMUTT

CH2 Exploring Control Types and Methods

CompTIA Security+

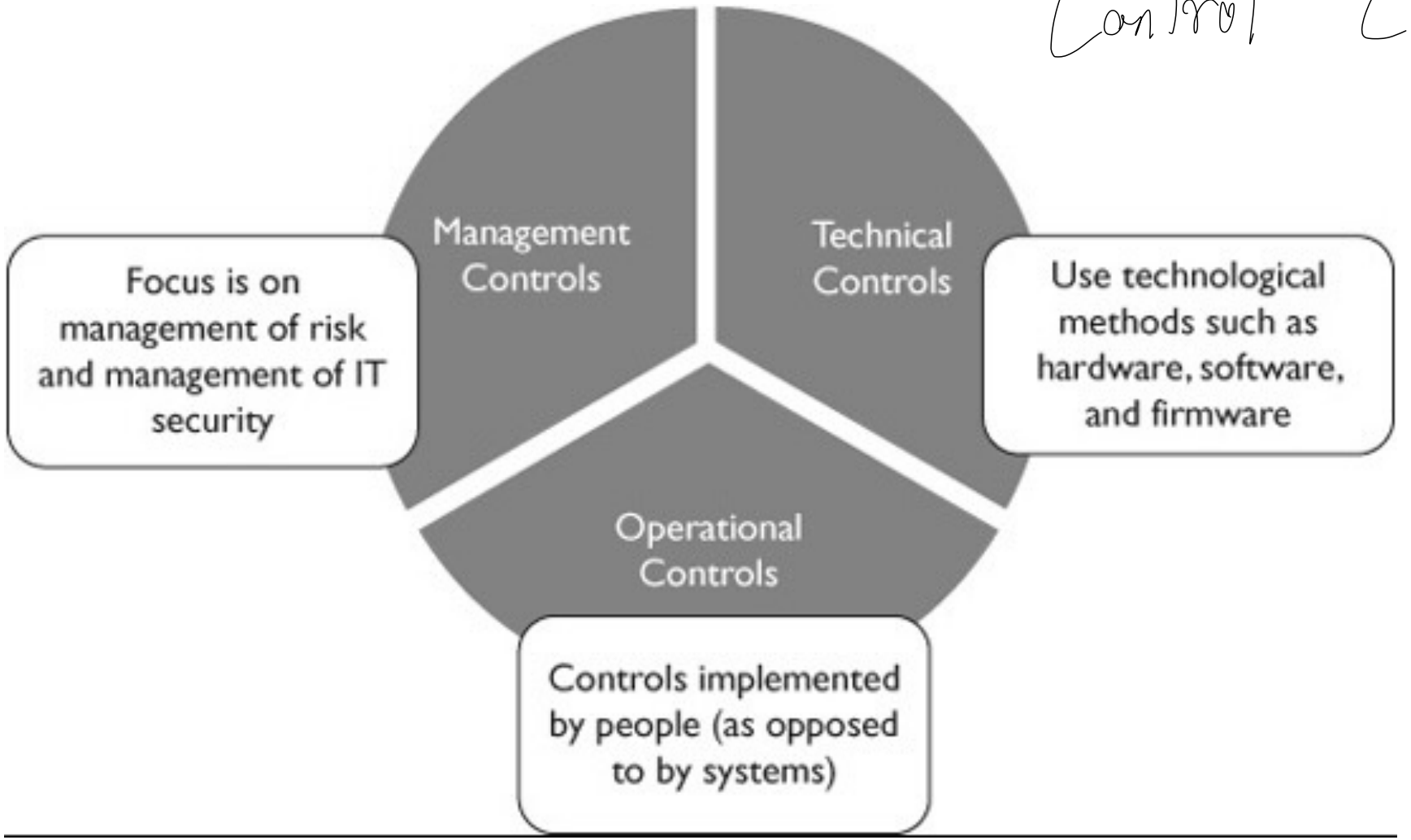
0100010101111000011100000110110001101111011100100110100101101
1100110011100100000010000110110111101101110011101000111001001
1011110110110000100000010101000111100101110000011001010111001
1100100000011000010110111001100100001000000100110101100101
0111010001101000011011110110010001110011

Introduction

1. Understanding control types
2. Comparing physical security controls
3. Implementing logical access controls
4. Comparing access control models

Comparing the Classes of Controls

Control Class ☆



https://www.safaribooksonline.com/library/view/sscp-systems-security/9780071771566/lev225.html

Electrosoft

NIST SP 800-53 Rev 3

ID	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

- **Title**: Recommended Security Controls for Federal Information Systems and Organizations
- **Published:** August 2009
- **Approach**: Risk Management Framework
  - Categorize Information System
  - Select Security Controls
  - Implement Security Controls
  - Assess Security Controls
  - Authorize Information System
  - Monitor Security Controls
- **18 families** of Security Controls

Control Goals

Preventive controls

- Attempt to prevent an incident from occurring
- Hardening, training, guards, change management, disabling accounts

Detective controls

- Attempt to detect incidents after they have occurred
- Log monitoring, trend analysis, security audit, video surveillance, motion detection

Corrective controls

- Attempt to reverse the impact of an incident
- Active IDS (Intrusion Detection System), backups, system recovery

Control Goals

Deterrent

- Attempt to discourage individuals from causing an incident
- Cable locks, hardware locks

Compensating

- Alternative controls used when a primary control is not feasible
- TOTP (Time-based One-Time Password) instead of smart card

Control Goals (CISSP)

Type of Control	Administrative	Technical	Physical
Directive	- Policy	- Configuration Standards	- Authorized Personnel Only Signs - Traffic Lights
Deterrent	- Policy	- Warning Banner	- Beware of Dog Sign
Preventative	- User Registration Procedure	- Password Based Login	- Fence
Detective	- Review Violation Reports	- Logs	- Sentry - CCTV
Corrective	- Termination	- Unplug, isolate, and terminate connection	- Fire Extinguisher
Recovery	- DR Plan	- Backups	- Rebuild
Compensating	- Supervision - Job Rotation - Logging	- CCTV - Keystroke Logging	- Layered Defense

Control Type

1. Physical Control
2. Logical Control

Physical Security Controls

Physical Security Controls

- Defense in depth with boundaries
  - Perimeter (ขอบเขตของพื้นที่) layer แรกสุด
  - Building
  - Secure work areas
  - Server and network rooms
  - Hardware (such as cable locks)

https://www.indiamart.com/proddetail/computer-cable-lock-2m-20908425188.html

Physical Security Controls

- Door access systems
  - Cipher locks
  - Proximity cards
  - Biometrics
- ID badges

