ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1996

Seria: INFORMATYKA z. 31 Nr kol. 1348

Bożena MAŁYSIAK

OCHRONA DANYCH W SYSTEMIE MICROSOFT ACCESS 2.0

Streszczenie. W artykule przedstawiono model zabezpieczeń systemu Microsoft Access 2.0 oraz sposoby tworzenia bezpiecznych aplikacji. Pokazano, jak tworzy się konta grupowe i konta pojedynczych użytkowników. Opisano także domyślne konta definiowane przez Microsoft Access. W pracy podano również kilka sposobów zabezpieczania baz danych i aplikacji.

MICROSOFT ACCESS 2.0 SECURITY

Summary. This article presents the Microsoft Access security model and how to create secure applications. It explains how to create group and user accounts. It describes the default accounts, which are defined by Microsoft Access. This paper also introduces several ways of database's and application's protection.

DATEISCHUTZ IM MICROSOFT ACCESS 2.0

Zusammenfassung. Im Artikel wurde ein Modell des MS Access Netschutz dargestellt und in welche weise eine sichere Applikationen eingebildet wurden. Es wurde auch gezeigt wie eines Gruppenkonto oder eines Einzelpersonkonto eröffnet wird. Es wurden dort auch eine MS Access definierde Vermutungskonto eingeschrieben. Im Artikel wurde auch verschiedene Methode Dateisicherstellungen und Applikationenabschirmungen bekanntgegeben.

1. Wprowadzenie

Aplikacje korzystające z bazy danych przetwarzają ogromne ilości informacji. Mają one podstawowe znaczenie dla użytkowników. Konieczność ochrony tych informacji (danych) jest jednym z głównych powodów używania mechanizmów zabezpieczeń w systemach baz danych. W systemie MS Access mechanizmy zabezpieczeń są stosowane do:

- ochrony kodu procedur i funkcji napisanych w języku Access Basic;
- zabezpieczania aplikacji przed dostępem niepowołanych osób, które mogłyby zmienić istniejące w aplikacji obiekty;
- ochrony ważnych danych w aplikacji.

Mechanizmy ochrony umożliwiają między innymi kontrolę zakresu czynności dozwolonych dla użytkowników lub grup użytkowników. Administrator przydziela odpowiednie uprawnienia konkretnemu użytkownikowi lub grupie użytkowników do obiektów aplikacji. Różni użytkownicy mogą mieć różne prawa do tych samych obiektów. Konta grupowe lub pojedynczych użytkowników są tworzone przez administratora systemu lub przez właściciela bazy danych.

2. Zabezpieczenia w systemie Microsoft Access

Informacje o kontach użytkowników i kontach grupowych przechowywane są w systemowej bazie danych. Plik Msacc20.ini określa, jaka baza systemowa jest dołączona do systemu. W systemowej bazie zapamiętane są informacje o nazwach kont grupowych istniejących w bazie danych, nazwach kont wszystkich użytkowników, zaszyfrowane hasła użytkowników, grupy, do których dany użytkownik należy, oraz wewnętrzne chronione identyfikatory (security identifier - SID) użytkowników. Systemowa baza danych wraz ze wszystkimi zawartymi w niej informacjami definiuje grupę roboczą. Domyślną bazą systemową tworzoną przy instalacji pakietu MS Access jest System.mda.

3. Użytkownicy i grupy

Użytkownik może należeć do jednej lub więcej grup. Użytkownicy i grupy współdzielą ten sam obszar na nazwy, dlatego nazwy użytkowników i grup muszą być różne. Każde konto użytkownika i grupowe jest jednoznacznie identyfikowane poprzez identyfikator

ochrony (SID-security identifier). Microsoft Access sprawdza ten identyfikator, gdy decyduje, czy użytkownik ma odpowiednie uprawnienia do wykonania danej operacji na obiekcie. Podczas tworzenia nowego konta użytkownika lub grupy należy wpisać nazwę użytkownika lub grupy oraz identyfikator PID (personal identifier). Nazwa użytkownika i identyfikator PID są wykorzystywane w programie szyfrującym, który generuje identyfikator SID dla danego konta. Identyfikator PID to ciąg alfanumeryczny o zmiennej długości, nieszyfrowany. Identyfikator SID jest to 128-bitowy numer, którego nie można zmienić.

