Российские системы двухфакторной аутентификации: просто, удобно, без проблем

En

The Russian Two-Factor Authentication Systems: Simple, Convenient and Flawless

G. A. Namestnikov,
Lead Specialist of Network Security Department
german.namestnikov@rcntec.com

M. I. Krylova,
PR-manager
marina.krylova@rcntec.com

RCNTEC

Some russian industrial sectors have long been exclusively using only domestic products in their activities. First and foremost, this relates to national security issues. If security equipment or tools are not produced and controlled domestically within a country, the use of imported products could become a potential means of aggression or interference in such country's internal affairs. One of the most obvious threats to IT security is an unauthorized access to confidential information.

Keywords: information security, import substitution, unauthorized access, two-factor authentication, data protection, software tokens and hardware tokens

В некоторых отраслях российской промышленности уже давно используются исключительно отечественные продукты. Прежде всего, это касается вопросов национальной безопасности. Если средства безопасности не производятся и не контролируются внутри страны, они могут стать потенциальным средством агрессии или вмешательства во внутренние дела. Одна из наиболее явных угроз ИТ-безопасности – несанкционированный доступ к конфиденциальной информации.

Ключевые слова: информационная безопасность, импортозамещение, несанкционированный доступ, двухфакторная аутентификация, защита данных, программные токены, аппаратные токены

Герман Александрович Наместников,
ведущий специалист отдела сетевой безопасности
german.namestnikov@rcntec.com

Марина Игоревна Крылова,
PR-менеджер
marina.krylova@rcntec.com

RCNTEC

Вместо предисловия

Можно долго спорить по поводу того, есть ли реальные перспективы у российской программы импортозамещения, однако нельзя не признавать тот факт, что некоторые сферы деятельности уже достаточно давно ориентированы на использование отечественных продуктов. В первую очередь это касается вопросов национальной безопасности, в том числе и в ИТ-отрасли.

«В России не вы занимаетесь импортозамещением, а импортозамещение занимается вами», – подметил в своем докладе на московском ИТ-фестивале «Импортозамещение-2017» руководитель направления по внедрению ИТ-сервисов концерна «Швабе» Владислав Баренбойм. С ним сложно не согласиться.

Одним из мощных толчков, изменивших вектор предпочтений в сторону российских программных средств, главным образом в плане обеспечения ИТ-безопасности, явился Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [1]. Следует также сказать, что с 1 июля 2017 года ужесточена ответственность за его нарушение. Решающую роль при выполнении требований данного закона играет использование соответствующих аппаратных и программных средств, имеющих

сертификаты ФСТЭК России, ФСБ России.

Напомним также, что с 1 января 2016 года вступило в силу Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» [2], которое исключает возможность госзакупок иностранного программного обеспечения при наличии аналогов отечественного производства. Тогда же Минкомсвязи РФ создало «Единый реестр российских программ для электронных вычислительных машин и баз данных» [3], в который уже вошли лучшие отечественные разработки.

Основные причины перехода на отечественные продукты в сфере ИТ

В первую очередь отметим стремление обезопасить себя и свою ИТ-инфраструктуру от потенциальных уязвимостей, вызванных наличием скрытых недокументированных функций, проще говоря – закладок (backdoors). Использование отечественных продуктов уменьшает подобную опасность. Российские компании работают в другой плоскости политической мотивации, что значительно минимизирует риски, прежде всего для государственных структур, где применяются данные продукты. Программы отечественного производства проще проверить, и руководство ИТ-компаний гораздо охотнее предоставляет свои разработки (главным образом, программный код) для контроля со стороны сертифицирующих организаций: ФСТЭК России, ФСБ России, Министерства обороны.

Следует также отметить наличие рисков отказа в предоставлении сервиса или снятия с поддержки в рамках экономических санкций против России. Снятие с технической поддержки может означать отклонение запроса необходимой помощи при внедрении, отказ в продаже технических средств (например, токенов) и другие неприятности, которые в итоге сведут на нет все усилия по обеспечению нужного уровня безопасности.

Еще один немаловажный фактор – цена вопроса. В ситуации, когда рубль дешевеет относительно доллара и евро, приобретать решения, полностью привязанные к иностранной валюте, – невыгодно и недальновидно. Даже при отсутствии других угроз этот нюанс сам по себе является серьезной помехой на пути внедрения решений в рамках ИТ-безопасности.

