Kontrola dostępu

Materiały pomocnicze do wykładu

Bezpieczeństwo systemów informatycznych

Kontrola dostępu

Macierz dostępu (model *Bell-La Padula*)

Obiekty

Podmioty	Plik 1	Plik 2	. . .
Użytkownik 1	Czytanie	Czytanie	
Aplikacja A		Czytanie Pisanie	
Użytkownik 2			

Listy kontroli dostępu (*access control lists*)

ACL dla *Pliku 1*
Użytkownik 1 (Czytanie)

ACL dla *Pliku 2*
Użytkownik 1 (Czytanie)
Aplikacja A (Czytanie, Pisanie)

Listy możliwości (*capability lists*)

Lista możliwości dla *Użytkownika 1*
Plik 1 (Czytanie)
Plik 2 (Czytanie)

Lista możliwości dla *Aplikacji A*
Plik 2 (Czytanie, Pisanie)

Etykiety poziomów zaufania (*sensitivity labels*)

Poziom ochrony określony jest przez parę (C, G):

C – zbiór poziomów zaufania,

G – podzbiór zbioru kategorii informacji.

Dla poziomów ochrony **X** i **Y**

$X=(C_X, G_X)$, $Y=(C_Y, G_Y)$, $Y \geq X \Leftrightarrow C_Y \geq C_X \wedge G_Y \supseteq G_X$

Przykładowo:

Etykieta = < poziom zaufania, kategoria informacji>

Poziomy zaufania = {ściśle tajne, tajne, poufne, jawne}

lub { dla zarządu, do użytku wewn., ogólnie dostępne }

Kategorie reprezentują typy danych np.:

{wypłata, podwyżki, dane osobowe}

Etykiety poziomów zaufania - procedura

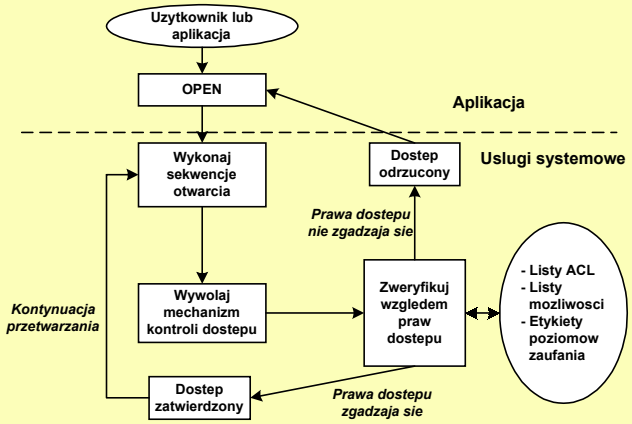
1. Każdemu użytkownikowi przypisany jest maksymalny poziom ochrony MPO.
2. Użytkownik nie może czytać danych z obiektu, gdy POO ≥ MPO, gdzie POO jest poziomem ochrony obiektu (tzw. *prosta zasada bezpieczeństwa*).
3. Użytkownik o bieżącym (roboczym) poziomie ochrony L_n może zapisywać dane tylko do tych obiektów, dla których poziom ochrony MPO ≥ POO ≥ L_n.
4. Użytkownik o bieżącym poziomie ochrony L_n może czytać dane tylko z tych obiektów, dla których L_n ≥ POO.
5. Poziomy ochrony obiektów nie mogą być zmieniane przez użytkowników – są nadawane np. przez administratora.
6. Obiekty nie posiadające nadanego poziomu ochrony – nie są dostępne.

Inne modele kontroli dostępu

- model Wooda,
- model Sea View,
- model Grahama-Denninga,
- model Harrisona-Ruzzo-Ullmana (HRU),
- model *take-grant*.

  - Dostęp uznaniowy DAC (*Discretionary Access Control*)
  - Dostęp narzucony MAC (*Mandatory Access Control*)

Funkcjonowanie mechanizmu kontroli dostępu



Ukryte kanały

Kanałem ukrytym (*covert channel*) nazywamy kanał wymiany informacji wykorzystany do nielegalnego przesłania informacji z ominięciem istniejących mechanizmów kontroli.

Poufnej informacji może dostarczyć np. nazwa pliku. W tym przypadku kanał został wykorzystany nielegalnie, gdyż został zaprojektowany do innych celów. Kanały ukryte są trudne do wykrycia i czasami trudne do usunięcia.

- Kanały pamięciowe
- Kanały czasowe

Kanały ukryte

Warunki powstawania kanałów ukrytych:

- Podczas projektowania lub implementacji sieci nie zwrócono uwagi na możliwość nadużywania kanału jawnego.
- Nieprawidłowo zaimplementowano mechanizmy kontroli dostępu lub działają one niewłaściwie.
- Istnieją zasoby współdzielone pomiędzy użytkownikami.