ВОПРОСЫ ПРОЕКТИРОВАНИЯ РЕЛЯЦИОННЫХ БАЗ ДАННЫХ С МНОГОУРОВНЕВЫМ ДОСТУПОМ

Я.А. Быков, М.В. Аксарин, М.В. Тарасюк

Санкт-Петербургский институт информатики и автоматизации РАН
199178, Санкт-Петербург, 14-я линия ВО, д.39
<yar@rol.ru>

УДК 681.3.06
Я. А. Быков, М. В. Аксарин, М. В. Тарасюк. **Вопросы проектирования реляционных баз данных с многоуровневым доступом** // Труды СПИИРАН, Вып. 2, т. 2. — СПб.: Наука, 2005.
Аннотация. *Рассматриваются вопросы организации многоуровневого режима обработки информации с распределенных системах на основе СУБД, в числе которых решение проблем агрегации и многозначности.* — Библ. 6 назв.

UDC 681.3.06
Y. A. Bykov, M. V. Aksarin, M. V. Tarasjuk. **The problems of the relational databases design with multilevel access** // SPIIRAS Proceedings. Issue 2, vol. 2. — SPb.: Nauka, 2005.
Abstract. *The problems of the organization of the multilevel mode of the information processing on the distributed systems for DBMS, including the problems of the aggregation and polysemy.* — Bibl. 6 items.

Реляционные СУБД представляют пример технологии, для которой выполнение требований к защите информации от НСД, позволяющих использовать их в составе автоматизированных систем с многоуровневым доступом представляет серьезную проблему. Эти проблемы связаны не только с практической сложностью монитора обращений СЗИ для СУБД и обеспечением необходимых гарантий безопасности реализации проектов, но также и с разработкой формальных моделей защиты.

Традиционные методики оценки защищенности информационных технологий [1, 2], ориентированы в первую очередь на системы обработки неструктурированных наборов данных. Для таких систем отдельные (неделимые), семантически значимые информационные элементы формируются и обрабатываются независимо, что позволяет использовать модели защиты, для которых решения по предоставлению доступа принимаются также независимо.

Однако для приложений и систем на основе реляционных СУБД такое допущение не всегда оправдано, вследствие чего при проектировании структуры БД и реализации модели защиты необходимо учитывать взаимосвязь между информационными элементами. Данная взаимосвязь порождает две фундаментальные проблемы применимости универсальных СУБД в системах с многоуровневым доступом, а именно проблему агрегации и проблему многозначности.

Проблема агрегации

Проблема агрегации практически актуальна для любых систем[1], однако в большинстве случаев обработки слабо связанной между собой информации она

[1] Например, формирование несекретных выписок из секретных документов (документ может рассматриваться как пример неструктурированного массива информации) представляет плохо формализованную для СЗИ задачу.

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

решается на уровне пользователя без необходимости принятия СЗИ автоматизированных решений.

Принято выделять два вида агрегации — структурную и множественную [3]. Под структурной агрегацией понимается зависимость уровня секретности информационной совокупности от связей между отдельными объектами (внешняя агрегация) либо между атрибутами одного объекта (внутренняя агрегация) в пределах информационной совокупности. Проявление структурной агрегации основывается на различных, способах установления зависимостей между элементами данных и предсказания одних данных (к которым пользователь не допущен) через другие данные (к которым пользователь допущен). Механизм предсказания базируется на логическом (дедуктивном) выводе данных либо статистических методах обработки данных с целью получения вероятностных оценок секретных данных.

В качестве примера структурной агрегации можно привести систему, обрабатывающую данные по агентурной разведке. Отдельные пользователи системы могут иметь доступ к разведывательным сведениям либо к информации о должностных лицах, работающих в подразделениях разведывательной службы, однако не все пользователи могут быть допущены к информации, связующей конкретных должностных лиц с конкретными видами деятельности сотрудников подразделений.

Под множественной агрегацией понимается зависимость уровня секретности совокупности объектов БД от числа элементов в данной информационной совокупности. В качестве примера множественной агрегации можно привести агрегацию данных в телефонных справочниках. Отдельный телефонный номер, как правило, не относится к разряду критичной информации, однако полный телефонный справочник с указанием адресных и других реквизитов абонентов часто может быть отнесен к разряду конфиденциальной информации. Сложность разработки и использования формальных моделей защиты, учитывающих агрегацию, в конкретной системе может проявляться:

- в трудности точного и полного указания правил, посредством которых отдельные элементы и связи между ними могут классифицироваться по уровню критичности,
- неформальным процессом вывода одних данных через другие, который может использовать для этого совершенно разнородную и нечеткую информацию, в том числе внешнюю информацию, не обрабатываемую в системе,
- свойством накопления информации, когда пользователь последовательно выдает запросы к информационным объектам, а затем комбинирует с их помощью интересующие его данные.

