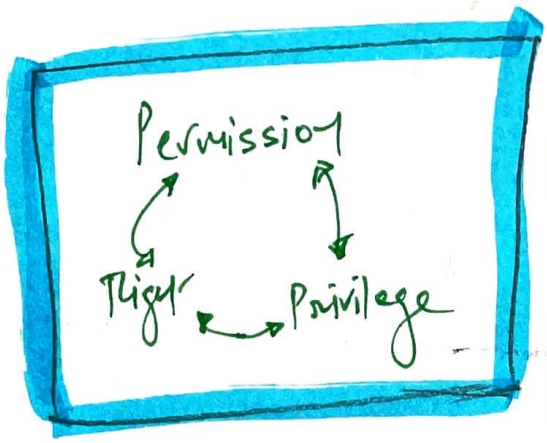
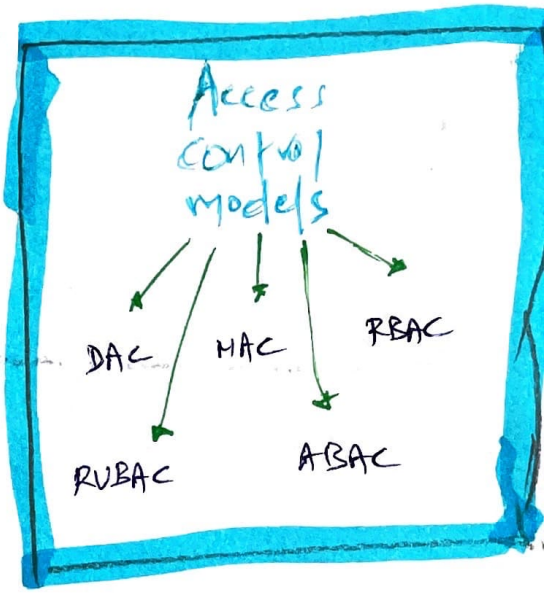
14. Controling & Monitoring Access





Access control Attacks

PERSPECTIVE

CoVe = Authorization methods + Access control Attacks

Understand Authorization Mechanisms

Implement Defense in Depth

Permission + Right = Privilege

↑ Grant access what can we do with object

↑ Ability to take action on the object

↑ Admin have few permission & right of pc data

* Authorization Mechanisms

Implicit Deny
- Firewall
- Everything deny by default until explicitly granted

Access control matrix
- object focused table that includes subjects, objects & assigned Privileges to subjects
- E.g ACL → Focused on objects

Constrained Interface
- Restricts what user can do or see based on privilege
- E.g Executives only see Reports in web UI

Capability Tables
- Subject focused
- Table has list of objects that subject can access.

Content-Dependent control
- Restricts access based on content within an object
- E.g Database view (selected columns)

Context-dependent control
- Requires specific activities before granting the access
- Restrict based on date & time

Need-to-know
- based on work task & job functions

P.P.O

Least Privilege

- Required privilege + Need to know

Separation of Duties and Responsibilities

- Split sensitive functions into two or more employees
- Prevent fraud

Need-to-know / Access granted to read time b/w 9 to 5

vs.

least privilege / Can read the time + change during PM hours.

ACLs / Access control matrix
↳ Focused on objects

Capability Tables
↳ focused on subjects

Dave may have clearance to access classified data but access is not granted until Dave's role ~~~~ verify requires a need to perform a job.

✱ Defense-in-depth concepts

Administrative controls + technical controls + physical controls

- Security policy + Awareness Training
- FW / IPS-IDS
- Perimeter security

✱ Access Control Models

Revise MAC notes/vedio OSN P633-635

DAC - Discretionary Access control

- Every object has owner / Data custodian
- owner has full control over object to grant or deny access to subjects

RBAC

- Permission based on role / job function / user groups

Attribute Based AC

- More granular/specific than RUBAC
- Use of rules with multiple attributes
- ABAC used by way software-defined networks

Rule Based A C (RUBAC)

- Apply global rules that apply to all subjects (FW)

MAC - Mandatory AC

- Use of labels that applies to objects & subjects
- Top secret user = Top secret document

✱ Access Control Models : Detailed concepts

Focused on USER IDENTITY

DAC Model = ACL = Object Focused

↳ Data custodian give permission to DAC

DAC ≠ Centrally managed system

because ACLs are easy to modify

↳ DAC is Flexible

To manage central Access control

↳ Non-discretionary AC

- RBAC
- RUBAC
- ABAC
- MAC

Non-DAC model does not focus on user identity. Instead, set of rules govern & manage the Access.