Microsoft Access definiuje dwóch domyślnych użytkowników (*Admin i Guest*) i trzy domyślne grupy (*Admins, Users, Guest*). Identyfikator SID grupy *Admins* jest unikalny dla każdej grupy roboczej. Identyfikatory SID grup *Users* i *Guests* oraz użytkowników *Admin* i *Guest* są tworzone podczas instalacji MS Access i są jednakowe we wszystkich instalacjach MS Access.

3.1. Użytkownik Admin

Użytkownik *Admin* to domyślny użytkownik, należący do grupy *Admins*. Jeżeli podczas ładowania systemu nie zostanie uruchomiona procedura (*logująca*) umożliwiająca wprowadzenie nazwy oraz hasła, każdy użytkownik uruchamiający system jest użytkownikiem *Admin* (bez hasła) i posiada jego uprawnienia. Baza danych, w której użytkownik *Admin* jest właścicielem większości obiektów, jest bazą niechronioną, gdyż każda osoba uruchamiająca system jest użytkownikiem *Admin*. Można to zmienić uaktywniając procedurę logowania użytkowników (poprzez nadanie hasła użytkownikowi *Admin*), tworząc nowe konta użytkowników, nowe konto administratora systemu (o innej nazwie) i usuwając uprawnienia użytkownikowi *Admin*. Proces ochrony bazy danych można ułatwić i usprawnić używając programu Security Wizard.

3.2. Grupa Users

Jest to domyślna grupa, do której wszyscy użytkownicy w systemie muszą należeć. Wszystkie uprawnienia nadane tej grupie są dostępne wszystkim użytkownikom we wszystkich instalacjach MS Access. Domyślnie użytkownicy grupy *Users* mają wszystkie uprawnienia dostępu do nowo tworzonych obiektów. W celu ochrony bazy danych należy usunąć uprawnienia grupie *Users*.

3.3. Grupa Admins

Jest to domyślna grupa, tworzona podczas instalacji MS Access. Wszyscy członkowie tej grupy to administratorzy grupy roboczej. Mają oni prawo nadawania uprawnień, zmiany lub usuwania hasła użytkownikom. Uprawnień grupy *Admins* nie da się zmienić. W grupie roboczej powinien istnieć tylko jeden administrator. W każdym systemie potrzebny jest użytkownik sprawujący kontrolę nad operacjami wykonywanymi przez pozostałych użytkowników. Posiada on uprawnienia usuwania skutków niepożądanych operacji.

Program Administrator Grupy Roboczej (Workgroup Administrator) wymaga podania nazwy instytucji, nazwy użytkownika oraz identyfikatora grupy roboczej. Używając tych ciągów i kodując je tworzy identyfikator SID grupy *Admins*. Zapamiętując te dane można w przypadku uszkodzenia systemu bazy danych, używając programu Administrator Grupy Roboczej (Workgroup Administrator) wygenerować na ich podstawie nową grupę *Admins* z identycznym identyfikatorem SID. Członkowie odtworzonej grupy *Admins* będą mieli te same prawa do wszystkich obiektów, które były stworzone, gdy był używany stary system bazy danych.

3.4. Użytkownik Guest i grupa Guests

Jest to domyślny użytkownik i domyślna grupa tworzone podczas instalacji MS Access. W wersji MS Access 2.0 użytkownik *Guest* i grupa *Guests* domyślnie nie mają żadnych uprawnień do nowo tworzonych obiektów.

4. Przykłady różnych sposobów zabezpieczania baz danych przez MS Access

Istnieją dwa sposoby zmiany właściciela obiektu (dotyczy to przypadku, gdy właścicielem obiektów jest użytkownik *Admin*):

- wybór z menu opcji *Security* oraz z podmenu opcji *Change Owner*;
- odtworzenie obiektu poprzez import lub eksport obiektu do nowej bazy. Można to zrobić wykorzystując komendę *Import Database* znajdującą się w opcji *Menu/Add-ins* menu lub pozwolić, by zrobił to program Security Wizard. Aby odtworzyć obiekt, trzeba posiadać uprawnienia do odczytu obiektu.

