STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Marcin GORAWSKI, Jacek FRĄCZEK
Politechnika Śląska, Instytut Informatyki

KONTROLA DOSTĘPU DO INFORMACJI W HURTOWNIACH DANYCH

Streszczenie. Praca opisuje charakterystyczne dla hurtowni danych modele kontroli dostępu do informacji oraz mechanizmy ich implementacji. Analizowane są zabezpieczenia dostępu do bazy hurtowni danych typu ROLAP i do jej poszczególnych obiektów, ze szczególnym uwzględnieniem dostępu do danych na poziomie wierszy.

Słowa kluczowe: hurtownie danych, kontrola dostępu, model bezpieczeństwa.

THE CONTROL OF ACCESS TO INFORMATION IN DATA WAREHOUSES

Summary. The research describes the access control models typical for data warehouses and mechanisms of their implementation. The means of access authorization to objects' data in ROLAP data warehouses are analyzed with particular regard to row level access.

Keywords: data warehouse, access control, security model.

1. Wstęp

Hurtownia danych jest centralnym źródłem informacji o całym przedsiębiorstwie [2,3]. Z danych umieszczonych w hurtowni korzystają najczęściej sami pracownicy danej firmy, ale w wielu przypadkach sposób działania przedsiębiorstwa (czy nawet sama działalność marketingowa) wymaga udostępnienia części danych podmiotom trzecim (dostawcom, odbiorcom, klientom indywidualnym), a nawet anonimowym użytkownikom Internetu. W rezultacie jeden z najważniejszych systemów przedsiębiorstwa zostaje udostępniony społeczności użytkowników, której interakcja z systemem powinna mieć ściśle określony

charakter, zapewniający zabezpieczenie danych przedsiębiorstwa przed ujawnieniem. Zabezpieczenie systemu bazodanowego można rozpatrywać na wielu płaszczyznach [1,2,4,5]: zapewnienia poufności informacji [10,11,13], jej integralności [6] i dostępności [17,18]. Niniejsza praca koncentruje się na pierwszym z tych zagadnień, ze szczególnym uwzględnieniem kontroli dostępu użytkowników końcowych do wierszy danych przechowywanych w hurtowniach wykorzystujących relacyjną bazę danych (hurtownia danych typu ROLAP, ang. *Relational Online Analytical Processing*).

Problem autoryzacji dostępu do danych w hurtowni jest zagadnieniem złożonym [8]. Wymagania nakładane na projektowany system zabezpieczeń charakteryzują się wysoką specyfiką, silnie uzależnioną od stosowanych procedur i sposobu działania danego przedsiębiorstwa. Z tego względu system autoryzacji jest zazwyczaj opracowywany od podstaw, przy uwzględnieniu znaczących ograniczeń na stopień złożoności systemu bezpieczeństwa.

2. Model bezpieczeństwa hurtowni danych

W przypadku dużych systemów hurtowni danych do przechowywanych informacji mają dostęp różne grupy użytkowników:

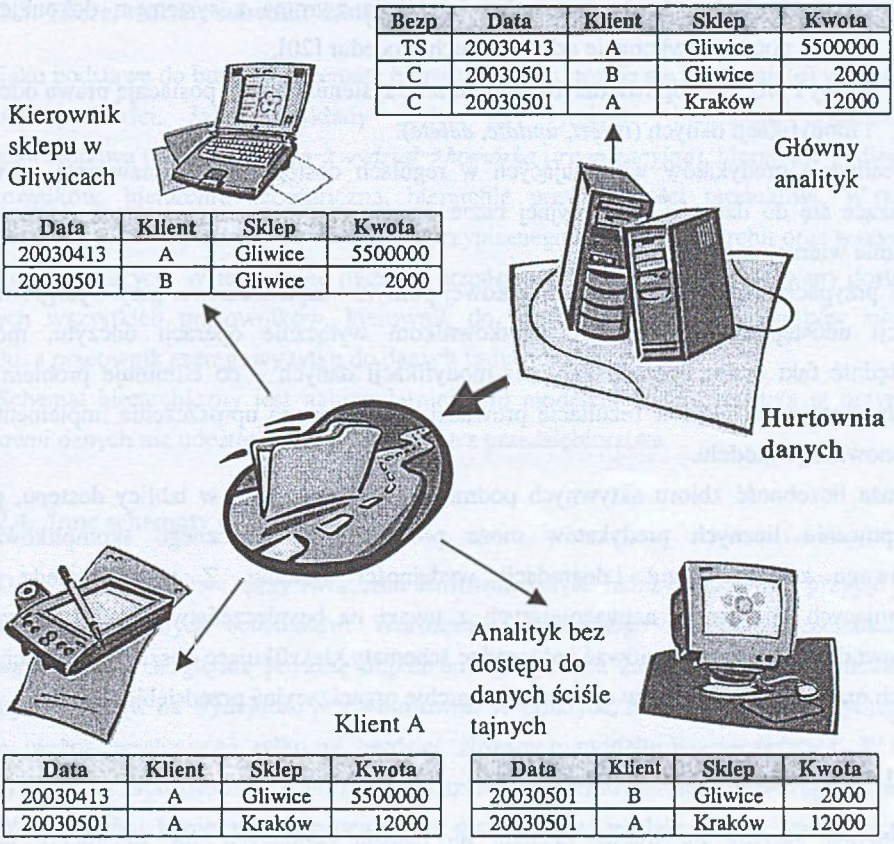
- wewnątrz przedsiębiorstwa: administratorzy, analitycy, kadra zarządzająca, pozostali pracownicy,
- na zewnątrz przedsiębiorstwa: pracownicy firm partnerskich, klienci indywidualni, pozostali użytkownicy Internetu.

W obszarze danego przedsiębiorstwa dostęp do danych zazwyczaj regulowany jest stanowiskiem w hierarchii organizacyjnej firmy. Stopień poufności danych udostępnianych na zewnątrz przedsiębiorstwa uzależniony jest od stopnia współpracy firmy i jej partnerów/użytkowników zewnętrznych.

Wymagania zebrane podczas procesu projektowania systemu hurtowni danych są podstawą do opracowania modelu bezpieczeństwa. Model ten powinien być zbudowany w oparciu o jeden z modeli formalnych [1,19]. W przypadku hurtowni danych najbardziej odpowiedni jest model systemu zamkniętego, bazującego na regułach dopuszczających wykonanie poszczególnych operacji.

Procedury zabezpieczeń wykorzystywane w hurtowniach danych są zazwyczaj implementowane w oparciu o system użytkowników i przydzielanych im praw do obiektów. Każdemu użytkownikowi systemu nadaje się odpowiedni dla niego zestaw praw, który umożliwia dostęp do ściśle określonego zestawu danych. Nadawanie praw odbywa się zgodnie z procedurami delegacji uprawnień (i jest realizowane np. przez właściciela danych,

przez administratora bezpieczeństwa itp.). Polityka bezpieczeństwa tego typu nazywana jest polityką uznaniową (ang. *discretionary*)[1]. Inne spotykane rozwiązania to tzw. obowiązkowy (ang. *mandatory*) [14,16] typ kontroli oparty na etykietach bezpieczeństwa danych i użytkowników oraz typ oparty na rolach (ang. *role-based*) [12].



