Принципы анонимности

Ни строчки о себе

Анонимность в Интернете... С этим понятием связано очень много заблуждений. И самое большое из них звучит так: «Мне анонимность не нужна, я не делаю ничего плохого, мне нечего скрывать». Это в корне неверно! Давайте проведем аналогию с реальной жизнью: вам ведь не понравится, если кто-то в окне напротив будет постоянно следить за тем, что вы делаете в своей квартире. Так почему же люди позволяют следить за собой в Интернете?

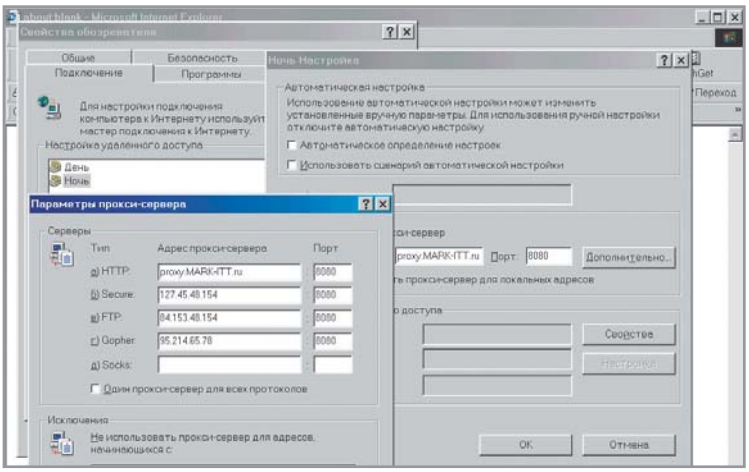
С одной стороны, опасаться за соблюдение анонимности больше всего нужно тем, кто занимается чем-то предосудительным, то есть злыми розыгрышами, хакерством, рассылкой спама и тому подобными вещами. Но и нам, законопослушным «гражданам» Рунета, стоит подумать о себе. Ведь та информация, которую злоумышленник может получить, будет использована против нас. А это может быть, например, массовая рассылка тематической рекламы: согласитесь, можно узнать интересы человека по тому, какие сайты он посещает. Кроме того, существуют сайты, доступные только людям из определенного региона, что, на мой взгляд, является совершенно неправильным. В общем, причин в защиту анонимности можно привести много, но самая главная — безопасность. Помните, что чем меньше злоумышленник знает о вас, тем меньше у него шансов на атаку или обман. Что? Вы называете меня параноиком и не верите, что кто-то может получить информацию о вас? Загляните на сайт www.privacy.net/anonymizer. Там, кроме вашего IP-адреса (о том, что это такое, читайте дальше), вы узнаете свою страну, провайдера, операционную систему, версию браузера и многое другое.

IP-адрес

Думаю, начать лучше с самых азов, а точнее, с IP-адреса. IP-адрес (Internet Protocol address) — это число, которое является идентификатором компьютера в сети. Дли- »

на адреса — 4 байта, для удобства принято его обозначать четырьмя десятичными цифрами от 0 до 255, разделяемыми точками, например, вот так: 217.14.191.17. Думаю, все понимают, что каждый IP-адрес в Сети в данный момент может быть только один. Обратите внимание на словосочетание «в данный момент». То есть в разное время один и тот же IP-адрес может определять разные компьютеры. Здесь все зависит от типа вашего подключения к провайдеру.

Определить IP-адрес человека в Интернете не составляет никакого труда: эта информация передается серверу, дабы последний смог отправить вам запрошенную информацию. А вот узнать по четырем байтам можно многое: например, ваш регион, услугами какого провайдера вы пользуетесь, ну и, естественно, вас. Конечно же, все эти данные не передаются серверу. Но ведь информация о том, какому провайдеру какой IP-адрес «принадлежит», не является секретной. В Интернете существуют специальные службы, называемые whois, для определения пользователя по IP-адресу. «Постойте, — воскликнет нетерпеливый читатель, — но ведь одним и тем же IP-адресом могут пользоваться разные люди, как кто-то может найти меня?» Ответ на этот вопрос очень прост. Неужели вы думаете, что провайдер не записывает, кто, когда и каким IP-адресом пользовался?



