Одной из основных проблем информационной безопасности, особенно с увеличением количества сотрудников, работающих удалённо, является проблема аутентификации.

С давних пор решение доступа было связано с использованием паролей. Но сегодня с учётом психологии пользователей применение паролей становится небезопасным по целому ряду причин:

- всё больше пользователей применяет один и тот же пароль и в корпоративной сети, и для личных нужд
- пароли пользователей, как правило, содержат словарные слова либо так или иначе связаны с личностью самого пользователя (имя жены, ребёнка, название любимой футбольной команды, номер и марка автомобиля и т.д.), а так как сегодня многие описывают свою жизнь в социальных сетях достаточно подробно, то такие пароли легко взламываются.

В дальнейшем эти требования будут только ужесточаться. К чему это приведёт, вернее, уже привело? Чем сложнее пароли, чем больше приложений требуют ввод пароля, тем выше вероятность того, что пользователи для всех приложений, в том числе и для аутентификации в ОС, будут использовать один и тот же пароль, к тому же записывая его на бумаге. Хорошо это или плохо? Допустимо ли?

С одной стороны – явно недопустимо, так как резко возрастает риск компрометации пароля, с другой – слишком сложный пароль (например, PqSh*98+) трудно удержать в памяти. Вероятно, что пользователи будут или выбирать простой пароль, или постоянно забывать сложный и отвлекать администратора от более важных дел.

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

По данным IDC, каждый забытый пароль обходится организации в 10-25 долл. Добавим сюда ещё необходимость его постоянной смены и требование оригинальности паролей. Что делать? Какой выход?

Но уже сегодня существует несколько вариантов решения этой проблемы.

Первый вариант. На видном месте в комнате (на стене, на столе) вывешивается плакат с лозунгом. После этого в качестве пароля используется текст, содержащий, предположим, каждый третий символ лозунга, включая пробелы и знаки препинания. Не зная алгоритма выбора знаков, подобный пароль подобрать довольно сложно.

Второй вариант. В качестве пароля выбирается (генерируется с помощью специального ПО) случайная последовательность букв, цифр и специальных символов. При этом указанный пароль распечатывается на матричном принтере на специальных конвертах, которые нельзя вскрыть, не нарушив их целостность. Примером такого конверта может служить конверт с PIN-кодом к платёжной карте. Эти конверты хранятся в сейфе начальника подразделения или в сейфе службы информационной безопасности. Единственной сложностью при таком способе является необходимость немедленной смены пароля сразу после вскрытия конверта и изготовления другого подобного конверта с новым паролем, а также организация учёта конвертов. Но если принять во внимание экономию времени администраторов сети и приложений, то эта плата не является чрезмерной.

Третий вариант – использование многофакторной аутентификации на базе новейших технологий аутентификации. В качестве примера рассмотрим двухфакторную аутентификацию. Основным преимуществом такой аутентификации является наличие физического ключа и PIN-кода к нему, что обеспечивает дополнительную устойчивость к взлому. Ведь утрата аппаратного ключа не влечёт за собой компрометацию пароля, поскольку, кроме ключа, для доступа к системе нужен ещё и PIN-код.

Отдельно стоит рассмотреть системы с применением разовых паролей, которые получают всё большее распространение в связи с широким развитием интернет-технологий, и системы биометрической аутентификации.

Системы биометрической аутентификации

Технологией, особенно широко рекламируемой при использовании смартфона, является биометрическая аутентификация на основе использования отпечатка пальца, радужки глаза. Реже встречается трёхмерный снимок лица или так называемый «клавиатурный» почерк.

Наиболее распространены следующие виды биометрической аутентификации:

- по отпечатку пальца
- по лицу, как по двухмерному, так и по трёхмерному изображению
- по голосу
- по радужной оболочке глаза
- по геометрии ладони или рисунку вен на ладони

Классификация средств идентификации и аутентификации

Современные программно-аппаратные средства идентификации и аутентификации по виду идентификационных признаков можно разделить на электронные, биометрические и комбинированные (рис. 1). В отдельную подгруппу в связи с их специфическим применением можно выделить входящие в состав электронных средств системы одноразовых паролей.