Physical Security Controls

- Tailgating (Turnstile) and mantraps
- Security guards, access lists, and logs
- Video surveillance (CCTV)
- Fencing, lighting, and alarms
- Barricades and signs
- Hardware locks
  - Doors, locked cabinets, and safes

Physical Security Controls

Turnstile gate

https://www.grainger.com/product/TURNSTILE-Hi-Gate-Turnstile-3YMF1

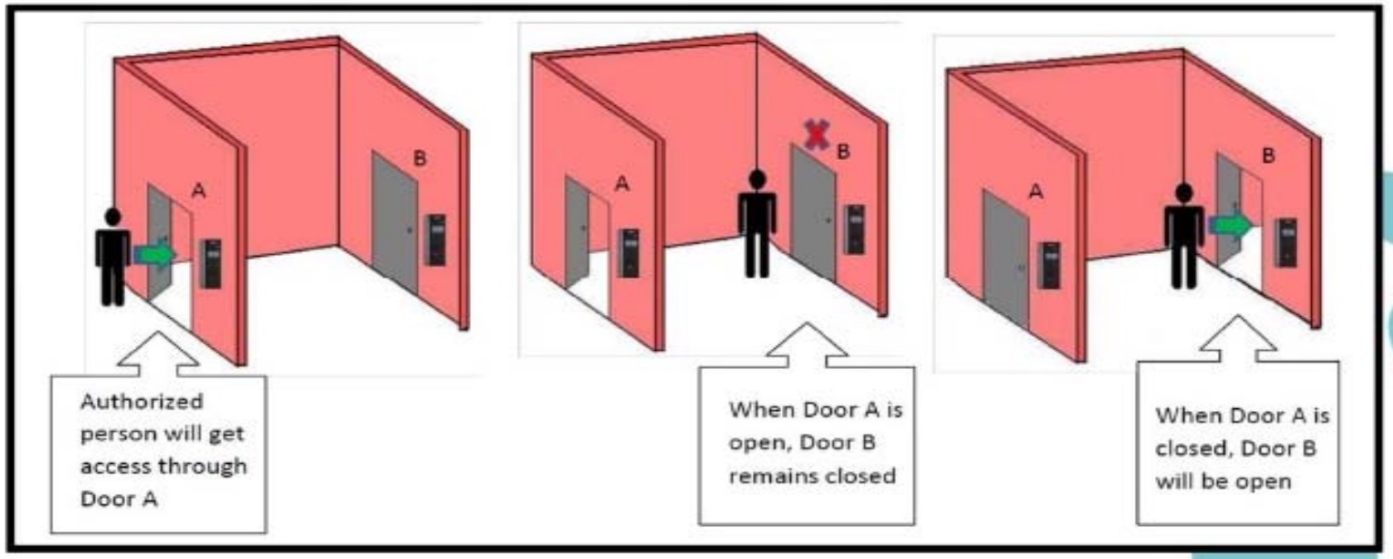
https://www.indiamart.com/primedoor-automation/tripod-turnstile-gate.html

https://www.alibaba.com/product-detail/Pedestrian-waist-height-swing-turnstile-tourniquet_60020947855.html

Physical Security Controls

Man-Trap (Deadman door)

- Useful for Multiple Doors, Arranged in a Sequence
- Regulate Opening and Closing of Doors
- Second Door will Open only After First Door has Closed
- Manage Traffic and Control Dust and Heat
- Useful to Restrict Intruder from Escaping the Premises Quickly



http://www.slideshare.net/GbsHyd1/matrix-cosec-acm-presentation-v1-r1

Logical access Controls

Need-to-know

Subjects should only have access to objects that enables them to perform their assigned job functions.

Least privilege

Subjects should only have sufficient access privilege that allows them to perform their assigned work.

Logical access Controls

Information Security Models

Access Control Matrix

- Access control matrix specifies access relations between Subject-Subject or Subject-Object.
  - One row per subject.
  - One column per subjects or object.

		Object / Subject						
		A	B	C	D	E	F	G
Subject	1							
	2							
	3							
	4							
	5							
	6							
	7							

https://www.slideshare.net/aouyang/8-access-control

Logical access Controls

Principle of least privilege

- Rights identify what a user can do, such as changing the
- system time or rebooting a system
- Permissions define access to resources, such as being able to read or modify a file
- Rights and permissions combined called privileges
- Least privilege ensures users granted only the rights and permissions needed to perform assigned tasks or functions
- Technical control

Logical access Controls

Separation of duties

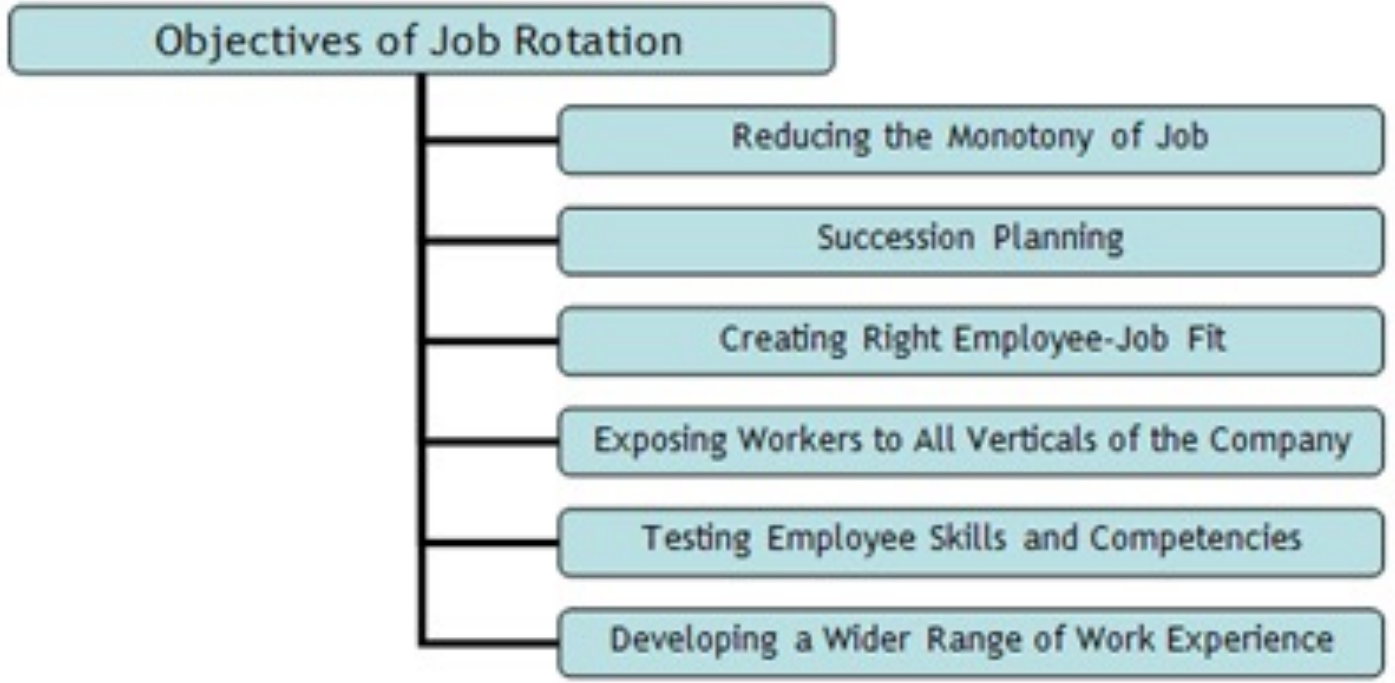
- No single person should be responsible for approving his/her own work.

