УДК: 004.9

МЕТОДЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ИНТЕРНЕТЕ

Беляев А.Э., Негребецкая, В.И.

ФГБОУ ВО «Курский государственный университет», колледж коммерции, технологий и сервиса, Россия, Курск, e-mail: lisa.maverik@yandex.ru , violetta-negrebe1@mail.ru

Современные методы аутентификации позволяют осуществить подбор подходящей конфигурации с учетом различных требований, к примеру, интернет-банк использует двухфакторную аутентификацию, отдельные сервисы государственных услуг применяют помимо постоянного и временного пароля, еще и документ, подтвержденный электронной цифровой подписью. В представленной статье раскрыты основные методы аутентификации, применяемые в настоящее время планируемые для использования на ближайшую перспективу.

Ключевые слова: идентификация, аутентификация, авторизация, аутентификация на основе сессий, цифровой сертификат, аппаратный токен, Cookies, OAuth, OAuth2, биометрическая аутентификация, многофакторная аутентификация.

METHODS FOR AUTHENTICATING USERS ON THE INTERNET

Belyaev A. E., Negrebetskaya, V. I.

Kursk state University, College of Commerce, technology and service, Kursk, Russia, e-mail: lisa.maverik@yandex.ru , violetta-negrebe1@mail.ru

Modern authentication methods make it possible to select the appropriate configuration to meet various requirements, for example, the Internet Bank uses two-factor authentication, and certain public services services use a document confirmed by an electronic digital signature in addition to a permanent and temporary password. This article describes the main authentication methods that are currently being used and are planned for use in the near future.

Keywords: identification, authentication, authorization, session-based authentication, digital certificate, hardware token, Cookies, OAuth, OAuth2, biometrical authentication, multi-factor authentication.

Процесс регистрации пользователя в системе состоит из трех взаимосвязанных, выполняемых последовательно процедур: идентификации, аутентификации и авторизации.

Идентификация - это процедура распознавания субъекта по его идентификатору. В процессе регистрации субъект предъявляет системе свой идентификатор и она проверяет его

наличие в своей базе данных. Субъекты с известными системе идентификаторами считаются легальными (законными), остальные субъекты относятся к нелегальным [4].

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 [1]. Для этого он должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т.п.).

Авторизация — процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к ее ресурсам.

На данный момент лидером в удобстве и частоте использования является обычный пароль. Он используется при аутентификации на различных сайтах, сервисах, личных кабинетах. Но главные проблемы паролей – это фишинг, легкий подбор брутфорсом [2]. Чтобы войти в доступ в тот или иной сайт или сервис, нужно знать лишь тот набор символов, который вы и задавали. Короткий пароль с банальными годами рождения и кличками домашних животных – легко подобрать и без подручных программ, а длинные и сложные в написании и в запоминании – пишутся на бумаге и клеятся на мониторы. Так же существуют одноразовые пароли, которые обычно отправляются на номер телефона. Однако, например, передачу временного кода по SMS ,которую практикуют многие банки, относительно просто перехватить путем анализа радиосигнала или посредством обычного вируса. Потому, кстати, этот способ доставки одноразовых паролей обоснованно считается ненадежным, и финансовые организации переходят на альтернативные варианты вроде использования Push-уведомлений.

Самый распространённый и широко известный метод – это аутентификация на основе сессий. Аутентификационная запись или сессия храниться на сервере и на клиенте. Сервер должен отслеживать активные сессии в базе данных или памяти, а на фронтенде создаётся кука, в которой хранится идентификатор сессии.

Процедура аутентификации на основе сессий проходит так [2]:

1. Пользователь вводит в браузере своё имя и пароль, после чего клиентское приложение отправляет на сервер запрос.

2. Сервер проверяет пользователя, аутентифицирует его, шлёт приложению уникальный пользовательский токен (сохранив его в памяти или базе данных).

3. Клиентское приложение сохраняет токены в куках и отправляет их при каждом последующем запросе.

4. Сервер получает каждый запрос, требующий аутентификации, с помощью токена аутентифицирует пользователя и возвращает запрошенные данные клиентскому приложению.

5. Когда пользователь выходит, клиентское приложение удаляет его токен, поэтому все последующие запросы от этого клиента становятся неаутентифицированными.

