

The Switch

Where technology and policy connect



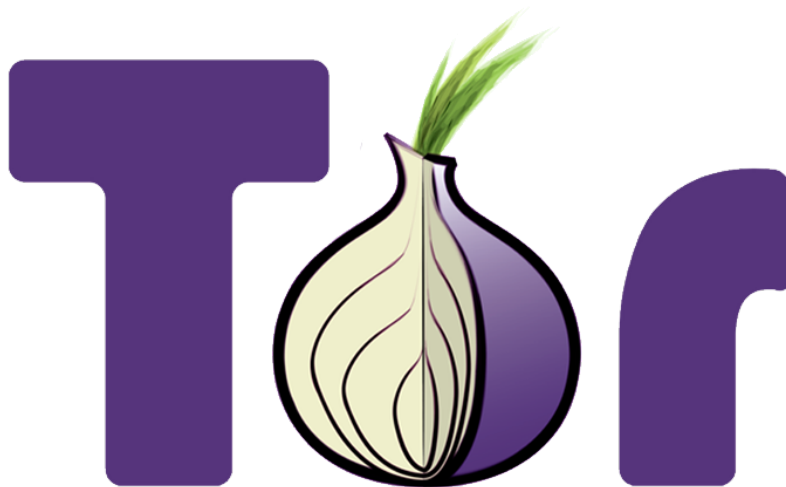
ArkeFly Voordelige retourtickets naar ruim 70 bestemmingen! Boek nu



Comments

The feds pay for 60 percent of Tor's development. Can users trust it?

By Brian Fung, Published: September 6 at 4:17 pm [E-mail the writer](#)



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
Total Major Program			<u>876,099</u>

(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

13

Comment

[Discussion Policy](#) | [FAQ](#) | [About Discussions](#)

Type your comment here

Sort: **Newest First** [Comments Live](#)



Roy Lawson wrote:
7:55 PM EDT

I'm not sure where the TOR project lives, but most open source projects utilize check-ins and it is quite easy not only to see the source but more importantly identify changes and who made them over time.

I would suggest analysis of all check-ins. Look for users who have relatively few changes to source control, or changes that don't appear to relate to what their comments are. My guess is that the top contributors won't have introduced back doors because it would be quite a conspiracy if they did. Unless they were bought off or blackmailed, but that seems like a remote possibility.

Personally I think any open source security project should require code reviews prior to acceptance by randomly assigned contributors. The chances that more than a couple are involved would probably be slim.

Like . Reply . Share . Report Abuse

SiIver1ock wrote:



9/7/2013 12:57 PM EDT

A back door into Visual Studio would really annoy. It means you have a tap on most commercial software development. Visual Studio is known to be "leaky." Whether that translates into an NSA back-door is unknown.

Like · Reply · Share · Report Abuse



ontheotherhand... wrote:

9/7/2013 7:55 AM EDT

Unfortunately, looks like another rotten apple.

There's no way, NO WAY I can believe the US military will give out millions of dollars to tech business without stings attached. NO WAY.

It's very unfortunate this report. Big Brother can't be defeated unless there is an uprising. Otherwise, BB will simply, left unchecked, fortify itself and adjust, like all viruses, to the new conditions.

Our government is, truly, a fascist state. We have to take it from there.

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



spankyfrost responds:

9/7/2013 10:09 AM EDT

Exactly! The Pentagon isn't in the business to give out hundreds of thousands with a label called grant.. ahhhahhhh! Anyone that believes that can take off your tin-foil hat now and live with it!

But this is just another reason I don't mess with TOR. I prefer other VPN not related to the US! And that is hard to find... but there are a still a few.

Like Liked by 1 reader · Report Abuse



knettles responds:

9/7/2013 1:04 PM EDT

the DOD funds many things as research grants, such as the CDMRP, which funds cancer research. There are is no insidious plot behind their funding cancer research. They were appropriated funds by congress to do so, so they do.

Like · Report Abuse



gudguy1 responds:

11:49 AM EDT

I agree with this comment:

"There's no way, NO WAY I can believe the US military will give out millions of dollars to tech business without stings attached. NO WAY."

Not many deep pockets simply hand out grants without gaining something in return... And I really do not believe this is a case of charity for improving the 'Net for all...

Like · Report Abuse

Add your thoughts...



mhenriday wrote:

9/7/2013 5:49 AM EDT

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 Liked by 2 readers · Reply · Share · Report Abuse



Winston_Smith_II wrote:

9/7/2013 2:24 AM EDT

Follow the money.

Like Liked by 2 readers · Reply · Share · Report Abuse



bocam48 wrote:

9/6/2013 9:21 PM EDT

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 2 readers · Reply · Share · Report Abuse



DonKiyoti responds:

9/7/2013 12:12 AM EDT

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



hedonistbot responds:

9/7/2013 8:30 AM EDT

Using TOR is a clear sign of a terrorist or at least criminal intent. Why else would you be anonymous on the internet or use encryption? (Irony alert!)

Like · Report Abuse



spankyfrost responds:

9/7/2013 10:11 AM EDT

Please type your bank account, access code and password please. Hurry up! You have nothing to hide IDIOT!

Like Liked by 1 reader · Report Abuse



IAF101 responds:

9/7/2013 12:27 PM EDT

The only truly "safe" place that is relatively un-hackable/crackable is inside your brain - though some would argue even your "thoughts" can be monitored given the right tools.

Like · Report Abuse

Add your thoughts...

Classifieds

[More ways to get us](#)

[Home delivery](#)
[Mobile & Apps](#)
[RSS](#)
[Facebook](#)
[Twitter](#)
[Social Reader](#)

[Newsletter & Alerts](#)
[Washington Post Live](#)
[Reprints & Permissions](#)
[Post Store](#)
[e-Replica](#)
[Archive](#)

[Contact Us](#)

[Help & Contact Info](#)
[Reader Representative](#)
[Careers](#)
[Digital Advertising](#)
[Newspaper Advertising](#)
[News Service & Syndicate](#)

[About Us](#)

[The Washington Post Company](#)
[In the community](#)
[PostPoints](#)
[Newspaper in Education](#)
[Digital Publishing Guidelines](#)

[Partners](#)

washingtonpost.com

© 1996-2013 The Washington Post [Terms of Service](#) [Privacy Policy](#) [Submissions and Discussion Policy](#)
[RSS](#) [Terms of Service](#) [Ad Choices](#)