Rys. 1. Przykładowe wymagania szczegółowej kontroli dostępu do danych
Fig. 1. The example of requirements of fine-grained access control to data

Projekt modelu bezpieczeństwa dla systemu hurtowni danych posiada następujące cechy charakterystyczne:

- reguły dostępu zawierają predykaty uszczegóławiające zakres dostępnych danych,
- ogranicza się uznaniowość polityki bezpieczeństwa – zarządzaniem uprawnieniami (*grant/revoke*) zajmuje się zazwyczaj pojedyncza osoba – administrator bezpieczeństwa hurtowni danych, chociaż stosowane są i tradycyjne, znane z systemów bazodanowych, zasady administracji uprawnieniami [13],
- dla użytkowników końcowych:

- dominującą operacją jest operacja odczytu danych (*read*); operacja ta realizowana jest czasami niejawnie poprzez wywołanie procedur dostępu do danych – co wymaga z kolei posiadania prawa wykonania (*use, execute*),
- użytkownicy końcowi zazwyczaj nie mają nadanych praw modyfikacji danych (*write, update*), ewentualna interakcja zwrotna z systemem dokonuje się poprzez wykonanie odpowiednich procedur [20],

- osoby i procesy odpowiedzialne za zasilanie systemu danymi posiadają prawa odczytu i modyfikacji danych (*insert, update, delete*).

Realizacja predykatów występujących w regułach dostępu (są to zazwyczaj warunki odnoszące się do danych) w relacyjnej bazie danych często wymaga kontroli dostępu na poziomie wierszy danych.

W przypadku implementacji obowiązkowej polityki bezpieczeństwa, przy występowaniu sytuacji udostępnienia końcowym użytkownikom wyłącznie operacji odczytu, można uwzględnić fakt braku operacji zapisu i modyfikacji danych – co eliminuje problem ich wieloinstancyjności [1] i w rezultacie prowadzi do znacznego uproszczenia implementacji proponowanego modelu.

Duża liczebność zbioru aktywnych podmiotów występujących w tablicy dostępu, przy występowaniu licznych predykatów może prowadzić do znacznego skomplikowania końcowego zestawu reguł i degradacji wydajności systemu. Z tego względu, dla dominujących liczebnie i najważniejszych z uwagi na bezpieczeństwo grup końcowych użytkowników można zdefiniować jednorodne schematy klasyfikujące obszary informacji, do których mają one dostęp (np. w oparciu o hierarchię organizacyjną przedsiębiorstwa).

2.1. Indywidualny schemat dostępu

Schemat zakłada możliwość dostępu do danych osobistych, np. pracownik może przeglądać informacje o swoich zarobkach, godzinach pracy, klient – o swoich zakupach. Ten schemat dostępu do danych jest najczęściej stosowany w przypadku dostępu do hurtowni osób z zewnątrz przedsiębiorstwa.

2.2. Grupowy schemat dostępu

Schemat zakłada możliwość równoprawnego dostępu do informacji osób przypisanych do danej grupy, np. struktury organizacyjnej przedsiębiorstwa (wydziału, komórki organizacyjnej) lub grupy osób odpowiedzialnych za dany produkt (menedżerowie produktów).

Ze względu na to, że w schemacie grupowym prawa są nadawane na poziomie grup użytkowników, hurtownie wykorzystujące ten system zazwyczaj przechowują znacząco mniejsze ilości informacji nadmiarowej - przez co są wydajniejsze w działaniu.

2.3. Hierarchiczny schemat dostępu

Jako podstawę do budowy schematu hierarchicznego stosuje się hierarchię(e) występującą w rzeczywistości. Jako przykłady można tu wymienić: hierarchię organizacyjną przedsiębiorstwa (*pion→podpion→wydział→komórka organizacyjna*), hierarchię podległości pracowników, hierarchię geograficzną, hierarchię przynależności produktów. W ramach hierarchii użytkownik ma dostęp do danych przypisanego poziomu hierarchii oraz wszystkich poziomów niższych. W ten sposób dyrektor przedsiębiorstwa ma zagwarantowany dostęp do danych wszystkich pracowników, kierownik do danych swoich i pracowników swojego działu, a pracownik szeregowy tylko do danych indywidualnych.

Schemat hierarchiczny jest najpopularniejszym modelem bezpieczeństwa w przypadku hurtowni danych nie udostępnianych na zewnątrz przedsiębiorstwa.

2.4. Inne schematy dostępu

O ile jest to możliwe, przy tworzeniu hurtowni danych należy uzgodnić i przyjąć jeden z wyżej wymienionych schematów. Wdrożenie jednorodnego schematu bezpieczeństwa pozwala uzyskać względną prostotę implementacji systemu zabezpieczeń i ogranicza jego negatywny wpływ na wydajność pracy hurtowni. W praktyce, mogą pojawić się wymagania, które można zrealizować tylko w bardziej złożonym modelu bezpieczeństwa. W takiej sytuacji można zaproponować stworzenie mieszanego systemu hierarchiczno-grupowego.

W przypadku konieczności zapewnienia maksymalnej wydajności dla zaufanej grupy użytkowników danego przedsiębiorstwa można zbudować dziedzinową hurtownię danych, która:

- ma zdefiniowany uproszczony zbiór reguł dostępu lub
- nie posiada systemu bezpieczeństwa na poziomie wierszy, a dostęp do danych jest ograniczany poprzez mechanizmy autentykacji.

3. Realizacja wymagań kontroli dostępu do danych

W zakresie ograniczenia widoczności danych w hurtowni można wyróżnić następujące wymagania [15]:

- wymagania proste:
  - ukrywanie całych kostek danych,
  - ukrywanie wybranych miar (faktów),
  - ukrywanie przekrojów kostek,
  - ukrywanie danych szczegółowych (danych na niższych poziomach),
- wymagania zaawansowane:
  - ukrywanie danych szczegółowych dla wybranych przekrojów kostek w pojedynczym wymiarze,
  - ukrywanie wybranych miar w wybranych przekrojach kostek,
  - ukrywanie złożonych przekrojów kostki (w różnych płaszczyznach),
  - ukrywanie danych szczegółowych dla wybranych przekrojów kostek w różnych wymiarach,
  - dynamiczne ograniczenia dostępu (oparte na wartościach danych).