Job rotation

- To reduce risk of collusion and to ensure no single point of failure.

Mandatory vacation

- To allow auditors to review records.



https://www.managementstudyguide.com/job-rotation.htm

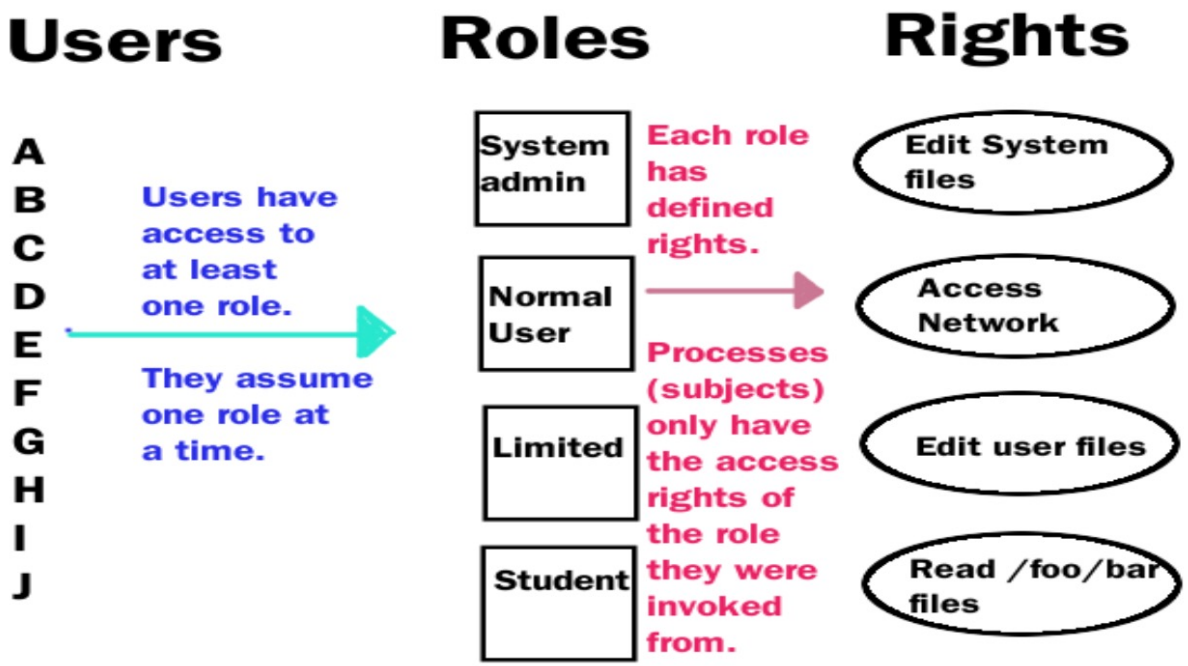
Logical access Controls

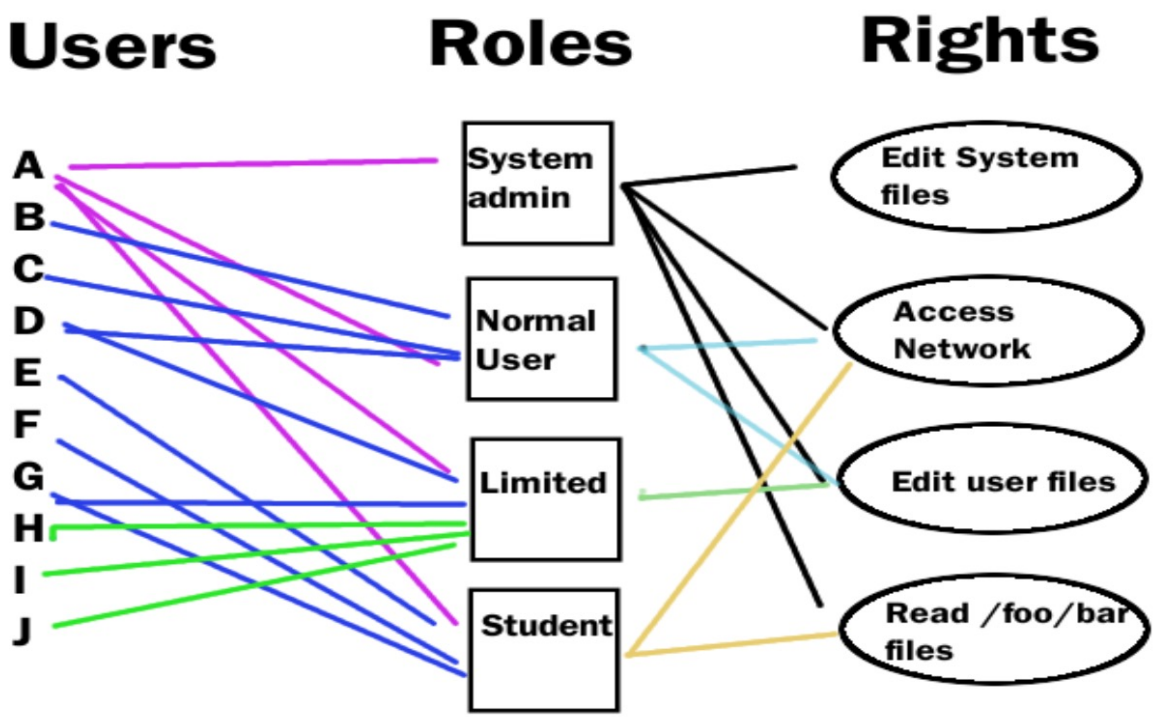
Access Control Types

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

Logical access Controls

Role Based Access Control (RBAC)

