Wild Bee

Original reporting

- home
- archives
- about

← Carrying Gunpowder through Airport Security

Internet Volunteers Outmaneuver Dictators

January 22nd, 2010 | Open source software, Privacy

by Rhona Mahony. Google revealed last week that network intruders have read email messages in the Google accounts of Chinese human rights activists. Someone–still unknown–is determined to spy on Chinese dissidents. Other someones are determined to identify undercover police officers, ferret out employees who secretly inform the police about their company's crimes, and stalk their own wives who have left home to escape battering. Hundreds of volunteers are now running an Internet service for people who need to protect their privacy.  The service is called Tor, the Onion Router. Anyone can provide Tor, for free. Anyone can use Tor to protect his privacy, for free.

Bill McGonigle, of Lebanon, New Hampshire, decided to become a Tor volunteer when he learned that people in Iran were protesting the results of their June Presidential election. They were using the Internet to organize their meetings. The Iranian government was trying to censor their messages to one another. "I have a soft-spot for people trying to gain liberty for themselves," he wrote in an email, "especially against tyrannical regimes. It became known that they were using Tor to get around the censorship, so at that point I put up a relay….The people I'd like to help are those living under violence-based oppression, most commonly orchestrated by dangerous and corrupt individuals posing as legitimate governments. I'd like to see an end to oppression wherever it exists."

Get Tor

To become a volunteer, download this software.
To use Tor to protect your own privacy, download this software

How It Works

How Tor works is complicated. It uses fancy cryptography, which is difficult mathematics. It uses technical features of the Internet, which is difficult network engineering. The good news is that neither Tor volunteers nor Tor users need to know any of the hard stuff. Curious readers may enjoy technical explanations by the Tor Project programmers and classroom slides, written by Dan

Boneh, a computer science professor at Stanford University specializing in cryptography. The inventors of the original Onion Router have published many papers, as has the team now working on Tor.

To get started, a volunteer–for example, Bill McGonigle in New Hampshire–downloads a software program from the Tor Project, based in Massachusetts, that lets him share a small fraction of his broadband Internet connection with people who use Tor. He chooses how much bandwidth he will set aside for Tor users. It can be as little as 20 kilobits per second, a small fraction of a 1.5 megabyte connection. The person who wants privacy, let's say Abigail, downloads a small program that adds a Tor button to her Firefox Web browser. When Abigail clicks on her Tor button, Tor encrypts the message that Firefox sends out, passes that message along three or more randomly-chosen volunteers' computers, which may include Bill's, and then connects her to the Web site she wants. Tor then encrypts and bounces the messages along the same path from the destination Web site back to Abigail. Each computer on the path know only which computer preceded it and to which computer it must relay the message. After a short time, Abigail's Tor chooses a new, random path among volunteers' computers for her messages to follow. The result: Abigail is using the Web anonymously. Companies, government agencies, and spies have a very hard time figuring out where Abigail is, what site she is visiting, what she is writing or learning, and, if they are monitoring the destination Web site, who is visiting it. Right now, volunteers worldwide are offering Tor on 1755 computers.

China Plays Cat, Tor Plays Mouse, or Is It the Other Way Around?

Zhan Bin, who teaches at the Business School of the Beijing Institute of Fashion Technology, has written forcefully in his blog in favor of more openness and freedom in China.

In a recent email, he said that he uses Tor every day to read Internet sites, because the Chinese government has blocked so many. If Tor became unavailable to him, he would immediately search for a substitute. At the moment, though, there is no substitute that is as secure or useful as Tor. Tor

encrypts people's messages, unlike most other proxy services. It then passes the messages through a far-flung network of computers not controlled by any single group. It also works with different kinds of Internet communication, such as instant messaging. Because the program is open source, any programmer can build it into his software.

On September 25, 2009, the Chinese government did its best to blockade Tor, possibly in preparation for China's National Day on October 1. The Tor Project had, from its beginning in 2006, published a list of volunteers' computers' IP addresses on several Web sites. The government employees who run China's Internet gateway simply looked up the Web site and added those publicly-listed Tor IP addresses to the long list of IP addresses whose messages could not enter China. Two days later, 80 percent of those relays were still blocked. The number of Tor relays inside China that could contact the outside world had fallen from over 60–before the blockade–to zero.

