А. В. Гурман

АНОНИМНОСТЬ РАДИ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ АНОНИМАЙЗЕРОВ

Рассматриваются анонимайзеры, особенности передачи информации и уязвимости браузеров.

Введение

Помимо провайдеров, обладающих информацией о всех действиях пользователей их сети, информацию посещений также сохраняют открытые пользователем страницы во время каждой интернет-сессии. Для того чтобы загрузить ресурс необходимо передавать информацию по протоколам передачи информации, обязательное требование которых - знать адреса отправителя и получателя. Таким образом, чтобы скрыть адрес пользователя, который запрашивает или отправляет данные, нужно найти способ подмены настоящего адреса. Но сначала предстоит убедиться, что браузер не сохраняет лишние данные, которые могут раскрыть настоящий адрес.

I. Отпечатки Браузера

Для обеспечения быстрого и удобного доступа к интернет-ресурсам, разработчики пишут код, который опирается на сохранённые в браузере ранее данные сайта или пользователя. Все HTTP-запросы сначала направляются браузером в его кеш, чтобы проверить наличие действительного сохраненного ответа. Если совпадение найдено, ответ считывается из кеша, уменьшая время загрузки сайта и объем скачиваемых данных. Например для того, чтобы определить, надо ли загружать статичный контент, в общении браузера с HTTP-сервером используется ETag. Это контрольная сумма, которая должна меняться вместе с изменением файла. При первой загрузке файла браузер получает ETag. Далее браузер передаёт ETag серверу, и тот проверяет, не поменялась ли контрольная сумма, и следовательно — файл. Таким образом, вместо использования по назначению, веб-сервер может использовать этот ETag как идентификатор пользователя. Чтобы остановить кеширование необходимо в настройках браузера отключить соответствующий флажок и очистить кеш браузера. Также особенно часто используются - Cookies, текстовые файлы с какими-либо значениями, хранимые браузером для разных задач, например, аутентификации. К примеру, если пользователь сначала посетил ресурс из открытого сеанса, браузер сохранил cookies, а потом пользователь соединился из анонимного сеанса, тогда сервер может сопоставить cookies и вычислить пользователя. Также существуют 3rd-party cookies, которые сохраняются после просмотра рекламного баннера с другого сайта (3rd-party). И сайт-владелец этого баннера способен отслеживать пользователя на всех ресурсах, где размещены его баннеры. Cookies также можно запретить в настройках браузера. На сайтах могут встретиться такие плагины, как Flash, Java, Adobe. Эти плагины являются отдельными приложениями, которые запускаются от имени пользователя. Они могут обходить настройки прокси, хранить свои отдельные долгоживущие cookies. Для каждого запуска такого плагина нужно подтверждение пользователя, поэтому следует запрещать запуск в появившемся окне. Также, браузер предоставляет серверу user agent (полная информация о приложении и устройстве). Необходимо изменить в настройках браузера user agent на другое значение.

II. Подмена адреса с помощью анонимайзеров

По причине отсутствия шифрования в прокси-серверах, не стоит рассматривать их как анонимайзеры. Рассмотрим VPN. При подключении к VPN пользователь подключается к другой сети, а она обеспечивает зашифрованное соединение с нужным сервером напрямую. Внутри этой сети существуют свои серверы и выходной узел. Но владельцы VPN могут хранить или продавать данные о пользователях. Рассмотрим TOR. TOR — это система маршрутизаторов, в которой пользователь соединяется с Интернетом через цепочку узлов. Цепочка состоит из трех узлов, каждому из них неизвестны адреса клиента и ресурса одновременно. TOR шифрует сообщения отдельно для каждого узла, а открытый трафик виден только выходному роутеру. Но уже существуют способы перехвата данных направленных к цепочке TOR. Для обеспечения анонимности самым лучшим решением будет включение VPN, а затем TOR. Сторонним лицам виден лишь двойной слой шифрования данных (один от TOR, другой от VPN), а дальше трафик проходит по шифрованной цепочке TOR до адреса назначения. В такой системе трафик нельзя перехватить.

Гурман Артём Витальевич, студент кафедры информационных технологий автоматизированных систем БГУИР, goodjman@outlook.com.

Научный руководитель: Ярмолик Валерий Иванович, ассистент кафедры информационных технологий автоматизированных систем БГУИР, v.jarmolik@bsuir.by.