ИНФОРМАТИКА

В.Г. Ермошин

Защита информации от инсайдерских угроз современными методами аппаратной аутентификации

Проблема внутренних угроз информационной безопасности стоит сейчас наиболее остро. Внутренние инциденты часто приводят к утечке персональных данных. По данным аналитического центра InfoWatch, из года в год убытки от них растут на 20–25%. Причем внутренние угрозы в последнее время стали одерживать верх над внешними. В 2007 году их соотношение составило 56,5% против 43,5%. При этом самой серьезной из внутренних угроз являются лица, имеющие санкционированный доступ к конфиденциальной информации организации, то есть инсайдеры [2].

По статистике три четверти случаев утечки или потери конфиденциальных данных связаны с человеческим фактором: умышленными или случайными действиями сотрудников компании. При этом 50% приходится на ошибку сотрудников, 25% – на целенаправленную работу по организации несанкционированной передачи данных заинтересованной стороне. Инсайдеры хорошо знают, как можно использовать для извлечения личной выгоды доступные корпоративные ресурсы, такие как: документы, представляющие собой коммерческую тайну, персональные данные о сотрудниках и клиентах.

Основная проблема борьбы с инсайдерами заключается в том, что они являются легальными пользователями корпоративной информационной системы и обладают серьезными

полномочиями и правами доступа к конфиденциальным данным.

Наиболее эффективное решение проблемы защиты от инсайдеров – это контроль доступа, важнейшим приоритетом в котором является четкое разграничение доступа к информационным ресурсам. В среднестатистической организации используются свыше нескольких десятков различных информационных ресурсов – бухгалтерская система, внутренний корпоративный сайт, почтовый сервер, файловый сервер, CRM-система и т.п. Каждый из этих ресурсов должен требовать аутентификации (процедуры проверки подлинности пользователя) при попытке доступа.

Сегодня наиболее традиционным способом аутентификации является парольная аутентификация. Преимущества парольной аутентификации заключаются в том, что это самый простой метод, который появился намного раньше остальных методов аутентификации. К настоящему времени он реализован в огромном количестве различных компьютерных программ, а также является базовым стандартом аутентификации всех операционных систем. Она не требует дополнительных расходов, так как является составной частью всех операционных систем.

К недостаткам парольной аутентификации относится частая утрата паролей. Пароль может быть подсмотрен или перехвачен при вводе. Пользователя, аутентифицирующегося по паролю, сложно уличить в неправомерных действиях. Он всегда может сослаться на то, что его пароль был украден или подсмотрен. Кроме того, подавляющее большинство паролей укладывается в относительно небольшой список «наиболее частых паролей». Часто пользователи выбирают простые или легко угадываемые пароли. Существует большое количество программ подбора паролей для распространенных операционных систем. Качественный, стойкий к взлому пароль должен соответствовать определенным требованиям, устанавливаемым

службой информационной безопасности организации: длина, уникальность, минимальное количество символов и цифр. Как правило, сотрудники не запоминают пароли, а записывают их на листках бумаги и прячут их в доступных для окружающих местах, что негативно сказывается на сохранности и конфиденциальности корпоративной информации. С развитием информационных технологий парольная аутентификация пользователей не является единственным средством аутентификации пользователей. Уже разработаны более надежные методы: аутентификация по отпечаткам пальцев, аутентификация на основе электронных USB-ключей и смарт-карт.

Биометрическая аутентификация. Сегодня биометрические технологии переживают период бурного развития. Они предназначены для аутентификации пользователей по их уникальным биометрическим характеристикам.

Отпечатки пальцев уникальны для каждого человека и никогда не повторяются [1]. Этот метод аутентификации прост и удобен для пользователей, он не вызывает каких-либо опасений. Однако сканеры отпечатков пальцев начального уровня можно обмануть специально изготовленным искусственным муляжом. Например, сотрудники американского университета Clarkson продемонстрировали, что обычные сканеры отпечатков пальцев удается обмануть в 90% случаев, что совершенно неприемлемо с точки зрения информационной безопасности [3].

Доля отказов в доступе незарегистрированным пользователям в процессе биометрической аутентификации по отпечаткам пальцев составляет 0,01–0,0001% [4].

Смарт-карты представляют собой пластиковые карты с интегрированными электронными схемами. В России, в частности, они удерживают лидерство из-за широкого распространения в банковских структурах. Технология аутентификации пользователей на основе смарт-карт сегодня пользуется большим спросом в банковской сфере деятельности [5].

Основными преимуществами смарт-карт являются распространенность на рынке, а также наличие памяти и возможность реализации криптоалгоритмов. Использование для аутентификации смарт-карт значительно улучшает масштабируемость и управляемость информационной системы организации, снижает затраты на ее администрирование и сопровождение.

Недостатком смарт-карт является необходимость устройства считывания, что значительно повышает стоимость развертывания такой системы аутентификации. Однако в организациях, где общее количество сотрудников превышает количество рабочих станций, общая стоимость развертываемой системы будет значительно ниже. Это обусловлено небольшой стоимостью смарт-карт.

Токены представляют собой USB-ключи размером с брелок. В технологическом и функциональном плане токены аналогичны смарт-картам и отличаются лишь вариантом исполнения. Они могут быть применены для хранения многосимвольных сложных паролей, персональных данных пользователя, цифровых сертификатов, а также ключевой информации.

Преимущества токенов заключаются в том, что они имеют небольшой размер, не требуют специальных устройств-считывателей и обеспечивают мобильность пользователей, поскольку подключаются непосредственно к USB-порту компьютера. Кроме того, отсутствует вероятность создания дубликата токена другим пользователем организации, не имеющим на это прав.

