ТЕКУЩЕЕ СОСТОЯНИЕ РЫНКА АППАРАТНЫХ СРЕДСТВ АУТЕНТИФИКАЦИИ

ТЕРМИНОЛОГИЯ

Для разграничения прав доступа субъектов к информации необходимо уметь проводить их идентификацию и аутентификацию[1].

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности[2].

Примеры идентификаторов – логин, Dallas Touch Memory, proximity-карты с RFID-метками. В качестве факторов аутентификации могут выступать пароли, аппаратные средства аутентификации (eToken, ruToken, Шипка), биометрические характеристики либо информация о местонахождении субъекта (IP-адрес, координаты GPS и т.п.)

ВВЕДЕНИЕ

Биометрия пока не является масштабно используемым методом аутентификации, для её успешного продвижения и крупных продаж на данном этапе необходимы существенные вложения как в технологические разработки, так и в маркетинговую активность.

Аппаратные идентификаторы в информационных системах являются морально устаревшими и находят своё применение исключительно по причине наличия больших объёмов внедрения в узких нишах программных или аппаратных средств их использующих (напр. Сбербанк). Основной проблемой при переходе на современные средства аутентификации является проблема цены и ранее выполненных внедрений: переобучение персонала, переоснащение рабочих мест, "слом" идеологии руководителей и т.п. Отдельно стоит рассмотреть proximity-карты, которые по сути тоже являются идентификаторами. В своей нише (СКУД) данные решения не имеют аналогов, и пока никаких предпосылок к их исчезновению нет.

В дальнейшем будем рассматривать только аппаратные средства аутентификации, обобщённо называемые **токенами** (от англ. token - жетон, метка).

ФОРМ-ФАКТОРЫ И КЛАССЫ УСТРОЙСТВ

ГЕНЕРАТОРЫ ОДНОРАЗОВЫХ ПАРОЛЕЙ

[1] http://zlonov.ru/wp-content/uploads/%D0%A1%D0%BE%D0%B2%D1%80%D0%B5%D0%BC%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5-%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%D1%8B-%D0%B0%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8-%D1%82%D0%BE%D0%BA%D0%B5%D0%BD-%D0

[2] РД. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992

Одноразовые пароли (OTP – one-time password) пришли на смену классическим многоразовым паролям. Суть данной технологии – использование нового пароля каждый раз при установлении соединения. По мере развития электроники на смену простым распечаткам и скретч-картам пришли аппаратные генераторы одноразовых паролей. Из-за отсутствия встроенной в серверные операционные системы (прежде всего, Microsoft) поддержки аутентификации по OTP обязательно наличие серверной компоненты (сервер аутентификации), проверяющей валидность введённого пользователем одноразового пароля. Установленное на сервере ПО и сам аппаратный генератор должны быть синхронизированы с тем, чтобы сервер ожидал именно то значение, которое для данного сеанса связи сгенерирует устройство. Различают два основных вида синхронизации: по событию и по времени.

Основная область применения генераторов OTP – аутентификация удалённых пользователей при обращении к web-сайту. Наибольшее распространение имеют в финансовых компаниях (для аутентификации клиентов), реже используются в крупных корпорациях для аутентификации сотрудников. Главное удобство при использовании заключается в отсутствии необходимости что-либо подключать к компьютеру. Данную технологию можно также использовать при работе с КПК и смартфонов.

Главные игроки в России:

- Aladdin – eToken NG-OTP и eToken PASS
- ActivIdentity (Rainbow) – широкий модельный ряд
- Vasco – DIGIPASS

СМАРТ-КАРТЫ

Исторически появились раньше, чем USB-ключи. Чип смарт-карты представляет собой микрокомпьютер на одном кристалле. Технологически более защищённое решение, чем микроконтроллер. В настоящее время широко распространены на Западе. В России менее популярны, чем USB-ключи, т.к. внедрение данной технологии в нашей стране происходило значительно позже. Основное удобство заключается в возможности нанесения на смарт-карту изображения (существуют специальные принтеры) с фотографией сотрудника, ФИО и его должностью. Для работы обязательно наличие карт-ридера (считывателя смарт-карт), что повышает стоимость одного рабочего места при закреплении за каждым пользователем отдельного компьютера и понижает при одновременной (посменной) работе нескольких сотрудников на одном оборудованном рабочем месте.