Ряд «историй успеха» отечественных компаний связан с процессом импортозамещения в организациях, попавших либо под западные санкции, либо под ответ России на эти санкции.

Двухфакторная аутентификация для защиты информации

Одна из наиболее явных угроз ИТ-безопасности – несанкционированный доступ к конфиденциальной информации. Компания Trustwave еще в 2011 году проводила масштабное исследование в этой области и пришла к выводу, что подавляющее большинство (80 %) инцидентов в сфере информационной безопасности происходит из-за использования слабых паролей [5].

Более того, в отчете Trustwave Global Security Report за 2017 год отмечается, что почти треть инцидентов ИБ в 2016 году была вызвана некорректной организацией удаленного доступа. В качестве меры противодействия таким угрозам компания Trustwave предлагает, в том числе, использование двухфакторной аутентификации [6].

Слабый пароль никуда не годится с точки зрения информационной безопасности, сложный – плох с точки зрения удобства пользователя. Один и тот же пароль на отдел, пара «логин – пароль» в рабочем ежедневнике, приклеенная к монитору записка – ситуации, знакомые многим. Очень часто злоумышленникам не составляет большого труда получить доступ к информации, а несанкционированное проникновение к важным данным для многих компаний может обернуться финансовыми потерями или даже разорением.

Информация к размышлению

Утечки информации порой достигают огромных масштабов и способны нанести серьезный урон экономической и политической стабильности государств.

Пример 1. В начале сентября текущего года в североамериканском подразделении бюро кредитных историй Equifax произошла утечка данных 143 млн граждан США. На сегодняшний день бюро кредитных историй собирает и хранит информацию более чем 800 млн потребителей и более 88 млн компаний по всему миру [7].

Пример 2. Утечка персональных данных 49 611 709 турецких граждан произошла в апреле 2016 года. Данный инцидент считается политической акцией, однако ответственность за проведение атаки пока никто не взял на себя [8].

В 2013 году ФСТЭК России утвердила «Методический документ. Меры защиты информации в государственных информационных системах» [9]. И надо сказать, что использование второго фактора аутентификации в последнее время стало де-факто стандартом при обеспечении безопасного доступа к данным и в крупных, и в небольших компаниях.

С каждым годом стремительно растут вычислительные мощности, которые можно применить для вскрытия паролей, в том числе простым перебором, а также с использованием различных словарей и других методов взлома. Приходится идти в ногу со временем, создавая препятствия злоумышленникам. При защите только посредством традиционной пары «логин – пароль» придется идти путем постоянного усложнения пароля. Секретные сочетания становятся все длиннее, запутаннее и труднее для запоминания. Сокращается и стандартный период автоматической смены пароля. В итоге пользователи оказываются не в состоянии держать эти наборы случайных символов в голове. Дело при-

нимает особенно опасный оборот, когда пользователь в целях экономии умственных ресурсов использует один и тот же пароль на все случаи жизни.

В результате, усложнение паролей, с одной стороны, вроде бы повышает уровень защищенности ИТ-системы, с другой – облегчает правонарушителям получение доступа к ней с использованием социальной инженерии и других средств обхода защиты.

Однако даже простой взлом аккаунта электронной почты, например, с использованием процедуры восстановления пароля через «секретный вопрос», позволяет злоумышленникам добраться до многих других данных. После этого можно восстанавливать пароль к публичным и приватным ресурсам, но уже через взломанную электронную почту. Таким образом, становится легко зайти в чужой аккаунт социальной сети, скачать файлы из облачного хранилища, перехватить управление мессенджером коротких сообщений, блогом, интернет-сайтом и другими ресурсами.

Двухфакторная аутентификация призвана решить эти проблемы. При наличии второго фактора похищение пароля уже не дает ожидаемого результата. Например, если в мобильном устройстве пользователя работает приложение с постоянно обновляемыми ключами, взломщику нужно заполучить еще и мобильный телефон (или планшет) своей жертвы.

Кроме того, в случае программных решений на мобильном устройстве можно настроить генерацию ключей для доступа на каждый отдельный ресурс. Таким образом, даже если пользователь не изобретает в каждом случае новый пароль, – это не очень хорошо, но, по большому счету, уже не столь ритично.