Для создания СЗИ, реализующих модель защиты с учетом агрегации, необходимо определить базу правил, устанавливающих уровень секретности для обнаруженных типов связей между объектами. Монитор обращений в этом случае будет обрабатывать каждый запрос от пользователя путем последовательного сравнения сигнатуры запрошенного набора объектов с каждым правилом. Однако построение функционально полных и непротиворечивых правил требует всестороннего анализа возможных зависимостей между элементами данных и метадан-

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ных[2], что для более или менее реальных по сложности систем трудно выполнимая задача. Функциональная полнота предполагает, что для каждого из теоретически допустимых наборов объектов (атрибутов) в базе правил найдется правило для определения уровня секретности данного набора. Под непротиворечивостью правил понимается единственность выбора правила для определения уровня секретности любого набора объектов или атрибутов либо равнозначность определения уровня секретности данного набора двумя и более правилами. Можно конечно упростить ограничения и классифицировать запросы в соответствии с правилом, устанавливающим максимально высокий по сравнению с другими правилами уровень секретности. При этом нарушения безопасности отсутствуют, но появляются проблемы доступности ресурсов.

Физическое воплощение надстройки монитора обращений информационной системы на основе реляционной СУБД с обработкой семантики решающих правил могут быть реализованы в виде набора определенным образом сгруппированных SQL предложений, что может сказаться на производительности, а также на затратах на хранение и поддержание целостности базы правил. В связи с этим возможности подобных технологий зависят от оптимальности алгоритмов поиска подходящего правила и их факторизации с целью сокращения объема хранимых правил. Ведь в общем случае число таких зависимостей может возрастать экспоненциально с ростом числа типов объектов (атрибутов), накапливаемых в БД.

Эффективная реализация монитора обращений в соответствии с рассмотренными принципами возможна, когда в обрабатываемых данных могут быть выделены сравнительно независимые совокупности объектов малого объема, в пределах которых агрегация не возникает, а число правил классификации связей внутри каждой совокупности объектов (атрибутов) относительно невелико.

Способы решения проблемы множественной агрегации основываются на контроле максимального объема данных, выбираемых пользователем за один сеанс доступа, и сохранением информации о фактических объемах предоставленной информации в регистрационном журнале (при подходе к пороговому значению работа пользователя может быть заблокирована). Для этого необходима синхронизация регистрационных журналов, что для распределенной системы не слишком хорошее решение.

Проблема многозначности

Суть проблемы состоит в противоречивом характере требований к БД, с одной стороны, гарантирующих целостность данных, а с другой стороны — строго реализующих требования мандатной политики [4]. Надо заметить, что наиболее известной промышленной СУБД общего назначения, реализующей мандатную политику, является СУБД TRUSTED ORACLE [5]. Данная СУБД сертифицирована NSA как система, соответствующая классу защищенности B1 (наименьший класс систем с мандатной политикой) при достаточно жестких ограничениях применения. Одним из таких ограничений является функционирование под управлением много-

[2] Под метаданными понимаются сведения о структуре системы, которые, как правило, известны потенциальному нарушителю. Например, в случае СУБД метаданные – это словарь данных или схема данных.

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

уровневой ОС при условии, что все файлы базы данных используются для хранения одноуровневой информации.

Проблема многозначности имеет два аспекта. Первый аспект касается невозможности нормализации представления данных в соответствии с требованиями реляционной модели, поскольку поля записей в одном и том же отношении различным образом представляются для пользователей различного уровня допуска. Пользователь высшего уровня допуска может обладать истинными данными, а пользователь низшего уровня допуска – легендой прикрытия для этих данных. Естественно встает вопрос о том, как организовать хранение таких данных.

Если принять стратегию отказа в предоставлении пользователю истинного содержимого атрибутов, к которым он не допущен (например, выдавать пустое значение — NULL), то пользователь узнает факт сокрытия от него информации, а это неприемлемо с точки зрения строгой реализации MLS политики в форме решающих правил Белла Лападулы. Такая ситуация влечет за собой скрытый канал утечки информации, который можно описать следующим образом.

Троянская программа, встроенная в приложение на более высоком уровне секретности, выбирает необходимую для передачи на более низкий уровень информацию, создает и удаляет записи в таблице БД, содержащей атрибут с высшим уровнем секретности. Приложение приемник анализирует последовательные появления и пропадания строки с указанным атрибутом, тем самым, опознавая передаваемые символы.

Для борьбы подобными СК данные с высоким уровнем секретности нуждаются в легендах прикрытия[3]. Однако если определить легенду прикрытия для секретных данных, возникает проблема множественного хранения в одной строке отношения нескольких значений одного атрибута. Это не позволяет рассматривать БД как реляционную, поскольку ей не может быть назначена даже первая нормальная форма! Особенно остро проблема стоит в случае, если атрибут с легендой прикрытия является первичным ключом и индексирует данные отношения. Возможна и обратная ситуация, когда для формирования скрытых каналов используются ограничения ссылочной целостности.

Предположим, что в некоторой записи с внешним ключом одного уровня секретности присутствует поле с более низким уровнем, доступное для просмотра пользователю с низким уровнем допуска. В целом, такая ситуация является осмысленной и может быть вызвана противодействием агрегации связей.

