ЦИФРОВЫЕ СЕРТИФИКАТЫ ЗАЩИТЯТ КОММЕРЧЕСКИЕ СЕКРЕТЫ И ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Р.М. Рыжков
«ФОРС — Центр разработки»

Сегодня нет, пожалуй, ни одной компании, которая не задумывалась бы серьезно над проблемой информационной безопасности. Решения и технологии, позволяющие защитить персональный компьютер, корпоративные сети или базы данных, постоянно совершенствуются.

Старейший способ не допустить к своей информации посторонних - организовать доступ к ней через ввод имени пользователя и пароля, иначе говоря, через авторизацию пользователя. По данным авторитетной аналитической компании IDC (www.idc.com), на долю средств авторизации и администрирования (необходимого для надежной авторизации) уже приходится более 70% от общей суммы затрат, связанных с обеспечением информационной безопасности, и инвестиции в эту сферу ежегодно растут на 30%.

Средства опознания пользователя на основе имени и пароля встроены в операционные системы, СУБД и прикладные программы, что обеспечивает определенную степень защиты, но не самую надежную идентификацию. Если сочетание «имя пользователя/пароль» попадет в руки злоумышленника, то он без труда выдаст себя за легального пользователя и информация окажется под угрозой. По этой причине для более безопасного доступа весьма желательным может оказаться применение дополнительных средств. Среди них такие, как идентификация по отпечаткам пальцев, радужной оболочке и сетчатке глаза, а также с помощью смарт-карт и цифровых сертификатов. Использование этих средств, как правило, организуется на уровне прикладного программного обеспечения. На рынке представлены информационные системы, имеющие встроенную возможность строгой аутентификации при доступе к данным.

Можно предложить решение, реализовав механизм строгого управления доступом к своим прикладным системам на основе использования цифровых сертификатов и LDAP-каталогов. В основе лежат технологии Oracle, обеспечивающие строгую аутентификацию пользователей с помощью цифровых сертификатов стандарта X.509. Такое решение не позволяет злоумышленнику, работая под чужим именем, похитить информацию из базы, а также совершить несанкционированный доступ к приложениям, использующим СУБД Oracle.

ПРЕИМУЩЕСТВА

Решение ориентировано на использование в информационных системах, которые хранят и обрабатывают сведения, представляющие коммерческую тайну или персональные данные. Оно может с успехом применяться и в системах, обслуживающих рынок телекоммуникаций. Интерес к обеспечению безопасности данных под управлением СУБД Oracle при помощи технологий смарт-карт проявляют операторы связи, стремящиеся защитить свои биллинговые системы.

По оценкам специалистов, основная угроза утечки информации исходит со стороны сотрудников, имеющих официальный доступ к данным. Привычный способ входа в систему с использованием имени пользователя и пароля (на основе того, что человек знает) практически не позволяет установить, кто же в действительности работает с данными, даже если факт доступа зарегистрирован системой мониторинга. Связано это с тем, что узнать сочетание «имя пользователя/пароль» сравнительно несложно, а потому и трудно утверждать, что несанкционированные действия произвел именно тот, под чьим именем осуществлен вход в систему.

Более безопасным считается доступ в систему на основе того, что человек имеет. Тайно похитить или присвоить на время материальный носитель, хранящий идентификатор пользователя, не так легко, как узнать пароль. Факт пропажи носителя (смарт-карты, eToken и пр.) легко обнаруживается и немедленно вызывает запрет доступа в систему для его владельца. Владелец же смарт-карты несет ответственность за ее сохранность, а утеря может вызвать для него такие же последствия, как утеря ключей от сейфа, пропуска на режимный объект и т. п.

С другой стороны, хищение материальной ценности (носителя) может грозить злоумышленнику теми же неприятностями, что и кража любого другого имущества компании, в то время как ответственность за подглядывание имени пользователя и пароля законом не предусмотрена. Таким образом, вход в систему на основе некоего материального «пропуска» существенно снижает риск получения несанкционированного доступа к информации.

РЕАЛИЗАЦИЯ

Переход от технологий, использующих имя пользователя и пароль, к более надежным методам позволяет значительно усилить безопасность системы, исключить перехват идентификационной информации пользователя потенциальным злоумышленником.

Решение, повышающее безопасность данных, можно построить на основе трех основных компонент:

- использования цифрового сертификата в качестве идентификатора пользователя;
- применения технологий Oracle для организации SSL-соединения LDAP-каталога;
- использования смарт-карты как носителя цифрового сертификата и ключа.