Главные игроки в России:

- Aladdin – смарт-карты eToken и ASECard
- ActivIdentity (Rainbow) – смарт-карта ActivIdentity.
- Интеллектуальные системы управления бизнесом – ESMART Access card

USB-КЛЮЧИ

Компания Aladdin Knowledge Systems изобрела и запатентовала устройство, совмещающее в себе чип смарт-карты и USB-считыватель. Такой USB-ключ не требует отдельного карт-ридера и может быть подключен к любому современному компьютеру. Право на производство аналогичных устройств приобрела компания Rainbow. Других широко известных подобных устройств (по крайней мере в России) нет. Производимые, в частности, Активом ruToken не содержат чип смарт-карты и являются технологически другими устройствами.

Удобство USB-ключей обуславливает их более широкую популярность в России по сравнению со смарт-картами (примерно 85% против 15%). Чаще всего смарт-карты используются в российских представительствах зарубежных компаний, где корпоративным стандартом является именно такой форм-

фактор. С точки же зрения функционала и USB-ключи (на чипе смарт-карты) и смарт-карты являются идентичными устройствами.

В настоящее время USB-ключами называют любые устройства, подключаемые к USB-порту и используемые для аутентификации пользователя/субъекта (например, ключи HASP фактически "аутентифицируют" легального приобретателя копии программы).

Главные игроки в России:

- Aladdin – eToken PRO, eToken Java, гибридные eToken NG-OTP и eToken NG-FLASH
- Rainbow – ActivKey, SafeNet iKey
- Актив – ruToken
- ОКБ САПР – Шипка
- Интеллектуальные системы управления бизнесом – Plug`n`Crypt

ГИБРИДНЫЕ УСТРОЙСТВА

Базовый функционал, обеспечиваемый токенами, расширяется путём интеграции их с другими технологиями/устройствами.

ТОКЕН + RFID-МЕТКА

Интеграция с СКУД позволяет не только облегчить жизнь пользователю (одно устройство вместо нескольких), но и вносит дополнительный элемент контроля: сотрудник не может покинуть помещение, дверь которого оборудована считывателем proximity-карт без физического отключения токена от компьютера и автоматической блокировки в результате этого его рабочей станции.

Технологически имплантацию метки в смарт-карту выполнить проще из-за наличия достаточного места для передатчика и антенны. Строго говоря, это чип смарт-карты имплантируется в стандартную proximity-карту, которая для этого должна удовлетворять стандарту ISO 7816. Данный стандарт подразумевает наличие специального места в карте для имплантации чипа без вероятности повреждения антенны. Имплантация в корпус USB-ключа требует специального вида метку уменьшенного размера.

Данное решение популярно и для успешной игры на этом рынке наличие в продуктовой линейки можно считать обязательным. Среди самих меток наиболее популярны EM-Marine и HID, реже используются Mifare, Indala, Cotag, Ангстрем и т.д.

Главные игроки в России:

- Aladdin – ключи смарт-карты eToken с RFID
- Актив – ruToken RF
- Интеллектуальные системы управления бизнесом – ESMART Access card

ТОКЕН + OTP

Такие устройства позволяют их использовать в двух режимах – при подключении к компьютеру и без него. В России незначительно распространены Aladdin eToken NG-OTP, до выхода eToken PASS в продуктовой линейке не было аналогов. Похожие устройства делает Rainbow – ActivDisplay V2.

ТОКЕН + FLASH-ПАМЯТЬ

Добавление к функционалу токена дополнительного модуля flash-памяти позволяет существенно расширить область применения устройства. По понятным причинам, интеграция со смарт-картами не возможна, только с USB-ключами.

