DAC: acces control pe bază identității celui care cere accesul.
↗ bazat pe reguli de acces explicite.
→ ignoră distincția dintre sub ↗ obiect.
- vulnerabilă cal troian.

MAC • Acces control bazat pe reguli dictate de o autoritate centrală -
- Nu există ownership în MAC
- se face distincție S/O
- Bell-LaPadula, Biba, Bidul Chinezesc.

Modele latticeale:
- entitățile sunt grupate în clase de securitate.
- Obiectele = containere de informație → fișiere, etc.
→ Controlul accesului = se asignează obiectelor o clasă de sec

Model Latticeal: Clasă de securitate, relație binară (permisiune acces)
⊕ operator
A → B = inf poate curge de la A la B
A ⊕ B = inf din cele 2 clase se combină, rez. = apartine claselor A⊕B
Axiomele Denning: 1) Mț claselor de securitate e finită
2) rel de ordine parțială = rel de transf al informației - (Refl, simv, tranzitivă)
3) Mț claselor de sec SC are un cel mai mic elem (clasa inf publice).
4) Când se combină 2 clase de sec, rezultatul e cea mai mică clasă de sec →.
Orice model ce satisface cele 4 cond e o latice.

! Clasa A domină clasa B dacă inf poate curge de la B la A

MODELUL ASIGURĂ DOAR CONFIDENȚIALITATE -
- entități = plasate pe niv de securitate.
- Niv subiecților = gradul de încredere pe care-l acord subiectului de a nu divulga inf
Niv obiectelor = gradul de confidențialitate al inf din obiectul resp

1) MAC Politici ~~de~~ confidențialitate ~~bazate pe Modelul~~ Mandatore -
• Scopul = controlul curgerii de inf
- prevenirea scurgerilor de inf către subiecți neautorizați
Bell LaPadula: îmbogățire DAC cu MAC - pt a impune politicile de curgere a inf.
1) Matrice de control a accesului
2) Operațiile să fie autorizate de politicile de acces mandatorii MAC.