Разнообразие рынка

На мировом рынке токенов двухфакторной аутентификации присутствует множество игроков. Среди заграничных компаний основными вендорами являются VASCO, RSA, Protectimus и Gemalto.

На российском рынке двухфакторной аутентификации в первую очередь стоит отметить компании «Аладдин Р. Д.» [11] и RCNTEC [12]. Ряд продуктов этих отечественных разработчиков входит в ранее упомянутый «Единый реестр российских программ для электронных вычислительных машин и баз данных», в том числе предлагаемый RCNTEC сервис двухфакторной аутентификации AUTH.AS (см. рисунок).

Рисунок

Практически все компании, производящие средства двухфакторной аутентификации, предоставляют свои услуги в виде готовой платформы, устанавливаемой в защищаемом периметре заказчика, а также в виде онлайн-сервиса – в соответствии с подходом Software as a Service.

Несмотря на то что развертывание платформы двухфакторной аутентификации внутри собственного сетевого периметра может быть правильным решением с точки зрения безопасности, это далеко не во всех случаях удобно, особенно в современных ИТ-инфраструктурах, все больше стремящихся к распределенным системам и облачным решениям. И хотя использование «классических» токенов типа U2F имеет некоторые плюсы, популярность программных токенов постоянно повышается.

Эта тенденция связана, в первую очередь, с удобством их использования: с распространением смартфонов и развитием дешевого мобильного Интернета все больше людей регулярно работают с информацией удаленно.

В тот момент, когда в 2014 году специалисты RCNTEC приступили к разработке собственного сервиса, у большинства заказчиков выросла потребность использовать вместо классических аппаратных токенов мобильные телефоны. Технология создания одноразовых паролей появилась до эпохи массового распространения смартфонов, поэтому большинство вендоров еще не задумывалось над созданием мобильных клиентов.

Для ответа на запросы рынка, параллельно с backend'ом в RCNTEC было создано user-friendly мобильное приложение для генерации одноразовых паролей на платформах iOS и Android.

Помимо удобства для пользователей использование аппаратных токенов менее предпочтительно, когда для клиента важна конечная стоимость решения. В случае с аппаратными ключами заказчик вынужден не только покупать лицензию на право использования сервиса двухфакторной аутентификации, но и сами аппаратные токены. С программными решениями таких дополнительных закупок делать не нужно. К тому же аппаратный токен в виде отдельного устройства можно потерять, а в территориально-распределенных организациях стоимость доставки курьерскими службами новых ключей взамен утраченных может быть очень высокой.

В компаниях, где аппаратные токены внедрены в небольших количествах (например, у руководящего состава), можно расширить сферу применения двухфакторной аутентификации путем предоставления всем другим сотрудникам программных токенов. В сервисе AUTH.AS реализована возможность интеграции с любыми существующими на рынке OTP-токенами.

Аутентификация может быть реализована разными способами: кому-то по ряду причин больше подойдут

программные токены, кому-то аппаратные, – но нужно признать, что и те и другие значительно надежнее, чем одноразовые SMS-пароли или пароли, доставляемые по электронной почте.

Разнообразие технологий

Различные токены отличаются и технологиями, на базе которых они работают. Так, например, чаще всего для двухфакторной аутентификации используются токены на базе симметричных криптосистем, которые реализуют TOTP и HOTP в соответствии с документами RFC 4226 [13] и RFC 6238 [14].

Некоторые производители создают собственный уникальный проприетарный алгоритм, на базе которого будут функционировать их ключи. Однако использование скрытых алгоритмов, представляющих собой внутренние разработки компании, является примером подхода «безопасность через неясность», который считается многими специалистами ошибочным, так как исключает возможность проведения независимой оценки недостатков используемых алгоритмов.

Сервис AUTH.AS генерирует одноразовые пароли на основании вышеуказанных RFC.

Интеграция со сторонними производителями

Важный момент для любого сервиса усиленной аутентификации – легкость интеграции с продуктами сторонних производителей.