В электронных системах идентификационные признаки представляются в виде кода, хранящегося в защищённой области памяти идентификатора (носителя) и, за редким

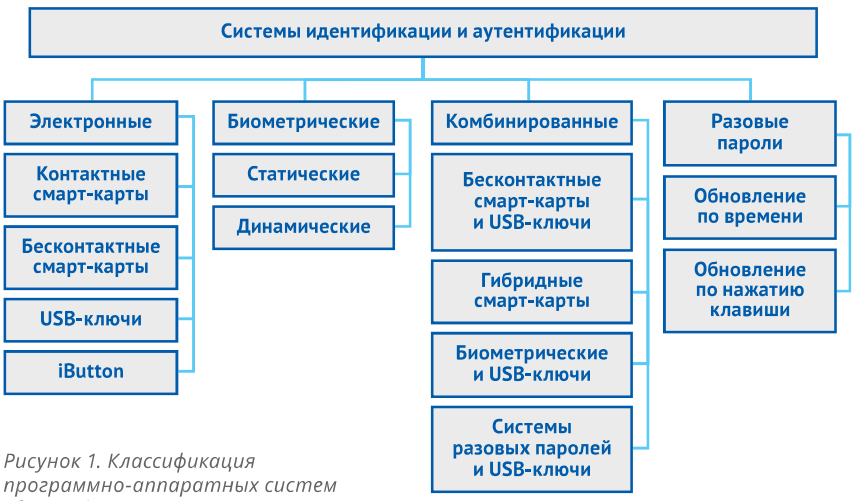

Рисунок 1. Классификация программно-аппаратных систем идентификации.

исключением, фактически не покидающего её. Идентификаторы в этом случае бывают следующие:

- контактные смарт-карты
- бесконтактные смарт-карты
- USB-ключи (USB-token)
- iButton

В биометрических системах идентификационными являются индивидуальные особенности человека, которые в данном случае называются биометрическими признаками. Идентификация производится за счёт сравнения полученных биометрических характеристик и хранящихся в базе шаблонов. В зависимости от характеристик, которые при этом используются, биометрические системы делятся на статические и динамические.

Статическая биометрия основывается на данных (шаблонах), полученных путём измерения анатомических особенностей человека (отпечатки пальцев, узор радужки глаза и т.д.), а динамическая – на анализе действий человека (голос, параметры подписи, её динамика).

На мой взгляд, биометрические системы аутентификации не получили широкого распространения по нескольким причинам:

- высокая стоимость подобных систем
- отсутствие хорошо подготовленного профессионального персонала
- сложность настройки таких систем
- противодействие со стороны сотрудников, так как руководство получает возможность контролировать все их перемещения и фактически производить контроль рабочего времени

В комбинированных системах применяется одновременно несколько признаков, причём они могут принадлежать как к системам одного класса, так и к разным.

Биоэлектронные системы

Как правило, для защиты компьютерных систем от несанкционированного доступа применяется комбинация из двух систем: биометрической и контактной на базе смарт-карт или USB-ключей.

Что скрывается за понятием «биометрия»? Фактически мы используем такие технологии каждый день, но как технический способ аутентификации биометрия стала применяться относительно недавно. Биометрия – это идентификация пользователя по уникальным, присущим только ему одному биологическим признакам. Такие системы являются самыми удобными, с точки зрения самих пользователей, поскольку не нужно ничего запоминать, а потерять биологические характеристики весьма сложно.

При биометрической идентификации в базе данных хранится цифровой код, ассоциированный с определённым человеком. Сканер или другое устройство, используемое для аутентификации, считывает конкретный биологический параметр. Далее он обрабатывается по определённым алгоритмам и сравнивается с кодом, содержащимся в базе данных.

Просто? С точки зрения пользователя – безусловно. Но у данного метода существуют как достоинства, так и недостатки.

К **достоинствам** биометрических сканеров обычно относят то, что они никак не зависят от пользователя (например, пользователь может ошибиться при вводе пароля) и тот не может передать свой биологический идентификатор другому человеку, в отличие от пароля. А подделать уникальный узор, имеющийся на пальце у каждого человека, практически невозможно. Но, как показали исследования, проведённые в США, биометрические сканеры, основанные на отпечатках пальцев, довольно легко вводили в заблуждение с помощью муляжа отпечатка пальца или даже пальца трупа. Распространён также отказ в доступе, осуществляемый на основании распознавания голоса, если человек, например, простыл. Но самый большой недостаток биометрических систем – это их высокая цена.

Все биометрические технологии можно разделить на две группы:

- статические методы, которые основываются на физиологической (статической) характеристике человека, то есть уникальном свойстве, присущем ему от рождения и неотъемлемом от него. К статическим биологическим признакам относятся форма ладони, отпечатки пальцев, радужная оболочка, сетчатка глаза, форма лица, расположение вен на кисти руки и т.д.
- динамические методы, которые основываются на поведенческой (динамической) характеристике человека – особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия (подписи, речи, динамики клавиатурного набора)

Идеальная биометрическая характеристика человека (БХЧ) должна быть универсальной, уникальной, стабильной и собираемой.