Недостатком токенов в отличие от смарт-карт является отсутствие возможности нанесения на их поверхность опознавательных знаков (название компании, ФИО, должность и фото владельца, его подпись и т.п.).

По оценке целесообразности использования методов аппаратной аутентификации выступает такой критерий, как стоимость. Для полной оценки целесообразности применения ме-

тодов аутентификации, по данным, полученным от разработчиков систем аутентификации Российской компании Aladdin – разработчика систем защиты информации, и Российской компании BioLink Technologies – разработчика масштабируемых и производительных биометрических решений и систем, была составлена таблица стоимости методов аутентификации (таблица).

Таблица

Стоимость методов аутентификации на 3 квартал 2008 года

Средства аутентификаци	Стоимость устройства (руб.)
Отпечатки пальцев	3.920
Смарт-карта + считыватель	270 + 2.040
Токены	1.620

При крупномасштабных организационных изменениях в компании, высокой текучке кадров, распределенной филиальной структуре и при большом числе сотрудников – риск ошибки администратора, распределяющего права доступа, очень высок. Если учесть отсутствие системы мониторинга действий пользователей и отслеживания попыток превышения полномочий, то образуется благодатная среда для безнаказанной деятельности сотрудников, решивших улучшить свое материальное положение за счет компании-работодателя.

Для эффективной профилактики инсайдерской деятельности необходима максимально удобная, управляемая и масштабируемая система для централизованного управления жизненным циклом смарт-карт, USB-ключей и используемых с ними приложений по обеспечению информационной безопасности. Такая система способна обеспечить строгое соответствие современным требованиям бизнеса и в то же время упростить процесс развертывания, эксплуатации и обслужи-

вания различных типов информационных систем токенов и смарт-карт. Подобным связующим звеном между пользователями, средствами аутентификации и политикой безопасности, закрепленной в организационных правилах, являются системы класса Token Management System (TMS). Настроенная в строгом соответствии с корпоративными политиками безопасности TMS способна автоматизировать большинство типовых операций, связанных с управлением доступа пользователей к корпоративным ресурсам (выпуск ключа, персонализация, добавление/отзыв прав доступа, замена/временная выдача нового ключа, отзыв токена). При появлении нового сотрудника, при его переводе в другой отдел или филиал в TMS будут автоматически произведены обновления цифровых сертификатов и паролей, что обеспечит своевременное предоставление всех необходимых для работы прав. При этом доступ пользователя к информации будет запрещен, если его новый статус не предполагает копирование или модификацию.

TMS обеспечивает надежный отзыв всех предоставленных прав доступа при увольнении сотрудника. Иногда необходима быстрая реакция администратора на те или иные события. При увольнении сотрудника важно в сжатые сроки ограничить или запретить возможность доступа к корпоративной информационной системе. Несвоевременное блокирование доступа уволенному сотруднику увеличивает риск потери и разглашения конфиденциальной информации. Если в информационной системе предприятия развернута система управления аппаратными аутентификаторами, администратор может отозвать сертификат сотрудника сразу после получения сообщения о его увольнении. После этого пользователь не сможет получить доступ к информационным ресурсам при помощи токена.

TMS имеет широкий спектр применения, включающий организацию безопасного доступа к информационной сети, вэб-сайтам, электронной почте, шифрованным данным и т.д.

Система управления жизненным циклом ключей и смарт-карт существенно повышает управляемость ИТ-инфраструктурой, снижает влияние на нее человеческого фактора, а также позволяет избежать ошибок администратора при распределении прав доступа к информационным ресурсам предприятия. Таким образом, снижается риск нарушений политики безопасности.

Использование решений такого класса позволяет отойти от сложных, запутанных схем распределения прав легитимных пользователей и на практике реализовать принятую в компании политику информационной безопасности. Это повысит не только надежность защиты, но и уменьшит затраты на управление информационной системой.

Существующие на сегодняшний день методы аутентификации различны по степени надежности, и с усилением защиты резко возрастает их цена, что требует при выборе средств аутентификации анализа рисков и оценки экономической целесообразности применения тех или иных мер защиты.

Анализ средств аппаратной аутентификации показал, что наиболее надежным и наименее дорогостоящим методом для организаций, решивших обезопасить свои данные, является аутентификация на основе электронных ключей – токенов. В организациях, где количество сотрудников превышает количество рабочих станций, более целесообразным является применение методов аутентификации на основе смарт-карт. Применение биометрических методов аутентификации на сегодняшний день является менее целесообразным в связи с их высокой стоимостью.

Список литературы

1. Криминалистика – Дактилоскопия. [Электронный ресурс] – Режим доступа: http://www.koranru.ru/scientific_66.html

2. *Курбатов В.А., Скиба В.Ю.* Руководство по защите от внутренних угроз информационной безопасности. СПБ.: Питер, 2008.

3. Портал полезной информации. Тендеры на Урале и в Екатеринбурге – Ural.RU. [Электронный ресурс] – Режим доступа: http://www.ural.ru/news/techno/news-56455.html

4. Российский биометрический портал – biometrics.ru. [Электронный ресурс] – Режим доступа: http://www.biometrics.ru

5. Aladdin – защита информации, информационная безопасность, аутентификация. [Электронный ресурс] – Режим доступа: http://www.aladdin.ru/press-center/publications/publication3703.php

Научный руководитель – Ф.А. Юн, кандидат технических наук