To prevent the Privilege creep — implement Least privilege

helps to implement

RBAC model

MAC model enforce Need-to-know principle using Compartmentization.

TBAC — Task Based AC — Control Access by assigning tasks, not user identity.

Attribute Based AC (ABAC) — Example — Allow Managers to use WAN from smartphones & Tablets

MAC Model = Lattice-Based Model

Users with sensitive label can access sensitive data

Uses implicit deny philosophy

Also allows label to identify more defined security domains

Adds level of compartmentization for objects / data

Compartmentization enforces Need-to-know principle

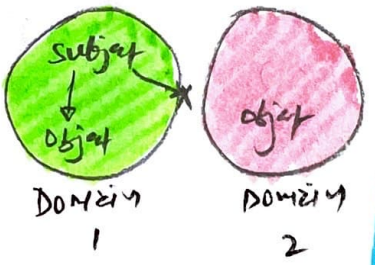
Classification within MAC Model uses three types of Environment :

Hierarchical

- Clearance in one level grant subject access to object in thy level + to all objects in lower level. But, it prohibits access to all objects in higher levels.

Compartmentalized

- Each compartment is isolated environment
- No relation b/w security domains.



Hybrid

- Subject must have clearance + need to know data within specific compartment to gain access to compartmentalized object.

MAC is different

Dave = secret clearance

g can only access files with secret clearance.

Not the ~~lower~~ higher classifications such as ~~sensitive, unclassified~~ top secret

But g can access lower - sensitive, unclassified.

NOTE - In MAC model, every subject & object has ~~one~~ one or more labels. Those labels are predefined, and system determines access based on assigned labels.

* ACCESS CONTROL ATTACKS

GOAL

Prevent unauthorised access to objects

Threat Modeling

- identify, understand & categorize potential threats.

Approaches

- Focus on Assets
- Focus on Attackers
- Focus on software

identify Attackers

Remember? S.T.R.I.D.E OSCP (31)

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- DOS
- Elevation of privilege

From the context of the Attack

- It's important to evaluate the value of Data
- find the Asset valuation

→ this helps to prepare scenario for Attack

Attacks detail - P.T.O end

DAC → identity-based AC

RBAC → Role or Group Membership

MAC → Labels to assign access

~~RUBAC~~
RUBAC → Rules within ACL

RBAC = Nondiscretionary model + use of hierarchy

Rainbow Attacks — Attackers already have password hashes

Resource based Access controls —
| match permission to resource such as storage
common for cloud-based App

storage X
User A - Read
User B - Read, write

CONFUSION MASTERS — VIDEO

Constrained Interface — Restrictions based on user privilege (Engaged on button) — Restrict what user can see or do. (limited menu options)

Access control model

RBAC

Least privilege — Provide user rights that requires to finish the job.

Access control concept

MAC

Need-to-know — Limits the access based on whether subject needs to know the information to accomplish assigned task regardless of their clearance

Access control concept

P.T.O

Seperation of Duties — Focusing on preventing fraud or mistakes by spliting task b/w multiple subjects