- **Универсальность** – наличие биометрической характеристики у каждого человека
- **Уникальность** – не может быть двух человек, имеющих идентичные значения БХЧ
- **Стабильность** – независимость БХЧ от времени
- **Собираемость** – возможность получения биометрической характеристики от каждого индивидуума

Реальные БХЧ не идеальны, и это ограничивает их применение. В результате экспертной оценки таких источников БХЧ, как форма и термограмма лица, отпечатки пальцев, геометрия руки, структура радужной оболочки глаза (РОГ), узор сосудов сетчатки, подпись, особенности голоса, форма губ и ушей, динамика почерка и походки было установлено, что ни один из них не удовлетворяет всем требованиям по перечисленным выше свойствам. Необходимым условием использования тех или иных БХЧ является их универсальность и уникальность, что косвенно может быть обосновано их взаимосвязью с генотипом или кариотипом человека.

Распознавание по отпечаткам пальцев

Это самый распространённый статический метод биометрической идентификации, в основе которого лежит уникальность для каждого человека рисунка папиллярных узоров на пальцах. Изображение отпечатка пальца, полученное с помощью специального сканера, преобразуется в цифровой код (свёртку) и сравнивается с ранее введённым шаблоном (эталоном) или набором шаблонов (в случае аутентификации).

Ведущие производители сканеров отпечатков пальцев:

- BioLink – www.biolink.ru
- Bioscrypt – www.bioscrypt.com
- DigitalPersona – www.digitalpersona.com
- Precise Biometrics – www.precisebiometrics.com

Ведущие производители сенсоров (считывающих элементов для сканирующих устройств):

• Atmel – www.atmel.com
• Fujitsu – www.fujitsu.com

Распознавание по форме руки

Данный статический метод построен на распознавании геометрии кисти руки, также являющейся уникальной биометрической характеристикой человека. С помощью специального устройства, позволяющего получать трёхмерный образ кисти руки (некоторые производители сканируют форму нескольких пальцев), делаются измерения, необходимые для получения уникальной цифровой свёртки, идентифицирующей человека.

Ведущий производитель такого оборудования:

• Recognition Systems – www.recogsys.com

Распознавание по радужной оболочке глаза

Данный метод распознавания основан на уникальности рисунка радужной оболочки глаза. Для реализации этого метода необходима камера, позволяющая получить изображение глаза человека с достаточным разрешением, и специализированное программное обеспечение, выделяющее из полученного изображения рисунок радужной оболочки глаза, по которому строится цифровой код для идентификации человека.

Фирма Iridian (www.iridiantech.com) – крупнейший производитель в данной области, на её решениях базируются практически все разработки таких компаний, как LG, Panasonic, OKI, Saflink и др.

Распознавание по форме лица

В данном статическом методе идентификации строится двух- или трёхмерный образ лица человека. С помощью камеры и специализированного программного обеспечения на изображении или наборе изображений лица выделяются контуры бровей, глаз, носа, губ и т.д., вычисляются расстояния между ними и другие параметры в зависимости от используемого алгоритма. По этим данным строится образ, который преобразуется в цифровую форму для сравнения. Причём количество, качество и разнообразие (разные углы поворота головы, изменение нижней части лица при произношении ключевого слова и т.д.) считываемых образов может варьироваться в зависимости от алгоритмов и функций системы, реализующей данный метод.

Ведущие производители подобных устройств:

• Cognitec Systems – www.cognitec.com
• Vicar Vision – www.vicarvision.nl
• ZN Vision – www.zn-ag.com

Распознавание по почерку

Как правило, для этого динамического метода идентификации человека используется его подпись или написание кодового слова.

Цифровой код идентификации формируется по динамическим характеристикам написания, то есть для идентификации строится свёртка, в которую входит информация по графическим параметрам подписи, временным характеристикам нанесения подписи и динамике нажима на поверхность в зависимости от возможностей оборудования (графический планшет, экран карманного компьютера и т.д.).

Распознавание по набору на клавиатуре

Метод в целом аналогичен вышеописанному, но вместо подписи в нём используется некое кодовое слово, а из оборудования требуется только стандартная клавиатура. Основная характеристика, по которой строится свёртка для идентификации, – динамика набора кодового слова.

Ведущий производитель подобного оборудования:

• Checco – www.biochec.com

Распознавание по голосу

В настоящее время развитие этой одной из старейших технологий ускорилось, так как предполагается её широкое использование при сооружении интеллектуальных зданий. Существует достаточно много способов построения кода идентификации по голосу – это, как правило, различные сочетания частотных и статистических характеристик последнего.

Ведущие производители таких устройств:

• Nuance – www.nuance.com
• Voicevault – www.voicevault.com

Стоит учесть, что идентификация по статическим характеристикам более надёжна, так как не зависит от психоэмоционального состояния идентифицируемого субъекта.