4.1. Ochrona dostępu do projektu tabeli przed niepowołanymi użytkownikami

Aby uniemożliwić użytkownikom dostęp do widoku projektu tabeli (zapytania), można wykorzystać właściwość zapytania *run permission*. Są dwa możliwe ustawienia tej właściwości: "*User's*" lub "*Owner's*". Jeżeli wybierze się "*User's*" (opcja domyślna), użytkownik nie zauważy żadnej różnicy w działaniu zapytania. Jeśli ustawiona zostanie opcja "*Owner's*", tylko właściciel zapytania będzie mógł je uruchomić i uzyskać dostęp do tabeli (lub zapytania), w celu jego wykonania. Nawet członkowie grupy *Admins* nie mogą modyfikować zapytania stworzonego przez innego użytkownika, gdy właściwość *run permission* tego zapytania ustawiona jest na "*Owner's*".

W celu zabezpieczenia dostępu do widoku projektu tabeli danych należy:

- usunąć wszystkie uprawnienia użytkownikom i grupom do interesującej nas tabeli lub zapytania (np.: Personel);
- zbudować nowe zapytanie (np.: MójPersonel), zawierające wszystkie pola interesującej nas tabeli;
- upewnić się, czy nasz użytkownik lub grupa, do której należy, jest właścicielem zapytania, jeśli nie, to należy zmienić właściciela zapytania na grupę, która będzie miała prawa do modyfikowania i zmiany zapytania MójPersonel;
- ustawić właściwość *run permission* na "*Owner's*";
- dodać użytkownikom lub grupom, które powinny modyfikować dane, ale nie powinny mieć dostępu do projektu tabeli, uprawnienia do odczytu projektu oraz do odczytu, modyfikowania, kasowania i wstawiania danych;
- zapewnić, by formatki ekranowe i raporty, bazujące na danych z tabeli Personel, korzystały z danych zapytania MójPersonel.

Użytkownicy będą mogli teraz uaktualniać dane w chronionej tabeli poprzez formatki oparte na zapytaniu, nie będą jednak mogli zobaczyć projektu tabeli. Próba obejrzenia projektu tabeli zakończy się komunikatem "You don't have permissions to view Personel".

4.2. Szyfrowanie

Szyfrowanie stosowane jest w celu ochrony danych przed odczytem przez niepowołane osoby za pomocą np.: disk editor'a. Jeśli plik .mdb nie jest szyfrowany, niepowołana osoba może odczytać identyfikator SID właściciela lub grupy *Admins* i włamać się do bazy. Dlatego jeśli baza powinna być chroniona, należy ją szyfrować. Tylko członkowie grupy *Admins* oraz właściciel bazy mogą kodować bądź dekodować bazę. Kodowanie bazy danych jest także częścią procesu zabezpieczania bazy przez program Security Wizard.

4.3. Instalacja programu Security Wizard

Wykorzystanie narzędzia, jakim jest MS Access Security Wizard, jest najprostszym sposobem ochrony bazy danych. Security Wizard pozwala wybrać, które rodzaje obiektów powinny zostać objęte ochroną.

W celu zainstalowania programu Security Wizard należy:

- z opcji *File* w menu głównym wybrać opcję *Add-Ins*, a następnie opcję *Add-in Manager*. Na ekranie pojawi się okno *Add-in Manager* (menadżer dodatków);
- wybrać przycisk *Add New* (dodaj nowy), na ekranie pojawi się okno z plikami z rozszerzeniem .mda;
- wybrać plik SECURE20.MDA. *Add-In manager* skopiuje wybrany plik do kartoteki, w której zainstalowany jest MS Access i wprowadzi konieczne zmiany do pliku MSACC20.INI.

Po ponownym uruchomieniu systemu MS Access, Security Wizard jest widoczny jako jedna z opcji podmenu *File/Add-ins*.

Aby zabezpieczyć bazę danych, używając narzędzia Security Wizard należy uruchomić system nie jako użytkownik *Admin* lub *Guest*, ale jako inny użytkownik mający pełne uprawnienia w bazie danych. Następnie należy otworzyć wybraną bazę danych i uruchomić program Security Wizard. Utworzy on nową chronioną kopię bazy danych, pozostawiając oryginalną bazę niezmodyfikowaną.