Jako cechy charakterystyczne implementacji systemu autoryzacji w hurtowni danych typu ROLAP można wyróżnić:

- konieczność zachowania schematu wielowymiarowego modelu hurtowni danych,
- nadawanie praw na poziomie wierszy – uprawnienia nadawane na poziomie tablic lub partycji tablic są z reguły niewystarczające,
- w większości przypadków zarządzanie prawami użytkowników końcowych, ogranicza się do zapewnienia odpowiednich praw do odczytu danych,
- konieczność zachowania akceptowalnej wydajności systemu przy założeniu:
  - przyszłych zmian procedur bezpieczeństwa,
  - potencjalnie bardzo dużej społeczności użytkowników hurtowni danych.

Implementację wymienionych wymagań w konkretnym systemie hurtowni danych typu ROLAP można zlecić pojedynczemu komponentowi systemu: serwerowi bazy danych, serwerowi OLAP, aplikacji OLAP lub też zrealizować przy współpracy kilku elementów.

Zabezpieczenie dostępu do danych w systemach hurtowni danych realizowane jest zasadniczo w oparciu o wykorzystanie mechanizmów bezpieczeństwa wbudowanych w system zarządzania bazą danych. Rozwiązanie takie pozwala zbudować elastyczny i jednolity system zabezpieczeń dla wszystkich aplikacji korzystających z hurtowni danych. Do zalet rozwiązania można zaliczyć:

- realizację procedur bezpieczeństwa na serwerze bazy danych – wszystkie aplikacje łączące się z hurtownią danych wykorzystują ten sam system bezpieczeństwa, niezależnie od rodzaju aplikacji - użytkownik może użyć do połączenia z hurtownią aplikacji innej niż aplikacja OLAP i będzie ona podlegała tym samym regułom dostępu,

- uproszczenie zasad tworzenia aplikacji OLAP, które nie musi implementować systemu zabezpieczeń lub czyni to w niewielkiej części (np. ustawienie kontekstu [22]),
- ułatwienie rozwoju systemu – zmiany w polityce bezpieczeństwa, które zostają zaimplementowane w bazie danych – nie wpływają na pracę aplikacji OLAP w sensie konieczności jej modyfikacji,
- wymuszenie używania – przy logowaniu do bazy danych – indywidualnych nazw użytkowników, co pozwala na prowadzenie audytu na poziomie pojedynczego użytkownika,
- możliwość budowy jednorodnego systemu zabezpieczeń obejmującego nie tylko hurtownię danych, ale i zasilające ją – a zwykle niezależnie administrowane – źródła danych [7].

Rozwiązanie wykorzystujące mechanizmy bazy danych ma również pewne wady, które opisano w dalszej części artykułu.

Drugą z możliwości autoryzacji dostępu do danych jest wbudowanie mechanizmów bezpieczeństwa w aplikację OLAP końcowego użytkownika. Rozwiązanie to można stosować w przypadku, gdy do pracy z hurtownią danych użytkownikom udostępnia się pojedynczą aplikację. Aplikacja ta jest w pełni odpowiedzialna za kontrolę prezentowanych danych oraz czynności, które może wykonać użytkownik. W tym rozwiązaniu należy ukryć – przed osobą pracującą z aplikacją – nazwę i hasło użytkownika wykorzystywanego do połączenia z bazą hurtowni danych. Postępowanie takie zabezpiecza przed nieautoryzowanym dostępem do poufnych danych z poziomu innego narzędzia, co pozwoliłoby obejść zabezpieczenia zaimplementowane w aplikacji OLAP.

Wbudowanie mechanizmów bezpieczeństwa w aplikację ułatwia sterowanie funkcjonalnością aplikacji oraz zakresem widoczności danych. Dodatkowo omawiane rozwiązanie może pozwolić na budowę systemu o większej szybkości działania w porównaniu do klasycznego rozwiązania opartego na mechanizmach bazy danych, które wykorzystuje perspektywy. Wymienione zalety rozwiązania z mechanizmami bezpieczeństwa wbudowanymi w aplikację OLAP nie rekompensują jego wad:

- aplikacja OLAP powinna być jedyną aplikacją umożliwiającą użytkownikom pracę w systemie,
- z reguły brak rozróżnienia użytkowników na poziomie bazy danych – używane jest pojedyncze konto użytkownika posiadającego pełne prawa,
- wzrost złożoności aplikacji,
- zazwyczaj konieczność modyfikacji aplikacji przy zmianach procedur bezpieczeństwa.

Najnowsze systemy OLAP pozwalają na wybór jednego z wyżej wymienionych mechanizmów, a nawet wspierają system mieszany. MicroStrategy 7i umożliwia zdefiniowanie na poziomie aplikacji OLAP tzw. widoków bezpieczeństwa. Widoki te przypisywane są poszczególnym użytkownikom i definiują one warunki, o które uzupełniane są frazy WHERE tworzonych na ich żądanie poleceń SQL [21]. Z drugiej strony, system ten obsługuje widoki bezpieczeństwa oraz pozwala na przypisanie własnym użytkownikom aplikacyjnym różnych użytkowników bazy danych (przez definicję tzw. map połączeń, ang. *connection maps*).

W systemach z wyróżnionym serwerem OLAP jest on najbardziej odpowiednim komponentem do realizacji mechanizmów bezpieczeństwa [15]. Moduł serwera OLAP jest często obecny w systemach wielowymiarowych baz danych (MOLAP) i w systemach hybrydowych (HOLAP). W systemach ROLAP funkcjonalność motoru OLAP może być wbudowana w serwer relacyjnej bazy danych lub w aplikację użytkownika końcowego.

Autorzy prac [8,9] zwracają uwagę na możliwość wystąpienia sytuacji, w których konieczne jest dodatkowe zabezpieczenie danych poprzez szyfrowanie. Prace te wskazują na możliwość uzyskania dostępu do danych poprzez wykorzystanie mechanizmów dostępu do systemu plików z poziomu systemu operacyjnego. Rozważania te leżą poza obszarem niniejszej pracy.

4. Mechanizmy zabezpieczeń w hurtowniach danych

Zastosowanie mechanizmów bezpieczeństwa wbudowanych w bazę danych jest najbardziej naturalnym sposobem rozwiązania problemu implementacji polityki bezpieczeństwa. Szczególnie w przypadku hurtowni danych typu ROLAP możliwe jest wykorzystanie dużej różnorodności metod dostępnych w relacyjnych bazach danych.

Dostęp do informacji w relacyjnych bazach danych ograniczany jest przypisanym do użytkownika zbiorem przywilejów i praw. Stosowane ograniczenia mają zastosowanie na różnych poziomach dostępu do informacji:

- na poziomie dostępu do bazy danych hurtowni,
- na poziomie dostępu do obiektów bazy danych (tablic, widoków i innych),
- na poziomie dostępu do danych:
    - danych przechowywanych w pewnych kolumnach tablic,
    - danych przechowywanych w pewnych wierszach tablic (rekordach).