Middleware

Кроме вышеуказанных производителей, в настоящее время на рынке биометрии появилась новая группа компаний, решения которых называются middleware. Как правило, это «программное обеспечение – посредник между конечным оборудованием и программными системами, в которые интегрируются процедуры биометрической идентификации. Причём middleware может реализовать как просто вход в систему с использованием измерений биометрического сканера (например, Windows Logon), так и самостоятельную функциональность, например создание криптографических контейнеров с помощью ключа, получаемого только по определённому отпечатку пальца.

Недостатки биометрической аутентификации

В биометрической аутентификации есть свои недостатки.

Во-первых, это недостатки самих биометрических сканеров. Конечно, они будут разными у различных типов сканеров. Но их объединяет то, что они есть! Например, сканеры отпечатков пальцев могут быть оптическими и электронными. Первые обеспечивают более качественное изображение, но быстрее загрязняются и более требовательны к чистоте рук. Вторые – менее надёжные и качественные, однако могут распознавать даже грязные руки. Можно сделать вывод, что выбор биометрической технологии для каждого конкретного случая должен быть разным.

Во-вторых, это крайне сложная корректная настройка оборудования, точнее, установка корректного порогового значения ошибки. FAR (False Acceptance Rate) – это процент ложных отказов в допуске, FRR (False Rejection Rate) – вероятность допуска в систему незарегистрированного человека. Порог чувствительности является своеобразной гранью идентификации. Человек, имеющий сходство какой-либо характеристики выше предельного, будет допущен в систему, и наоборот. Значение порога администратор может изменять по своему усмотрению, то есть это предъявляет к нему весьма высокие требования, ведь поддержка баланса между удобством и надёжностью требует больших усилий.

В-третьих, при внедрении биометрических систем можно столкнуться с сопротивлением сотрудников компаний, обусловленным возможностью контроля их рабочего времени. Тем более что системы для учёта рабочего времени сотрудников тоже существуют.

Биометрические сканеры невозможно применять для идентификации людей с некоторыми физическими недостатками, утверждает профессор антропологии Университетского колледжа (University College) Лондона Анжела Сесс (Angela Sasse). Так, применение сканеров сетчатки глаза будет сложным для тех, кто носит очки или контактные линзы, а человек, больной артритом, не сможет ровно положить палец на сканер отпечатка.

Ещё одна проблема – рост. Сканирование лица может стать затруднительным, если рост человека менее 1,55 метра или более 2,1 метра. Преступники, по словам г-жи Сесс, смогут легко обмануть биометрические системы. Некоторые срезают свои отпечатки пальцев или сжигают их кислотой. Есть и неумышленные случаи: например люди с повреждённой кожей рук.

К недостаткам такого способа идентификации можно отнести возможность воспользоваться муляжом отпечатка, что было успешно продемонстрировано заключёнными шотландской тюрьмы строгого режима Glenochil.

Анализ мер по снижению риска биометрической аутентификации

Если на предприятии вместе с Windows 7 планируется внедрение биометрического механизма проверки, например сканирования отпечатков пальцев, следует заранее учесть следующие соображения:

- биометрические системы обычно требуют хранения на компьютере информации, которая может использоваться для установления личности. По этой причине предприятию придётся заниматься обеспечением конфиденциальности
- многие современные переносные компьютеры обладают встроенными сканерами отпечатков пальцев, что может упростить внедрение биометрического решения, но по функциональности и качеству распознавания такие встроенные устройства уступают специализированному оборудованию. Следует сравнить относительное качество по таким показателям, как коэффициент ложного пропуска, коэффициент ложного отказа, коэффициент ошибок кроссовера, коэффициент ошибок регистрации и пропускная способность
- если по характеру работы пользователи или компьютеры оказываются в загрязнённых помещениях, где сложно поддерживать чистоту рук или требуются перчатки, сканеры отпечатков использовать не удастся. Эту проблему можно решить за счёт систем анализа других физиологических параметров, например геометрии лица, радужной оболочки глаза или ладони
- наряду с биометрическим подтверждением пользователю необходимо предоставлять какое-либо иное свидетельство, например ключевую фразу, PIN-код или смарт-карту, поскольку биометрические устройства можно обмануть

Процесс снижения рисков

Особенности внедрения биометрических средств на каждом предприятии свои. Но общую последовательность действий определить можно.

