Література: ***1.*** *Закон України "Про метрологію та метрологічну діяльність"від 15 червня 2004 р., № 1765-IV//Відомості Верховної Ради України,2004, №37, ст.449.* ***2.*** *Наказ Держспоживстандарту України "Про затвердження Правил уповноваження та атестація у державній метрологічній системі"від 29 березня 2005 р., № 71// Збірник нормативно - правових актів України та організаційно-методичних документів з питань метрології, 2005, №5, ст.65.* ***3.*** *ДСТУ ISO/TR 10013-2003. Настанови з розроблення документації системи управління якістю.* ***4****. ДСТУ ISO/IEC 17025:2006 Загальні вимоги до компетентності вимірювальних та калібрувальних лабораторій.* ***5****. ДСТУ 1.5-2003. Правила побудови, викладення , оформлення та вимоги змісту нормативних документів.*

УДК 004.056.53

РЕОРГАНИЗАЦИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ БАЗ ДАННЫХ ПО РЕЗУЛЬТАТАМ АУДИТА

Михаил Коломыцев, Светлана Носок

Национальный технический университет Украины «Киевский политехнический институт»

Анотація: **Одним із головних джерел загроз безпеці в інформаційних системах взагалі, і базах даних зокрема, є інсайдери [1]. Причинами уразливості баз даних (БД) до інсайдерських атак є помилки формування політики безпеки БД. Часто положення політики безпеки формулюються як реакція на поточні потреби, які з часом перестають бути актуальними, а то і зовсім, зайвими. У статті пропонується підхід до коректування політики безпеки на основі профілів користувачів.**

Summary: **One of the main sources of security threads in information systems in common and databases as a part, is insiders [1]. Mistakes connected with security policy development are the main purposes of database vulnarabilities related to the insiders' attacs. In most cases security policy is based on information that becomes useless with the time. In this article a new method for correction of security policy based on users' profiles was proposed.**

Ключові слова: **Політика безпеки, інсайдер, інсайдерська атака, аудит, бази даних.**

I Определения

Технические положения политики безопасности формулируются в виде ограничения в настройках безопасности системы. Применительно к базам данных к числу объектов политики безопасности относятся:

- множество учетных записей пользователей $\mathbf{U_{db}}$,
- множество роли БД $\mathbf{R_{db}}$,
- множество объектов $\mathbf{DB_{obj}}$: таблицы, представления, хранимые процедуры,
- множество учетных записей пользователей в прикладных программах $\mathbf{U_a}$, поскольку пользователи, как правило, получают доступ к БД через программный интерфейс.

Политика безопасности определяет круг пользователей БД и учетные записи для них в прикладных программах, соответствующие им учетные записи БД ($\mathbf{U_a \rightarrow U_{db}}$), перечень ролей, которые могут быть активизированы учетной записью ($\mathbf{U_{db} \rightarrow R_{db}}$), предоставленные ролям привилегии доступа к объектам БД ($\mathbf{R_{db} \rightarrow DB_{obj}}$). Совокупность указанных отображений образует *путь доступа* пользователя к объектам БД (рис. 1). Политика безопасности должна устанавливать согласованные ограничения на всех участках пути доступа, предоставляя минимально необходимый набор привилегий.

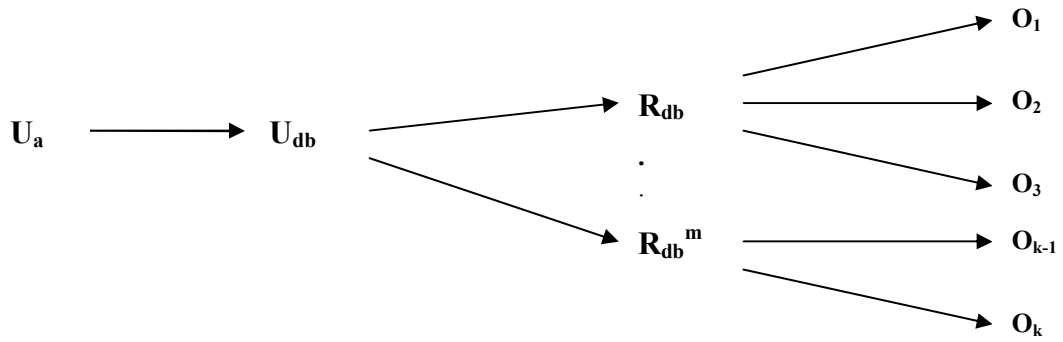

Рисунок 1 – Путь доступа пользователя прикладной программы к объектам БД

Неточности, неполнота описания, динамический характер изменения условий функционирования БД – эти и другие факторы приводят к тому, что система безопасности перестает отвечать предъявляемым к

