Безопасный доступ и хранение данных: СУБД Oracle

Рассматриваются вопросы обеспечения безопасности хранения данных и доступа к ним в приложениях на основе СУБД Oracle и решений компании Aladdin.

Введение

Статистика финансового ущерба от краж и потерь информации стабильно растет год от года. Достаточно обратиться, например, на сайт компании "Privacy Rights Clearinghouse", содержащий годовые отчеты о подобных нарушениях, чтобы убедиться в этом *(http://www.privacyrights.org/ar/ChronDataBreaches.htm)*.

Огромное количество записей – 165 891 898 (и оно далеко не полное), содержащих конфиденциальную информацию, было украдено из десятков компаний. Убытки от таких краж составляют миллионы долларов. К сожалению, подробной статистики по российским компаниям не ведется. Однако компании, специализирующиеся на оценке рисков по информационной безопасности в России, делают неутешительный вывод – положение дел в нашей стране далеко не безоблачное. Практически каждая из 400 организаций, принявшая участие в исследовании компании InfoWatch, отметила риски финансовых потерь из-за кражи информации. По данным InfoWatch, реальные потери компании численностью от 1000 человек могут составить $180 тыс., и потери прямо пропорциональны численности персонала. Кроме того, наиболее вероятна потеря информации вследствие действий инсайдеров, прежде всего, персонала, обслуживающего IT-инфраструктуру компании – администраторов ОС и БД. Методы борьбы с подобными злоупотреблениями, как правило, строятся на сочетании административных (законодательные акты, регламенты, правила) и технических мер (права, роли, политики, аудит и т.п.).

Правовое регулирование в РФ данной области имеет тенденцию к ужесточению. Например, совсем скоро стандарт центрального Банка России по информационной безопасности может стать обязательным для исполнения. ФЗ "О персональных данных" прямо предписывает защищать приватную информацию и, возможно, в его рамках появятся новые требования. В рамках практически любой организации имеются свои регламенты и требования к обеспечению ИБ, учитывающие собственно специфику ее деятельности.

Любая информация, используемая в рамках какой-либо информационной системы, как правило, хранится в структурированном виде и управляется некоторым набором ПО, что и представляет собой СУБД – систему управления базами данных. В силу того, что СУБД является прикладной задачей по отношению к операционной системе, она наследует практически все уязвимости ОС. В дополнение СУБД имеют уязвимости, специфичные для них, например, SQL-инъекции.

Классификация методологий защиты

Защиту данных криптографическими методами принято классифицировать по месту применения шифрования:

- уровень приложения;
- уровень файловой системы;
- сетевой уровень;
- уровень устройства.

Первый из упомянутых методов является наиболее привлекательным, так как он наиболее "приближен" к защищаемым данным и позволяет более точно провести соответствие между данными, ролями, пользователями и приложениями. В качестве приложения, предоставляющего защиту данных с помощью шифрования, можно привести СУБД Oracle. Корпорация Oracle традиционно уделяет серьезное внимание вопросам безопасности своих программных продуктов. С версии 8i сервер БД Oracle обеспечивает строгую аутентификацию пользователей, защиту сети, множество механизмов ограничения и разделения доступа, начиная с ролевой защиты и заканчивая технологией доступа на основе меток безопасности. В версии 10g набор средств обеспечения безопасности расширился за счет опций "прозрачного" шифрования данных (Transparency Data Encryption) и усиленного хранилища БД (Database Vault). Именно две эти опции при совместном использовании дают эффект защиты от кражи информации со стороны привилегированных пользователей – администраторов БД. Transparency Data Encryption (TDE) позволяет выборочно зашифровывать данные на уровне колонок таблиц, таблиц в целом и схем пользователя с использованием какого-либо симметричного алгоритма шифрования, встроенного в сервер БД (DES/TripleDES с ключом длиной до 192 бит или AES с ключом

