ОСНОВНИ ПРОБЛЕМИ НА ЗАЩИТА НА ИНФОРМАЦИЯТА В БАЗИ ДАННИ

проф. дтн. Димо Димитров Арнаудов
Технически Университет- София

инж. Константин Николов Колев
фирма „Колбис“

инж. Юлия Евстатиева Русева
„Аркус“ ООД

Nowadays, with the increasingly widespread use of different types of computer networks the question about the realization and application of new and more complicated methods for data protection is particularly important. In this article different aspects in data protection are considered. The stress is on one of the most important problems concerning t he database security: the inference control. The problem about the inference, i.e., the opportunity of obtaining confidential information by means of processing the accessible data occurs when the security classes do not correspond to the defined structure in the database. Also the database protection requirements are taken into consideration and the essential stages in the realization of reliable database protection are defined.

Понастоящем с повсеместното разпространение на различни видове мрежи от компютри, особено актуален е въпросът с проектирането и прилагането на нови и по-усъвършенствувани методи на защита на информацията в бази данни. Изборът на правилна стратегия на защита на информацията в БД е от решаващо значение. Защитата на информацията в БД може да бъде разгледана главно в два аспекта /1/:

- защита от несанкциониран достъп;
- защита от индиректен достъп.

За осигуряване на защита от несанкциониран достъп е необходимо най-напред да се извърши класифициране на информацията на отделни нива според степента й на секретност и точно конкретизиране на потребителите, които имат достъп до отделните нива. По такъв начин се избягва нежелан трансфер на информация до неупълномощени потребители. За да се осигури възможност за контрол и за извършване на проверки трябва всички достъпи до защитените данни и извършените операции над тях да се запишат в специален файл /контролен журнал/.

Управлението на достъпа до информацията в БД се осъществява чрез система „контрол на достъпа". Тя осигурява всички достъпи на субектите /потребители, процеси/ до обектите /програми, данни/ за извършване на операциите четене, запис, обновяване и изтриване на информацията. Достъпът, който се определя за различните субекти може да се зададе като комбинация от следните условия:

- частично четене - субектът може да прочете само определена част от данните, като не може да ги променя;
- пълно четене - субектът може да прочете цялата БД, но не може да я променя;
- вмъкване на записи от определен тип - субектът може да вмъква записи от даден тип, но не може да ги променя;
- вмъкване на записи от всички типове - субектът може да вмъква записи от всички типове, но не може да ги променя;
- изтриване на записи от определен тип;
- изтриване на записи от всички типове;
- обновяване на записи от определен тип;
- обновяване на записи от всички типове;

Системата „контрол на достъпа" включва субекти /потребители, процеси/, които имат достъп до обекти /данни, програми/ за операциите четене, запис и обработка на информацията. Функционално тя се състои от две части:

- файл или таблица, където са фиксирани различните потребители / така наречените профили на потребителите / и правилата на достъп;

- файл с процедури за контрол, които проверяват заявките за достъп и техните права. След проверката достъпът може да бъде разрешен, отказан или модифициран.

Таблицата с правилата за достъп е израз на избраната от ръководството на организацията стратегия за защита. За да се избере подходящ метод на защита трябва да се вземе предвид предназначението на БД. Обикновено при БД за университети или изследователски центрове, които не се нуждаят от строга защита се избира методът на максимална привилегия /"maximum availability"/, съгласно който субектите имат достъп до максимално количество информация в БД. При изграждане на БД в организации, които се нуждаят от строга защита, например в банки, трябва да се избере метода на минимална привилегия /"need-to-know" policy/, при който субектите в системата използват минимално количество информация, нужно за тяхната дейност. Недостатък на този метод е, че може да доведе до безполезни ограничения на субектите.

Изборът на стратегия на защита на информацията в БД включва и определянето на типа на системата за контрол на достъпа. Системата за контрол на достъпа може да бъде от затворен или отворен тип. В затворените системи /closed system/ само изрично съществуващите достъпи в таблицата с правилата за достъп са разрешени. Това означава, че за всеки субект съществуват правила, определящи привилегиите за достъп на даден субект към обектите в системата. В отворените системи /"open system"/ за всеки субект съществуват правила, определящи привилегиите, които субекта не притежава за обектите в системата. Това ще бъдат единствените права, които ще бъдат отказани.