By January 5, 2010, though, Zhan Bin and many other Chinese were once again able to use Tor. The number of connections from China had recovered to roughly 40,000 per hour, about half the pre-blockade number. What happened? As Andrew Lewman, the Executive Director of the Tor Project, explained in a telephone call, he and his colleagues had long anticipated and prepared for China's blockade. Many volunteers had set up secret relays, which were not listed on the public

Web sites. Those secret relays are called bridges. On September 25, Lewman and his colleagues faced a challenge right out of a spy novel. How could they communicate the bridges' secret IP addresses to people far away–and unknown to them–without the Chinese government intercepting the list? The solution: a widely distributed dribble. The Tor Project is releasing the list of bridges, a few at a time. They are using many methods: word of mouth, email, Twitter, other new social media, and Web sites. They reveal no more than one-eighth of the list by any one method. The Chinese government will intercept, and then block, some of the IP address, but not all.

This pouncing and parrying is a game of cat and mouse. Right now, though, Andrew Lewman, Karen Reilly, and the other staff members at Tor do not feel like mice. They say that they are confident that they can continue to move people's words and photos in and out of China. What they need, they say, is more volunteers to run bridges.

Does the Chinese government feel like the mouse in this game? Half of the Tor Project's $514,000 annual funding comes from the U.S. government, through the International Broadcasting Bureau, an independent agency that runs radio transmissions for the Voice of America, Radio Free Europe, and Radio Free Asia. Ken Berman, the IBB's head of engineering, sought out Tor, according to Lewman, because he wanted to support new Internet software that circumvented censorship.

Paul Syverson, co-inventor of the original Onion Router, worked and still works in the cryptographic laboratory of the U.S. Navy. In other words, he makes codes for the U.S. Defense Department. As in

a delicious paradox common to logic puzzles, after inventing the Onion Router, Syverson told his Navy bosses that the Onion Router could keep the Navy's secrets secret only if the Navy gave away the Onion Router.

Paul Syverson

Why? Only when people sending messages through the Onion Router network are indistiguishable from average Internet users, can hostile observers not tell which messages to capture and inspect. The more numerous, varied, and ordinary Onion Router users become, the more they camouflage one another. In this way, sharks can hide among minnows.

Today, because Navy officials did–maybe to their dismay–understand the unforgiving logic of espionage–anyone can read the Onion Router source code and contribute to it. It is a civilian project–the Tor Project–and a non-profit organization.

Roger Dingledine and Nick Mathewson, computer scientists trained at MIT, do most of the research and programming to improve Tor. They are idealistic fellows. They say in their mission statement, "…for human rights workers, journalists, democracy activists and many others world-wide, anonymity online can be an issue of life and livelihood. The Tor Project believes that we should have the same expectation of privacy online as we have in the real world…."

Roger Dingledine

Nick Mathewson

Yet, how does Tor look to the Chinese government, or to the government of Iran, Syria, or even Russia? Or to zealous nationalists of those countries? They may look over the shoulders of Dingledine and Mathewson. They may see the propaganda arm and war machine of the West.

Ordinary People Help One Another

In so-called open societies, though, people see the issue differently. Most Westerners disdain censorship. The Tor button for Firefox has been downloaded three million times. Lots of those freeloading downloaders–the ones with a broadband Internet connection–could also be offering the Tor service. A remaining question: do home computer users have permission to run an Internet

server program that gives services to people outside their house? The answer is: maybe.

The Acceptable Use Policy of many Internet Service Providers–such as Verizon and Earthlink–explicitly prohibits residential customers from running any Internet server program. AT&T and Comcast's iBurst do not. To check any company's policy, type its name and "AUP" into a search engine.

What are the prohibitive ISPs worried about? That a customer will run an enterprise using most of the contracted bandwidth round-the-clock. That traffic could strain the ISP's gear, hurt service to other customers, and get the ISP sued. By prohibiting all server programs, the company saves its employees the work of researching each customer's case.

A little arithmetic shows how harmless and costless to her ISP Abigail actually will be if she offers Tor to the world, instead of merely using it herself. Let's say that she has a 1 MB broadband connection. She considers setting aside a maximum at any given time of 20 kilobits per second for a Tor bridge, since bridges are now needed most urgently. A bit is one-eighth of a byte. A kilobyte is one-thousandth of a megabyte. Abigail, at maximum burst, will have 1/400th of her broadband connection busy with Tor users. She is paying $50 per month. She will have to decide for herself what her conscience permits. Then she can help her grandchildren set up Tor on their computers.

A person who sets up a Tor relay gets to give it a name. Bill McGonigle, the man in Lebanon, New Hampshire, who was moved by the Iranian election protesters, also admires John Lennon's music. He calls his relay, "imagineallthepeople."

Legal guidance for people running Tor relays in the United States
Video of a talk by Roger Dingledine

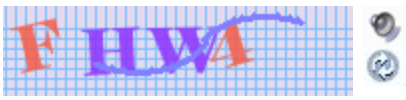
0 comments ↓

Leave a Comment

Name

Mail

Website



CAPTCHA Code

Submit

- **Search**

To search, type and hit ente

Copyblogger design by Chris Pearson