КАК ВЕСТИ БЛОГ **АНОНИМНО**

Этан Цукерман (Ethan Zuckerman)

Предлагаемое краткое техническое руководство по анонимному ведению блога предназначено для активных критиков властей в странах с далеко не прозрачным правительством. Оно - не для киберпанков, а для граждан развивающихся стран, которые стремятся обеспечить свою безопасность и неприкосновенность частной жизни.
В пособии «Как вести блог, не подвергаясь опасности», подготовленном Electronic Frontier Foundation (http://www.eff.org/Privacy/Anonymity/blog-anonymously.php), также можно найти ряд очень полезных советов.

СОДЕРЖАНИЕ

Знакомство с Сарой
Шаг 1 - Псевдонимы
Шаг 2 – Общедоступные компьютеры
Шаг 3 – Анонимные proxy-серверы
Шаг 4 – Раскрыть имя
Шаг 5 – Луковичная маршрутизация (onion routing) через Tor
Шаг 6 - MixMaster, Invisiblog и GPG
Степень анонимности

ЗНАКОМСТВО С САРОЙ

Сара работает бухгалтером в правительственном учреждении. Она узнает, что ее начальник, заместитель министра, присваивает государственные деньги. Она хочет, чтобы мир узнал о преступлении, но боится потерять работу. Если она сообщит о преступлении министру (в случае, если удастся добиться встречи), ее могут уволить. Она звонит репортеру местной газеты, но та отвечает, что для статьи нужно гораздо больше информации, а также документы, подтверждающие подозрения.

Поэтому Сара решает начать веблог, чтобы рассказать о махинациях в министерстве. Чтобы защитить себя, она должна быть уверена, что никто не узнает об авторе заметок в блоге. Поэтому она может вести блог только анонимно.

Существует два способ выяснить, кто ведет анонимный блог. Во-первых, это можно понять из заметок. Например, если она напишет «я являюсь помощником главного бухгалтера в аппарате заместителя министра угольной промышленности», читатель довольно легко может установить ее имя.

Второй способ – это возможность установить личность Сары на основании информации, сообщаемой web-браузерами и почтовыми программами. Каждый компьютер, подключенный к интернет, имеет IP адрес – серию из пяти цифр от 0-255, разделенных точками. Например, 213.24.124.38. Когда Сара использует web-броузер для размещения заметки, IP адрес включается в текст заметки.

Немного поработав, министерские компьютерщики смогут найти Сару по IP адресу. Сара может использовать домашний компьютер, связываясь с провайдером (ISP) с помощью модема. Но каждый провайдер фиксирует IP адрес и номер телефона пользователя. В одних странах министру потребуется специальное разрешение для получение этой информации, в других (прежде всего, в тех, где доступ в интернет предоставляется государственными компаниями), провайдеры спокойно предоставят эту информацию, и Сара может оказаться в скверной ситуации.

Однако существует ряд способов сохранить анонимность при использовании интернет. Чем в большей безопасности хочет оказаться человек, тем больше работы ему придется проделать. Сара, как и любой другой человек, который хочет вести анонимный блог, должна решить, до какой степени сильна ее паранойя, и сколько усилий она в состоянии потратить на то, чтобы ее не нашли. Как вы узнаете, некоторые стратегии требуют солидных технических знаний и большой работы.

ШАГ 1- ПСЕВДОНИМЫ

Самый простой способ обеспечит анонимность - использовать бесплатную интернет почту и бесплатную блоговую платформу за пределами страны. (Использовать платные сервисы не следует, поскольку по номеру счета или кредитной карты можно установить имя пользователя). Однако Сара может пользоваться псевдонимом. Тогда, найдя ее блог, министр обнаружит, что он принадлежит "A. N. Ymous", а электронный адрес автора блога - anonymous.whistleblower@hotmail.com.

