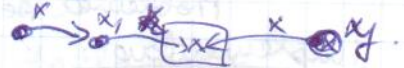


DAC : acces control pe baza identității celui care cere accesul.  
A fost pe reguli de acces explicit.

→ ignoro distinctly a diuturne rule of object

- vulnerable cal troian.



**MAC** • Acces control bazat pe reguli dictate de o autoritate centrală -

- Nu există ownership în MAC

- se face distincție  $S_n$ /Obiect

- Bell-La Padula, Biba, Bidul Chinoyeso

## Modelle laticeale

- entitățile sunt grupate în clase de securitate.

- Objet de la = contenu de l'information  $\rightarrow$  figure, etc.

→ Controlul accesului = se atribuie obiectelor o clasă de sec.

Model Latticeal : Clasa de securitate, relatie binară (permisiune acces)  
• operator

$$A \rightarrow B = \inf_{\text{route}} \text{charge de la } A \text{ la } B$$

$A \oplus B$  = inf. din cele 2 clase se construiește, rez. = cuprindere celorlalte  $A \oplus B$

Axiomele Denning: 1) Mt. closelor de securitate e fructos

3) rel de ordine parțială = rel de tranșal  
informației - (Reflexiv, sim, tranșitiv).

3) Mt cloşelor de sec SC all un al mai mic  
eleu (closo inf publice).

4) Când se combină 2 clase de sec, rezultatul e cel mai mică clasă de sec  $\rightarrow$ .

Price model ce notifice cele 4 cond e o lastica.

Closa A domină closa B dacă inf poate curge de la B la A

## MODELUL ASIGURĂ DOAR CONFIDENTIALITATE.

- eufra = plouate pe nivel de secunitate.

- Niv subiectiv = gradul de încredere pe care-l acord sub-  
iectul de a nu divulga inf.

Niv obiectelor = gradul de confident al inf din obiectul resp

1) MAC Politici depline Confidentialitate ~~protejeaza~~ ~~Mandator~~ Mandatore -

- Scopul = controlul cergerii de inf

- prevenirea scurgerilor de inf. către org. neautorizate

Bell La Padula : Embargo/22 DAC cu MAC - pt a apoi politice  
de curge a inf.

4) Matrice de control a adesei lui

2) Operatiunile sã sã fie autorizate de politicile de acces mandator  
MAC.