Тет-а-тет с Интернетом

Владимир Воротников, *руководитель отдела интеграционных решений, ООО "С-Терра СиЭсПи"*

Фулл-тайм онлайн

Развитие техники в последние десять-пятнадцать лет приучило нас к тому, что мы всегда "на связи" и всегда и везде можем получить доступ к информации. Мы читаем почту по дороге на работу, рецензируем важный документ вечером дома, отвечаем на срочное сообщение из кафе за обедом, продолжаем работать с корпоративными ресурсами из гостиницы, находясь в командировке.

При этом мы выходим на связь не со стационарного ПК, а с ноутбука, планшета или смартфона. Да что там смартфон, многие читают почту уже с умных часов. Кроме того, удаленная работа происходит из самых разных мест, через разные каналы связи и провайдеров. Где-то есть ограничения по скорости доступа, где-то закрыты большинство портов, где-то все данные проходят через прокси-сервер. Во-первых, совершенно очевидно, что при такой схеме нужна защита передаваемых данных. Надеяться на безопасность неподконтрольной вам инфраструктуры, настроенной, быть может, не слишком квалифицированным администратором, категорически нельзя. Во-вторых, широкий спектр используемых устройств и каналов связи накладывает ограничение на технологии, которые можно применять.

Архитектурно возможно построить защиту удаленного доступа и другими способами. Если нам необходимо защитить только HTTP-трафик, идущий на определенный портал, или данные от другого определенного приложения, то нам достаточно осуществлять перехват на более высоких уровнях модели OSI.

Старый добрый IPsec

Так, например, технология IPsec хорошо зарекомендовала себя на рынке защиты каналов связи. Она универсально защищает любые приложения на устройстве, не требуя их модификации. Часто в состав IPsec-продуктов входят и функции межсетевого экранирования, что повышает общий уровень защищенности системы. Однако работу через провайдеров с сильно ограниченным диапазоном открытых портов и прокси-серверами нельзя отнести к сильным сторонам IPsec-технологии. Поскольку IPsec-продукты могут защитить весь трафик и работают на сетевом уровне модели OSI, чаще всего они требуют прав администратора устройства и зависят от платформы. Есть ряд продуктов для защиты канала, в которых такие проблемы решены, но иногда за это приходится платить сложностью в распространении и эксплуатации.

Одним из важных преимуществ IPsec является возможность защиты трафика от всех приложений на устройстве по всем сетевым протоколам прикладного и транспортного уровней. Но всегда ли это нужно?

История из моего опыта. Недавно я перешел на домашнем ПК с Windows на Linux. Примерно через две недели я осознал, что вообще не ощутил разницы по одной простой причине: все две недели единственным приложением, которым я пользовался, был Web-браузер. Возможно, это несколько частный случай, однако общая тенденция такова: все больший и больший процент времени пользователи проводят именно в Web-браузерах, протокол HTTP является доминирующим в Интернете, и его защита позволяет решить очень широкий спектр задач.

В России TLS нет?

Если смотреть на западный опыт, то хорошо видно, что работа в этом направлении идет давно и плодотворно. Серьезные Web-порталы, которые работают по протоколу HTTP (не HTTPS), можно пересчитать по пальцам, и, вероятно, их скоро вообще не останется. Все необходимые компоненты для использования протокола TLS (или ранее – SSL) уже встроены в современные ОС, браузеры, Web-серверы. Инфраструктура для работы по HTTPS прошла долгий путь и сейчас работает отлично и практически абсолютно прозрачно для конечного пользователя.

Однако если вы хотите (или вам необходимо в соответствии с требованиями законодательства) защищать передаваемые данные с использованием российских сертифицированных средств – все не так радужно. И тому есть несколько объективных причин. Во-первых, распространение сильной криптографии – регулируемая деятельность, и этот вопрос требует определенной юридической проработки, особенно в случае, если продукт, содержащий криптографию, может быть скачан и использован за пределами РФ. Во-вторых, для лидирующих мировых ИТ-компаний (Apple, Google и др.) российский рынок зачастую не настолько важен, чтобы они легко шли на партнерские отношения и вносили изменения в свои флагманские продукты. Да если они и решатся на тесное партнерство – еще непонятно, как к этому отнесутся российские регуляторы.

Компаниям, производящим отечественные средства защиты, можно пойти по пути кооперации с российскими производителями, такими, например, как "Яндекс". Так или иначе, это не решает всех проблем: нужно обеспечить поддержку российских криптоалгоритмов на серверной части, не все пользователи готовы пользоваться "Яндекс.Браузером", остается проблема с необходимостью установки дополнительного ПО и, в целом, такое решение не является универсальным.

Если смотреть на западный опыт использования протокола TLS, то хорошо видно, что работа в этом направлении идет давно и плодотворно.