1. Установить, какие из имеющихся механизмов проверки биометрических данных больше подходят нуждам предприятия.
2. Проанализировать внутреннюю документацию по обеспечению конфиденциальности, чтобы убедиться в возможности управления конфиденциальными биометрическими данными.
3. Определить требования к оборудованию, используемому при биометрическом сканировании, и наметить сроки выполнения этих требований.
4. Определить элементы инфраструктуры, необходимые для биометрического сканирования, такие как инфраструктура публичных ключей или требования к клиентскому программному обеспечению.
5. Установить, у каких сотрудников могут возникнуть проблемы с использованием биометрической системы, и подобрать для них альтернативные варианты, например проверку по имени пользователя и паролю или смарт-карте с PIN-кодом.
6. Заранее обучить пользователей обращению с системой биометрической проверки подлинности, а тех, кто не сможет ею пользоваться, – альтернативным методам проверки.
7. Провести масштабный пилотный запуск в целях выявления и разрешения проблем до начала повсеместного внедрения.
8. Следуя инструкциям производителя по сканированию и проверке, ввести данные о пользователях в биометрическую систему.
9. Обучить пользователей обращению с системой, обеспечить помощь для тех, кто испытывает трудности.
10. Необходимо учесть, что некоторые пользователи могут категорически отказаться применять биометрическую систему. Для них следует предусмотреть альтернативный способ проверки подлинности.

В заключение подчеркнём, что биометрическая аутентификация пока не может служить альтернативой многофакторной аутентификации на смарт-картах. На сегодня, по моему мнению, это скорее удобство, чем полноценная технология безопасности. Но, может быть, это поможет пользователям не забывать свои пароли, кто знает?

Электронные системы идентификации и аутентификации

В состав электронных систем идентификации и аутентификации входят контактные, бесконтактные и виртуальные смарт-карты и USB-ключи (USB-token).

Контактные смарт-карты и USB-ключи

USB-ключи работают с USB-портом компьютера и изготавливаются в виде брелоков. Что такое USB-ключ, мы рассмотрим на примере токенов от компании Thales.

Поддерживаемые методы аутентификации включают контекстную аутентификацию, одноразовый пароль (OTP) и решения на основе сертификатов X.509. Все методы аутентификации доступны в различных форм-факторах, включая смарт-карты, USB-токены, программное обеспечение, мобильные приложения и аппаратные токены.

USB-токены на основе сертификатов

USB-токены на основе сертификатов Thales обеспечивают безопасный удалённый доступ, а также другие приложения, включая цифровую подпись, управление паролями, вход в сеть и комбинированный физический/логический доступ в одном USB-токене безопасности.

До сих пор можно услышать вопрос, а в чём же разница между eToken и смарт-картой?

eToken – персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и элек-

тронными цифровыми подписями (ЭЦП). eToken может быть выполнен в виде стандартной смарт-карты или USB-ключа.

- Смарт-карта требует для подключения к компьютеру PC/SC-совместимого устройства чтения смарт-карт. Она может применяться как средство визуальной идентификации (на смарт-карте может быть размещена информация о её владельце и фотография (ID-бэдж) для использования службой безопасности предприятия). Смарт-карты могут быть изготовлены из белого пластика для последующей печати (фотографии, персональных данных и т.д.) с предварительной надпечаткой, а также с наклеенной магнитной полосой либо в виде эмбосированных карт (с выдавленными символами).
- USB-ключ – напрямую подключается к компьютеру через порт USB (Universal Serial Bus), совмещая в себе функции смарт-карты и устройства для её считывания.

Если сравнивать две эти технологии, то становится очевидно, что выбор одной из них зависит от технологии безопасности, принятой в компании. Так, если планируется введение автоматизированного пропускного режима и при этом на пропусках должны быть фотография, имя владельца и прочая информация, то предпочтительно воспользоваться смарт-картами. Но стоит учесть, что потребуется купить также устройства чтения смарт-карт.

Если пропускной режим уже введён и необходимо лишь обеспечить дополнительный контроль и ужесточить режим входа в некоторые помещения, то стоит обратить внимание на eToken PRO со встроенными радиометками. Ведь службе физической безопасности, отвечающей за пропускной режим, гораздо проще контролировать пропуска при наличии на них фотографии, фамилии и имени владельца, хотя eToken PRO со встроенным RFID-чипом и аналогичная смарт-карта одинаковы по функциональности.

Основные области применения eToken

- двухфакторная аутентификация пользователей при доступе к серверам, базам данных, приложениям, разделам веб-сайтов
- безопасное хранение секретной информации: паролей, ключей ЭЦП и шифрования, цифровых сертификатов
- защита электронной почты (цифровая подпись и шифрование, доступ)
- защита компьютеров от несанкционированного доступа (НСД)
- защита сетей и каналов передачи данных (VPN, SSL)
- клиент-банк, системы типа e-banking и e-commerce

При работе с многофакторной аутентификацией пользователь получает целый ряд преимуществ. В частности, ему требуется помнить всего один пароль к eToken вместо нескольких паролей к приложениям. Кроме того, теперь отпадает необходимость в регулярной смене паролей. И в случае утери eToken ничего страшного не произойдёт: чтобы воспользоваться найденным (украденным) eToken, необходимо ещё знать его пароль. Всё это существенно повышает уровень безопасности организации. Вместе с тем нужно понимать, что eToken поддерживает работу и интегрируется со всеми основными системами и приложениями, использующими технологии смарт-карт или PKI (Public Key Infrastructure), так называемыми PKI-ready-приложениями.

