The Tor Project: Applying Censorship Resistance Research to the Field

3rd QUARTER OF PROJECT, Q2 OF THE YEAR: APRIL 1 2015 – JUNE 30 2015

Project Overview

Part one: Pluggable transport integration

Part two: Testing and network simulation improvements

Part three: Enhanced outreach

Foreign Assistance Framework: Internet Freedom Specific Indicators:

Q2 Project Timeline (April 1, 2015 – June 30, 2015) – Activity Summary

Pluggable transport integration

Project Objectives:

Outputs for the Quarter:
Outcomes:

Challenges:

Successes:

Testing and network simulation improvements

Project Objectives:

Outputs for the Quarter:

Outcomes:

Challenges:

Successes:

Enhanced outreach

Project Objectives:

Outputs for the Quarter:

Outcomes:

Challenges:

Successes:

Press:

Next Quarter’s Planned Activities:

Pluggable Transport Integration

Testing and network simulation improvements

Enhanced Outreach

Project Overview

The project contains three main activities:
Part one: Pluggable transport integration

Tor will work to safely deploy transport technology to resist censorship, especially censorship based on deep packet inspection. This will be achieved by working with researchers to improve the usability, portability, security and code maintainability for transports; integrating mature transports into experimental bundles for real users and feeding those results into further improvements; and improving and maintaining the application programming interface between Tor and the pluggable transport layer.

Part two: Testing and network simulation improvements

Tor will improve the correctness and stability of the core Tor software by streamlining and automating the process of launching a complete test; designing and scripting an automated test suite to exercise and stress as much of Tor's functionality as possible; and extending Tor's controller interface to allow better monitoring.

Part three: Enhanced outreach

To increase awareness and improve the sustainability of the Tor technology and research, Tor will develop dynamic messaging and targeted campaigns aimed at end users and volunteers. Tor will identify partner organizations for outreach activities, including diaspora populations from countries with low press freedom rankings, open source development groups, and NGOs supporting civil society.
Foreign Assistance Framework: Internet Freedom Specific Indicators:

a. Number of unique users of circumvention technology or secure communication technology (measured monthly):

The Tor network had between 1.9 and 2.5 million daily users that were able to connect directly to the network without having to circumvent censorship. In addition to these, there were around 20,000 daily users that had to use Tor bridges as entry point into the Tor network, most likely because their Internet provider would otherwise prevent them from connecting.

![Bridge users graph](https://metrics.torproject.org/)

The anomalous spike in bridge users visible in this graph was investigated¹ and determined to be the result of statistics briefly reported by a single bridge relay that are unlikely to reflect actual usage. An issue has been filed to ensure such anomalies are accounted for in future metrics reporting.

On the graph below you can see the total number of users of any pluggable transport to access the network. You will notice a slight growth towards the end of the quarter. Please ignore the part missing for May, which was due to a technical problem rather than the real pattern of usage.

---

¹ [https://trac.torproject.org/projects/tor/ticket/16555](https://trac.torproject.org/projects/tor/ticket/16555)
One thing we would like to highlight here is the increased usage of meek, the pluggable transport based on domain-fronting: as you can observe in the graph below, usage doubled over the quarter. We attribute this to our work on improving its performance. The spike in April was a novelty effect due to our public announcement of our performance improvements in Tor Weekly News:

---

b. Number of civil society actors trained in circumvention or digital safety techniques:

Result: 1200 civil society actors trained in circumvention or digital safety techniques:

<table>
<thead>
<tr>
<th>Actors trained</th>
<th>Country</th>
<th>Event and/or partner organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>United States</td>
<td>18F/U.S. Digital Services/Presidential Innovation Fellows</td>
</tr>
<tr>
<td>50</td>
<td>United States</td>
<td>Sam Houston State University</td>
</tr>
<tr>
<td>65</td>
<td>United States</td>
<td>Mattapoissett Library, Massachusetts</td>
</tr>
<tr>
<td>45</td>
<td>United States</td>
<td>CUNY graduate center</td>
</tr>
<tr>
<td>65</td>
<td>United States</td>
<td>Bard College</td>
</tr>
<tr>
<td>110</td>
<td>United States</td>
<td>NJ Library Association Conference</td>
</tr>
<tr>
<td>40</td>
<td>United States</td>
<td>Connecticut Library Association Conference</td>
</tr>
<tr>
<td>45</td>
<td>United States</td>
<td>Massachusetts Library Association Conference</td>
</tr>
<tr>
<td>100</td>
<td>United States</td>
<td>LACUNY conference</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>45</td>
<td>United States</td>
<td>Bedford Library, Massachusetts</td>
</tr>
<tr>
<td>60</td>
<td>Australia</td>
<td>New South Wales library conference (online)</td>
</tr>
<tr>
<td>80</td>
<td>United States</td>
<td>NNYLN meeting, NY State</td>
</tr>
<tr>
<td>25</td>
<td>United States</td>
<td>Westford Library, MA</td>
</tr>
<tr>
<td>20</td>
<td>United States</td>
<td>Kilton Library, NH</td>
</tr>
<tr>
<td>50</td>
<td>United States</td>
<td>Cannabis Society, MA</td>
</tr>
<tr>
<td>70</td>
<td>United States</td>
<td>Rhode Island Library Association Conference</td>
</tr>
<tr>
<td>15</td>
<td>United States</td>
<td>Minuteman Library Network, Natick MA</td>
</tr>
<tr>
<td>100</td>
<td>United States</td>
<td>Philly Keyspots/Free Library of Philadelphia</td>
</tr>
<tr>
<td>100</td>
<td>United States</td>
<td>Digital Rights in Libraries (LFP Conference)</td>
</tr>
<tr>
<td>35</td>
<td>France</td>
<td>Free public training on Internet privacy, Paris</td>
</tr>
<tr>
<td>20</td>
<td>France</td>
<td>Free public training on Internet privacy, Nancy</td>
</tr>
<tr>
<td>20</td>
<td>France</td>
<td>Free public training on Internet privacy, Rennes</td>
</tr>
</tbody>
</table>

c. Number of USG-supported online tools developed or improved to maintain an open Internet:

**Results:**

- **Highlights for Pluggable Transport (PT) development:**
  - Preliminary review of:
    - Dust2 Pluggable Transport
  - Fixed a big performance limitation in the meek-azure\(^3\) transport tripling its bandwidth usage.
  - obfs4 use is still on an upswing, it's now the 3rd most popular pluggable transport, after obfs3 and meek.
- **Highlights for Testing improvements:**
  - Unit test coverage is now at 37%

---

\(^3\) [https://lists.torproject.org/pipermail/tor-dev/2015-April/008637.html](https://lists.torproject.org/pipermail/tor-dev/2015-April/008637.html)
d. Number of individuals or organizations operating in Internet-repressive countries that are provided with technical assistance to increase online security:

**Result:** No in-person trainings were carried out during this quarter, but the Tor Help Desk continued to provide individual technical assistance to users in Internet-repressive countries including Iran and China.

e. USG-assisted campaigns and programs to enhance public understanding, NGO support and media coverage of digital threats and promotion of an open Internet:

**Result:** The following is a summary of our four main outreach efforts, for which more information can be found in the body of this report:

- Direct work with organizations:
  - Contributions to the UN report on freedom of expression;
  - Collaboration with Amnesty International to help them add Tor to their staff curriculum;
  - Global Voices blogger training;
  - Survey for trainers to help build a guide for them.
- Outreach materials
  - Creation of the Community team (to help expand outreach initiatives)
  - Revamp of the T-shirts program, distributing free shirts to individuals who have made a contribution to Tor’s work.
- Social Media:
  - Verification of Twitter account
  - Fast response to current events
  - Live tweeting of events
- Media Support:
  - Proactively pitching media
  - Dealing quickly with "attack" media requests--Starting big media list of researchers to help triage and vet attacks
  - Blogged about our funding rationale in “How We Work”

---

4 https://blog.torproject.org/blog/how-we-work
f. Number of times USG-supported analytic reports are cited by national and international media outlets:

**Result:** The metrics published by the Tor Project help illustrate stories about the impact of censorship circumvention tools. They also help provide educational information about the Tor network and services (i.e. Hidden Services, Pluggable Transports, etc.).

It is difficult to keep count of all the articles in which our metrics are cited, but below is a selection of articles that highlights how the most-used metrics are cited in the media.

<table>
<thead>
<tr>
<th>Title</th>
<th>Media outlet</th>
<th>Metric cited</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tor Use in Russia Spiking in Response to Kremlin's Censorship Efforts⁵</td>
<td>Global Voices</td>
<td>Direct connected users from Russia</td>
<td>June</td>
</tr>
<tr>
<td>The state of encryption tools, 2 years after Snowden leaks⁶</td>
<td>Daily Dot</td>
<td>Total users direct connected to the network and total network bandwidth</td>
<td>June</td>
</tr>
<tr>
<td>How the Tor Project is bringing anonymity back to the web⁷</td>
<td>First Post</td>
<td>Total users direct connected to the network</td>
<td>May</td>
</tr>
<tr>
<td>Tor Hidden Services And Drug Markets Are Under Attack, But Help Is On The Way⁸</td>
<td>Forbes</td>
<td>Estimation of total Hidden Services in the network</td>
<td>April</td>
</tr>
</tbody>
</table>

g. Number of times USG-supported analytic reports are discussed in established social media sites:

**Result:**

Our metrics are discussed on social media with direct links to our websites or stories published in media outlets about them. With hundreds of millions of users potentially seeing our posts, it is hard to measure the total number of these mentions and their reach (total number of impressions).

---

⁵ https://globalvoicesonline.org/2015/06/02/tor-use-in-russia-spiking-in-response-to-kremlins-censorship-effort
⁶ https://www.dailydot.com/politics/encryption-since-snowden-trending-up/
A search for keywords such as “#Tor, usage, metrics” on Twitter\(^9\) provides us with some examples of these conversations in social media.

We also promote our metrics through our Twitter account. For the Q2 2015 period, one of our top Tweets\(^10\) was about our network bubble graph\(^11\) (127 engagements).

Q2 Project Timeline (April 1, 2015 - June 30, 2015) - Activity Summary

Pluggable transport integration

Project Objectives:

The idea is to separate Tor’s anonymity and privacy properties from its censorship-resistance properties: The core Tor software focuses on building Tor circuits and getting the multi-layer encryption right, while the transport layer focuses on preventing an attacker from recognizing or blocking the client’s connections to the rest of the Tor network. This modular approach lets us

---

\(^9\) [https://twitter.com/search?q=tor%2C%20metrics%2C%20usage%23tor&src=typd](https://twitter.com/search?q=tor%2C%20metrics%2C%20usage%23tor&src=typd)

\(^10\) [https://twitter.com/torproject/status/588445797206753281](https://twitter.com/torproject/status/588445797206753281)

\(^11\) [https://metrics.torproject.org/bubbles.html#country](https://metrics.torproject.org/bubbles.html#country)
“plug in” new transports as needed — and since the transport layer is a separate program, it can be written in whatever rapid prototyping language is most convenient, allowing Tor to adapt much more quickly to a censor’s new Deep Packet Inspection (DPI) tactics without needing to touch the core Tor program at all.