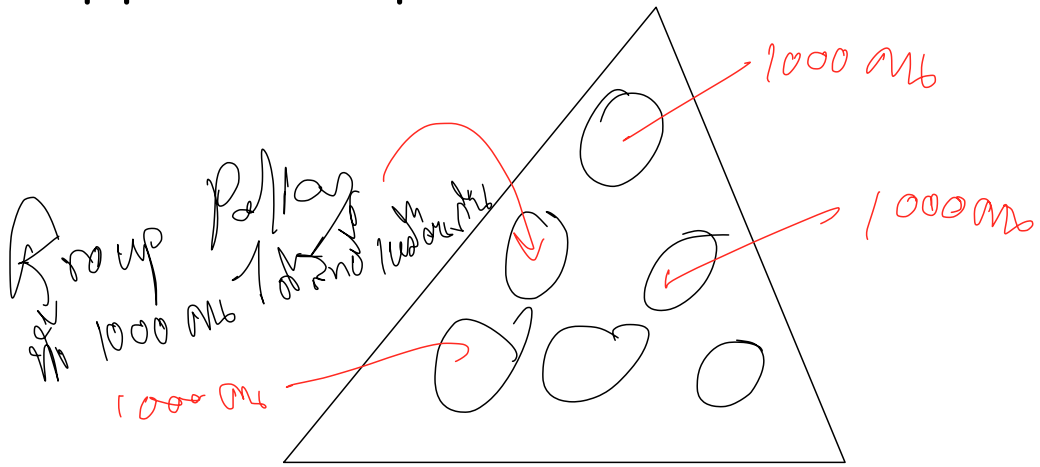




Logical access Controls

Group Policy

- Implemented on a domain controller
- Local password policy
- Domain password policy
- Application password

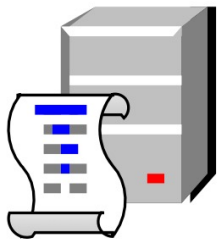


Policy

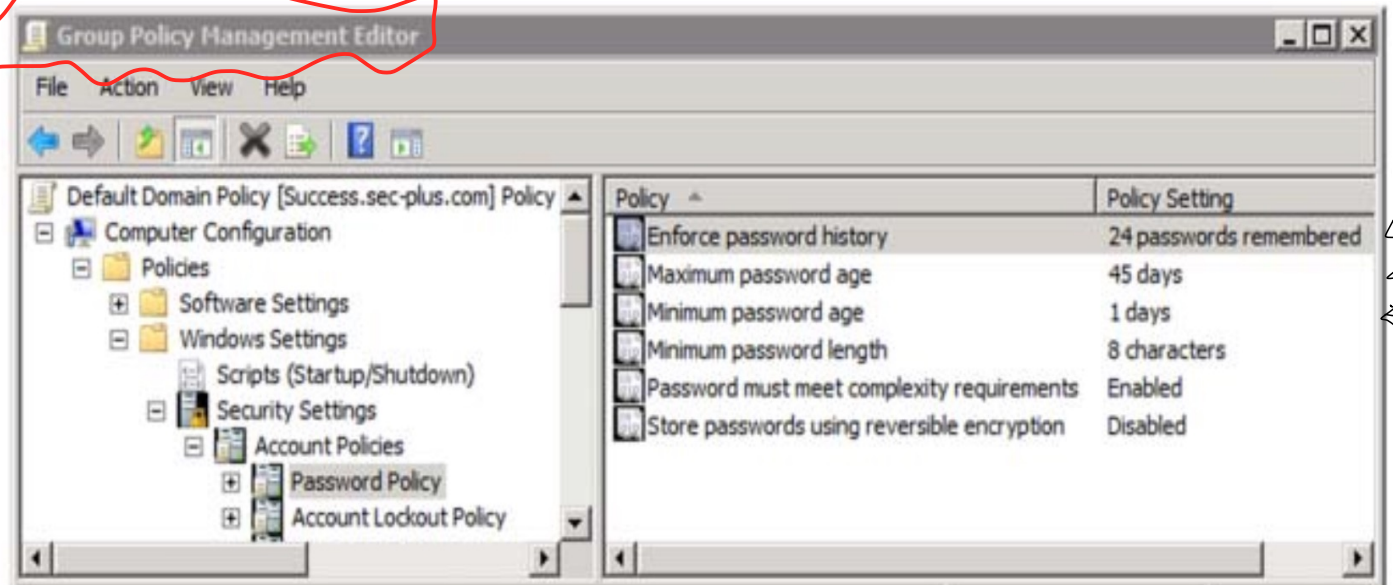
Logical access Controls

Domain Password Policy

- Enforce password history
- Minimum password
- Maximum password age
- Minimum password age
- Length
- Password must meet complexity requirements