Основное назначение eToken

- строгая двухфакторная аутентификация пользователей при доступе к защищённым ресурсам (компьютерам, сетям, приложениям)
- безопасное хранение закрытых ключей цифровых сертификатов, криптографических ключей, профилей пользователей, настроек приложений и пр. в энергонезависимой памяти ключа
- аппаратное выполнение криптографических операций в доверенной среде (генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хеш-функции, формирование ЭЦП)
- продукты для многофакторной аутентификации на основе мобильных телефонов и программного обеспечения, при использовании которых пользователи не нуждаются в отдельном аппаратном токене
- программные решения для аутентификации с использованием технологии OTP (One Time Password) – одноразовый пароль
- токены OTP для смартфонов SafeNet сочетают в себе безопасность проверенной двухфакторной строгой аутентификации с удобством и простотой использования OTP, генерируемых на мобильном телефоне. Токены для смартфонов SafeNet доступны для всех мобильных устройств, включая iOS, Android

Если использование аппаратных токенов известно довольно давно, то, на мой взгляд, использование мобильных телефонов в качестве токенов OTP становится особо актуальным в сложное время пандемии. Тем более что пользователи внутренне уже готовы к этому. Ведь мультифакторная аутентификация сегодня применяется как во многих сервисах электронной почты, так и социальных сетях.

Не буду подробно на этом останавливаться, тем более что не так давно уже вышли подобные статьи и видео.

В качестве средства аутентификации eToken поддерживается большинством современных операционных систем, бизнес-приложений и продуктов по информационной безопасности и может применяться для решения следующих задач:

- строгая аутентификация пользователей при доступе к информационным ресурсам: серверам, базам данных, разделам веб-сайтов, защищённым хранилищам, зашифрованным дискам и пр.
- вход в операционные системы, службы каталога, гетерогенные сети и бизнес-приложения
- внедрение систем PKI (Entrust, Microsoft CA, RSA Keon, а также в удостоверяющих центрах и системах с использованием отечественных криптопровайдеров «Крипто-Про», «Сигнал-Ком» и т.д.) – хранение ключевой информации, аппаратная генерация ключевых пар и выполнение криптографических операций в доверенной среде (на чипе смарт-карты)
- построение систем документооборота, защищённых почтовых систем – ЭЦП и шифрование данных, хранение сертификатов и закрытых ключей
- организация защищённых каналов передачи данных с использованием транспорта Интернет (технология VPN, протоколы IPSec и SSL) – аутентификация пользователей, генерация ключей, обмен ключами
- межсетевые экраны и защита периметра сети (продукты Cisco Systems, Check Point) – аутентификация пользователей
- шифрование данных на дисках – аутентификация пользователей, генерация ключей шифрования, хранение ключевой информации

- единая точка входа пользователя в информационные системы и порталы (в продуктах eTrust SSO, IBM Tivoli Access Manager, WebSphere, mySAP Enterprise Portal) и приложения под управлением СУБД Oracle – строгая двухфакторная аутентификация
- защита веб-серверов и приложений электронной коммерции – аутентификация пользователей, генерация ключей, обмен ключами
- управление безопасностью корпоративных информационных систем, интеграция систем защиты информации – eToken является единым универсальным идентификатором для доступа к различным приложениям
- поддержка унаследованных приложений и разработка собственных решений в области ИБ

USB-ключи – это преемники смарт-карт, поэтому структура USB-ключей и смарт-карт идентична.

Бесконтактные смарт-карты

Бесконтактные смарт-карты (БСК) широко используются в различных приложениях как для аутентификации (режим электронного пропуска, электронный ключ к двери и т.д.), так и для разного рода транспортных, идентификационных, расчётных и дисконтных приложений.

Важным свойством БСК, выделяющим её из ряда других смарт-карт, является отсутствие механического контакта с устройством, обрабатывающим данные с карты. Фактически надёжность технических элементов систем, использующих БСК, определяется надёжностью микросхем. Последнее обстоятельство приводит к существенному снижению эксплуатационных расходов на систему по сравнению с аналогичными системами, применяющими смарт-карты с внешними контактами.