Użytkownicy otrzymują odpowiednie prawa indywidualnie lub poprzez role. Należy przy tym przyjąć politykę nadawania użytkownikom minimalnego – wystarczającego do wykonania przypisanych im zadań – zestawu uprawnień.

Częstym wymaganiem stawianym implementacji systemu bezpieczeństwa jest zachowanie jednorodności listy obiektów widzianych przez wszystkich użytkowników. Jeżeli użytkownicy mają dostęp do danych poprzez obiekty (np. perspektywy, procedury) o tych samych nazwach, to – przy braku innych szczególnych wymagań – ze względu na zachowanie jednorodnego (wg nazw, zaś niekonieczne wg definicji) zbioru obiektów możliwe jest utworzenie pojedynczej, uniwersalnej aplikacji OLAP obsługującej wszystkich użytkowników. W takim przypadku motor bazy danych odpowiedzialny jest za dostarczenie informacji autoryzowanej, a aplikacja tylko umożliwia dostęp do otrzymanego (zależnego od użytkownika) zestawu danych. Takie rozwiązanie znacząco obniża koszty implementacji aplikacji oraz administrowania systemem. Obecnie wykorzystywane systemy relacyjnych baz danych posiadają mechanizmy, pozwalające na realizację postulatu jednorodności.

4.1. Dostęp do bazy hurtowni danych

Dostęp do hurtowni danych można ograniczyć na różnych poziomach wielowarstwowej architektury systemu komputerowego. Dalsze rozważania prowadzone w tym rozdziale ograniczono do opisu zabezpieczenia dostępu na poziomie serwera bazy danych.

W ogólnym przypadku użytkownicy hurtowni danych powinni posiadać prawo łączenia się z bazą danych (*connect*). Niektóre systemy OLAP wymagają do poprawnej pracy pewnych dodatkowych praw i przywilejów systemowych (np. aplikacje Micro*Strategy* wymagają posiadania prawa tworzenia zasobów (*resource*), gdyż system podczas pracy tworzy w hurtowni danych dodatkowe tablice do przechowywania wyników).

4.2. Dostęp do obiektów hurtowni danych

W celu uzyskania dostępu do tablic i widoków hurtowni danych administrator bezpieczeństwa systemu powinien jawnie przypisać użytkownikowi wymagane prawa. Z tego też względu należy unikać udostępniania obiektów jako obiektów publicznych.

Użytkownicy systemu otrzymują prawa odczytu danych (*select*) do poszczególnych tablic hurtowni danych. Administrator hurtowni – poprzez nadawanie/odbieranie praw do tablic implementujących wielowymiarowy model danych – zarządza możliwościami dostępu do poszczególnych obszarów informacji (dane kadrowe, płacowe itp.). Osoby mające dostęp do danych określonego typu:

- posiadają prawo *select* do tablic bazowych i związanych z nimi tablic wymiarów i tablic relacji,
- nie posiadają prawa *select* do pozostałych tablic.

W niektórych systemach bazodanowych dostęp do obiektów nie jest realizowany bezpośrednio, ale z użyciem procedur składowanych. W takim przypadku użytkownikowi należy nadać odpowiednie prawa wykonywania tych procedur (*execute*), bez nadawania bezpośrednich praw do obiektów. Wykorzystanie procedur składowanych pozwala na realizację kompletnego systemu autoryzacji kontrolującego dostęp do danych na poziomie rekordów (opis poniżej).

Przy zróżnicowaniu dostępu do obiektów hurtowni danych należy zapewnić odpowiednią reakcję aplikacji OLAP na możliwe pojawienie się błędu dostępu. Aplikacje OLAP z reguły generują jednakowy kod poleceń (np. *SQL*) dostępu do danych dla wszystkich użytkowników aplikacji. W przypadku gdy użytkownik nie ma prawa odczytu z określonego obiektu, to wykorzystujący go raport nie wykona się. W takim przypadku należy raport ten zmodyfikować lub udostępniać tylko dla użytkowników posiadających odpowiednie prawa.

4.3. Dostęp do danych

Zarządzanie prawami dostępu do obiektów hurtowni pozwala na nadanie użytkownikowi możliwości dostępu pełnego lub też całkowitego zakazu dostępu do danych tych obiektów. Często zachodzi potrzeba zapewnienia użytkownikowi dostępu tylko do podzbioru danych przechowywanych w obiekcie. Podział zbioru danych na podzbiory może mieć charakter:

- podziału pionowego – np. użytkownik nie powinien mieć dostępu do pewnych kolumn tablic,
- podziału poziomego – np. użytkownik nie powinien mieć dostępu do pewnych wierszy tablic,
- podziału mieszanego – pionowo-poziomego.

Metody rozwiązania problemu dostępu do podzbioru danych różnią się w zależności od charakteru podziału podzbioru. Rozwiązania te często nie są trywialne i mogą wpłynąć na projekt aplikacji systemu OLAP.

4.3.1. Dostęp do kolumn tablic

Zapewnienie pionowego podziału danych – na część udostępnioną i zastrzeżoną – jest częstym wymaganiem występującym w modelu bezpieczeństwa hurtowni danych. Podział ten może dotyczyć tablic faktów, jak i tablic wymiarów. Jako przykład można tu przedstawić raport z systemu *Analizy Zasobów Ludzkich* wykorzystujący atrybuty wymiaru opisującego pracownika przedsiębiorstwa (np. płeć, staż) i fakty związane z czasem pracy bez

udostępnienia pełnych danych osobowych analizowanych pracowników (np. imię, nazwisko, numer PESEL, data urodzenia) i faktów związanych z nieobecnościami. Osoby, które nie mają dostępu do pełnych danych osobowych, powinny mieć dostęp do danych częściowych, aby np. móc zliczyć ilość zatrudnionych kobiet i mężczyzn.

W celu umożliwienia wykonywania tego typu raportów należy zachować możliwość korzystania z atrybutów nie będących danymi chronionymi oraz z identyfikatorów łączących tablice wymiarów z tablicami faktów. Warunek ochrony części danych osobowych wymaga natomiast zapewnienia niedostępności tych danych (z reguły opisów) przechowywanych w tablicach wymiarów.

Dostęp do kolumn tablic można kontrolować poprzez:

- kontrolę praw do kolumn,
- wykorzystanie perspektyw,
- wykorzystanie procedur składowanych.

4.3.1.1. Kontrola praw odczytu do kolumn tablic i widoków

W systemach pozwalających na nadawanie praw odczytu do poszczególnych kolumn tablic (np. Informix) można uzyskać podział pionowy poprzez nadanie praw *select*, nie do całej tablicy, ale tylko do jej odpowiednich kolumn.

