УДК 004.94 **DOI: 10.18413/2518-1092-2022-7-1-0-3**

Жихарев А.Г.[1]
Фефелов О.С.[2]
Маматов М.Е.[2]

ОБЗОР НЕКОТОРЫХ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ С ПОЗИЦИИ ИХ БЕЗОПАСНОСТИ

[1)] Белгородский государственный технологический университет им. В.Г. Шухова, ул. Костюкова, 46, Белгород, 308012, Россия
[2)] Белгородский государственный национальный исследовательский университет, ул. Победы, 85, Белгород, 308015, Россия

e-mail: zhikharev@bsu.edu.ru

Аннотация
В статье рассматриваются некоторые протоколы передачи данных в компьютерных сетях с позиции обеспечения защиты информации. Показано, что в настоящее время, вопросы безопасной передачи информации приобретают все большую актуальность. Особенно, это касается защищенности автоматизированных систем на уровне протоколов передачи данных. В частности, рассматриваются протоколы передачи данных, использующиеся для организации виртуальных частных сетей. Это связано с тем, что современные реалии побуждают пользователей к активному использованию подобных технологий как для реализации санкционированного функционала, так и для обхода регламентов предоставления доступа к запрещенным электронным ресурсам. Кроме того, в работе показано, что использование различных протоколов передачи информации создает определенные проблемы при разработки автоматизированных решений, в частности в вопросах интерпретации сетевого трафика. Авторами предлагается гибкий механизм динамического формирования правил передачи данных в зависимости от задач, стоящих перед разработчиками подобных систем.
Ключевые слова: протокол передачи данных; информационная безопасность; сетевой трафик; интеллектуальные сетевые технологии
Для цитирования: Жихарев А.Г., Фефелов О.С., Маматов М.Е. Обзор некоторых протоколов передачи данных с позиции их безопасности // Научный результат. Информационные технологии. – Т.7, №1, 2022. – С. 27-31. DOI: 10.18413/2518-1092-2022-7-1-0-3

Zhikharev A.G.[1]
Fefelov O.S.[2]
Mamatov M.E.[2]

REVIEW OF SOME DATA TRANSFER PROTOCOLS FROM THE POSITION OF INFORMATION SECURITY

[1)] Belgorod state technological university named after V.G. Shukhov, 46 Kostyukova St., Belgorod, 308012, Russia
[2)] Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia

e-mail: zhikharev@bsu.edu.ru

Abstract
The article identifies and describes the main problems in the field of recreational fishing: the The article discusses some data transfer protocols in computer networks from the standpoint of information security. In particular, data transfer protocols used to organize virtual private networks are considered. This is due to the fact that modern realities encourage users to actively use such technologies both to implement authorized functionality and to circumvent the regulations for providing access to prohibited electronic resources. In addition, the paper shows that the use of various information transfer protocols creates certain problems in the development of automated solutions, in particular, in the interpretation of network traffic.
Key words: data transfer protocol; information security; network traffic; intelligent network technologies

For citation: Zhikharev A.G., Fefelov O.S., Mamatov M.E. Review of some data transfer protocols from the position of information security // Research result. Information technologies. – T.7, №1, 2022. – P. 27-31. DOI: 10.18413/2518-1092-2022-7-1-0-3

ВВЕДЕНИЕ

Прежде чем рассматривать протоколы, используемые для реализации технологии VPN, рассмотрим подробнее, что из себя представляет данная технология. VPN (Virtual Private Network) – виртуальная частная сеть [1]. Разберём подробнее каждое слово в названии данной технологии. Слово «сеть», для многих, достаточно понятно – как минимум это объединение двух или более устройств (узлов) поддерживаемым ими видом связи для обмена информацией. Слово «частная» – означает, что эта сеть организованна для дозволенных (санкционированных) узлов сети, собственно данная составляющая VPN является самой главной, определяя ряд требований этой самой дозволенности (частности), из которых можно выделить:

1. Маркировка пользователей «частной» сети.
2. Маркировка информации которой обмениваются пользователи, для того чтобы она не смешивалась с чужой информацией.
3. Защита информации, к примеру – шифрованием.
4. Сохранение целостности способа передачи информации – защита от проникновения посторонних в «частную» сеть, проверка источников передачи информации, защита от утечек информации в незашифрованном виде.