Пользователь, как правило, ожидает, что подобное устройство представляет собой "защищённую флэшку", данные на которой злоумышленник не сможет прочесть. На практике для решения этой задачи требуется установка дополнительного ПО для шифрования.

Другое интересное применение такого устройства – загрузка операционной системы с устройства.

Главные игроки в России:

- Aladdin – eToken NG-FLASH
- ОКБ САПР – Шипка 2.0
- Интеллектуальные системы управления бизнесом – Plug`n`Crypt

ПОТРЕБНОСТИ ПОЛЬЗОВАТЕЛЕЙ

Основой безопасности любой информационной системы служит разграничение прав доступа. В большинстве случаев в современном мире для этого используется парольная аутентификация. Для повышения степени защищённости информационных систем от НСД одним из способов является отказ от паролей либо дополнение парольной аутентификации ещё чем-либо.

ДОМАШНИЕ ПОЛЬЗОВАТЕЛИ

Мало обеспокоены проблемами защиты информации. Имеют интерес больше вызванный любопытством к следующим категориям решений:

- шифрование жёстких дисков с использованием токена
- вход в операционную систему с использованием токена
- хранение логинов и паролей от web-сайтов и приложений в защищённой памяти токена

Продажи данных решений вряд ли могут принести серьёзную прибыль. Такие разработки, ориентированные на домашних пользователей, имеет смысл вести скорее для популяризации и поддержания бренда: "Использую что-то дома – буду использовать это же на работе".

Единственная сколько-нибудь чётко выраженная аудитория – руководители некрупных фирм с ноутбуками, приобретающие решения самостоятельно для шифрования данных с целью защиты от администратора.

Для данного сегмента крайне желательно наличие гибких схем оплаты: наличные, кредитные карты, Webmoney, Яндекс-деньги и т.п.

МАЛЫЕ ПРЕДПРИЯТИЯ

В компании любого размера при наличии сервера есть интерес к системам шифрования данных на сервере. Наличие в таких решениях аппаратной составляющей в виде токена является дополнительным положительным аргументом.

При количестве пользователей от 15-20 в данных компаниях периодически возникает интерес к решениям по защищённому входу в ОС. Не редки случаи приобретения одного-двух изделий для тестов и полное оснащение офиса в дальнейшем.

В целом данному сегменту интересны следующие решения:

- шифрование серверов с аутентификацией администратора с использованием токенов
- вход в операционную систему с использованием токенов
  - с использованием встроенных механизмов ОС MS Windows 2000/XP/Vista/2003
  - с установкой специализированного ПО на каждое рабочее место (при отсутствии домена Windows)
- хранение на токенах электронных ключей клиент-банка или других систем
- шифрование данных на рабочих станциях сотрудников (особенно при их высокой мобильности)
- имплантация в токен RFID-меток для совмещения с СКУД
- хранение логинов и паролей от веб-сайтов и приложений в защищённой памяти токена

Основной доход на данном сегменте приносят продажи серверных систем шифрования из-за их высокой маржинальности. В данном сегменте есть класс компаний, являющихся дилерами какой-либо сети, вход на портал которой требует наличия токенов.

СРЕДНИЕ ПРЕДПРИЯТИЯ

Достаточно массовый и разношёрстный сегмент, границу для которого можно условно провести на рубеже 50 пользователей. Всё сказанное выше про малые предприятия почти полностью справедливо для этих компаний со следующими дополнениями:

- вход в операционную систему с использованием токенов чаще осуществляется с использованием встроенных механизмов ОС MS Windows 2000/XP/Vista/2003, т.к. наличие домена и квалифицированных сотрудников позволяет использовать более надёжное решение (по сравнению с хранение в токене логина и пароля)
- имплантация в токен RFID-меток для совмещения с СКУД является более важным фактором при выборе продукта, чем для более мелких компаний
- хранение логинов и паролей от веб-сайтов и приложений в защищённой памяти токена используется крайне редко и в основном для экзотических приложений
- вполне вероятен интерес к приобретению централизованной системы управления токенами

По обороту данный сегмент (среди рассматриваемых) стоит на третьем месте после государственных и крупных коммерческих организаций. Основной доход приносят продажи самих токенов и серверных систем шифрования данных.