Отворените и затворените системи са взаимно изключващи се. Изборът на едната или другата система зависи от характеристиките и изискванията на БД, от организационни аспекти и т. н. Затворените системи изискват използването на метода на минимална привилегия /"need-to-know"policy/, докато отворените системи - метода на максимална привилегия /"maximum availability"/. Защитата е по-висока в затворените системи, тъй като в отворените системи грешки, например като липсващо правило, могат да доведат до несанкциониран достъп. Предимство на затворените системи е, че процедурата за обработка на правилата за достъп е по-проста.

Друг основен проблем при осъществяване на защитата на информацията в БД е защитата от индиректен достъп /3,4/. Индиректен достъп означава възможността за получаване на поверителна информация

посредством общодостъпни данни. Типичен пример са корелационните данни, където общодостъпната информация X е семантично свързана с поверителната информация Y.Следователно информацията, отнасяща се за Y може да бъде получена чрез четене на X. Друг класически пример е така наречения достъп чрез точката на свързване /join inference(2)/, при който чрез обходни пътища се получава достъп до поверителната информация. В този случай е необходимо да се анализират възможните обходни пътища. Друга страна на проблема е защитата от индиректен достъп на статистически БД, които включват дедукция на данните. Основните положения на защитата на статистическите БД са представени в /1/. При релационни БД проблемът с индиректния достъп се появява ако класовете на защита на данните не съответстват на дадената структура на БД. Например нека да преобразуваме БД с определена „стара" структура и с дефинирани класове на защита на информацията в друг „нов" тип структура. В този случай ако класовете на защита на информацията са несъвместими с „новия" тип структура, възниква проблема с индиректния достъп.

Най-добрият метод за защита на релационни БД е използването на модела на решетъчна структура /1/.
Съществуват различни средства за защита на информацията в БД. Най-общо към тях могат да бъдат формулирани следните изисквания:

- осигуряване на семантична цялост на данните. Това изискване цели да се поддържа логическа свързаност на модифицираните данни чрез контрол на стойностите на данните в дадения обхват;
- осигуряване на работна цялост на данните, което цели да не се нарушава логическата структура на данните.

Могат да се дефинират следните основни етапи при проектирането на надеждна защита на информацията в БД:

- организационен етап, при който се регламентират функциите на администратора на БД по осигуряване на защитата, извършва се класификация на информацията от гледна точка на секретността й, определят се организационни мерки за контрола на достъпа до информацията. Определянето на идентификаторите и паролите на потребителите е от голямо значение, от чиято секретност зависи до голяма степен защитата на информацията.
- избор на система за контрол на достъпа, която осъществява управлението на достъпа до информацията в БД. На този етап се избира типа на системата и типа на управление /централизирано, децентрализирано или йерархично децентрализирано/.
- избор на метод за защита от индиректен достъп до информацията в БД. На този етап трябва да се сравнят различните методи за защита

по следните критерии: ниво на защита, качество /загуба на информацията/, точност, съвместимост и разходи за реализацията.

В заключение може да се изтъкне, че усложняването на системата за защита води до увеличаване на разходите за реализирането й. Поради това е необходимо да се намери оптимален вариант по отношение на сложността на системата и разходите, необходими за реализирането й.

ЛИТЕРАТУРА

1. Castano S., Fugini M., Martella G., Samarati P., Database Security, Addison Wesley,1994.
2. Lin T.Y., Inference Secure Multilevel Databases,IFIP Transactions, Database Security,VI Status & Prospects,edited by C.E.Landwehr,North Holland,1993.
3. Hinke T.H., Inference Aggregation Detection in Databse Management Systems, Proceedings of the 1988 IEEE Symposium on Security & Privacy,April 1988.
4. Lunt T.F., Aggregation & Inference : Facts & Fallacies,Proceedings of 1989 IEEE Symposium on Security & Privacy,1989.