ЦИФРОВОЙ СЕРТИФИКАТ КАК ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ

Цифровой сертификат представляет собой электронный документ, выданный удостоверяющим центром. Традиционно он используется для идентификации владельца сертификата (компании или пользователя) путем проверки содержащегося в сертификате цифрового ключа. Удостоверяющий центр, выдающий сертификаты (Certification Authority, CA), заверяет своей электронной подписью соответствие между открытым ключом и именем (идентификатором) его владельца. Подписанные таким образом данные (открытый ключ, идентификатор владельца и некоторые другие связанные с ним атрибуты) и представляют собой цифровой сертификат. Генерация цифровых сертификатов регламентируется стандартом X.509.

Цифровой ключ, входящий в состав сертификата, также может использоваться для электронно-цифровой подписи и шифрования электронных писем, файлов или трафика, передаваемого по каналам связи. Только определенный получатель может расшифровать сообщение или принятый трафик, при этом он будет уверен, что письмо пришло от легального отправителя и не было изменено при пересылке. Эти и многие другие возможности предусматривает концепция PKI (инфраструктура открытых ключей).

LDAP-КАТАЛОГ И SSL-СОЕДИНЕНИЕ В ORACLE

LDAP-каталог, LDAP-сервер, SSL-протокол - эти понятия сегодня известны всем, кто хотя бы немного интересуется IT-тематикой. Облегченный протокол доступа к каталогу (Lightweight Directory Access Protocol, LDAP) обеспечивает работу клиентских приложений, в том числе «легких» пользовательских агентов, таких как Internet-броузеры, с каталогами, использующими архитектуру X.500. Протокол рассчитан исключительно на использование поверх TCP. Конкретные реализации протокола могут отличаться, например, поддержкой шифрования трафика по SSL 3.0 или проверкой права на установление соединения на основе имени и пароля в операционной системе. Текущая, третья версия этого протокола поддерживает репликацию каталогов и улучшенные средства защиты, в том числе проверку права на установление соединения на основе цифрового сертификата.

Для обеспечения безопасного обмена данными между клиентом и сервером применяется протокол SSL (Secure Sockets Layer), по которому обмен производится в зашифрованном виде. SSL-соединение в реализации Oracle обеспечивает Oracle Advanced Security, осуществляя обмен трафиком между клиентом и сервером по SSL-протоколу, что делает его перехват практически невозможным.

SSL-соединение между клиентом и базой данных обслуживает LDAP - сервер Oracle, называемый Oracle Internet Directory Server. Именно он хранит учетные записи пользователей и связывает их с цифровыми сертификатами и цифровыми ключами, которые могут размещаться в различных хранилищах. На основе цифровых ключей, являющихся частью цифрового сертификата, производится шифрование SSL-трафика.

ИСПОЛЬЗОВАНИЕ СМАРТ-КАРТ

Цифровой сертификат, на основе которого происходит идентификация пользователя, может храниться как в самом компьютере, так и на устройстве, которое владелец носит с собой. Для хранения цифровых сертификатов особенно перспективно применение смарт-карт или USB-ключей eToken, поскольку конструктивные особенности не позволяют похитить цифровой сертификат из их памяти. Впервые технология аутентификации с использованием eToken при доступе к базам данных Oracle была представлена компанией «Аладдин» в апреле 2004 года.

Несомненным достоинством использования технологий смарт-карт для реализации SSL-доступа к БД Oracle является мобильность хранилища сертификатов. В случае размещения сертификатов в традиционных хранилищах (реестр компьютера, файл или Oracle Wallet) для корректной аутентификации необходимо, чтобы доступ осуществлялся с того же компьютера, на котором был выписан сертификат и где зарегистрировано хранилище. При механическом копировании хранилища на другой компьютер аутентификация на основе цифрового сертификата с этого компьютера невозможна. Хранение сертификата на eToken или смарт-карте позволяет пользователю получить доступ к базе и прикладной системе с любого клиентского рабочего места.

ОПИСАНИЕ

Продемонстрируем на примере одного из решений, как выглядит диалог входа в систему при использовании цифровых сертификатов.

1. Традиционное окно входа в систему на основе имени пользователя и пароля в случае авторизации по цифровому сертификату не появляется.
2. При размещении в USB-порте компьютера eToken, хранящего цифровые сертификаты, появляется окно выбора нужного сертификата.
3. Пользователь выбирает сертификат, но для работы с ним система просит предварительно ввести PIN-код eToken.
4. Предлагает стандартный диалог по смене PIN-кода.
5. После этого происходит аутентификация пользователя и запуск системы.