длиной до 256 бит). Ключ для симметричного шифрования генерируется случайным образом и сохраняется в секретном хранилище – файле PKCS#12 формата, защищенном паролем, который задается администратором. Создание ключа и зашифрование/расшифрование производится пользователем с правами администратора БД. После зашифрования данные физически хранятся на дисках в преобразованном виде. Расшифрование при чтении (операция SELECT) и зашифрование при записи (операции INSERT и UPDATE) производится сервером "на лету", что определяет возможность работы всех приложений с защищенными данными без какой-либо доработки. Подобный способ довольно хорошо отрабатывает сценарий "кража носителя" или "кража файла", однако он не лишен недостатков. Самый существенный из них – нулевая стойкость к злонамеренным действиям со стороны администраторов БД, которые могут на время отменить шифрование и вновь его назначить. Для предотвращения подобного рода недостатков предназначена опция Database Vault (DV). С ее помощью можно ограничить права доступа к данным и выполнение определенных SQL-команд для любых пользователей, включая имеющих административные привилегии. Разделение доступа очень гибкое, управление правами интуитивно понятное, реализовано в виде web-интерфейса, что позволяет управлять доступом удаленно. Связка TDE + DV обеспечивает высокий уровень защиты от несанкционированного доступа к данным, но и здесь имеют место некоторые ограничения использования:

- становится невозможным использовать технологию Oracle Automated Storage Management (ASM);
- возникают проблемы с установкой обновлений сервера БД (следует отменять защиту DV – многошаговый процесс, затем восстанавливать заново);
- возникают проблемы с экспортом и импортом данных;
- остается основная проблема доверия администратору, только теперь в его качестве выступает администратор DV;
- отсутствует связь между пользователем с его служебными полномочиями по работе с конфиденциальными данными и набором ограничений, накладываемым СУБД;
- остается проблема с хранением ключей шифрования;
- невозможно применение криптоалгоритмов ГОСТ, что требуется в некоторых организациях.

Можно ли достичь разумного компромисса между техническими возможностями сервера БД и степенью защиты информации, предписываемой административными регламентами и служебными инструкциями?

Рис. 1. Исходное состояние информационной системы.

Планирование и внедрение системы защиты с использованием опций Oracle Advanced Security и решений Aladdin

Рассмотрим типичный пример защиты данных и доступа к ним из приложений, использующих СУБД Oracle. Допустим, что имеется хранилище данных и приложения, составляющие корпоративную информационную систему, которые манипулируют ими. Определим роли пользователей по отношению к нашей информационной системе:

- пользователи – лица, имеющие доступ к конфиденциальным данным, в соответствии со своими служебными обязанностями;
- администраторы БД – лица, отвечающие за функционирование БД; имеют доступ ко всем данным, включая конфиденциальные;
- администраторы безопасности (АБ) – лица, отвечающие за разработку и исполнение регламентов по ИБ. Доступа к данным информационной системы не имеют.

Постановка задачи по защите может звучать как "разрешить доступ классифицированным данным только для лиц с ролью *пользователь*". При этом необходимо выполнить ряд общепринятых ограничений:

- ключи шифрования не должны храниться где-либо в открытом виде;
- время передачи ключа в открытом виде должно быть минимальным;
- каждый конечный пользователь должен иметь "личную" копию ключа шифрования;
- ПО, реализующее шифрование данных, должно быть защищено от компрометации;
- приложения ИС не должны модифицироваться.

Исходное состояние информационной системы изображено на рис. 1.

Администратору безопасности предварительно требуется:

1. Определить данные, классифицируемые как секретные/конфиденциальные/личные и т.п.

2. Выбрать соответствующие каждой категории данных криптоалгоритм и длину ключа для симметричного шифрования.

3. Определить схемы, таблицы и колонки, содержащие классифицированную информацию.

Дальнейшие шаги проиллюстрированы на рис. 2.

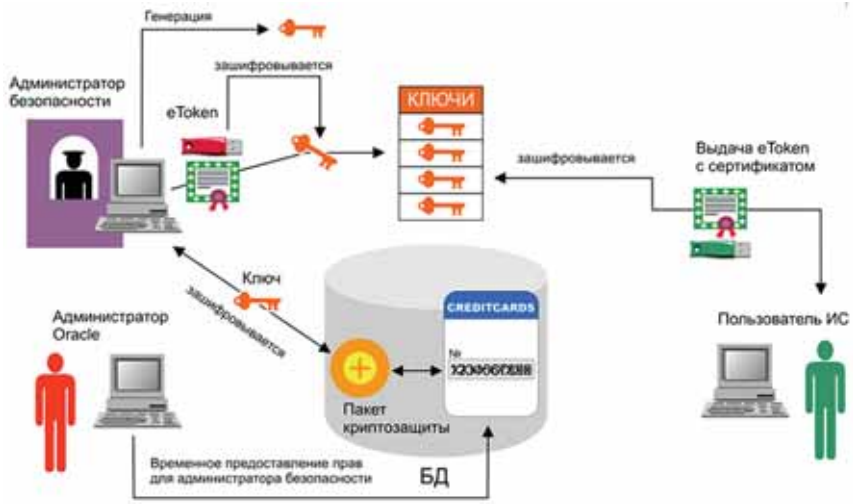

Рис. 2. Инсталляция криптозащиты на БД состоит из 5 шагов: (1) АБ временно получает полномочия для работы с защищаемой колонкой от администратора БД; (2) АБ устанавливает ПО (Aladdin) "пакет криптозащиты", реализующий выбранный алгоритм шифрования и логику работы с ключами шифрования; (3) АБ генерирует ключ шифрования для колонки и зашифровывает данные в колонке с помощью выбранного алгоритма; (4) АБ создает для каждого пользователя ИС копии ключа шифрования, зашифрованные на соответствующем сертификате открытого ключа, помещенного на смарт-карту; (5) администратор БД изымает права на доступ к защищенной колонке у АБ.

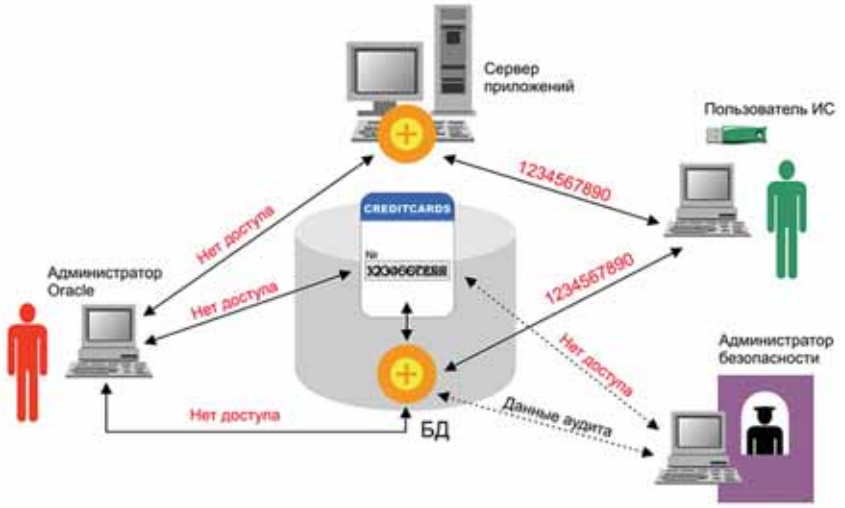

Рис. 3. Функционирование ИС в защищенном режиме.

1. Администратор безопасности временно получает полномочия для работы с защищаемой колонкой от администратора БД.

2. Администратор безопасности устанавливает ПО (Aladdin) "пакет криптозащиты", реализующий выбранный алгоритм шифрования и логику работы с ключами шифрования.

3. Администратор безопасности генерирует ключ шифрования для колонки и зашифровывает данные в колонке с помощью выбранного алгоритма.

4. Администратор безопасности создает для каждого пользователя ИС копии ключа шифрования, зашифрованные на соответствующем сертификате открытого ключа, помещенного на смарт-карту.

5. Администратор БД изымает права на доступ к защищенной колонке у администратора безопасности.

Дальнейшее функционирование ИС происходит в защищенном режиме (рис. 3).

Администратор безопасности не имеет доступа к колонке, т.к. ему не делегированы соответствующие права со стороны администратора БД, хотя он имеет валидный ключ шифрования. При этом он имеет возможность отслеживать попытки доступа к защищенной колонке. Администратор БД не имеет возможности адекватного доступа к данной колонке ввиду отсутствия у него копии ключа шифрования. При этом неважно, как он пытается прочесть данные – через пакет криптозащиты или напрямую из таблицы.

Пользователь ИС, имея зашифрованную копию ключа, которую он может расшифровать, используя закрытый ключ, установленный на смарт-карте (этим занимается ПО SecurLogon для Oracle и пакет криптозащиты), продолжает работать в обычном режиме. Для такого пользователя подобная защита "прозрачна".

Таким образом, проблема соответствия должностных обязанностей, обозначенных административными регламентами, и технических средств ограничения доступа может быть решена.

