Технические решения для безопасности данных в ORACLE.

Программные средства Oracle поддерживают механизмы безопасности, основанные на стандартных алгоритмах защиты и встроенных методах работы с объектами для поддержания и сохранности хранимой в базе информации. О надежности системы безопасности говорит тот факт, что СУБД Oracle получила Сертификат №168 от Государственной технической комиссии при Президенте РФ соответствующий системе сертификации средств по требованиям безопасности №РОСС RU.0001. Данный сертификат удостоверяет, что встроенные в Oracle 8 и выше элементы системы управления распределенными базами данных и промышленными серверами соответствует требованиям Руководящего документа Гостехкомиссии России. Полученный сертификат соответствует классу защищенности 1В (1V). Полученный сертификат был внесен в Государственный реестр сертифицированных средств защиты информации. Данный сертификат рекомендован к использованию в государственных учреждениях. Уровень защищенности серверов БД Oracle позволяет использовать их в системах обработки информации, хранящих Государственную тайну. На данный момент не существует СУБД, который получили сертификат Гостехкомиссией более высокого класса защищенности. СУБД Oracle также обладает Аттестатом Соответствия уровня требования безопасности, установленным приказом МО РФ №423 (Аттестат №234) что позволяет ему быть использованным на объектах МО РФ. СУБД Oracle8i Release 3 (на текущий момент выпущено Oracle 9.0.2 и на стадии тестирования находится Oracle 10) и выше поддерживает и активно использует мощный стандарт тройного шифрования данных (Triple DES), который позволяет надежно защищать хранящуюся в базе данных информацию. Вопросы безопасности в корпоративной среде на основе продуктов Oracle решаются с использованием трех компонентов системы: администрированием сервера БД Oracle используя встроенные и поставляемые дополнительно средства, управление серверами приложений на основе продуктов Oracle и средствами настройки Oracle Applications/Приложения Oracle. Используя три уровня защиты, в совокупности с аппаратными методами, выполняющими контроль сетевого трафика на различных участках корпоративной сети, позволяет администратору реализовать наиболее надежную и полную систему безопасности предупреждающей несанкционированный доступ и утечку финансово-промышленной информации конфиденциального характера.

Работа с пользователями.

Основа безопасности в Oracle работа с пользователями.
На все операции в базе данных пользователю предоставляется разрешение в виде привилегии. Различают системные и объектные привилегии. Системные привилегии дают право манипулировать объектами базы данных. Объектные привилегии позволяют манипулировать с данными в объектах. Для работы с базой данных пользователь должен быть авторизован, и должен пройти идентификацию. Каждый пользователь имеет имя и пароль. Администратору базы данных обладает возможностями работы с паролями пользователей, задавать длину, сложность и срок его действия пароля. Все пароли хранятся в базе данных в зашифрованном виде, причем длинна зашифрованного пароля, постоянна и равна 16 байт. Для шифрования пароля применяется один из следующих методов хеширования.

1. MD4 – 128-битный алгоритм хеширования
2. MD5 – улучшенная и более сложная версия MD4
3. SHA – Secure Hash Algorithm, который производит 160-битное хеширование, длиннее чем MD5. Алгоритм немного медленнее, чем MD5, но большее количество значений делает его более защищенным против совпадений и атак на проникновения.
4. UNIX Crypt – UNIX шифрующий алгоритм
5. No Encryption – Не шифровать данные.

Причем одинаковые пароли имеют разные зашифрованные последовательности. После ввода пользователем пароля, система кодирует его и сравнивает его с зашифрованным паролем в системе. Если зашифрованный введенный пароль и хранящийся в базе совпадают, то пользователь считается идентифицированным. Допускается также идентификация средствами операционной системы. Существуют способы, для администратора, использования зашифрованных паролей для входа в систему под именем пользователя, хотя для этого нет оснований, поскольку администратор владеет всеми правами для доступа к информации пользователя. Существует также большое число приемов работы с пользователями для увеличения уровня защищенности данных в базе, на уровне представления информации.

Шифрование данных на сервере.

В базе данных Oracle предусмотрены средства шифрования (криптозащиты) данных на основе технологии Oracle Advanced Security при передаче данных из базы и обратно. Встроенные возможности шифрования защищают наиболее ценную информацию даже от очень привилегированных пользователей, которые могут превысить свои полномочия, а также от злонамеренных пользователей, пытающихся прочесть файлы данных из операционной системы. По выбору пользователя могут применяться известные алгоритмы шифрования:

- 3DES112: Тройной DES (размер ключа 112 бит)
- 3DES168: Тройной DES (размер ключа 168 бит)
- DES40: DES40 (размер ключа 40 бит)
- DES: Стандартный DES (размер ключа 56 бит)
- RC4_40: RSA RC4 (размер ключа 40 бит)
- RC4_56: RSA RC4 (размер ключа 56 бит)
- RC4_128: RSA RC4 (размер ключа 128 бит)
- RC4_256: RSA RC4 (размер ключа 256 бит)

Избирательное шифрование сохраненных данных

Для избранных приложений, можно указать шифровать данные для дополнительной степени защищенности. С особо ценной информацией можно будет работать, выполнив идентификацию и получив доступ, чтобы быть уверенным, что лишь пользователи с достаточными правами получают к ней доступ.