4.3.1.2. Wykorzystanie perspektyw

Perspektywy budowane na tablicach (lub też innych perspektywach) pozwalają w prosty sposób uzyskać podział pionowy [25]. W definicji perspektywy specyfikujemy kolumny, do których dany użytkownik ma mieć dostęp. Niestety, dla każdego użytkownika, któremu udostępniane są dane z określonej części obiektu, należy stworzyć oddzielną perspektywę. Istnienie wielu nazw dla tego samego źródła danych może prowadzić do konieczności utworzenia wielu konfiguracji projektu OLAP – po jednej dla każdego wyróżnionego użytkownika. Zadanie utrzymywania różnorodnych konfiguracji może być bardzo uciążliwe administracyjnie – zwłaszcza w systemach, które często podlegają rozbudowie lub z których korzysta wielu użytkowników.

4.3.1.3. Wykorzystanie procedur składowanych

Wykorzystanie procedur składowanych w systemach bazodanowych pozwala na budowę bezpiecznego i elastycznego systemu bezpieczeństwa [22]. W rozwiązaniu tym użytkownikom nie nadaje się bezpośrednich praw do obiektów, ale do procedur, które działają na tych obiektach. Procedury składowane kontrolują zakres operacji, które może wykonać wywołujący je użytkownik. W rzeczywistych systemach autoryzacji wykorzystujących procedury składowane z reguły stosuje się je do zabezpieczenia operacji zapisu, modyfikacji i usuwania danych. W przypadku odczytu danych kontrola dostępu jest zazwyczaj realizowana poprzez przydzielanie praw odczytu (*select*) do widoków

zbudowanych na tablicach przechowujących dane (choć i w tym przypadku można skorzystać z procedury).

Wykorzystanie procedur składowanych w aplikacjach OLAP może być utrudnione ze względu na to, że aplikacje te zazwyczaj wymagają zachowania modelu wielowymiarowego i potrafią realizować operacje jedynie na obiektach typu tablica i perspektywa. W tym przypadku – o ile zezwala na to system zarządzania bazą danych – można spróbować wykorzystać procedury składowane do budowy „zabezpieczonej" perspektywy. „Zabezpieczona" perspektywa pozwala użytkownikowi na odczyt tylko autoryzowanych danych. W definicji takiej perspektywy nie korzysta się bezpośrednio z nazw kolumn zabezpieczanego obiektu, ale z nazw procedur sterujących odpowiednim udostępnianiem danych. Parametrem procedury jest kolumna zabezpieczanego obiektu. W swoim działaniu procedura sprawdza uprawnienia wywołującego ją użytkownika do danej kolumny i w zależności od posiadanych uprawnień zwraca rzeczywistą wartość danych lub też pewną zdefiniowaną stałą (np. wartość NULL). Niestety, skuteczna implementacja metody wymaga istnienia w systemie znacznych rezerw wydajnościowych.

Uprawnienia użytkowników są przechowywane w dodatkowej tablicy, zwanej **tablicą praw dostępu do kolumn**. Tablice te przechowują krotki o postaci {*identyfikator użytkownika, obiekt, kolumna*}, wskazujące na posiadanie przez użytkownika o podanym identyfikatorze prawa do kolumny pewnego obiektu. Uwzględniając sposób dostępu do kolumny, można dokonać rozszerzenia tablicy praw do postaci: {*identyfikator użytkownika, obiekt, kolumna, typ dostępu*}.

Użycie procedur składowanych w procesie kontroli dostępu do kolumn tablic (perspektyw) pozwala zachować jednorodność nazw obiektów hurtowni danych widzianych przez wszystkich użytkowników i nie wymaga ingerencji w sposób działania aplikacji.

4.3.2. Dostęp do danych na poziomie wierszy

Zabezpieczenie dostępu do danych na poziomie wierszy jest najczęstszą konsekwencją istnienia warunku predykatu występującego w tablicy dostępu stosowanego modelu. Problem ten jest często kluczowym problemem bezpieczeństwa występującym w systemie hurtowni danych. Autoryzacji dostępu podlegają dane tablic bazowych oraz w niektórych przypadkach dane wybranych wymiarów.

System autoryzacji dostępu do wierszy danych można zrealizować za pomocą:

- perspektyw bezpieczeństwa,
- partycjonowania poziomego tablic,
- procedur składowanych,
- prywatnych, wirtualnych baz danych,
- etykiet bezpieczeństwa.

4.3.2.1. Perspektywy bezpieczeństwa

Zbudowanie na obiekcie perspektywy z wykorzystaniem statycznego warunku WHERE pozwala w prosty sposób ograniczyć widoczność danych (np. WHERE id_kom_org=13). Niestety, konstrukcja warunku w tej formie nie daje możliwości budowy uniwersalnej perspektywy obsługującej wszystkich użytkowników. Rozwiązaniem problemu jest zastosowanie – podobnie jak w przypadku wyżej opisywanych procedur składowanych – tablicy **praw dostępu** (nazywanej też **tablicą bezpieczeństwa**). Tablica ta przechowuje uprawnienia użytkowników w postaci: {*identyfikator użytkownika, identyfikator prawa*}, co oznacza posiadanie przez użytkownika o podanym identyfikatorze pewnego prawa. Identyfikatory praw w tablicy bezpieczeństwa mogą bezpośrednio odnosić się do identyfikatorów atrybutów, do których użytkownik ma dostęp. W przypadku konieczności zabezpieczenia wielu obiektów można stosować kilka tablic praw dostępu lub też pojedynczą, zbiorczą tablicę praw. Rozwiązaniu z pojedynczą tablicą sprzyja fakt, że w hurtowni danych identyfikatory mają jednolity format identyfikatorów numerycznych. W przypadku gdy tablica bezpieczeństwa przechowuje prawa dotyczące wielu obiektów, to jej definicję można rozszerzyć do postaci: {*identyfikator użytkownika, identyfikator obiektu, identyfikator prawa*}, a po uwzględnieniu sposobu dostępu do danych do postaci: {*identyfikator użytkownika, identyfikator obiektu, identyfikator prawa, typ dostępu*}. W szczególnym przypadku systemu bezpieczeństwa, w którym wyróżniono tylko jedno uprawnienie, tablica praw może przechowywać tylko nazwy użytkowników posiadających to uprawnienie: {*identyfikator użytkownika*}. W hurtowniach danych posiadających rozbudowany system kontroli dostępu oparty na tablicy bezpieczeństwa, zbiorcza tablica praw może być największą tablicą występującą w systemie. Z tego m.in. względu warto utrzymywać restrykcyjną politykę nadawania uprawnień.

Podczas korzystania z perspektywy bezpieczeństwa, na podstawie nazwy użytkownika, dokonywana jest selekcja tylko tych wierszy tablic (perspektyw), do których użytkownik ma prawo. Definicja perspektywy bezpieczeństwa zawiera warunek złączenia tablicy bezpieczeństwa z obiektem chronionym według identyfikatora prawa (atrybutu) przy spełnieniu warunku odpowiedniej nazwy użytkownika.