Вот список некотрых провайдеров бесплатных почтовых услуг:

Hotmail
Yahoo
Hushmail - бесплатная почта
с хорошей криптографической защитой

Вот некоторые провайдеры бесплатного хостинга для блогов:

Blogsome - free WordPress blogs
Blogger
Seo Blog

Однако здесь существует одна проблема. Когда Сара подписывается на бесплатную услугу, вебсервер регистрирует ее IP адрес. В этом случае, ее можно найти, если она

пользуется компьютером дома или на работе и если компания, предоставляющая услуги почты и блоггинга, сообщит требуемую информацию. Не так-то просто заставить компании, предоставляющие данные услуги, предоставить такие сведения. Например, чтобы Hotmail сообщил IP адрес Сары, необходимо особое предписание или специальное решение судебных органов США. Но Сара не хочет рисковать в случае, если ее правительство сможет убедить компании сообщить ее IP адрес.

ШАГ 2 – ОБЩЕДОСТУПНЫЕ КОМПЬЮТЕРЫ

Для того, чтобы остаться неузнанной, Сара может использовать компьютеры, которые доступны многим людям. Зарегистрировать свою почту и блог она может при помощи компьютера в интернет-кафе, библиотеке или университетской компьютерной лаборатории. Если министр обнаруживает IP адрес отправителя заметок или комментариев, он видит что сообщения посланы из интернет-кафе, где за компьютером работали сотни людей.

У этой стратегии также есть слабые места. Если в кафе или лаборатории можно установить, кто пользовался компьютером в определенное время, Сару легко найдут. Она не должна отправлять сообщения поздно вечером, когда в лаборатории кроме нее никого нет, поскольку лаборант обязательно ее запомнит. Кроме того, ей все время нужно будет работать в разных интернет-кафе. Если министр обнаружит, что все сообщения были посланы из кафе "Joe's Beer and Bits" на Главной улице, он может приказать установить слежку и легко найти Сару.

ШАГ 3 – АНОНИМНЫЕ PROXY-СЕРВЕРЫ

Саре надоело ходить в интернет-кафе каждый раз, когда нужно отправить сообщение. С помощью соседа-компьютерщика она получила доступ к анонимному proxy-серверу с домашнего компьютера. Пользуясь почтой или платформой для блоггинга, она оставляет IP адрес прокси-сервера, а не адрес домашнего компьютера... теперь министру очень трудно найти ее.
Во-первых, она находит в Google список proxy-серверов по ключевым словам "proxy server". Она выбирает из списка publicproxyservers.com серверы с пометкой "high anonymity", она выписывает адрес proxy и порта.

Вот несколько надежных списков proxy-серверов:
• publicproxyservers.com - анонимные и не-анонимные proxy;
• Samair (http://www.samair.ru/proxy/) - только анонимные прокси, дает информацию о прокси-серверах, которые поддерживают SSL;
• rosinstrument proxy database (http://tools.rosinstrument.com/proxy/) - поиск по базе данных proxy-серверов.

Затем она переходит в раздел "preferences". В разделах «general", "network" или "security", она устанавливает необходимые опции для интернет - доступа через proxy-сервер. (В браузере Firefox эта опция - в разделах Preferences - General - Connection Settings). Она переходит к ручной настройке proxy, вводит IP адрес proxy-сервера, переносит

в поля HTTP proxy и SSL proxy и сохраняет параметры. Она перезагружает браузер и начинает работу в интернет.
Она замечает, что скорость несколько уменьшилась. Это из-за того, что каждая страница, которую она запрашивает, загружается обходным путем. Вместо прямого соединения с hotmail.com, она сначала связывается с proxy-сервером, который, в свою очередь, связывается с Hotmail. Пакет с Hotmail также идет сначала на proxy-сервер, а потом к Саре. Она также отмечает, что возникли задержки при доступе к вебсайтам, особенно к тем, которые требуют регистрации. Но зато ее IP адрес неизвестен провайдеру.