4.4. Zabezpieczenie istniejącej bazy przy użyciu narzędzia Security Wizard

Załóżmy, że w systemie istnieje przykładowa baza danych gabinet.mdb, której wszystkie obiekty zostały stworzone przez użytkownika *Admin*. Chcąc zabezpieczyć tę bazę należy:

- za pomocą programu Administrator Grupy Roboczej (Workgroup Administrator) stworzyć grupę roboczą (zapisać i schować w bezpiecznym miejscu nazwę, nazwę instytucji oraz identyfikator grupy, by zachować możliwość odtworzenia grupy w przypadku awarii);
- utworzyć nowego użytkownika i dołączyć go do grupy *Admins*;
- nadać hasło użytkownikowi *Admin* (wejść do opcji *Security/Change Password*), by aktywować procedurę logowania;
- zainstalować program Security Wizard, jeśli jeszcze nie został zainstalowany;
- "zamknąć" MS Access i ponownie uruchomić, wchodząc do systemu jako nowo utworzony użytkownik;
- otworzyć bazę gabinet.mdb;

- uruchomić program Security Wizard, wybierając komendę *Security Wizard* z podmenu *File/Add-ins*;
- po tych czynnościach wybrać typy obiektów objętych ochroną. Security Wizard utworzy nową, szyfrowaną bazę danych, wyeksportuje wszystkie obiekty z bieżącej bazy danych i zabezpieczy je przez odebranie uprawnień do wszystkich chronionych obiektów wszystkim użytkownikom, z wyjątkiem użytkownika (tego, który uruchomił program Security Wizard);
- utworzyć w chronionej bazie własne konta użytkowników i grup.

Tak utworzona baza jest chroniona, tylko użytkownicy i grupy, którym uprawnienia nadała osoba zabezpieczajaca bazę, mają w niej prawa, inni nie (poza członkami grupy *Admins*).

4.5. Likwidacja zabezpieczeń chronionej bazy danych

Załóżmy, że w systemie istnieje zabezpieczona baza danych, której właścicielem jest użytkownik uruchamiający program Security Wizard. Posiada on prawa zmiany uprawnień użytkownikom. Może udostępnić bazę danych wszystkim użytkownikom, korzystając z tego, że identyfikatory SID użytkownika *Admin* i grupy *Users* są jednakowe we wszystkich instalacjach MS Access. Dając pełne uprawnienia użytkownikowi *Admin* i grupie *Users* pozbawi się bazę danych jakiejkolwiek ochrony.

W celu pozbawienia ochrony bazy danych należy wykonać więc następujące czynności:

- zrobić kopię chronionej bazy danych;
- uruchomić ponownie MS Access, wchodząc jako użytkownik mający prawa administratora;
- otworzyć kopię bazy danych;
- nadać grupie *Users* pełne prawa do wszystkich obiektów bazy danych;
- nadać użytkownikowi *Admin* pełne prawa do wszystkich obiektów bazy danych.

4.6. Ochrona aplikacji z umieszczonym oddzielnie kodem i danymi

Należy założyć, że w systemie istnieje aplikacja, której dane umieszczone są w pliku dane.mdb, a kod, formatki i raporty w pliku gabinet.mdb. Chcąc zabezpieczyć oba pliki, by móc je dystrybuować klientom, należy:

- dla obu plików powtórzyć kroki realizowane w celu ochrony bazy za pomocą programu Security Wizard;
- nadać użytkownikom uprawnienia odczytu i zapisu danych w bazie dane.mdb. Można nie nadawać praw, opuścić plik dane.mdb i tak skonfigurować gabinet.mdb, by

wszystkie odczyty i modyfikacje były zapamiętywane poprzez wykorzystanie zapytań z ustawioną opcją *Run Permission* na *Owner Permission* bezpośrednio w pliku gabinet.mdb;

- sprawdzić, czy użytkownicy mają prawa *Run/Open* (uruchamiania i otwierania) w pliku dane.mdb;
- dodać uprawnienia *Modify Design* użytkownikom do dołączonych tabel w bazie gabinet.mdb.

