передающей и принимающей станциями. Это позволяет обеспечить защиту от имитопомех. Однако характеристики декаметрового канала радиосвязи требуют оптимизации данных методов, чтобы формируемый алгоритм защиты информации обеспечивал требуемый уровень безопасности при имеющихся ограничениях канала передачи.

Список использованных источников

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с анг. – М.: Издательский дом «Вильямс», 2003. – 1104 с. : ил. – Парал. тит. англ.
2. Ступницкий М. М., Лучин Д. В. Потенциал КВ-радиосвязи – для создания цифровой экосистемы России// Электросвязь. – 2018. – № 5.
3. Технологии GPS. [Электронный ресурс]. – Режим доступа: http://www.univers-spb.ru/technologys/gps.php (10.05.2019).
4. Корсунский А. С. Анализ протоколов аутентификации абонентских терминалов в сетях подвижной радиосвязи// Автоматизация процессов управления. – 2009. – №4.
5. Шифрование и защита информации. TETRA. [Электронный ресурс]. – Режим доступа: http://kunegin.com/ref8/tetra/tetra5.htm (14.05.2019).

20.53.17

ПОДГОТОВКА К РАЗРАБОТКЕ ПРОГРАММЫ ШИФРОВАНИЯ ПРОГРАММИРУЕМЫХ ОБЪЕКТОВ БД

Автор: Кригер Роман Владимирович, студент 4 курса кафедры информационных технологий Государственного университета «Дубна» (филиал Протвино).

Научный руководитель: к.т.н., доцент Нурматова Елена Вячеславовна, заведующий кафедрой информационных технологий Государственного университета «Дубна» (филиал Протвино).

Аннотация

В данной статье рассмотрены способы шифрования БД, а также готовые решения для обеспечения безопасности БД. Это сделано для последующей разработки программного обеспечения для шифрования программируемых объектов БД.

Ключевые слова: шифрование, безопасность, база данных, SQL Server.

Annotation

This article describes the methods of database encryption, as well as ready-made solutions for database security. This is done for the subsequent development of software to encrypt programmable database objects.

Keywords: encryption, security, database, SQL Server.

Актуальность темы обосновывается тем, что информация разной структуры и степени важности на электронных носителях часто не защищена, вследствие чего данные могут пострадать. Примерами несанкционированных действий пользователей клиент-серверных приложений могут быть удалённые случаи взлома сервера, удаления базы данных и изменения её на сервере. И в том случае, даже когда есть бэкап для последующего восстановления БД, хакер всё-равно будет иметь доступ к тем данным, которые он украл. Это может являться причиной крупных потерь в компании, которая не позаботилась о своей безопасности.

Объектом данной работы является база данных, созданная и управляемая СУБД SQL Server.

Предметом исследования данной работы является шифрование данных и других объектов данной СУБД.

Цель исследования – разработка и использование приложения криптографического преобразования данных и прочих программируемых объектов в SQL Server, как дополнительной меры по обеспечению информационной безопасности объектов СУБД.

Задачи:

1) Ознакомиться с имеющимися продуктами для шифрования данных БД;
2) Изучить модель шифрования различных объектов SQL Server;
3) Разработать криптоалгоритмы для преобразования файлов текстового формата (например, *.sql).

Существует не так много готовых решений для автоматизации шифрования данных, и в основном они используются в БД не под управлением SQLServer. В качестве примера можно привести популярный сервис от Amazon - *AWSSecretsManager*. Его описание гласит, что «сервис предоставляет возможность простой ротации и извлечения данных для доступа к БД, ключей API и других конфиденциальных данных, а также управления ими на протяжении всего жизненного цикла». Как мы можем понять, AWSSecretsManager отвечает за безопасность данных для доступа к самой БД, но он не шифрует сами данные, которые находятся в БД. Не будем спорить, это хорошее решение для сохранности безопасности данных, но перед нами стоит задача немного поинтереснее.

