Наступление карантина во всём мире привело к необходимости пересмотра привычных подходов к аутентификации. Увы, но стоит признать, что аутентификация с помощью привычных нам паролей не оправдала себя. А если добавить к этому то, что большинство пользователей и ранее использовали не стойкие, а главное, не уникальные пароли, то это привело к тому, что такая защита на сегодня обеспечивает крайне низкий уровень стойкости.

Владимир Безмалый
Microsoft Security Trusted Advisor
Microsoft MVP
Kaspersky Certified Trainer
Консультант ООН по информационной безопасности

Биометрическая аутентификация, на которую возлагались такие огромные надежды, также не получила широкое распространение. Причина вполне понятна. Увы, но хорошие биометрические датчики стоят дорого, вернее, очень дорого. Большинство существующих таких датчиков не могут отличить живое от неживого. Как быть?

Пожалуй, вполне достойным выходом может быть применение аппаратных токенов. Но здесь тоже есть своя цена. Ведь при оставлении компьютера без присмотра, токен чаще всего остаётся подключённым в USB-порт. Это огромная проблема. И если на работе это ещё как-то отслеживается, то дома следить некому и некогда. Как быть?

Одним из выходов из сложившейся ситуации будет использование технологии, получившей название One Time Password (OTP) или применение одноразовых паролей. Наверное, кто-то из читателей, как и я, применяет подобный подход при использовании сервисов Microsoft (например, Outlook, Skype и т.д.) или сервисов Google. В обоих случаях необходимо заранее установить на свой смартфон соответствующие приложения Microsoft Authenticator и Google Authenticator. Это необходимо, чтобы не использовать для получения одноразового пароля SMS: использование SMS признано небезопасным.

Какие виды OTP существуют в этом случае, рассмотрим на примере OTP-аутентификаторов и продуктов OTP-аутентификации семейства SafeNet компании Thales.

SafeNet OTP 110 токен

SafeNet OTP 110 (ранее IDProve) – это аппаратный токен OTP, обеспечивающий двухфакторную аутентификацию для широкого спектра ресурсов и поддерживает функции протоколов OATH TOTP и HOTP.

SafeNet Trusted Access поддерживает токены аутентификации OATH и позволяет организациям сохранить свои текущие инвестиции для эффективной и действенной защиты от несанкционированного входа в систему из-за скомпрометированных статических паролей.

Что такое OATH-аутентификация?

OATH – это открытая эталонная архитектура для реализации строгой аутентификации, созданная отраслевым сообществом поставщиков безопасности для универсального применения строгой аутентификации.

Стандарт OATH может использоваться ИТ-специалистами и специалистами по безопасности в качестве шаблона для интеграции строгой аутентификации в существующую инфраструктуру их организации.

Для получения дополнительной информации посетите openauthentication.org.

Описание токена

SafeNet OTP 110 представляет собой аппаратный токен OTP, сертифицированный OATH, который обеспечивает многофакторную аутентификацию для широкого спектра ресурсов. Работа SafeNet OTP 110 основана на смене одноразового пароля через определённый промежуток времени и может применяться везде, где используется обычный статистический пароль, что существенно повышает безопасность.

При этом OTP-аутентификация помогает организациям устранить риски, связанные с фиксированными паролями, и повысить безопасность контроля доступа пользователей, реализованного для защиты доступа к локальной сети, доступа к удалённой сети (VPN), облачных приложений, VDI, веб-порталов и пользовательских приложений.

Проблемы, которые могут возникнуть при использовании аппаратных токенов OTP

Прежде всего это несовпадение временных интервалов между токеном и вашим сервером. Как это решается? Можно увеличить (уменьшить) интервал действия пароля. Могу сказать одно: данная проблема вполне решаема.

Удобство:

- Пожизненная гарантия на SafeNet OTP 110 предоставляется на весь срок действия подписки SafeNet Trusted Access, включая бесплатную замену
- Безопасный удалённый доступ к сетям (Vpns), приложениям SaaS, VDI, веб-порталам и пользовательским приложениям
- Пользователи могут легко носить устройство с собой, куда бы ни отправились
- Простое управление благодаря лёгкой внутренней конфигурации, низкому техническому обслуживанию и длительному сроку службы аккумулятора
- Обеспечивает соответствие отраслевым нормам

Особенности:

- Устройство аутентификации OTP с ЖК-дисплеем, батареей и кнопкой генерации OTP
- Поддержка протоколов OATH TOTP и HOTP

SafeNet OTP Display Card

В данном случае мы имеем OTP-карту SafeNet. При нажатии кнопки карта сгенерирует одноразовый пароль, привязанный к данной карте.

При этом одноразовый пароль, сгенерированный картой, может объединяться с другими факторами аутентификации, например PIN-кодом или паролем. Ведь необходимо убедиться, что карта находится в руках подлинного владельца.

OTP-карта SafeNet взаимодействует с SafeNet Trusted Access, сервисом управления облачным доступом, который предлагает единый вход, защищённый детальными политиками доступа.

Удобства

- Легко переносить: помещается в ваш кошелёк
- Простота в использовании: нажмите кнопку и получите свой OTP
- Пожизненная гарантия. Гарантийный талон на SafeNet OTP Display Card предоставляется на весь срок действия подписки Gemalto, включая бесплатную замену. Как и все аутентификаторы Gemalto, токен никогда не истекает
- Безопасный доступ к удалённым сетям (VPN), облачным (SaaS) приложениям, VDI, веб-порталам и пользовательским приложениям
- Простое управление с лёгкой внутренней конфигурацией и автоматизированными рабочими процессами администрирования
- Обеспечивает соответствие отраслевым нормам, требующим многофакторной аутентификации

Особенности:

- OTP-токен в форм-факторе кредитной карты
- Высокая читаемость экрана ePaper
- Синхронизация времени – OATH TOTP

eToken PASS OTP Аутентификатор

eToken PASS — это компактное и портативное устройство строгой аутентификации с использованием одноразовых паролей (OTP), которое позволяет организациям удобно и эффективно устанавливать контроль доступа на основе OTP. Он поддерживает протоколы OATH TOTP и HOTP, а также стандартную поддержку RADIUS OTP и многое другое.

Thales SafeNet GOLD

Разработан для защиты идентификационных данных и безопасного доступа, представляет собой высокоэффективное двухфакторное OTP-устройство, обеспечивающее дополнительную защиту с помощью **PIN-кода и ответа на вызов**.

GOLD активируется с помощью персонального идентификационного номера (ПИН), который запрашивает у аутентификатора одноразовый динамический пароль. Затем пользователь вводит этот пароль в веб или сетевое приложение для аутентификации своей личности.

Как работает GOLD

GOLD предоставляет провайдерам онлайн-услуг, таким как банки, платёжные порталы, очень надёжное средство предложить своим клиентам защищённую онлайн-среду для проведения финансовых транзакций и доступа к конфиденциальной информации.

В дополнение к защите ПИН-кодами расширенные возможности OTP и ответа на вызовы GOLD предназначены для борьбы с мошенничеством в Интернете, таким как фишинг, и помогают поставщикам онлайн-услуг и банкам поддерживать целостность пароля, усложняя для клиентов потерю или обмен паролями.

Доступен на корпоративной платформе SafeNet Trusted Access. Эта уникальная платформа управления доступом обеспечивает гибкость и масштабируемость, позволяя организациям централизованно управлять GOLD с помощью других аутентификаторов Thales SafeNet или добавлять их в будущем по мере роста потребностей бизнеса. STA позволяет организациям защищать доступ ко всем ресурсам и переходить в облако.

Преимущества

- Безопасный удалённый доступ
- Аппаратная защита PIN-кода и ответ на вызов
- Портативность
- Большой удобный дисплей

Но стоит помнить, что кроме аппаратных токенов, можно использовать и программный токен SafeNet MobilePASS+ — программный токен следующего поколения, который обеспечивает безопасную одноразовую генерацию пароля на мобильных устройствах, а также аутентификацию одним нажатием для повышения удобства пользователя.

SafeNet MobilePASS+ интегрируется с ведущими облачными приложениями, шлюзами безопасности и виртуальными частными сетями и обеспечивает администрирование жизненного цикла без каких-либо ограничений, что делает его идеальным для обеспечения безопасного доступа к консультантам, партнёрам и разрозненной рабочей силе.

Для пользователей SafeNet MobilePASS+ предлагает удобный доступ благодаря простой активации QR-кода, дополнительному биометрическому PIN-коду и выбору стандартных режимов OTP и push-аутентификации. В режиме push при каждом обращении к защищённому ресурсу на устройство пользователя автоматически отправляется push-уведомление. Пользователь нажимает на уведомление MobilePASS+, затем, чтобы подтвердить запрос на вход в систему, а после входит в систему на ресурсе. Если политика ПИН была определена, пользователь вводит свой буквенно-цифровой ПИН или использует TouchID/FaceID для ввода своего биометрического ПИН (необязательно).

Можно также утверждать запросы входа в систему прямо с экрана блокировки — просто откройте push-уведомление, нажмите «Утвердить», а затем авторизуйтесь на своём устройстве, чтобы получить доступ к онлайн-ресурсу.

Начиная с MobilePASS+ v1.6, теперь можно проходить сквозной процесс аутентификации для доступа к личным токенам и паролям с полностью обновлённым пользовательским интерфейсом.

По аналогии с MobilePASS+ v1.6 работают существующие средства аутентификации сервисов Google и Microsoft, в частности push-аутентификация Microsoft и Google на iPhone.

Достоинство мобильной аутентификации состоит прежде всего в том, что это удобно и дёшево. Сегодня у большинства пользователей есть смартфоны. Вместе с тем это и недостаток данного способа аутентификации, ведь в таком случае необходимо контролировать смартфоны пользователей. А позволят ли это пользователи?

Необходимо убедиться в том, что смартфоны пользователей не взломаны, не заражены, на них не проведён rooting или jailbreak и для их блокирования используется устойчивый PIN-код.

Вы можете это гарантировать? Я — нет!

Вывод

На мой взгляд, с точки зрения безопасности, альтернативы использованию аппаратных токенов OTP сегодня просто не существует. Заставить пользователей использовать свои смартфоны для OTP и тем более заставить их безопасно использовать, увы, невозможно!