Проект невидимого интернета i2p

Шубенков Н.А.
Информатика
2 курс, Технический колледж ФГБОУ ВО «Тамбовский государственный технический университет», г. Тамбов, Тамбовской области
Научный руководитель: Мосягина Н.Г., Технический колледж ФГБОУ ВО «Тамбовский государственный технический университет», г. Тамбов, Тамбовской области

Введение. В современном мире очень остро стоит проблема приватной коммуникации. Большинство решений в этой сфере фиктивны и созданы из коммерческого интереса. Всё больше людей, осознав насколько их данные плохо защищены, задаются вопросом: «Как же обезопасить себя от нежелательной утечки личной информации?». Как получить такое очевидное, но труднодоступное право на приватность? Не всё так безысходно, как может показаться - в нашем мире существуют энтузиасты, которые создают проекты, не преследуя злые умыслы, а, наоборот, работая во благо людей.

Цель работы: поиск альтернативы сети Интернет, которая могла бы называться по-настоящему анонимной и свободной.

Задачи:

- исследовать современные сети;
- обеспечивающие приватность информации;
- осуществить обоснованный выбор проекта защищённой сети;
- изучить принцип работы и устройство сети;
- удостовериться в надёжности алгоритмов шифрования и маршрутизации.

Методы исследования: анализ и обобщение специальной литературы, публикаций и интернет изданий, системный анализ, сравнение, типологизация.

Основная часть. Как было сказано выше, множество якобы анонимных проектов созданы исключительно для прибыли, их код закрыт, а лица на которых зарегистрированы юридические организации, занимающиеся разработкой подобного ПО, являются подставными и легко находятся, что противоречит философии кибер-анонимности.

Процесс поиска занял много времени, и в результате было найдено самое оптимальное решение, которое отвечало требованиям — Invisible Internet Project или же I2P.

В 2003 году неизвестный человек под псевдонимом JRANDOM начал разработку будущего свободного Интернета. В этом же году и вышла первая версия Invisible Internet Project. Прошло несколько лет и JRANDOM безвестно покинул разработку, а на его место встал пользователь под никнеймом zzz, который по сей день является курирующей фигурой. Уже больше 10 лет энтузиасты-разработчики созидают и улучшают технологию. [1]

Так что же такое Невидимый Интернет? Это приватная сеть с открытым исходным кодом. Она работает поверх других сетей, например Интернет сети. В отличие от традиционной централизованной сети Интернет, I2P – децентрализованная и одноранговая, а значит, она не зависима от определённых машин в сети. Даже если отключится половина компьютеров, сеть всё равно будет работать, ведь у каждого участника сети равные права и возможности.

Каждая из машин может посылать запросы другим машинам на предоставление каких-либо ресурсов в пределах этой сети и, таким образом, выступать в роли клиента.

Обращая внимание только на эти характеристики, уже можно сделать промежуточный вывод о том, что I2P по умолчанию не может быть полностью подконтрольна одному лицу, ведь над разработкой работало множество свободных людей. Любой желающий может проверить код на наличие «скрытых дверей» или изменить индивидуально под свои нужды. В самой же сети принцип равноправия не позволяет допустить зависимость участников от определённых машин. К слову, рассмотрим, как реализован этот принцип.

Введём два основных понятия: роутер и конечная точка. Роутер – устанавливаемый программный клиент. Посредством клиента производится доступ в сеть. Конечная точка – машина, к которой происходит конечное обращение (пункт назначения).

В I2P для передачи пакетов информации используются туннели. Каждый участник сети строит свои маршруты через другие компьютеры. Эти же участники выступают транзитными узлами для других пользователей. Туннели однонаправленны, передача происходит в одном направлении. Для каждой машины строятся исходящий и входящий туннели. Роутер использует локальную базу сети для построения маршрутов и выбирает самые стабильные и совместимые узлы. Среднее время жизни туннеля – 10 минут. Потом строятся новые туннели. При обращении пользователь не имеет прямого доступа к конечной точке. Имеется лишь информация о её начальном узле во входящем туннеле. Отправитель посылает обращение через свой исходящий туннель во входящий туннель получателя. Как можно понять, чем больше узлов в сети, тем больше туннелей, а значит сеть быстрее работает.

Эта сеть построена так, что невозможно с точностью определить, кто является отправителем, а кто получателем, ведь никто не знает точного расположения друг друга в сети, а потенциальный отправитель может быть обычным транзитным узлом.

Для пересылки пакетов на транспортном уровне используются аналоги TCP и UDP – NTCP2 и SSU соответственно. Эти два протокола отличаются от предков повышенной атакоустойчивосью вследствие сложного шифрования.[1]

Конечно, если сеть претендует на роль анонимной и приватной, то её разработчики должны сделать большой упор на шифрование данных, что и было сделано в рассматриваемом нами случае. Invisible Internet Project использует ассиметричное алгоритмы шифрования, но не в чистом виде, ведь иначе скорость сети заметно снизится. При ассиметричном шифровании применяются два ключа: публичный и приватный. Открытый ключ нужен для шифрования, а закрытый для расшифровки сообщения. В I2P пользователи обмениваются публичными ключами, а далее выводится общий симметричный ключ.

