Инженерный вестник Дона, №12 (2024)
ivdon.ru/ru/magazine/archive/n12y2024/9708

Метод множественных стартовых соединений как инструмент повышения информационной безопасности в одноранговых виртуальных частных сетях

В.Д. Зюзин, П.Б. Болдыревский

Нижегородский государственный университет им. Н.И. Лобачевского

Аннотация: В статье представлен метод множественных стартовых соединений, направленный на повышение информационной безопасности одноранговых виртуальных частных сетей. Метод обеспечивает одновременное установление нескольких стартовых соединений через промежуточные узлы, что позволяет усложнить перехват данных и минимизировать риски компрометации соединений. В работе описана алгоритмическая основа метода, а также продемонстрировано его применение на примере сети из четырех узлов. Проведен анализ маршрутизации пакетов, включая этапы их формирования, модификации и передачи. Для вычисления количества уникальных маршрутов и оценки рисков перехвата данных разработан программный комплекс, зарегистрированный в Федеральной службе по интеллектуальной собственности. Программное обеспечение использует матричные и комбинаторные методы, что обеспечивает высокую точность расчетов и эффективность анализа. Представленный метод имеет широкие перспективы применения в одноранговых сетях, системах Интернета вещей и распределенных системах управления.

Ключевые слова: множественные стартовые соединения, одноранговая сеть, виртуальная частная сеть, информационная безопасность, маршруты передачи данных, промежуточные узлы, уникальные маршруты.

Введение

Современные одноранговые виртуальные частные сети (ВЧС) являются ключевым инструментом для организации защищенной передачи данных в распределенных системах. Эти сети обеспечивают высокий уровень конфиденциальности и устойчивость к внешним угрозам [1 – 2], что делает их особенно востребованными в условиях роста числа кибератак, направленных на перехват информации и компрометацию узлов [3 – 6]. Однако усложнение методов атак злоумышленников ставит перед исследователями задачу разработки новых подходов, направленных на повышение информационной безопасности и отказоустойчивости одноранговых сетей [7,8].

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

Одним из перспективных направлений является метод множественных стартовых соединений. Первоначальная концепция метода была изложена в работе [9], где были предложены основные принципы его функционирования. Настоящая статья представляет собой развитие указанного подхода. Метод доработан и дополнен пошаговым описанием процесса его реализации на примере системы с четырьмя узлами, что позволяет наглядно продемонстрировать этапы формирования, модификации и передачи пакетов в сети.

Метод множественных стартовых соединений направлен на повышение уровня информационной безопасности за счет одновременного установления нескольких стартовых соединений через промежуточные узлы. Это позволяет значительно усложнить идентификацию конечного получателя данных и минимизировать вероятность успешного перехвата трафика.

Алгоритмическая основа метода множественных стартовых соединений в одноранговых виртуальных частных сетях

Метод множественных стартовых соединений направлен на создание устойчивого и защищенного канала связи за счет использования нескольких дополнительных туннелей в процессе установления соединения (первой фазы протокола обмена ключами в интернете 2-ой версии (Internet Key Exchange version 2 – IKEv2). Основная цель этого подхода заключается в усложнении перехвата или блокировки соединения злоумышленником путем создания избыточности на начальном этапе передачи данных.

Процесс установления соединения по методу множественных стартовых соединений включает три основных этапа:

На первом этапе узел-инициатор соединения отправляет сообщение трем узлам-ретрансляторам, выбранным из множества N доступных узлов в сети. Каждое сообщение содержит базовую информацию для установления соединения, включая номер текущего этапа, идентификаторы узлов-

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

инициатора и предполагаемого узла-получателя, а также параметры безопасности. Эти параметры включают ключи шифрования, список поддерживаемых протоколов шифрования и хэширования, а также сетевой протокол.

На втором этапе узлы, получившие сообщения на первом этапе, обрабатывают полученные пакеты, модифицируя их содержимое. В частности, происходит изменение номера маршрута (поля S_t), после чего каждый из узлов отправляет модифицированный пакет еще трем промежуточным узлам в сети.

На третьем этапе выполняется процедура, аналогичная этапу 2, с одним важным изменением: модифицированные пакеты отправляются не трем, а двум промежуточным узлам, чтобы уменьшить избыточность на завершающем этапе маршрутизации. Эти узлы затем передают сообщения напрямую узлу-получателю.