Настройка Internet Explorer для работы с прокси-серверами

Прокси-сервер

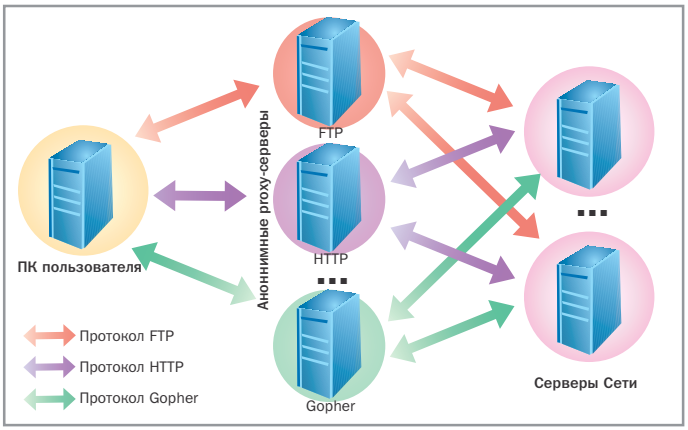
Прокси-сервер — это как бы промежуточный узел, являющийся посредником при работе в Интернете. Он принимает запросы с компьютеров и передает их дальше на нужный узел Сети. Сервер же отправляет данные на прокси-сервер, который затем пересылает их на компьютер пользователя. Такая схема работы помогает решить три различные задачи. Во-первых, использование прокси-сервера позволяет нескольким компьютерам, объединенным в локальную сеть, использовать одно подключение к Интернету. Во-вторых, прокси используется провайдерами для временного хранения информации, что увеличивает скорость работы при модемном подключении. Третье применение прокси-серверов — обеспечение анонимности работы в Сети.

Давайте же разберемся, как прокси-сервер может спрятать человека. Мы теперь знаем, что главный «предатель» — это IP-адрес, необходимый для передачи данных с сервера на компьютер пользователя. Но ведь прокси-сервер сам передает запросы и принимает информацию, то есть он имеет возможность скрыть ПК пользователя. »

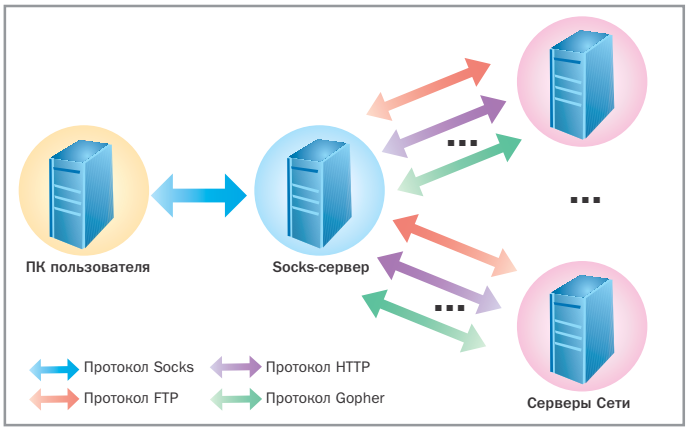
Файлы cookies

Почем печенье для народа?

Мы поговорили об информации, которую браузер пользователя автоматически передает серверу при каждом запросе. Но существуют и более активные способы «слежки». И самый распространенный из них — использование cookies, кстати, с английского это слово переводится как «пирожки» или «печенье». Давайте разбираться, что же это за «пирожки». Итак, cookie — это строка символов длиной не более 4 Кбайт. Соответственно, cookies — это набор таких строк, которые хранятся в специальном файле. Записываются же туда эти данные по запросам различных серверов Интернета. Иными словами, любой сервер может записать какую-либо информацию на ваш жесткий диск, а потом считать ее оттуда. Разработчики, естественно, предполагали вполне мирное использование cookies. Например, при заходе в какой-нибудь интернет-магазин сервер «вспоминает» вас и ваши увлечения и, соответственно, выдает информацию, которая может оказаться интересной. Или другой распространенный случай — форум или гостевая книга, при входе в которую происходит автоматическая авторизация посетителя. Но любую технологию можно использовать как для пользы, так и во вред. Правда, создатели предусмотрели эту ситуацию и попытались защитить пользователя. Для этого они ввели некоторые ограничения. Во-первых, сервер не может записывать в файл более 20 строк, а во-вторых, существует правило, согласно которому считать информацию, записанную определенным сервером, может только он сам. Правда, эти ограничения достаточно просто обойти. Вы же знаете, что практически на любой странице в Интернете можно увидеть баннеры или счетчики посещений (а чаще всего и то и другое), которые всегда загружаются с одного и того же сервера. Ну так скажите, кто же может помешать тому же самому счетчику записывать и считывать данные из cookies? Получается, что у кого-то появляется возможность отследить маршрут вашего серфинга в Сети. А это уже очень важная информация, за которую маркетинговые агентства платят немалые деньги. Тем более что данные о ваших увлечениях часто используются не только для маркетинговых исследований, но и для рассылки непрошенной рекламы (проще говоря, спама). Избавиться от cookies довольно легко. Для этого достаточно залезть в настройки браузера и отключить их. Правда, в этом случае многие сервисы просто-напросто не пустят вас дальше заглавной страницы. Так что лучше использовать более мягкий вариант — разрешить использование временных «пирожков» (это те записи, которые хранятся во время работы, а потом удаляются) или сделать так, чтобы браузер запрашивал у вас разрешение при каждом обращении к файлу с cookies. Правда, второй вариант очень утомителен и вряд ли кому-то понравится.