Недостатками данного метода аутентификации следующие:

- при каждой аутентификации пользователя сервер должен создавать у себя запись. Обычно она хранится в памяти, и при большом количестве пользователей есть вероятность слишком высокой нагрузки на сервер;

- т.к. сессии хранятся в памяти, масштабировать не так просто. Если вы многократно реплицируете сервер, то на все новые серверы придётся реплицировать и все пользовательские сессии. Это усложняет масштабирование.

Цифровой сертификат – электронное удостоверение, что именно этот субъект (пользователь) имеет доступ к тому или иному объекту, или данным. Он является обязательной частью инфраструктуры открытых ключей (public key infrastructure, PKI), поскольку без подобной верификации открытый ключ уязвим для злонамеренных манипуляций.

Во время аутентификации сервер выполняет проверку сертификата на основании следующих правил [3]:

1.Сертификат должен быть подписан доверенным certification authority (проверка цепочки сертификатов).

2.Сертификат должен быть действительным на текущую дату (проверка срока действия).

3.Сертификат не должен быть отозван соответствующим CA (проверка списков исключения).

Вообще пользователи чаще всего соприкасаются с цифровыми сертификатами при зашифрованных соединениях с ресурсами Интернета по протоколу SSL. Здесь удостоверяется подлинность не пользователя, а сервера – т.е. посетитель имеет возможность убедиться, что подключается к настоящему сайту, а не фишинговой копии. Помимо прочего, цифровой сертификат является частью электронной цифровой подписи (ЭЦП), поскольку она является по сути результатом преобразования документа. В каком-то смысле, ЭЦП также является средством аутентификации, она имеет подтверждение авторства: говорит, что вход выполнен от определенного лица и может рассматриваться как официальное выражение его намерений. К сожалению, ответственность за защиту ЭЦП носит сам владетель, ведь он

принимает решения о защите данных. Злоумышленники могут украсть цифровой ключ, это и делает его слабее перед обычными паролями.

Аппаратный токен - это устройство, предназначенное для аутентификации. В простейшем случае - токен сам по себе является удостоверением, т.е. пользователь должен иметь его при себе и тем или иным образом предъявить системе – например, подключить к компьютеру или поднести к считывателю [4].

В этих же целях используются пластиковые банковские карты или телефоны с функцией NFC. Однако, даже в тех случаях, когда токен или смарт-карта играют роль обычного удостоверения, «изнутри» процедура аутентификации тоже может быть построена на сопоставлении временных паролей или на криптографических операциях. Например, устройство пользователя может получать от сервера случайную последовательность данных, шифровать ее и отправлять обратно, позволяя системе определить, чьим именно ключом было проведено преобразование. Каким бы именно образом ни работал аппаратный токен, для системы будет подлинным тот пользователь, который держит устройство в руках. Так же, как и в двух предыдущих случаях, наличие токена никоим образом не связано с конкретным человеком: устройство можно украсть и использовать злонамеренно.

Аутентификация с использованием Cookies. Куки — небольшой массив данных, который отправляется интернет-сервером и хранится на ПК пользователя. Браузер при каждой попытке подключения к данному ресурсу посылает Cookies как одну из составных частей HTTP-запроса. Данная технология, помимо аутентификации, используется для [1]:

- сохранения индивидуальных настроек и предпочтений;

- слежения за состоянием сеанса;

- сбора статистических данных о пользователях (частота посещений, уникальные посещения и т.д.).

Как средство аутентификации куки используются для систем безопасности чатов, форумов и различных интернет-игр. Cookies обладают низкой степенью защиты — если сессия плохо фильтруется, то похитить их не составляет труда. Поэтому применяется дополнительная привязка по IP-адресу, с которого пользователь вошел в систему.

Аутентификация и авторизация OAuth представляет собой разновидность единой точки входа с упрощением процесса регистрации/входа пользователя в приложение. Используется при регистрации/входе в приложение через социальные сети.

Преимущество: пользователи могут войти в приложение одним кликом, если у них есть аккаунт в одной из соцсетей. Им не нужно помнить логины и пароли. Это сильно улучшает опыт использования приложения. Разработчику не нужно волноваться о

безопасности пользовательских данных и думать о проверке адресов почты — они уже проверены соцсетями. Кроме того, в соцсетях уже есть механизмы восстановления пароля.

Большинство соцсетей в качестве механизма аутентификации используют авторизацию через OAuth2 [3].