Последнее слово это «виртуальная». В данном контексте это понятие означает, что такая сеть абстрагирована от физических линий связи и устройств. Такой сети не важно, по каким и скольким каналам связи она проложена, т.е. для связи, пользователям такой сети, не нужно иметь собственные линии связи или арендованные, где бы они не находились им достаточно иметь выход в сеть Интернет, а соединение построится «виртуально» на существующих линиях связи в сети Интернет.

Разобрав сущность технологии VPN, рассмотрим основные сценарии использования этой технологии. Анализ классических публикаций по данной тематике [2,3] показывает, что данная технология является средством защиты информации при организации коммуникации между двумя и более объектами информационной инфраструктуры. Но, у данной технологии, также есть «полезное» побочное свойство, которое позволяет скрыть физическое местоположение объекта информационной инфраструктуры. Таким образом, технология виртуальных частных сетей используется при:

1. Построение защищённого канала связи между двумя или более сегментами сети. К примеру: подразделения одной организации, находящиеся в разных городах или странах.
2. Построение защищённого канала при удалённом подключении сотрудника к корпоративной сети организации.
3. «Виртуальное» изменение местоположения пользователя с помощью услуг различных VPN сервисов. В таком случае весь трафик пользователя будет проходить через сервер, принадлежащий VPN сервису, того региона из которого нужно отразить местоположение заказчика.

Для реализации VPN технологии и вышеуказанных сценариев служат различные протоколы сетевой безопасности, служащие для связи и шифрования. На основании подходящих протоколов, специалист, может строить своё решение того или иного сценарии применении данной технологии. Рассмотрим основные протоколы сетевой безопасности для реализации технологии VPN.

МЕТОДЫ

Для реализации виртуальной сети всегда применяются, так называемые, туннельные протоколы [4]. Протокол PPTP [5] (Point-to-Point Tunneling Protocol). Протокол PPTP – это

туннельный протокол типа точка-точка, позволяющий компьютеру абонента устанавливать защищённое соединение с сервером или с компьютером другого абонента за счёт создания специального туннеля в стандартной, незащищённой сети на канальном уровне модели OSI. Каналом называется защищённая линия связи в сети Интернет, а точками являются абоненты защищённой линии связи. Канал выполняет роль только посредника.

PPTP использует два соединения типа PPP – одно для управления и обслуживания, а другое для инкапсуляции данных. Первое соединение работает с протоколом TCP и использует порт 1723. Второе соединение работает с протоколом GRE. PPTP инкапсулирует кадры PPP в IP-пакеты для передачи по глобальной сети Интернет.

Точки соединяются посредством PPP-сессии, данная сессия формируется на базе протокола GRE. За инициализацию протокола GRE и его управление несёт ответственность второе TCP подключение. Информация в формате зашифрованного пакета IPX передаётся от точки к точке дополняется управляющей информацией. Когда пакет попадает на другой конец линии связи, специальное приложение извлекает содержащиеся в нём данные и отправляет на постобработку, которая производится встроенными средствами системы соответственно указанному протоколу. Взлом данных возможен только в процессе получения, для чего нужно уделить особое внимание на надёжность логина и пароля.

Можно выделить следующие средства организации безопасности при работе с PPTP:

- протокол проверки подлинности MSCHAP-v1 [6].
- протокол проверки подлинности MSCHAP-v2 [6].
- протокол проверки подлинности EAP-TLS [7].
- протокол шифрования данных MPPE.