Outputs for the Quarter:

Task 1 (SponsorT, aka the work we did via the Internews contract): Write the initial evaluation (to be continually revised) of existing and soon-to-be-deployed transports following the evaluation criteria set out in the proposal.

We started our preliminary evaluation\(^\text{12}\) of Dust2 using the older attached list of criteria\(^\text{13}\) for questions we can begin answering. The code in general appears to be of high quality, and it will not take long for us to be comfortable merging it into obfs4proxy from an “implementation quality” perspective. Our recommendations for further development are as follows:

- Figure out how to offer bridge packages in Debian, ideally without adding more work for the volunteer packager. Debian requires each dependency to have a separate package, and if we merge the obfs4proxy component of the code as is, this will mean the Debian packager needs to create two additional packages (one if we rip out the go-logging code).
- Create a Dust repo under git.torproject.org/pluggable-transports.
- Rip out the “go-logging” code. We have some ideas on how to do this without making the rest of Dust2 depend on obfs4proxy.
- Add code to write a bridge line to a file. Most people do not/should not have logging enabled. They need to be able to get at the bridge line.
- We are not thrilled about including dchests’s skein code as is in the Dust2 repo. Look into using other primitives, preferably from the standard library or golang.org/x/crypto.
- Write some benchmarking to get a rough idea of how expensive the mimicry/statistical transform step actually is.
- We are somewhat hesitant to recommend Dust2 for deployment at this point, as some of the issues raised in our preliminary evaluation may suggest. This is not a code quality issue, but more of a series of design-related ones. Specifically:
  - No adversaries we are aware of use statistical attacks. Instead they rely on various form of blacklisting, or protocol whitelists. Everywhere Dust2 will work, scramblesuit/obfs4 should work as well.
  - The mimicry offered is not good enough to get past DPI that is actually protocol-aware, only statistical tests (by design). We expect Dead Parrot + follow-up probing style attacks to be able to trivially break Dust2, despite the shared secret in the bridge line, because error behavior will fail to match. We don’t therefore see this buying anything

\(^{12}\) Dust2TransportPreliminaryEvaluation.pdf
\(^{13}\)PluggableTransportEvaluationCriteria.pdf
over FTE with improved regexes. The same argument applies to FTE. The regexes aren’t great, and there are trivial distinguishers that can identify FTE traffic with <1 KiB of initial data. The point of FTE is that it’s easy to write new regexes, but so far no one has done this, and thus it doesn’t have a huge userbase. We are open to being convinced otherwise on this matter.

- Who is going to continue to improve/maintain Dust2 models? Documentation on how to generate them/write them didn’t appear to be in the code drop, and versioning here will rapidly become nightmarish since there is no negotiation mechanism.

We have also been participating in research into the evaluation of obfuscation tools.

- Last year we met and worked with researchers from the University of Berkeley, once in October and again in November. These hours of brainstorming contributed to the “Censorship Arms Race: Research vs. Practice” paper\(^\text{14}\) presented this year at HotPETs\(^\text{15}\). Part of that paper aims to answer the question of what we should look for in a pluggable transport design. We will continue to work with this research group, and anticipate that this work and follow-on work will improve our evaluation criteria document for Pluggable Transports.

- Also back in November 2014 we worked with a team of researchers from University of Berkeley, led by professor Vern Paxson\(^\text{16}\), on a proposal to NSF to fund further research on what properties of pluggable transports make them more or less successful. They were going to do the research side, and we were going to do the deployment and transition-to-practice side. In May 2015, we learned that the main research grant will be funded, but unfortunately our deployment side will not. Even so, we still plan to collaborate with them, and it’s great that they have funding to be able to focus on the topic.

**Task 2 (SponsorS, aka this direct contract):** Maintain and extend obfsproxy, obfs4proxy, obfsclient and other Pluggable Transport codebases as needed, and assist developers and researchers who wish to use our frameworks to do relevant research.

---


\(^\text{15}\) [https://petsymposium.org/2015/hotpets.php](https://petsymposium.org/2015/hotpets.php)

\(^\text{16}\) [http://www.eecs.berkeley.edu/Faculty/Homepages/paxson.html](http://www.eecs.berkeley.edu/Faculty/Homepages/paxson.html)
• obfs4\textsuperscript{17} use is still on an upswing after the Tor Browser team included it in their 4.5 stable release (more below). It is now the third most popular pluggable transport, after obfs3 and meek.

![Bridge users using transport obfs4](https://metrics.torproject.org/)

• Another important piece of work we would like to mention was our move to Golang. The PT work used to be done in Python, which was very impractical to support on Android. Having the code in Golang makes this possible\textsuperscript{18}, and we now have the full obfs4proxy and meek codebases written in Go. Google should soon add support for x86 and mips processors to Golang, allowing us to expand Android support beyond ARM chips.

