О. В. Куликова

МЕТОДЫ И СРЕДСТВА АУТЕНТИФИКАЦИИ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ[1]

Введение

Задача идентификации и аутентификации пользователей является ключевой задачей защиты информации от несанкционированного доступа, решаемой системой защиты информации в любой информационной системе. В последнее десятилетие интенсивно развивается направление электронной цифровой аутентификации, в которой сбор информации происходит с минимальным участием человека. Технологии автоматической аутентификации наиболее полно соответствуют требованиям компьютерных систем и систем управления, где нужно четко распознавать объекты в режиме реального времени.

Перед получением доступа к ресурсам компьютерной системы пользователь должен зарегистрироваться. Процесс регистрации пользователя в любой системе состоит из трех взаимосвязанных последовательно выполняемых процедур: идентификации, аутентификации и авторизации [1]. При этом под идентификацией понимается процедура распознавания субъекта по его идентификатору. Для контроля процедуры идентификации используется аутентификация.

Аутентификация — процедура проверки подлинности субъекта, которая позволяет достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Цель идентификации и аутентификации заключается в том, чтобы гарантировать, что в корпоративной информационной системе работают только легальные пользователи. Эти две процедуры можно считать основой программно-технических средств безопасности, поскольку вся разграничительная политика доступа к ресурсам реализуется относительно идентификаторов пользователей. После прохождения субъектом процедуры аутентификации ему предоставляются определенные права доступа к ресурсам системы, т. е. выполняется авторизация. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к ее ресурсам.

Для подтверждения свой подлинности субъект должен предоставить некоторую секретную информацию, которая должна быть доступна только ему одному. Он может предъявлять системе различные виды информации, называемые факторами аутентификации. Выделяют три фактора аутентификации, которые могут использоваться в различных комбинациях: «на основе знания чего-либо» (например, пароль, PIN-код), «обладания чем-либо» (например, смарт-карта, токен), «на основе биометрических характеристик» (например, отпечаток пальца, голос). Аутентификация, в процессе которой используется только один фактор аутентификации, называется однофакторной. Многофакторной называется аутентификация, в процессе которой используются несколько факторов аутентификации, такая аутентификация более безопасна по сравнению с однофакторной.

Далее в статье рассматриваются и анализируются основные технологии аутентификации, которые могут использоваться в различных комбинациях.

1. Парольная аутентификация

Для проверки подлинности пользователей в информационных системах наиболее широко используется аутентификация по паролю. Каждый субъект компьютерной системы имеет пароль — секрет, который он разделяет с системой. Демонстрация знания этого секрета (чаще всего путем

[1]Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

разглашения самого пароля) принимается системой как подтверждение подлинности субъекта [2, 3]. Такая аутентификация проста и уже давно встроена в операционные системы и другие сервисы. Данный вид аутентификации характеризуется практически полным отсутствием вероятностных ошибок аутентификации, однако по совокупности характеристик он считается самым слабым средством аутентификации, поскольку пароль можно украсть, подсмотреть, подобрать и т. д. На стойкость пароля влияют его длина, алфавит, предельное количество попыток его ввода, минимальное время, которое должно пройти между попытками. Пароли можно разделить на две большие группы: фиксированные (многоразовые) пароли и одноразовые пароли.

Фиксированные пароли. Обычная парольная схема основывается на не зависящих от времени паролях и устроена следующим образом. Для каждого пользователя имеется пароль, который пользователь способен запомнить. Эта последовательность выступает в качестве общего секрета пользователя и системы. Для того чтобы получить доступ к системному ресурсу (базе данных, приложению и т. д.), пользователь предоставляет свой идентификатор и пароль и прямо или косвенно определяет необходимый ресурс. Для повышения надежности парольной защиты применяются различные защитные меры, тем не менее они лишь затрудняют или замедляют процесс доступа к паролю, его перебора или случайного угадывания, ни одна из них не решает проблемы защиты пароля радикально. В настоящее время методы аутентификации с фиксированными паролями используются, как правило, в не очень ответственных случаях или когда процесс доступа субъектов к системе необходимо максимально упростить. Парольные схемы различаются между собой по методам хранения парольной информации в системе и методам ее проверки.

Разновидностью фиксированных паролей являются PIN-коды. Это числовые пароли длиной от 4 до 8 десятичных цифр. Как правило, они используются совместно с микропроцессорными пластиковыми картами или картами с магнитной полосой. PIN-код обычно обеспечивает второй уровень защиты на случай, если карта потеряна или украдена. Для защиты от полного перебора такого маленького ключевого пространства необходимы дополнительные меры: организационная или физическая защита.

Одноразовые пароли. Один из вариантов защиты от различных атак на аутентификацию на основе пароля — переход на аутентификацию с помощью одноразовых паролей. Применение схем одноразовых паролей стало заметным шагом вперед по сравнению с использованием фиксированных паролей. Одноразовые пароли (OTP, One Time Passwords) — динамическая аутентификационная информация, генерируемая для единичного использования с помощью аутентификационных устройств (программных или аппаратных). Одноразовые пароли в основном нашли применение для удаленного доступа пользователей к защищенным информационным ресурсам. Суть концепции одноразовых паролей состоит в использовании различных паролей при каждом новом запросе на предоставление доступа. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от внешних угроз. В целом технология OTP основана на использовании двухфакторных схем аутентификации и может быть классифицирована как усиленная технология аутентификации. Методы аутентификации по одноразовому паролю также подвержены атакам, наиболее известными из которых являются «человек посередине», кража аутентификационного токена, подбор PIN-кода токена.

Таким образом, можно сделать вывод, что, каким бы надежным ни был механизм парольной аутентификации, он сам по себе, в отдельности, без применения иных механизмов защиты, не может обеспечить сколько-нибудь высокого уровня безопасности защищаемого объекта.

2. Аутентификация методом «запрос-ответ»

Вместо запроса пароля компьютерная система для аутентификации может использовать другой метод («на основе знания чего-либо») — метод секретных запросов и ответов. Такая аутентификация

является двусторонней (т. е. взаимной аутентификацией клиента и сервера) [2, 3]. Идея построения таких протоколов состоит в том, что доказывающий убеждает проверяющего в своей аутентичности путем демонстрации своего знания некоторого секрета. Знание секрета подтверждается выдачей ответов на меняющиеся с течением времени запросы проверяющего. Как правило, запрос — это число, выбираемое одной стороной в начале протокола. В таких протоколах обычно используются либо случайные числа, либо числа из неповторяющихся последовательностей, либо метки времени. Основным международным стандартом по криптографическим протоколам аутентификации является стандарт Международной организации по стандартизации и Международной электротехнической комиссии ISO/IEC 9798, описывающий механизмы аутентификации. Рекомендованными протоколами в этом стандарте являются «запрос-ответ» с использованием симметричных криптосистем и «запрос-ответ» с использованием асимметричных криптосистем.

3. Протоколы с нулевым разглашением знаний

Общая идея асимметричных протоколов аутентификации, основанных на доказательствах с нулевым разглашением знания, состоит в том, что законный пользователь, имеющий открытый и секретные ключи, и проверяющий выполняют совместный криптографический протокол интерактивного доказательства, в процессе которого пользователь должен доказать свою подлинность, продемонстрировав знание секретного ключа законного пользователя, но не разгласив его для проверяющего. В протоколах с нулевым разглашением доказательство имеет вероятностный характер. Это означает, что утверждение имеет место с некоторой вероятностью, которая может быть выбрана сколь угодно близкой к единице.

4. Биометрическая аутентификация

Биометрическая аутентификация — аутентификация на основе физиологических, химических или поведенческих характеристик [4]. К числу неоспоримых преимуществ биометрической аутентификации относится использование параметров, которые невозможно забыть, украсть и очень трудно подделать. Однако данная технология в большинстве случаев требует значительных вычислительных ресурсов, обладает рядом функциональных ограничений и предоставляет вероятностное решение. Поскольку биометрический параметр уникален, его можно использовать как для однофакторной аутентификации, так и для двухфакторной совместно с паролем или устройством аутентификации (например, со смарт-картой).

В биометрических системах может возникать 2 вида ошибок: ошибочное соответствие (FAR, False Accept Rate) и ошибочное несоответствие (FRR, False Reject Rate) полученных признаков эталону. Причинами возникновения этих ошибок может послужить то, что биометрические параметры изменяются с течением времени, в процессе аутентификации возможно некорректное взаимодействие пользователя со считывателем и т. д. Сортировать и сравнивать биометрические методы по показаниям ошибок первого и второго рода очень сложно, так как они сильно разнятся для одних и тех же методов из-за сильной зависимости от оборудования, на котором они реализуются. Каждый метод аутентификации имеет свои преимущества и ограничения, поэтому выбор метода определяется применением конкретной биометрической системы.

Использование биометрии для аутентификации личности является традиционным, имеет большую историю изучения и применения. В целом методы биометрической аутентификации хорошо отработаны и успешно применяются на практике, несмотря на существование до сих пор не решенных вопросов, связанных с качеством биометрических систем. Эти методы постоянно развиваются и совершенствуются, что делает их привлекательными для массового использования. Основными сферами применения биометрии являются контроль доступа к компьютеру, электронная коммерция, интернет-банкинг, смарт-карты, мобильные телефоны, банкоматы и кредитные карты, контроль доступа в помещения и учет рабочего времени. В последнее время выделилось новое направление

применения биометрии в системах защиты информации, а именно использование биометрии в системах криптографической защиты информации. Здесь биометрия стала применяться для защиты от несанкционированного доступа к криптографическому ключу и в качестве источника ключевого материала. Как и в случае аутентификации, в этом направлении тоже есть ряд сложностей. Но помимо тех, которые существуют для биометрической аутентификации, здесь появляются дополнительные, которые возникают при попытке применить биометрические данные в качестве криптографического ключа. Это обусловлено тем, что биометрические данные нечетко воспроизводимы и не имеют равномерного распределения, в то время как большинство криптографических преобразований биективны, а следовательно, требуют точного значения ключа.

5. Методы аутентификации в системах управления базами данных (СУБД)

Среди СУБД явным лидером является СУБД Oracle. В ней реализованы наиболее передовые технологии защиты данных непосредственно в базе данных. СУБД Oracle предоставляет множество способов аутентификации и позволяет использовать один или несколько методов одновременно. Аутентификация в СУБД Oracle означает проверку подлинности субъекта (пользователя, приложения, устройства), которому требуется доступ к данным, ресурсам или приложениям. В СУБД Oracle возможна аутентификация средствами операционной системы, с помощью сетевых сервисов, средствами базы данных (БД).

Аутентификация средствами операционной системы. Некоторые операционные системы позволяют СУБД Oracle использовать ту информацию о пользователях, которой они управляют. Это создает следующие преимущества: аутентификация может проходить без указания имени пользователя и пароля, при записи событий аудита средствами ОС и СУБД можно использовать одно и то же имя пользователя, сервер БД не должен хранить пароли и управлять ими. Однако при этом возникают проблемы в распределенных системах, использующих различные ОС.

Аутентификация с помощью сетевых сервисов. Среди встроенных в СУБД Oracle средств защиты можно выделить опцию Oracle Advanced Security (OAS) — комплекс средств защиты данных, аутентификации и обеспечения сетевой безопасности. В OAS предусмотрена аутентификация службами третьих сторон: Kerberos, Entrust/PKI, RADIUS, службой LDAP-каталога.

Аутентификация средствами базы данных. СУБД Oracle может аутентифицировать пользователя (приложение), используя информацию, хранимую в базе данных. Если субъектом аутентификации является пользователь, то для проверки его подлинности может запрашиваться некоторая дополнительная информация, например пароль. Информация о пользователе и пароле хранится в словаре базы данных, причем пароль криптографически защищен от несанкционированной модификации и передается по сети в шифрованном виде. Аутентификация средствами БД обеспечивает шифрование пароля во время соединения, блокирование учетной записи, управление жизненным циклом пароля, хранение истории паролей, управление качеством паролей.

6. Методы аутентификации в локальной сети

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. Наиболее распространенным и защищенным на сегодняшний день протоколом аутентификации в локальных сетях является протокол Kerberos, который поддерживается в ОС Microsoft, начиная с Windows 2000.

Протокол 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 могут быть перехвачены и модифицированы. Последняя версия протокола подробно описана в RFC 1510 и RFC 1964.

Одним из преимуществ протокола Kerberos, обеспечивающим очень высокий уровень сетевой безопасности, является то, что во всех сетевых взаимодействиях не передаются ни пароли, ни значения хеш-функций паролей в открытом виде. В качестве примера реализации протокола Kerberos следует отметить доменную аутентификацию пользователей в операционных системах компании Microsoft, начиная с Windows 2000.

7. Система одноразовых паролей S/Key

Система S/Key разработана в качестве метода регистрации для UNIX-систем. В качестве одноразового пароля пользователь должен предоставлять предпоследнее значение хеш-функции. Как правило, пользователи системы S/Key используют для генерации одноразовых паролей программно реализованные OTP-токены. Программные реализации устройства аутентификации существуют для операционных систем типа UNIX, Microsoft и Macintosh. Хотя аппаратная реализация устройства аутентификации для системы S/Key технически несложна, на данный момент промышленных моделей не существует.

8. Методы аутентификации для удаленного доступа

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. К важнейшим стандартным интерфейсам и протоколам для защиты доступа относятся RADIUS и TACACS+.

RADIUS. Протокол RADIUS был разработан в качестве протокола аутентификации серверного доступа и учета и основан на технологии «клиент—сервер». Протокол аутентификации RADIUS (Remote Authentication Dial-in User Service) 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 системе RADIUS функции аутентификации и авторизации совмещены. Если имя пользователя найдено в базе данных и пароль указан верно, сервер RADIUS выдает положительный ответ, в котором приводится список пар атрибутов для данной сессии. Транзакции между клиентом и сервером RADIUS аутентифицируются с помощью общего секрета, который никогда не передается по сетевым каналам. Кроме того, обмен любыми пользовательскими паролями между клиентом и сервером идет только в шифрованном виде. Поддержка протокола RADIUS реализована на многих современных платформах, что позволяет использовать его в межплатформенных решениях. Протокол RADIUS детально описан в открытых стандартах RFC 2138 и 2139.

TACACS+. Система контроля доступа с контроллером терминального доступа (Terminal Access Controller Access Control System, TACACS+) является протоколом последнего поколения из серии протоколов TACACS и представляет собой фактический стандарт, разработанный компанией Cisco Systems для централизованной аутентификации и авторизации пользователей по типу RADIUS. Протокол TACACS+ работает по технологии «клиент—сервер», где клиентом TACACS+ обычно является сервер сетевого доступа, а сервером TACACS+, как правило, считается «демон» (т. е. процесс, запускаемый на машине UNIX или NT). Фундаментальным структурным компонентом протокола TACACS+ является разделение аутентификации, авторизации и учета. Это позволяет обмениваться аутентификационными сообщениями любой длины и содержания и, следовательно,

использовать для клиентов TACACS+ любой аутентификационный механизм, в том числе PPP, PAP, CHAP, Kerberos. Описание протокола содержится в RFC 1492.

9. Аппаратные средства аутентификации

Для поддержки процедур аутентификации требуются технические средства. Они могут хранить и обрабатывать конфиденциальные и аутентификационные данные и выполнять операции для аутентификации пользователей. Большинство аппаратных средств реализуют двухфакторную аутентификацию на основе знания (PIN-код) и обладания (средство аутентификации). Наиболее распространенными устройствами данного класса являются следующие.

Электронные ключи. В качестве носителя информации могут использоваться специализированные устройства аутентификации Touch Memory (iButton) и Memory — карты с встроенной микросхемой. Оба устройства представляют собой сменный носитель информации с уникальным номером, прошиваемым при изготовлении, и памятью, в которой можно хранить данные пользователя. Некоторые типы таких устройств предусматривают возможность двухфакторной аутентификации, требуя ввода PIN-код для доступа к памяти, где хранится пользовательская информация.

Смарт-карты. Смарт-карты, или интеллектуальные карты, представляют собой пластиковые карты со встроенным программируемым микропроцессором. Главное отличие смарт-карт от других типов карт заключается в способности обрабатывать хранящуюся и поступающую информацию при помощи микропроцессора. На смарт-карте может храниться разнообразная информация, имеющая отношение к ее владельцу, в том числе криптографические ключи и персональные данные. Смарт-карты нашли применение в электронной коммерции, для выполнения криптографических преобразований информации, безопасного доступа в корпоративную сеть, к защищенным информационным ресурсам и др. Такие карты могут дополнительно снабжаться средствами логической и биометрической аутентификации владельца карты [2].

USB-ключи. Наиболее популярны аппаратные ключи, использующие порт USB. Такие устройства не требуют установки каких-либо считывателей. Каждый ключ имеет уникальный серийный номер, прошиваемый при изготовлении. USB-ключи являются преемниками смарт-карт и имеют с ними практически идентичные структуры.

Генераторы паролей. В качестве возможных устройств для генерации одноразовых паролей обычно используются OTP-токены. OTP-токен — мобильное персональное устройство, которое принадлежит определенному пользователю и генерирует одноразовые пароли. Многие из них требуют от пользователя введения PIN-кода для активации токена, в качестве дополнительной информации при генерации одноразового пароля, а также для предъявления серверу аутентификации вместе с одноразовым паролем. Для генерации одноразовых паролей OTP-токены используют хеш-функции или криптографические алгоритмы. Обычно в OTP-токенах применяется симметричная криптография. Такие токены могут работать в асинхронном и синхронном режимах.

Мобильные устройства. Мобильные телефоны, смартфоны, коммуникаторы, КПК могут использоваться для аутентификации пользователя в сети благодаря наличию у них SIM-карт, несущих в себе уникальные идентификационные данные пользователя. При этом аутентификация абонента в сети осуществляется по принципу «запрос-ответ». SIM-карта защищается PIN-кодом. Она представляет собой один из вариантов технологии смарт-карт и фактически является смарт-картой со встроенным программным обеспечением.

Существуют комбинированные средства аутентификации, использующие одновременно несколько аутентификационных признаков. Внедрение таких систем позволяет повысить защищенность компьютеров и корпоративных сетей от несанкционированного доступа. В последнее время прослеживаются тенденции интеграции логических средств аутентификации и средств

контроля и управления доступом. Смарт-карты, используемые для аутентификации пользователя при доступе к ресурсам компьютерной системы, интегрируются со средствами радиочастотной идентификации. В этом случае появляется возможность дополнительно использовать смарт-карты для аутентификации человека при его доступе в различные помещения. Такая интеграция расширяет возможности использования смарт-карты, дает дополнительные удобства для пользователя, но не повышает качество аутентификации.

Заключение

В работе проведен анализ наиболее часто используемых в корпоративных информационных системах методов аутентификации. Выявлены достоинства и недостатки, а также возможности и области применения различных методов аутентификации.

Изложенные результаты получены в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Афанасьев А. А., Веденьев Л. Т., Воронцов А. А. и др.* Аутентификация. Теория и практика безопасного доступа к информационным ресурсам. М.: Горячая линия — Телеком, 2009. — 552 с.
2. *Запечников С. В.* Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. М.: Горячая линия — Телеком, 2007. — 320 с.
3. *Menezes A. J., van Oorschot P. C, Vanstone S. A.* Handbook of Applied Cryptography. 5th ed. CRC Press, 2001.
4. *Jain A. K., Flynn P., Ross A. A.* Handbook of Biometrics. Springer Press, 2008.