К моменту завершения третьего этапа узел-получатель получает до 9 идентичных пакетов. Количество фактически полученных пакетов зависит от конфигурации сети и успешности передачи через промежуточные узлы. Узел-получатель анализирует полученные данные, выбирает один из пакетов и использует его для инициации второй фазы IKEv2.

Процесс маршрутизации в системе с 4-мя узлами

В рассматриваемой системе представлены четыре узла (№1, №2, №3, №4), где узел №1 выполняет роль инициатора соединения, а узел №2 – роль получателя данных. Оба узла, как инициатор, так и получатель, также задействованы в процессе промежуточного обмена данными.

Передача данных осуществляется с учетом следующих параметров:

- номер текущего шага процесса маршрутизации;
- уникальные идентификаторы узлов-инициатора и узлов-получателя;

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

- криптографические ключи и перечень поддерживаемых алгоритмов шифрования и хэширования;
- протокол сетевого взаимодействия (в данном случае безопасному протоколу Интернета (Internet Protocol Security – IPSec).

Для демонстрации механизма метода множественных стартовых соединений выбран маршрут передачи данных через промежуточные узлы, обозначенный как (3,1,2).

На первом этапе узел №1, выступающий в роли инициатора соединения, формирует и отправляет три пакета данных остальным узлам в сети. В данном случае:

- пакет с меткой (2) направляется узлу №2;
- пакет с меткой (3) передается узлу №3;
- пакет с меткой (1) отправляется узлу №4.

На втором этапе узлы, получившие пакеты от инициатора на первом этапе, пересылают данные к остальным участникам сети. Процесс распределения пакетов осуществляется следующим образом:

1. Узел №2, получивший пакет с меткой (2), формирует и передает:

- пакет с меткой (2,2) узлу №1;
- пакет с меткой (2,3) узлу №3;
- пакет с меткой (2,1) узлу №4.

2. Узел №3, получивший пакет с меткой (3), осуществляет распределение данных между остальными узлами сети. Формируются и отправляются следующие пакеты:

- пакет с меткой (3,1) направляется к узлу №1;
- пакет с меткой (3,3) направляется к узлу №2;
- пакет с меткой (3,2) направляется к узлу №4.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

3. Узел №4, получивший пакет с идентификатором (1), осуществляет передачу данных к остальным узлам сети. Процесс включает формирование и отправку следующих пакетов:

- пакет с меткой (1,1) направляется в адрес узла №1;
- пакет с меткой (1,3) передается узлу №2;
- пакет с меткой (1,2) отправляется узлу №3.

По итогам второго этапа маршрутизации, узлы сети обменялись пакетами следующим образом:

1. узел №1 получил 3 пакета ((2,2), (3,1), (1,1));
2. узел №2 отправил 3 пакета ((2,1), (2,2), (2,3)) и принял 2 пакета ((3,3), (1,3));
3. узел №3 отправил 3 пакета ((3,1), (3,2), (3,3)) и принял 2 пакета ((2,3), (1,2));
4. узел №4 отправил 3 пакета ((1,1), (1,2), (1,3)) и принял 2 пакета ((2,1), (3,2)).

На третьем этапе алгоритма, каждый узел, получивший пакеты на предыдущем этапе, обязан отправить их модифицированные версии остальным узлам. Рассмотрим действия узла №1, который получил три пакета: (2,2), (3,1), (1,1). Для каждого полученного пакета выполняются следующие операции:

1. Для пакета (2,2):

- формируется пакет (2,2,2), который передается узлу №2;
- формируется пакет (2,2,3), который передается узлу №3;
- формируется пакет (2,2,1), который передается узлу №4.

2. Для пакета (3,1):

- формируется пакет (3,1,2), который передается узлу №2;
- формируется пакет (3,1,3), который передается узлу №3;
- формируется пакет (3,1,1), который передается узлу №4.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

3. Для пакета (1,1):

- формируется пакет (1,1,2), который передается узлу №2;
- формируется пакет (1,1,3), который передается узлу №3;
- формируется пакет (1,1,1), который передается узлу №4.

Рассмотрим действия узла №2, который получил два пакета: (3,3), (1,3). Для каждого полученного пакета выполняются следующие операции:

1. Для пакета (3,3):

- формируется пакет (3,3,1), который передается узлу №4;
- формируется пакет (3,3,2), который передается узлу №1;
- формируется пакет (3,3,3), который передается узлу №4.

2. Для пакета (1,3):

- формируется пакет (1,3,1), который передается узлу №4;
- формируется пакет (1,3,2), который передается узлу №1;
- формируется пакет (1,3,3), который передается узлу №4.

Рассмотрим действия узла №3, который получил два пакета: (2,3), (1,2). Для каждого полученного пакета выполняются следующие операции:

1. Для пакета (2,3):

- формируется пакет (2,3,1), который передается узлу №1;
- формируется пакет (2,3,2), который передается узлу №4;
- формируется пакет (2,3,3), который передается узлу №2.

2. Для пакета (1,2):

- формируется пакет (1,2,1), который передается узлу №1;
- формируется пакет (1,2,2), который передается узлу №4;
- формируется пакет (1,2,3), который передается узлу №2.

Рассмотрим действия узла №3, который получил два пакета: (2,1), (3,2). Для каждого полученного пакета выполняются следующие операции:

1. Для пакета (2,1):

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

- формируется пакет (2,1,1), который передается узлу №1;
- формируется пакет (2,1,2), который передается узлу №3;
- формируется пакет (2,1,3), который передается узлу №2.

2. Для пакета (3,2):

- формируется пакет (3,2,1), который передается узлу №1;
- формируется пакет (3,2,2), который передается узлу №3;
- формируется пакет (3,2,3), который передается узлу №2.

Анализ маршрутизации пакетов

Для анализа маршрутизации пакетов была рассмотрена сеть, состоящая из четырех узлов (№1, №2, №3, №4). Узел №1 выполняет функцию инициатора соединения, а узел №2 является узлом-получателем. Помимо этих функций, оба узла, как инициатор, так и получатель, участвуют в промежуточной маршрутизации. Узлы №3 и №4 функционируют в качестве ретрансляторов, обеспечивая передачу пакетов между инициатором и получателем.

Передача пакетов организована поэтапно, с использованием метода множественных стартовых соединений. На каждом этапе происходит отправка и модификация пакетов, что позволяет увеличить вариативность маршрутов и затруднить анализ и перехват данных

На основании выполненного анализа итоговые результаты для каждого узла системы можно представить следующим образом:

1. узел №1 передал 9 пакетов с метками ((2,2,1), (2,2,2), (2,2,3), (3,1,1), (3,1,2), (3,1,3)) и получил 6 пакетов с метками ((3,3,2), (1,3,2), (2,3,1), (1,2,1), (2,1,1), (3,2,1)).
2. узел №2 передал 6 пакетов с метками ((3,3,1), (3,3,2), (3,3,3), (1,3,1), (1,3,2), (1,3,3)) и получил 7 пакетов с метками ((2,2,2), (3,1,2), (1,1,2), (2,3,3), (1,2,3), (2,1,3), (3,2,2)).

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

3. узел №3 передал 6 пакетов с метками ((2,3,1), (2,3,2), (2,3,3), (1,2,1), (1,2,2), (1,2,3)) и получил 7 пакетов с метками ((2,2,3), (3,1,3), (1,1,3), (3,3,3), (1,3,3), (2,1,2), (3,2,2)).
4. узел №4 передал 6 пакетов с метками ((2,1,1), (2,1,2), (2,1,3), (3,2,1), (3,2,2), (3,2,3)) получил 7 пакетов с метками ((2,2,1), (3,1,1), (1,1,1), (3,3,1), (1,3,1), (2,3,2), (1,2,2)).

На рисунках 13 – 16 представлены этапы выбора пакетов на каждом шаге маршрутизации. Общая картина маршрутизации показана на рисунке 16, где видно, как пакеты распределяются между узлами.

