Systemy Operacyjne

Ochrona i Bezpieczeństwo

Woźniak Andrzej

Ochrona i jej cele

Ochrona to mechanizmy kontrolowania dostępu do zasobów.

Celem ochrony jest poufność danych.

Metodą uzyskania ochrony jest niezawodność systemu.

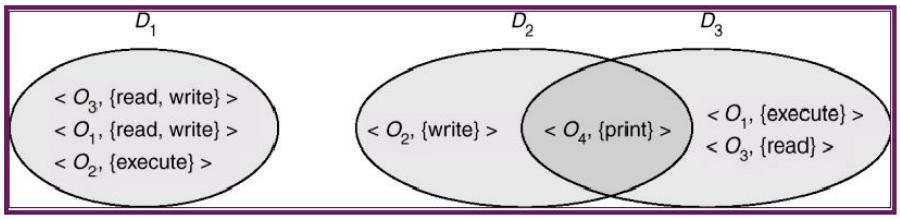
Domeny ochrony

Zasada wiedzy koniecznej - proces w każdej chwili powinien mieć uprawnienia tylko do tych zasobów, których potrzebuje do wykonania zadania.

Domena ochrony - Zbiór obiektów i operacji na tych obiektach dostępnych dla procesu

Prawo dostępu - możliwość wykonania operacji na obiekcie.

System z trzema domenami



Przełączanie domen

- Bit setuid (UNIX)
- specjalny katalog
- proces-demon

Macierz dostępów

object / domain	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	

Macierz dostępów - domeny jako obiekty

object / domain	F_1	F_2	F_3	laser printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch
D_3		read	execute					
D_4	read write		read write		switch			

Macierz dostępów - kopiowanie

object / domain	F_1	F_2	F_3
D_1	execute		write*
D_2	execute	read*	execute
D_3	execute		

(a)

object / domain	F_1	F_2	F_3
D_1	execute		write*
D_2	execute	read*	execute
D_3	execute	read	

(b)

Macierz dostępów - właściciel

object / domain	F_1	F_2	F_3
D_1	owner execute		write
D_2		read* owner	read* owner write*
D_3	execute		

(a)

object / domain	F_1	F_2	F_3
D_1	owner execute		
D_2		owner read* write*	read* owner write*
D_3		write	write

(b)

Macierz dostępów - kontrola

object / domain	F_1	F_2	F_3	laser printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch control
D_3		read	execute					
D_4	write		write		switch			

Implementacje macierzy dostępów

- Tablica globalna - uporządkowany zbiór trójek <domena, obiekt, zbiór praw>
- Lista dostępów do obiektów - dla każdego obiektu osobna tablica <domena, zbiór- praw>
- Lista uprawnień domen - dla każdej domeny osobna tablica <obiekt, zbiór- praw>
- Mechanizm zamka-klucza - wzory binarne dla obiektu i domeny,

Cofanie uprawnień - problemy

- Natychmiast czy z opóźnieniem?
- Wybiórczo czy ogólnie?
- Częściowo czy całkowicie?
- Czasowo czy na stałe?

Schematy cofania uprawnień

- Wtórne pozyskiwanie
- Wskaźniki zwrotne
- Adresowanie pośrednie
- Klucze

Bezpieczeństwo

Ochrona rozumiana w szerszym zakresie. Oprócz środków na poziomie systemów informatycznych obejmuje środki z zakresu zarządzania:

- strefy bezpieczeństwa,
- fizyczny dostęp do urządzeń i pomieszczeń,
- procedury postępowania

Złośliwe naruszenia bezpieczeństwa

- Kradzież danych
- zmiana danych bez upoważnienia
- niszczenie danych
- blokowanie usług

Poziomy środków bezpieczeństwa

- Fizyczny
- Ludzki
- Sieciowy
- Systemu operacyjnego

Uwierzytelnianie

- certyfikat i PIN
- nazwa i hasło
- biometryczne

Mechanizmy utrudniające złamanie hasła

- określanie minimalnej długości hasła,
- wymuszanie okresowej zmiany haseł,
- pamiętanie n haseł użytkownika,
- blokowanie konta po k błędnych próbach
- wymuszanie stosowania znaków specjalnych,
- uniemożliwianie stosowania trywialnych haseł
- wygasanie kont

Zagrożenie programowe

- Konie trojańskie
- Boczne wejścia
- Przepełnienie bufora i stosu
- Robaki
- Wirusy
- spyware

Zabezpieczenia

- Analiza systemu pod kątem luk
- Zapory ogniowe
- dziennik kontroli
- wykrywanie włamań
- kryptografia