Современные методы аутентификации: токен и это все о нем..!

Алексей Комаров,
эксперт по информационной безопасности,
Aladdin Software Security R.D.

Аутентификация и идентификация

В современном мире невозможно представить себе офис какой-либо компании без компьютеров. С их помощью обрабатывается вся информация, создаются документы, ведется бухгалтерский учет и выполняется множество другой необходимой работы. Между тем многие данные, хранящиеся на ПК, являются конфиденциальными и составляют коммерческую тайну, которую необходимо защищать.

Для того чтобы обеспечить **конфиденциальность** информации, необходимо ограничить к ней доступ. Другими словами мы должны знать, кто получил доступ к информации, и быть уверены, что это именно тот человек, за которого он себя выдает.

Для достижения этих целей используют процедуры идентификации и аутентификации. Несмотря на близость этих понятий, обозначают они принципиально разные вещи. Дадим определения, чтобы лучше понять различия.

• **Идентификация** — процедура распознавания субъекта по его идентификатору (некоторой информации — числу, строке символов).

• **Аутентификация** (подтверждение подлинности) — процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации.

Таким образом, идентификация — это всего лишь поиск идентификатора в базе данных учетных записей, а аутентификация — это проверка соответствия между субъектом и предъявляемым им идентификатором. Чтобы доказать свою подлинность, субъект должен предъявить нечто, называемое фактором аутентификации. Строго говоря, **фактор аутентификации** — это определенный вид уникальной информации, предоставляемый субъектом системе при его аутентификации.

Всего различают четыре фактора аутентификации:

• субъект имеет нечто (*дискету, токен,...*);

• субъект знает нечто (*пароль, логин,...*);

• субъект обладает некой биологической особенностью (*отпечаток пальца, структура ДНК,...*);

• субъект находится в определенном месте (*IP-адрес, данные от радио-метки,...*).

Факторы аутентификации

Парольная аутентификация

Самый распространенный способ аутентификации — парольный. Однако слабая парольная защита не удовлетворяет современному уровню требований информационной безопасности. Надежность этого способа аутентификации в значительной степени зависит от человеческого фактора, то есть от того, насколько качественные ключевые слова будут выбирать пользователи и насколько серьезно они будут относиться к их хранению. Часто сотрудники стараются упростить свою жизнь, нарушая при этом правила безопасности, и фактически, подчас сами того не сознавая, открывают злоумышленникам дорогу к "святая святых" — коммерческой информации компании.

Обратимся к аналитике: лишь 23% ИТ-сотрудников, опрошенных Ponemon Institute, высказали уверенность в том, что неструктурированные данные (например, текстовые документы), которыми обладает компания, надежно защищены. Наоборот, 84% заявило, что к конфиденциальной информации имеют доступ слишком многие, а 76% признало, что не располагают средствами контроля доступа сотрудников к данным. Таким образом, продолжая тратить значительные суммы на системы хранения данных, компании недостаточно внимания уделяют их защите и контролю доступа к ним.

Как это ни парадоксально звучит, парольная защита является одним из самых дорогих в эксплуатации способов аутентификации. Казалось бы, наоборот, система защиты встроена в ОС, никаких дополнительных затрат не нужно... Но обслуживание и сопровождение парольной защиты отнимает много времени у сотрудников компании, ответственных за работоспособность информационной системы. Им необходимо регулярно проводить аудит паролей пользователей, консультировать по правилам выбора и хранения паролей, производить замену паролей для профилактики, а также в случае их утери или забывчивости пользователей. Все это требует времени и ресурсов, причем нема-

лых. Исследования Gartner показывают, что от 10 до 30 % звонков в службу технической поддержки компании — просьбы сотрудников восстановить забытые ими пароли.