Перейдём к следующему решению, но уже от отечественных разработчиков. В недалёком прошлом компания *Spelabs* анонсировала продукт, организующий дополнительную безопасность бухгалтерских 1С на уровне шифрования данных, причем на полностью прозрачном уровне. Пользовательские приложения не подозревали о надстройке и работали в обычном режиме. Но вскоре разработка и поддержка этого ПО прекратилась.

Возможность шифрования данных более серьёзно реализована в *Postgres Pro* – СУБД от российских разработчиков. В ней реализованы следующие возможности: шифрование хранимых паролей, шифрование избранных столбцов, шифрование раздела данных, шифрование паролей при передаче по сети, шифрование данных при передаче по сети, проверка подлинности сервера SSL, шифрование на стороне клиента.

Так же есть программа *xpcrypt*, которая, по сути, автоматизирует весь процесс шифрования, который можно произвести вручную. Однако, на официальном сайте последнее обновление было в 2011 году, поэтому можно сказать о том, что разработчик прекратил поддержку своего *soft*-а.

Модель шифрования SQL Server

В SQL Server при создании нового файла БД можно применять ключи шифрования. Это делается для защиты данных, информации об учетных данных, а также соединениях, которые хранятся в серверной БД.

Данная модель в основном даёт функции управления ключами шифрования, которые соответствуют такому стандарту, как ANSI X9.17. В нём определены несколько уровней ключей шифрования, которые используются для шифрования других ключей, те, в свою очередь используются для шифрования данных.

Главный ключ службы Service master key (SMK) - это ключ верхнего уровня и предшественник всех ключей в SQL Server. Он создается или изменяется при помощи оператора ALTER SERVICE MASTER KEY. SMK - асимметричный ключ, шифруемый с использованием Windows Data Protection API (DPAPI). SMK автоматически создается, когда шифруется какой-либо объект. Так же он привязан к учетной записи службы SQL Server. SMK используется для шифрования главного ключа базы данных Database master key (DMK).

Второй уровень иерархии ключей шифрования - DMK. С его помощью шифруются симметричные ключи, асимметричные ключи и сертификаты. Каждая база данных располагает лишь одним DMK.

На следующем уровне содержатся как симметричные и асимметричные ключи, так и сертификаты. Симметричные ключи - основа шифрования в базе данных. Компания Microsoft рекомендует шифровать данные только с помощью симметричных ключей. Помимо этого, в SQL Server, начиная с версии 2008, есть сертификаты уровня сервера и ключи шифрования базы данных для прозрачного шифрования данных.

Зашифровывать другие объекты БД, такие как: таблицы, секции, представления, хранимые процедуры, триггеры и пр. можно при помощи опции WITH ENCRYPTION. SQL Server использует для шифрования операторов SQL тот же метод, что и для паролей. Этот метод обеспечения безопасности окажется полезным, если стоит необходимость в том, чтобы определенные классы пользователей знали, к каким таблицам осуществляется доступ.

Способы шифрования SQL Server

В SQL Server есть следующие способы шифрования:

- шифрование на уровне ячеек;
- прозрачное шифрование данных;
- шифрование на транспортном уровне;
- шифрование на уровне файлов через Windows.

Шифрование на уровне ячеек. Начиная с версии 2005, доступна возможность шифровать и дешифровать данные на сервере. Делать это можно разными способами. Например, с использованием одним из следующих методов: пароль, сертификат, симметричный ключ, асимметричный ключ.

Прозрачное шифрование данных. В SQL Server 2008 появилась возможность зашифровать всю базу данных с использованием прозрачного шифрования. При таком шифровании можно защитить базы данных без изменения существующих приложений, структур баз данных или процессов. Так же прозрачное шифрование данных шифрует базы данных в реальном времени, по мере внесения записей в файлы (*.mdf) базы данных SQL Server и файлы (*.ldf) журнала транзакций.