• meek-azure has shown a great increase in usage following the resolution of a performance issue, making the connection much faster. You can see the bandwidth increase\textsuperscript{19} on the graph below:

\textsuperscript{17} https://metrics.torproject.org/userstats-bridge-transport.html?graph=userstats-bridge-transport&start=2015-04-01&end=2015-06-31&transport=obfs4
\textsuperscript{18} https://lists.mayfirst.org/pipermail/guardian-dev/2015-April/004316.html
\textsuperscript{19} https://globe.torproject.org/#/bridge/AA033EEB61601B2B7312D89B62AAA23DC3ED8A34
<table>
<thead>
<tr>
<th>Periods</th>
<th>3 days</th>
<th>1 week</th>
<th>1 month</th>
<th>1 months</th>
<th>1 year</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bandwidth</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mean written bytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 469.67 kB/s</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mean read bytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 511.17 kB/s</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

And the usage increase here:

![Bridge users using transport meek](https://metrics.torproject.org/)

Below is a quote from the costs summary report for April\(^2^0\) that gives more insight into the spike we see for April.

“The number of simultaneous users increased hugely in April, from 2000 to around 5000. There are big increases around April 9 and April 15, which I conjecture were caused by a performance improvement in meek-azure\(^2^1\) and its coverage in TWN\(^2^2\) (Tor Weekly News). meek-azure used to be hugely bottlenecked, but now it should handle as many users as the others.”


Here's the summary of meek's CDN fees for April 2015.

<table>
<thead>
<tr>
<th>Month</th>
<th>App Engine +</th>
<th>Amazon +</th>
<th>Azure = total by month</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2014</td>
<td>$0.09</td>
<td>-</td>
<td>$0.09</td>
</tr>
<tr>
<td>March 2014</td>
<td>$0.00</td>
<td>-</td>
<td>$0.00</td>
</tr>
<tr>
<td>April 2014</td>
<td>$0.73</td>
<td>-</td>
<td>$0.73</td>
</tr>
<tr>
<td>May 2014</td>
<td>$0.69</td>
<td>-</td>
<td>$0.69</td>
</tr>
<tr>
<td>June 2014</td>
<td>$0.65</td>
<td>-</td>
<td>$0.65</td>
</tr>
<tr>
<td>July 2014</td>
<td>$0.56</td>
<td>$0.00</td>
<td>$0.56</td>
</tr>
<tr>
<td>August 2014</td>
<td>$1.56</td>
<td>$3.10</td>
<td>$4.66</td>
</tr>
<tr>
<td>September 2014</td>
<td>$4.02</td>
<td>$4.59</td>
<td>$8.61</td>
</tr>
<tr>
<td>October 2014</td>
<td>$40.85</td>
<td>$130.29</td>
<td>$171.14</td>
</tr>
<tr>
<td>November 2014</td>
<td>$224.67</td>
<td>$362.60</td>
<td>$587.27</td>
</tr>
<tr>
<td>December 2014</td>
<td>$326.81</td>
<td>$417.31</td>
<td>$744.12</td>
</tr>
<tr>
<td>January 2015</td>
<td>$464.37</td>
<td>$669.62</td>
<td>$1133.99</td>
</tr>
<tr>
<td>February 2015</td>
<td>$650.53</td>
<td>$604.83</td>
<td>$1255.36</td>
</tr>
<tr>
<td>March 2015</td>
<td>$690.29</td>
<td>$815.66</td>
<td>$1505.97</td>
</tr>
<tr>
<td>April 2015</td>
<td>$886.43</td>
<td>$785.37</td>
<td>$1671.80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$3292.25 + $3792.79 + $0.00 = $7085.04 grand total</td>
</tr>
</tbody>
</table>

Another result of our collaboration with research teams was the work we did last year with researchers from Stony Brook University. Their poster\textsuperscript{23}, which is partly a result of our discussions with them, was accepted to IEEE Security & Privacy for May 2015\textsuperscript{24}. It presents a very interesting approach to circumvention, explained more fully in the following quote:

In this poster, we argue that multi-player games as a covert channel presents a solution that can tip the scales heavily in the favor of circumvention tool developers. The large number of games and common features of games within a given genre facilitate adaptation of existing game-based covert channels to new games. Further, security features of games and their ability to leverage either a central server or peer-to-peer architecture significantly raise the bar for censors that aim to detect and block covert channels. Finally, as we will demonstrate with our prototype (named Castle), game-based covert channels can be designed such that they match the three properties highlighted by Geddes et al.

Task 3 (SponsorS): Tor side pluggable transport-related (and other) improvements.

- Below are some extracts from our software changelogs showing relevant improvements to our Tor and Tor Browser codebases.
  - Core Tor: Changes related to pluggable transports in version 0.2.7.1-alpha\textsuperscript{25}:

\textsuperscript{23} \url{http://nrg.cs.stonybrook.edu/wp-content/uploads/2015/04/sp-abstract.pdf}
\textsuperscript{24} \url{http://www.ieee-security.org/TC/SP2015/program-posters.html}
\textsuperscript{25} \url{https://blog.torproject.org/blog/tor-0271-alpha-released}
- When launching managed pluggable transports on Linux systems, attempt to have the kernel deliver a SIGTERM on tor exit if the pluggable transport process is still running. Resolves ticket 15471\textsuperscript{26}.
- When launching managed pluggable transports, setup a valid open stdin in the child process that can be used to detect if tor has terminated. The "TOR_PT_EXIT_ON_STDIN_CLOSE" environment variable can be used by implementations to detect this new behavior. Resolves ticket 15435\textsuperscript{27}.

This specific feature was very important for meek, as it is actually meek-client that drives the pluggable transport negotiation with tor. This change inside Tor simplified things a lot for meek to interact with Tor\textsuperscript{28}.

- **Tor Browser Alpha: Changes related to pluggable transports in version 5.0a3 alpha release:**
  - Update meek to 0.2
  - Update Tor Launcher to 0.2.6.7
    - Bug 15145: Visually distinguish “proxy” and “bridge” screens.
  - Bug 13247: Fix meek profile error after browser restarts
  - Bug 16446: Update FTE bridge #1 fingerprint

- **Tor Browser Stable: 4.5.1**
  - The 4.5 series\textsuperscript{29} also features a rewrite of the obfs2, obfs3, and ScrambleSuit transports in GoLang, as well as the introduction of the new obfs4 transport. The obfs4 transport provides additional DPI and probing resistance features which prevent automated scanning for Tor bridges. As long as they are not discovered via other mechanisms, fresh obfs4 bridge addresses will work in China today. Additionally, barring new attacks, private obfs4 addresses should continue to work indefinitely.
  - Bug 15872: Fix meek pluggable transport startup issue with Windows 7

- During the recent Privacy-Enhancing Technologies Symposium\textsuperscript{30}, the University of Berkeley published a paper describing a study they will coordinate with the participation of the Tor Project, focused on the usability of pluggable transports in combination with Tor Browser, “an essential facet for adoption and use”: “We focus our analysis on the

\textsuperscript{26} [Link](https://trac.torproject.org/projects/tor/ticket/15471)
\textsuperscript{27} [Link](https://trac.torproject.org/projects/tor/ticket/15435)
\textsuperscript{28} [Link](https://gitweb.torproject.org/pluggable-transport/meek.git/diff/?id=0.17&id2=0.16)
\textsuperscript{29} [Link](https://blog.torproject.org/blog/tor-browser-45-released)
\textsuperscript{30} [Link](https://petsymposium.org/2015/hotpets.php)
connection configuration dialog of Tor Browser, as censorship circumvention requires correct transport configurations."

Task 4 (SponsorS): Pluggable transport R&D (Catchall)

- We worked with an undergraduate student under Prof. Nick Feamster\(^\text{31}\) at Princeton University who looked at a DNS-based Pluggable Transport as a semester project (experimental, not deployable).
- We have continued talking with Kevin Dyer\(^\text{32}\), who has an upcoming Usenix Security paper called “Marionette”\(^\text{33}\) extending the FTE transport.

Outcomes:

- We started a preliminary evaluation of Dust2;
- obfs4 continues to grow, now ranking in third place by popularity with 1.5k daily users;
- meek-azure’s bandwidth was improved, tripling the bandwidth availability and therefore increasing its speed and user adoption.

Challenges:

During this quarter, the Tor Project had some challenges that took time away from our tech lead for the Pluggable Transports project. We had to ask him to step up and take some of Nick Mathewson’s tasks for Core Tor development, since Nick was appointed as deputy interim Executive Director while we search for a new permanent executive director.

The three most notable instances in which this affected our working capacity were two newly-disclosed DoS vulnerabilities against hidden services, and a regression in the OpenSSL code that had an impact on Tor:

- **Hidden service vulnerabilities:**
  - Incident 1: The attacker could flood the hidden service’s introduction point with introduction requests. By reusing the same circuit for each new introduction request, the attacker could very efficiently get a very large number of requests to the hidden service, and since it couldn't keep up with the rate of requests, it became unreachable to normal users\(^\text{34}\). After considerable analysis, we discovered that the fix is to prevent reuse of the introduction circuit for subsequent introduction attempts\(^\text{35}\).
  - Incident 2: The attacker could establish a circuit all the way through to the hidden service, and then flood it with stream "begin" requests, causing the hidden

\(^{32}\) [https://kpdyer.com/](https://kpdyer.com/)
\(^{34}\) [https://trac.torproject.org/projects/tor/ticket/15463](https://trac.torproject.org/projects/tor/ticket/15463)
\(^{35}\) [https://trac.torproject.org/projects/tor/ticket/15515](https://trac.torproject.org/projects/tor/ticket/15515)
service to create thousands of connections to its underlying application (e.g. the 
webserver), which overwhelms both Tor and the underlying application.\footnote{36} The fix 
is to give hidden services a configurable (off by default) cap on the number of 
simultaneous connections a given circuit can make to the hidden service.\footnote{37}

- **OpenSSL 1.1 breaking:**
  - We also discovered that recent changes to OpenSSL 1.1 had caused Tor to stop 
    compiling properly. In most cases these were fixed with changes to the Tor code, 
    but in one instance we had to write a patch for OpenSSL in order to ensure 
    continued compatibility with Tor. We submitted this patch to upstream OpenSSL, 
    and it was accepted.\footnote{38}

Successes:

Our meek-azure improvements are a clear success. Having more people opt for meek-azure will 
also help us minimize our costs for maintaining the infrastructure required by meek (since we 
have a research grant from Microsoft to cover all the azure costs for a while yet).

Based on his experiences with operating meek’s infrastructure on the live Tor network, David 
Fifield, meek’s lead developer, co-authored a paper\footnote{40} entitled “Blocking-resistant communication 
through domain fronting”, domain fronting being the technique that meek, along with other 
software such as Lantern and Psiphon, uses to ensure that its connections to the Tor network 
can’t be blocked by a censor without incurring significant collateral damage.

