ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ

КАРТ БЛАНШ

КАРТОЧНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Рынок платежных карт Украины: **итоги 9 месяцев**

Перспективные направления **развития карточного бизнеса**

Обеспечивая свободу выбора. **Новые возможности карт**

В Новый Год — с новыми технологиями

#09'2008

www.cartoblanche.com.ua

Система однократной аутентификации:

когда нет времени терять успех

1С, Novell Border, LotusNotes, Netscape, CRM, Internet Explorer, FireFox, Mozilla Suite, система "Мини-Банк", система экспортно-импортных операций "Starcon", система денежных переводов "Western Union"... Вереница корпоративного программного обеспечения продолжает свой бесконечный счет.

Сергей ЯКОВЛЕВ

ООО "Автор"

Ваш бизнес постоянно меняется и Вы запускаете одни продукты и отказываетесь от других. Новые законы и распоряжения требуют все большего количества данных о вашей деятельности в строго определенном формате. И вместе с тем, от года к году необходимо увеличивать эффективность, скорость реакции бизнеса и качество продукции. Если ваша корпоративная информационная система не проводит необходимые действия так же быстро, как развивается Ваш бизнес, тогда она просто мешает Вам в достижении целей.

Информационная система современного предприятия представляет собой комплекс разнородных программных приложений, каждое из которых обладает собственными механизмами разграничения доступа, базами данных пользователей, подсистемой аутентификации и авторизации. Количество учетных записей у каждого сотрудника может исчисляться десятками. Процесс создания, изменения и удаления учетных записей зачастую неформализован, длителен по времени и не имеет единой точки контроля в рамках всей информационной системы.

Поэтому нередко программные приложения превращают работу в поиск секретных мест хранения и надоедливого ввода замысловатых паролей в каждое окно доступа - и так у каждого сотрудника. Вы тратите свое драгоценное время на вводы немыслимого количества паролей.

Вы неоднократно задавали себе вопрос о том, а можно ли вводить только один пароль для доступа ко всем необходимым программам?

На сегодняшний день можно однозначно ответить положительно, потому

что специалистами украинской компании "Автор" разработана система однократной аутентификации - CryptoSSO. Главная задача системы - замена многократного ввода пароля (или других видов аутентификации) при доступе к различным приложениям корпоративных информационных систем, а также упрощение управлением пользовательскими учётными записями и правилами доступа.

CryptoSSO направлена на решение двух проблем: обеспечение единого подхода к процессу авторизации пользователей (аутентификация выполняется автоматически и по единому механизму) и защищенного хранения и автоматизации обработки паролей пользователей для доступа к различным системам и информационным ресурсам. Инфраструктура CryptoSSO состоит из трёх основных

КЛИЕНТЫ ИНТЕРЕСУЮТСЯ, МЫ ПРОЯСНЯЕМ

1. Как правило, в компании установлено большое количество программного обеспечения, разработанного в различное время и разными производителями. Все программные комплексы имеют свои настройки и системы аутентификации. Как обеспечить их совместимость и единую точку входа?

Эту проблему решают агенты системы CryptoSSO - SSODesktop со стороны клиента, а также агенты CryptoSSO со стороны серверов. Они выполняют аутентификацию в приложения без участия пользователя посредством введения PIN-кода защищенного носителя ключевой информации (смарт-карта, секретный ключ).

2. Весьма актуальна проблема дисциплины владельцев ключей. Нередки факты передачи, обмена и пр., и доказать такой факт – нелегкая задача. Как решить этот вопрос на программном и аппаратном уровнях, и какие дополнительные требования накладываются на работу всех используемых банком программ?

Пользователь не обладает информацией о ключе, содержащимся на его носителе ключевой информации (смарт-карта, секретный ключ), и поэтому не может передать его третьим лицам. Возможность передачи самого носителя ключевой информации также исключена - смарт-карты и секретные ключи маркированы для определенного пользователя, и он будет нести ответственность в случае их незаконной передачи.

3. Как известно системы однократной аутентификации порождают единую точку компрометации в приложения. Какие контрмеры предпринимаются в этом случае?