Стандартные алгоритмы шифрования использующиеся в Oracle.

Некоторые стандартные алгоритмы шифрования полезные при шифровании данных на сервере. Два наиболее распространенных.

Data Encryption Standard (DES)	Производит стандартное шифрование частных данных.
Triple DES (3DES)	Шифрование тройным алгоритмом DES.

Стандартные средства защиты. Ограничение имен доменов и IP-адресов

Сервер приложений позволяет отслеживать входящие IP адреса и домены, либо разрешать, либо запрещать доступ для конкретных IP-адресов и имен доменов (как разновидности представления IP-адресов). Для примера, часть имени домена может содержать универсальный шаблон-маску, так что строки типа *.mipt.ru запретят доступ всем клиентам, не входящих в структуру "МФТИ".

Использование Firewall для защиты сервера приложений

Существует несколько разновидностей построения защиты от попыток проникновения в корпоративный Web-узел, с использованием аппаратных средств "защитных стен" так называемых Firewall. Web-сервер приложений Oracle находится между двумя Firewall, внутренним и внешним. Внешний Firewall поддерживает прослушеватель SQL*Net Oracle. Внешний Firewall защищает Web-сервер приложений от прямых атак из внешней интернет-сети, он же выполняет механизм SSL шифрования запросов, посылаемых Web-сервером приложений во внешнюю сеть. Внутренний Firewall осуществляет дополнительную защищенность участка между Web-сервером и сервером базы данных приложений Oracle (так называемая трехуровневая архитектура), он также может поддерживать свой дополнительный SSL протокол шифрования SQL запросов на своем участке сети.

Авторизация через сеть с использованием SSL (Secure Sockets Layer)

Сертифицированная цифровая идентификация

Соединяясь с базой данных через браузер (например, на Web-сайте), браузер предлагает ему ввести имя и пароль. Администратор базы данных имеет возможность определять, будет ли пароль при передаче кодироваться, также он может определять алгоритм кодирования. Для шифрования идентификационных данных, можно использовать SSL (Secure Sockets Layer). SSL является частью стандартного протокола HTTP, он используется при передаче данных по открытым каналам связи, через Internet, на сервер приложений или в базу данных. Пользователь и Web-сервер приложений видят незашифрованные данные, хотя для любого постороннего человека, который пытается подсмотреть данные "в середине транзакции" (то есть в процессе пересылки имени и пароля пользователя), они представляются в зашифрованном виде. Протокол SSL поддерживается всеми поставщиками интернет-браузеров. Кроме поддержки протокола SSL, Oracle Developer выполняет обязательное шифрование данных, передаваемых на открытых участках сети между клиентской машиной и сервером приложений, с применением алгоритма шифрования RSA RC4 (с 40-битным ключом) и поточного, симметричного шифрования с длиной ключа 128 бит. Java-машина идентифицирует загружаемый апплет на проверку соответствия "свой/чужой", используя стандарт DSA X.509, до выполнения на клиентской части.

SSL - стандартный протокол, использующийся для защищенного соединения по сети. Проводит идентификацию посредством обмена сертификатами.

Можно использовать SSL в одном из трех идентификационных видов:

SSL вид	Описание
Без идентификации	Ни клиент, ни сервер не идентифицируют себя. Не происходит обмена сертификатами. В этом случае, только SSL шифрование /дешифрование используется.
Односторонняя идентификация	Только directory server идентифицирует себя клиенту. Directory server шлет клиенту сертификат подтверждающий, что сервер защищен.
Двухсторонняя	И клиент и сервер идентифицируют себя друг другу. И клиент и сервер шлют друг другу сертификаты.

Компоненты SSL включают в себя:

Сертификат/Certificate

Сертификат удостоверяет, что данная идентификационная информация правильная и публичный ключ действительно соответствует организации. Сертификат создается когда публичный ключ организации подписывается доверенной организации, это идентификация сертификата (CA). Сертификат содержит название организации публичный ключ, серийный номер, дату окончания. Он может содержать информацию о привилегиях связанных с сертификатом. Сертификат действителен до даты его окончания или до его аннулирования.

Доверенный сертификат/Certificate Authority

Certificate Authority/Доверенный Сертификат доверенная третья сторона которая, удостоверяет, что владелец сертификата именно тот, кому он выдан. Certificate authority, подтверждает идентификацию владельца и предоставляет сертификат, подписанный секретным ключом CA.

