БЕЗОПАСНАЯ ПОРТАТИВНАЯ ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ С АЛГОРИТМОМ ШИФРОВАНИЯ RABBIT STREAM

Рубинштейн Р. Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В. Ю. – д. т. н., доцент

В работе рассмотрена безопасная портативная виртуальная частная сеть с алгоритмом шифрования Rabbit Stream и проблемы, связанные с обеспечением ее безопасности и конфиденциальности.

Мобильность сотрудников стала одним из основных требований корпораций в наше время. Сотрудники часто получают командировку в филиалы или клиентские компании, которые находятся внутри или за пределами своей страны. Компания может соединить компьютерную сеть в центральном офисе с ее филиалами, расположенными далеко от Интернета, но она также может предоставить сотрудникам полномочия для доступа к внутренней сети компании. Однако, при передаче информации через Интернет существуют потенциальные уязвимости, такие как: перехват, мониторинг, модификация или изменение информации неуполномоченными сторонами .

Решение, которое можно использовать для преодоления такой уязвимости, заключается в использовании виртуальной частной сети (VPN). Компания предпочитает использовать VPN, а не использовать выделенную линию или выделенный путь провайдера. Помимо большей рентабельности, VPN также обеспечивает функции безопасности, например, шифрование и аутентификация. VPN-туннель сформирован для защиты связи между объектами в системе. OpenVPN является одной из самых популярных платформ VPN с открытым исходным кодом, разработанной Джеймсом Йонаном в 2002 году, и до сих пор продолжает разрабатываться сообществом разработчиков со всего мира.

Что касается платформы поддержки, OpenVPN уже может использоваться на многих платформах, например Операционная система на основе Linux, Debian, BSD, Microsoft Windows, Mac OS X и Solaris 4.

Существует два вида реализации VPN, то есть программная VPN и аппаратная VPN. Программная VPN является наиболее распространенной реализацией VPN. Он может быть установлен поверх операционной системы, поэтому пользователь может осуществлять удаленный доступ через свой ноутбук. Слабость этого типа реализации VPN заключается в том, что он потребляет память или ресурсы ЦП пользовательского ПК во время удаленного доступа. Поэтому производительность пользовательского ПК может быть ниже во время операции удаленного доступа. С другой стороны, в аппаратной VPN, отдельное оборудование используется для работы удаленного доступа. Аппаратная VPN имеет несколько преимуществ. Во-первых, его можно использовать в разных операционных системах ПК пользователя (независимо от платформы). Во-вторых, он более надежен, поскольку построен на отдельном оборудовании от ПК пользователя. В-третьих, у него также есть дополнительные функции, такие как встроенный брандмауэр и интернет-маршрутизация. В последнее время raspberry pi стала решением для ПК с низким энергопотреблением для любых приложений. Некоторые исследования были проведены для разработки аппаратного VPN на Rasberry Pi7,8.

В этом исследовании автор предлагает аппаратный прототип шлюза VPN, который работает на модели OSI уровня 4 (SSL VPN). SSL VPN выбран из-за фактора гибкости или простоты конфигурации, совместимости с трансляцией сетевых адресов (NAT) и отсутствия проблемы с правилами. Аппаратное обеспечение, используемое в предлагаемой системе, - SBC Raspberry Pi 3 Model B + с основными приложениями, которые модифицированы с помощью OpenVPN. Вдобавок к OpenVPN, алгоритм поточных шифров Rabbit реализован как альтернативный вариант шифровальных пакетов TLS. Алгоритм потоковых шифров Rabbit выбран из-за его криптографической стойкости и простых операций 10. Этот алгоритм также был стандартизирован IETF RFC 4503. По результатам тестирования и анализа этот алгоритм доказал свою эффективность в качестве криптографических и устойчивых криптографических аналитических методов.

Исследование состоит из нескольких этапов. Во-первых, мы выявили проблему с традиционным программным обеспечением VPN, как описано во введении. Во-вторых, мы проводим обзор литературы, чтобы найти современное состояние развития технологии VPN, как программного, так и аппаратного решения. В-третьих, мы предъявляем требования к проектированию и планируем разработку аппаратного и программного обеспечения. Наконец, мы выполняем оценку разработанного прототипа. В остальной части этой статьи обсуждается процесс проектирования и оценки прототипа.

Прототип предназначен для поддержки командировочных сотрудников для выполнения удаленного доступа к внутренней сети компании. Мы называем прототип AR-6000. На рисунке 1 показан сценарий использования AR-6000. Из рисунка 1 видно, что в системе зон AR-6000 есть два основных объекта:

• Пользовательская зона путешественника. Это зона, в которой находится деловой путешественник, который выполняет удаленный доступ пользователя. В этой зоне требуются следующие устройства: ПК или ноутбук, AR-6000 и точка доступа WLAN.

