УДК 621.3

АНАЛИЗ НАДЕЖНОСТИ ЗАЩИТЫ БАЗ ДАННЫХ МЕТОДАМИ СОВРЕМЕННОЙ КРИПТОГРАФИИ

Федосевич Э.А.

Научный руководитель – Сапожникова А.Г.

В работе приведены результаты сравнительного анализа надежности, технологичности и удобства пользователей при различных методах реализации криптографической защиты баз данных в зависимости от целей и задач такой защиты. Показано, что при естественных предположениях о возможностях потенциального злоумышленника (противника) криптографическая защита данных в основных распространенных типах баз данных может обеспечить наибольшую надежность защиты при минимальных затратах по сравнению с любым другим способом защиты данных, не внося значительного неудобства в работу пользователей.

Современная криптография позволяет наиболее эффективно решать многие практические задачи в области зашиты информации, которые возникают перед организацией, использующей компьютеры. В частности, задачу зашиты баз данных, которая в силу требований действующего законодательства и в силу практической необходимости на сегодняшний день стоит практически перед каждой реально работающей организацией.

Во многих случаях для решения задачи надежной защиты базы данных чисто организационных мер и встроенных в систему управления базами данных средств зашиты оказывается недостаточно. Например, немаловажной особенностью зашиты информации в базах данных является наличие файлов-триггеров, с помощью которых выполняются запросы. В таких файлах данные для запросов хранятся в открытом виде. При наличии у злоумышленника физического доступа к месту установки системы управления базой данных, просмотр информации, содержащейся в триггерах, не составляет труда.

Криптографические методы зашиты данных, хранимых и обрабатываемых как записи базы данных можно грубо разделить на два основных класса: методы защиты от несанкционированного просмотра данных при помощи их шифрования как в процессе хранения, так и процессе передачи по каналам связи на компьютеры пользователей: методы авторизации доступа пользователей к различным разделам базы данных, а также аутентификации блоков данных (записей базы данных)

Шифрование непосредственно записей базы данных (или даже отдельных их частей) на различных ключах при использовании современных стойких алгоритмов позволяет радикально решить проблему надежного разграничения доступа к различным разделам базы данных и не нуждается в больших затратах на физическую защиту непосредственно самих носителей данных.

Аутентификация отдельных разделов базы данных, отдельных записей или даже отдельных их наиболее важных частей с помощью технологии электронной подписи позволяет гарантировать защиту от несанкционированных изменений в базе данных с любой наперед заданной степенью детализации и документирования. Следует отметить тот факт, что на сегодня ни один способ зашиты баз данных, кроме криптографического, не может обеспечить того уровня надежности защиты данных и удобства пользователей, которые обеспечиваются криптографическими технологиями.

Однако, как показывает практика, в опоре исключительно на криптографические методы зашиты баз данных есть и заметные недостатки. Так, достаточно сложная для понимания средним пользователем техника применения криптографических методов, в частности, методов управления ключами шифрования, аутентификации и паролями доступа к данным и ресурсам приводит к тому, что обычный пользователь невольно «перепоручает» большинство своих обязанностей по работе с ключами системным администраторам. А это, в свою очередь, приводит к таким явлениям как несанкционированный доступ

администраторов баз данных даже к тем их разделам, к которым они доступ заведомо иметь не должны.

Наиболее надежным и удобным, как для пользователей, так и для администраторов базы данных, представляется такой, при котором шифруются отдельные записи на индивидуальных ключах, причем сам процесс шифрования и расшифрования блока данных происходит на компьютере пользователя. а его индивидуальный пользовательский ключ для шифрования данных позволяет сформировать только ключи шифрования расшифрования тех записей базы данных, доступ к которым ему разрешен. При этом пользовательские криптографические ключи могут генерироваться и храниться в защищенной памяти аппаратного токена пользователя. Такого рола схема управления ключами может быть построена по принципу, описанному в работе.

Кроме того, представляется заманчивым использовать гомоморфные шифры, которые позволяют осуществлять управление базой данных непосредственно с шифрованными записями и не требуют предоставления прав доступа к данным администраторам базы.

Для этого должны быть разработаны достаточно эффективные гомоморфные шифры, которые бы не замедляли работу базы данных на порядок. Это – предмет дальнейших исследований и разработок.