Шифрование на транспортном уровне. В SQL Server учтено два варианта шифрования данных, передаваемых по сети между экземпляром СУБД и клиентским приложением. Ими являются IPsec и SSL. Первый реализован на уровне операционной системы и обеспечивает проверку подлинности с использованием Kerberos, сертификатов и общих ключей. IPsec обеспечивает прозрачные для приложений службы шифрования с надежной фильтрацией для блокирования трафика по протоколам и портам. SSL же, проверяет сервер, когда клиент запрашивает шифрованное соединение. Если экземпляр SQL Server функционирует на компьютере с сертификатом от публичного удостоверяющего центра, то удостоверение компьютера и экземпляр SQL Server гарантируют, что цепочка сертификатов ведет к корневому центру сертификации. Для такой проверки на стороне сервера требуется, чтобы компьютер, на котором функционирует клиентское приложение, доверял корневому удостоверяющему центру, используемому сервером. Возможно шифрование с использованием самозаверяющего сертификата, но защита самозаверяющего сертификата ненадежна.

Шифрование на уровне файлов через Windows. Весь каталог данных SQL Server можно зашифровать с использованием Encrypting File System (EFS), компонента шифрования операционной системы Windows и более новых версий.

Разработка приложения для шифрования

В основе разработке ПО лежит вопрос о выборе способа шифрования БД под управлением SQL Server. В результате рассмотрения всех способов, был сделан выбор в пользу шифрования на уровне файлов.

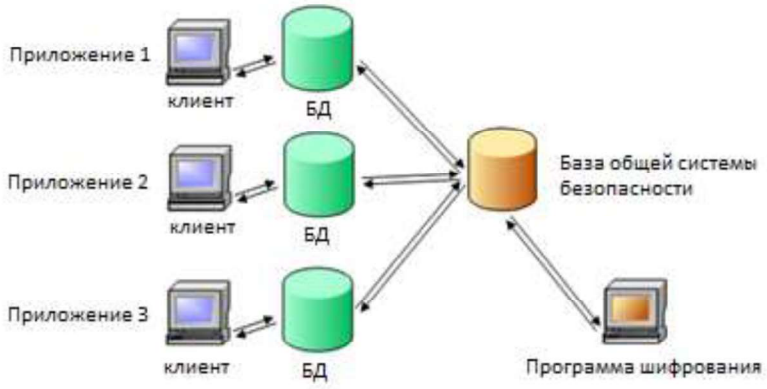

Рисунок 1 – Схема организации безопасности объектов БД

На уровень базы общей системы безопасности дополнительно можно вынести:

- добавление, удаление, изменение учётных записей пользователей;
- контроль над подключениями;
- фиксирование событий в логе.

Список использованных источников

1. Документация по AWS Secrets Manager // Amazon – URL:https://aws.amazon.com/ru/secrets-manager (дата обращения: 15.10.2019).
2. Нурматова Е.В. Разработка БД [Электронный ресурс]: лабораторный практикум/ Е.В. Нурматова, Е.В. Крехов – М.: РТУ МИРЭА, 2018. – 77 с. – Режим доступа: https://library.mirea.ru/share/2910
3. Статья о способах защиты данных в таблице БД// Хакер – URL:https://xakep.ru/2009/06/02/48406/(дата обращения: 15.10.2019).
4. Статья о шифровании в БД SQL Serverhttp://www.itshop.ru/Shifrovanie-v-bazah-dannyh-SQL-Server/l9i36233(дата обращения: 15.10.2019).

81.93.29

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ПК ОТ АТАК ВРЕДОНОСНЫХ ПРОГРАММ

Автор: Ксензук Александр Александрович, студент 4 курса УЦ «Интеграция» МАИ

Научный Руководитель: к.п.н, доцент Васильев Геннадий Иннокентьевич, доцент МАИ

Аннотация

Вопрос безопасности и защиты всегда стоял перед пользователями персональных компьютеров, но на сегодняшний день как никогда растет осознание того, насколько важна безопасность персональных данных. Если не принимать различные меры для зашиты от вирусов, то следствия заражения могут быть очень серьезными. В данной статье мы разберем основные мотоды защиты ПК от атак вредоносных программ и посмотрим с помощью каких средств можно защититься.