Аудит – составляющая часть безопасности

Говоря о безопасном доступе, следует помнить правило "доверяй, но проверяй". Обычно вопросы по поводу тех или иных действий с защищенной информацией возникают по факту "разбора полетов". Расследование тех или иных инцидентов проводится на основе данных из различных источников – журналов ОС, серверов приложений и, если дело касается кражи информации, журналов аудита БД. СУБД Oracle предоставляет мощные средства для сбора данных аудита – опции Fine-Grained Audit Control и Audit Vault (в версиях 9.2.0.8 и 10.2.0.3), которые позволяют получить данные о пользователе, времени и характере доступа к данным и защитить данные аудита от модификации. И если же характер и время доступа не вызывают вопросов, то определение физического лица – субъекта доступа – задача более сложная. Набор информации, по которой можно идентифицировать пользователя, достаточно широк: идентификатор пользователя (имя, отличительное имя (DN), прокси-имя, имя пользователя ОС), IP-адрес и имя рабочей станции, имя приложения. Но и такой информации бывает недостаточно для доказательства факта доступа конкретного лица. Это связано с несовершенством парольной аутентификации, а также с все той же проблемой привилегированных пользователей.

Рассмотренный выше метод защиты данных позволяет дополнить механизмы штатного аудита Oracle для повышения достоверности определения субъекта доступа. Идентификация субъекта доступа в данном случае базируется не на идентификаторе пользователя, а на идентификаторе копии ключа шифрования. Ведь расшифровать ключ (естественно, за приемлемое время) можно, лишь предъявив закрытый ключ, установленный на смарт-карте. Потенциальный злоумышленник не может его скопировать или извлечь из смарт-карты, а в случае утери или кражи подбор PIN-кода маловероятен – на это есть всего насколько попыток. Таким образом, в сочетании со штатными механизмами аудита поиск злоумышленника значительно упрощается.

Основные проблемы

Внедрение системы защиты данных с помощью шифрования напрямую влияет на производительность ИС. Поэтому следует очень внимательно относиться к выбору информации – кандидата на шифрование, алгоритмов и длины ключей для шифрования.

Следует также помнить, что необходимо по максимуму защитить используемое ПО от взлома со стороны "продвинутых" пользователей. Так, ПО от Aladdin проверяет ЭЦП всех пакетов, используемых на стороне сервера, прежде чем проводить процедуру вычисления ключей шифрования для пользователя.

Правовое регулирование

Требования к ИБ для ИС, используемых в госучреждениях, предписывают, в частности, использовать криптоалгоритмы от сертифицированных производителей. В рассмотренном решении возможно применение российской криптографии (например, от известной компании КриптоПро) как для шифрования данных, так и для создания зашифрованных копий ключей.

Заключение

В заключение хотелось бы отметить, что Россия, как и любая другая страна, обладает определенной спецификой в сфере информационной безопасности. Концепция Oracle, с этой точки зрения, базируется на двух основных составляющих – использовании технологий мирового уровня и учете особенностей и потребностей российского заказчика. Именно эта цель лежит в основе партнерских отношений Oracle и Aladdin.

В рамках технологического сотрудничества особый акцент совместных решений сделан на управлении учетными записями и доступом к информационным ресурсам, что предполагает администрирование учетных данных, использование службы каталогов, а также аудит и контроль в соответствии с требованиями ИБ. Усиление безопасности доступа к приложениям Oracle при помощи аппаратных электронных ключей eToken обеспечивает ряд дополнительных возможностей, таких как интеграция с PKI, организация безопасной работы в Интернет, проверка подлинности пользователя, а также преимущества мобильного доступа к защищенным информационным ресурсам с использованием комбинированного устройства eToken NG-OTP.

Еще раз подчеркнем, что проблема защиты доступа, в том числе и удаленного, сейчас как никогда актуальна для многофилиальных организаций, а также структур, использующих Интернет-сервисы и предоставляющих своим бизнес-партнерам возможность мобильного использования информационных ресурсов. При объединении технологических возможностей бизнес-приложений Oracle с аппаратными средствами защиты Aladdin можно создать действительно надежное решение, отвечающее высоким требованиям современного бизнеса и российского законодательства.

Александр Додохов,
руководитель направления защиты баз данных Aladdin Software Security R.D.