Policy

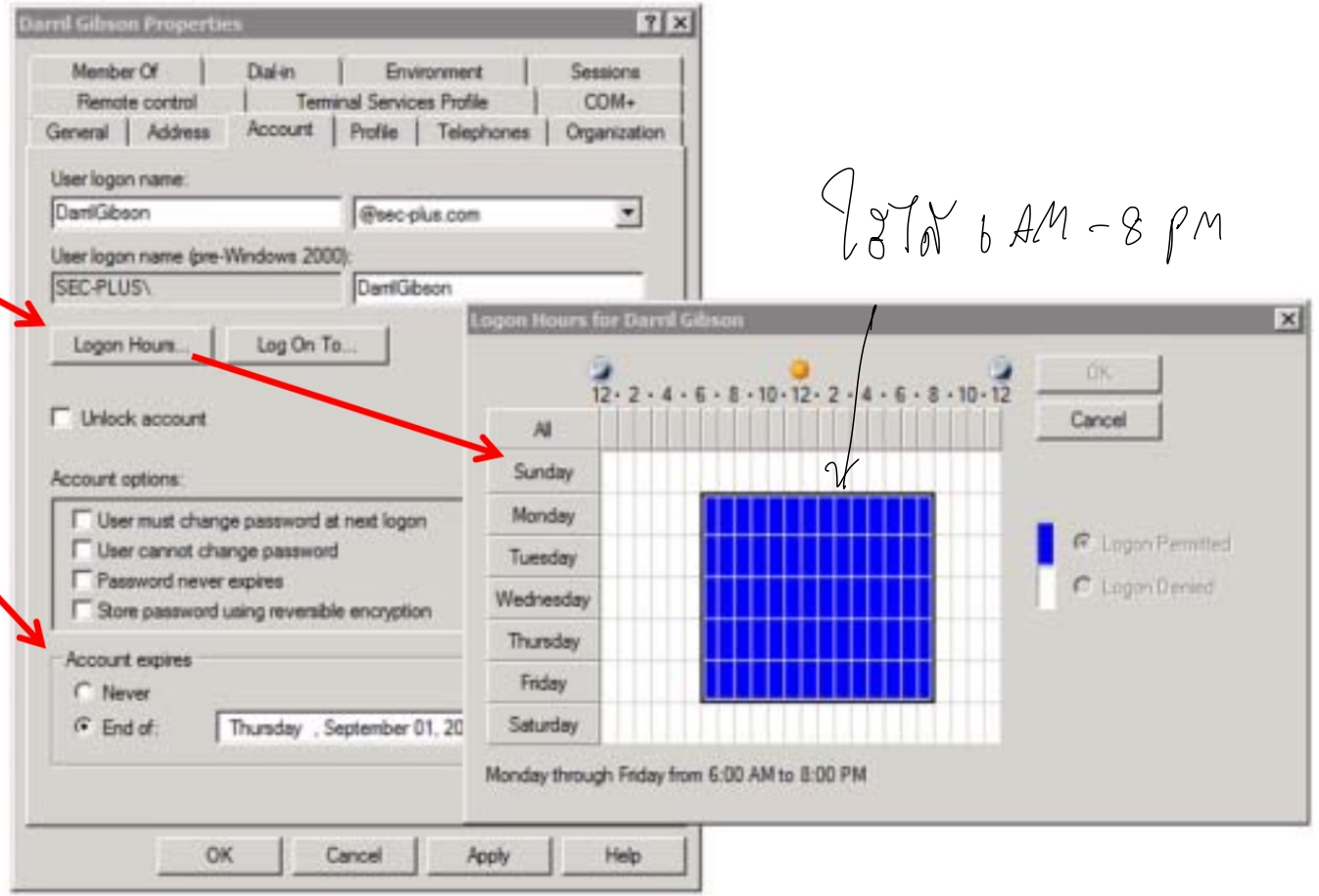


Logical access Controls

1 User

Account Management

- Disabling and deleting accounts
- Recovering accounts
- Prohibiting generic accounts
- Time-of-day restrictions
- Account expiration
- Account access review



Logical access Controls

Comparing Access Control Models

- **Role-Based Access Control (RBAC)**
  - Uses roles (often implemented as groups)
  - Grant access by placing users into roles based on their assigned jobs, functions, or tasks
  - Often use a matrix

Role	Server Privileges	Project Privileges
Administrators	All	All
Executives	None	All
Project Managers	None	All on assigned projects No access on unassigned projects
Team Members	None	Access for assigned tasks Limited views within scope of their assigned tasks No views outside the scope of their assigned tasks

Logical access Controls

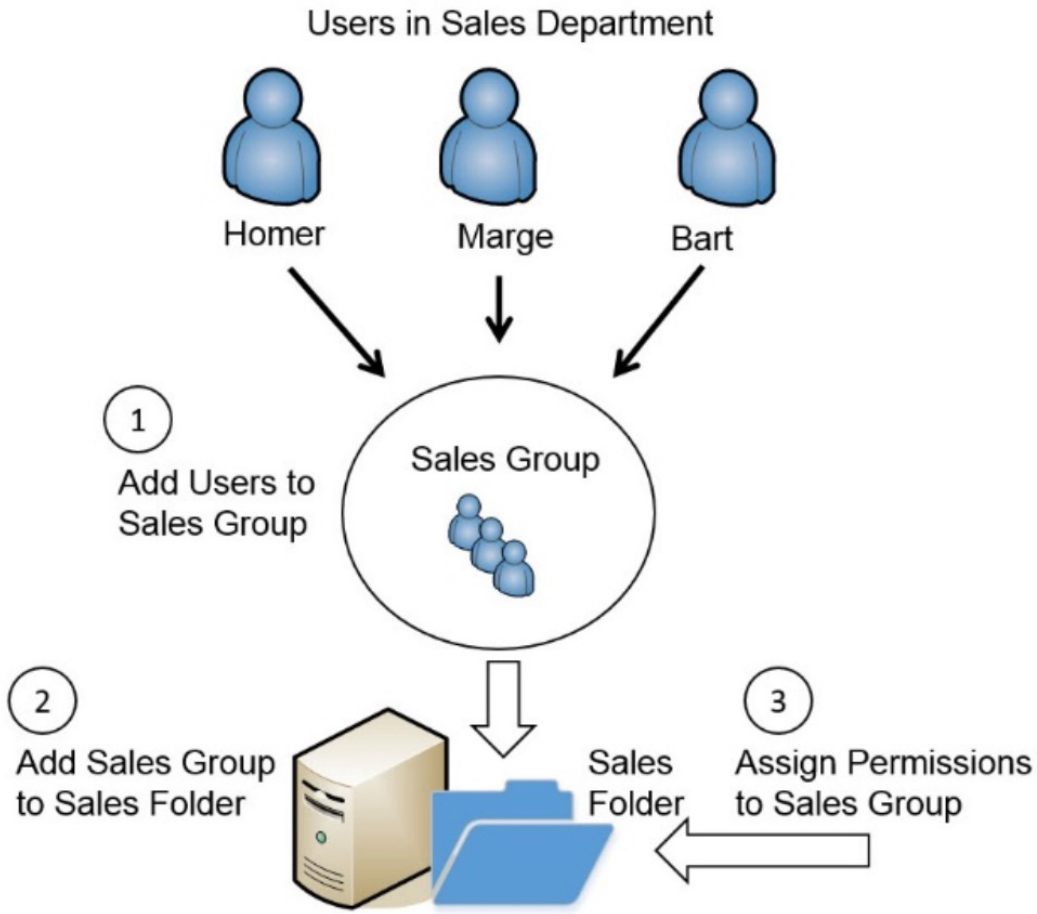
Role-Based Access Control (RBAC)

- A user account is placed into a role or group
- User inherits rights and permissions of the role
- Simplifies administration
- Helps enforce principle of least privilege
- User templates include group membership

Logical access Controls

Group-Based Privileges

1. Create a Sales group and add each of the user accounts to the Sales group
2. Add the Sales group to the Sales folder
3. Assign appropriate permissions to the Sales group for the Sales folder



