

Modele bezpieczeństwa

Kontrola dostępu – ogólne modele

- DAC (ang. Discretionary Access Control) – uznaniowa kontrola dostępu:
 - Kontrole są uznaniowe w tym sensie, że podmiot z określonym zezwoleniem na dostęp lub jest w stanie przekazać to zezwolenie (być może pośrednio) dowolnemu innemu podmiotowi (chyba że jest to ograniczone obowiązkową kontrolą dostępu)
- MAC (ang. Mandatory Access Control) – obowiązkowa kontrola dostępu:
 - odnosi się do typu kontroli dostępu, dzięki której system operacyjny ogranicza zdolność podmiotu lub inicjatora do uzyskania dostępu lub ogólnie do wykonania pewnego rodzaju operacji na obiekcie lub celu

Implementacja DAC

- DAC, posiada 2 implementacje:
 - Z właścicielem (ang. with owner) – kontekst bezpieczeństwa narzuca właściciel obiektu, w systemie istnieje znacznik własności
 - Ze zdolnościami (ang. with capability) – kontekst bezpieczeństwa narzucany jest przez zdolności narzucane w ramach modelu bezpieczeństwa

Implementacja MAC

- MAC ma wiele implementacji, stąd trudno wyróżnić wiodące
- Większość z nich odnosi się do Common Criteria (dalej)
- Większość pierwotnych implementacji, odnosi się do pojęć pierścieni bezpieczeństwa i poziomów bezpieczeństwa
- Siłę implementacji MAC, ocenia się z użyciem poziomów EAL (ang. Evaluation Assurance Level 1-7 z Common Criteria)

Model Bell-La Padula

- Koncentracja na zapewnieniu by podmioty o różnych zezwoleniach (ściśle tajne, tajne, poufne...), są prawidłowo uwierzytelnione i posiadają niezbędne poświadczenie bezpieczeństwa
- Zasady modelu:
 - Prosta reguła bezpieczeństwa (reguła „bez odczytu”) - podmiot na danym poziomie nie może odczytać danych na wyższym poziomie bezpieczeństwa
 - Słaba reguła gwiazdy (reguła braku zapisu) – podmiot na danym poziomie bezpieczeństwa, nie może zapisać danych na niższym poziomie bezpieczeństwa
 - Mocna reguła gwiazdy (operacje na danym poziomie) – podmiot z możliwością zapisu i odczytu, może wykonywać te operacje wyłącznie na danym poziomie. Nic powyżej i poniżej
 - Zasada spokoju (ang. tranquility) – podmiot i obiekt nie może po utworzeniu zmienić poziomu bezpieczeństwa po utworzeniu
- MAC jest oparty na tym modelu

Model maszyny stanów

- Stan maszyny w celu weryfikacji bezpieczeństwa systemu
- Stany odzwierciedlają wszystkie możliwe (i dopuszczalne) instancje obiektów i podmiotów uzyskujących dostęp do tych obiektów
- Implementacja:
 - Należy identyfikować i określić gdzie (i jakie kombinacje), odzwierciedlają stany
 - Należy zdefiniować pożądane stany zmiennych
 - Należy określić przejścia (tranzycje) pomiędzy stanami
 - Funkcje przejść należy zdefiniować i przetestować w celu upewnienia się co do poprawności modelu
 - Należy wymuszać niepożądane warunki tranzycji w celu wykluczenia nieprawidłowych przejść

