Содержание:

Введение

В настоящее время информационные системы (ИС) различного масштаба стали неотъемлемой частью базовой инфраструктуры государства, бизнеса, гражданского общества. Все больше защищаемой информации переносится в ИС. Современные информационные технологии не только обеспечивают новые возможности организации бизнеса, ведения государственной и общественной деятельности, но и создают значительные потребности в обеспечении безопасности для защиты информации.

Основными процедурами регистрации пользователей в ИС являются процедура идентификации - получение ответа на вопрос «Кто Вы?» и аутентификации - доказательства того, что «Вы именно тот, кем представляетесь». Несанкционированное получение злоумышленником доступа к ИС связано, в первую очередь, с нарушением процедуры аутентификации.

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация - это первая линия обороны, "проходная" информационного пространства организации.

Аутентификация и идентификация

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации - процедура входа пользователя в систему.

Этапы аутентификации: Процесс аутентификации пользователя компьютером можно разделить на два этапа: ·подготовительный - выполняется при регистрации пользователя в системе. Именно тогда у пользователя запрашивается образец аутентификационной информации, например, пароль или контрольный отпечаток пальца, который будет рассматриваться системой как эталон при аутентификации; ·штатный - образец аутентификационной информации запрашивается у пользователя снова и сравнивается с хранящимся в системе эталоном. Если образец схож с эталоном с заданной точностью - пользователь считается узнанным, в противном случае пользователь будет считаться чужим, результатом чего будет, скажем, отказ в доступе на компьютер.

В открытой сетевой среде между сторонами идентификации и аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения и/или воспроизведения данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

Надежная идентификация и аутентификация затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Вещественный фактор

Вещественный фактор (Аппаратная аутентификация) — «то, чем ты владеешь». Второй по популярности фактор аутентификации. В первую очередь под этим понимаются аппаратно-программные системы идентификации и аутентификации (СИА) или устройства ввода идентификационных признаков. В состав СИА входят аппаратные идентификаторы, устройства ввода-вывода (считыватели, контактные устройства, адаптеры, разъемы системной платы и др.) и соответствующее ПО. Идентификаторы предназначены для хранения уникальных идентификационных признаков. Кроме этого они могут хранить и обрабатывать конфиденциальные данные. Устройства ввода-вывода и ПО осуществляют обмен данными между идентификатором и защищаемой системой.

В электронных СИА идентификационные признаки представляются в виде цифрового кода, хранящегося в памяти идентификатора. По способу обмена данными между идентификатором и устройством ввода-вывода электронные СИА подразделяются на:

контактные:

- iButton — information button — информационная «таблетка»;
- смарт-карты — интеллектуальные карты;
- USB-ключи или USB-токены (token — опознавательный признак, маркер);

бесконтактные:

- RFID-идентификаторы — radio-frequency identification — радиочастотные идентификаторы;
- смарткарты.

Биофактор

Биофактор (Биометрическая аутентификация) — «то, что является частью тебя». Биометрические данные, для снятия которых, как правило, необходимы специальные программно-аппаратные средства — так называемые,

биометрические сканеры, которые различаются по характеру считываемых данных.

В соответствии с этим и биометрические характеристики можно разделить на две большие группы:

1. физиологические биометрические характеристики (также называемые физическими биометрическими характеристиками, статическими биометрическими характеристиками). Съём этих характеристик производится сканерами основанными на статистических методах:

- Распознавание по отпечаткам пальцев. Это — самый распространенный 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 (свертку) и сравнивается с ранее введенным шаблоном (эталоном) или набором шаблонов;
- Распознавание по геометрии руки. Данный статический метод построен на распознавании геометрии кисти руки, также являющейся уникальной биометрической характеристикой человека. С помощью специального устройства, позволяющего получать трехмерный образ кисти руки (некоторые производители сканируют форму нескольких пальцев), получаются измерения, необходимые для получения уникальной цифровой свертки, идентифицирующей человека;
- по расположению вен на лицевой стороне ладони. С помощь инфракрасной камеры считывается рисунок вен на лицевой стороне ладони или кисти руки, полученная картинка обрабатывается и по схеме расположения вен формируется цифровая свертка;
- .по радужной оболочке глаза. Этот метод распознавания основан на уникальности рисунка радужной оболочки глаза. Для реализации метода необходима камера, позволяющая получить изображение глаза человека с достаточным разрешением, и специализированное программное обеспечение, позволяющее выделить из полученного изображения рисунок радужной оболочки глаза, по которому строится цифровой код для идентификации человека.
- По капилярам сетчатки глаз.
- По форме лица. В данном методе идентификации строится трехмерный образ лица человека. На лице выделяются контуры бровей, глаз, носа, губ и т.д., вычисляется расстояние между ними и строится не просто образ, а еще множество его вариантов на случаи поворота лица, наклона, изменения