Tor Browser’s adoption of obfs4 in its stable 4.5 release demonstrated that this pluggable 
transport has the potential to be a very popular censorship-circumvention solution.

**Testing and network simulation improvements**

**Project Objectives:**

Tor will improve the correctness and stability of the core Tor software by streamlining and 
automating the process of launching a complete test; designing and scripting an automated test 
suite to exercise and stress as much of Tor’s functionality as possible; and extending Tor’s 
controller interface to allow better monitoring.

\footnote{36} \url{https://trac.torproject.org/projects/tor/ticket/16052} 
\footnote{37} \url{https://lists.torproject.org/pipermail/tor-dev/2015-May/008838.html} 
\footnote{38} \url{https://lists.openssl.org/pipermail.openssl-commits/2015-May/001192.html} 
\footnote{39} \url{https://lists.torproject.org/pipermail/tor-dev/2015-May/008767.html} 
\footnote{40} \url{https://lists.torproject.org/pipermail/tor-dev/2015-June/008940.html}
Outputs for the Quarter:

Over the past quarter, we have continued our strategy of giving testability a high priority in all Tor development. As a result, our unit test coverage is now at 37%, and our total coverage, using stem and Chutney, is up to 62%.

Chutney’s coverage of Tor has itself extended to include more network types and functionality, including basic hidden service functionality, larger networks, and a larger fraction of directory authority functionality. In addition, we have extended Tor with functionality to give Chutney greater control over how directory authorities configure the network. Based on earlier work on Chutney, we are continuing to incrementally refactor the Chutney2 deployment, adding more features and improving its usability.

Following our earlier work to identify the most problematic or tricky aspects of Tor from the perspective of testing, we have identified some of the most essential and under-tested areas of our code, and begun to write tests for them. We produced a list of the most complex or volatile Tor functions\(^4\)\(^1\), and assessed the relative coverage of these functions by our unit tests\(^4\)\(^2\). We’re using these to drive and focus some of our refactoring/testing efforts.

We have also identified another target for the Tor re-modularization effort. Previously, we had focused our modularity designs on searching for cases where pieces of Tor could be broken out into different processes. But there are also significant pieces of the Tor ecosystem — notably, the scripts that authorities use to produce essential network measurements such as weighted bandwidth — that could be pulled in to such an effort. We’re adapting our multi-process modularization design (currently a work in progress) to ensure that it can accommodate the management of existing tools as well.

Outcomes:

- Unit Test coverage is at 37% - a result of making testability a requirement for development.
- Total coverage using Chutney and Stem is up to 62%
- New functionalities in Chutney:
  - Hidden Service functionality
  - Large networks functionality
  - Directory Authority functionality
- Prioritized list of functions needing test coverage - to drive our refactoring/testing efforts.
- Start drafting a modularization design for significant pieces of the Tor ecosystem.

\(^4\)\(^2\) [https://trac.torproject.org/projects/tor/ticket/16506#comment:1](https://trac.torproject.org/projects/tor/ticket/16506#comment:1)
Below we present extracts from our software changelogs that cover the relevant enhancements in full detail:

Core Tor 0.2.7.1-alpha release changes:\footnote{https://blog.torproject.org/blog/tor-0271-alpha-released}:

- **Minor features (testing):**
  - Add a test to verify that the compiler does not eliminate our memwipe() implementation. Closes ticket 15377.
  - Add make rule `check-changes` to verify the format of changes files. Closes ticket 15180.
  - Add unit tests for control\_event\_is\_interesting(). Add a compile-time check that the number of events doesn't exceed the capacity of control\_event\_t.event\_mask. Closes ticket 15431, checks for bugs similar to 13085. Patch by "teor".
  - Command-line argument tests moved to Stem. Resolves ticket 14806.
  - Integrate the ntor, backtrace, and zero-length keys tests into the automake test suite. Closes ticket 15344.
  - Remove assertions during builds to determine Tor's test coverage. We don't want to trigger these even in assertions, so including them artificially makes our branch coverage look worse than it is. This patch provides the new test-stem-full and coverage-html-full configure options. Implements ticket 15400.

**Challenges:**

We expect further improvements in total test coverage, but must (as before) emphasize that the rate of further improvement is likely to be somewhat slower, since we are running out of "low-hanging fruit" for which the benefits will be outsized in relation to the effort.

**Successes:**

Alongside the additional tests we have added to already-existing functions in the Tor code, we have successfully begun to inculcate in our development community the idea of testing as an essential aspect of the development process. Our present unit test coverage of 37% testifies to this.

We are very happy with our continued improvement of Chutney: the ability to simulate large networks and hidden services will be extremely helpful to our community members, especially researchers and developers who need to test and simulate experiments or new features in networks with these characteristics.
Enhanced outreach

Project Objectives:

We will make more people aware of the benefits of Tor, especially when censorship circumvention needs to be combined with privacy and anonymity to extend the time that civil society members can work in Internet-repressive environments.

Outputs for the Quarter:

Direct work with organizations:

- We contributed substantially to the first report to the United Nations Human Rights Council by its Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye.44 A couple of highlights about Tor from the report:

52. States have also attempted to combat anonymity tools, such as Tor, proxies and VPNs, by denying access to them. China has long blocked access to Tor;55 and Russian government officials reportedly offered more than $100,000 for techniques to identify anonymous users of Tor.56 In addition, Ethiopia,57 Iran (Islamic Republic of)58 and Kazakhstan59 have reportedly sought to block Tor traffic. Because such tools may be the only mechanisms for individuals to exercise freedom of opinion and expression securely, access to them should be protected and promoted.