Биометрия

При использовании биометрии пользователь предоставляет образец — опознаваемое, необработанное изображение или запись физиологической или поведенческой характеристики — с помощью регистрирующего устройства (например, сканера или камеры). Этот биометрический образец обрабатывается для получения информации об отличительных признаках, в результате чего получается контрольный шаблон (или шаблон для проверки). Шаблоны представляют собой достаточно большие числовые последовательности; сам образец невозможно восстановить из шаблона. Контрольный шаблон и есть "пароль" пользователя.

Контрольный шаблон сравнивается с эталонным или зарегистрированным шаблоном, созданным на основе нескольких образцов определенной физиологической или поведенческой характеристики пользователя, взятых при его регистрации в биометрической системе. Поскольку эти два параметра (контрольный и эталонный шаблон) полностью никогда не совпадают, то биометрической системе приходится принимать решение о том, "достаточно" ли они совпадают. Степень совпадения должна превышать определенную настраиваемую пороговую величину.

В силу этих ограничений, биометрию нельзя относить к методам строгой аутентификации, т.к. по своей природе она является вероятностной и подвержена различным видам атак:

- подделка отличительной черты;
- воспроизведение поведения пользователя;
- перехват биометрических показателей;
- воспроизведение биометрической подписи.

Среди других недостатков стоит отметить сложность внедрения биометрических систем и дополнительные личные, культурные и религиозные аспекты применения биометрических технологий аутентификации, связанные с вмешательством в частную жизнь.

Многофакторная аутентификация

Для повышения безопасности на практике используют несколько факторов аутентификации сразу. Однако, при этом важно понимать, что не всякая комбинация нескольких методов является многофакторной аутентификацией. Например, использование для аутентификации лица и голоса пользователя не может быть признана таковой, поскольку оба используемых фактора относятся к одному типу- "на основе биометрических данных". Специалисты по информационной безопасности чаще всего относят биометрию (на данном этапе ее развития) к дополнительным методам, позволяющим идентифицировать пользователя.

В основе самого надежного на сегодня метода многофакторной аутентификации лежит применение персональных аппаратных устройств — токенов. Аутентификация на базе токенов является высокотехнологичной и, главное, надежной альтернативой и парольным, и биометрическим методам, и кроме того она существенно превосходит их по простоте интеграции и дальнейшей эксплуатации.

По сути, токен — это небольшой USB-картридер с интегрированным чипом смарт-карты. Токены, реализованные на основе смарт-карт, позволяют генерировать и хранить ключи шифрования, обеспечивая тем самым строгую аутентификацию при доступе к компьютерам, данным и информационным системам.

Токен можно использовать для решения целого ряда различных задач, связанных с шифрованием пользовательских данных, электронной цифровой подписью документов и аутентификацией самого пользователя. С одной и той же смарт-картой пользователь может входить в операционную систему, участвовать в защищенном информационном обмене с удаленным офисом (например, с помощью технологии VPN), работать с web-сервисами (технология SSL), подписывать документы (ЭЦП), а также надежно сохранять закрытые ключи, логины, пароли и сертификаты в памяти своего токена.

В сочетании с криптографическим шифрованием системных дисков, защитой отдельных файлов и съемных носителей, а также аутентификацией до загрузки операционной системы, токены позволяют обеспечить необходимый уровень безопасности ИС для организаций любого масштаба со сколь угодно высоким уровнем требований к системе информационной безопасности и защиты данных.

Тенденции на рынке современных токенов

В сложившейся терминологии и смарт-карты, и USB-ключи с чипом смарт-карты, а также любое другое персональное средство аутентификации пользователя, принято называть токеном (от английского token — метка, жетон).

Токены успешно используются в различных областях, от систем накопительных скидок до кредитных и дебетовых карт, студенческих билетов, телефонов стандарта GSM (знакомая всем SIM-карта, по сути та же смарт-карта, только без лишнего пластика и со специальным ПО), проездных билетов.

Как и любая современная технология, токены постоянно модифицируются и развиваются. Рассмотрим основные направления этого развития.

