Содержание

1. Понятие

Аутентификация — процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является

именно тем субъектом, идентификатор которого он использует. Для этого он должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т.п.).

2. Основные методы

2.1 Методы аутентификации

Способы аутентификации пользователей различаются прежде всего аутентификационными факторами.

Аутентификационный фактор — определенный вид информации, предоставляемый субъектом системе при его аутентификации.

Нечто, нам известное: пароль. Отличительная характеристика представляет собой секретную информацию, которая неизвестна непосвященным людям. При некомпьютерном использовании это может быть произносимый голосом пароль или запоминаемая комбинация для замка. В случае вычислительных систем это может быть пароль, вводимый с помощью клавиатуры.

Разработчики могут дешево и легко реализовать паролевый механизм. Запоминаемое секретное слово может быть наиболее удобным средством с точки зрения перемещающихся пользователей, т.е. для людей, которые подключаются к системе из непредсказуемых удаленных мест.

Однако использование паролей не лишено недостатков. Во-первых, их эффективность зависит от секретности, а хранить пароли в тайне нелегко. Существует бессчетное количество способов выведать или перехватить пароль, и обычно обнаружить активную разведку до нанесения урона невозможно. Во-вторых, развитие методов нападения сделало для взломщиков определение паролей, обычно выбираемых людьми, относительно простым делом. Даже если выбираются трудноугадываемые пароли, их где-нибудь записывают, чтобы при необходимости иметь под рукой. Но конечно же, записываемый пароль более уязвим в плане возможной кражи, чем запоминаемый. Даже действующие из лучших побуждений люди в какой-то момент нарушают правила использования паролей просто для того, чтобы иметь возможность воспользоваться своим компьютером именно тогда, когда в этом возникнет необходимость.

Нечто, присущее нам: биометрика. Отличительной характеристикой является какая-нибудь физическая особенность, уникальная для аутентифицируемого лица. До появления компьютеров это могли быть личная подпись, фотография, отпечаток пальца или письменное описание внешнего вида человека. При компьютерном использовании отличительная характеристика физического лица измеряется и сравнивается с ранее полученными данными, снятыми с достоверно установленной личности. В хорошо известных методиках для аутентификации используются голос человека, отпечатки пальцев, письменная подпись, форма кисти или особенности радужной оболочки глаза.

Нечто, имеющееся у нас: устройство аутентификации. Отличительной характеристикой является наличие у авторизованного лица некоего конкретного предмета. При некомпьютерном использовании это могли быть печать или ключ от замка. В компьютерных системах это может быть не более чем носитель с файлом данных, содержащим отличительную характеристику. Часто характеристика встраивается в устройство, например в карту с магнитной полосой, смарт-карту, USB-ключ или в OTP-токен. Кроме того, подобные устройства часто предлагают возможность так называемой многофакторной аутентификации.

Многофакторная аутентификация — аутентификация, в процессе которой используются аутентификационные факторы нескольких типов.

Например, пользователь должен предоставить смарт-карту и дополнительно ввести пароль. Также используются понятия двухфакторной и трехфакторной аутентификации при использовании в процессе аутентификации комбинации двух и трех типов аутентификационных факторов соответственно.

Метод аутентификации (метод регистрации) — специфика использования определенного типа аутентификационных факторов в процедуре аутентификации.
Кроме методов локальной аутентификации — входа пользователя локально в компьютер, существуют методы для аутентификации в локальных вычислительных сетях, при доступе к удаленным ресурсам, веб-приложениям и др. Методы используются в рамках аутентификационных протоколов.

