## 4. MODELE DE SECURITATE

Dupa implementarea securitatii la nivelul componentelor fizice, administratorul trebuie sa se asigure ca resursele retelei sunt protejate impotriva accesului neautorizat si a distrugerilor accidentale sau intentionate. Atribuirea permisiunilor si drepturilor de folosire a resurselor retelei reprezinta factorul principal care face ca o retea sa devina un puternic instrument de afaceri.

Pentru protejarea datelor si a resurselor hardware s-au dezvoltat doua modele de securitate :

- Partajari protejate prin parola
- Permisiuni de acces

Aceste modele se mai numesc si *securitate la nivel de partajare* (share-level), respectiv *securitate la nivel de utilizator* (user- level).

Unele companii utilizeaza ambele metode de securitate.

### Partajari protejate prin parola

Partajarile protejate prin parola se axeaza pe resursele partajate. Un utilizator trebuie sa introduca o parola pentru a avea acces la o anumita resursa. Implementarea partajarii protejate prin parola presupune atribuirea unei parole pentru fiecare resursa partajata. In multe sisteme, resursele pot fi partajate folosind diferite tipuri de permisiuni.

De exemplu in Windows 95 (Fig. 1) directoarele pot fi partajate **Read Only** (protejate la scriere), **Full** (complet la dispozitia utilizatorului pt. : vizualizari, scrieri, modificari, stergeri) sau **Depends of Password** (in functie de parola).

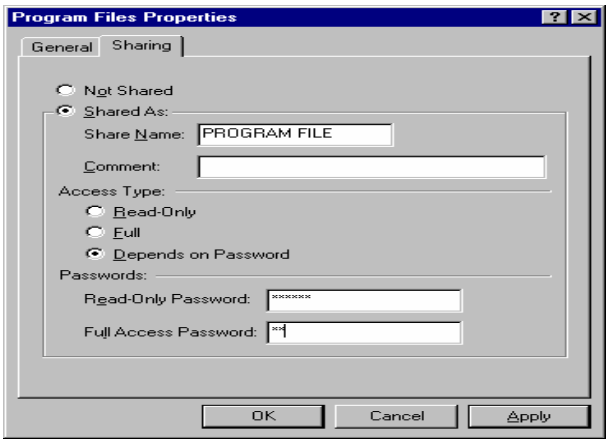


***Fig. 1 Partajarea protejata prin parola a directorului Program File***

Sistemul de partajare protejata prin parola reprezinta o metoda simpla de a asigura securitatea retelei, permitând accesul la o anumita resursa pentru orice utilizator care stie parola.

### Permisiuni de acces

Acest model de securitate presupune atribuirea anumitor drepturi la nivel de utilizator. Atunci când deschide o sesiune de lucru in retea, utilizatorul scrie o parola (Fig. 2). Serverul valideaza combinatia *nume utilizator – parola* si o foloseste pentru a acorda sau a interzice accesul la resursele partajate, verificând baza de date cu permisiunile de acces ale utilizatorilor.

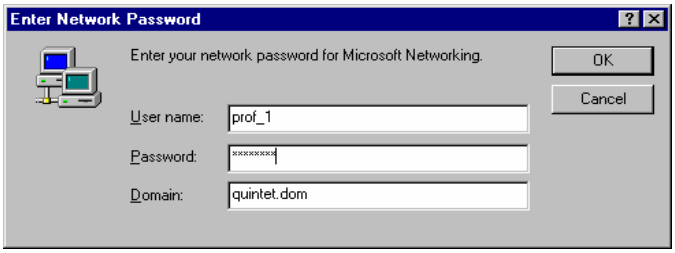


***Fig. 2 Verificarea parolei de acces in retea***

## Protejarea resurselor

Dupa ce un utilizator a fost autentificat si i s-a permis accesul in retea, conform reprezentarii din fig. 2, sistemul de securitate ii ofera acces la resursele respective.

De retinut : *utilizatorii au parole,* iar *resursele au permisiuni.*

Fiecare resursa este protejata printr-un “gard” de protectie. Acest gard are mai multe porti prin care un utilizator poate patrunde. Anumite porti acorda utilizatorilor privilegii deosebite fata de resursa respectiva. Administratorul hotaraste care utilizatori pot trece si prin care porti. Una dintre porti ofera utilizatorului acces complet la resursa. Alta poarta acorda doar dreptul de citire a informatiilor. Fiecare resursa partajata (sau fisier) este pastrata impreuna cu o lista de utilizatori sau grupuri si permisiunile asociate acestora.