Можно провести с proxy-серверами следующий эксперимент. Зайдите на oreply.org, популярный римейлер (remailer). Вы увидите приветствие со своим IP адресом: "Hello pool-151-203-182-212.wma.east.verizon.net 151.203.182.212, pleased to meet you." А теперь посмотрите anonymizer.com, который позволяет видет некоторые вебстраницы через анонимный proxy. В правое верхнее окно страницы анонимайзера введите URL для http://www.noreply.org (или просто щелкните ссылку http://anon.free.anonymizer.com/; http://www.noreply.org). Вы увидите, что noreply.org теперь считает, что вы пришли с vortex.anonymizer.com (анонимайзер – хороший способ проверить proxy, не изменяя установок браузера, однако этот инструмент не работает с webmail или weblogging серверами).
Наконец, следуя инструкциям, настройте свой web-браузер на работу с анонимным proxy и зайдите на noreply.org, чтобы проверить, определяет ли он ваш IP. Увы, proxy также несовершенны. Если Сара живет в стране, где интернет фильтруется, многие пользователи будут работать с proxy-серверами, чтобы получить доступ к заблокированным сайтам. Правительство, в свою очередь, будет блокировать популярные proxy. Пользователи будут переходить на другие, правительство блокирует и их – и так по кругу. Все это будет отнимать достаточно много времени.

Сара столкнется с проблемами и в том случае, если она – одна из немногих, кто пользуется услугами proxy-серверов. Если заметки на ее блог пересылает один и тот же proxy-сервер, и если министр может потребовать регистрационные записи (logs) у любого провайдера, он может увидеть, что компьютер Сары – один из немногих, имеющих доступ к этому серверу. Он не сможет доказать, что Сара использовала proxy именно для разрешения заметок на блоге. Но он может придти к выводу, что поскольку блог анонимный, а Сара – одна из немногих в стране, кто пользуется доступом к proxy–серверам, значит, именно она отправляла заметки. Поэтому Саре лучше использовать популярные в стране proxy и часто менять их.

ШАГ 4 - РАСКРЫТЬ ИМЯ

Сара начинает думать о том, что владелец proxy-сервера, который она использует, пойдет на компромисс. Что если министр убедит оператора proxy сервера (силой закона или посредством взятки, фиксировать, кто из граждан его страны пользуется

услугами сервера и какие сайты эти люди посещают). Сара надеется, что администратор proxy -сервера защитит ее, но она даже не знает этого администратора. Кроме того, даже если администратор не интересуется подобными вещами, proxy-серверы могут оказаться открытыми.
У Сары есть друзья в Канаде (а в этой стране интернет не подвергается такой цензуре, как у нее на родине), которые могут помогать ей вести блог, сохраняя анонимность. Сара звонит другу и просит установить у себя систему обхода интернет-фильтров (circumventor) – один из десятков proxy-серверов, который пользователь может установить сам, что позволяет другим использовать его компьютер как proxy-сервер.

Джим, друг Сары, загружает circumventor (систему обхода), выложенную на сайте Peacefire.org (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html) и устанавливает его. Это не просто, так как сначала надо установить Perl, затем OpenSA и только после этого – саму систему (circumventor). Кроме того, его компьютер должен быть постоянно подключен к интернет, чтобы Саре не нужно было просить его подключиться каждый раз, когда она посылает заметки. Он устанавливает программное обеспечение, звонит Саре по мобильному телефону и сообщает URL , чтобы Сара могла иметь интернет-доступ через его прокси-серврер или для того, чтобы размещать заметки на блоге. Это особенно удобно, поскольку Сара может использовать proxy-сервер как дома, так и в интернет-кафе.

Хотя Джим очень помогает Саре, существует все же одна серьезная проблема. Джим работает с Windows , поэтому компьютер часто приходится перегружать. Каждый раз, когда это происходит, провайдер присваивает машине новый IP адрес. При этом Сара теряет доступ к серверу. Джим должен снова связаться с Сарой и сообщить новый адрес. Это неудобно и дорого. Сару также беспокоит то, что, если она использует один и тот же IP адрес достаточно длительное время, ее провайдер может под давлением правительства блокировать этот адрес.