▲ Схема передачи запросов и данных через анонимные прокси-серверы по наиболее распространенным протоколам



▲ Схема передачи запросов и данных из Интернета на локальный компьютер через socks-сервер

» И вот тут-то нас поджидает подводный камень: подавляющее большинство прокси-серверов не хочет заботиться об анонимности пользователей. В своих запросах они в специальном поле (x-forwarded-for) передают IP-адрес вашего компьютера. Исключения встречаются очень редко, и только они обеспечивают приватность пользователя. Искать анонимные прокси-серверы лучше на специальных сайтах, например на www.proxylist.com. Кстати, на этом сервере вы также сможете проверить любой прокси-сервер на анонимность.

Анонимайзеры

Некоторое время назад в Интернете стали появляться специальные службы — анонимайзеры. Фактически эти сайты являются web-интерфейсами анонимных прокси-серверов. То есть вы заходите на сервер анонимайзера и в специальном поле вводите нужный адрес, через некоторое время загружается запрошенная страничка, при этом можно быть уверенным в своей приватности. Вроде бы все здорово, но на самом деле у анонимайзеров есть несколько существенных недостатков.

Во-первых, анонимайзер существенно замедляет скорость загрузки страниц. Второй недостаток этих несомненно полезных сервисов — небесплатность. Да, совсем недавно услуги всех анонимайзеров были абсолютно бесплатны. Но сейчас все изменилось. Теперь бесплатны только «молодые» анонимайзеры, находящиеся на стадии раскрутки, но даже и эти сервисы пытаются заработать и поэтому показывают баннеры своим пользователям. Либо они имеют ограничения доступа ко многим наиболее популярным сайтам.

И все-таки, несмотря на свои недостатки, в некоторых случаях анонимайзеры могут существенно помочь пользователям. Знаете ли вы, что делать, если работаете в локальной сети, а злой администратор перекрыл доступ к некоторым очень важным сайтам? Единственный выход в этом случае (если не считать ящик пива для администратора) — анонимайзер. Именно этот сервис поможет вам «обмануть» сервер сети и получить доступ к заблокированным сайтам.

Socks-протоколы

В принципе, socks-протокол очень похож на прокси-сервер: он принимает информацию и передает ее дальше «от себя», скрывая тем самым реальный адрес компьютера пользователя. Причем передача IP-адреса не предусмотрена даже в принципе. Фактически вы просто соединяетесь с socks-сервером по своему собственному протоколу, а дальше он уже передает данные по общепринятым протоколам (HTTP, FTP и т. п.), но уже от своего имени. В результате мы можем не беспокоиться о настройке каждой отдельной программы и поиске анонимного прокси-сервера для каждого протокола. Еще один большой плюс рассматриваемой технологии — это то, что socks-сервер никак не изменяет полученную информацию, в отличие от прокси-серверов, он просто передает ее.

Последние советы

Напоследок хочу ответить на самый распространенный вопрос, волнующий многих российских пользователей Интернета. Оказывается, за рубежом существует большое количество форумов, конференций и различных клубов, куда не хотят принимать наших сограждан. Как исправить столь вопиющую несправедливость? Во-первых, вам придется отказаться от русифицированной версии Windows и перейти на стандартную английскую. Это касается и браузера. Почему, думаю всем понятно — эта информация не относится к секретной, а американец, пользующийся русифицированным ПО, вызывает серьезные подозрения. Далее нужно перевести часы примерно «по-американски» (или куда вы там хотите попасть), а также найти и использовать анонимный прокси-сервер или socks-сервер, располагающийся в выбранной стране. Теперь вы можете быть более-менее уверены в том, что никто не догадается, где вы живете. Надеюсь, что вы не используете мои советы в неблаговидных целях.

■ ■ ■ Марат Давлетханов

Ссылки по теме

- **http://www.all-nettools.com** — сайт с огромным количеством наиболее полезных интернет-сервисов с web-интерфейсом

Популярные интернет-анонимайзеры:
- **http://anonymouse.ws/anonwww.html**
- **http://www.safeproxy.org/cgi-bin/nph-proxy.cgi**
- **http://www.anonymizer.com**
- **http://www-new.the-cloak.com/anonymous-surfing-home.html**

WHOIS-ресурсы:
- **http://www.internic.net/whois.html** — сервер whois, также позволяет проверять домены
- **ftp://sipb.mit.edu/pub/whois** — большой список whois-серверов