Современные криптографические методы зашиты данных не имеют альтернативы ни по надежности зашиты, ни по эффективности и удобству пользователей. Однако, неправильное или неаккуратное их применение, в частности, нерешенные проблемы управления ключами пользователей могут свести на нет все эти преимущества.

Важным фактором при выборе криптографических методов зашиты в базах данных является структура хранения информации в базах данных и необходимость ее удаленной обработки. Существуют два основных принципа зашиты данных на удаленном сервере. Первый предполагает выполнение операций с данными через систему управления базой данных на компьютерах пользователей или промежуточных серверах (прокси-серверах). При такой схеме зашиты применяется один тип шифрования ко всей базе данных.

Второй принцип зашиты предполагает применение разных типов шифрования для различных полей таблицы, при этом на прокси-серверах кодируются сами данные. При таком применении криптографических методов зашиты производить операции над данными и устанавливать систему управления базой данных можно на удаленном сервере (или в облачной инфраструктуре).

Обеспечение эффективной защиты информационных ресурсов предполагает соблюдение высоких критериев комплексности, как необходимого условия сохранения конфиденциальности критически важной информации практически в любых областях деятельности. Система безопасности баз данных представляет собой комплексное решение защиты информации.

Криптография представляет собой лишь часть такой комплексной защиты. В многоуровневой системе безопасности – это последний внутренний уровень защиты. Она используется для аутентификации пользователей, невозможности отказа от совершенного действия (non-repudiation), шифрования пользовательских данных для защиты от несанкционированного просмотра.

Шифрование в криптографии представляет собой способ скрытия данных с помощью ключа или пароля, т. е. хранение и передачу особо важных данных в зашифрованном виде. Исходные данные невозможно получить из зашифрованных без знания соответствующего ключа или пароля для дешифрования. Могут использоваться как симметричные (одноключевые), так и асимметричные (двухключевые) криптосистемы.

В серверах БД на этапе подключения к БД производится идентификация и аутентификация (проверка подлинности) пользователей. В дальнейшем пользователь или процесс получает доступ к данным согласно его набору полномочий. В случае разрыва соединения пользователя с базой данных текущая транзакция откатывается, и при

восстановлении соединения требуется повторная идентификация пользователя и проверка его полномочий.

Наиболее общий способ идентификации и аутентификации – использование имени и пароля. Эта информация оценивается системой для определения, является ли субъект допустимым пользователем. В серверах БД пароли хранятся в зашифрованном виде. Применяется шифрование на основе алгоритма MD5, который использует необратимую хэш-функцию. Требование необратимости обязательно, иначе пароли можно будет получить, используя обратимое шифрование данных. Алгоритм MD5 является усовершенствованным алгоритмом MD4. Алгоритм используется для проверки подлинности данных, когда происходит их передача в зашифрованном виде. Следует отметить, что алгоритм MD5 уязвим к некоторым атакам, например, возможно создание двух сообщений с одинаковой хэш-суммой.

С широким распространением в современном мире электронных форм документов (в том числе и конфиденциальных) и средств их обработки особо актуальной стала проблема установления подлинности и авторства безбумажной документации. Реализация требования невозможности отказа не позволяет, кому бы то ни было отрицать, что он отправил или получил определенный файл или данные. В конце обычного письма или документа исполнитель или ответственное лицо ставит свою подпись. В конце электронного документа ставится электронная цифровая подпись, которую получают, используя алгоритм цифровой подписи, основанный на использовании асимметричных криптоалгоритмов. Например, в основу алгоритма цифровой подписи DSA (Digital Signature Algorithm) в стандарте DSS (Digital Signature Standard), положены асимметричные криптоалгоритмы Эль-Гамаля и RSA. При возникновении споров отказаться от подписи невозможно в силу ее неподделываемости, проверить подлинность подписи может любой абонент, знающий открытый ключ.

Что касается шифрования пользовательских данных, то процесс шифрования данных в серверах БД претерпел значительные изменения. Ранее использовалась концепция API, который позволяет обращаться к провайдерам службы шифрования – Cryptographic Service Provider (CSP), реализующим тот или иной алгоритм шифрования. Процедура шифрования была достаточно сложной. Например, в MS SQL Server (до 2005 версии) шифрование реализовывалось с помощью команд API, которые вызывались специальными командами из библиотек MSSQLCryptography.dll [4].