Для систематизации результатов была составлена таблица 1, в которой указано количество пакетов, переданных и полученных каждым узлом на каждом этапе маршрутизации.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

№ узла	Пакеты	
1	Шаг №1	
	Отправлено	(1), (2), (3)
	Получено	-
	Шаг №2	
	Отправлено	-
	Получено	(2,2), (3,1), (1,1)
	Шаг №3	
	Отправлено	(2,2,1), (2,2,2), (2,2,3), (3,1,1), (3,1,2), (3,1,3), (1,1,1), (1,1,2), (1,1,3)
	Получено	(3,3,2), (1,3,2), (2,3,1), (1,2,1), (2,1,1), (3,2,1)
2	Шаг №1	
	Отправлено	-
	Получено	(2)
	Шаг №2	
	Отправлено	(2,1), (2,2), (2,3)
	Получено	(3,3), (1,3)
	Шаг №3	
	Отправлено	(3,3,1), (3,3,2), (3,3,3), (1,3,1), (1,3,2), (1,3,3)
	Получено	(2,2,2), (3,1,2), (1,1,2), (2,3,3), (1,2,3), (2,1,3), (3,2,2)
3	Шаг №1	
	Отправлено	-
	Получено	(3)
	Шаг №2	
	Отправлено	(3,1), (3,2), (3,3)
	Получено	(2,3), (1,2)
	Шаг №3	
	Отправлено	(2,3,1), (2,3,2), (2,3,3), (1,2,1), (1,2,2), (1,2,3)
	Получено	(2,2,3), (3,1,3), (1,1,3), (3,3,3), (1,3,3), (2,1,2), (3,2,2)
4	Шаг №1	
	Отправлено	-
	Получено	(1)
	Шаг №2	
	Отправлено	(1,1), (1,2), (1,3)
	Получено	(2,1), (3,2)
	Шаг №3	
	Отправлено	(2,1,1), (2,1,2), (2,1,3), (3,2,1), (3,2,2), (3,2,3)
	Получено	(2,2,1), (3,1,1), (1,1,1), (3,3,1), (1,3,1), (2,3,2), (1,2,2)

Рис. 1. – Маршрутизация пакетов

Для вычисления количества уникальных маршрутов, сценариев и вероятность перехвата данных в одноранговой виртуальной частной сети было нами разработано программное обеспечение, которое зарегистрировано в Федеральной службе по интеллектуальной собственности [10]. Комплекс использует матричные и комбинаторные методы, обеспечивая высокую точность и надежность расчетов для анализа информационной безопасности и оценки рисков компрометации передачи данных в одноранговых сетях.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

Заключение

В статье представлен метод множественных стартовых соединений, направленный на повышение информационной безопасности в одноранговых виртуальных частных сетях. Проведенный анализ подтвердил, что применение метода позволяет значительно увеличить количество уникальных маршрутов передачи данных и усложнить процесс их перехвата злоумышленниками. Использование промежуточных узлов и избыточных маршрутов снижает риски компрометации соединений, повышая уровень защиты сети.

Применение разработанного нами метода продемонстрировано на примере сети из четырех узлов, что позволило наглядно представить процесс формирования и передачи данных, а также оценить эффективность предложенного подхода. Для реализации расчетов и анализа параметров маршрутов нами разработан программный комплекс, зарегистрированный в Федеральной службе по интеллектуальной собственности, что подтверждает его прикладное значение. Комплекс использует современные матричные и комбинаторные методы, обеспечивая точность и надежность вычислений.

Разработанный нами алгоритм будет реализован в виде программного обеспечения, предназначенного для интеграции в современные системы информационной безопасности. В ходе реализации планируется использовать язык программирования Python, что обеспечит поддержку популярных операционных систем, таких как Windows (версии 7 и выше) и Linux.

Литература

1. Организация защищенного обмена данными с помощью виртуальных частных сетей (VPN) // IBM URL: ibm.com/docs/ru/i/7.1?topic=options-virtual-private-network-secure-private-communications (дата обращения: 20.09.2024).