Соцсеть — это сервер ресурсов, приложение — клиент, а пытающийся войти в это приложение пользователь — владелец ресурса. Ресурсом называется пользовательский профиль / информация для аутентификации. Когда пользователь хочет войти в приложение, оно перенаправляет пользователя в соцсеть для аутентификации (обычно это всплывающее окно с URL'ом соцсети). После успешной аутентификации пользователь должен дать приложению разрешение на доступ к своему профилю из соцсети. Затем соцсеть возвращает пользователя обратно в приложение, но уже с токеном доступа. В следующий раз приложение возьмёт этот токен и запросит у соцсети информацию из пользовательского профиля.

Для реализации такого механизма может понадобиться зарегистрировать приложение в разных соцсетях, где ему будут присвоены app_id и другие ключи для конфигурирования подключения к соцсетям.

Биометрическая аутентификация использует биометрические характеристики человека, такие как: отпечаток пальца, лицо, сетчатка глаз, голос. Все это обещает избавление от традиционных недочетов перечисленных выше методов: биометрические параметры не только уникальны, но и неотделимы от человека, что позволяет с гораздо большей уверенностью говорить о подлинности пользователя. Тем не менее, пока что технологии считывания этих показателей не вполне совершенны, и специалисты еще не могут рекомендовать полагаться всецело на биометрию. Известны случаи, когда при получении незначительной царапинки, грязи на пальцах, биометрические данные считались неверными. Однако это – проблема не самого метода аутентификации, а технических средств его реализации, которые имеют свойство совершенствоваться. Впрочем, те или иные риски характерны для любого механизма, и присутствие этих проблем кажется скорее естественным побочным эффектом, чем опасным изъяном метода в целом. В скором будущем, по моему мнению, биометрическая аутентификация обгонит всех лидеров в этой категории защиты данных. Впрочем, те или иные риски характерны для любого механизма, и присутствие этих проблем кажется скорее естественным побочным эффектом, чем опасным изъяном метода в целом [2].

Идеология многофакторной аутентификации (multi-factor authentication, MFA) заключается в том, чтобы взаимно компенсировать недостатки нескольких отдельных факторов, как минимум двух, у которых различаются ключевые риски. Чаще всего на

практике используется двухфакторная аутентификация. К примеру: вы вводите свой обычный пароль, и к нему еще тот одноразовый пароль, который приходит по SMS или Push-уведомлению. Казалость бы – вот она, лучшая система для защиты данных! Но нет. Надо иметь в виду, что двухфакторная аутентификация не решает проблем той же парольной защиты в корне – она лишь усложняет задачу злоумышленника за счет ввода еще одного пароля. Ключевой изъян – отсутствие прямой связи с личностью пользователя – остается на месте. Поскольку возможность выдать себя за другого человека сохраняется, взломщики ищут (и находят) обходные пути.

Следовательно, для защиты и аутентификации в сети нужно выбирать способы защиты, которые разрешены по закону и более удобны пользователю. Если нет возможности или надобности использовать тот либо другой способ защиты, то тогда и не стоит заморачиваться. Это создает очевидные риски, однако, поскольку этих мер оказывается достаточно и для них нет более выгодных альтернатив, эксплуатанты готовы мириться с их недостатками. В конце концов, идеальная защищенность в любом случае недостижима, а если система аутентификации справляется со своими задачами, то менять ее на нечто более совершенное ни к чему.

В завершении следует сказать, что аутентификация пользователей обычно выполняется неким программным модулем, находящимся непосредственно на компьютере, на который пользователь пытается получить прямой или удаленный доступ. Методы аутентификации разделяются в зависимости от типа ресурса, структуры и тонкостей организации сети, удаленности объекта и технологии, которая используется в процессе распознавания.

Список литературы:

1. Методы аутентификации [Электронный ресурс] / URL: https://tyapk.ru/blog/post/authentication-methods (дата обращения: 22.01.2020).

2. Методы аутентификации пользователей информационных систем [Электронный ресурс] / URL: https://studfile.net/preview/5795257/page:7/ (дата обращения: 22.01.2020).

3. Обзор способов и протоколов аутентификации в веб-приложениях [Электронный ресурс] / URL: https://habr.com/ru/company/dataart/blog/262817/ (дата обращения: 22.01.2020).

4. Системы и методы аутентификации пользователей [Электронный ресурс] / URL: https://www.anti-malware.ru/analytics/Technology_Analysis/overview-of-user-authentication-systems-and-methods (дата обращения: 22.01.2020).