Далее рассмотрим подробнее структуры пакетов при использовании различных протоколов передачи данных.

Таблица 1

Структура пакета для передачи по туннелю PPTP

Table 1

Packet structure for transmission over the PPTP tunnel

Заголовок кадра передачи	IP заголовок	GRE заголовок	PPP заголовок	Зашифрованные данные PPP	Окончание кадра передачи

Универсальность протокола PPTP позволяет обеспечить базовую защиту данных в локальных сетях где реализованы протоколы IPX и является самым простым средством сетевой безопасности, но данный протокол устарел и не рекомендуется для использования.

Далее рассмотрим подробнее протокол L2TP (Layer 2 Tunneling Protocol) [8]. Протокол L2TP – схожий с PPTP туннельный протокол. В отличии от протокола PPTP, который обеспечивает туннелирование и шифрование передаваемых данных, протокол L2TP поддерживает только туннелирование. L2TP не имеет привязки к протоколу IP. Кроме того, в протоколе L2TP реализована функция управления потоками данных, а также ряд функций защиты, к примеру возможность работы с протоколами AH и ESP, которые являются основой стека протокола IPSec. Хоть данный протокол действует по подобию протокола канального уровня модели OSI, на самом деле он является протоколом сеансового уровня. Использует передачу данных поверх протокола UDP и имеет зарегистрированный порт 1701. Использует одинаковый формат сообщений как для управления туннелем, так и для пересылки данных.

Можно считать, что L2TP это логичное развитие протокола PPTP, который избавился от двух соединений (одно из которых – GRE) и добавил себе новые логические сущности - LNS (сервер или маршрутизатор) и LAC (провайдер). То есть теперь протокол L2TP использует схемы, где туннель создается между сервером удаленного доступа провайдера и маршрутизатором локальной сети. Также протокол может открывать несколько туннелей, каждый из которых может использоваться для конкретного приложения.

Соединение по протоколу L2TP реализуется в три этапа:

- Установка соединения с сервером удаленного доступа локальной сети. Пользователь создает PPP-соединение с провайдером ISP. Концентратор доступа LAC принимает соединение, и создает канал PPP. Также концентратор выполняет аутентификацию пользователя и конечного узла. На основе имени пользователя провайдер ISP решает, нужно ли ему туннель на основе L2TP, если нужно, то создается туннель.
- LSN локальной сети реализует аутентификацию пользователя. Для этого может быть использован любой протокол аутентификации пользователя.
- При успешной аутентификации создается защищенный туннель между LAC и LNS локальной сети.

В протоколе L2TP могут быть использованы различные методы аутентификации – PAP, CHAP, MS-CHAPv1, MS-CHAPv2. PAP и MS-CHAPv1 являются наиболее ненадежными методами аутентификации для соединения с использованием протокола L2TP.

У протокола L2TP нет механизма шифрования данных. Для шифрования используется работа L2TP поверх протокола IPsec.

L2TP обладает встроенным механизмом проверки работоспособности соединения в виде посылки keepalive пакетов «Hello». Механизм гарантирует корректный разрыв соединения и освобождение ресурсов с обеих сторон сессии. Также важным аспектом является способность клиентского ПО переустановить VPN соединение при пропадании действующего, такую операцию может осуществляться только клиентом, но не LAC или LNS.

Таблица 2

Структура пакета для передачи по туннелю L2TP

Table 2

Packet structure for transmission over the L2TP tunnel

IP заголовок	UDP заголовок	L2TP заголовок	PPP заголовок	PPP данные (IP датаграмма)

Таблица 3

Структура пакета для передачи по туннелю L2TP с применением шифрования IPsec

Table 3

Packet structure for transmission over the L2TP tunnel using IPsec encryption

IP заголо-вок	ESP заголовок IPsec	UDP заголовок	L2TP заголовок	PPP заголовок	PPP данные (IP датаграмма)	ESP замыкатель IPsec	Замыкатель проверки подлинности IPsec
		Зашифровано IPsec					