Video

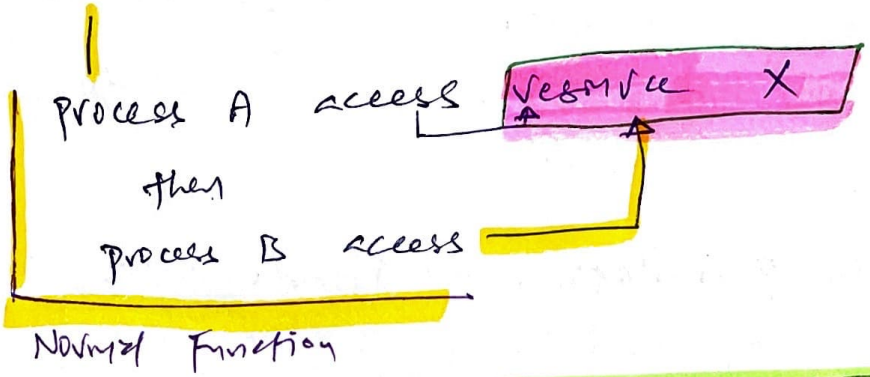
Constrained Interface — Don't see the clocks on wall

Least privilege (Action) — change time in day / business hours

Need to know (No action) — ~~change~~ Read time for only red clocks

Seperation of Duties — A moves minute hand } 6PM.
B moves small hand }

Race conditions – Two or more process need to access same resource in right order.



Split Knowledge

- Requires something you know
- E.g password is "SkyisBluefor46"

Person 1 → Skyis
person 2 → Blue
person 3 → for
person 4 → 46

- Split knowledge is logical

Dual Control

- Requires something you do
- E.g. President + secretary of defense + General turn their key to launch nuclear missile
- Dual control is physical

Split knowledge and Dual control similarity :-
Both holds two or more people responsible for one critical function.

Common Access Control Attacks

1. Access Aggregation Attack

collect non-sensitive information → to learn sensitive information

E.g → Reconnaissance Attack

Prevention → Least privilege, Need-to-know & Defense-in-depth

2. Password Attacks

P.T.O end

Hybrid Attack first use dictionary then it use Brute-force.

P.T.O

Dictionary Attack

- Use of predefined passwords from Database

Brute-Force Attacks

- Attempt to discover password using all possible combination of letters, numbers & symbols.

possible key values

Prevention → Use longer password with uppercase / lowercase / numbers & symbols

Birthday Attacks

- Focuses on finding collisions.
- This method doesn't need all possible hashes to see a match.

Prevention - Don't use MD5
Use SHA-3 with enough bits
SHA-3 with 512 bits.

All password cracking tool does is to find matching hash value of guess password. Hashing being a one way function, it's impossible then two hashing value but MD5 is not collision free. Remember that collision means it can match the hash.

Rainbow table

Why waste time guessing passwords & matching / calculating hash values when Rainbow table reduces this time by using large database of precomputed hashes.

Prevention → Use Salt to reduce rainbow attack

Random bits added to password before hashing it.

Password-based Key Derivation Function 2

Bcrypt & PBKDF2 are common algorithm to salt passwords

Further prevention → Add Pepper

- If attacker gets the database, they also gets salts for the password
- Pepper is large constant number stored elsewhere

3. Sniffer Attacks

- Snooping or Eavesdropping Attack

Prevention

- IDS
- Use one time passwords
- Protect w/ device with physical security
- Encrypt all sensitive Data

4. Spoofing Attacks

- phone spoofing.
- IP Spoofing
- Email spoofing

Prevention

- Don't click on suspicious email / link
- Don't open unexpected email attachment
- Be carefy from unknown senders

Phishing Attack

- Trick users to give up their sensitive information
- E.g Email with link

Drive-By Download

- Type of malware that installs itself without user's knowledge when user visits the website. it traces advantage of vulnerabilities in Browser / plugins.

5. Phishing

Spear

- Target to specif group of users, employees within a specific organization.

Whaling

- Targets senior / high-level executives (CFO), president of company

Vishing

- use of phone / VoIP
- commonly spoof caller ID to impersonate Bank / financial institutions.

6. Social Engineering Attacks

Shoulder surfing

7. Smart-card Attacks

Side channel Attack

- Passive Attack where Attacker learn valuable info. contained within card such as Encryption key.