Poziomy EAL

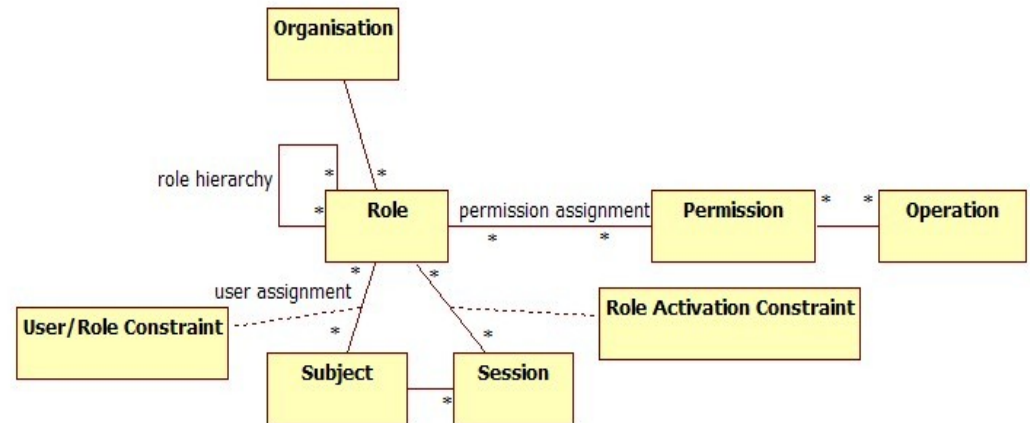
- Poziomy EAL oznaczają stopień weryfikacji właściwości związanych z bezpieczeństwem rozwiązania. Nie mają nic wspólnego z celem bezpieczeństwa (ang. Security Target)
 - EAL1 – rozwiązanie funkcjonalnie przetestowane
 - EAL2 – rozwiązanie strukturalnie przetestowane
 - EAL3 – rozwiązanie metodycznie przetestowane i sprawdzone
 - EAL4 – rozwiązanie metodycznie tworzone przetestowane i przeglądane (tu występuje szereg systemów z rozszerzeniem „trusted”)
 - EAL5 – pół-formalnie projektowane i testowane
 - EAL6 – pół-formalnie zweryfikowany projekt, testowanie metodyczne (np.. Green Hills INTEGRITY-178B RTOS)
 - EAL7 – formalnie zweryfikowane i przetestowane
- Formalna weryfikacja poziomów EAL jest kosztowna i zabiera wiele czasu (EAL4 ~od 10 do 25 msc. i od 150 do 350 tys. \$)

Model kratowy

- Krata (ang. lattice) to concept matematyczny bazujący na koncepcji grupy
- Krata zawiera:
 - Zestaw elementów
 - Częściową relację uporządkowania – dowolne dwa elementy muszą mieć unikalne najmniejsze górne i największe dolne ograniczenie
 - Model kratowy łączy wielopoziomowe i wielostronne zabezpieczenia
 - Elementy kraty to etykiety bezpieczeństwa które składają się z poziomu bezpieczeństwa i zestawu kategorii bezpieczeństwa

RBAC

- RBAC (ang. Role-based access control) – model bezpieczeństwa oparty na rolach
- W modelu wydzielono:
 - Prawa rodzajowe (ang. permissions) – podstawowe prawa do obiektów (read, write, execute, print, transfer permission ...)
 - Role – gromadzą wydzielone prawa rodzajowe przydzielone do obiektów (np. podsystemów lub programów) w grupy umożliwiające wykonanie zadań
 - Podmiot (ang. subject) – najprościej.. konto użytkownika
 - Sesja – mapowanie podmiotu, roli i/lub praw rodzajowych



Modyfikacje RBAC

- CBAC – model RBAC rozszerzony o kontekst (np. źródła wykonanego połączenia – system)
- ERBAC – model RBAC z dodanymi prawami do encji
- ABAC – model RBAC bazujący na atrybutach

ACL

- ACL (ang. Access Control Lists) – kontrola dostępu bazująca na listach
- Obiekt z kontrolą dostępu, posiada listę podmiotów oraz praw rodzajowych przydzielonych temu podmiotowi
- To obiekt przenosi zestaw atrybutów bezpieczeństwa a nie konto czy rola
- ACL jest najczęściej stosowanym modelem bezpieczeństwa w systemach głównego nurtu (GNU/Linux, Windows, *BSD...)