ЗАКЛЮЧЕНИЕ

Рассмотренные выше протоколы передачи данные являются малой частью огромного массива существующих протоколов передачи информации в компьютерных сетях. Действительно, протоколы создаются отдельными производителями программного обеспечения, сетевого оборудования. Часто при реализации той или иной технологии, разработчик сталкивается с вопросом выбора стека протоколов передачи данных для решения своих задач. Эта проблема заключается в том, что не существует единого подхода к описанию таких технологий с едиными критериями их эффективности. Наличие такой системы протоколов передачи данных позволило бы в перспективе реализовать динамическое использование протоколов передачи данных для различных задач, в зависимости от различных параметров передачи данных.

Список литературы

1. Петренко С. Защищенная виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных // Мир Internet. М. 2001. № 2.
2. Файльнер М. Виртуальные частные сети нового поколения LAN // Журнал сетевых решений. М. 2005. № 11.
3. Фратто М. Секреты виртуальных частных сетей. Сети и системы связи // Emergent Actors in World Politics: How States and Nations Develop and Dissolv. Princeton University Press. 1997. № 3.
4. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. М. КУДИЦ-Образ. 2001.
5. Колесников О. Linux: создание виртуальных частных сетей (VPN): пер. с англ. / О. Колесников, Б. Хетч. М. КУДИЦ-Образ. 2004. 459 с.
6. M. W. Youssef, Hazem El-Gendy. Securing Authentication of TCP/IP Layer Two By Modifying Challenge-Handshake Authentication Protocol // Advanced Computing: An International Journal. 2012. P. 11.
7. Rand Morimoto, Kenton Gardinier, Michael Noel and Joe Coca. Microsoft Exchange Server 2003 Unleashed. 2003. P. 244.
8. Kaufman. C., Perlman. R., и Speciner. M., Network Security: Private Communications in a Public World // Prentice Hall. 1995.

References

1. Petrenko S. Protected virtual private network: a modern view on the protection of confidential data // World of the Internet. M. 2001. No. 2.
2. Faylner M. Virtual private networks of the new generation LAN // Journal of Network Solutions. M. 2005. No. 11.
3. Fratto M. Secrets of virtual private networks. Networks and communication systems // Emergent Actors in World Politics: How States and Nations Develop and Dissolv. Princeton University Press. 1997. No. 3.
4. Ivanov M. A. Cryptographic methods of protecting information in computer systems and networks. M. KUDITs-Obraz. 2001.
5. Kolesnikov O. Linux: the creation of virtual private networks (VPN): per. from English. / O. Kolesnikov, B. Hatch. M. KUDITs-Obraz. 2004. 459 p.
6. M. W. Youssef, Hazem El-Gendy. Securing Authentication of TCP/IP Layer Two By Modifying Challenge-Handshake Authentication Protocol // Advanced Computing: An International Journal. 2012. P. 11.
7. Rand Morimoto, Kenton Gardinier, Michael Noel and Joe Coca. Microsoft Exchange Server 2003 Unleashed. 2003. P. 244.
8. Kaufman. C., Perlman. R., and Speciner. M., Network Security: Private Communications in a Public World // Prentice Hall. 1995.

Жихарев Александр Геннадиевич, кандидат технических наук, доцент, доцент кафедры программного обеспечения вычислительной техники и автоматизированных систем
Фефелов Олег Сергеевич, студент 4-го курса направления подготовки «Информационные системы технологии»
Маматов Михаил Евгеньевич, студент 4-го курса направления подготовки «Математическое обеспечение и администрирование информационных систем»

Zhikharev Alexander Gennadievich, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Engineering and Automated Systems Software
Fefelov Oleg Sergeevich, 4th year student of the field of study "Information Systems Technology"
Mamatov Mikhail Evgenievich, 4th year student of the specialization "Mathematical support and administration of information systems"