Предположим, что этот внешний ключ связан каскадным ограничением целостности с некоторым первичным ключом отношения высокого уровня секретности. Пусть пользователь с высоким уровнем допуска удаляет из своей таблицы запись, содержащую данный первичный ключ. В соответствии с политикой каскадного удаления внешних ключей, запись, содержащая внешний ключ, ссылающийся на удаляемую запись, также должна быть удалена. Таким образом, пользователь с низким уровнем, наблюдавший ранее доступную ему часть удаляемой записи, обнаружит ее отсутствие. Это позволяет скрытым образом передавать информацию между уровнями секретности и ведет к образованию скрытого канала.

[3] Легендами прикрытия обычно называют внешне правдоподобную (непротиворечивую) информацию, маскирующую истинное содержание каких-либо скрываемых сведений.

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Для предотвращения такого СК к внешнему ключу может предъявляться дополнительное требование: уровень секретности полей записи, содержащей внешние ключи, не должен быть ниже, чем уровень секретности этих внешних ключей. Сегментация таблиц отношений с дублированием записей, содержащих поля разной секретности, предотвращает возникновение этого вида скрытых каналов.

Еще более широкие возможности скрытого взаимодействия дает политика запрещения удаления первичных ключей при наличии внешних ключей. Пусть в БД некоторая таблица с высоким уровнем секретности ссылается на таблицу с низким уровнем секретности. Допустим также, что пользователь с низким уровнем допуска удаляет или модифицирует в своей таблице некоторую запись, первичный ключ которой служит внешним ключом для записей в таблице высокого уровня.

Руководствуясь политикой ссылочной целостности путем запрета удаления первичных ключей, на которые есть ссылки, СУБД не позволит пользователю с низким уровнем допуска удалить соответствующие записи. Из этого пользователь сможет сделать заключение о наличии в таблице с высоким уровнем секретности записей, ссылающихся на удаляемые записи. Создавая и удаляя такие записи, пользователь с высоким уровнем допуска сможет организовать скрытую передачу информации в таблицы БД низкого уровня, что ведет к образованию скрытых каналов. Единственной возможностью исключения этого вида скрытого взаимодействия является отказ от запрета удаления первичных ключей, на которые есть ссылки. Вместо нее может использоваться каскадное удаление зависимых записей, или присвоение в них внешнему ключу нулевого значения (NULL), либо значения по умолчанию.

Итак, реализация политики управления внешними ключами может привести к возникновению скрытых каналов. Во избежание их следует с осторожностью применять политику соблюдения ссылочной целостности путем запрета изменения и удаления первичных ключей, для которых имеются внешние ключи, или же отказаться от ее использования вовсе.

Проблема многозначности имеет отношение в основном к реляционным СУБД. Например, для СУБД, разработанной в соответствии с рекомендациями ITU–T X.500, модель защиты аналогична используемой в ОС с древовидной структурой файловой системы, где проблема многозначности не возникает. Для реляционных СУБД решения проблемы многозначности, пригодного на все случаи жизни, не существует, в том числе, ввиду рассмотренных выше причин. Однако для конкретных задач можно воспользоваться комплексным применением следующих технических решений [6]:

- введением ограничений проектирования информационной структуры БД, в рамках которых данные структурируются таким образом, чтобы обеспечить их одинаковую классификацию при размещении в таблицах отношений. Одинаковая классификация означает, что в каждой таблице БД хранится информация строго одного уровня доступа;
- использованием специальных программных компонентов — шлюзов БД, представляющих собой функционирующие на платформе СУБД приложения, обеспечивающие фиксированный доступ пользователей к динамическим наборам данных, построенным на базе одноуровневых таблиц. При этом произвольный

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

доступ пользователей к таблицам путем самостоятельного формирования SQL запросов не допускается;

- использованием нескольких экземпляров БД, обрабатывающих информацию только одного уровня доступа. Если в системе обрабатывается несекретная, секретная и совершенно секретная информация, можно определить три экземпляра БД, в первом из которых обрабатывается только несекретная информация, во втором — секретная и несекретная, а в третьем — несекретная, секретная и совершенно секретная информация (очевидно, что каждый экземпляр такой БД работает с одноуровневыми запросами). Экземпляры БД связаны между собой посредством доверенного диспетчера запросов. Применительно к различным вариантам архитектуры, распределенные БД реализованы в ряде исследовательских проектов ВВС США Rome Air Development Center (RADC) ВВС США. В рамках этих проектов разработано несколько версий СУБД SDDBMS, реализующих мандатную политику.

Литература

[1] Department of Defence Trusted Computer Evaluated Criteria, DoD 5200.28-STD, Washington, 1986.

[2] Руководящий документ Гостехкомиссии РФ “Средства вычислительной техники. Защита информации от несанкционированного доступа. Показатели защищенности от НСД к информации”. 1992.

[3] ГОСТ ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

[4] NCSC. TECHNICAL REPORT-005. Volume 1/5 (1996). USA. P.78.

[5] Trusted Oracle Server 7.1 Server Administrator’s Guide. NCSC.

[6] *С. Асанов, А. Кузнецов, М. Тарасюк.* Технология построения АС с многоуровневым доступом для государственных и правительственных структур РФ. // Конфидент, №6, 2003. — с. 20–25.