Logical access Controls

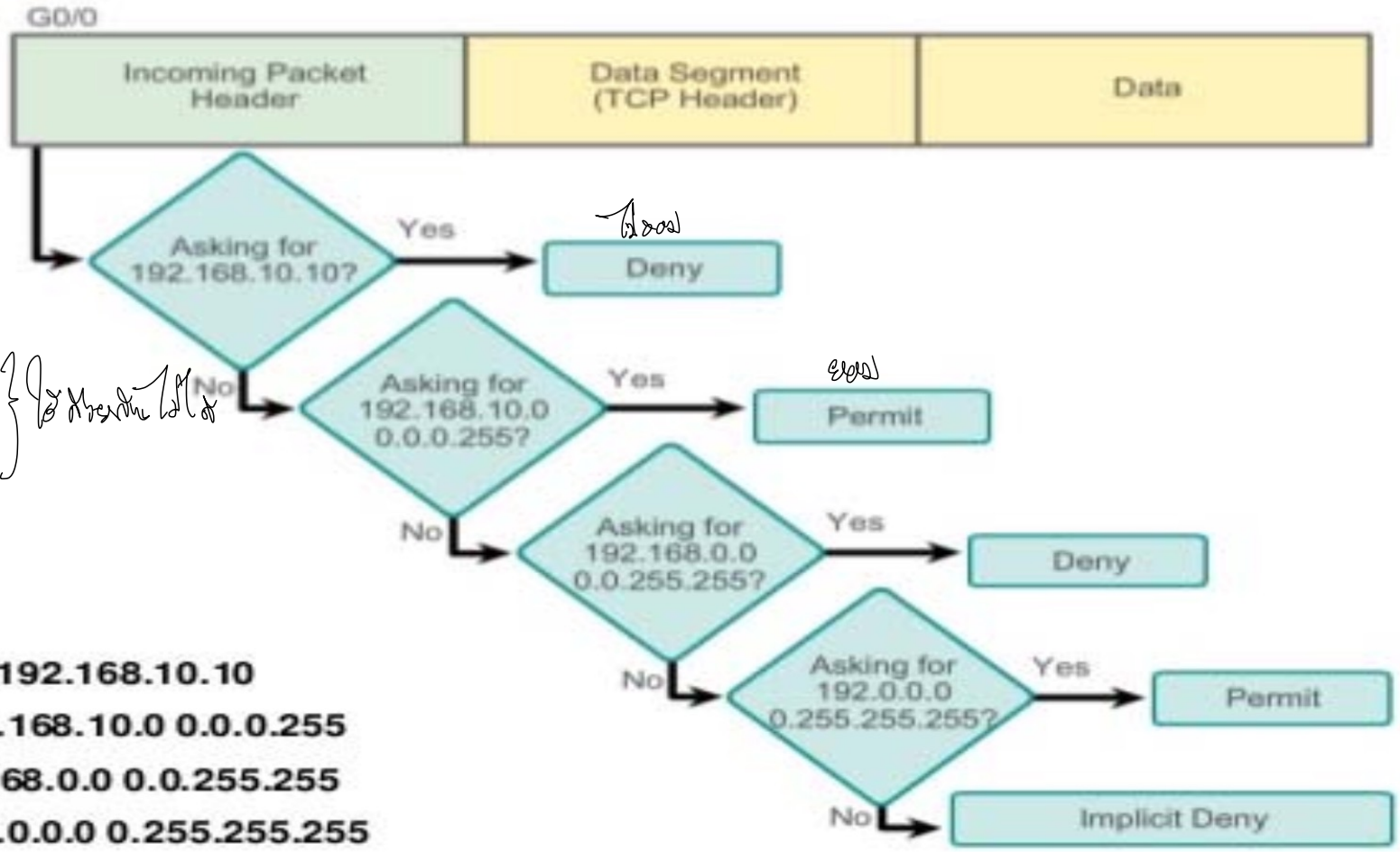
- **Rule-Based Access Control (RBAC)**
  - Access is either allowed or denied based on a set of **predefined rules that are established by the administrator**
  - Example: Limited login hours, Limited BitTorrent traffic
  - Based on a set of approved instructions, such as an access control list.
  - Can use triggers to respond to an event.

https://www.slideshare.net/hawa143/week3-lecture

Logical access Controls

Configure Standard IPv4 ACLs

Configuring a Standard ACL (Access Control List)



Example ACL

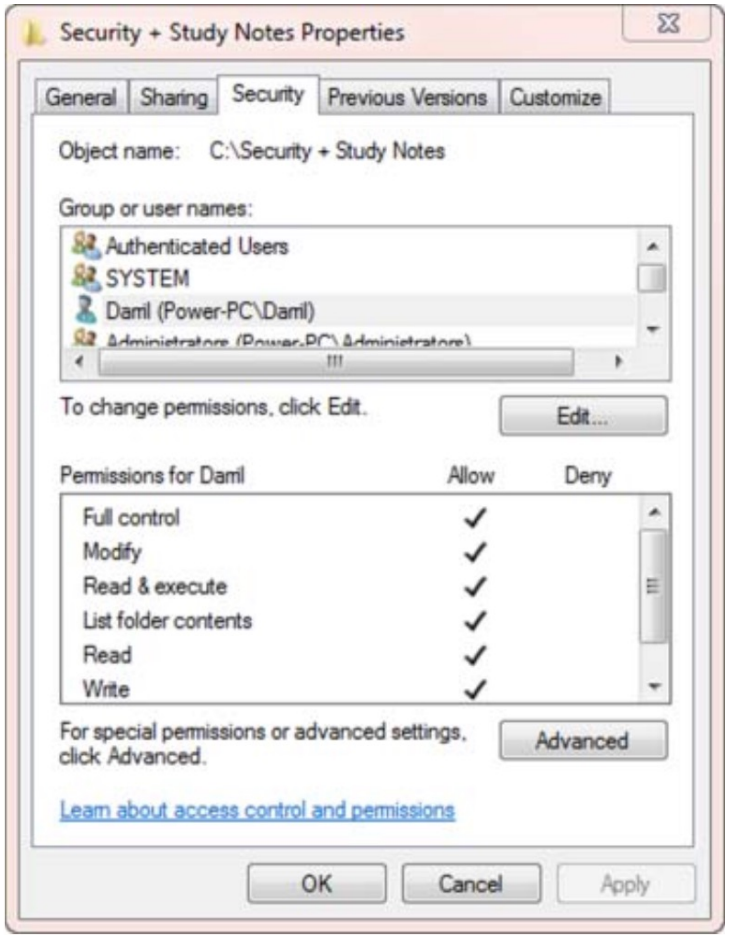
- access-list 2 deny host 192.168.10.10
- access-list 2 permit 192.168.10.0 0.0.0.255
- access-list 2 deny 192.168.0.0 0.0.255.255
- access-list 2 permit 192.0.0.0 0.255.255.255

https://www.slideshare.net/vuzlego/chapter9-access-control-lists

Logical access Controls

Discretionary Access Control (DAC)

- Resources identified as objects
- Files, folders, shares
- Specifies that every object has an owner
- Owner has full, explicit control of the object
- Beware of Trojans
  - Dual accounts for administrators
- Microsoft's NTFS uses the DAC model
- Discretionary access control lists (DACLs, but often shortened to ACLs) form the primary means by which authorization is determined.
  - List of access permissions
- SIDS
  - Uniquely identifies users and groups