КРУПНЫЕ ОРГАНИЗАЦИИ

Наиболее готовые к внедрению аппаратных средств аутентификации компании на российском рынке. Среди отраслей приносят наибольший доход:

- телекоммуникационные компании
- банки и другие финансовые организации
- компании нефтегазового сектора
- тяжёлая промышленность и электроэнергетика

Почти обязательное требование для внедрения токенов - наличие централизованной системы управления в масштабах предприятия. Такая система должна быть максимально совместима с продуктами других вендоров (Microsoft, Sun, etc.) В отдельных (очень, впрочем, редких) случаях заказчика самостоятельно дорабатывают собственные прикладные системы для работы с токенами (например, серверная компонента для OTP).

Интересующие решения:

- вход в операционную систему с использованием токенов с использованием встроенных механизмов ОС MS Windows 2000/XP/Vista/2003
- реализация ЭЦП с использованием токенов
- безопасный удалённый доступ для клиентов
- безопасный удалённый доступ для сотрудников (в т.ч. VPN)
- имплантация в токен RFID-меток для совмещения с СКУД
- централизованная система управления токенами
- услуги по внедрению и интеграции
- консалтинговые услуги (разработка политик, регламентов и т.п.)

Почти обязательное требование для внедрения токенов – наличие централизованной системы управления в масштабах предприятия. Такая система должна быть максимально совместима с продуктами других вендоров (Microsoft, Sun, etc.) В отдельных (очень, впрочем, редких) случаях заказчики самостоятельно дорабатывают собственные прикладные системы для работы с токенами (например, серверная компонента для OTP).

Для банковского сегмента помимо использования токенов во внутренних информационных системах интерес представляет возможность предоставить клиентам безопасный удалённый доступ при использовании интернет-банкинга (теле-банкинга). Разные банки реализуют различный подход к обеспечению безопасности. В частности, банки предлагают три основных подхода: OTP, токены и западная криптография, токены и российская криптография. Последний подход вызывает меньше всего юридических вопросов (в том числе у проверяющих органов), но требует (в настоящее время) обязательной установки на каждое рабочее место помимо драйверов токена ещё и криптосервис-провайдера (CSP), реализующего российскую криптографию. Не редко банки предлагают клиентам своё собственное ПО – банк-клиент, в который уже интегрирован какой-либо CSP (КриптоПро, Сигнал-КОМ, Агава-С и т.д.). Разработчиков клиент-банков на рынке не так много – банки редко делают эти разработки сами, предпочитая использовать готовые решения. Один из игроков этого рынка, компания Бифит, предлагает собственные токены iBank 2 Key и не планирует интеграцию с другими вендорами.

Для ряда компаний (в первую очередь системообразующих) помимо описанного выше верны положения следующего раздела – Государственные учреждения. Например, для успешной продажи решения в Газпром нужна соответствующая сертификация Газпромсерт.

ГОСУДАРСТВЕННЫЕ УЧРЕЖДЕНИЯ

Для поставки в государственные организации токен должен быть сертифицирован. Рынок гостайны является отдельным вопросом, для большинства министерств и ведомств достаточно сертификата ФСТЭК.

Для данного сегмента обязательно совместимость токена с CSP, реализующими российские алгоритмы, либо реализация этих алгоритмов самим токеном. С точки зрения безопасности преимущества второго варианта очевидны, однако на сегодняшний день в целом по России мы имеем большую инсталляционную базу CSP, которые изначально поставлялись с хранилищами закрытых ключей – дискетами, а сейчас постепенно переоборудуются токенами, выступающими в роли "дискеты с ПИН-кодом". Массовая полномасштабная деинсталляция имеющегося ПО и замена его на токены, аппаратно реализующие ГОСТ, вряд ли возможна.