ШАГ 5 - ЛУКОВИЧНАЯ МАРШРУТИЗАЦИЯ (ONION ROUTING) И TOR

Джим предлагает Саре поэкспериментировать с Tor. Это относительно новая система, обеспечивающая достаточно хорошую защиту анонимности в интернет. «Луковичная» маршрутизация (onion routing) развивает идею proxy-серверов – компьютеров, которые действуют от вашего имени. Каждый запрос, сделанный через этот маршрутизатор, проходит через ряд дополнительных компьютеров – от 2 до 20. Это практически исключает возможность определения, с какого компьютера был послан запрос.
Каждый шаг в цепочке зашифрован, что также усложняет для правительства процесс установления личности Сары. Более того, каждый компьютер в цепочке знает только ближайших соседей. Другим словами, маршрутизатор B знает, что запрос на вебстраницу пришел от маршрутизатора A и что необходимо передать этот запрос маршрутизатору C. Но сам запрос зашифрован – маршрутизатор B на самом деле не знает, какую страницу запрашивает Сара или какой маршрутизатор завершает цепочку.

Несмотря на сложность технологии, Сара приятно удивлена легкостью установки Tor (http://tor.eff.org/cvs/tor/doc/tor-doc-win32.html) и системы «луковичной маршрутизации» (onion routing). Она загружает программу установки, которая инсталлирует Tor, затем скачивает и устанавливает Privoxy, прокси, работающий с Tor. Кроме того, она получает дополнительные преимущества, так как со страниц, которые она запрашивает, автоматически убирается реклама.

После установки программного обеспечения и перезагрузки компьютера, Сара заходит на noreply.org и узнает, что она надежно защищена программой Tor - noreply.org считает, что запрос пришел из Гарвардского университета. Она делает вторую попытку, noreply показывает запрос из Германии. Так она узнает, что Tor меняет адрес для каждого запроса, что позволяет ей сохранять анонимность.
Однако это имеет некоторые неприятные последствия. При доступе к Google через Tor, переключается язык – английский, японский, датский, голландский – все в течении нескольких минут. Сара рада возможности изучать новые языки, но есть и другие неприятности. Саре нравится писать для Wikipedia, но она обнаруживает, что Wikipedia блокирует ее попытки редактировать статьи, используя Tor.

Tor также не лишен некоторых недостатков других proxy. Tor несколько уменьшает скорость, так что она использует его только в случае необходимости послать заметку на блог или просмотреть запрещенный сайт. Кроме того, она привязана к домашнему компьютеру.
Однако больше всего ее беспокоит то, что иногда Tor не работает. Очевидно, ее провайдер блокирует некоторые маршрутизаторы «луковицы»: когда Tor пытается связаться с блокированным маршрутизатором, после нескольких минут ожидания страница так и не открывается.

ШАГ 6 - MIXMASTER, INVISIBLOG И GPG

Однако существуют возможности решения нашей проблемы и без использования proxy-серверов, даже таких сложных, как Tor.
Из разговоров с местными компьютерщиками, она находит новое решение: Invisiblog (http://www.invisiblog.com/). Сайт поддерживается анонимно группой австралийцев, называющих себя vigilant.tv. Это сайт создан настоящими параноиками для параноиков. Это почта специального формата, которая посылается через римейлерную систему (remailer) MixMaster, имеющая криптографическую подпись.
Чтобы понять последнее предложение, Саре понадобилось немало времени. В конце концов, она установила GPG (http://www.gnupg.org/) – систему шифровки с открытым ключом (public-key encryption: http://en.wikipedia.org/wiki/Public-key_cryptography).
Кратко это можно описать следующим образом: система шифровки с открытым ключом позволяет посылать сообщения, которые может прочитать только адресат. При этом адресат не сообщает свой ключ, так что вы не можете читать письма его корреспондентов. Кроме того, данная система позволяет «подписывать» сообщения, так что их практически невозможно подделать. Таким образом, если посылать

сообщения на блог с такой подписью, блог сможет проверять, действительно ли данное сообщение отправлено Сарой (см. также главу «Как обеспечить тайну переписки?»).

