Высокоскоростная луковая маршрутизация на сетевом уровне

Калабухов Евгений Романович,
Мустафаев Роман Валех оглы,
Панов Илья Владимирович
Студенты Института инженерной физики и радиоэлектроники СФУ,
Россия, Красноярск,
E-mail: komall@bk.ru

Аннотация

В данной статье представлены различные способы защиты персональных данных, при использовании сети интернет. Рассматриваются принципы устройства и основные аспекты работы HORNET. Предложен оригинальный способ обеспечения конфиденциальности пользовательских данных.

Ключевые слова: масштабируемость, хоп, Tor, криптографический ключ.

Одной из актуальных проблем, с которой сталкиваются люди, использующие глобальную сеть интернет в настоящее время, является низкий уровень конфиденциальности данных пользователей.

Опасность заключается в том, что, раз предоставив информацию, персональные данные пользователь перестает её контролировать. А так называемый «электронный след» оставляемый пользователем в сети несет в себе метаданные, для сохранения и обработки которых не требуется согласие самого пользователя, оставляющего их.

Для защиты от этих и других угроз, касающихся конфиденциальности личности пользователя, и его данных, существуют множество средств. Например, использование (Прокси-серверов; Протокола VPN/SSH; анонимной сети I2P; и др.) [1, с. 6]. Но все перечисленные средства обладают рядом тех или иных серьезных недостатков. Наиболее надежным из уже существующих и используемых средств является Tor (The Onion Router) [2, с. 27].

Структура сети, используемой Tor эффективно справляется с задачей анонимной передачи сообщений. При увеличении же количества абонентов, использующих Tor. Которое за последнее время только увеличивалось. Существенно понижается масштабируемость [3, с. 8].

Очевидно, что обеспечение конфиденциальности личности пользователя – это комплексная задача, решение которой без существенных недостатков до сих пор не найдено [4, с. 6].

Решением поставленной проблемы, без вышеперечисленных недостатков, систем, рассмотренных ранее, может стать система Hornet (High-speed Onion Routing at the Network Layer) [3, с. 10]. Главное преимущество разработки высокая скорость, и крайне низкая вероятность утечки данных, что достигается благодаря архитектуре нового поколения, основанной на уже известном принципе «луковой маршрутизации». Основными задачами проекта приложения для HORNET являются масштабируемость и отказоустойчивость.

Чтобы подключить анонимную передачу данных через Интернет, промежуточные узлы HORNET должны избегать сохранения каждого состояния сеанса (например, криптографические ключи и информацию о маршрутизации). Вместо этого, состояние сеанса выгружается на конечный хост, который затем встраивает это состояние в пакеты так, что каждый промежуточный узел может извлечь свое собственное состояние как часть процесса передачи пакетов.

Выгрузка каждого состояния сеанса представляет две проблемы. Во-первых, узлы должны уберечь свои выгруженные состояния от утечки информации (например, сеансовые криптографические ключи). Для решения этой проблемы, каждый узел HORNET поддерживает локальный секретный ключ для шифрования экспортированного состояния сеанса. Это зашифрованное состояние называется сегментом пересылки (FS). FS позволяет своему генерирующему узлу динамически выгружать интегрированную информацию (т.е. следующий хоп, ключ с общим доступом, время окончания сеанса), скрывая эту информацию от неавторизованных третьих сторон.

Вторая задача при выгрузке каждого состояния сеансам – это объединить данные сеансы (т.е. FS) в пакет таким образом, чтобы каждый узел мог восстанавливать свой собственный FS, без разглашения информации о расположении в сети конечных хостов, длине пути, или расположении отдельных узлов на пути. Изучение данной информации может помочь в деанонимизации атак.