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

2. Основы построения защищенных компьютерных сетей // vec.etu.ru URL: vec.etu.ru/moodle/pluginfile.php/294002/mod_resource/content/1/Виртуальные%20частные%20сети%20презентация.pdf (дата обращения: 25.09.2024). — С. 1–25.
3. Лекция 3: Виртуализация сетей // intuit.ru URL: intuit.ru/studies/courses/2324/624/lecture/13588 (дата обращения: 30.09.2024).
4. Наполова Е. И., Кожевников С. В. Защита компьютерных сетей на основе технологии virtual private network // Экономика и качество систем связи. 2018. №2 (8). URL: cyberleninka.ru/article/n/zaschita-kompyuternyh-setey-na-osnove-tehnologii-virtual-private-network/viewer.
5. Росляков, А.В. Виртуальные частные сети. Основы построения и применения. - М.: Эко-Трендз, 2006. - 597 с.
6. Омельченко М. В., Плотникова К. А., Дяглев С. П. Виртуальная частная сеть // Инновационная наука. 2020. №2. — С. 27–29.
7. Васильев Алексей Викторович. Причины роста количества кибератак: анализ технических и нетехнических факторов // Системный анализ и прикладная информатика. 2023. №3. — С. 48–54.
8. Экспертно-Аналитический центр InfoWatch. Тенденции развития киберинцидентов АСУ ТП за 2023 год: аналитический отчет. — М.: InfoWatch, 2024. — 21 с.
9. Зюзин, В. Д., Рябов А.А., Тетеркин М.А. Использование метода множественных стартовых соединений в задаче маскировки VPN-соединения // Труды XXVI научной конференции по радиофизике, посвященной 120-летию М.Т. Греховой : Материалы конференции, Нижний Новгород, 12–27 мая 2022 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

университет им. Н.И. Лобачевского, 2022. – С. 535-536. – EDN YFVKGA.

10. Зюзин В. Д. Программный комплекс анализа сетевой безопасности в VPN-сети на основе технологии P2P (версия 1.0). Свидетельство о регистрации № 2024610455. Бюллетень № 1. 2024. URL: elibrary.ru/download/elibrary_59916237_58704812.PDF (дата обращения: 10.01.2024).

References

1. Organizatsiya zashchishchennogo obmena dannymi s pomoshchyu virtualnykh chastnykh setey (VPN) [Organization of Secure Data Exchange Using Virtual Private Networks (VPN)]. IBM. URL: ibm.com/docs/ru/i/7.1?topic=options-virtual-private-network-secure-private-communications (accessed: 20.09.2024).
2. Osnovy postroeniya zashchishchennykh komp'yuternykh setey [Fundamentals of Secured Computer Networks]. URL: vec.etu.ru/moodle/pluginfile.php/294002/mod_resource/content/1/Virtualnye%20chastnye%20seti%20prezentatsiya.pdf (accessed: 25.09.2024). P. 1–25.
3. Lektsiya 3: Virtualizatsiya setey [Lecture 3: Network Virtualization]. URL: intuit.ru/studies/courses/2324/624/lecture/13588 (accessed: 30.09.2024).
4. Napolova E. I., Kozhevnikov S. V. Ekonomika i kachestvo sistem svyazi. 2018. No. 2 (8). URL: cyberleninka.ru/article/n/zaschita-kompyuternyh-setey-na-osnove-tehnologii-virtual-private-network/viewer.
5. Roslyakov A.V. Virtualnye chastnye seti. Osnovy postroeniya i primeneniya [Virtual Private Networks: Fundamentals of Construction and Application]. M.: Eko-Trendz, 2006. 597 p.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

6. Omelchenko M. V., Plotnikova K. A., Dyaglev S. P. Innovatsionnaya nauka. 2020. No. 2. P. 27–29.
7. Vasil'ev A. V. Sistemnyi analiz i prikladnaya informatika. 2023. No. 3. — P. 48–54.
8. Ekspertno-Analiticheskiy tsentr InfoWatch. Tendentsii razvitiya kiberintsidentov ASU TP za 2023 god: analiticheskiy otchet [Trends in the Development of Cyber Incidents in ICS for 2023: Analytical Report]. M.: InfoWatch, 2024. 21 p.
9. Zyuzin V. D., Ryabov A. A., Tetyerkin M. A. Trudy XXVI nauchnoy konferentsii po radiofizike, posvyashchennoy 120-letiyu M.T. Grekhovoy : Materialy konferentsii, Nizhniy Novgorod, 12–27 maya 2022 goda. Nizhniy Novgorod: Natsionalny issledovatelsky Nizhegorodsky gosudarstvenny universitet im. N.I. Lobachevskogo, 2022. pp. 535-536. EDN YFVKGA.
10. Zyuzin V. D. Programmnyy kompleks analiza setevoy bezopasnosti v VPN-seti na osnove tekhnologii P2P [Software package for network security analysis in VPN network based on P2P technology] (version 1.0). Certificate of registration No. 2024610455. Bulleten No. 1. 2024. URL: elibrary.ru/download/elibrary_59916237_58704812.PDF (accessed: 10.01.2024).

Дата поступления: 6.11.2024

Дата публикации: 14.12.2024

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024