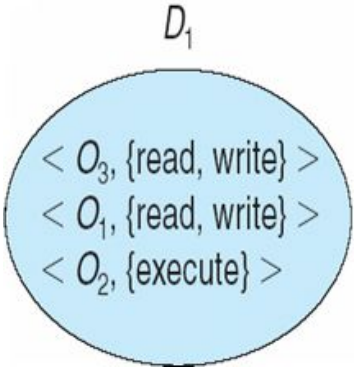
Ochrona

Mechanizmy ochrony umożliwiają dostęp kontrolowany przez ograniczanie rodzajów dostępu do plików udzielanych użytkownikom. Poza nadzorowaniem plików ochrona ma również zapewnić, że z segmentów pamięci, procesora i innych zasobów będą mogły korzystać tylko te procesy, które otrzymały odpowiednie pełnomocnictwa od systemu operacyjnego.
Ochrona (*protection*) jest realizowana za pomocą mechanizmu, który nadzoruje dostęp programów, procesów lub użytkowników do zasobów zdefiniowanych w systemie komputerowym. Mechanizm ten powinien umożliwiać określanie zasad nadzoru, jak również pozwalać na ich egzekwowanie.

System operacyjny składa się ze zbioru obiektów sprzętowych lub programowych.
Każdy obiekt ma unikatową nazwę i jest osiągalny za pomocą dobrze zdefiniowanych operacji.
Problem ochrony: zapewnić, że dostęp do każdego obiektu odbywa się w sposób właściwy i mają go tylko procesy do tego upoważnione.

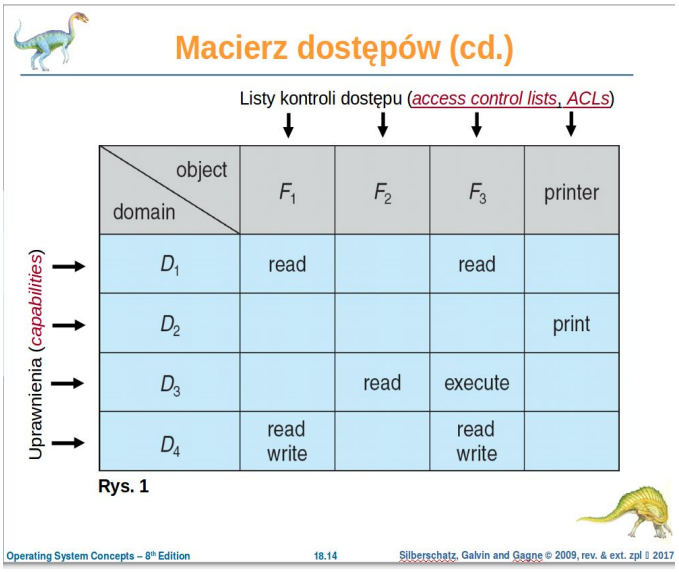
Naczelna zasada: minimalizacja przywilejów (*principle of least privilege*)
Programy, użytkownicy i systemy powinny mieć tylko tyle przywilejów, ile trzeba do wykonania ich zadań.



Prawo dostępu(*access right*) = <nazwa-obiektu, zbiór praw>, gdzie zbiór praw jest podzbiorem operacji dozwolonych na obiekcie.

Domena (*domain*) = zbiór praw dostępu

System ochrony można postrzegać jako macierz dostępów (*access matrix*).



Ochrona dynamiczna umożliwia:

- operacje dodawania i usuwania praw dostępu
- właściciel Oi
- kopiowanie operacji z Oi do Oj
- kontrolowanie: Di może modyfikować prawa dostępu Dj
- przekazanie: przełączenie z domeny Di do domeny Dj .

Mechanizm zamka-klucza (*lock-key scheme*) jest formą pośrednią między listami dostępów a listami uprawnień. Obiekt ma unikatowy wykaz wzorców binarnych (zamków). Domena ma analogiczny wykaz wzorców (kluczy). Proces w domenie

ma dostęp do obiektu tylko wtedy, kiedy domena ma klucz pasujący do jednego z zamków obiektu.

Prawa:

- Prawo kopiowania (copy) - Umożliwia kopiowanie prawa dostępu z jednej domeny do drugiej, tylko w kolumnie, w której je zdefiniowano (dot. danego obiektu)
- Prawo właściciel (owner) Jeśli element dostęp(i, j) zawiera to prawo, wówczas proces działający w domenie Di może dodawać lub usuwać dowolne prawa do elementów w kolumnie j.
- Prawo kontroler? (control) Di - pozwala usuwać dowolne prawa domenie Di

Kontrola dostępu podług roli (*role-based access control*)

- Przywilej oznacza prawo wykonania wywołania systemowego
- Może być przypisany procesowi
- Przyznawanie dostępu do przywilejów odbywa się według ról przypisanych użytkownikom

Systemy uprawnień

- Hydra
    - Ustalony zbiór praw dostępu znanych przez system i przez system interpretowanych.
    - Interpretacja praw zdefiniowanych przez użytkownika zależy wyłącznie od programu użytkowego; system dostarcza ochrony dostępu do tych praw.
- System Cambridge CAP
    - Uprawnienia zadane – umożliwiają typowe operacje „czytaj”, „pisz” i „wykonaj” dotyczące segmentów pamięci obiektu.
    - Uprawnienia programowe – ich interpretacja jest pozostawiona podsystemowi za pośrednictwem jego chronionych procedur.