Для решения этой проблемы источник строит анонимный заголовок (AHDR), объединяя множественные FS, и добавляет этот заголовок к каждому пакету сеанса AHDR, предоставляет каждому узлу на пути доступ к FS, созданный им, без разглашения информации о пути, кроме данных о прошлом и следующем узлах. Для эффективной обработки пакета, каждый узел HORNET выполняет одну операцию обмена ключами с использованием протокола Диффи — Хеллмана (ДХ) один раз за сеанс во время установки. Для всех пакетов данных в рамках сеанса, узлы HORNET используют только симметричные шифры для восстановления состояния, обработки AHDR и многослойного дешифрования (или шифрования) полезных данных. Для уменьшения задержки установки, HORNET использует только два пакета установки с одним прохождением сигнала в обоих направлениях между источником и приемником. Вследствие этого, установление сеанса подвергается только O(n) задержке распространения сигнала по сравнению с O(n2) посредством итеративного метода, используемого в Tor (где n является числом анонимных узлов, пройденных на пути). В то время как для Tor значением по умолчанию n является 3, для HORNET n может быть значением вплоть до 14.

Анонимность отправителя. Анонимные сеансы между источником и приемником требуют, чтобы источник установил состояние между самим собой и каждым узлом на пути. Состояние будет переноситься в последующие пакеты с данными, разрешая промежуточным узлам восстанавливать их соответствующее состояние и направлять пакет к следующему хопу. Это состояние используется для передачи пакетов данных.

Этап передачи данных. Собрав FS, источник может теперь построить прямой AHDR и обратный AHDR для прямой и обратной маршрутизации соответственно. AHDR-ы выполняют FS, которые содержат все требуемые состояния узлов для обработки и пересылки пакетов на следующий хоп. При отправке пакета данных, источник зашифровывает свой слой «луковицы» полезных данных, включенных в пакет, используя сеанс симметричных ключей с общим доступом, и добавляет AHDR. Каждый узел после этого извлекает свои FS из AHDR, дешифрует пакет и пересылает его наследующий хоп, до тех пор, пока он не достигнет приемника.

Анонимность Отправителя – Получателя. Анонимность отправителя-получателя, где ни S, ни D не знают расположение друг друга (напр., скрытый сервис), дает новую возможность: если первый пакет потеряется, источник может просто переслать обратно AHDR, используя новый пакет данных. Поскольку S не знает расположение D (и наоборот), S не может восстановить путь к D, исключающий создание состояния между S и узлами на пути к D. Общим подходом к данной проблеме (в соответствии с Tor и LAP) для приемника является объявление пути обратно к себе (или подобного) через «точку встречи» с общим доступом (RP). Источники устанавливают анонимные сеансы RP, которые, в свою очередь, перенаправляют трафик к месту назначения,

сохраняя расположение S и D скрытым друг от друга. Это решение также будет работать для HORNET. Однако, оно требует, чтобы RP поддерживала состояние сеанса между источниками и приемниками, что повышает сложность, ограничивает число получателей, и использует состояние истощения вектора атаки типа «отказ в обслуживании».

Одним из преимуществ схемы, является то, что любой узел в сети может служить точкой встречи. На самом деле, несколько точек могут быть отобраны и объявлены, позволяя источнику выбрать ближайшую к нему RP. Более того, как только сеанс HORNET установлен, S и D могут договориться о лучшей (более близкой) RP (например, использующей скрытое пересечение множеств). Недостатком технологии составного AHDR является то, что он увеличивает вдвое размер заголовка. Для экономии места, детали формального протокола и сектора оценки фокусируются только на анонимности отправителя. Детали анонимности отправителя-получателя содержатся в полном объеме на бумажных носителях [3, с. 63-97].

В данной статье была рассмотрена проблема конфиденциальности данных пользователей в сети интернет, а также предложен новый способ обеспечения конфиденциальности пользовательских данных. Так же были рассмотрены основные принципы устройства и работы сети HORNET. Актуальность затронутых проблем обусловлена масштабным влияния информатизации на все стороны жизни человека. И данное влияние со временем только увеличивается, тем самым повышая требования к информационной безопасности и конфиденциальности данных пользователей сети.

Литература

1. Олифер В., Олифер Н., Компьютерные сети. 4 изд. - СПб.: Петербург, 2015. – 916 с.
2. Damon M., Kevin B. - Shining Light in Dark Places: Understanding the Tor Network. Leuven, Belgium, July 2008, – 15 pp .
3. Chen C., Daniele A., HORNET: High-speed Onion Routing at the Network Layer, 2015, – 14pp.
4. Колисниченко, Д.Н. Анонимность и безопасность в Интернете. - БХВ-Петербург, 2012. – 229 с.