Po wykonaniu tych czynności baza danych będzie chroniona. Użytkownicy będą mogli wykonywać tylko te czynności, do jakich mają uprawnienia, a nie będą mogli oglądać i modyfikować projektu tabel.

Przy pierwszej instalacji aplikacji uruchomi się *Attachment Manager* w celu podania ścieżek do dołączanych tabel znajdujących się w bazie dane.mdb. Nadanie uprawnień *Modify Design* do dołączonych tabel w bazie gabinet.mdb umożliwi użytkownikom wprowadzenie poprawnej ścieżki dostępu do bazy dane.mdb w przypadku zmiany jej położenia na dysku, ale nadal nie będą oni mogli modyfikować projektu tabel.

4.7. Ochrona bazy danych bez potrzeby logowania użytkowników

Jeśli chce się zabezpieczyć pewne obiekty w bazie danych, lecz nie jest potrzebne nadawanie różnych praw różnym użytkownikom, można zabezpieczyć bazę danych bez uruchamiania procedury logowania się. W tym celu należy:

- powtórzyć kroki potrzebne do uruchomienia programu Security Wizard;
- uruchomić system jako użytkownik, będący członkiem grupy *Admins* (użytkownikowi Admin nadać takie uprawnienia, jakie są potrzebne użytkownikom);
- usunąć użytkownika *Admin* z grupy *Admins*;
- wyczyścić hasło użytkownikowi *Admin*.

Wykonanie wyżej podanych czynności spowoduje, że każda osoba uruchamiająca system będzie domyślnie użytkownikiem *Admin*, z takimi prawami, jakie będzie on posiadał.

Wystąpi tu jednak problem, jak uruchomić system jako administrator (właściciel bazy). Aby to zrobić, należy w *Program Manager* wybrać ikonę Microsoft Access i w linii poleceń dopisać opcje */User /Pwd*, podając nazwę użytkownika oraz jego hasło. Uruchamiając MS Access za pomocą tej ikony wejdzie się do systemu jako określony użytkownik.

Uwaga! Jeżeli operacja taka nie będzie już potrzebna, należy skasować wprowadzone dane o użytkowniku (zmazując wpisane w linii poleceń hasło i nazwę użytkownika), gdyż mogą stać się one źródłem informacji dla niepowołanych osób.

4.8. Tworzenie grupy roboczej, zawierającej konto administratora mogącego tworzyć użytkowników i dodawać ich do odpowiednich grup, lecz nie mającego praw modyfikowania obiektów bazy danych

Należy założyć, że w systemie isnieje wielodostępna aplikacja, w której poszczególni użytkownicy mają różne prawa do różnych obiektów bazy danych, ponieważ mają różne obowiązki. Autor systemu nie jest w stanie przewidzieć wszystkich użytkowników, dlatego tworzy konto administratora, który będzie mógł tworzyć konta użytkownikom i przydzielać ich do poszczególnych grup.

Aby utworzyć konto administratora, należy:

- używając programu Administrator Grupy Roboczej (Workgroup Administrator) należy stworzyć grupę roboczą z przykładową bazą systemową główna.mda;
- uruchomić w opisany wcześniej sposób program Security Wizard i zabezpieczyć bazę danych;
- stworzyć konta grupowe, które odpowiadałyby dostępnym uprawnieniom użytkowników (zapisać dokładne informacje o tych grupach, tzn. nazwę i identyfikator PID);
- dołączyć do grup odpowiednie uprawnienia, upewniając się, czy nie dodano uprawnień administratora;
- użyć ponownie programu Workgroup Administrator w celu stworzenia grupy roboczej z systemową bazą danych użytk.mda dystrybuowaną klientom wraz z aplikacją;
- dołączyć do systemu systemową bazę użytk.mda (za pomocą Workgroup Administrator);
- utworzyć na podstawie zapisanych informacji dokładnie te same grupy, które są w pliku główny.mda;
- stworzyć konto administratora, dodać go do grupy *Admins*;
- usunąć użytkownika Admin z grupy Admins i nadać mu hasło w celu uruchomienia procedury logowania;
- dystrybuować plik użytk.mda z aplikacją.