выражения. Количество образов варьируется в зависимости от целей использования данного способа (для аутентификации, верификации, удаленного поиска на больших территориях и т.д)
- По термограмме лица. В основе данного способа аутентификации лежит уникальность распределения на лице артерий, снабжающих кровью кожу, которые выделяют тепло. Для получения термограммы, используются специальные камеры инфракрасного диапазона. В отличие от предыдущего – этот метод позволяет различать близнецов.
- По ДНК. Преимущества данного способы очевидны, однако используемые в настоящее время методы получения и обработки ДНК – работают настолько долго, что такие системы используются только для специализированных экспертиз.
- по подногтевому слою кожи;
- по объему указанных для сканирования пальцев;
- по форме уха;
- по запаху тела.

1. поведенческие биометрические характеристики (также называемые динамическими биометрическими характеристиками) — биометрические характеристики, основанные на данных, полученных путем измерения действий человека. Характерной чертой для поведенческих характеристик является их протяженность во времени — измеряемое действие имеет начало, середину и конец. Съём этих характеристик производится биометрическими сканерами, основанными на динамических методах:

- Распознавание по рукописному почерку. Как правило, для этого динамического метода идентификации человека используется его подпись (иногда написание кодового слова). Цифровой код идентификации формируется по динамическим характеристикам написания, то есть для идентификации строится свертка, в которую входит информация по графическим параметрам подписи, временным характеристикам нанесения подписи и динамики нажима на поверхность в зависимости от возможностей оборудования (графический планшет, экран карманного компьютера и т. д.);
- Распознавание по клавиатурному почерку. Метод в целом аналогичен вышеописанному, однако вместо подписи в нем используется некое кодовое слово, а из оборудования требуется только стандартная клавиатура. Основная характеристика, по которой строится свертка для идентификации, — динамика набора кодового слова;

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

Использование смарт-карт и USB-ключей

Несмотря на то что криптография с открытым ключом согласно спецификации X.509 может обеспечивать строгую аутентификацию пользователя, сам по себе незащищенный закрытый ключ подобен паспорту без фотографии. Закрытый ключ, хранящийся на жестком диске компьютера владельца, уязвим по отношению к прямым и сетевым атакам. Достаточно подготовленный злоумышленник может похитить персональный ключ пользователя и с помощью этого ключа представляться этим пользователем. Защита ключа с помощью пароля помогает, но недостаточно эффективно — пароли уязвимы по отношению ко многим атакам. Несомненно, требуется более безопасное хранилище.

Аутентификацию на основе смарт-карт и USB-ключей сложнее всего обойти, так как используется уникальный физический объект, которым должен обладать человек, чтобы войти в систему. В отличие от паролей владелец быстро узнает о краже и может сразу принять необходимые меры для предотвращения ее негативных последствий. Кроме того, реализуется двухфакторная аутентификация. Микропроцессорные смарт-карты и USB-ключи могут повысить надежность служб PKI: смарт-карта может использоваться для безопасного хранения закрытых ключей пользователя, а также для безопасного выполнения криптографических преобразований. Безусловно, данные устройства аутентификации не обеспечивают абсолютную безопасность, но надежность их защиты намного превосходит возможности обычного настольного компьютера.

Заключение

Различные технологии идентификации и аутентификации используются уже более 20 лет. Тем не менее они продолжают активно развиваться во всех направлениях,

создавая все новые способы идентифицировать пользователя или процесс в системе. Существует много различных способов аутентификации и идентификации, от считывания биометрической информации, до ввода обычных паролей в системе. У каждых из этих способов есть свои преимущества и недостатки, связанные с удобством для самих пользователей, удобством администрирования всего этого и степенью безопасности.

Литература

1. Идентификация и аутентификация. [Электронный ресурс]. – Режим доступа: http://pmn.narod.ru/secur/audit/ia.htm
2. Классификация механизмов аутентификации пользователей и их обзор. [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/177551/
3. О технологиях идентификации и аутентификации. [Электронный ресурс]. – Режим доступа: http://www.aladdin-rd.ru/company/pressroom/articles/8097/