Защита и управление данными в TDMS

Принимая решение о создании собственной системы управления техническими данными, наша компания ясно отдавала себе отчет в том, что мы отнюдь не первые, кто взялся за решение подобной задачи.

Продавая чужие системы и анализируя представленные на рынке отечественные и западные программные продукты, предназначенные для коллективной работы с технической информацией, мы пришли к неутешительному выводу. Помимо наследия устаревшей архитектуры, завышенных цен, запутанных интерфейсов и настроек, многие из этих систем банально не обеспечивали необходимого уровня безопасности хранения и управления данными. Речь не идет об общепризнанных мировых лидерах на рынке PDM/PLM – в этих системах, как правило, всё в порядке и с функциональными возможностями, и с безопасностью. Но по причине высокой стоимости продукта и еще большей стоимости внедрения эти системы недоступны большинству российских предприятий. Явные проблемы с безопасностью обнаружились у систем "среднего класса", к которым относятся все российские продукты и десятки аналогичных западных разработок.

Технические специалисты вряд ли найдут в этой статье что-то новое: мы расскажем об основных принципах, на которых строится система защиты и управления данными в TDMS. Но тем более удивительно, что на российском рынке так трудно найти систему, в которой учтены все столь очевидные требования к построению систем коллективного доступа с целью обеспечения необходимого уровня безопасности.

Выбор СУБД

Первое, на что мы обратили внимание, – это выбор системы управления базами данных (СУБД). Выбор производился по целому ряду критериев: распространенность, удобство работы, масштабируемость и т.д. Одним из определяющих факторов стали требования к обеспечению необходимого уровня безопасности и бесперебойной работы. Многие поставщики сетевого ПО любят рассказывать о многоплатформенности, гибкости и т.д. На деле же часто оказывается, что некоторая часть предлагаемых ими СУБД не может соответствовать требованиям безопасности, а сама гибкость решения, поддерживающего большое количество платформ, дости-

гается за счет упрощения серверной части ПО, игнорирования рекомендаций по защите данных – как следствие, такая СУБД не может использоваться в системах коллективного доступа. Изучая платформы СУБД, мы руководствовались принципом "лучше меньше, да лучше". Выбор для российского рынка был достаточно очевиден: Microsoft SQL Server 2000 и Oracle 9i. Другим возможным вариантом была DB2, но эта система почти неизвестна в России, и потому уже на начальном этапе развития TDMS решено было не тратить ресурсы компании на поддержку еще одной платформы.

И SQL Server, и Oracle имеют сертификаты безопасности уровня C2[1]. Обе системы надежны и обеспечивают круглосуточную бесперебойную работу без вмешательства администратора. Обе имеют многоуровневые системы защиты данных, встроенные средства резервного копирования и мониторинга. SQL Server, пожалуй, самая легкая и удобная в администрировании СУБД, которая одинаково хорошо работает с любыми объемами данных. Oracle же, помимо C2, имеет еще более десяти различных сертификатов безопасности и de facto является стандартом для создания информационных систем масштаба предприятия. Не случайно большинство российских и западных предприятий использует именно SQL Server и Oracle.

Защита БД

Для подключения к серверу БД TDMS использует классическую трехуровневую систему аутентификации. Подключаясь к серверу с "прошитой" учетной записью, пользователь проходит только первый уровень защиты. Подключившись, он получает право запустить процедуру проверки имени и пароля пользователя, а также пароля учетной записи приложения. В базе данных хранятся не сами пароли, а только их цифровые образы, полученные после обработки паролей специальной хэш-функцией.

Такой способ аутентификации позволяет избежать двойного ввода пароля, сохраняя при этом необходимый уровень безопасности.

Стоит отметить, что учетная запись приложения не работает напрямую с таблицами базы данных. Работа приложения осуществляется через хранимые процедуры, обеспечивая соответствие между правами доступа пользователя и разрешенными ему операциями над данными.

Обеспечив защиту на стороне сервера БД, но не позаботившись о необходимом уровне организации коллективного труда в электронной системе, мы предоставили бы расхлябанному пользователю прекрасную возможность творить чудеса, которых вдоволь наелись проектные и конструкторские организации, осуществив массовую компьютеризацию и превратив свои проекты в файловую свалку.