Порядок проведения операций с БСК и устройством чтения/записи памяти карты (далее – считывателем) определяется программным приложением. При поднесении пользователем карты к считывателю происходит транзакция, то есть обмен данными между картой и считывателем и возможное изменение информации в памяти карты. Максимальное расстояние для осуществления транзакций между считывателем и картой составляет 10 см. При этом карту можно и не вынимать из бумажника. С одной стороны, это позволяет пользователю удобно и быстро произвести транзакцию, а с другой – при попадании в поле антенны карта вовлекается в процесс обмена информацией независимо от того, желал этого пользователь или нет.

Типичная начальная последовательность команд для работы приложения с картой включает следующее:

- захват карты (выбирается первая находящаяся в поле антенны считывателя карта), если необходимо – включение антиколлизионного алгоритма (команда антиколлизии сообщает приложению уникальный серийный номер захваченной карты, точнее, уникальный номер встроенной в карту микросхемы)
- выбор карты с данным серийным номером для последующей работы с памятью карты или её серийным номером.

Указанная последовательность команд выполняется за 3 мс, то есть практически мгновенно.

Далее следует аутентификация выбранной области памяти карты. Она основана на использовании секретных ключей и будет описана ниже. Если карта и считыватель узнали друг друга, то данная область памяти открывается для обмена данными и в зависимости от условий доступа могут быть выполнены команды чтения и записи, а также специализированные команды электронного кошелька (если, конечно, область соответствующим образом была размечена при персонализации карты). Команда чтения 16 байтов памяти карты выполняется за 2,5 мс, команды чтения и изменения баланса кошелька – за 9-10 мс. Таким образом, типичная транзакция, начинающаяся с захвата карты и приводящая к изменению 16 байтов памяти, совершается максимум за 16 мс.

Для аутентификации сектора памяти карты применяется трёхпроходный алгоритм с использованием случайных чисел и секретных ключей согласно стандарту ISO/IEC DIS 9798-2.

В общих чертах процесс аутентификации можно представить так. Чипы карты и устройства для работы с ней обмениваются случайными числами. На первом шаге карта посылает считывателю сформированное ею случайное число. Считыватель добавляет к нему своё случайное число, шифрует сообщение и отправляет его карте. Карта расшифровывает полученное сообщение, сравнивает своё случайное число с числом, полученным в сообщении; при совпадении она заново зашифровывает сообщение и направляет его считывателю. Считыватель расшифровывает послание карты, сравнивает своё случайное число с числом, полученным в сообщении, и при совпадении чисел аутентификация сектора считается успешной.

Итак, работа с сектором памяти возможна только после успешной аутентификации сектора выбранной карты и пока карта находится в поле антенны считывателя. При этом все данные, передаваемые по радиочастотному каналу, всегда шифруются.

Начальные (так называемые транспортные) ключи, а также условия доступа к секторам задаются во время первичной персонализации карты на заводе-изготовителе и секретным образом сообщаются эмитенту. В процессе вторичной персонализации карточки эмитентом или пользователем приложения ключи обычно меняются на другие, известные только эмитенту или пользователю. Так же (это определяется конкретным приложением) при вторичной персонализации изменяются и условия доступа к секторам памяти карты.

Бесконтактные смарт-карты разделяются на идентификаторы PROximity и смарт-карты, базирующиеся на международных стандартах ISO/IEC 15693 и ISO/IEC 14443. В основе большинства устройств на базе бесконтактных смарт-карт лежит технология радиочастотной идентификации.

Основными компонентами бесконтактных устройств являются чип и антенна. Идентификаторы могут быть как активными (с батареями), так и пассивными (без источника питания). Идентификаторы имеют уникальные 32/64-разрядные серийные номера.

Системы идентификации на базе PROximity криптографически не защищены, за исключением специальных заказных систем.

Каждый ключ имеет прошиваемый 32/64-разрядный серийный номер.

Комбинированные системы

Внедрение комбинированных систем существенно увеличивает количество идентификационных признаков и тем самым повышает безопасность.

В настоящее время существуют комбинированные системы следующих типов:

- системы на базе бесконтактных смарт-карт и USB-ключей
- системы на базе гибридных смарт-карт
- биоэлектронные системы

В корпус брелока USB-ключа встраиваются антенна и микросхема для создания бесконтактного интерфейса. Это позволяет организовать управление доступом в помещение и к компьютеру, используя один идентификатор. Такая схема применения идентификатора исключает ситуацию, когда сотрудник, покидая рабочее место, оставляет USB-ключ в разъёме компьютера, что даёт возможность работать под его идентификатором.