Затем она устанавливает MixMaster, почтовую систему, созданную для того, чтобы скрывать происхождение электронного сообщения. MixMaster использует систему анонимных римейлеров – компьютерные программы, которые убирают всю информацию о происхождении электронного сообщения и отправляют его по назначению. Сообщение, прошедшее через 2-20 римейлеров, очень трудно трассировать, даже если один из римейлеров сохраняет информацию об отправителе. Для создания MixMaster необходимо менять исходники, что, конечно, не сделаешь без помощи компьютерщиков.
Она посылает первое MixMaster сообщение, содержащее открытый ключ, на Invisiblog. Invisiblog использует его, чтобы установить новый блог с замечательным названием "invisiblog.com/ac4589d7001ac238", включающее последние 16 байтов ее GPG-ключа. Последующие сообщения, подписанные отрытым ключом, она посылает на Invisiblog через MixMaster.

При этом скорость также замедляется. Поскольку мейлеры MixMaster перенаправляют сообщения, это может отнять от двух часов до двух дней. И она должна очень осторожно приходить на свой блог. Если она будет делать это часто и ее IP адрес будет часто протоколироваться блогом, можно будет догадаться, что именно она и является автором. Однако ее может успокоить тот факт, что владельцы Invisiblog не имеют ни малейшего представления о том, кто она такая.
Основная проблема Invisiblog заключается в том, что система чрезвычайно сложна для пользователей. Для многих довольно трудно установить GPG и понять все тонкости открытых и закрытых ключей. Даже системы криптографии, созданные для обычного пользователя, например, Ciphire, не так уж просты. В результате, очень немногие - даже среди тех, кому это действительно нужно – используют шифрование в электронной переписке.

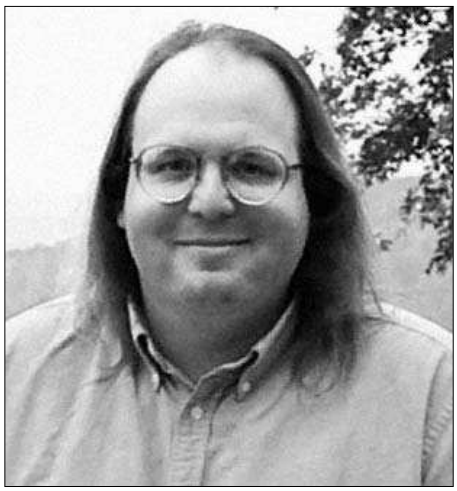
MixMaster – это технически сложная система. Пользователи Windows могут обратиться к ранним DOS-версиям программы, которые доступны на http://prdownloads.sourceforge.net/mixmaer/mix204b46.zip&download. Правда, когда я тестировал ее, она не стала работать... или моя почта все ходила взад-вперед между римейлерами. Все, кто хочет использовать более новые версии или установить программу на Linux или Mac, должны писать программы сами, а это умеют далеко не все опытные пользователи. Возможно Invisiblog станет более доступным, если будет принимать сообщения римейлеров доступных через веб, например riot.eu.org. Но пока вряд ли он сможет помочь тем, кто действительно в нем нуждается.

В странах с репрессивными режимами существуют и другие проблемы с шифрованием. Например, если компьютер Сары будет конфискован и ее ключ станет известен, это даст доказательство того, что Сара является автором подрывного

блога. А в странах, где шифрование не слишком популярно, уже сам факт отправления сообщения через MixMaster, где оно тщательно шифруется, может быть достаточным для того, чтобы ее деятельность привлекла пристальное внимание властей.

СТЕПЕНЬ АНОНИМНОСТИ

Подходит ли вам решение Сары – обучиться криптографии, программированию и использовать MixMaster? А может быть комбинации шагов 1-5 достаточно, чтобы вести блог анонимно? На эти вопросы нет единственно правильного ответа. При принятии решения всегда необходимо учитывать местные условия, уровень своей технической подготовленности и степень паранойи. Если вы считаете, что ведение блога рискованно и если вы сможете установить Tor, это очень хорошее решение.



И помните: не следует подписывать заметки блога своим настоящим именем!

Этан Цукерман, сотрудник Центра «Интернет и общество» Гарвардской юридической школы. Тема его исследований - отношения между гражданской журналистикой и традиционными медиа, главным образом, в развивающихся странах. Он основал и некоторое время возглавлял Geekcorps, некоммерческую организацию, проводившую тренинги в развивающихся странах. Этан Цукерман также один из основателей хостинговой компании Tripod.

KAMUNIKAT.org