ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СУБД ORACLE

Анастасия СИДОРЕНКО

Технический Университет Молдовы, Департамент Программной Инженерии и Автоматики

Аннотация: *В данной статье раскрывается технология защиты персональных данных в одной из самых распространенных СУБД на сегодняшний день – Oracle Database. Приведен пример механизма шифрования, используемого в рассматриваемой СУБД – прозрачное шифрование данных.*

Ключевые слова: *база данных, прозрачное шифрование, конфиденциальность, Oracle, защита.*

Введение в понятие шифрования данных

В современном мире, где информация становится одним из основных ресурсов в экономике, становится все труднее обеспечивать защиту данных от злоумышленников. Заполняя анкету на Интернет-форуме или делая заказ в онлайн-магазине, личные данные пользователя попадают напрямую в базу данных приложения. Существуют различные меры предосторожности для сохранения информации в базе данных и обеспечения ее конфиденциальности и целостности, например, проектирование безопасной системы, шифрование конфиденциальных активов, а также создание брандмауэра вокруг серверов баз данных. Данные методы могут быть очень эффективны для достижения вышеназванной цели, но в одном случае они не смогут уберечь личные данные от кражи – в случае похищения физических носителей хранения базы данных. Тогда в ход вступает технология шифрования конфиденциальных данных и соответствующая защита ключей, используемых в криптографическом процессе, с помощью так называемых сертификатов.

1. Шифрование данных в СУБД Oracle Database

На сегодняшний день одной из самых распространенных и надежных систем управления базами данных является объектно-реляционная СУБД Oracle Database, созданная в 1979 году группой американских программистов: Ларри Эллисон, Боб Майнер и Эд Оутс. Своей надежностью она обязана поддержкой технологии прозрачного шифрования данных, которая в англоязычных источниках называется TDE, то есть Transparent Data Encryption. TDE входит в состав опции Oracle Advanced Security с версии 10g, выпущенной на пользовательский рынок в 2005 году. Эта технология позволяет «прозрачно» для приложений шифровать данные на уровне колонок таблиц или табличных пространств.

Прозрачное шифрование позволяет защитить различные конфиденциальные данные: от номеров кредитных карт и банковских реквизитов до номеров социального и медицинского страхования. Значительным преимуществом прозрачного шифрования является тот факт, что зашифрованные данные видны в своем первоначальном виде для разработчика базы данных или для пользователя, имеющего доступ к базе данных, что значительно упрощает манипуляцию данными для ИТ-специалиста.

Теперь стоит рассмотреть технологию прозрачного шифрования данных в рамках системы управления базы данных Oracle Database. Здесь используется аутентификация, авторизация и другие механизмы обеспечения безопасности данных непосредственно в базе данных, но не в файлах данных операционной системы, что и делает их наиболее уязвимыми для злоумышленников. Именно для защиты этих данных предусмотрена поддержка TDE в СУБД Oracle.

Как было отмечено ранее, прозрачное шифрование может применяться по отношению к столбцам таблиц: как к одному, так и ко всем, а также к табличным пространствам. Однако для понимания принципа прозрачного шифрование данных достаточно рассмотреть механизм TDE лишь на уровне колонок. Например, если таблица имеет четыре столбца, два из которых необходимо подвергнуть процессу шифрования то сервер Oracle Database генерирует один зашифрованный ключ. Таким образом, на диске значения обычных столбцов будут храниться в виде текста, а зашифрованные столбцы будут представлены в шифрованном формате. В случае, когда пользователь захочет выбрать зашифрованные столбцы, сервер Oracle прозрачно для приложения извлечет из словаря данных ключ шифрования таблицы, а главный ключ из так называемого «бумажника», который представляет собой файл, защищенный паролем, для хранения ключей шифрования, паролей, а также личных ключей, сертификатов, и находящийся в файловой системе сервера базы данных. На следующем шаге происходит расшифровка данных сервером и возвращение их

пользователю в виде обычного текста. Ключи, с помощью которых и происходит процесс шифрования персональных данных в технологии TDE хранятся в модуле защиты внешне по отношению к базе данных. Таким образом, даже в случае, когда злоумышленник получает доступ к базе данных, он не сможет провести криптоанализ и расшифровать данные без знания пароля бумажника. Этот факт обеспечивает еще один уровень защиты персональных данных в СУБД Oracle.

