

# Ochrona zasobów

1. Cele ochrony
  - ☞ mechanizm ochrony
  - ☞ polityka ochrony
2. Domeny ochrony
3. Macierz dostępów
4. Implementacja macierzy dostępów

## Cele ochrony

- ☼ zapobieganie (złośliwym lub przypadkowym) naruszeniom ograniczeń dostępu
- ☼ wymuszenie przestrzegania polityki ochrony przez procesy
- ☼ wczesne wykrycie błędów w dostępie do zasobów

## Polityka i mechanizm ochrony

- ☼ Polityka ochrony jest zbiorem reguł dostępu do zasobów.
- ☼ Mechanizm ochrony jest zbiorem dostępnych środków do wymuszania polityki ochrony

## Polityka ochrony

- ☼ Polityka może wynikać z:
  - projektu systemu (ustalona jest na etapie projektowania systemu),
  - wytycznych kierownictwa (ustalana jest na etapie instalacji lub eksploatacji systemu),
  - decyzji indywidualnych użytkowników (podjętych w trakcie eksploatacji systemu).

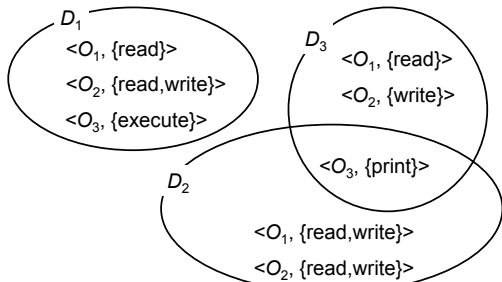
## Mechanizm ochrony

- ☼ Mechanizm ochrony powinien być na tyle uniwersalny, żeby dało się go dostosować do zmian w polityce ochrony.
- ☼ W skrajnym przypadku każda zmiany polityki mogłaby wymagać zmiany mechanizmu.

## Podstawowe pojęcia modelu systemu ochrony

- ☼ Proces — jednostka aktywna, ubiegająca się o dostęp do zasobu w celu wykonania operacji
- ☼ Obiekt — jednostka zasobu dostępna poprzez ściśle zdefiniowany zbiór operacji
- ☼ Prawo dostępu — możliwość wykonania określonej operacji na obiekcie
- ☼ Domena ochrony — zbiór obiektów wraz ze zbiorem praw dostępu (zbiorem operacji, które można na tych obiektach wykonać, dla których jest prawo wykonania)

## Przykład domen ochrony



## Związek pomiędzy procesem a domeną

- ☼ Proces może działać w domenie, co oznacza, że ma dostęp do obiektów objętych tą domeną w zakresie określonym przez prawa dostępu, zdefiniowane dla każdego obiektu w tej domenie.
- ☼ Związek procesu z domeną może być
  - statyczny — związek pomiędzy procesem i domeną ustalany jest raz na cały czas działania procesu i nie ulega zmianie
  - dynamiczny — proces może się przełączać z jednej domeny do drugiej

## Zasada wiedzy koniecznej

- ☼ Proces powinien mieć dostęp w określonym zakresie tylko do tych zasobów, których potrzebuje do zakończenia zadania.
- ☼ Ograniczenie dostępności zasobów zgodnie z zasadą wiedzy koniecznej umożliwia zmniejszenie negatywnych skutków działania procesów błędnych.

## Przestrzeganie zasady wiedzy koniecznej

- ☼ W przypadku statycznego związku proces-domena przestrzeganie uwarunkowane jest możliwością zmiany zawartości domeny.
- ☼ Dynamiczny związek proces-domena umożliwia przełączanie procesu pomiędzy domenami, dzięki czemu zamiast zmiany zawartości domeny, można utworzyć nową domenę i się do niej przełączyć.

## Macierz dostępów

Obiekt Domena	F <sub>1</sub>	F <sub>2</sub>	F <sub>3</sub>	F <sub>4</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>
D <sub>1</sub>	read				print		
D <sub>2</sub>		read write	exec				
D <sub>3</sub>		read					
D <sub>4</sub>	read write						

## Prawo przełączania domen

Obiekt Domena	F <sub>1</sub>	F <sub>2</sub>	F <sub>3</sub>	D <sub>1</sub>	D <sub>2</sub>	D <sub>3</sub>	D <sub>4</sub>
D <sub>1</sub>	read				switch		
D <sub>2</sub>		read write	exec			switch	
D <sub>3</sub>		read					
D <sub>4</sub>	read write						

## Kontrola zmian zawartości macierzy dostępów (1)

- ☼ prawo kopiowania — pozwala kopiować prawa dostępu w ramach kolumny macierzy, może mieć formę:
  - przekazywania
  - kopiowania (właściwego)
  - ograniczonego kopiowania — kopiowanie prawa bez prawa dalszego kopiowania

## Kontrola zmian zawartości macierzy dostępów (2)

- ☼ prawo właściciela — pozwala na dodawanie i usuwanie praw
- ☼ prawo kontroli — stosowane w odniesieniu do domeny, pozwala procesowi działającemu w określonej domenie na modyfikację domeny, dla której jest ustawione prawo kontroli

## Problem zamknięcia

- ☼ Problem zamknięcia polega na zagwarantowaniu, że żadna informacja przechowywana w obiekcie nie wydostanie się na zewnątrz jego środowiska wykonania.
- ☼ Prawa kopiowania i właściciela umożliwiają ograniczenie rozchodzenia się praw dostępu, ale nie gwarantują zabezpieczenia przed rozchodzeniem się informacji (jej ujawnianiem).

## Implementacja macierzy dostępu (1)

- ☼ tablica globalna — tablica trójek postaci  $\langle D_i, O_j, R_k \rangle$
- ☼ wykazy dostępu do obiektów — z obiektem wiąże się odpowiednie kolumny macierzy dostępów, określające prawa do obiektu w poszczególnych domenach

## Implementacja macierzy dostępu (2)

- ☼ wykazy uprawnień do domen — z domeną wiąże się wykaz obiektów wraz z dostępnymi operacjami na tych obiektach
- ☼ mechanizm zamka-klucza — związanie odpowiednich wzorców binarnych zwanych zamkami z obiektami i wzorców zwanych kluczami z domenami