Интеграция с системами управления доступом

При использовании аппаратных USB-ключей или смарт-карт для аутентификации пользователей, например, при входе в операционную систему, рабочая станция автоматически блокируется при отключении токена. Как правило, согласно корпоративным политикам безопасности каждый сотрудник, оставляя свое рабочее место должен забирать токен с собой, но на практике, к сожалению, это не всегда выполняется. Оставленный без присмотра компьютер до включения программы-заставки является серьезной брешью в системе безопасности.

Для решения этой задачи в современные токены производители предлагают встраивать RFID-метки, полностью аналогичные тем, что встроены в бесконтактных проксимити-картах, так широко используемых в современных офисах. Достаточно установить на двери помещения считыватель, совмещенный с замком и сотрудник выходя из комнаты фактически будет вынужден отсоединить токен и тем самым заблокировать рабочую станцию.

Другой сферой использования меток в токенах является контроль выноса этих аппаратных средств аутентификации за пределы территории организации. Для этих целей встраиваются другие, более дальнодействующие метки, а все проходные оборудуются детекторами, аналогичными тем, что используются в супермаркетах.

Встроенная флэш-память

Несмотря на возможность с помощью печати на специальных принтерах превратить токен в форм-факторе смарт-карты в универсальное устройство, объединяющее бэйдж (с фотографией и ФИО владельца), средство аутентификации и карточку для прохода в помещения, в России наиболее распространенный форм-фактор подключаемых к компьютерам токенов — это USB-ключи.

Связано это в первую очередь с удобством подключения — нет необходимости оборудовать каждую рабочую станцию карт-ридерами (считывателями смарт-карт). Психология пользователей, ожидающих при

подключении USB-ключа появления нового диска в папке "Мой компьютер", желание сэкономить на дополнительных портах, а так же современные требования информационной безопасности во многом предопределили появление нового класса устройств.

Ведущие производители аппаратных средств аутентификации предлагают комбинированную модель аппаратного USB-токена с интегрированной флэш-памятью. Помимо освобождения дополнительного USB-разъема такое устройство имеет целый ряд преимуществ по безопасному хранению, транспортировке и удаленному доступу к конфиденциальным данным

Приложения безопасности удобно хранить и запускать непосредственно из памяти токена. Аппаратная реализация криптографических алгоритмов позволяет в одном корпусе объединить сами защищаемые данные и ключи шифрования, необходимые для доступа к ним.

Большой объем памяти (до 4 Гб) позволяет размещать и автоматически запускать при подключении:

- драйверы самого токена;
- приложения безопасности (например, приложения для шифрования данных);
- приложения, предназначенные специально для отдельных пользователей или групп пользователей;
- операционные системы;
- файлы установки.

Подобные устройства позволяют реализовать доверенную загрузку рабочих станций, терминальных клиентов и даже серверов непосредственно из самой памяти токена вне зависимости от установленной на недоверенном компьютере операционной системы и наличия у него жесткого диска. Интересным решением с таким токеном может быть поставка, дистрибуция, установка и тиражирование ПО.

Генераторы одноразовых паролей

Для работы вне стен офиса с необорудованных и ненастроенных рабочих мест, например, в интернет-кафе использовать USB-ключи и смарт-карты фактически невозможно, особенно с учетом того, что последние помимо драйверов требуют наличия карт-ридера.

Использование классических "многоразовых" паролей является серьезной уязвимостью при работе в таких недоверенных средах. Это подтолкнуло ведущих вендоров рынка аутентификации к созданию аппаратных генераторов одноразовых паролей (OTP-устройств, от англ. One Time Password). Такие устройства генерируют очередной пароль, который сотрудник вводит в окно запроса либо по расписанию (например, каждые 30 секунд) либо по запросу (при нажатии на кнопку). Каждый такой пароль можно использовать только один раз. Проверку правильности введенного значения на стороне сервера проверяет специальный сервер аутентификации, вычисляющий текущее значение одноразового пароля программно.

