УГРОЗЫ И ЗАЩИТА ДАННЫХ ДЛЯ ТЕХНОЛОГИИ VPN

Койпиш К.А.

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Скудняков Ю.А.- доцент каф. ПЭ, к.т.н,, доцент

В работе рассматривается ряд угроз и подходов защиты данных для технологии VPN.

VPN – это технология, обеспечивающая защищённую (закрытую от внешнего доступа) связь логической сети поверх частной или публичной при наличии высокоскоростного Интернета.

Приватность VPN обычно достигается шифрованием данных, при этом применяемые криптографические методы обеспечивают такую защиту, чтобы посторонние не могли ни прочитать сообщение, ни установить источник передачи. Однако, для того чтобы посмотреть данные в зашифрованном соединении, злоумышленникам вовсе необязательно взламывать алгоритм шифрования.

Каждый клиент использует VPN для решения определенных задач. С помощью этой технологии к сети центрального офиса подключаются удаленные филиалы, дистанционные рабочие места или мобильные сотрудники. Банки могут предоставлять услуги доступа к платежным сервисам, обеспечивая безопасность по VPN, а операторы — предлагать услуги защищенного соединения своим клиентам. Но массовую популярность технология VPN приобрела после создания реестра запрещенных сайтов и ограничения доступа к ним.

Услуги VPN обхода блокировки сайтов предоставляют в основном иностранные компании. В этом случае канал между клиентом и оператором шифруется, чтобы не было понятно, к какому сайту запрашивается доступ, а само подключение выполняется с иностранного IP, принадлежащего оператору. Чаще всего для этого используется Tor — тогда маршрутизатор оператора, который должен заблокировать трафик, не может определить конечного получателя и отправителя пакета.

В зависимости от цели использования VPN, можно выделить следующие основные угрозы:

Man-in-the-middle (MITM) — «шпионпосредине». Это атака на VPN, при которой злоумышленник вклинивается в канал шифрования между отправителем и получателем, создавая два отдельных шифрованных соединения. Обычно такая атака осуществляется в момент обмена ключами шифрования: злоумышленник перехватывает их и навязывает обеим общающимся сторонам свои ключи. При использовании SSL и сертификатов ему достаточно встроиться в цепочку доверия браузера.

Например, именно так перехватываются SSL-VPN правительствами США, Японии и Китая, поскольку сертификаты правительственных центров этих стран находятся в числе доверенных в большинстве браузеров. Методика перехвата зашифрованного соединения при этом следующая: в инфраструктуре DNS соответствующей страны для сайтов, которые нужно прослушивать, указываются IP-адреса правительственного центра. Когда клиент пытается обратиться к подконтрольному сайту, ему возвращаются адреса правительственного центра.

Поскольку используемый сертификат признается как доверенный, клиент полагает, что соединение защищено. Далее уже правительственный центр расшифровывает трафик, протоколирует его, вновь зашифровывает и пересылает на соответствующий сайт. В результате клиент может и не знать, что взаимодействует с серверами перечисленных правительств, считая, что взаимодействует с требуемым ему сайтом.

Примерно по такой схеме, например, работает Большой китайский межсетевой экран. В отношении правительств США и Японии нет данных о таком способе прослушки, однако среди доверенных сертификатов есть в том числе и правительственные центры сертификации указанных стран.

Общим же методом защиты от MITM-атак является взаимная аутентификация отправителя и получателя до установления соединения, для чего обычно используются инфраструктура открытых ключей (PKI) или другие методы верификации отправителя и получателя.

Man-in-the-browser (MITB) — «шпион в браузере». Это вариант атаки MITM, при котором перехват шифрованного соединения происходит в браузере отправителя или получателя, то есть информация перехватывается еще до шифрования с помощью вредоносных компонент, написанных на Java Script,. NET или других языках, с использованием которых создаются модули расширения для браузеров. Эта атака характерна в основном для SSL VPN, организуемой посредством браузера, и браузерного модуля Tor.

В случае сетевых VPN браузер может быть использован для раскрытия анонимного источника. Например, во многие браузеры встраивается поддержка Web RTC, которая позволяет провести видеоконференцию непосредственно в web-интерфейсе. Однако, если страница с конфигурацией Web RTC загружается с сервера, то само взаимодействие между клиентами выполняется напрямую. В результате появляется возможность раскрытия анонимности путем обращения через анонимное соединение к нужному абоненту и навязывания ему

общения напрямую. Конечно, сам Web RTC предусматривает механизмы шифрования и защиты от прослушивания, но реальный IP-адрес уже будет идентифицирован. Аналогичным способом злоумышленник может раскрыть анонимность с помощью DNS, например, подставив на сайт, защищенный с помощью Tor, ссылку на собственный открытый web-ресурс.

Защититься от MITB можно посредством контроля среды исполнения модулей браузера — например, с помощью антивируса. Некоторые антивирусы позволяют проверять сценарии, написанные на Java Script и других браузерных языках, на вредоносность, так что не стоит ими пренебрегать. А некоторые решения для организации SSL VPN способны осуществлять проверку на наличие шпиона в браузере, поэтому в первую очередь следует внедрять именно их. Кроме того, рекомендуется удостовериться, что в браузере нет подозрительных модулей. Если таковые окажутся, необходимо выяснить, для чего они установлены, и избавиться от ненужных.

Identity Theft — кража личности. В организациях, где VPN используется для защиты доступа к корпоративным ресурсам, у злоумышленников появляется возможность проникновения внутрь сети с помощью аутентификационной информации легальных пользователей. Ее можно получить путем перехвата паролей в результате атаки MITM или MITB. Подключившись к корпоративному шлюзу и создав защищенное соединение, злоумышленник может действовать от имени сотрудника компании и получить расширенные полномочия и доступ к внутренней структуре сети, которая не всегда сегментирована и дополнительно укреплена.

Фактически такое использование VPN позволяет проникнуть сквозь защищенный периметр компании. Именно поэтому и говорят о размывании защитного периметра: часть удаленных устройств находится на неподконтрольной администратору территории, и что с ними происходит — неизвестно. Во избежание компрометации нужны механизмы, которые позволяли бы осуществлять строгую аутентификацию пользователей независимо от того, какие устройства они выбирают для работы. В частности, для решения этой задачи предлагаются специальные аппаратные идентификаторы. Кроме того, необходимо осуществлять контроль за действиями удаленных пользователей для выявления аномального поведения. Некоторые решения даже предусматривают жесткую привязку клиентов VPN к определенному оборудованию и не дают подключаться с посторонних устройств. Наконец, не стоит забывать и о сегментации корпоративной сети, предусмотрев дополнительные проверки при попытке доступа к закрытой информации.

Конечно, всегда возможна атака на криптографические VPN с помощью методов криптоанализа — вплоть до замораживания памяти мобильных устройств с помощью низких температур с целью кражи ключа шифрования. Однако современные алгоритмы и протоколы шифрования настолько сложны, что применение методов криптоанализа для их взлома требует высочайшей квалификации, не всегда позволяет достичь нужного результата и обходится очень дорого. Возможно, в полной модели угроз их надо рассматривать и учитывать, но на практике с этим сталкиваются редко — в основном в случае атак на VPN со стороны спецслужб. Частным лицам и даже небольшим компаниям защититься от подобных атак трудно, поэтому следует относиться к ним как к форс-мажору. Обычно контроль за исправлением ошибок в протоколах и алгоритмах осуществляют сами производители средств VPN, поэтому рекомендуется своевременно устанавливать обновления соответствующих продуктов и библиотек, а также продлевать контакты на техническую поддержку.

Список использованных источников:

1. osp.ru [электронный ресурс]. – Режим доступа: https://www.osp.ru/lan/2016/12/13051078/– Дата доступа: 10.03.2019.

2. tvoi-setevichok.ru[электронный ресурс]. – Режим доступа:https://tvoi-setevichok.ru/korporativnaya-set/vpn-podklyuchenie-chto-eto-takoe-i-dlya-chego-nuzhen-vpn-kanal.html /– Дата доступа: 10.03.2019.