После рассмотрения технологии прозрачного шифрования данных с теоретической точки зрения стоит взглянуть, как данный механизм ведет себя на практике, а именно – как ИТ-специалист может настроить и установить TDE для своей базы данных в СУБД Oracle.

Первым шагом в этом процессе станет открытие упомянутого выше бумажника и определение его местоположения. Для удобства использования Oracle прописывает путь хранения бумажника в файле sqlnet.ora, который по умолчанию будет иметь значение $ORACLE_BASE/admin/$ORACLE_SID/wallet. Однако можно установить пользовательское значение, прописав в данном файле следующие строки:

ENCRYPTION_WALLET_LOCATION = (SOURCE (METHOD=file) (METHOD_DATA=(DIRECTORY=<пользовательское_значение_директории>)))

После успешного определения расположения бумажника можно приступить к его непосредственному созданию, путем выполнения следующего оператора, который не только создает бумажник в указанном каталоге, но и открывает его для хранения и извлечения главного ключа средствами TDE: alter system set encryption key authenticated by “remnant”; Чтобы шифровать столбцы таблиц, используя средства прозрачного шифрования, все, что достаточно сделать, это добавить к определениям самих столбцов дескриптор ENCRYPT. Однако до этого необходимо решить и установить какой именно тип шифрования будет использоваться и какой будет длина ключа. Стоит отметить, что по умолчанию СУБД Oracle использует алгоритм шифрования AES (Advanced Encryption Standard) с 192-битовым ключом.

Для рассмотрения примера использования шифрования в случае уже существующей таблицы, можно предположить, что в базе данных имеется отношение, определенное следующим образом:

ACCOUNT_NUMBER	NUMBER
ACCOUNT_NAME	VARCHAR(20)
SSN	VARCHAR(10)

При создании этой таблицы не было указано, стоит ли применять шифрование к одному или нескольким ее столбцам, поэтому данные в настоящий момент времени представлены в виде обычного текста. Можно предположить, что требуется применить алгоритм AES с ключом в 128 бит для шифрования столбца SSN. Тогда необходимо выполнить оператор alter table accounts modify (ssn encrypt using ‘AES128’); который не только создает ключ шифрования для указанной таблицы, но и преобразовывает все значения столбца SSN в формат, соответствующий алгоритму шифрования.

Заключение

Встроенные в СУБД Oracle Database механизмы шифрования конфиденциальных данных отвечают нуждам и требованиям современных разработчиков и клиентов к архитектуре и безопасности базы данных. Технология прозрачного шифрования данных полностью интегрирована в систему Oracle, что делает ее использование наиболее удобным для ИТ-специалиста. Но не только удобство и относительная простота использования делают данный механизм одним из самых распространенным в среде разработки и проектирования базы данных, ведь, как было сказано ранее, он обеспечивает очень высокий уровень безопасности и надежности хранения персональных данных пользователей, защищая их даже от угрозы физической кражи.

Библиография

1. А. Нанда, Прозрачное шифрование данных – М.: Oracle Magazine – 2005
2. А. Л. Додохов, А. Г. Сабанов, Исследование применения СУБД Oracle для защиты персональных данных – 2011
3. ArcGIS, Прозрачное шифрование данных (TDE) для рабочей области Reviewer в Oracle. – [Электронный ресурс.]. – Режим доступа: https://desktop.arcgis.com/ru/arcmap/latest/extensions/data-reviewer-guide/admin-dr-oracle/transparent-data-encryption-tde-for-the-reviewer-workspace-in-oracle.htm
4. ISO27000, Обеспечение защиты персональных данных в СУБД Oracle. - [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/obespechenie-zaschity-personalnyh-dannyh-v-subd-oracle