Сложность так же заключалась в объеме кода, который необходимо было прописать для подключения библиотек, обработки ошибок и включения самого шифрования. В него входило объявление библиотек, передача дескриптора, указатели начала и конца текста, размер входных данных и буфера и др. Кроме того при переполнении буфера вызывалась ошибка, которая позволяла исключить возможность извлечения секретных данных путем заполнения буфера лишней информацией.

В настоящее время большинство серверов БД имеют встроенные механизмы шифрования и шифрование стало более доступно и менее ресурсозатратно. Но наличие встроенных механизмов не исключает использования библиотек CryptoAPI, который широко используют приложения БД.

Обычно сервер БД поддерживает несколько встроенных механизмов шифрования: специальные функции шифрования, асимметричные ключи, симметричные ключи, сертификаты, прозрачное шифрование данных – TDE.

Специальные функции шифрования вызываются с передачей параметров. В этом случае можно шифровать отдельные элементы по мере того, как они вставляются, или обновляются в базе данных. Для их вызова удобнее всего использовать хранимые процедуры и триггеры сервера БД.

Асимметричные ключи. Асимметричный ключ состоит из закрытого ключа и соответствующего открытого ключа. Отправитель шифрует данные при помощи открытого ключа получателя, который свободно может получить любой человек или программа. Когда пользователь получает данные, он расшифровывает их при помощи своего закрытого ключа.

Открытый ключ в этом случае расшифровать данные не может. На выполнение асимметричных операций шифрования и дешифрования требуется сравнительно много ресурсов, но они обеспечивают более надежную защиту, чем симметричное шифрование. Асимметричный ключ можно использовать для шифрования симметричного ключа перед его сохранением в базе данных. Использование в асимметричном шифровании пары ключей (в сравнении с симметричным шифрованием, у которого используется только один ключ) повышает сложность криптоанализа для злоумышленника. Обычно в серверах БД встроена реализация асимметричного алгоритма RSA с ключами длиной 512, 1024 и 2048 бит. Чем длиннее ключ, тем сложнее осуществить его вскрытие, но и тем дольше будут выполняться операции шифрования и дешифрования.

При использовании асимметричных криптоалгоритмов возникает проблема распространения множества открытых ключей, которая решается с помощью построения Инфраструктуры Открытых Ключей (Public Key Infrastructure – PKI), на основе базы данных цифровых сертификатов.

Симметричные ключи используются как для шифрования данных, так и для шифрования других ключей. При шифровании симметричными ключами отправитель и получатель имеют один и тот же ключ. Главное преимущество такого подхода состоит в том, что производительность шифрования и дешифрования гораздо выше, чем при использовании асимметричных ключей. Данные при использовании симметричного ключа шифруются и дешифруются быстро, и он вполне подходит для повседневной защиты конфиденциальных данных, хранящихся в базе данных. Обычно в серверах БД встроена реализация нескольких наиболее распространенных и надежных симметричных алгоритмов, как блочных, так и поточных: DES, Triple_DES, Triple_DES_3KEY, DESX, RC2, RC4, RC4_128, AES с ключами длиной 128 (Rijndael), 192 и 256 бит.

Сертификаты – это по существу асимметричные ключи, которые содержат дополнительные метаданные. Эти метаданные включают в себя такую информацию, как время окончания и центр сертификации, выдавший данный сертификат. В случае если необходимо удостовериться в том, что отправитель или получатель данных является тем за кого себя выдает, сертификаты помогают решить эту проблему. Центры сертификации создают сертификат со своей подписью, который отправляется тому пользователю, который его заказал. Когда он будет использовать этот сертификат для отправки данных, получатель сможет проверить его в центре сертификации и удостовериться в подлинности отправителя. Отличие сертификатов от ключей состоит в задании промежутка времени, в течение которых они действуют и уникальных метаданных, указывающих на владельца сертификата. Существуют самозаверительные сертификаты. Например, в своих последних версиях MS SQL Server автоматически создает самозаверительный сертификат при своем первом запуске. Этот сертификат используется для шифрования подключения при выполнении аутентификации MS SQL Server. TDE (Transparent Data Encryption) – прозрачное шифрование данных. Прозрачное шифрование данных (TDE) является особым случаем шифрования с использованием симметричного ключа.

Литература

1. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М. : ДМК Пресс, 2012. – 592 с.

2. Баричев, С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М. : Горячая линия – Телеком, 2001. – 120 с.

3. Назначение Secret Disk Server NG // http://www.aladdm-rd.ru/catalog/secret_disk/server/2016/.