Многофакторная аутентификация

W
ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B3%D0%BE%D1%84%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D0%B0%D1%8F_%D0%B0%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F

Многофакторная аутентификация (МФА, англ. *Multi-factor authentication*, *MFA*) — расширенная аутентификация, метод контроля доступа к компьютеру, в котором пользователю для получения доступа к информации необходимо предъявить более одного «доказательства механизма аутентификации». К категориям таких доказательств относят:

- Знание — информация, которую знает субъект. Например, пароль, пин-код.
- Владение — вещь, которой обладает субъект. Например, электронная или магнитная карта, токен, флеш-память.
- Свойство, которым обладает субъект. Например, биометрия, природные уникальные отличия: лицо, отпечатки пальцев, радужная оболочка глаз, капиллярные узоры, последовательность ДНК.

Факторы аутентификации

Основная статья: ***Аутентификация***

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:

- **Фактор знания, что-то, что мы знаем — пароль**. Это тайные сведения, которыми должен обладать только авторизованный субъект. Паролем может быть речевое слово, текстовое слово, комбинация для замка или личный идентификационный номер (PIN). Парольный механизм может быть довольно легко воплощён и имеет низкую стоимость. Но имеет существенные недостатки: сохранить пароль в тайне зачастую бывает сложно, злоумышленники постоянно придумывают новые способы кражи, взлома и подбора пароля (см. бандитский криптоанализ, метод грубой силы). Это делает парольный механизм слабозащищённым. Многие секретные вопросы, такие как «Где вы родились?», элементарные примеры фактора знаний, потому что они могут быть известны широкой группой людей, или быть исследованы .
- **Фактор владения, что-то, что мы имеем — устройство аутентификации**. Здесь важно обстоятельство обладания субъектом каким-то неповторимым предметом. Это может быть личная печать, ключ от замка, для компьютера это файл данных, содержащих характеристику. Характеристика часто встраивается в особое устройство аутентификации, например, пластиковая карта, смарт-карта. Для злоумышленника заполучить такое устройство становится более сложно, чем взломать пароль, а субъект может сразу же сообщить в случае кражи устройства. Это делает данный метод более защищённым, чем парольный механизм, однако стоимость такой системы более высокая.
- **Фактор свойства, что-то, что является частью нас — биометрика**. Характеристикой является физическая особенность субъекта. Это может быть портрет, отпечаток пальца или ладони, голос или особенность глаза. С точки зрения субъекта, данный способ является наиболее простым: не надо ни запоминать пароль, ни переносить с собой устройство аутентификации. Однако биометрическая система должна обладать высокой чувствительностью, чтобы подтверждать авторизованного пользователя, но отвергать злоумышленника со схожими биометрическими параметрами. Также стоимость такой системы довольно велика. Но, несмотря на свои недостатки, биометрика остается довольно перспективным фактором.

Безопасность

Согласно мнению экспертов, многофакторная аутентификация резко снижает возможность кражи личных данных онлайн, так как знание пароля жертвы недостаточно для совершения мошенничества. Тем не менее, многие многофакторные подходы аутентификации остаются уязвимыми для «фишинга», «человек-в-браузере», «человек по середине».

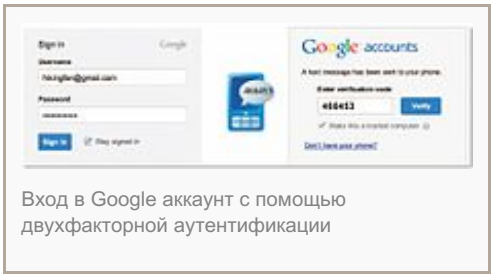
Основная статья: ***Аутентификация***

Выбирая для системы тот или иной фактор или способ аутентификации, необходимо, прежде всего, отталкиваться от требуемой степени защищенности, стоимости построения системы, обеспечения мобильности субъекта.

Можно привести сравнительную таблицу:

Уровень риска	Требования к системе	Технология аутентификации	Примеры применения
Низкий	Требуется осуществить аутентификацию для доступа к системе, причём кража, взлом, разглашение конфиденциальных сведений **не будут иметь значительных последствий**	Рекомендуется минимальное требование - использование многоразовых паролей	Регистрация на портале в сети Интернет
Средний	Требуется осуществить аутентификацию для доступа к системе, причём кража, взлом, разглашение конфиденциальных сведений причинят **небольшой ущерб**	Рекомендуется минимальное требование - использование одноразовых паролей	Произведение субъектом банковских операций
Высокий	Требуется осуществить аутентификацию для доступа к системе, причём кража, взлом, разглашение конфиденциальных сведений причинят **значительный ущерб**	Рекомендуется минимальное требование - использование многофакторной аутентификации	Проведение крупных межбанковских операций руководящим аппаратом

Двухфакторная аутентификация



Вход в Google аккаунт с помощью двухфакторной аутентификации

Двухфакторная аутентификация (ДФА, англ. *Two-factor authentication*, также известна как двухэтапная верификация), является типом многофакторной аутентификации. ДФА — представляет собой технологию, обеспечивающую идентификацию пользователей с помощью комбинации двух различных компонентов.