Szczególnie ważną zaletą rozwiązania stosującego perspektywy bezpieczeństwa jest istnienie tylko jednego, wspólnego schematu obiektów hurtowni dla wszystkich użytkowników systemu. Jednolity schemat pozwala na utrzymywanie tylko jednego projektu metadanych aplikacji OLAP dla wszystkich użytkowników.

W rozwiązaniu tym użytkownikom nadawane jest wyłącznie prawo odczytu do zabezpieczonej perspektywy.

4.3.2.2. Dynamiczne perspektywy bezpieczeństwa

W celu uniknięcia wykonywania kosztownego złączenia tablicy danych z tablicą bezpieczeństwa możliwe jest dynamiczne tworzenie perspektyw. W takim przypadku – na podstawie nazwy użytkownika – w procesie uruchamiania aplikacji OLAP tworzony jest zestaw perspektyw z odpowiednią definicją frazy warunku. Przypisane do danego użytkownika frazy warunku mogą być przechowywane w dedykowanej tablicy fraz, możliwe jest także ich wyznaczanie na podstawie informacji z tablicy bezpieczeństwa.

Stworzenie systemu opartego na metodzie dynamicznych perspektyw wymaga włożenia znacznego wysiłku programistycznego. Stąd też ten typ zabezpieczeń realizowany jest z reguły w kooperacji aplikacji OLAP i bazy danych, choć można go również zrealizować korzystając wyłącznie z mechanizmów bazy danych.

4.3.2.3. Partycjonowanie poziome tablic

W przypadku gdy aplikacja OLAP potrafi obsługiwać partycjonowanie tablic, możliwe jest wykorzystanie tej cechy do zabezpieczenia dostępu do danych. Przez partycjonowanie tablic na poziomie aplikacji rozumiemy obsługę wielu fizycznie różnych tablic o takiej samej strukturze jako jednej tablicy logicznej. Każda z tablic („partycja") przechowuje pewien wycinek danych wydzielonych z całości na podstawie przyjętego kryterium podziału (np. dane związane z konkretnym regionem sprzedaży lub też informacje z danego roku). Użytkownikom systemu nadaje się prawa odczytu do tych tablic partycji, które przechowują dane, do których powinien mieć on dostęp (np. każdy sprzedawca ma dostęp do partycji przechowującej dane ze swojego regionu). Jeżeli możliwe jest stworzenie mechanizmu autoryzacji w oparciu o kontrolę dostępu do poszczególnych partycji, to implementacja takiego mechanizmu bezpieczeństwa może nie wnosić dodatkowych obciążeń wydajnościowych (patrz uwaga niżej).

Mechanizm ten ma pewne wady związane z koniecznością partycjonowania danych:

- konieczna jest obsługa partycjonowania na poziomie aplikacji,
- efektywna implementacja musi bazować na wydzieleniu niewielu rozłącznych grup danych,
- dane najczęściej partycjonuje się według atrybutów wymiaru czasu, którego z reguły nie da się wykorzystać przy definiowaniu procedur bezpieczeństwa (chyba że zostanie ustalony podział na grupę użytkowników danych bieżących i historycznych),
- zmniejsza się wydajność przetwarzania zapytań przekrojowych – wymagających danych z wielu (wszystkich) tablic partycji,
- utrudnione jest zarządzanie systemem, a procesy ekstrakcji danych są bardziej złożone.

4.3.2.4. Wykorzystanie procedur składowanych

Sposób wykorzystania procedur składowanych w procesie autoryzacji dostępu do wierszy danych jest podobny jak przy ograniczeniu widoczności kolumn danych. Procedury składowane na podstawie nazwy użytkownika i informacji zawartych w tablicy bezpieczeństwa umożliwiają dostęp tylko do danych autoryzowanych.

4.3.2.5. Modyfikacja zapytań

Największą zaletą wbudowania mechanizmów bezpieczeństwa w aplikację współpracującą z bazą danych jest możliwość zachowania wysokiej wydajności pracy systemu. Ograniczenie widoczności danych uzyskuje się w aplikacji poprzez modyfikację generowanych w imieniu użytkownika zapytań według aktualnie posiadanych przez niego uprawnień. Wbudowanie podobnie działającego mechanizmu w motor zarządzania bazą danych pozwala na implementację systemu bezpieczeństwa o najlepszych cechach klasycznego rozwiązania aplikacyjnego i bazodanowego.

W przypadku *SQL*'owych baz danych uzyskiwane przez użytkownika wyniki można ograniczać poprzez modyfikację frazy WHERE wysyłanych przez niego zapytań. Użytkownikowi można przypisać różne postacie frazy modyfikującej w zależności od:

- obiektów, na których działa zapytanie,
- aktualnego stanu, w jakim znajduje się system (aktualnego czasu, wcześniejszego wykonania przez system/użytkownika pewnych operacji itp.) – nazywanego kontekstem.

Komercyjnym przykładem implementacji mechanizmu tego typu jest prywatna, wirtualna baza danych (ang. *Virtual Private Database*) dostępna w środowisku Oracle 8i/9i [22]. Zaproponowane rozwiązanie uzupełnia opisane wcześniej „klasyczne" metody implementacji kontroli dostępu. Możliwość zdefiniowania w bazie danych kodu (funkcji) odpowiedzialnego za dynamiczną generację frazy ograniczającej zapewnia bardzo dużą elastyczność rozwiązania. Przy ustalaniu formuły frazy warunku mogą być wykorzystywane informacje o użytkowniku, jego prawach, sposobie połączenia do bazy danych, stanie systemu itp. W przypadku istnienia – dla danego użytkownika – kilku funkcji generujących frazy warunku rezultaty ich działania są łączone operatorem AND. Mechanizm modyfikacji poleceń *SQL* w Oracle jest uniwersalny i można go stosować nie tylko do poleceń *select*, ale i do poleceń *insert*, *update* i *delete*. Mechanizmem pomocniczym w realizacji prywatnej, wirtualnej bazy danych jest kontekst aplikacji (ang. *application context*), który umożliwia zarządzanie dodatkową informacją o użytkowniku (np. o jego statusie, przynależności do pewnej grupy) i stanie, w jakim znajduje się aplikacja.

Metoda kontroli dostępu oparta na modyfikacji zapytań przez motor bazy danych łączy w sobie zalety implementacji autoryzacji na poziomie bazy danych z wydajnością uzyskiwaną

w rozwiązaniach aplikacyjnych. Możliwość programowego ustalania sposobu modyfikacji zapytań pozwala na stosunkowo prostą implementację nawet bardzo złożonych schematów bezpieczeństwa. Zgrupowanie logiki zarządzającej polityką bezpieczeństwa w pojedynczej funkcji (pakiecie funkcji) znakomicie upraszcza zarządzanie i ewentualną modyfikację stosowanych w systemie procedur.