В сети I2P отсутствуют DNS-сервера. Вместо них используют так называемые адресные книги, которые, подобно торренту, постоянно автоматически обновляются у пользователей от других клиентов. Адрес

представляет собой идентификатор, образованный с помощью уникальной хэш-суммы. Для удобства обращения используются короткие псевдодоменные имена. Но знать адрес ресурса для обращения – мало, нужно знать ещё дополнительную информацию, называемую лизсетом(LeaseSet). Лизсет включает в себя полный адрес конечной точки, ключ шифрования и список входящих туннелей.

Предоставляют такую информацию флудфилы – роутеры, собирающие информацию об участниках сети. Обращаясь по адресу, происходит автоматическое обращение к флудфилу для получения лизсета. Флудфилом может стать любой доброволец, правильно настроив роутер.

Когда два пользователя устанавливают соединение, роутеры получают инф-ию о IP-адресах друг друга, но ничего, кроме потенциального использования сети, эта информация не говорит. Вместо IP-адресов в сети используются открытые криптографические ключи, не имеющие никакой логической связи с реальным компьютером.

Для построения туннелей в I2P используется чесночная маршрутизация [2] – технология, зашифрованного обмена информацией. Название говорит само за себя. Перед отправкой создаётся «чеснок», в который закладываются сообщения – «зубчики». Они закладываются совершенно случайно, поэтому порядковый номер не имеет значения. Каждый транзитный узел сверяет идентификатор «зубчика» со своим адресом, остальные же «зубчики» роутер не видит, что предотвращает попытки заполучить информацию об участниках туннеля. После «чеснок» отправляется далее по туннелю.

Если чесночная маршрутизация применяется для построения туннеля, то при передаче сообщения добавляется так же луковичное шифрование – многослойное шифрование симметричным ключом. Проходя по туннелю, транзитные узлы снимают слои шифрования. Когда пакет доходит до последнего узла в исходящем туннеле, тот снимает последний слой и передаёт во входящий туннель. Там сообщение поочерёдно через узлы, которые послойно

зашифровывают «чеснок». Когда сообщение приходит в конечную точку, сообщение расшифровывается ассиметричным ключом.

Может показаться, что сообщение на позиции перехода от исходящего туннеля во входящий совершенно не защищено, но это не так, к сообщению применяется дополнительно сквозное шифрование.

Скачивание установщика клиента I2P производится с официального сайта проекта https://geti2p.net/ru. Перед запуском роутера i2p следует выбрать браузер, через который будет происходить доступ к сайтам сети. В этом браузере требуется настроить прокси. После установки клиента производится запуск роутера. Страницу его настройки открыть нужно в заранее подготовленном браузере. Для корректной работы сети настраиваем роутер и открываем порты TCP и UDP в настройках маршрутизатора. Так, система настроена для работы с сетью I2P. [3]

Проект I2P не ограничивается только одним клиентом. Русский программист под псевдонимом orignal исследовал просторы Интернет-сети и на одном сайте-библиотеке обнаружил, что скачать литературу пользователь может только через I2P. Используя уже имеющийся клиент на Java, orignal не оценил такую реализацию протокола и сам в кратчайшие сроки (3 месяца) написал клиент на C++, назвав проект I2PDeamon или сокращенно i2pd.

I2PD работает значительно быстрее своего прототипа на Java и потребляет меньше ресурсов. Именно этому клиенту многие отдают своё предпочтение.

Для чего нужна сеть I2P? В этой сети, как и в обычной, можно размещать свои веб-сайты, блоги, форумы, делиться гит-репозиториями, общаться с людьми. Конечно, некоторые читатели, возможно, подумали о незаконной деятельности, но поспешу предотвратить возмущения и злые умыслы. Анонимность и приватность требуются далеко не только одним преступникам. У обычных людей так же существует потребность в приватной коммуникации и в анонимном исследовании веб-ресурсов. Многие законопослушные граждане переживают за сохранность своих данных и остерегаются утечки данных

третьим лицам. Поэтому желание человека оставаться анонимным и держать под защитой информацию совершенно естественное.

Вывод. В ходе исследования было установлено что, сети с децентрализованной организацией и одноранговой структурой уступают по скорости традиционным централизованным сетям, но располагают необходимыми технологиями для безопасного пользования. В качестве надёжного инструмента предлагается Internet Invisible Project, который среди конкурентов выделяется оптимальными функциями, принципом работы и открытым исходным кодом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Семенов, Ю.А. Telecommunication technologies-телекоммуникационные технологии: учебное пособие ГНЦ ИТЭФ, 2009. -600с. [Электронный ресурс] – Режим доступа: https://book.itep.ru/6/i2p.htm
2. Туннели I2P: Чесночное шифрование и однонаправленная передача информации -Режим доступа https://hubr.com/ru/post/576094/ (дата обращения 12.04.2022)
3. Маршрутизация сети I2P [Электронный ресурс].-Режим доступа https://hubr.com/ru/post/563958/ (дата обращения 12.04.2022)