Сервис двухфакторной аутентификации AUTH.AS предлагает к применению пользователям API RADIUS или REST HTTP. В частности, благодаря этим API существует возможность интеграции сервиса со шлюзами Check Point и другими устройствами или программным обеспечением: платформами 1С, 1С-Bitrix, серверами под управлением ОС на базе Linux, web-приложениями, созданными на базе разнообразных CMS типа Drupal и Wordpress.

Если мы говорим о двухфакторной аутентификации как о способе усилить защищенность своих пользователей или охраняемого периметра, будет важна возможность получения информации о событиях, имеющих отношение к данному сервису. AUTH.AS поддерживает отправку логов при использовании как локальной инсталляции, так и облачного сервиса, что позволяет всегда быть в курсе происходящих событий.

Вместо заключения

Возвращаясь к вопросу импортозамещения, можно смело сказать, что в области двухфакторной аутентификации альтернатива зарубежным производителям есть, и весьма хорошего качества.

Главное преимущество мировых гигантов заключается в их известности и возможности использовать некоторые средства воздействия на общемировой рынок, доступные только крупным корпорациям. Однако у отечественных производителей есть ряд своих «бонусов», помимо того, что это наши разработки. Нужно понимать, что игроки мирового уровня также не лишены ряда специфических проблем, и главная из них – отсутствие возможности быстро перестроиться под требования рынка, опреативно реагировать на его новые тенденции. Сервисы таких компаний крайне медлительны и неудобны.

Отечественные производители в этом плане куда более гибки. Они готовы оперативно доработать свой продукт не только под быстро меняющиеся рыночные реалии, но и под насущные нужды конкретных заказчиков.

Государство сейчас оказывает активную помощь в продвижении отечественных разработок, поэтому хочется верить, что российские ИБ-продукты начнут в итоге превалировать на российских просторах, а их качество будет неуклонно повышаться, что в итоге позволит им найти свое место под солнцем и на глобальном рынке. ■

ЛИТЕРАТУРА

1. Федеральный закон «О персональных данных» от 27 июля 2006 года № 152-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/.

2. Постановление Правительства РФ от 16 ноября 2015 года № 1236 [Электронный ресурс]. – Режим доступа: http://www.garant.ru/products/ipo/prime/doc/71152170/#ixzz4sYLbOsrE/.

3. Единый реестр российских программ для электронных вычислительных машин и баз данных [Электронный ресурс]. – Режим доступа: https://reestr.minsvyaz.ru/reestr/.

4. Динамика и особенности импортозамещения в информационной безопасности. Аналитическое исследование [Электронный ресурс]. – Режим доступа: https://www.securitycode.ru/upload/Importozameschenie_2017.pdf.

5. Многофакторная (двухфакторная) аутентификация / Tadviser: Государство. Бизнес. ИТ [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Многофакторная_(двухфакторная)_аутентификация/.

6. 2017 Trustwave Global Security Report. Аналитическое исследование [Электронный ресурс]. – Режим доступа: https://www2.trustwave.com/2017-Trustwave-Global-Security-Report.html.

7. Произошла утечка информации 143 миллионов клиентов бюро кредитных историй Equifax / Secure News [Электронный ресурс]. – Режим доступа: https://securenews.ru/equifax/.

8. В Интернет «утекла» база данных граждан Турции / Вести.Ру [Электронный ресурс]. – Режим доступа: http://hitech.vesti.ru/article/625633/.

9. Методический документ. Меры защиты информации в государственных информационных системах [Электронный ресурс]. – Режим доступа: http://lawru.info/dok/2014/02/11/n4312.htm.

10. Gartner User Authentication Magic Quadrant [Электронный ресурс]. – Режим доступа: http://www.safenet-inc.pt/authentication-magic-quadrant/.

11. Сайт компании «Аладдин Р. Д.» [Электронный ресурс]. – Режим доступа: https://new.aladdin-rd.ru/.

12. Сайт компании RCNTEC [Электронный ресурс]. – Режим доступа: http://www.rcntec.com/ru/.

13. HOTP: An HMAC-Based One-Time Password Algorithm [Электронный ресурс]. – Режим доступа: http://www.ietf.org/rfc/rfc4226 /.

14. TOTP: Time-Based One-Time Password Algorithm [Электронный ресурс]. – Режим доступа: https://tools.ietf.org/html/rfc6238/.