ней требованиям. Ограничения, установленные на различных участках пути доступа, могут оказаться несогласованными, а сама БД становится уязвимой к атакам, в первую очередь к инсайдерским. Традиционные системы обнаружения вторжений в этом случае бессильны, поскольку инсайдеры являются легитимными пользователями БД и прикладных программ, и их действия не подходят под шаблоны атак сетевого уровня или уровня ОС. Проблема состоит также в том, что предоставление привилегий в БД осуществляется с помощью команды **grant,** которая не позволяет тонко настраивать права доступа. Например, с ее помощью нельзя установить возможность вставлять в таблицу только те строки, которые отвечают заданным условиям.

Исправить ситуацию можно путем корректировки настроек безопасности используя информацию аудита БД, точнее, используя информацию о профилях пользователей построенных по данным аудита.

Аудит – это процесс отслеживания и фиксации событий, происходящих в системе. NIST определил [2] такие компоненты системы аудита: выбора событий, подлежащих регистрации, генерации сообщений о событиях, хранения данных регистрации, визуализации данных регистрации, анализа данных, автоматизированной реакции на события. Современные СУБД отвечают этим требованиям. Кроме того, встроенные возможности аудита могут быть расширены за счет таких объектов БД как триггеры и хранимые процедуры. С их помощью можно дополнительно регистрировать информацию по критериям, которые невозможно задать встроенными средствами.

Профиль – обобщенная характеристика объекта, выраженная в числовых показателях, имеющих обычно статистический характер. Профиль пользователя отражает типичное поведение последнего при работе с БД – используемые объекты БД, характер операций над ними (чтение и модификация таблиц, вызовы процедур, обращения к представлениям).

II Построение профилей пользователей

Задача построения профиля пользователя $\mathbf{U_{db}}$ является типичной для систем обнаружения аномального поведения пользователей в БД [3 – 6]. В таких системах решающим фактором является отклонение характеристик текущего поведения пользователя от его профиля. Следуя работе [3] определим профиль пользователя как набор троек:

$$User\ \mathrm{Pr}\,of\left(t_1,t_2\right)=\left\{<c>,<T>,<A>\right\} \tag{1}$$

где $<c>$ – выполняемая команда,
$<T>$ – список таблиц которыми оперирует команда с,
$<A>$ – список атрибутов таблиц $<T>$, участвующих в команде,
$[t_1,t_2]$ – временной интервал построения профиля.

Зададим также расширенный вариант профиля пользователя

$$User\ \mathrm{Pr}\,of\left(t_1,t_2\right)=\left\{<U>,<c>,<T>,<A/V>\right\} \tag{2}$$

где $<U>$ – учетная запись БД, активизировавшая данную роль,
$<A/V>$ – набор пар «атрибут/значение».

Сохраняемая информация (по всем профилям) может быть представлена в виде таблицы (например, как в табл. 1). В реальных таблицах все параметры представлены идентификаторами [3].

Таблица 1 – Результаты аудита

Роль	Учетная запись	Таблица	Команда	Атрибуты / Значения
Менеджер	User1	Таблица 2	Select	NULL
Инженер	User2	Таблица 2	Insert	A1,8; A2,12; A3, 4.5
Инженер	User3	Таблица 3	Update	A2, TRUE

Профиль пользователя строится для той роли, которую пользователь активизировал. Если в течении сессии он активизировал несколько ролей, то для него будет построено несколько профилей. Хранится профиль во вспомогательной таблице, желательно в другой базе данных, чтобы обращения к таблице не меняли общую картину активности в БД. В СУБД Oracle такую возможность предоставляет продукт Audit Vault.

Используя SQL запросы с группировкой можно из таблиц, хранящих профили, извлечь информацию о функционировании БД. Так из расширенных профилей можно получить наиболее характерные образцы (шаблоны) доступа к данным. Например, для операции вставки строки можно определить типичные значения или типичный интервал добавляемых значений. Для операции удаления строки можно определить типичные характеристики удаляемой строки.

