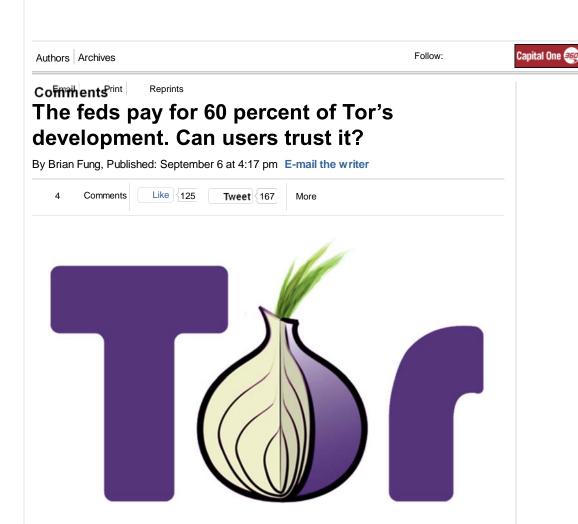
PostTV Politics

Opinions Local Sports National World Business Tech Lifestyle Entertainment Jobs More

Search The Washington Post





This week, we learned that the NSA had managed to circumvent much of the encryption that secures online financial transactions and other activities we take for granted on the Internet. How? By inserting backdoors into the very commercial software designed to keep sensitive medical records, bank files and other information private.

The NSA's sustained attempt to get around encryption calls into question many of the technologies people have come to rely on to avoid surveillance. One indispensable tool is Tor, the anonymizing service that takes a user's Internet traffic and spits it out from some other place on the Web so that its origin is obscured.

So far there's no hard evidence that the government has compromised the anonymity of Tor traffic. But some on a Tor-related e-mail list recently pointed out that a substantial chunk of the Tor Project's 2012 operating budget came from the Department of Defense, which houses the NSA.

Federal Grantor/Pass-Through Grantor/Program Title	Federal CFDA Number	Award Number	Federal Expenditures
Major Program:			
U.S. Department of Defense			
Pass-Through from SRI International Basic and Applied Research and Development in			
Areas Relating to the Navy Command, Control,			
Communications, Computers, Intelligence,			
Surveillance, and Reconnaissance	12.335	N66001-11-C-4022	\$ 876,099

(The Tor Project)

Last year, DoD funding accounted for more than 40 percent of the Tor Project's \$2 million budget. Other major donors include the U.S. State Department, which has an interest in promoting Internet freedom globally, and the National Science Foundation. Add up all those sources, and the government covers 60 percent of the costs of Tor's development.

Tor Executive Director Andrew Lewman wrote in an e-mail to users that just because the project accepts federal funding does not mean it collaborated with the NSA to unmask people's online identities.

"The parts of the U.S. and Swedish governments that fund us through contracts want to see strong privacy and anonymity exist on the Internet in the future," Lewman wrote. "Don't assume that 'the government' is one coherent entity with one mindset."

And Roger Dingledine, a founder of the Tor Project, says that the Defense Department money is much more like a research grant than a procurement contract.

"They aren't 'buying products' from us,"
Dingledine tells me. "They're funding
general research and development on
better anonymity, better performance
and scalability and better blocking-

resistance. Everything we do we publish in the open."

Dingledine acknowledges that "bad guys" could conceivably introduce vulnerabilities into Tor's open-source code. But one of the major advantages of open-source software is that the product can be inspected by anyone for defects, which raises its security somewhat. There'd only be a problem if the NSA were somehow able to insert malicious code that nobody recognized.

The NSA didn't immediately respond to a request for comment Friday afternoon.

Update: Roger Dingledine writes in to explain why the government has never asked the Tor Project to install a backdoor:

I think this is mainly due to two reasons:

A) We've had that faq entry up for a long time, including the part where we say we'll fight it and that we have lots of lawyers who will help us fight it. So they know it won't be easy.

B) I do a lot of outreach to various law enforcement groups to try to teach them how Tor works and why they need it to be safe. See e.g. the first two paragraphs of this:

I think 'A' used to be a sufficient reason by itself, but now we're reading about more and more companies and services that have tried to fight such a request and given up. The architecture of the Tor network makes it more complex (there's no easy place in the deployed network to stick a backdoor), but that doesn't mean they won't try.

I guess we rely on 'B' for now, and see how things go.



Brian Fung covers technology for The Washington Post, focusing on electronic privacy, national security, digital politics and the Internet that binds it all together. He was previously the technology correspondent for National Journal and an associate editor at the Atlantic. His writing has also appeared in Foreign Policy, Talking Points Memo, the American Prospect and Nonprofit Quarterly.

« PREVIOUS NEXT »

These NASA superfans won a chance to watch a rocket take off for the moon By Andrea Peterson September 6, 2013

I'm going to watch a rocket take off tonight. Here's how you can, too. By Andrea Peterson September 6, 2013

4

Comment

Discussion Policy | FAQ | About Discussions

Type your comment here

Sort: Newest First

Comments Live



mhenridav wrote:

5:49 AM EST

Given the record of the US and Swedish governments with respect to snooping on all available traffic, the fact that these entities are important sources of funding for Tor must give us all pause....

Henri

Like • Reply • Share • Report Abuse



Winston_Smith_II wrote:

2:24 AM EST

Follow the money.

Like Liked by 1 reader • Reply • Share • Report Abuse



I used to be an avid Tor user. However, years ago there were a number of papers and presentations that focused on breaking Tor's anonymity, and more recently, on breaking the keys. I would suspect that for the U.S., or other governments with significant IT resources, the idea of needing a backdoor is just an unnecessary waste of time and risk of public ire. If they can identify and control the networks where the exit nodes exist or break the cryptographic keys, Tor's value becomes diminished. Of course, we would be none the wiser...which is exactly what some governments would want. Here are a couple of URLs from different years discussing weaknesses from different perspectives:

http://www.csnc.ch/misc/files/publications/the_oni... http://arstechnica.com/security/2013/09/majority-o...

Like Liked by 1 reader • Reply • Share • Report Abuse



DonKiyoti responds:

12:12 AM EST

I would think that while NSA may be able to decrypt traffic between endpoints and/or Tor proxy relays, they cannot in general associate traffic with an individual except by obtaining all associated proxy relay logs as well as PPP session logs from the individuals ISP.

IF everybody obeys the rules, a court order would be required for NSA to obtain that information. I would hope that even the FISA kangaroo court would reject a request for such an order unless it was supported by some real indication of terrorist intent in the decrypted traffic.

Like . Report Abuse

Add your thoughts...

Politics Opinions Local Sports National World Business Tech Lifestyle Entertainment Photo Video Blogs Classifieds

More ways to get us

Home delivery Mobile & Apps RSS Facebook

Post Store Twitter e-Replica Social Reader Archive

Contact Us

Reader Representative Careers Digital Advertising Newspaper Advertising

News Service & Syndicate

Help & Contact Info

About Us

Guidelines

The Washington Post Company In the community **PostPoints** Newspaper in Education Digital Publishing

Partners

washingtonpost.com

© 1996-2013 The Washington Post Terms of Service Privacy Policy Submissions and Discussion Policy RSS Terms of Service

Ad Choices

Newsletter & Alerts

Washington Post Live

Reprints & Permissions