Математические структуры и моделирование 2022. № 4 (64). С. 112–116

УДК 004.056
DOI 10.24147/2222-8772.2022.4.112-116

ПРОТОКОЛ ОБМЕНА КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ В МУЛЬТИМАРШРУТНОЙ СРЕДЕ ПЕРЕДАЧИ ДАННЫХ

А.А. Богаченко[1]
студент, e-mail: bogachenko03@mail.ru
Н.Ф. Богаченко[2]
к.ф.-м.н., доцент, e-mail: nfbogachenko@mail.ru
Д.Д. Лаврова[2]
студент, e-mail: drlvrv@gmail.com
Д.Н. Лавров[2]
к.т.н., доцент, e-mail: dmitry.lavrov72@gamil.com

[1]Университет ИТМО, Санкт-Петербург, Россия

[2]Омский государственный университет им. Ф.М.Достоевского, Омск, Россия

Аннотация. В статье предлагается принципиально новый протокол обмена криптографическими ключами, использующий наличие нескольких альтернативных маршрутов передачи данных в сети с коммутацией пакетов, при условии, что не все маршруты контролируются потенциальным противником.

Ключевые слова: протокол обмена, криптографические ключи, сеть с коммутацией пакетов, защита информации.

1. Мотивация

Современные распределённые компьютерные сети представляют собой сложную систему узлов (компьютеров и активного сетевого оборудования), которая описывается семиуровневой эталонной моделью взаимодействия открытых систем [1].

Как правило сети реализуются на технологии коммутации каналов или пакетов. В обоих случаях подразумевается наличие одного установленного канала или маршрута между взаимодействующими узлами.

Тем не менее, существуют технологии, которые позволяют предавать данные по нескольким путям одновременно, например [2]. Как правило, цель этих технологий — это увеличение потока передаваемых данных и повышение отказоуйсточивости канала связи (с точки зрения доставки данных).

Интересным направлениям является построение собственных сетей связи поверх существующей инфраструктуры публичных сетей. Осуществляться это за счёт разных технологий, в том числе числе технологии VPN [3] (реализуемые на разных уровнях модели OSI со 2 по 4), так и сетей Dark Internet типа

I2P [4] или TOR [5][1].

В нашей статье мы покажем что такие мультимаршрутные сети можно использовать для повышения уровня конфиденциальности передаваемых данных.

В предыдущих статьях [7–11] рассматривались вопросы передачи с защитой передаваемой информации на основе различных вариантов протокола разделения секрета. Основным недостатком использования классических вариантов разделения секрета является тот факт, что размеры теней, как правило равны размерам самого сообщения. В дальнейшем в нашей статье мы рассмотрим вариант с существенно меньшей избыточностью.

С другой стороны для обеспечения конфиденциального канала передачи данных, необходим обмен криптографическими ключами между адресатом и отправителем. Для этого используют протоколы на основе асимметричной криптографии. Для взлома асимметричной системы шифрования используется знание открытого ключа, который, как правило, передаётся по открытому же каналу связи. Считается, что это сложная задача для современной вычислительной техники. В тоже время, в последние годы активно ведутся работы по достижению, так называемого «квантового превосходства», идёт гонка за первенство в построении квантового вычислителя. В связи с этим возникает угроза взлома криптосистем на основе асимметричного ключа с помощью алгоритма Шора [6]. Возникает проблема «взлома из будущего»: взлом ранее перехваченных данных обмена ключами. Под угрозой взлома вся современная криптографическая инфраструктура распределения ключей.

Мы предлагаем использовать мультимаршрутные сети для повышения защищённости процедуры передачи открытого ключа шифрования и защиты как от перехвата передачи, так и от «взлома из будущего» при соблюдении определённых условий.

2. Постановка задачи

Имеется мультимаршрутная сеть, в которой между отправителем и получателем можно построить n независимых маршрутов (т.е. не имеющих общих участков). Потенциальный противник может контролировать часть из них, но не все.

Требуется передать сообщение, содержащее информацию о ключе, получателю через мультимаршрутную сеть так, чтобы перехватив часть фрагментов сообщения потенциальный противник не был в состоянии восстановить по ним ключ.

Одним из подходов к решению данной задачи может быть использование алгоритмов разделения секрета [1]. Ранее мы уже упоминали, что основным недостатком такого подхода является избыточность: размер каждой тени (части секрета) равен размеру всего сообщения. Предлагаем иной подход.

[1]В момент написания статьи проект TOR заблокирован Роскомнадзором на территории РФ, URL: `https://habr.com/ru/news/t/596507/`

3. Идея алгоритма

Идея алгоритма основана на результатах [8]. Суть алгоритма обмена ключами в многоканальной среде передачи данных заключается в следующем:

Шаг 1. Формируем ключ истинно случайным образом (с соблюдением требований безопасности конкретной асимметричной криптосистемы).

Шаг 2. Разбиваем ключ K на число фрагментов равное количеству используемых каналов $K_1, \ldots, K_n$.

Шаг 3. Формируем данные для передачи по i-му каналу:
$D_i = K_i \oplus K_{i+1}$, $i = \overline{1, n-1}$

Шаг 4. Формируем данные для передачи по последнему n-му каналу:
$D_n = K_n \oplus (K_1 \gg 1)$.

Для усиления безопасности вместо циклического сдвига можно использовать произвольную не тождественную перестановку, о которой взаимодействующие стороны должны договориться заранее.

Действия на принимающей стороне.

Шаг 1. Получаем $D_1, \ldots, D_n$.

Шаг 2. Вычисляем $P = \bigoplus\limits_{i=1}^{n} D_i = K_1 \oplus (K_1 \gg 1)$.