4.3.2.6. Etykiety bezpieczeństwa

Systemy zabezpieczeń oparte na tradycyjnej uznaniowej kontroli dostępu nie zabezpieczają w należyty sposób przed przepływem informacji poufnej do osób nieuprawnionych oraz przed utratą integralności danych [1]. Wymagania te spełniają systemy obowiązkowej kontroli dostępu (MAC – ang. *mandatory access policy*).

W systemie implementującym MAC dokonuje się klasyfikacji podmiotów (użytkowników) i obiektów (tablic, plików) występujących w systemie według kryteriów poufności. Użytkownikom systemu nadaje się tzw. poziom uwierzytelnienia, a obiektom przechowującym dane przypisuje się tzw. poziom wrażliwości informacji. Użytkownik pracujący w systemie może zmieniać swój poziom uwierzytelnienia w zakresie nie przekraczającym przypisanego mu poziomu maksymalnego. Użytkownik pracujący na wybranym przez siebie poziomie uwierzytelnienia ma dostęp do danych o równym lub niższym poziomie wrażliwości. Etykieta wrażliwości informacji zazwyczaj zbudowana jest z dwóch elementów:

1. **poziomu** określającego stopień jawności danych, np. *ściśle tajny, tajny, poufny, niesklasyfikowany*,
2. opcjonalnego zestawu **kategorii** danych rozdzielających logicznie dane na podzbiory, np. *finanse, produkcja*.

Sposób pracy w modelu MAC określony jest poprzez dwie podstawowe reguły [11,1]:

1. brak możliwości odczytu danych o wyższych etykietach wrażliwości niż aktualna etykieta uwierzytelnienia (ang. „*no read-up*"),
2. brak możliwości zapisu danych z niższą etykietą wrażliwości niż aktualna etykieta uwierzytelnienia (ang. „*no write-down*").

Reguły te zapobiegają nieautoryzowanemu przepływowi informacji pomiędzy obiektami (tablicami, plikami) występującymi w systemie (co jest podstawowym warunkiem zapewnienia poufności informacji).

W najbardziej ogólnym przypadku MAC wymaga sklasyfikowania danych na poziomie elementów danych (krotek danych czy nawet ich elementów składowych). Wymaganie to koresponduje z występującą w wielu hurtowniach danych koniecznością kontroli dostępu na poziomie wierszy. Dodatkowo ten typ modelu dobrze sprawdza się w przypadku dużych ilości informacji, które wymagają dokładnego zabezpieczenia, co jest charakterystycznym

wymaganiem stawianym hurtowniom danych udostępniających informacje szerokiej rzeszy odbiorców (np. w sieci Internet).

Komercyjnym przykładem implementacji MAC jest technologia etykiet bezpieczeństwa *Oracle Label Security* (OLS) wprowadzona w Oracle 9i [23]. Rozwiązanie to jest rozwinięciem technologii wirtualnych, prywatnych baz danych Oracle 8i. W przypadku OLS etykieta wrażliwości obok poziomu i kategorii może mieć zdefiniowany trzeci, opcjonalny element: zestaw **grup**. Grupy, podobnie jak kategorie, opisują przynależność danych do pewnego podzbioru, ale w przeciwieństwie do kategorii (których struktura jest zazwyczaj płaska) mogą one tworzyć struktury hierarchiczne, np. *1. Świat → 1.1. Europa, 1.2. Ameryka → 1.1.1 Polska, 1.1.2. Wielka Brytania, 1.2.1 Stany Zjednoczone, 1.2.2 Kanada*. Elementy niższych poziomów hierarchii logicznie wchodzą w skład wyższych poziomów hierarchii. Użytkownik, który pragnie mieć dostęp do danych pewnej grupy, może mieć przypisany bezpośredni dostęp do tej właśnie grupy lub też może mieć przypisany dostęp do dowolnej grupy wyższego poziomu hierarchii zawierającej pożądaną grupę.

Rozbudowany format etykiet OLS (*poziom:kategorie:grupy*) pozwala na implementację różnorodnych schematów dostępu wymaganych w realizowanym projekcie hurtowni danych. Należy tu zaznaczyć, że technologia OLS uzupełnia podstawowe uznaniowe mechanizmy zabezpieczeń Oracle i jest ona uruchamiana na ostatnim etapie autoryzacji po stwierdzeniu posiadania przez użytkownika wszelkich koniecznych systemowych praw do obiektu.

5. Wpływ mechanizmów kontroli dostępu na pracę hurtowni danych

Uruchomienie systemu zabezpieczeń ma znaczący wpływ na pracę hurtowni danych. Podstawowymi niedogodnościami związanymi z wprowadzeniem systemu autoryzacji jest złożoność implementacji i częste ograniczenie wydajności hurtowni danych (obserwowane spadki wydajności to 20-500%). Co więcej, zdarza się, że polityka zabezpieczeń uniemożliwia tworzenie pewnych klas zmaterializowanych struktur zagregowanych, tak ważnych dla efektywnej pracy hurtowni danych. Każdy agregat ma naturę tablicy bazowej, gdyż przechowuje fakty, a dostęp do nich powinien podlegać autoryzacji. Stąd też wypływa ograniczenie możliwości budowy niektórych agregatów – każdy z nich powinien bowiem posiadać niezagregowane atrybuty kontrolujące dostęp do danych (chyba że polityka bezpieczeństwa jest inna i np. umożliwia nielimitowany dostęp do podsumowań).

Poprawę wydajności hurtowni danych z zaimplementowanym systemem kontroli dostępu można osiągnąć poprzez:

- wybór jak najmniej złożonej polityki bezpieczeństwa,

- ograniczenie rozmiaru tablicy praw dostępu – liczby praw i użytkowników (ew. utworzenie grup),
- załadowanie tablic praw dostępu do pamięci operacyjnej,
- implementację hurtowni danych w schemacie płatka śniegu, w którym implementacja systemu bezpieczeństwa jest prostsza,
- budowę i utrzymanie dwóch aplikacji OLAP:
  - aplikacji standardowej, korzystającej z mechanizmów bezpieczeństwa,
  - aplikacji dla użytkowników specjalnych, która pomija mechanizmy bezpieczeństwa i bezpośrednio odwołuje się do danych.

Oprócz spadku wydajności, system zabezpieczeń wnosi duże obciążenia administracyjne związane z zarządzaniem prawami oraz dodatkowymi strukturami danych. Jak wspomniano już wcześniej, tablica praw dostępu może być największą tablicą hurtowni danych. Zazwyczaj konieczne jest też dostarczenie dodatkowej aplikacji zarządzającej prawami (rolami, użytkownikami i grupami użytkowników). Zmiany polityki bezpieczeństwa mogą wymusić przebudowę systemu autoryzacji, co może prowadzić do spadku wydajności poza akceptowalny poziom.