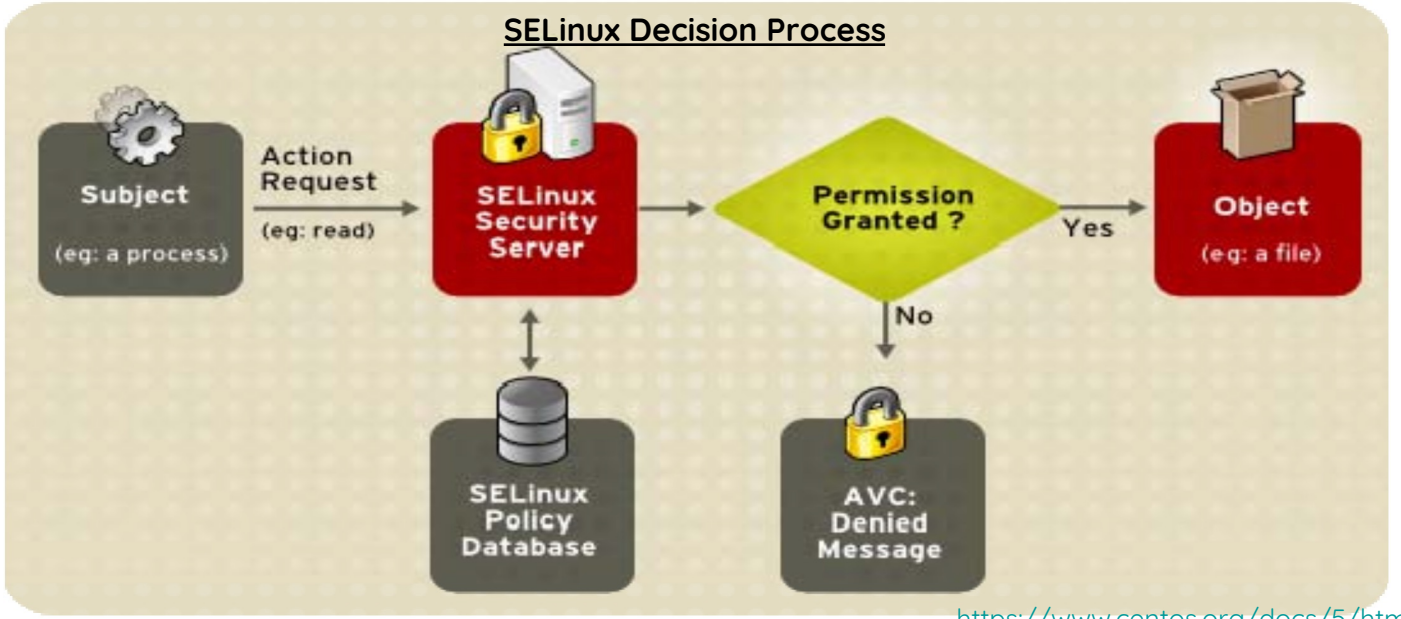


Logical access Controls

Linux

Mandatory Access Control (MAC)

- Uses labels to determine access
- Subjects and objects are assigned labels
- Permissions granted when the labels match
- SELinux (Security-Enhanced Linux)
  - Uses MAC model
  - Helps prevent malicious or suspicious code from executing

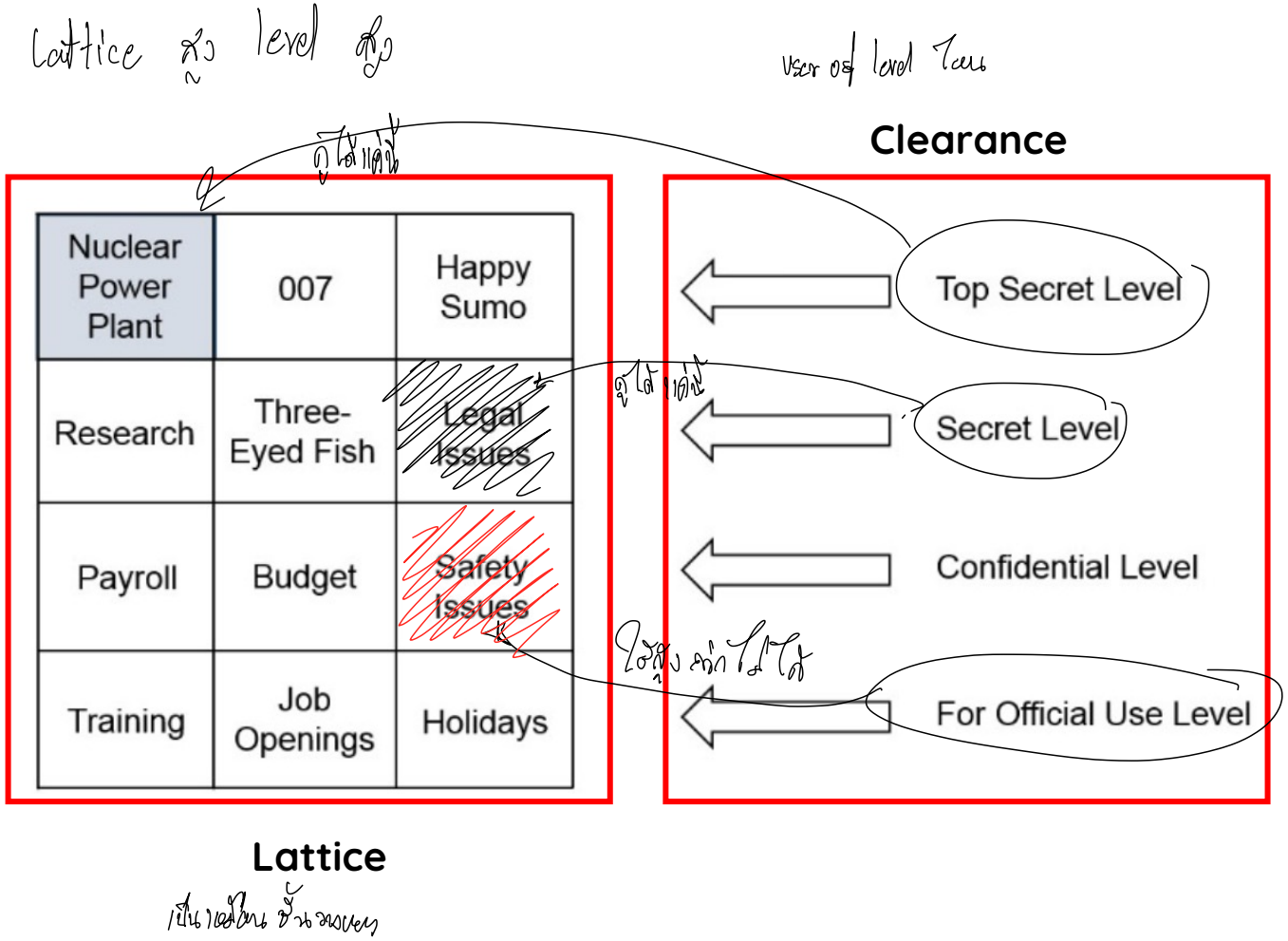


https://www.centos.org/docs/5/html/Deployment_Guide-en-US/ch-selinux.html

Logical access Controls

Lattice (Mandatory Access Control (MAC))

- Imagine that Homer has a Top-Secret clearance with a Nuclear Power Plant label. This gives him access to data within the Nuclear Power Plant compartment. However, he does not have access to data in the 007 or Happy Sumo compartment unless he also has those clearances (and associated labels).
- Higher-level clearances include lower-level clearances. For example, because Homer has a Top-Secret clearance, he can be granted access to Secret and lower-level data. Again though, he will only be able to access data on these lower levels based on his need to know.