Po wykonaniu powyższych czynności administrator może tworzyć konta użytkownikom, dodawać użytkowników do odpowiednich wcześniej stworzonych grup. Poszczególne grupy istniejące w systemowej bazie użytk.mda mają takie same uprawnienia do obiektów jak grupy w systemowej bazie główny.mda, ponieważ mają jednakowy identyfikator SID. Natomiast identyfikator SID grupy *Admins* jest inny dla każdej grupy roboczej (jest generowany na podstawie informacji wprowadzonych w programie Workgroup Administrator o każdej grupie roboczej, a informacje te są różne). Nowo utworzony administrator ma prawo tworzenia użytkowników, natomiast nie ma prawa nadawania sobie uprawnień do obiektów, nie może

modyfikować obiektów, jeśli nie ma do tego praw. Oznacza to, że baza jest zabezpieczona przed dokonywaniem niepowołanych zmian, jednocześnie jeśli uruchomi się tę bazę z dołączoną bazą systemową główny.mda, to użytkownik, który jest właścicielem chronionej bazy (tzn. który zabezpieczył bazę używając programu Security Wizard), będzie mógł dokonywać niezbędnych modyfikacji w bazie danych.

5. Wpływ zabezpieczeń na czas dostępu do danych

Chcąc znaleźć odpowiedź na to, jaki wpływ mają zastosowane zabezpieczenia na czas przetwarzania danych, przeprowadzono prosty test. Na potrzeby tego testu stworzono aplikację, korzystającą z tabel, zawierających duże ilości danych (od kilku do kilkunastu tysięcy rekordów), skonstruowano zapytania wybierające: jedno proste, odwołujące się do jednej tabeli, oraz drugie złożone, przetwarzające dane z wielu tabel, wykorzystujące grupowanie. Stworzono także zapytanie modyfikujące dane.

Zapytanie pierwsze: Podać dane studentów - mężczyzn wydziału Automatyki, Elektroniki i Informatyki, kierunku Informatyka, semestru drugiego, zamieszkałych w Gliwicach.

```
SELECT DISTINCTROW STUDENDZ.NAZWISKO, STUDENDZ.IMIE, STUDENDZ.DATAURODZ,
    STUDENDZ.MIASTO, STUDENDZ.WYDZIAL, STUDENDZ.KIERUNEK, STUDENDZ.SEMESTR,
    STUDENDZ.PLEC FROM STUDENDZ
WHERE ((STUDENDZ.MIASTO='Gliwice') AND (STUDENDZ.WYDZIAL='RAU') AND
(STUDENDZ.KIERUNEK='I') AND (STUDENDZ.SEMESTR='02') AND (STUDENDZ.PLEC='M'));
```

Zapytanie drugie: Dla każdego studenta kierunku Informatyka podać informacje (data, semestr, przedmiot, ocena) dotyczące wszystkich egzaminów, jakie do tej pory student zdawał w pierwszym terminie.

```
SELECT DISTINCTROW STUDENDZ.KIERUNEK, STUDENDZ.SEMESTR, STUDENDZ.ALBUM,
    STUDENDZ.NAZWISKO, STUDENDZ.IMIE, EGZAMIDZ.SEMESTR, EGZAMIDZ.TERMIN,
    PRZEDMDZ.NAZWA, EGZAMIDZ.DATA, EGZAMIDZ.OCENA
FROM (STUDENDZ INNER JOIN EGZAMIDZ ON STUDENDZ.ALBUM = EGZAMIDZ.ALBUM) INNER
    JOIN PRZEDMDZ ON EGZAMIDZ.PRZEDMIOT = PRZEDMDZ.PRZEDMIOT
GROUP BY STUDENDZ.KIERUNEK, STUDENDZ.SEMESTR, STUDENDZ.ALBUM,
    STUDENDZ.NAZWISKO, STUDENDZ.IMIE, EGZAMIDZ.SEMESTR, EGZAMIDZ.TERMIN,
    PRZEDMDZ.NAZWA, EGZAMIDZ.DATA, EGZAMIDZ.OCENA, EGZAMIDZ.PRZEDMIOT
HAVING ((STUDENDZ.KIERUNEK='I') AND (STUDENDZ.SEMESTR='02') AND
    (EGZAMIDZ.TERMIN='1'));
```