Для сохранения принципа двухфакторности аутентификации помимо сгенерированного устройством значения пользователь вводит постоянный пароль.

Генераторы одноразовых паролей появились до широкого распространения смарт-карт в ответ на растущее число инцидентов с кражей конфиденциальной информации при помощи удаленного доступа. Такой метод аутентификации не является строгим и носит название — усиленный. Основная уязвимость одноразовых паролей — атака типа "человек посередине". При такой атаке злоумышленник вклинивается в коммуникацию между пользователем и сервером, полностью контролируя весь информационный обмен между ними. Отсутствие криптографических преобразований как в случае с использованием смарт-карт и цифровых сертификатов снижает уровень обеспечиваемой безопасности, позволяя использовать данный способ только в определенных случаях. Так, например, банки в зависимости от метода аутентификации (по одноразовому паролю или цифровому сертификату) устанавливают различные лимиты на проведение операций.

Стоит отметить, что в России в связи с более поздним становлением рынка аппаратных токенов и из-за наличия к тому времени более совершенных смарт-карт, генераторы одноразовых паролей не так широко распространены, как, например, на западе.

Java-токены

Смарт-карта, а точнее ее чип, имплантированный в пластик или встроенный в корпус USB-ключа является полноценным компьютером в миниатюре: с жестким диском (EEPROM), оперативной памятью (ROM), процессором и, конечно, операционной системой. Функционалом, операционной системой и "установленными" на нее приложениями и определяются возможности токена.

Предыдущие поколения токенов, как правило, использовали проприетарную лицензируемую операционную систему (один из монополистов этого рынка — компания Siemens с ее CardOS). Закрытая архитектура делала крайне сложной разработку дополнительных приложений и компонентов самой операционной системы, например, реализацию поддержки национальных криптографических алгоритмов.

Современные токены строятся на базе Java-карты, являющейся стандартом на рынке (более 10 крупных производителей). Функциональность конкретного токена определятся набором загруженных апплетов, выполняющихся на виртуальной Java-машине. Открытая платформа и широкая популярность языка программирования Java позволяет разрабатывать и в короткие сроки внедрять новые возможности. Среди перспективных разработок — реализация мобильного электронного кошелька пользователя, контроль целостности критических данных средствами апплета, выполняющего в заведомо доверенной среде смарт-карты и т.п.

Важной особенностью современных Java-токенов является поддержка USB CCID Class Driver. Это класс драйверов для USB-считывателей смарт-карт, позволяющий реализовать минимальный функционал по работе со смарт-картой без установки специализированных драйверов от производителя. Аналогичный класс драйверов, для, например, компьютерной мышки гарантирует работоспособность двух кнопок и колеса прокрутки любого устройства сразу после подключения.

USB CCID Class Driver встроен в операционную систему Windows Vista и автоматически скачивается с сайта Windows Update при обнаружении нового подключенного устройства в Windows XP, 2003.

Описанные технологии позволяют использовать современные токены, в отличие от устройств предыдущего поколения на более широком парке компьютерной техники и для решения более широкого спектра задач.

Централизованное управление средствами аутентификации

Крупные компании финансового сектора, а также телекоммуникационные компании, а вслед за ними и все остальные, вплоть до компаний малого бизнеса, на фоне все возрастающих угроз информационной безопасности постепенно приходят к пониманию необходимости использования средств строгой аутентификации пользователей.

Большое количество различных моделей аппаратных средств аутентификации, обилие технологий, методов аутентификации, а так же разнообразие приложений безопасности и целей использования приводит к определенным сложностям при внедрении токенов в масштабах организации.Типовыми сценариями, отнимающими дорогостоящее время системных администраторов, становятся сброс забытого PIN-кода токена, замена или выдача временного взамен поврежденного/утраченного токена.