Часть государственных организаций (и "полугосударственных") используют самописные приложения, в которых реализована поддержка того или иного токена.

ТЕХНИЧЕСКИЕ ДЕТАЛИ

АУТЕНТИФИКАЦИЯ ПРИ ВХОДЕ В ОПЕРАЦИОННУЮ СИСТЕМУ

не публиковалось

При использованием встроенных механизмов в ОС MS Windows 2000/XP/Vista/2003 необходима поддержка токеном функционала смарт-карты (MS CryptoAPI). Данному требованию удовлетворяют все модели eToken, ruToken и Шипка. С технической точки зрения используется протокол Kerberos, в котором для аутентификации пользователя применяются цифровые сертификаты. Для внедрения данного решения помимо приобретения самих токенов необходимо:

- наличие домена Windows на базе Windows Server 2000/2003/2008
- установка на каждом рабочем месте драйверов для токена (или поддержка USB CCID Class Driver - см.ниже) и установка криптосервис-провайдера (CSP) и специализированного ПО при необходимости использования российской криптографии
- разворачивания удостоверяющего центра (УЦ), в качестве которого может выступать Microsoft CA (входит в состав любой серверной операционной системы MS) или УЦ Криптопро (только для российской криптографии)

Удобство использования токенов в форм-факторе USB-ключа добавляет 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. Пример таких устройств – eToken Java.

При отсутствии развёрнутого домена Windows или нежелании разворачивать УЦ можно применить решение, позволяющее сохранить в токене логин и пароль пользователя. Для внедрения данного решения необходимо на каждое рабочее место установить специальное программное обеспечение, заменяющее стандартную компоненту Windows – GINA (отвечает за вход пользователя в ОС) на ПО, которое до входа пользователя в ОС считывает из подключенного токена логин и пароль пользователя и пробрасывает его операционной системе. Как правило, все решения имеют однофакторный режим работы – пользователь просто подключает токен к компьютеру и получает доступ. Несмотря на существенно меньший уровень безопасности такого решения, зачастую клиенты используют именно такой режим из соображений удобства и простоты.

Примеры таких решений:

- Aladdin – Windows Logon, поддерживает только eToken
- Securit – Zlogin, поддерживает ruToken, SafeNet iKey, eToken
- Rohos – Logon Key, поддерживает eToken, SafeNet iKey, Crypto Identity, ePass, ruToken и другие
- Интеллектуальные системы управления бизнесом – ESMART Access, поддерживает смарт-карты ESMART Access Card, CryptoFlex, eToken

Некоторые компании не видят в подобных решениях источника дохода и фактически отдают их "за копейки" (Aladdin), другие поступают наоборот. Чуть ли не единственными критериями выбора продукта данного класса являются: поддерживаемые ОС, токены, интерфейс и цена.

АППАРАТНАЯ РЕАЛИЗАЦИЯ ЗАРУБЕЖНОЙ КРИПТОГРАФИИ

В мире общепринятым стандартом ЭЦП является алгоритм RSA/1024 (RSA/2048). Как известно, для вычисления ЭЦП документа (файла, письма и т.п.) сначала нужно вычислить его хэш. Общемировые алгоритмы хэширования – это SHA1, MD5.

Приведённые алгоритмы интегрированы в подавляющее большинство современных операционных и прикладных системы, протоколы, сетевое и телекоммуникационное оборудование и т.д.

До появления смарт-карт (а позднее – токенов) все криптографические вычисления производились программно, а закрытые ключи хранились на жёстком диске компьютера (в реестре). Смарт-карты позволили не только безопасно хранить в защищённой ПИН-кодом памяти закрытые ключи, но и производить криптографические вычисления с ними аппаратно. Закрытые ключи никогда не покидают внутренней памяти чипа смарт-карты.