Zapytanie trzecie (modyfikujące): Każdemu studentowi, pobierającemu stypendium, zwiększyć podstawę stypendium o 100 zł.

```
UPDATE DISTINCTROW STUDENDZ INNER JOIN STYPENDZ ON
STUDENDZ.ALBUM = STYPENDZ.ALBUM SET STYPENDZ.STAWKA = [STAWKA]+"1000";
```

Korzystając z programu Security Wizard stworzono chronioną kopię aplikacji. Przeprowadzone badania polegały na wywoływaniu zapytań w chronionej i niechronionej bazie danych. Pomiaru czasu przetwarzania danych dokonano za pomocą stworzonego na potrzeby testów makra, podającego czas przed wywołaniem zapytania i po jego wywołaniu.

Wywołując proste zapytanie w obu bazach otrzymano jednakowe wyniki (tzn. czas dostępu do danych był taki sam i wynosił 2 sekundy).

Przy wywołaniu zapytania przetwarzającego dane z kilku tabel czas dostępu do danych w chronionej bazie był dłuższy (w niechronionej 18 sekund, w chronionej 21 sekund).

Przy wywołaniu zapytania modyfikującego dane (ok. 22000 rekordów) czas przetwarzania zapytania i dokonywania zmian w tabeli w chronionej bazie był dłuższy (w niechronionej 75 sekund, w chronionej 81 sekund).

W przypadku przetwarzania danych w chronionej bazie czas dostępu do danych jest powiększony o czas rozkodowywania zaszyfrowanej informacji. Największa różnica w czasie dostępu do danych wystąpiła w wywołaniu zapytania modyfikującego dane w tabeli, wydłużenie to spowodowane jest tym, że pierwsze należy rozkodować informacje w tabeli, zmodyfikować odpowiednie wartości i zakodować ponownie. W przypadku prostego zapytania i przetwarzania niewielkiej ilości danych różnice w czasie dostępu do danych w obu bazach są niezauważalne. Różnice w czasie dostępu do danych, gdy przetwarzane jest złożone zapytanie, są rzędu kilku procent, warto więc chronić swoje aplikacje.

6. Wykorzystanie programu Security Wizard w ochronie pliku z danymi

Obecnie często tworzy się aplikacje w różnych językach programowania, pobierające dane z baz danych utworzonych w Microsoft Access (pliki *.mdb). Dane przechowywane w tych plikach nie są chronione z poziomu systemu operacyjnego, czyli są dostępne dla każdego użytkownika.

Można na przykład za pomocą programu Norton Commander podejrzeć zawartość pliku bazy danych (*.mdb), gdyż informacje w bazie niechronionej są podane w sposób jawny i można odczytać zarówno nazwy pól, jak i dane zawarte w tabelach. Można dane te także modyfikować, używając oprogramowania narzędziowego zapisującego dane bezpośrednio na dysku, na przykład programu Dysk Edytor. Po zabezpieczeniu bazy programem Security Wizard informacje da się co prawda odczytać z poziomu systemu operacyjnego, lecz ich interpretacja jest niemożliwa ze względu na zastosowane algorytmy szyfrujące (dane są zakodowane).

Kolejnym słabym ogniwem ochrony plików baz danych Microsoft Access jest możliwość bezpośredniego dostępu do nich za pomocą mechanizmu ODBC systemu Windows. Można w ten sposób wykorzystać na przykład program Microsoft Query, dołączany do pakietu Microsoft Office i po skonfigurowaniu źródła danych w oprogramowaniu administracyjnym ODBC połączyć się z odpowiednią bazą danych i uzyskać pełny dostęp do danych. Dane nie będą chronione nawet po stworzeniu nowej grupy systemowej (plik *.mda) i stworzeniu grup użytkowników oraz nadaniu im odpowiednich uprawnień, gdyż po podłączeniu się za pomocą mechanizmu ODBC następuje sprawdzenie poprawności nazwy i hasła użytkownika, ale tylko w odniesiemiu do uzyskania dostępu do programu Microsoft Access. Nie są sprawdzane uprawnienia użytkowników w odniesieniu do bazy danych i jej obiektów. Dlatego znając nazwę użytkownika i jego hasło, za pomocą nechanizmu ODBC można uzyskać dostęp do wszystkich informacji zawartych w bazie danych bez względu na uprawnienia, jakie się posiada.