При значительном количестве пользователей (от 100 и выше) затраты на сопровождение средств аутентификации в масштабах компании становятся сравнимыми со стоимостью владения централизованной системой управления жизненным циклом токенов. При этом нужно отдавать себе отчет в том, что внедрение аппаратных средств аутентификации пользователей само по себе не позволяет повысить безопасность системы. Для действительно эффективного их использования необходимо грамотно разработать и внедрить соответствующие политики безопасности, определяющих регламенты и правила использования этих средств.

Не менее важен и контроль за правильностью применения политик, что особенно становится значимым в случае территориальной распределенности компании, обилия филиалов и групп пользователей, использующих те или иные виды токенов для доступа к информации различного уровня конфиденциальности.

Ручной учет токенов, персонализация и правильное назначение их пользователям в зависимости от должностных обязанностей, а так же аудит использования и контроль правильности применения политик в масштабах крупной компании просто немыслим.

Описанные выше и многие другие задачи из соображений безопасности и в том числе для уменьшения влияния человеческого фактора как правило автоматизируют с использованием специализированных систем класса Token Management System (TMS).

Собственно, TMS — это система, предназначенная для внедрения, управления, использования и учета аппаратных средств аутентификации пользователей (USB-ключей и смарт-карт) в масштабах предприятия. С момента инициализации токена и до его отзыва, то есть на протяжении всего времени его функционирования в инфраструктуре компании, основным инструментом для управления им является TMS. К базовым функциям TMS относятся: ввод в эксплуатацию токена (смарт-карты, USB-ключа, комбинированного USB-ключа или генератора одноразовых паролей), персонализация токена сотрудником, добавление возможности доступа к новым приложениям, а также его отзыв, замена или временная выдача новой карты, разблокирование PIN-кода, обслуживание вышедшей из строя смарт-карты и отзыв ее.

Итоги

При всем обилии методов аутентификации наиболее популярными на рынке по-прежнему остаются аппаратные токены во всех их модификациях и вариантах исполнения. Данная технология вне всякого сомнения будет востребована и спрос на нее будет расти. Производители аппаратных токенов постоянно предлагают все новые и новые модели, а разработчики прикладного ПО и операционных систем встраивают в свои продукты поддержку смарт-карт и не спешат от них отказываться.

Современные токены позволяют решить широкий спектр задач по обеспечение информационной безопасности и не редки случаи, когда крупные многофилиальные компании принимают токены как корпоративный стандарт, делая обязательным применение аппаратных средств аутентификации во всех своих дочерних подразделениях. Наличие у ведущих производителей токенов в России соответствующих лицензий и сертификатов на сами токены сделало возможным использование этой технологии в том числе и во многих государственных министерствах и ведомствах.

Средний и малый бизнес вслед за крупными компаниями и государством проявляют все больший интерес к токенам как средствам сохранения конфиденциальности коммерческой информации. Интерес со стороны домашних пользователей, вполне возможно, не за горами. Так популярность персональных средств антивирусной защиты сегодня уже никого не удивляет, а ведь токены позволяют защитить личную информацию и персональные данные от угроз, перед которыми антивирусы просто бессильны.

Пример внедрения

В апреле этого года Компания ВСС, бизнес-партнер Aladdin Software Security R.D., завершила проект по модернизации информационной инфраструктуры Юридического факультета Санкт-Петербургского государственного университета. В рамках проекта, выполненного с применением продуктов и технологий корпорации Microsoft и средств аутентификации от Aladdin, факультет получил одну из наиболее совершенных информационных систем, функционирующих в российских государственных высших учебных заведениях. Для поддержки образовательного процесса были установлены десятки терминалов со считывателями смарт-карт для публичного доступа к библиотеке факультета, введена система аутентификации по смарт-картам, обеспечивающая защищенный доступ всех студентов и аспирантов к факультетскому Web-порталу. Построенный на базе продукта Microsoft SharePoint Portal, портал юрфака служит не только для создания и хранения файлов, но и включает возможность сдачи экзаменов в режиме он-лайн, что будет полностью реализовано на последующих этапах проекта.