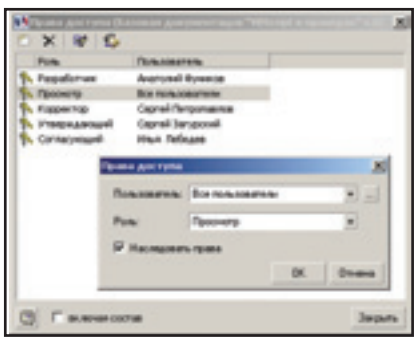
Права доступа

Система TDMS предназначена для коллективной работы с техническими данными и имеет в системе управления правами доступа ряд особенностей, которые отличают ее от "плоских" электронных архивов. К таким свойствам можно отнести возможность назначения прав доступа на каждый объект системы, наследование прав, иерархическую модель администрирования.

Возможность назначения прав на каждый объект означает, что для любого информационного объекта можно определить пользователей или группы пользователей, имеющих определенные права доступа к этому объекту. TDMS обладает гибкими настройками, позволяющими назначать права доступа вплоть до видимости объекта в системе. Для управления правами доступа у каждого объекта TDMS есть администратор. Администраторы TDMS образуют иерархию.

Иерархическая модель управления правами доступа взята из реальной жизни. На любом предприятии есть лицо (директор), которое имеет практически неограниченную власть. Есть люди – скажем, начальники подразделений, – которые находятся в его подчинении. У тех, в свою очередь, в подчинении находятся начальники отделов и т.д. Именно такой принцип администрирования используется и в TDMS. Главный, системный администратор имеет в подчинении группу администраторов рангом ниже. Он может передать им право управления доступом к объектам. Каждому из подчиненных администраторов могут подчиняться другие администраторы и т.д. Члены административной группы, каждый на своем уровне, распределяют права доступа пользователей к объектам. Администратор более высокого уровня может не только изменять права доступа к объекту, установленные подчиненным ему членом административной группы, но и заменить подчиненного администратора любым другим.

Основой модели представления и отображения информации в TDMS также служит древовидная структура. Объекты структурированы по иерархическому принципу, вложенность объектов подчинена заданным при настройке системы правилам вхождения объектов друг в друга. Наследование прав доступа существенно упрощает администрирование системы, построенной по иерархическому принципу. Администратору достаточно лишь один раз определить основной набор прав доступа (как правило, на просмотр), и наследуемые права будут автоматически переноситься на все вновь создаваемые объекты.



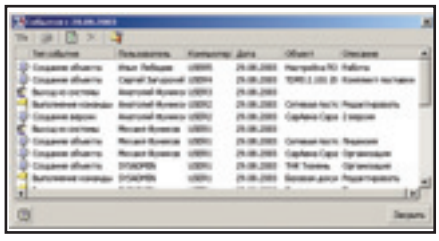
[1]C2 – сертификат безопасности, выдаваемый Национальным агентством безопасности США (NSA).

Любая система документооборота обладает возможностью отслеживать стадии работы с объектом (документом). На разных стадиях жизненного цикла проекта, изделия или отдельного документа пользователи имеют различные ограничения прав доступа к этим объектам. Но как система, предназначенная для работы с техническими данными, TDMS наделена дополнительными функциями по работе с иерархической структурой. Например, без всякого программирования можно задать условия, которые не позволят утвердить документ, если он содержит неутвержденные листы, или утвердить сборочную единицу, в составе которой есть неутвержденные детали.

Такой подход позволяет согласованно вести коллективную разработку проектов, структурированно хранить архивную информацию, строго определив границы прав доступа каждого пользователя по отношению к каждому объекту системы.

Мониторинг действий пользователей

TDMS позволяет фиксировать практически все действия пользователей, касающиеся их работы в системе: создание, просмотр, редактирование, удаление объектов, выполнение запросов, создание версий и т.д. Накапливаемую информацию можно группировать для дальнейшего изучения не только по пользователям или документам, но и по любым другим критериям. Одним словом, в руках системного администратора и службы безопасности находится поистине незаменимый инструмент.



Функции мониторинга могут пригодиться не только для пресечения действий "инсайдеров" и выявления непреднамеренных вредителей. Благодаря информации, полученной в результате мониторинга, добросовестный администратор способен оптимизировать некоторые действия пользователей. Если несколько пользователей ежедневно совершают несколько последовательных однотипных операций, администратор может автоматизировать их действия.