Sposobem na zabezpieczenie danych przed takim sposobem dostępu przez osoby nieupoważnione jest użycie programu Security Wizard (utworzenie chronionej kopii bazy danych). Program Security Wizard szyfruje dane, łączy prawa dostępu bezpośrednio z plikiem, co powoduje, że przy każdej próbie dostępu do bazy weryfikowane są uprawnienia użytkownika.

Zaszyfrowanie bazy i zapisanie uprawnień użytkowników w pliku razem z danymi oraz ich weryfikacja przy każdej próbie dostępu za pomocą programu Security Wizard są dobrym i wystarczającym sposobem na ochronę danych w prostych systemach baz danych opartych na systemie Microsoft Access lub tworzonych w innych narzędziach z użyciem plików Microsoft Access jako miejsc przechowywania danych.

7. Zakończenie

Przedstawione w artykule mechanizmy ochrony danych w systemie MS Access zostały zastosowane w aplikacji "Gabinet stomatologiczny", wspomagającej pracę poradni stomatologicznej.

Stosując program Security Wizard, tworząc własną bazę systemową, zawierającą informacje o utworzonych kontach grupowych i kontach pojedynczych użytkowników oraz odbierając uprawnienia użytkownikowi Admin i tworząc własne konto administratora systemu uzyskano pełną ochronę danych i kodu programu.

LITERATURA

[1] Podręcznik użytkownika. Microsoft Corporation, 1994.
[2] Tworzenie aplikacji. Microsoft Corporation, 1994.
[3] Date C. J.: Wprowadzenie do baz danych. WNT, Warszawa 1981.
[4] Delobel C., Adiba M.: Relacyjne bazy danych. WNT, Warszawa 1989.
[5] Mee M.: Programming Access Security. Microsoft Tex. Ed., 1995.
[6] Pankowski T.: Podstawy baz danych. WNT, Warszawa 1992.
[7] Tsichritzis D., S., Lochovsky F., H.: Modele danych. WNT, Warszawa 1990.
[8] Snelling G.: Microsoft Access 2.0 Security, Microsoft Tech. Ed., 1995, part 2.
[9] Ullman J.D.: Systemy baz danych. WNT, Warszawa 1988.

Recenzent: Dr inż. Maciej Bargielski

Wpłynęło do Redakcji 4 marca 1996 r.

Abstract

Presented Microsoft Access security model is used to protect the intellectual property of developer's code in Microsoft Access applications, to prevent users of database applications from inadvertently breaking them by changing code or objects on which the application depends and to protect sensitive data in a database.

The purpose of this article is to explain the Microsoft Access security model to potential administrators and users of secured applications. It describes how to turn security "on", and how permissions checking works. This paper presents how to create user and group accounts.

In Microsoft Access, users and groups accounts are designed and created by the database's owner or the system administrator. Next, the database's owner or system administrator grant permissions to users and groups on specific objects. Different users can have different permissions on the same objects (user-level security). Each user and group is identified to Microsoft Access by its own unique SID (security identifier). The SID is a machine-generated, non-readable binary string that uniquely identifies the user or group. The user name and personal identifier are fed to encryption program that generates the SID for that account.

Microsoft Access defines two default users: Admin and Guest, and three default groups: Admins, Users and Guests. The key thing to remember about the default accounts is that the

SID of the Admins group account is unique across workgroups, but the sid's of the other four default account: Admin user, Users group, Guest user and Guests group are identical across all installations of Microsoft Access. Thus permissions assigned to the Admins group are secure, but permissions assigned to any of the other accounts are available to anyone with a copy of Microsoft Access.

This article finally presents program the Access Security Wizard as the easiest way to secure databases. It allows to choose which object types to secure - Tables, Queries, Forms, Reports, Macros or Modules. The Security Wizard creates a new secured copy of the database. It leaves the original copy unmodified.