Каждая сетевая организация имеет список заверенных сертификатов. Перед приемом или передачей данных с другим объектом в сети, данная точка использует этот лист, чтобы удостовериться, что подпись на сертификате другого объекта из соответствует доверенному источнику CA. Различные сущности в сети могут получать сертификаты от одного или разных распространителей Доверенных сертификатов.

Бумажник/Wallet

Бумажник/Wallet некий собирательный инструмент, используемый для упрощения сохранения и управления идентификационной информацией. Бумажник сохраняет ключи, сертификаты, и доверенные сертификаты, то есть то, что используется в SSL. В окружении Oracle, каждая внутренняя система, использующая SSL, имеет бумажник, с сертификатом x.509 версии 3, частным ключом, и листом доверенных сертификатов.

Использование рукопожатия/SSL Handshake в начале работы с пользователями

В течении рукопожатия/SSL handshake, два узла определяют, какой набор шифров они будут использовать для дальнейшей пересылки данных туда и обратно.

В начале соединения, клиент и directory server выполняют SSL handshake/рукопожатие, которое включает в себя 3 важных шага:

1. Клиент и сервер договариваются об алгоритмах шифрования, которые они будут использовать.

2. Сервер шлет сертификат клиенту. Клиент удостоверяется что сертификат заверен надежной третьей стороной. Аналогично, если необходимо клиент шлет свой сертификат серверу.

3. Клиент и сервер обмениваются ключевой информацией, используя шифрование публичным ключом, используя эту информацию каждый генерирует ключ сессии. Весь последующий диалог между клиентом и сервером шифруется и дешифруется, используя этот ключ сессии и установленным набором шифров.

Набор шифров, поддерживаемый в Oracle для использования с SSL

Набор шифров это определенный набор алгоритмов идентификация, шифрования, и сохранения целостности данных используемых для передачи посланий сетевыми узлами.

Средства работы с шифрованием в Oracle, Oracle Internet Directory, поддерживает следующие SSL наборы шифров:

Набор шифров	Авторизация	Шифрование	Целостность данных
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES40	SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RC4_40	MD5
SSL_RSA_WITH_NULL_SHA	RSA	Нет	SHA
SSL_RSA_WITH_NULL_MD5	RSA	Нет	MD5

Авторизация через сеть с использованием Kerberos и Cyber SAFE

Oracle Advanced Networking Option/Расширенные Сетевые свойства Oracle представляет поддержку Kerberos и CyberSAFE. Kerberos и CyberSAFE предоставляет удобство предъявления пароля и централизованного хранения и идентификации в окружении Oracle. Адаптер идентификации (работающий с системой защиты в сети) расположен ниже интерфейса Net8 и позволяет существующим приложениям использовать преимущества новых систем идентификации прозрачно, без изменений в приложении.

Основная концепция протокола Kerberos очень проста — если есть секрет, известный только двоим, то любой из его хранителей может с лёгкостью удостовериться, что имеет дело со своим напарником. Для этого ему достаточно проверить, знает ли его собеседник общий секрет. Kerberos обеспечивает централизованное сохранение паролей, идентификацию связей баз данных, и поддержку усовершенствованной защиты PC.

Поддержка Kerberos обеспечена в Oracle Advanced Networking Option в двух видах:

- через Адаптер Идентификации Цербер/Kerberos Authentication Adapter.
- через Адаптер Идентификации Cyber SAFE Challenger.

Замечание: Oracle не предоставляет централизованный идентификационный сервер – лишь поддержку идентификационных служб, других производителей или серверов третьей стороны основанных на Kerberos таких как Cyber SAFE. Oracle Corporation обеспечивает распределенный идентификационный механизм, основанном на X.509 v1 сертификате через Сервер Безопасности Oracle/Oracle Security Server.

Авторизация через сеть использующая Token Cards

Token Card предоставляет метод идентификации основанный на двух факторах. Для получения доступа пользователь должен владеть физической карточкой и должен знать пароль. Некоторые Token Cards предоставляют пароль, синхронизированный с идентификационным сервисом. Сервер может сравнить пароль в любой момент, соединившись с идентификационным сервисом. Другие Token Cards работают по принципу запрос-ответ, в котором сервер предлагает запрос (число) и пользователь

возвращает серверу другое число, которое он получил с помощью Token Cards и полученного числа. Token cards предоставляет следующие преимущества:

1. простота использования для пользователя
2. простота управления паролем.
3. простота поддерживания защищенности пароля.

Материал подготовлен по:

Oracle.Help.Security Overview - Документация к Oracle 9

Oracle.Help. Advanced Security Administrator's Guide - Поддержка Администрирования Oracle

http://sunsite.usu.ru/documentation/oracle.8.0.4/network.804/a58229/ch1.htm

http://www.fors.ru/fors/docs/service/safe/oracle-safe.html

http://ixbt.ru