• Зона внутренних ресурсов: это местоположение сети внутренних ресурсов, где расположены серверы и компьютеры компании.

Пользователь берет с собой ноутбук AR-6000 во время командировки. AR-6000 действует как VPN-клиент. В случае, если он хочет получить доступ к внутренней сети, AR-6000 сформирует туннель для VPN-сервера. Он применяет SSL VPN для защищенных данных транзакций из внутренних сетей и через них. Затем пользователь может получить удаленный доступ к внутренней сети компании, чтобы продолжить свою работу на сервере. Есть несколько причин, по которым мы превращаем VPN-клиента в отдельное оборудование. Этот прототип предназначен для выполнения следующих требований:

• Прототип должен быть удобным для пользователя, что означает, что он может быть легко использован любым пользователем без необходимости выполнять настройку каждый раз, когда он хочет его использовать.

• Прототип необходим для работы на всех платформах. Это означает, что прототип можно использовать со всеми типами клиентских операционных систем (ОС) с помощью интернет-соединения.

• Если устройство нуждается в реконфигурации, мы можем настроить его, подключившись к устройству через безопасное соединение оболочки (SSH).

• Требуется, чтобы устройство было способно защищать передачу данных от VPN-клиента к VPN-серверу.

Каждый раз, когда пользователь выполняет удаленный доступ к внутренним ресурсам, AR-6000 получает запрос от ПК пользователя через порт Ethernet, который подключен через кроссовер UTP-кабеля, затем пересылает эти запросы на сервер VPN-ретрансляции предполагаемых получателей через интерфейс Wi-Fi. -Fi, интерфейс Wi-Fi, подключенный к точке доступа WLAN. В общем, AR-6000 служит для моста связи между пользователем ПК и внешней сетью, будь то для доступа в Интернет или удаленного доступа к внутренним ресурсам.

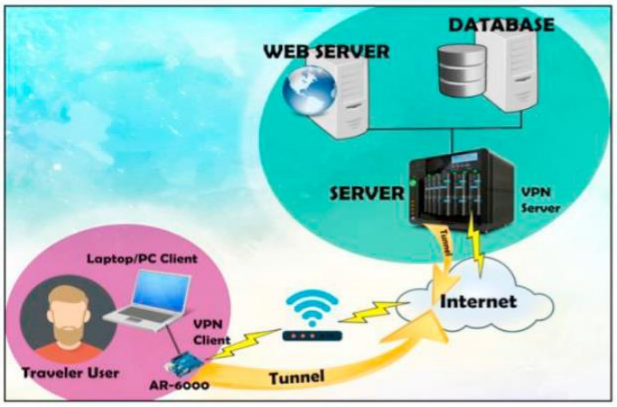

Рисунок 1 Portable VPN usage scenario (AR-6000)

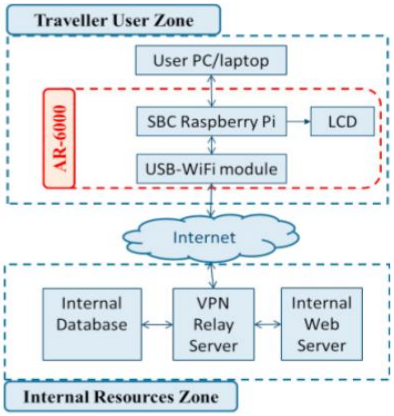

Рисунок 2 Hardware Design of AR-6000

Исходя из требований к дизайну, описанных в предыдущем подразделе, для реализации в пользовательской зоне путешественника и зоне внутренних ресурсов требуется немного оборудования, как показано на рис. 2. В пользовательской зоне путешественника используется пользовательский ПК / ноутбук и AR-6000. AR-6000 состоит из SBC Raspberry Pi 3 Model B + в качестве модуля микроконтроллера, модуля LCD для дисплея и модуля USB Wi-Fi в качестве средства связи. Микроконтроллер организует все функции прототипа AR-6000, например, управление связью с ПК пользователя, маршрутизация, переадресация IP, маскировка IP и т. д. OpenVPN-R устанавливается в качестве основных приложений в микроконтроллере. ЖК-модуль используется для отображения информации, такой как IP-порт Ethernet AR-6000, и для запуска приложения с помощью модуля с сенсорным экраном. Для подключения к Интернету AR-6000 оснащен модулем Wi-Fi в качестве средства связи с ближайшей точкой доступа WLAN. Пользовательский ПК выполняет запрос доступа к серверу ретрансляции VPN через AR-6000. Пользовательский ПК также может настроить AR-6000 через SSH-соединение. С другой стороны,

во внутренней зоне ресурсов есть 3 компонента, то есть сервер ретрансляции VPN, внутренняя база данных и внутренний веб-сервер. Сервер ретрансляции VPN - это компьютер, который используется в качестве цели удаленного доступа пользователя. Он получает и организует запрос удаленного доступа от AR-6000. Open VPN-R также устанавливается на сервере ретрансляции VPN, чтобы создать VPN-туннель к AR-6000 с шифротекстами Rabbit.