2.2. Протоколы сетевой аутентификации

Существует несколько различных протоколов, описывающих процесс аутентификации субъектов в локальной сети. В рамках операционных систем Windows компании Microsoft использовались протоколы LAN Manager (LM), NT LAN Manager (NTLM), NT LAN Manager версии 2 (NTLM v2) и Kerberos. В качестве примера рассмотрим последний как наиболее распространенный и защищенный на сегодняшний день протокол аутентификации в локальных сетях.
Протокол аутентификации Kerberos. Протокол Kerberos был специально разработан, для того чтобы обеспечить надежную аутентификацию пользователей. Протокол Kerberos может использовать централизованное хранение аутентификационных данных и является основой для построения механизмов Single Sign-On (возможность одноразовой аутентификации в нескольких приложениях). Протокол Kerberos предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними с учетом того, что начальный обмен информацией между клиентом и сервером может происходить в незащищенной среде, а передаваемые пакеты — перехвачены и модифицированы.
Протокол основан на понятии ticket (билет, удостоверение). Ticket является зашифрованным пакетом данных, выданным выделенным доверенным центром аутентификации, в терминах протокола Kerberos — Key Distribution Center (KDC — центр распределения ключей).
Когда пользователь выполняет первичную аутентификацию, после успешного подтверждения его подлинности KDC выдает первичное удостоверение пользователя для доступа к сетевым ресурсам — Ticket Granting Ticket (TGT). В дальнейшем при обращении к отдельным сетевым ресурсам пользователь, предъявляя TGT, получает от KDC удостоверение для доступа к конкретному сетевому ресурсу — Service Ticket.
Одним из преимуществ протокола Kerberos, обеспечивающим очень высокий уровень сетевой безопасности, является то, что во всех сетевых взаимодействиях не передаются ни пароли, ни хэши паролей в открытом виде. Все удостоверения являются зашифрованными пакетами данных.
В качестве примера реализации протокола Kerberos следует отметить доменную аутентификацию пользователей в операционных системах компании Microsoft, начиная с Windows 2000.
Последняя версия — Kerberos 5 описана в рамках стандарта IETF (RFC 1510, RFC 1964).

2.3 Протоколы аутентификации для удаленного доступа

Часть протоколов сетевой аутентификации были разработаны специально для обеспечения удаленного доступа к информационным ресурсам посредством открытых каналов связи (например, телефонные линии, Интернет). В качестве примера можно привести протоколы PAP, CHAP, EAP, RADIUS, TACACS и др. В качестве примера рассмотрим работу протокола RADIUS.
Протокол аутентификации RADIUS. Протокол аутентификации Remote Authentication Dial-in User Service (RADIUS) рассматривается как механизм аутентификации и авторизации удаленных пользователей в условиях распределенной сетевой инфраструктуры, предоставляющий централизованные услуги по проверке подлинности и учету для служб удаленного доступа.
В рамках стандарта выделяются следующие роли:

• *Клиент RADIUS. Клиент RADIUS принимает от пользователей запросы на аутентификацию. Все принятые запросы переадресовываются серверу RADIUS для последующей аутентификации и авторизации. Как правило, в качестве клиента протокола RADIUS выступает сервер удаленного доступа.*
• *Сервер RADIUS. Основная задача сервера RADIUS заключается в централизованной обработке информации, предоставленной клиентами RADIUS. Один сервер способен обслуживать несколько клиентов RADIUS. Сервер осуществляет проверку подлинности пользователя и его полномочий. При этом в зависимости от реализации сервера RADIUS для проверки подлинности используются различные базы данных учетных записей.*
• *Посредник RADIUS. Взаимодействие клиентов и серверов RADIUS осуществляется посредством специальных сообщений. В распределенных сетях клиент и сервер RADIUS могут быть разделены различными сетевыми устройствами (такими, например, как маршрутизатор). Под посредником RADIUS понимается сетевое устройство, способное осуществлять перенаправление сообщений протокола RADIUS.*

Поддержка протокола RADIUS реализована на многих современных платформах, что позволяет использовать его в межплатформенных решениях.

В качестве примера сервера и посредника RADIUS можно привести реализованную в Windows Server 2003 службу проверки подлинности в Интернете (Internet Authentication Service — IAS). Эта служба позиционируется как механизм централизованной аутентификации и авторизации пользователей, использующих различные способы подключений к сети. Служба IAS интегрирована с другими сетевыми службами Windows Server 2003, такими, как служба маршрутизации и удаленного доступа и служба каталога Active Directory.

Протокол RADIUS детально описан в открытых стандартах RFC 2138 и 2139.

2.4 Инфраструктура открытых ключей (PKI)

Для целей аутентификации в локальных сетях при удаленном и веб-доступе часто применяют криптографические механизмы, основанные на асимметричных алгоритмах шифрования и сертификатах открытого ключа. Данные механизмы, как правило, применяются в сочетании с инфраструктурой открытых ключей.

Инфраструктура открытых ключей (Public Key Infrastructure — PKI) — инфраструктура, предназначенная для управления сертификатами открытых ключей в целях поддержки услуг аутентификации, шифрования, целостности и неотказуемости (неотрицания авторства). Подлинность открытого криптографического ключа и его связь с определенным пользователем в рамках PKI удостоверяются сертификатом открытого ключа. Более того, принадлежность сертификата открытого ключа заверяется специальным доверенным учреждением — центром сертификации.

Сертификат открытого ключа — цифровой документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. В сертификате открытого ключа содержатся также сведения об открытом ключе, его назначении и области применения, а также наименование центра сертификации, выдавшего данный сертификат. Информация, содержащаяся в сертификате открытого ключа, снабжается цифровой подписью центра сертификации. На практике наиболее часто используются сертификаты стандарта X.509v3.

Центр сертификации (Certificate Authority — CA) — доверенная третья сторона, чья подпись под сертификатом подтверждает подлинность и целостность открытого ключа и принадлежность его соответствующему владельцу.

Список отозванных сертификатов (Certificate Revocation List — CRL) — каталог скомпрометированных сертификатов.

Простейшую модель PKI можно построить с использованием только одного CA. При этом пользователи будут применять криптографические операции с открытым ключом в своих приложениях при получении и обработку сертификатов и CRL. Однако достаточно трудно при наличии только одного CA обеспечить необходимый уровень масштабируемости при выполнении всех задач, связанных с созданием и распространением сертификатов и CRL.

Поэтому обычно PKI строится из различных компонентов, каждый из которых предназначен для специализированного выполнения нескольких задач.
Аутентификация с использованием сертификатов открытого ключа. Механизмы аутентификации на основе сертификатов обычно используют протокол с запросом и ответом. Согласно этому протоколу сервер аутентификации направляет пользователю последовательность символов, называемую запросом, а программное обеспечение клиентского компьютера для генерирования ответа вырабатывает с помощью закрытого ключа пользователя цифровую подпись под запросом от сервера аутентификации.
Общий процесс подтверждения подлинности пользователя состоит из следующих стадий:
1) получения открытого ключа CA (одноразовый процесс);
2) получения по некоторому незащищенному каналу от этого пользователя его сертификата открытого ключа;
3) получения идентификатора пользователя:
— проверка даты и времени относительно срока действия (при наличии такового), указанного в сертификате, на основе локальных доверенных часов (время/день/год);
— проверка действительности открытого ключа CA;
— проверка подписи под сертификатом пользователя с помощью открытого ключа CA;
— проверка сертификата на предмет отзыва;
4) если все проверки успешны, открытый ключ в сертификате считается подлинным открытым ключом заявленного пользователя;
5) проверки на наличие у пользователя закрытого ключа, соответствующего данному сертификату, с помощью алгоритма запрос-ответ.
В качестве примеров алгоритмов, работающих таким образом, можно назвать протокол SSL.
Аутентификация с открытым ключом используется как защищенный механизм аутентификации в таких протоколах, как SSL; также может использоваться как один из методов аутентификации в рамках протоколов Kerberos и RADIUS.

3. Технические средства

3.1 Биометрия

Современные технологии способны обеспечить удостоверение личности человека, используя характерные только для него одного характеристики. Данные технологии основаны на практическом применении знаний научной дисциплины биометрии. Данная дисциплина занимается статистическим анализом биологических наблюдений и явлений.
Биометрическая характеристика — это измеримая физиологическая или поведенческая черта живого человека.
Некоторые биометрические характеристики уникальны для данного человека, и их можно использовать для установления личности или проверки декларируемых личных данных:
— для идентификации пользователя (вместо ввода имени пользователя);
— для однофакторной аутентификации пользователя;
— совместно с паролем или аутентификационным токеном (таким, как смарт-карта) — для обеспечения двухфакторной аутентификации.
Биометрические характеристики делятся на группы.
Физиологические биометрические характеристики (также называемые физическими биометрическими характеристиками, статическими биометрическими характеристиками) — биометрические характеристики, основанные на данных, полученных путем измерения анатомических характеристик человека, таких, как отпечаток пальца, форма лица или кисти, сетчатка глаза.
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. К примеру: голос, подпись.

Хотя биометрические технологии отличаются в объектах и способах измерений, все биометрические системы работают одинаково. Пользователь предоставляет образец (sample) — опознаваемое необработанное изображение или запись физиологической или поведенческой характеристики — посредством 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 числовые последовательности; сам обра¬зец невозможно восстановить из шаблона.

Результат проверки других аутентификационных данных, как правило, однозначен — это решение «да» или «нет» (пароль совпал или нет). В случае проверки контрольного шаблона результат иной. Контрольный шаблон сравнивается с эталонным шаблоном (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 степень совпадения должна превышать определенную настраиваемую пороговую величину.

Соответственно в биометрических системах контрольный шаблон может быть ошибочно признан:

— соответствующим эталонному шаблону другого лица;

— не соответствующим эталонному шаблону данного пользователя, несмотря на то что этот пользователь зарегистрирован в биометрической системе.

Точность биометрической системы измеряется двумя параметрами:

— коэффициентом неверных совпадений (FMR), также известным под названием «ошибка типа I» или «вероятность ложного допуска» (FAR);

— коэффициентом неверных несовпадений (FNMR), также известным под названием «ошибка типа II» или «вероятность ложного отказа в доступе» (FRR).

Биометрическая аутентификация обычно является одним из наиболее легких подходов для тех людей, которые должны проходить аутентификацию. В большинстве случаев хорошо спроектированная биометрическая система просто снимает показания с человека и правильно выполняет аутентификацию.

Однако все преимущества сводятся на нет несколькими недостатками. Как правило, по сравнению с другими системами приобретение, установка и эксплуатация оборудования стоят дорого. При дистанционном использовании биометрические показания подвержены риску перехвата: похититель может воспроизвести запись показаний, чтобы замаскировать себя под владельца, или использовать их в целях выслеживания последнего. Если биометрические показатели попадают в плохие руки, то их владелец не имеет способа восполнения ущерба, так как биометрические особенности невозможно изменить.

Кроме того, сам процесс аутентификации сложен. Сложно также сделать систему достаточно чувствительной, чтобы она отвергала посторонних пользователей и при этом время от времени не отвергала своих. Биометрические показатели также могут быть признаны негодными вследствие физиологических изменений и телесных повреждений.

Был случай, когда биометрическое устройство не впустило в режимное помещение работавшую там женщину, потому что из-за беременности у нее изменилась картина кровеносных сосудов в сетчатке глаз.

3.2 Смарт-карты и USB-ключи

Несмотря на то что криптография с открытым ключом может обеспечивать аутентификацию пользователя, сам по себе 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.

Смарт-карты. Смарт-карты — пластиковые карты стандартного размера банковской карты (стандарт ISO 7816-1), имеющие встроенную микросхему. Они находят все более широкое применение в различных областях, от систем накопительных скидок до кредитных и дебетовых карт, студенческих билетов и телефонов стандарта GSM.

Для использования смарт-карт в компьютерных системах необходимо устройство чтения смарт-карт. Несмотря на название — устройство чтения (или считыватель), большинство подобных оконечных устройств, или устройств сопряжения (IFD), способны как считывать, так и записывать информацию, если позволяют возможности смарт-карты и права доступа. Устройства чтения смарт-карт могут подключаться к компьютеру посредством последовательного порта, слота PCMCIA или USB. Устройство чтения смарт-карт также может быть встроено в клавиатуру.

Как правило, для доступа к защищенной информации, хранящейся в памяти смарт-карты, требуется пароль, называемый PIN-кодом (англ. Personal Identification Number — персональ¬ный идентификационный номер).

USB-ключи. Некоторые производители выпускают другие виды аппаратных устройств, представляющие собой комбинацию смарт-карты и устройства чтения смарт-карт. Они по свойствам памяти и вычислительным возможностям полностью аналогичны смарт-картам. Наиболее популярны аппаратные «ключи», использующие порт USB. USB-ключи привлекательны для некоторых организаций, поскольку USB стал стандартным портом для подключения периферийных устройств: организации не нужно приобретать для пользователей какие бы то ни было считыватели.

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 (а в случае решений совместно с биометрической информацией и трехфакторная) аутентификация. Основными слабыми местами являются более высокая стоимость реализации и риск дополнительных расходов, связанных с потерей аппаратуры.

Смарт-карты, USB-ключи и другие устройства аутентификации могут повысить надежность служб PKI: смарт-карта может использоваться для безопасного хранения закрытых ключей пользователя, а также для безопасного выполнения криптографических преобразований. Безусловно, устройства аутентификации не обеспечивают абсолютную безопасность, но надежность их защиты намного превосходит возможности обычного настольного компьютера.

Хранить и использовать закрытый ключ можно по-разному, и разные разработчики используют различные подходы. Наиболее простой из них — использование устройства аутентификации в качестве защищенного носителя аутентификационной информации: при необходимости карта экспортирует закрытый ключ, и криптографические операции осуществляются на рабочей станции. Этот подход является не самым совершенным с точки зрения безопасности, зато относительно легко реализуемым и предъявляющим невысокие требования к устройству аутентификации. В качестве примера подобного рода устройств аутентификации можно привести Aladdin eToken R2, Rainbow iKey 1000, Актив ruToken.

Два следующих подхода более безопасны, поскольку предполагают выполнение устройством аутентификации криптографические операции. В первом случае пользователь генерирует ключи на рабочей станции и сохраняет их в памяти устройства, во втором — с помощью устройства. В обоих случаях, после того как закрытый ключ сохранен, его нельзя извлечь из устройства и получить любым другим способом.

Генерация ключевой пары вне устройства. В этом случае пользователь может сделать резервную копию закрытого ключа. Если устройство выйдет из строя, будет потеряно, повреждено или уничтожено, пользователь сможет сохранить тот же закрытый ключ в памяти нового устройства. Это необходимо, если пользователю требуется расшифровать

какие-либо данные, сообщения и так далее, зашифрованные с помощью соответствующего открытого ключа. Однако при этом закрытый ключ пользователя подвергается риску быть похищенным.

Генерация ключевой пары с помощью устройства. В этом случае закрытый ключ не появляется в открытом виде и нет риска, что злоумышленник украдет его резервную копию. Единственный способ использования закрытого ключа — это обладание устройством аутентификации. Являясь наиболее безопасным, это решение выдвигает высокие требования к возможностям самого устройства: оно должно обладать функциональностью генерации ключей и осуществления криптографических преобразований. Это решение также предполагает, что закрытый ключ не может быть восстановлен в случае выхода устройства из строя и т.п. Об этом необходимо беспокоиться при использовании закрытого ключа для шифрования, но не там, где он используется для аутентификации, или в других службах, использующих цифровые подписи.

Подобным образом способны работать процессорные смарт-карты и USB-токены на их основе, к примеру Aladdin eToken PRO, eToken NG OTP, Rainbow iKey 2000, iKey 3000, Athena ASECard Crypto, Schlumberger Cryptoflex, ActivCard USB Key и др.

3.2 Одноразовые пароли

В основе всех методов аутентификации с использованием пароля лежит предположение о том, что только законный пользователь может успешно пройти проверку личности, что только он знает свой пароль. Часто злоумышленник может легко узнать идентификатор пользователя. Особенно если в качестве идентификатора пользователя используется не случайная строка символов, состоящая из букв и цифр, а «имя пользователя». Так как обычно «имя пользователя» — это различные варианты комбинации имени и фамилии пользователя, то определить имя пользователя не составляет большого труда. Соответственно если злоумышленнику удастся узнать еще и пароль, то злоумышленнику будет легко представиться соответствующим пользователем. Сколь бы ни был пароль засекречен, узнать его иногда не слишком трудно. Злоумышленник может сделать это, используя различные способы атак.

Для каждой из этих атак есть методы защиты. Но большинство из этих методов обладают различными недостатками. Некоторые виды защиты достаточно дороги (борьба с паразитным излучением оборудования), другие создают неудобства для пользователей (правила формирования пароля, использование длинных паролей). Один из вариантов защиты от различных атак на аутентификацию по паролю — это переход на аутентификацию с использованием одноразовых паролей.

Одноразовые пароли (One-Time Passwords — OTP) — динамическая аутентпификационная информация, генерируемая для единичного использования с помощью аутентификационных токенов (программных или аппаратных).

OTP-токен — мобильное персональное устройство, принадлежащее определенному пользователю, генерирующее одноразовые пароли, используемые для аутентификации данного пользователя.

Аутентификация с одноразовым паролем обладает устойчивостью к атаке анализа сетевых пакетов, что дает ей значительное преимущество перед запоминаемыми паролями. Несмотря на то что злоумышленник может перехватить пароль методом анализа сетевого трафика, поскольку пароль действителен лишь один раз или в течение ограниченного промежутка времени, у злоумышленника в лучшем случае есть весьма ограниченная возможность представиться пользователем посредством перехваченной информации.

Для того чтобы сгенерировать OTP, необходимо иметь OTP-токен. Таким образом, при использовании OTP вместо аутентификационного фактора «нечто, нам известное» применяется другой аутентификационный фактор — «нечто, имеющееся у нас».

Другим важным преимуществом аутентификационных устройств является то, что многие из них требуют от пользователя введения PIN-кода или пароля, который может использоваться различными способами, в частности:

— *для активации OTP-токена;*
— *в качестве дополнительной информации, используемой при генерации OTP;*
— *для предъявления серверу аутентификации вместе с OTP.*

В этих методах аутентификации используются два аутентификационных фактора. Поэтому они относятся к двухфакторной аутентификации.

OTP-токены имеют небольшой размер и выпускаются в виде (форм-факторы):

— *карманного калькулятора;*
— *брелока;*
— *смарт-карты;*
— *устройства, комбинированного с USB-ключом;*
— *специального программного обеспечения для карманных компьютеров.*

В качестве примера решений OTP можно привести линейку RSA SecurlD, ActivCard Token, комбинированный USB-ключ Aladdin eToken NG-OTP.

4. Список литературы:

1. *Д. Ф. Куроуз. Компьютерные сети. 2-е изд. – СПб. Питер, 2004 г.*
2. *В. Столингс. Передача данных. 4-е изд. – СПб. Питер, 2004 г.*
3. *www.excode.ru*