Применение eToken для контроля физического доступа

RFID-технология (Radio Frequency IDentification – радиочастотная идентификация) является наиболее популярной сегодня технологией бесконтактной идентификации. Радиочастотное распознавание осуществляется с помощью закреплённых за объектом так называемых RFID-меток, несущих идентификационную и другую информацию.

Помимо традиционных преимуществ RFID-технологий, комбинированные USB-ключи и смарт-карты eToken, используя единый «электронный пропуск» для контроля доступа в помещения и к информационным ресурсам, позволяют:

- сократить расходы
- защитить инвестиции, сделанные в ранее приобретённые СКУД, за счёт интеграции eToken с большинством типов RFID-меток
- уменьшить влияние человеческого фактора на уровень информационной безопасности организации: сотрудник не сможет покинуть помещение, оставив комбинированную карту на рабочем месте
- автоматизировать учёт рабочего времени и перемещений сотрудников по офису
- провести поэтапное внедрение путём постепенной замены выходящих из эксплуатации идентификаторов

Применение гибридных смарт-карт для контроля физического доступа

Гибридные смарт-карты содержат разнородные чипы: один чип поддерживает контактный интерфейс, другой – бесконтактный. Как и в случае гибридных USB-ключей, гибридные смарт-карты решают две задачи: контроль доступа в помещение и к компьютеру. Дополнительно на карту можно нанести логотип компании, фотографию сотрудника или магнитную полосу, что позволяет заменить на такие карты обычные пропуска и перейти к единому электронному пропуску.

Электронные ключи с одноразовыми паролями

Идентификаторы на базе генераторов разовых паролей применяются чаще всего для организации веб-доступа или систем типа e-banking.

Аппаратные реализации генераторов одноразовых паролей называют OTP-токенами. Они имеют небольшой размер и выпускаются в различных форм-факторах:

- карманный калькулятор
- брелок
- смарт-карта
- устройство, комбинированное с USB-ключом
- специальное программное обеспечение для карманных компьютеров

Одной из распространённых аппаратных реализаций одноразовых паролей является технология SecurID, предлагаемая компанией RSA Security. Она основана на специальных калькуляторах – токенах, которые ежеминутно генерируют новый код. В токен встроена батарейка, заряда которой хватает на 3-5 лет, после чего токен нужно менять. Существуют и другие реализации одноразовых паролей. Например, можно генерировать пароль по событию – нажатию клавиши на устройстве. Такое решение предлагает компания Secure Computing в виде продукта Safeword. Аппаратную реализацию технологии «запрос-ответ» представляет корпорация Thales.

Различие между технологиями RSA Security ID и eToken Pass заключается в том, что разовый пароль в RSA SecurID изменяется через заранее заданные промежутки времени (синхронизация по времени), а в продукте eToken Pass смена разового пароля производится по нажатию кнопки (синхронизация по событию).

При необходимости получить соединение с сетью пользователь вводит PIN-код, а затем генерирует разовый пароль, нажимая кнопку на eToken Pass. При этом пароль формируется как PIN-код плюс Token-код. На стороне сети этот пароль проверяется с помощью специального серверного ПО.

Второй вариант такого подхода реализован в продуктах компании RSA Security. С точки зрения конечного пользователя, разница между обычной процедурой регистрации в системе Windows и аутентификацией в системе RSA SecurID состоит лишь в том, что вместо стандартного пароля требуется ввести составной код доступа, состоящий из личного PIN-кода и комбинации цифр, которая в данный момент отображается на экране жетона-аутентификатора. Затем этот код доступа отсылается серверу RSA Authentication Manager, который и выполняет проверку подлинности пользователя.

RSA SecurID for Microsoft Windows обеспечивает интеграцию с контроллерами доменов Windows и каталогами Active Directory. База данных пользователей и групп сервера аутентификации RSA Authentication Manager синхронизирована с каталогом Active Directory.

Выводы

Рассмотрев различные технологии аппаратно-программной и парольной аутентификации, можно сделать вывод, что применение паролей всё меньше соответствует требованиям безопасности, так как с увеличением сложности паролей и количества их для запоминания будет возрастать роль человеческого фактора, а значит:

- пользователи всегда будут выбирать наиболее простые, с их точки зрения, пароли
- при ужесточении политики паролей пользователи будут идти на всяческие ухищрения, облегчающие им пользование паролями, но снижающие безопасность (например, наклеивать стикеры с паролем на монитор, клавиатуру, записывать пароль в блокнот и т.д.)
- с ростом вычислительных мощностей процесс подбора паролей будет происходить всё быстрее.

В связи с этим необходим переход на многофакторную аутентификацию, из всех видов которой самым надёжным сегодня является применение USB-ключей (смарт-карт).

Владимир Безмалый
Kaspersky Certified Trainer