Важно отметить, что токены никогда не позиционировались в мире как криптографические ускорители, а реализованные функции хэширования используются исключительно для внутренних целей – вычислить хэш от большого документа токен не может (Шипка – исключение). Именно поэтому токенами чаще всего используется интерфейс USB 1.1

Поддержка токеном аппаратных реализаций зарубежных криптографических алгоритмов и стандартных интерфейсов (MS CryptoAPI, PKCS#11) автоматически делает токен совместимым с решениями всех ведущих мировых вендоров: Microsoft, Oracle, IBM, Cisco, CheckPoint, Citrix etc и любым прикладным ПО, в которых также реализованы такие интерфейсы Firefox, TheBat, OpenSSL etc.

АППАРАТНАЯ РЕАЛИЗАЦИЯ РОССИЙСКОЙ КРИПТОГРАФИИ

В РФ разработаны и используются собственные криптографические алгоритмы. И если частные лица и коммерческие компании могут использовать зарубежные разработки, то государственные организации – только российские. Такое ограничение де факто распространяется и на случаи, когда необходим юридически значимый документооборот. Именно по этой причине и возможен в России бизнес таких компаний как КриптоПро, Сигнал-КОМ и др.

До появления на российском рынке токенов использовались программные решения, основным минусом которых было небезопасное хранение закрытых ключей. Ещё совсем недавно для этих целей использовались дискеты, а многие токены, пришедшие им на замену, по сути являются теми же дискетами, но защищёнными ПИН-кодом. При вычислении той же ЭЦП закрытый ключ после ввода правильного ПИН-кода покидает защищённую память и теоретически становятся уязвим. Потребность рынка в надёжных сертифицированных токенах, аппаратно реализующих российские криптографические алгоритмы, и прежде всего ЭЦП, **крайне высока**. Банкам, полугосударственным и государственным компаниям такой токен нужен уже сегодня или понадобится в ближайшее время.

Невозможность отказа от программного вычисления хэша не позволяет пока некоторым производителям токенов отказаться от интеграции с CSP. Путь получения лицензии и разработки собственной программной реализации российской функции хэширования позволит отказаться от такого сотрудничества. Реализация такой функции аппаратно с точки зрения безопасности более перспективна.

РАБОТА БЕЗ УСТАНОВКИ ПО

Поддержка токеном спецификации CCID (USB Chip/Smart Card Interface Devices[3]) позволяет упростить использование этого устройства, так как для работы с ним не требуются специфические драйверы от производителя. На практике это означает отказ от какого-либо клиентского ПО на рабочем месте. Такое решение интересно в первую очередь банкам, т.к. их клиенты порой используют сложности с установкой и настройкой ПО клиент-банка.

Требование по использованию российских алгоритмов накладывает свой отпечаток на эту радужную картину: токены западного производства технически не могут вычислять хэш в силу своей "маломощности". Предлагаемые решения по загрузке, например, некоего java-апплета в браузер и вычисления хэша с его помощью вряд ли когда-либо будут сертифицированы.

[3] http://msdn.microsoft.com/en-us/windows/hardware/gg487509.aspx

Возможно, что аппаратная реализация функции хэширования в совокупности с поддержкой указанной спецификации позволит создать сертифицированный токен, не требующий никакого клиентского ПО. Данный вопрос требует отдельной проработки.

ХРАНЕНИЕ ЛОГИНОВ И ПАРОЛЕЙ В ПАМЯТИ ТОКЕНА

Вводимые с клавиатуры многочисленные пароли пользователь с удовольствием не вводил бы с клавиатуры, а хранил их в защищённом месте.

Пример продукта RoboForm показывает высокую заинтересованность домашних пользователей в подобном классе решений. Этот продукт хранит только пароли, вводимые в окне браузера, и хранит их на обычной флэшке или жёстком диске.

Идеальным с точки зрения безопасности видится интеграция подобного решения с гибридным токеном с FLASH-памятью.