Администратору системы достаточно заблокировать сертификат ключа пользователя. После этого система CryptoSSO откажет в авторизации пользователю даже при предъявлении смарт-карты с легитимным PIN-кодом.

4. Какие меры предпринимать в случае отказа сервера однократной аутентификации?

Система проектируется и интегрируется у заказчика с учетом возможного отказа аппаратуры. Для этого существуют дублирующие сервера, реплики хранилищ и т.д.

5. Вход в систему возможен только при предъявлении PIN-кода носителя ключевой информации. Но, что предпринять, если в случае утери или хищении смарт-карты злоумышленник предпримет попытку войти в систему от имени полноправного владельца: существует ли дополнительная защита?

Дело в том, что без знания PIN-кода злоумышленник не пройдет даже первый этап авторизации. А после трех попыток ввода неправильного пароля смарт-карта блокируется.

6. Как предотвратить возможность сознательной несанкционированной передачи смарт-карты и PIN-кода другому пользователю? Например, использовать в комплексе дополнительную биометрическую идентификацию?

Биометрическая идентификация также не защищает от обозначенного сговора пользователей.

В данной ситуации применимы только административные меры - постоянный аудит системы на предмет выявления "неправомерного" поведения пользователей.

компонент: клиентов SSO, Центра управления SSO и связующего сервиса.

В целом, комплексное решение CryptoSSO выполняет следующие функции:

- Расширение или замена разнородных механизмов аутентификации на единый метод строгой двухфакторной аутентификации.
- Управление средствами криптографической защиты информации.
- Создание управляющих директив.
- Регистрация прикладного программного обеспечения пользователя.
- Регистрация аутентификационной информации пользователя.
- Настройка программного обеспечения (предоставление пользователю возможности установки, настройки, сохранения и смены конфигурации ПО CryptoSSO).
- Управление и защита целостности журнала аудита.

Функциональные преимущества системы CryptoSSO:

- Возможность интеграции с "нестандартными" программными приложениями.
- Поддержка многопользовательского режима.
- Защищенный от модификации архив событий.
- Автоматическая обработка сообщений окна смены пароля.
- Возможность подключения внешних криптобиблиотек.
- Возможность хранения данных пользователя в произвольном LDAP-каталоге.
- Работа под управлением ОС Windows NT/2000/XP/2003.

Непосредственно авторизацией пользователей занимаются клиенты SSO. Клиенты совместимы с приложениями Windows, Java, Web и даже DOS. Все необходимые пароли хранятся в специальном защищённом контейнере на носителе пользователя; в качестве носителей используются смарт-карты "УкрКОС" и/или электронные ключи "Secure Token". Для каждого приложения можно при помощи специальных скриптов задать свои настройки применения и политику использования, включая автоматическую генерацию и периодическую смену паролей. Клиенты являются многопользовательскими: разные пользователи с разными правами могут бесконфликтно работать на одном рабочем месте. Все действия клиентов SSO протоколируются в специальных защищённых журналах.

Центр управления SSO в рамках всей корпоративной информационной системы позволяет создавать, удалять и блокировать учётные записи пользователей, изменять права доступа. Администраторы могут изменять настройки как отдельных пользователей, так и у целой группы. Также в Центре управления можно просмотреть все локальные журналы клиентов SSO на местах.

Связующий сервис SSO обеспечивает взаимодействие между клиентами и Центром управления. Все пересылаемые данные зашифрованы при помощи алгоритма ГОСТ 28147-89 и защищены цифровой подписью по стандарту ДСТУ 4145-2002.

Система однократной аутентификации CryptoSSO позволяет повысить эффективность работы корпоративной информационной системы (путем автоматического доступа к необходимым информационным ресурсам), создать безопасную корпоративную систему (электронная цифровая подпись, смарт-карт технологии), повысить надёжность корпоративной системы (снижение влияния человеческого фактора и, как следствие, снижение количества ошибок).

Решение об интеграции системы однократной аутентификации с информационной платформой компании, конечно, остается за вами. Важно иметь в виду, что лучший показатель успеха в будущем достигается правильными решениями в настоящем.

Удачной Вам работы, конкурентоспособных решений и победного курса при построении единой информационной магистрали Вашей компании.