III Рекомендации по реорганизации политики безопасности

Корректировка политики безопасности заключается в изменении настроек безопасности, ограничивающих возможности пользователей и ролей БД, таким образом, что они (возможности) как

можно более точно соответствовали принципу минимума привилегий. Надо помнить, что все вносимые ограничения должны согласовываться с моделью предметной области (бизнес-моделью), используемой при проектировании БД. Кроме того, необходимо учитывать такой фактор, как производительность. Ограничения целостности, триггеры, хранимые процедуры, процесс аудита – все это создает дополнительную нагрузку на сервер БД. При следовании предлагаемым рекомендациям необходимо придерживаться баланса между производительностью и требованиями безопасности.

Рекомендации по изменению политики безопасности разобьем на следующие группы.

1. Неиспользуемые учетные записи и роли. Анализ профилей пользователей (для ролей) и расширенных профилей пользователей (для учетных записей) позволяет выявить учетные записи и роли БД, которые за определенный промежуток времени не активизировались. Такие объекты должны быть заблокированы или даже удалены.
2. Неиспользуемые привилегии. Если, например, для определенной роли установлено право на модификацию записей в таблице, однако за продолжительный промежуток времени такая операция не разу не была выполнена, следует пересмотреть список прав доступа данной роли. Выполнить такой анализ можно как по расширенным так и по обычным профилям.
3. Изменение структуры ролей БД. Проанализировав набор операций над таблицами БД, можно составить перечень используемых прав доступа. На основе такого перечня можно решать задачу определения оптимального состава и структуры ролей БД [7, 8]. Выполнить такой анализ можно как по расширенным, так и по обычным профилям.
4. Модификация представлений (views) БД. С позиций безопасности непосредственный доступ пользователей к таблицам БД должен быть запрещен, а информацию он должен получать из представлений. В результате анализа расширенных профилей может оказаться, что некоторые пользователи используют в своей работе только те строки таблиц, которые отвечают определенным требованиям. Соответствующим образом можно изменить доступные этим пользователям представления. Решить данную задачу корректно можно при достаточно большом интервале времени формирования профиля $[t_1,t_2]$.
5. Формирование табличных ограничений целостности. На основе анализа расширенного профиля можно определить допустимые диапазоны изменения атрибутов таблиц. Сами ограничения на таблицы устанавливаются тривиально (с помощью ключевого слова **check** или триггера). Для корректного решения данной задачи также необходимо формировать профиль на большом интервале времени $[t_1,t_2]$.
6. Модификация хранимых процедур. Сами по себе хранимые процедуры (ХП) являются важным средством обеспечения безопасности данных. Хорошей практикой является организация доступа к объектам БД из прикладных программ только через ХП. Кроме того, зачастую необходимость предоставления определенных прав доступа к таблицам БД зависит от контекста, в котором выполняется операция. Этот контекст может включать в себя учет активных пользовательских сессий, источник запроса и т. д. Все это невозможно учесть в дискреционной модели доступа БД, команда **grant** является слишком «грубой». Хранимые процедуры являются мощным средством для сбора и анализа контекстной информации, в случае когда они вызываются из прикладных программ. Следовательно, их можно использовать для тонкой настройки прав доступа к объектам БД.

Литература: ***1.*** *Lawrence A., Gordon R, Martin P. Loeb. 2005 CSI/FBI computer crime and security survey. Technical report., Computer Security Institute, 2005.* ***2.*** *Common Criteria for Information Technology Security Evaluation (Version 3.1). Technical report. 2006.* ***3.*** *М. Коломыцев, С. Носок Аудит аномального поведения пользователей баз данных // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні // науково-технічний збірник. – Випуск 2(17). – Київ, 2008. – С.67 – 70.* ***4.*** *Y. Hu and B. Panda. Identification of malicious transactions in database systems. In Proceedings of the international Database Engineering and Applications Symposium (IDEAS), 2003.* ***5.*** *A. Kamra, E. Bertino, and E. Terzi. Detecting anomalous access patterns in relational databases. The International Journal on Very Large Data Bases (VLDB), 2008.* ***6.*** *C. Chung, M. Gertz, and K. Levitt. DEMIDS: a misuse detection system for database systems. In Proceedings of Integrity and Internal Control in Information Systems: Strategic Views on the Need for Control. IFIP TC11 WG11.5 Third Working Conference, 2000.* ***7.*** *J. Schlegelmilch, U. Steffens. Role mining with ORCA. In 10th ACM Symposium on Access Control Models and Technologies. P. 168-176, 2005.* ***8.*** *J. Vaidya, V. Atluri. The role mining problem: finding a minimal descriptive set of roles. In 12th ACM Symposium on Access Control Models and Technologies. P. 175-184, 2007.*