W przypadku wdrożenia mechanizmów bezpieczeństwa wbudowanych w system zarządzania bazą danych może pojawić się konieczność indywidualnego konfigurowania aplikacji OLAP dla każdego z użytkowników systemu. Indywidualna konfiguracja projektu powinna uwzględniać możliwość dostępu użytkownika do obiektów bazy danych (tablic, perspektyw) oraz do obiektów OLAP: poszczególnych wymiarów, atrybutów, faktów i raportów.

Wszyscy użytkownicy systemu OLAP powinni zostać poinformowani o wpływie systemu bezpieczeństwa na rodzaj informacji, którą otrzymują. Po wdrożeniu systemu bezpieczeństwa otrzymywane przez użytkowników raporty mogą sprawiać wrażenie niepoprawnych. Sytuacja ta związana jest z faktem, że dane i podsumowania, które widnieją na raportach, mogą dotyczyć nie całości, ale tylko tej części danych, do których w danej chwili ma dostęp wykonujący raport użytkownik.

6. Podsumowanie

Złożone i podlegające ciągłym zmianom wymagania związane z kontrolą udostępniania informacji w zasadniczy sposób wpłynęły na rozwój mechanizmów zabezpieczeń. Tradycyjny system kontroli dostępu – oparty na prawach oraz na wykorzystaniu perspektyw bazodanowych – został znacznie rozszerzony poprzez wprowadzenie rozwiązań o większej

elastyczności, niższej złożoności implementacji, przy jednoczesnym zapewnieniu odpowiedniej wydajności pracy systemu. Osoba tworząca system bezpieczeństwa hurtowni danych dysponuje obecnie szerokim zestawem mechanizmów implementacyjnych [24]. Wśród rozwiązań korzystających z możliwości wbudowanych w system zarządzania bazą danych za najbardziej odpowiedni można uznać mechanizm dynamicznej modyfikacji zapytań. W pewnych specyficznych sytuacjach konieczna może się okazać budowa systemu działającego w oparciu o etykiety bezpieczeństwa informacji.

LITERATURA

1. Castano S., Fugini M., Matrella G., Samarati P.: Database Security. ACM Press, 1995.
2. Kimball R., Reeves L., Margy R., Thornthwaite W.: The Data Warehouse Lifecycle Toolkit. John Wiley & Sons, 1998.
3. Kimball R.: The Data Warehouse Toolkit. John Wiley & Sons, Inc, 1996.
4. Stokłosa J., Bilski T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych. Wydawnictwo Naukowe PWN, Warszawa 2001.
5. Pipkin D.: Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa. Wydawnictwa Naukowo-Techniczne, Warszawa 2002.
6. Sandhu R., Jajodia S.: Integrity Mechanisms in Database Management Systems. Proc. 13th National Computer Security Conf., 1990.
7. Rosenthal A, Sciore E.: View Security as the Basis for Data Warehouse Security. Proc. of the Int. Workshop on Design and Management of Data Warehouses. Stockholm 2000.
8. Warigon S.: Data Warehouse Control and Security. Association of College and University Auditors LEDGER, Vol. 41, No. 2, 1997. http://www.all.net/books/audit/kits/dw.html.
9. Inmon W. H.: Data Warehouse and Security. www.BillInmon.com.
10. Bell E., La Padula L.: Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, vol. I, The MITRE Corporation, 1973.
11. Bell E., La Padula L.: Secure Computer Systems: A Mathematical Model. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, vol. II, The MITRE Corporation, 1973.
12. Ferraiolo D., Sandhu R., Gavrila S., Kuhn R. Chandramouli R.: Proposed NIST Standard for Role-Based Access Control. ACM Transactions on Information and System Security, Vol. 4, No. 3, 2001.
13. Sandhu R., Samarati P.: Access Control: Principles and Practice. IEEE Communications, vol.32, no.9, 1994.

14. Jajodia S. Sandhu R.: Toward a Multilevel Secure Relational Data Model. ACM SIGMOD Int. Conf. on Managament Data, 1991.
15. Priebe T., Penrul G.: Towards OLAP Security Design – Survey and Research Issues. Proc. of the 3rd ACM International Workshop on Data Warehousing and OLAP (DOLAP 2000). Washington 2000.
16. Pernul G., Tjoa A, Winiwarter W.: Modeling Data Secrecy and Integrity. Uniwersytet w Essen.
17. Thome B.: The High Availability Database Server Cookbook. Oracle Corporation.
18. Babb A. i in.: Maximum Availability Architecture. An Oracle white paper. High Availability System Group. Oracle Corporation, 2003.
19. Lunt T., Fernandez E.: Database Security. SIGMOD RECORD, Vol. 19, No. 4, 1990.
20. MicroStrategy Transactor Installation and Administration Guide. Version 7.2. Third Edition, MicroStrategy Incorporated, 2002.
21. Administrator, Intelligence Server, and Web Administrator Guide. Version 7.2. Third Edition, MicroStrategy Incorporated, 2002.
22. Oracle9i Application Developer's Guide - Fundamentals, Release 2 (9.2), Oracle Corporation, 2002.
23. Oracle Label Security Administrator's Guide, Release 2 (9.2), Oracle Corporation, 2002.
24. Oracle9*i* Security Overview Release 2 (9.2). Oracle Corporation 2002.
25. Elmasri R., Navathe Sh.: Foundamentals of Database Systems. Third Edition. Addison-Wesley, 2000.

Recenzent: Dr inż. Arkadiusz Sochan

Wpłynęło do Redakcji 16 kwietnia 2003 r.

Abstract

The problem of access control in a data warehouse system is very complex. A common requirement is to limit the access of various groups of users to specific portions of information (Fig.1). As the complexity of the requirements grows the implementation of the complete security policy becomes a not trite task. What is more, the introduction of the security subsystem can considerably affect the system performance.

The requirements of the security policy can be expressed in the form of one of the formal models. To make the implementation of possible complex policies simpler the research presents various types of access rules: individual, group and based on some kind of hierarchy.

Different components of the OLAP system may enforce the security mechanisms: a database management system, an OLAP server or an OLAP application. The research concentrates on the means available in rational databases. A lot of less sophisticated policies can be implemented by the use of the system and object database privileges. The more complex requirements need row level access control to be used. The common mechanisms for fine-grained access control are: complex and dynamic views, stored procedures, query modifications and the approach based on sensitivity labels.

Adresy

Marcin GORAWSKI: Politechnika Śląska, Instytut Informatyki, ul. Akademicka 16, 44-101 Gliwice, Polska, m.gorawski@zti.iinf.polsl.gliwice.pl .

Jacek FRĄCZEK: Politechnika Śląska, Instytut Informatyki, ul. Akademicka 16, 44-101 Gliwice, Polska, jacekf@zeus.polsl.gliwice.pl .