Шаг 3. Полагая первый бит заданным заранее в K_1, решаем уравнение с предыдущего шага и находим K_1.

Шаг 4. Восстанавливаем оставшиеся части ключа
$K_i = D_i \oplus K_{i-1}$, для $i = \overline{2, n-1}$;
$K_n = D_n \oplus (K_1 \gg 1)$.

В случае если злоумышленник контролирует все каналы передачи, то он способен перехватить открытый ключ и сложность взлома будет определяться сложностью вскрытия используемой открытой шифросистемы. Во всех остальных случаях информация о ключе не доступна напрямую. Рассмотрим случай, когда злоумышленник контролирует k каналов передачи информации, тогда мощность пространства перебираемых ключей сокращается с 2^m до $2^{m\cdot(n-k+1)/n}$.

Поясним работу алгоритма на примере при $k = 3$. Пусть $m = 9$, договорённость о первом бите ключа — всегда единица.

Шаг 1. Сгененрирован случайный ключ $K = 101110010$ (за исключением первого бита)

Шаг 2. $K_1 = 101$, $K_2 = 110$, $K_3 = 010$.

Шаг 3. $D_1 = K_1 \oplus K_2 = 101 \oplus 110 = 011$ $D_2 = K_2 \oplus K_3 = 110 \oplus 010 = 100$.

Шаг 4. $D_3 = K_3 \oplus (K_1 >> 1) = 010 \oplus (101 >> 1) = 010 \oplus 110 = 100$.

На принимающей стороне

Шаг 1. Получены $D_1 = 011$, $D_2 = 100$, $D_3 = 100$.

Шаг 2. $D_1 \oplus D_2 \oplus D_3 = 011 \oplus 100 \oplus 100 = 011$.

Шаг 3. Решаем уравнение для бит $K_1 = \overline{x_1x_2x_3}$ $110 = \overline{x_1x_2x_3} \oplus \overline{x_3x_1x_2}$. Считая $x_1 = 1$, получаем

$$1 \oplus x_3 = 0$$

$$x_2 \oplus 1 = 1$$

$$x_3 \oplus x_2 = 1$$

Следовательно, $x_2 = 0$ и $x_3 = 1$, а $K_1 = 101$.

Шаг 4. Восстанавливаем оставшиеся части ключа. $K_2 = D_1 \oplus K_1 = 011 \oplus 101 = 110$; $K_3 = D_2 \oplus K_2 = 100 \oplus 110 = 010$.

Заключение

Надёжность данного протокола в случае отсутствия контроля злоумышленником всех каналов передачи данных обусловлена фундаментальным результатом К. Шеннона об совершенной криптостойкости шифра Вернама в режиме работы одноразового блокнота. Действительно, основной операцией вычисления фрагментов секрета является операция исключающего ИЛИ, а гамма, накладываемая на фрагмент сообщения, — истинно случайна и повторно никогда не используется.

Литература

1. ГОСТ Р ИСО/МЭК 7498-1-99. ВОС. Базовая эталонная модель. Часть 1. Базовая модель.
2. Балансировка нагрузки между каналами связи используя протокол EIGRP на маршрутизаторах CISCO. URL: `https://nettips.ru/article/cisco_eigrp_balans.html` (дата обращения: 26.11.2022).
3. Куртуков Е. IPSec всемогущий // Хабр. URL: `https://habr.com/ru/post/504484/`
4. I2P. Проект The Invisible Internet. URL: `https://geti2p.net/ru/`
5. TOR Project. URL: `https://www.torproject.org/` (дата обращения: 26.11.2022).
6. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science : Conference Publications. 1997. P. 1484–1509.
7. Ефимов В.И., Файзуллин Р.Т. Система мультиплексирования разнесенного TCP/IP трафика // Математические структуры и моделирование. 2002. № 10. С. 170–171.
8. Лавров Д.Н. Схема разделения секрета для потоков данных маршрутизируемой сети // Математические структуры и моделирование. 2002. № 10. С. 192–197.
9. Лавров Д.Н., Дулькейт В.И., Михайлов П.И., Свенч А.А. Анализ надёжности алгоритма разделения секрета в сетевых потоках // Математические структуры и моделирование. 2003. № 12. С. 146–154.
10. Гусс С.В., Лавров Д.Н. Подходы к реализации сетевого протокола обеспечения гарантированной доставки при мультимаршрутной передаче данных // Математические структуры и моделирование. 2018. № 2(46). С. 95–101.
11. Лавров Д.Н. Принципы построения протокола гарантированной доставки сообщений // Математические структуры и моделирование. 2018. № 4(48). С. 139–146.
12. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М : ТРИУМФ, 2002. 816 с.

PROTOCOL FOR THE EXCHANGE OF CRYPTOGRAPHIC KEYS IN A MULTIPATH DATA TRANSMISSION MEDIA

Bogachenko A.A.[1]
Student, e-mail: bogachenko03@mail.ru
Bogachenko N.F.[2]
Ph.D. (Phys.-Math.), Associate Professor, e-mail: nfbogachenko@mail.ru
Lavrova D.D.[2]
Student, e-mail: drlvrv@gmail.com
Lavrov D.N.[2]
Ph.D.(Eng.), Associate Professor, e-mail: dmitry.lavrov72@gamil.com

[1]ITMO University, St. Petersburg, Russia
[2]Dostoevsky Omsk State University, Omsk, Russia

Abstract. The article proposes a fundamentally new cryptographic key exchange protocol that uses the presence of several alternative data transmission routes in a packet-switched network, provided that not all routes are controlled by a potential adversary.

Keywords: exchange protocol, cryptographic keys, packet-switched network, information security.

Дата поступления в редакцию: 27.11.2022