Разработка программного обеспечения

В этом разделе рассматривается дизайн программного обеспечения для прототипа переносного VPN. Программный пакет является модификацией OpenVPN. Он называется Open VPN + R. Это программное обеспечение работает на SBC Raspberry Pi Model B + в качестве основных приложений VPN. Принципиальным отличием OpenVPN + R от оригинального OpenVPN является включение шифровальных наборов Rabbit в качестве альтернативного варианта шифровальных наборов TLS для защиты пути или канала данных транзакции. OpenVPN использует OpenSSL для криптографических алгоритмов и предоставления шифровальных пакетов TLS. Поэтому, чтобы добавить шифровальные наборы Rabbit в OpenVPN-R, необходимо реализовать алгоритмы для потоковых шифров Rabbit в OpenSSL и изменить OpenVPN, чтобы они могли распознавать алгоритм потокового шифра, который реализован в OpenSSL Rabbit.

Для осуществления реализации необходимо разработать новые наборы шифров TLS, которые представляют собой комбинацию нескольких криптографических алгоритмов с алгоритмом шифрования потока Кролика в качестве алгоритма шифрования данных (алгоритм массового шифрования). Комбинация криптографических алгоритмов состоит из алгоритмов аутентификации сервера, алгоритмов обмена ключами, алгоритмов шифрования данных и алгоритмов дайджеста сообщений. Новые наборы шифров TLS, сделанные в этом исследовании, относятся к стандарту протокола TLSv1.2 (RFC 5246), как определено в таблице 2.

Ciphersuites Rabbit	Authentication	Key Change	Encryption	Message Digest
TLS_RSA_WITH_RABBIT_SHA	RSA	RSA	RABBIT	SHA
TLS_DHE_DSS_WITH_RABBIT_SHA	DSS	DSS	RABBIT	SHA
TLS_DHE_RSA_WITH_RABBIT_SHA	RSA	RSA	RABBIT	SHA

Таблица 2 Protocol Ciphersuite Rabbit in Open VPN-R

В этом исследовании используется OpenSSL версии 1.0.2h, которая, как утверждается, успешно закрыла пробел в безопасности. В общем случае реализация модификации исходного кода будет осуществляться как в библиотеках OpenSSL, так и в библиотеке криптографии и в библиотеке SSL. Добавления в библиотеку криптографии необходимы, потому что в этой библиотеке хранятся все криптографические функции, включая алгоритм шифрования потока Кролика, который будет реализован. Что касается библиотеки SSL, то основное внимание уделялось добавлению новых наборов шифров, в результате чего была реализована реализация SSL, поддерживающая использование алгоритма потокового шифра Rabbit. Его также необходимо изменить в некоторых скриптах компиляции, чтобы исходный код реализованного алгоритма потокового шифра Rabbit можно было интегрировать с OpenSSL. Результатом этого этапа реализации является версия OpenSSL 1.0.2h, которая загрузила алгоритм потокового шифра Rabbit в качестве одного из альтернативных вариантов алгоритма шифрования, как для кодирования на наборах TLS, так и для ручного кодирования через консольное приложение OpenSSL.

После завершения реализации алгоритма потокового шифра Rabbit, следующий будет изменен и перекомпилирован на OpenVPN для распознавания алгоритма потокового шифра Rabbit, реализованного в OpenSSL. OpenVPN, используемый в этом исследовании, является версией OpenVPN 2.3.10. Как только изменения в OpenVPN завершены, результатом является версия 2.3.10 OpenVPN, которая уже может распознавать алгоритм шифрования потока Кролика. Версия OpenVPN называется OpenVPN-R, которая будет использоваться в качестве основного приложения устройств AR-6000.

Список использованных источников:0

1.Choffnes D. A case for personal virtual networks. In: Proceedings of the 15th ACM Workshop on Hot Topics in Networks. 2016. p. 8– 14.

2.Alshalan A, Pisharody S, Huang D. A survey of mobile VPN technologies. IEEE Commun Surv Tutorials. 2016;18(2):1177–96.

3.Matotek D, Turnbull J, Lieverdink P. Networking with VPNs. In: Pro Linux System Administration. Springer; 2017. p. 701–31.