Не стоит забывать и о мониторинге средствами СУБД. Например, аудит уровня C2 Microsoft SQL Server поможет администратору уже на ранней стадии зафиксировать попытки несанкционированного доступа.

История разработки объекта

История разработки объекта не является частью системы безопасности. Но отражая всю информацию об объекте проектирования, связанных с ним почтовых сообщениях, его версиях, этапах и т.д., история разработки позволяет администратору объекта или другому уполномоченному лицу быстро определить, почему и на каком основании были приняты те или иные решения, были ли выполнены все необходимые требования, касающиеся правил разработки технической документации.

Внутренняя почта

Встроенный почтовый модуль является защищенным транспортом для передачи различных системных сообщений, таких как уведомление о начале или окончании разработки, сообщений о назначении пользователя на выполнение определенных работ, различного рода директив. Почта также используется для передачи сообщений от одного пользователя другому в результате маршрутизации документов. TDMS не переносит в почте тела документов – в этом нет необходимости. В почтовом сообщении содержится ссылка на версию документа, что позволяет в любое время одновременно увидеть состояние документа на момент передачи и его текущее состояние. Пользователь не имеет возможности удалить системное сообщение или сообщение, созданное в результате маршрутизации. Открыв TDMS, пользователь обязан открыть пришедшую к нему почту, что практически исключает возможность саботажа или элемент рассеянности.

Защита файлов

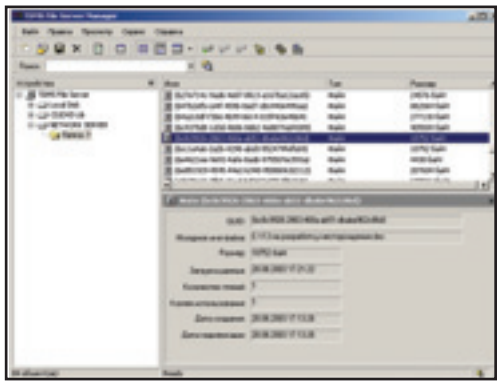
На первый взгляд ответ на вопрос, где и как хранить файлы, не так сложен. Обе используемые с TDMS СУБД позволяют достаточно эффективно хранить большие бинарные объекты. Размещая файлы непосредственно в СУБД, мы убиваем сразу трех зайцев: обеспечиваем максимальный уровень безопасности данных, осуществляем резервное копирование всех данных сразу и получаем возможность использовать встроенный в СУБД полнотекстовый поиск.

Казалось бы, можно поставить точку. Но серверы БД – не файловая система. И как бы мы ни старались, они не будут работать с файлами быстрее, чем операционная система. Падение производительности становится особенно заметным при работе с большими файлами. Еще один недостаток хранения файлов в СУБД проявляется, когда организация работает в распределенной сети, локальные сегменты которой связаны относительно медленными линиями связи. Представьте себе, что произойдет, когда сто человек, работающих в отдельном здании, придут в 8.00 на работу и, зайдя в систему, в течение получаса попытаются выгрузить из центрального хранилища файлы общим объемом 500 Мб через канал 2 Мбит/с.

Настройка репликации серверов БД – дело непростое и под силу только профессиональным администраторам. Большинство проектных организаций просто не располагает таким персоналом. Вдобавок к этому стоимость дополнительного сервера БД существенно увеличивает расходы компании на приобретение и обслуживание программного обеспечения.

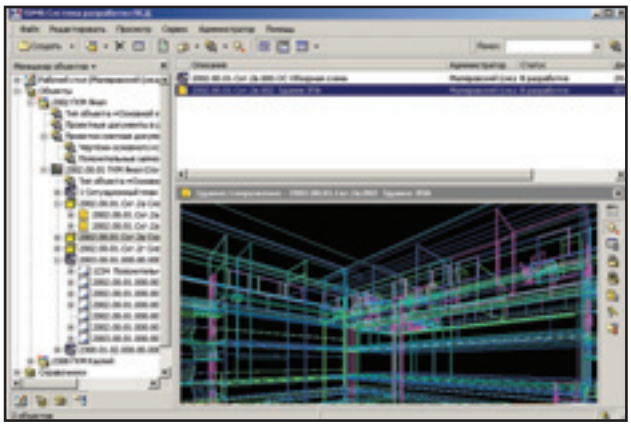
Для более эффективного использования ресурсов проектных организаций был разработан (как дополнение к серверу TDMS) файловый сервер TDMS – опциональное приложение, запускаемое на любом локальном или удаленном компьютере и позволяющее эффективно управлять файлами, размещенными на практически неограниченном количестве устройств хранения. Файловых серверов может быть сколь угодно много. Файловый сервер TDMS позволяет автоматически архивировать информацию, осуществлять резервное копирование, оптимизировать хранение файлов, учитывая скорость

работы устройств хранения и частоту обращения к файлам. Файловые серверы TDMS могут привязываться к подразделениям предприятия, что позволяет размещать файлы непосредственно в том сегменте сети, где они наиболее часто используются.



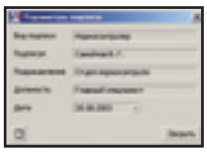
Для обычного пользователя файловый сервер выглядит как "черный ящик". Чтобы извлечь требуемый файл, клиентское приложение отправляет запрос на сервер БД, где происходит проверка прав на просмотр файла. Если право на просмотр имеется, служба файлового сервера получает "добро" на передачу защищенного пакета данных на рабочее место пользователя. Обновление данных на файловом сервере происходит по аналогичному сценарию: данные помещаются на файловый сервер только после подтверждения прав пользователя на редактирование файла. Такая схема позволяет создавать распределенные хранилища данных, не опираясь на политики безопасности отдельно взятой файловой системы.

Но и это еще не всё. Многие службы безопасности ревниво относятся к тому, что файлы при просмотре могут попасть на диск пользователя. Где бы ни находился файл, его открытие стандартными средствами редактирования, такими как Microsoft Word или AutoCAD, даст пользователю возможность сохранить его на локальном диске. И хотя правильно настроенные права доступа не позволят рядовому пользователю скопировать целый проект, злоумышленником может стать и пользователь с большими полномочиями – например, администратор TDMS. Чтобы решить эту проблему, TDMS предлагает дополнительную технологию, которая позволяет передавать не сам файл, а отображение его содержимого. Специальный сервис на сервере создает изображение, которое и передается пользователю. Пользователь работает с полученным с сервера изображением точно так же, как он работает со стандартным средством просмотра. Сервис обладает возможностью корректно отображать все основные форматы файлов: Microsoft Office, DWG, DXF, растровые форматы. Дополнительно поставляются специализированные форматы файлов.



Подписи

TDMS использует достаточно простой, но в то же время эффективный способ создания подписей на электронном документе. По мере прохождения этапов согласования, а затем и утверждения документ собирает подписи. Чтобы поставить подпись на документе, требуется ввести дополнительный пароль. Любое редактирование документа приводит к тому, что все подписи под документом аннулируются.



Сказав о подписях TDMS, стоит упомянуть об электронной цифровой подписи. Из опыта общения с нашими партнерами и клиентами выяснилась замечательная вещь. Многие из них считают, что механизм подписей, реализованный в TDMS, и есть электронная подпись. Боюсь их расстроить, но это не так. Вот что гласит закон: "Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе"[2]. Как видите, закон дает достаточно четкое определение электронной подписи. Более того, он запрещает использование несертифицированных алгоритмов криптования.

Если банки, страховые компании, некоторые государственные учреждения уже начали использовать электронную подпись при обмене документами (в особенности финансовыми), то нас это ждет не скоро. Бумажные документы еще никто не отменял, и в цех или на стройплощадку передаются всё те же бумажные чертежи или их копии, скрепленные обычными подписями и печатями. В этом нет ничего страшного. Не надо революции, сметающей всё на своем пути. Гораздо лучше, если электронные документы заменят бумажные естественным образом, как бумажные архивы постепенно заменяются электронными системами управления технической информацией. Правовое поле уже есть. Еще каких-нибудь 10-15 лет – и мастер цеха будет носить под мышкой не рулон кальки, а графический планшет.

Сергей Загурский
Consistent Software
Тел.: (095) 913-2222
E-mail: serge@csoft.ru

[2]Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи".