В настоящее время информационные системы различного масштаба стали неотъемлемой частью базовой инфраструктуры государства, бизнеса, гражданского общества. Все больше защищаемой информации переносится в информационные системы. 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.

Известно, что более 25 % злоупотреблений информацией в информационной системе совершаются внутренними пользователями, партнерами и поставщиками услуг, имеющими прямой доступ к информационной системе. До 70 % из них - случаи несанкционированного получения прав и привилегий, кражи и передачи учетной информации пользователей, что становится возможным из-за несовершенства технологий разграничения доступа и аутентификации пользователей информационной системы. Именно поэтому тема эссе так актуальна сегодня, ведь совершенствование методов системы управления доступом и регистрации пользователей является одним из приоритетных направлений развития.

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

Исходя из вышесказанного, целью написания работы будет раскрытие понятия аутентификации как способа подтверждения личности человека. Для достижения цели эссе потребуется выполнить некоторые задачи, например, описать стандарты аутентификации, ее элементы, а также факторы, способы и протоколы.

ОСНОВНАЯ ЧАСТЬ

Аутентификацию можно отождествить с установлением подлинности. Под ней понимается проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами,

аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

С древних времён перед людьми стояла довольно сложная задача - убедиться в достоверности важных сообщений. Придумывались речевые пароли, сложные печати, моноалфавитные шифры. Появление методов аутентификации с применением механических устройств сильно упрощало задачу, например, обычный замок и ключ были придуманы очень давно. Пример системы аутентификации можно увидеть в старинной сказке "Приключения Али-Бабы и сорока разбойников". В этой сказке говорится о сокровищах, спрятанных в пещере. Пещера была загорожена камнем. Отодвинуть его можно было только с помощью уникального речевого пароля: "Сезам, откройся!".

В настоящее время в связи с обширным развитием сетевых технологий, автоматическая аутентификация используется повсеместно.

Для корректной аутентификации пользователя необходимо, чтобы пользователь предъявил аутентификационную информацию (информацию, которой обладает только сам пользователь и никто другой).

Аутентификация пользователя в интернете требуется при доступе к таким сервисам как электронная почта, веб-форум, социальные сети, интернет-банкинг, платежные системы, корпоративные системы, интернет-магазины.

Стандарты аутентификации.

В нашей стране наиболее распространены 2 документа, определяющие стандарты аутентификации: ГОСТ Р ИСО/МЭК 9594-8-98 и FIPS 113. Первый стандарт определяет формат информации аутентификации, описывает способ получения из справочника информации аутентификации, устанавливает предпосылки о способах формирования и размещения в справочнике информации аутентификации и определяет три способа, с помощью которых прикладные программы могут использовать такую информацию аутентификации для выполнения аутентификации. Второй стандарт устанавливает Data Authentication Algorithm (DAA), который может быть использован для обнаружения несанкционированных изменений данных, как преднамеренных, так и случайных.

Элементы системы аутентификации.

В любой системе аутентификации можно выделить несколько элементов: субъект (проходящий процедуру), характеристика субъекта (отличительная черта), хозяин системы аутентификации (контролирующий и несущий ответственность), механизм аутентификации (принцип работы системы), механизм управления доступом (предоставляющий определённые права доступа субъекту).

Разобрать элементы системы можно на простом примере со снятием наличных в банкомате. Субъектом в данной ситуации будет человек (держатель карты), его характеристикой будет персональный идентификатор, данные карты, хозяином системы является банк-эмитент карты, механизмом аутентификации будет программное обеспечение, а механизм управления доступом – разрешение на выполнение банковских действий.

Факторы аутентификации.

Ещё до появления компьютеров использовались различные отличительные черты субъекта, его характеристики. Сейчас использование той или иной характеристики в системе зависит от требуемой надёжности, защищённости и стоимости внедрения. Выделяют 3 фактора аутентификации:

- нечто, что нам известно, например, какая-либо секретная информация;
- нечто, чем мы обладаем, например, какой-либо уникальный физический объект;
- нечто, что является неотъемлемой частью нас самих — биометрика.

Способы аутентификации.

На сегодняшний день в мире существует множество способов аутентификации пользователя. Самые распространенные среди них: аутентификация при помощи электронной подписи, по паролям, с помощью SMS, биометрическая, через GPS, многофакторная. Разберем немного подробнее каждую из них.

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» (с изменениями) предусматривает следующие виды электронной подписи: простая (электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом), неквалифицированная (получена в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяет определить лицо, подписавшее электронный документ, обнаруживает факт внесения изменений в электронный документ после

момента его подписания, создается с использованием средств электронной подписи), квалифицированная (обладает всеми признаками электронной подписи, а также имеет ключ проверки электронной подписи, который указан в квалифицированном сертификате). Для создания квалифицированной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Аутентификация по паролям предусматривает одноразовые и многоразовые пароли. С точки зрения наилучшей защищённости при хранении и передаче паролей следует использовать однонаправленные функции. Обычно для этих целей используются криптографически стойкие хеш-функции. В этом случае на сервере хранится только образ пароля. Получив пароль и проделав его хеш-преобразование, система сравнивает полученный результат с эталонным образом, хранящимся в ней. При их идентичности пароли совпадают. Для злоумышленника, получившего доступ к образу, вычислить сам пароль практически невозможно. Использование многоразовых паролей имеет ряд существенных недостатков. Во-первых, сам эталонный пароль или его хешированный образ хранятся на сервере аутентификации. Зачастую хранение пароля производится без криптографических преобразований, в системных файлах. Получив доступ к ним, злоумышленник легко доберётся до конфиденциальных сведений. Во-вторых, субъект вынужден запоминать (или записывать) свой многоразовый пароль. Злоумышленник может заполучить его, просто применив навыки социальной инженерии, без всяких технических средств. Кроме того, сильно снижается защищенность системы в случае, когда субъект сам выбирает себе пароль. Зачастую им оказывается какое-то слово или сочетание слов, присутствующие в словаре.

Актуальность обеспечения безопасности мобильных средств коммуникации, например, ip-phone, стимулирует новые разработки в этой области. Среди них можно назвать аутентификацию с помощью SMS-сообщений. Привлекательность данного метода заключается в том, что ключ получается не по тому каналу, по которому производится аутентификация (out-of-band), что практически исключает атаку типа «человек посередине». Дополнительный уровень безопасности может дать требование ввода PIN-кода мобильного средства. Данный метод получил широкое распространение в банковских операциях через интернет.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100 % идентификацию, решая проблемы утраты паролей и личных идентификаторов. Примерами внедрения указанных методов

являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, формам ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и даже по ДНК. Новым направлением является использование биометрических характеристик в интеллектуальных расчетных карточках, жетонах-пропусках и элементах сотовой связи. Например, при расчете в магазине предъявитель карточки кладет палец на сканер в подтверждение, что карточка действительно его. Наиболее используемыми биометрическими атрибутами являются: отпечатки пальцев, биометрия руки, радужная оболочка глаза, термический образ лица, голос.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Сложность взлома системы состоит в том, что аппаратура передает оцифрованный сигнал спутника, не производя никаких вычислений. Все вычисления о местоположении производят на сервере аутентификации.

В последнее время всё чаще применяется так называемая расширенная, или многофакторная, аутентификация. Она построена на совместном использовании нескольких факторов аутентификации. Это значительно повышает защищённость системы.

Протоколы аутентификации.

Процедура аутентификации используется при обмене информацией между компьютерами, при этом используются весьма сложные криптографические протоколы, обеспечивающие защиту линии связи от прослушивания или подмены одного из участников взаимодействия. А поскольку, как правило, аутентификация необходима обоим объектам, устанавливающим сетевое взаимодействие, то аутентификация может быть и взаимной.

Самыми популярными семействами аутентификации являются аутентификация пользователя на PC (шифрованное имя, связка логин-пароль, карта доступа, биометрия) и аутентификация в сети (использование цифровой подписи, SAML, Cookie-сессии, Сертификаты X.509 и т. д.).

ЗАКЛЮЧЕНИЕ

Подводя итоги, можно сделать вывод, что аутентификация является обязательной процедурой проверки подлинности данных, без которой защищаемая информации может оказаться под угрозой.

Несмотря на новизну определения и отнесения его к англицизмам, аутентификация имеет богатую историю и весьма обширную историческую справку. На сегодняшний день процедура аутентификации плотно вошла в повседневную жизнь. На государственном и международном уровнях были разработаны специальные стандарты для аутентификации, а также выделены ее субъекты и факторы. Способов аутентификации существует не менее дюжины, но самым безопасным из них, безусловно, является аутентификация по биометрии.

Таким образом, цель написания эссе была достигнута, а также были решены поставленные задачи.

При этом хочется добавить, что изучение процедуры аутентификации не изжило себя, вопрос остается актуальным и по сей день. С каждым годом появляются все новые способы идентификации, данные субъекта приобретают большую безопасность, а процедура аутентификации становится быстрее и проще.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие. - СПб.: Изд-во СПбГУЭФ, 2010.- 267 с.
2. Галатенко В.А. Идентификация и аутентификация, управление доступом лекция из курса "Основы информационной безопасности". - Интернет Университет Информационных Технологий, 2018 г.
3. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей = Authentication: From Passwords to Public Keys First Edition. — М.: Вильямс, 2016 г. — С. 432.
4. [Интернет-ресурс] Аутентификация // Wikipedia URL: https://ru.wikipedia.org/wiki/Аутентификация (дата обращения: 10.09.2020).