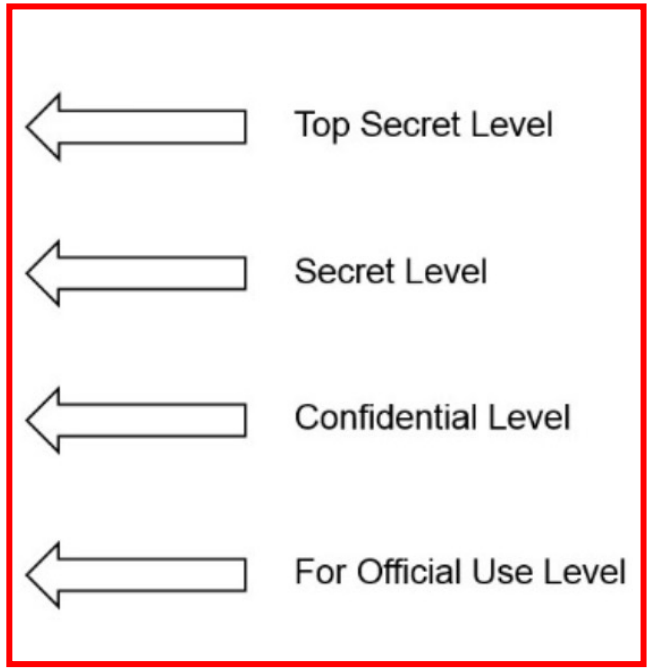


Logical access Controls

Lattice (Mandatory Access Control (MAC))

- As another example, imagine that Lisa has a Secret level clearance.
- Administrators can grant her access to data on the Secret level and lower levels, based on her need to know.
- For example, they might grant her access to the Research data by assigning the Research label to her, but not necessarily grant her access to Three-Eyed Fish or Legal Issues data. However, they cannot grant her access to any data on the Top Secret level.

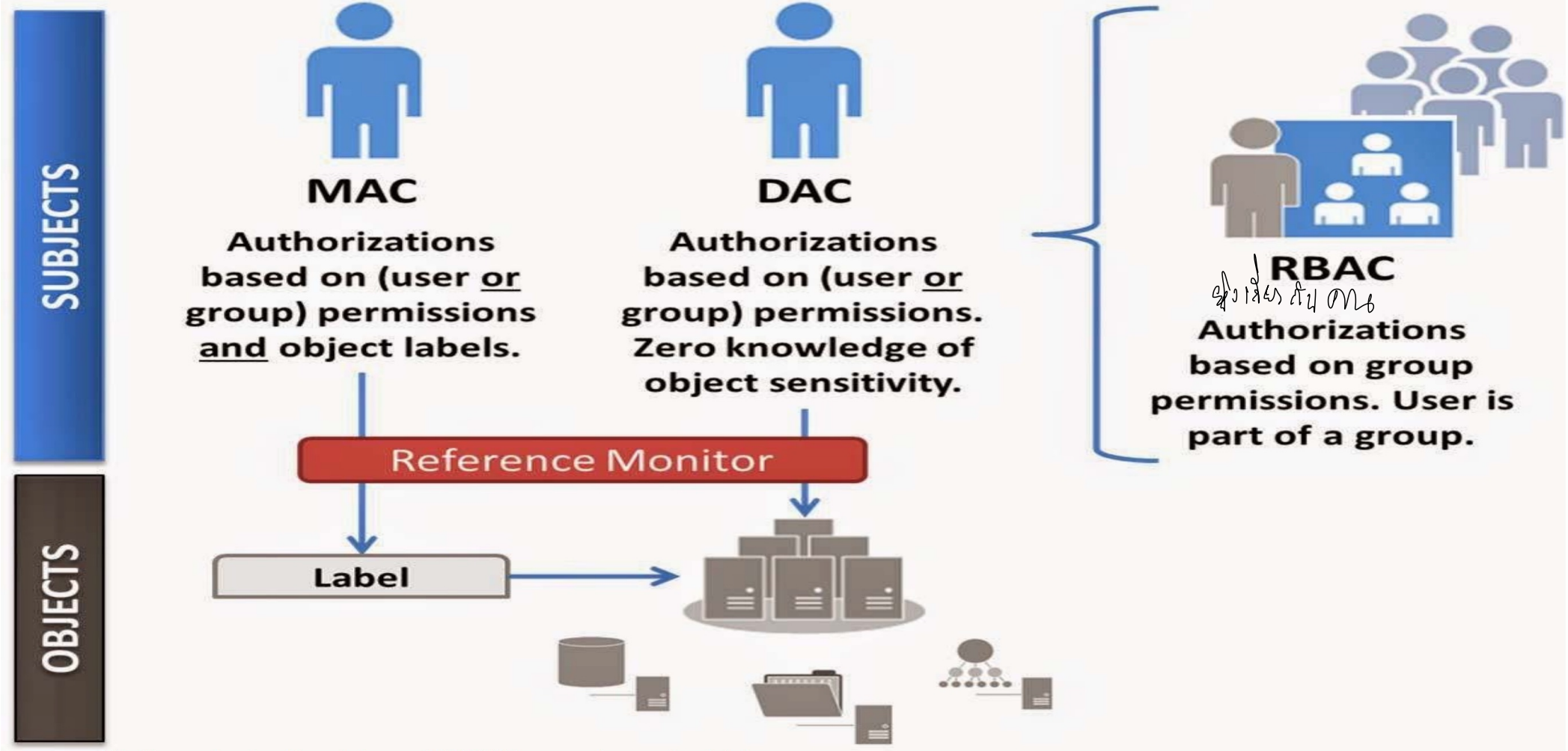
Lattice



Logical access Controls

RBAC ก็เป็น subset ของ DAC

MAC vs DAC vs RBAC



http://www.cloudauditcontrols.com/2014/09/mac-vs-dac-vs-rbac.html

Logical access Controls

Chapter 2 Summary

- Understanding control types
- Comparing physical security controls
- Implementing logical access controls
- Comparing access control models


Q&A