

## Modelul zidului chinezesc folosit în competențe diverse

- Scop: evitarea conflictelor de interese.

exemplu: o firmă oferă consultanță la 2 firme aflate în competiție.

- Companiile sunt grupate în clase de interese.

- Sub. au acces la inf cu anumite restricții: dacă un sub. are acces la inf din clasă  $C_1$ , atunci trebuie să i se dea acces la altă dată dacă e în conflict de interese cu  $C_2$  în care e compania concurentă → se creează un "zid" chinezesc în jurul obiectului - pentru că nu mi poți vedea mai departe.

• Dacă e un obiect din mulțimea  $D$  aflată în clasă de conflict de interese  $C_1$  e adev. se creează un zid în jurul lui  $D$  și nici o informație din  $C_1$  nu poate fi aleasă de acel obiect.

Simple Security Rule

• Subiectul  $S$  poate avea acces de read la un obiect  $O$ , doar dacă obiectul  $O$ :  
- e în aceeași mulțime cu cea a companiei ce deține obiectele deja accesate de  $S$ ; care e în interiorul zidului.  
- sau aparține unei alte clase de conflict de interese.

• Proprietatea (\*) - un subiect  $S$  poate scrie într-un obiect  $O$ , doar dacă:  
1)  $S$  poate citi  $O$  prin regula S. Securitate  
2) Nici un obiect care este într-o mulțime de interes a unei companii diferite nu poate fi citit -  
(un subiect poate scrie inf în  $O$  dacă poate citi inf din  $O$ , dar nici un alt subiect nu poate citi din  $O$  în care se scrie).

Visto → MIC = mandatory integrity control -

- 6 niv de securitate -

- la login, Visto atribuie SID la tokenul de acces al utilizatorului

- niv de integritate al obiectelor → fișierelor, proceselor, → SACL (system ACL - stocate).

MAC → oferă protecție împotriva piergerii indirecte de informații,  
→ e vulnerabil la canale acoperite -

curs 4 RBAC = role based acc. control

Drepturile de acces sunt grupate pe roluri - (o funcționalitate)

• fiecare rol are anumite drepturi/permisiuni -

• mecanism folosit de administratorii de sisteme pt a specifica privilegii cerute de diverse funcții într-o firmă.

- Basic

- ierarhic

- Restrictiv

- Constitutiv

• Un user care se mută pe alt rol este pur și simplu asignat rolului nou și i se șterge rolul vechi