Хорошим примером двухфакторной аутентификации является авторизация Google. Когда пользователь заходит с нового устройства, помимо аутентификации по имени-паролю, его просят ввести шестизначный код-подтверждения. Вы можете получить его по SMS, с помощью голосового звонка на ваш телефон, он может быть взят из заранее составленного реестра разовых кодов или вы можете использовать приложение-аутентификатор, генерирующее новый одноразовый пароль за короткие промежутки времени. Выбрать один из методов можно в настройках вашего Google-аккаунта.

Преимущество двухфакторной аутентификации через мобильный телефон:

- Не нужны дополнительные токены, потому что мобильник всегда под рукой.
- Код-подтверждения постоянно меняется, а это безопаснее, чем фиксированный логин-пароль

Недостатки двухфакторной аутентификации через мобильный телефон:

- Мобильный телефон должен ловить сеть, когда происходит аутентификация, иначе сообщение с паролем просто не дойдет.
- Вы делитесь с кем-то вашим мобильным телефоном, что влияет на вашу личную жизнь и быть может в будущем на него будет приходить спам.
- Текстовые сообщения (SMS), которые поступают на ваш мобильный телефон могут быть перехвачены[1].
- Текстовые сообщения приходят с некоторой задержкой, так как некоторое время уходит на проверку подлинности.
- Современные смартфоны используются, как для получения почты, так и для получения SMS. Как правило электронная почта на мобильном телефоне всегда включена. Таким образом, все аккаунты для которых почта является ключом могут быть взломаны(первый фактор). Мобильный телефон(второй фактор). Выходит смартфон смешивает два фактора в один.

Сейчас многие крупные сервисы, такие как Microsoft Outlook, Yandex, Dropbox, Facebook, уже предоставляют возможность использовать двухфакторную аутентификацию. Причём для всех из них можно использовать единое приложение аутентификатор, соответствующее определённым стандартам, такие как Google Authenticator, Authy или FreeOTP.

Практическая реализация

Многие продукты с функцией многофакторной аутентификации требуют от пользователя клиентское программное обеспечение, для того, чтобы система многофакторной аутентификации заработала. Некоторые разработчики создали отдельные установочные пакеты для входа в сеть, идентификационных данных веб-доступа и VPN-подключения. Чтобы использовать с этими продуктами токен или смарт-карту, потребуется установить на PC четыре или пять пакетов специального программного обеспечения. Это могут быть пакеты, которые используются для осуществления контроля версии или это могут быть пакеты для проверки конфликтов с безнес-приложениями. Если доступ может быть произведён с использованием веб-страниц, то тогда можно обойтись без непредвиденных расходов. С другими программными решениями многофакторной аутентификации, такими как «виртуальные» токены или некоторые аппаратные токены, ни одно ПО не может быть установлено непосредственными пользователями.

Многофакторная аутентификация не стандартизирована. Существуют различные формы её реализации. Следовательно, проблема состоит в её способности к взаимодействию. Существует много процессов и аспектов, которые необходимо учитывать при выборе, разработке, тестировании, внедрении и поддержке целостной системы управления идентификацией безопасности, включая все релевантные механизмы аутентификации и сопутствующих технологий: это всё описал Brent Williams, в контексте «Identity Lifecycle»[1]

Многофакторная аутентификация имеет ряд недостатков, которые препятствуют её распространению. В частности человеку, который не разбирается в этой области, сложно следить за развитием аппаратных токенов или USB-штекеров. Многие пользователи не могут самостоятельно установить сертифицированное клиентское программное обеспечение, так как не обладают соответствующими техническими навыками. В общем, многофакторные решения требуют дополнительных затрат на установку и оплату эксплуатационных расходов. Многие аппаратные комплексы, основанные на токенах, запатентованы, и некоторые разработчики взимают с пользователей ежегодную плату. С точки зрения логистики, разместить аппаратные токены трудно, так как они могут быть повреждены или потеряны. Выпуск токенов в таких крупных областях, как банки, или других крупных предприятиях должен быть отрегулирован. Помимо затрат на установку многофакторной аутентификации значительную сумму также составляет оплата технического обслуживания. В 2008 году крупный медиа-ресурс *Credit Union Journal* провел опрос среди более 120 кредитных союзов США. Цель опроса — показать стоимость технического

обслуживания связанную с двухфакторной аутентификацией. В итоге вышло, что сертификация программного обеспечения и доступ к панели инструментов имеют самую высокую стоимость.

Примечания

1. ↑ NIST Prepares to Phase Out SMS-Based Login Security Codes. Time Is Running Out For This Popular Online Security Technique (англ.), Fortune (July 26, 2016). Проверено 13 августа 2016. «“Due to the risk that SMS messages may be intercepted or redirected, implementers of new systems should carefully consider alternative authenticators,” NIST».

Ссылки

- Eric Grosse, Mayank Upadhyay, Authentication at Scale. IEEE Security and Privacy, January/February 2013, IEEE Computer and Reliability Societies. (англ.)
- DRAFT NIST Special Publication 800-63B. Digital Authentication Guideline. Authentication and Lifecycle Management // NIST, 2016 (англ.)