Однако если вы хотите защищать передаваемые данные с использованием российских сертифицированных средств – все не так радужно. Во-первых, распространение сильной криптографии – регулируемая деятельность, и этот вопрос требует определенной юридической проработки, особенно в случае, если продукт, содержащий криптографию, может быть скачан и использован за пределами РФ. Во-вторых, для лидирующих мировых ИТ-компаний российский рынок зачастую не настолько важен, чтобы они легко шли на партнерские отношения и вносили изменения в свои флагманские продукты. Да если они и решатся на тесное партнерство – еще непонятно, как к этому отнесутся российские регуляторы.

В сторону от мейнстрима

Стоит отметить, что использование HTTPS (TLS, в частности) не является единственным возможным решением проблемы удаленного доступа к Web-порталу. И тем более оно не позволяет защитить передачу данных для других протоколов и приложений.

В то же время для корректной работы IPsec-клиента требуется доступ ко всем передаваемым на устройстве данным (т.е. доступ к 3 уровню модели OSI). Чаще всего для получения такого доступа требуется установка специального драйвера в систему. Это ведет сразу к ряду проблем: необходимость установки в систему (зачастую для применения параметров требуется еще и перезагрузка), сложность разработки для широкого спектра операционных систем (конкретная версия ОС имеет существенное значение). Понятно, что при этих ограничениях сложно говорить о простоте распространения и использования, а также прозрачности работы программного средства для конечного пользователя.

Архитектурно возможно построить защиту удаленного доступа и другими способами. Если нам необходимо защитить только HTTP-трафик, идущий на определенный портал, или данные от другого определенного приложения, то нам достаточно осуществлять перехват на более высоких уровнях модели OSI.

Рассмотрим вариант, когда программа для защиты данных может открывать TCP-порт и пассивно ожидать поступления данных, подлежащих защите. Открытие TCP-порта не требует слишком больших привилегий на устройстве. Кроме того, эта операция является относительно платформонезависимой. Это значит, что такой программный продукт не будет требовать установки, административных прав и будет работать на широком спектре аппаратных платформ и семействах ОС.

Разумеется, за подобную простоту приходится платить. Необходимо обеспечить перенаправление конфиденциальных данных в программу защиты. Схема похожа на наличие локального прокси, и в большинстве случаев это возможно. Однако это справедливо не для всех приложений. Важно также проработать и вопрос первичной доверенной доставки программного средства и защиты от фишинга. Из других минусов можно отметить, что продукт, построенный по такой архитектуре, не сможет выполнять межсетевое экранирование (впрочем, и от HTTPS этого тоже никто не ждет).

Тем не менее, данная архитектура имеет преимущества перед TLS. Способность защищать более широкий спектр приложений и протоколов позволяет, например, защитить различные банковские приложения или клиенты удаленного присутствия (как rdesktop). А в случае защиты Web-трафика преимуществом является еще и независимость от используемого браузера. Кроме того, в такую архитектуру отлично вписывается предварительный анализ передаваемых данных (например, антивирусными продуктами или системами обнаружения вторжений).

Может защитить само приложение, не трогая ничего...

Еще одним вариантом защиты данных при удаленной работе является встраивание механизмов защиты непосредственно в целевое приложение. Очевидным плюсом такого подхода является прозрачность для конечного пользователя. Например, о том, что в мессенджер встроен механизм шифрования передаваемых данных, пользователь может даже и не догадываться. Но и минусов у такого подхода предостаточно. Если защищать данные требуется сертифицированным средством, то сертификация конечного приложения ставит крест на его частых релизах. О еженедельном обновлении и улучшении приложения можно забыть, сертифицированная версия будет выходить в лучшем случае раз в год. Кроме того, команды разработчиков специализированных продуктов для обеспечения безопасности зачастую обладают большей экспертизой в области ИБ, чем их коллеги, фокусирующиеся в первую очередь на развитии основной функциональности пользовательского продукта.

...или же изменить вообще всё?

Нельзя не упомянуть, что в противовес многим рассмотренным выше вариантам удаленного доступа с минимальным вмешательством в систему существуют радикально отличающиеся решения. Для случаев, когда безопасность передаваемых данных является безапелляционным приоритетом номер один, существуют механизмы создания доверенного сеанса, когда пользователь загружает на своем устройстве специальную ОС с аппаратно-защищенного носителя информации. Это зачастую ограничивает его в возможности выбора используемых устройств и прикладных программ, но предоставляет высочайший уровень безопасности.

В целом – "хэппи", но не совсем "энд"

Все рассмотренные варианты организации защиты мультиплатформенного удаленного доступа имеют право на жизнь. Все зависит от задач конкретного пользователя и его готовности жертвовать некоторыми удобствами в работе. Как и при решении любой другой технической задачи, важно соблюсти баланс между требованиями бизнеса по функциональности и защищенности, с одной стороны, и комфортом пользователя – с другой. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru