УЯЗВИМОСТИ VPN-ТЕХНОЛОГИЙ

Т.И. Солонович

В работе [1] рассмотрены назначение, принцип действия и разновидности Virtual Private Network (VPN). В настоящее время в связи с быстроразвивающейся сферой технологий и ростом популярности использования, среди VPN-сервисов, кроме безопасных и технологичных, появились мошенники. «Второй стороной медали» являются многочисленных атаки на VPN, кража данных пользователей и их продажа рекламодателям, с целью последующего использования в своих целях. Наиболее простой является дактилоскопия трафика веб-сайта. Шифрование трафика определенных веб-сайтов происходит по шаблону, в результате чего злоумышленник может догадаться, какой сайт посещается, хоть и не видит содержание передачи этого трафика.

Атаки на такие известные криптографические алгоритмы как DES, TripleDES, RSA, AES практически бессильны, ведь стойкость алгоритма определяется не его секретностью, а надежностью ключа, именно поэтому наиболее популярными являются атаки на криптографические ключи. Для того, чтобы обезопасить сервис от атак, в зависимости от необходимости времени хранения информации, ключ должен обладать достаточной длиной.

Механизм генерации ключей – еще одна уязвимость, составляющая алгоритм шифрования (для получения доступа к данным иногда достаточно атаковать всего один элемент алгоритма). Для предупреждения фактора предсказания ключа злоумышленников, необходимо отдавать предпочтения аппаратным системам генерации ключей.

Не стоит пренебрегать и возможными атаками на оборудование VPN, атаками на пользователей и ПО. Существует множество сервисов и приложений, изучив специфики которых, можно выделить наиболее оптимальные и безопасные для использования. Surfshark VNP использует метод шифрования AES-256-GCM. Он предоставляет конфиденциальность и аутентификацию переданных данных, является высоко эффективным и производительным. Имеет функции защиты от фишинга, различных вредоносных программ и утечек, благодаря частному DNS. Позволяет подключаться через несколько стран или с нескольких устройств одновременно при необходимости. Имеет строгую политику отсутствия журналов, обладает функцией раздельного туннелирования и аварийного выключателя, а также уникальной функцией Spoofing GPS. Однако из недостатков можно выделить наличие статических IP-адресов и неравномерности географического расположения серверов, что сказывается на скорости соединения.

Сервис NordVPN использует тот же метод шифрования, ведет политику полного отказа от ведения логов и хранения любой персональной информации пользователей. Так же отличается своей производительностью от конкурентов на рынке других приложений, но уступает им в стоимости ежемесячной подписки. Протоколы – IKEv2/IPsec и OpenVPN.

Сервис ExpressVPN в отличие от вышеперечисленных имеет функцию speed test, которая позволяет тестировать скорость в зависимости от точки подключения. Как и NordVPN поддерживает P2P, благодаря чему можно достаточно быстро загружать файлы. Построен на базе протоколов IKEv2, OpenVPN и L2TP/IPsec, для обеспечения безопасности данных пользователей, а также начал развертывание своего собственного протокола Lightway.

В результате проведенного анализа можно отдать преимущество сервису NordVPN. Немногим от него отличается Surfshark, однако с точки зрения безопасности является более не надежным. Безопасность всей системы равна безопасности самого слабого звена, именно поэтому стоит задумываться даже о самых мелких возможных уязвимостях, ведь даже они могут нанести значительный ущерб как отдельному пользователю, так и крупной компании.

Литература

1. Солонович Т.И. Использование технологии VNP как средства защиты информации // Материалы XVIII Международной научно-практической конференции «Управление информационными ресурсами», Минск, 24 февраля 2022 г. 4 с.