“Decentralized approaches like Tor’s, in which security is designed into the system and there is no central party to coerce or subvert, are as necessary a response to surveillance as encryption is.”

44 http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx
U.N. comment on Tor

We received very positive media coverage of this event: Washington Post\textsuperscript{45}, The Intercept\textsuperscript{46}, SC Magazine\textsuperscript{47}, to highlight only a few. We also blogged\textsuperscript{48} about the legal aspects of it, a post authored by our Board Member, Wendy Seltzer (Lawyer, cyberlaw professor, and founder of ChillingEffects.org), and promoted it on social networks\textsuperscript{49}, receiving hundreds of impressions and engagements.

\textbf{U.N. report: Tor must be protected and promoted}-- wpo.st/H2LJ0 c @davidakaye

"There are many millions of people who depend on tools like encryption or [the anonymous browsing tool] Tor to ensure as much as they can against disclosure of their communications and to seek out information," he said.

\begin{itemize}
\item \textsuperscript{45} \url{https://www.washingtonpost.com/blogs/the-switch/wp/2015/05/28/un-report-encryption-is-important-to-human-rights-and-backdoors-undermine-it/}
\item \textsuperscript{46} \url{https://firstlook.org/theintercept/2015/05/28/u-n-report-asserts-encryption-human-right-digital-age/}
\item \textsuperscript{47} \url{http://www.scmagazine.com/david-kaye-puts-together-united-nations-encryption-report/article/417501/}
\item \textsuperscript{48} \url{https://blog.torproject.org/blog/un-special-rapporteur-anonymity-gateway-free-expression}
\item \textsuperscript{49} \url{https://twitter.com/torproject/status/604026388081819649}
\end{itemize}
• We have been working with Amnesty International to integrate Tor into their curriculum and for internal use within their organization. We met with leaders from Amnesty’s DC office and taught them to use RedPhone; our next training will teach them how to use Tor.

• Having uncovered misconceptions about Tor when speaking to Amnesty International, we created a survey that identifies obstacles to the teaching of Tor to human rights defenders, as well as solutions to these problems.

We received feedback on the survey from three trainers in East Africa and the US, and it is being currently reviewed, for informal input, by Andrea Forte, PhD at Drexel University. We will then distribute the survey via email to people who teach workshops on privacy tools.

50. http://www.andreaforste.net/
We partnered with Global Voices for a “live video chat” about Tor.51

We also met with Ethan Zuckerman, Global Voices co-founder, in Berlin; he is interested in rolling out Tor for all their bloggers. GV is, among other things, a blogging platform for human rights-related bloggers, and enabling them to use anonymization tools will protect them while they are doing their jobs.

Media Support:

We continue to actively pitch to the media stories about our work, our community, and any other topics that we believe are important to help educate the public on Tor.

Dealing quickly with "attack" media requests — we constantly receive press requests about every single thing a journalist can put their hands on.

Sometimes these are about real and important attacks for which Tor wants to communicate openly with its community regarding the current situation, whether we are immune from the threat or are still working to protect Tor users from it.

To be able to triage these requests we created a media list that includes researchers who can help “vet” potential attacks for their severity. Thanks to this triage we are saying “no” to some requests for comment on attacks that are in reality not urgent.

51
• To help educate the public about our funding rationale (and to convey the fact that we are mission- rather than funding-driven) we published a post entitled “How We Work\textsuperscript{52}”. Much of the criticism of Tor's funding died down very quickly (though probably temporarily) when this blog post was published.

• In an article at The Nation\textsuperscript{53}, the author mentions Tor as the best tool for the average citizen to protect their metadata. Here is the full quote:

   The challenge of protecting the average citizen’s metadata is currently best handled by tools like the Tor project, an international network of volunteer proxies with an associated browser and other client software. Tor is used by journalists, activists, domestic-violence victims, and even US government investigators—all groups for whom surveillance can have serious consequences. Tor encrypts traffic and bounces it between several relays, ensuring that the relay a user connects to doesn’t know where the traffic is going, and the relay passing the traffic to its final destination doesn’t know the source.

\textsuperscript{52} https://blog.torproject.org/blog/how-we-work
\textsuperscript{53} http://www.thenation.com/article/key-ending-mass-surveillance-math/
• Libération (from France) -- This article\(^5\) quotes Tor Project contributors Lunar, Jacob Appelbaum, and Runa Sandvik, and talks about "the emancipatory use of technology." It shows the drama and the high stakes of what we do at The Tor Project, without resorting to sensationalism.

Outreach materials

• As part of a broader reorganization of Tor’s active contributors into a team-based structure, we created the Community team to simplify coordination between our diverse outreach efforts. The team is comprised of researchers, developers, community volunteers, organizational partners, and our media team, and has already held several IRC meetings; we believe that the combination of all these resources is a very powerful one, and we are looking forward to the work this team will be carrying out, of which a preview can be found at the end of this report.

\(^5\) [http://www.liberation.fr/economie/2015/06/18/tor-mails-toi-de-tes-oignons_1332660](http://www.liberation.fr/economie/2015/06/18/tor-mails-toi-de-tes-oignons_1332660)
• The time and resources offered by Tor’s many relay operators and other volunteers around the world are essential to our work, and one of the ways we have shown our gratitude over the past several years is by distributing free Tor t-shirts for certain levels of contribution. This program has been dormant recently due to lack of time on the part of those handling T-shirt requests, but during the past quarter we have recruited a member of Torservers.net to take on this responsibility, and 100 T-shirts have already been sent out, with a further 180 already in the queue for the next quarter.

Social Media:

• Twitter, which Tor has been using more intensely over the last quarter as a method of communication with users and the public at large, is all about the moment, and we are adopting a strategy to build fast responses to events so that our community and the media can hear Tor’s voice. A few examples:
  o Our response to a New York Times article about a supposed attack against Tor Browser in China:\(^\text{55}\):

---

\(^{55}\) [https://twitter.com/torproject/status/610542145305464832](https://twitter.com/torproject/status/610542145305464832)
Regarding the June 13th article on privacy tools and #China published @nytimes:
#anonymity #humanrights #Beijing #Tor

"Tests show that Tor browser users are unaffected by the browser attacks described in the recent New York Times article about China. This is a great example of why it's important to use Tor Browser when browsing over Tor."

-The Tor Project
(Download our browser: www.Torproject.org)

- Special Tweet celebrating Equal Marriage approval by the Supreme Court

---

56. https://twitter.com/torproject/status/614513026008399872
○ This post was recognized by many of our followers as a positive intervention:

● Live Tweeting events:
  ○ Live Tweeting of the recent Privacy Enhancing Technology Symposium67:

---

67 https://twitter.com/torproject/status/614513026008399872
IPhones vs other phones: “The rich get protection from surveillance and the poor get more and more surveillance.” - @csoghoian #PETS15

- Live Tweeting while Tor members were on stage at the DIVSI Convention in Germany:

- Other tweets announcing our participation in events:
  - re:publica 15
  - Workshop about Tor at Brazil’s Cryptorave
  - Talk about privacy at Penn Law

- We decided to also explore more story-like posts, for which we created a Medium blog. The first post had ~500 readers and 25 recommendations.

---

58 https://twitter.com/torproject/status/597919687347818496
59 https://twitter.com/torproject/status/592052190820327424
60 https://twitter.com/torproject/status/589532463816249344
61 https://medium.com/@torproject/tor-s-summer-of-privacy-2a090016f8b2
Tor’s “Summer of Privacy”
An idealistic new generation of hackers is working with Tor. Here’s one of them.

Jesse Victors was chosen as one of the Tor Project’s first class of Summer of Privacy students—he is currently working with Tor developers to refine tools that keep human rights activists, journalists, and others safe from being targeted by surveillance. We interviewed Jesse recently.

- Our Twitter account was verified by Twitter’s Open Source team. Our account has gained +10k followers in the past quarter and accumulated 3.3M impressions (for comparison, in the preceding quarter we had 2.1M impressions). The metrics show that we are gaining popularity on Twitter as a result of our more active engagement there.
Agility\textsuperscript{62} - a website that maintains ranks categorizing social media accounts that are proven to be experts on certain topics - ranked The Tor Project’s Twitter account as the #1 authority on Internet Privacy, and #9 for Cryptography:

Outcomes:

- Direct work with organizations:
  - UN Special Rapporteur David Kaye, in his report on the promotion and protection of the right to freedom of opinion and expression. recognizes Tor as an important

\textsuperscript{62} https://www.agility.com/
tool to guarantee those rights, and calls for its widespread adoption. We consider
this a very important accomplishment for our organization;

- Our partnership with Amnesty International continues to grow: we have trained
some of their staff in D.C. and are talking with them regarding the inclusion of Tor
in their curriculum;

- Our partnership with Global Voices also continues to grow: we did a live chat
about Tor and have more lined up for next quarter. We are also training their staff
to use Tor.

- **Media Support:**
  - We formed a dedicated team of researchers to help triage attacks and prepare
  for possible media questions;
  - We have had continued success in pitching stories to major media outlets.

- **Outreach:**
  - Our T-shirt program has been relaunched, and 100 shirts delivered already;
  - Our organization of the Community team brings together different actors who
  work with us on our various outreach initiatives.

- **Social Media:**
  - Popularity: an increase of one million impressions;
  - Verification of our Twitter account;
  - +10K followers

**Challenges**

A large part of the success we have seen in our work on the outreach and media fronts is due to
the contributions made by our community of users, volunteers, and developers.

The challenges we see ahead of us in the coming quarter are maintaining the consistency of our
outreach efforts, which are now founded largely on the work of volunteers, and balancing the
handling of media requests with the demands of leading a new, larger group of contributors in
the Community team.

**Successes:**

**Direct work with organizations**

- Without a doubt, the most important achievement for this quarter was the recognition by
the UN Special Rapporteur that Tor is one of the few mechanisms allowing individuals to
exercise their freedom of opinion and expression online. This was the result not only of
our having recognized the importance of the work, but also investing time and effort in
providing direct expert guidance to the report’s authors.
• Another success in our work with organizations is the different initiatives that are starting to emerge from the diverse group we are collaborating with. For instance, our project with Amnesty International showed us the need to build better materials for trainers and help correct mistaken assumptions about Tor that we have encountered during this working relationship. Our forthcoming trainers’ survey will be delivered to several organizations who may not know one another but who are all working together with the Tor Project in different ways. We have been capable of recognizing the value that each of them can bring when designing programs to educate others about Tor and privacy protection.

Outreach materials

• Our new Community team will aid coordination between the different actors who contribute to Tor’s outreach efforts. We are giving them the support they need to grow.
• Our popular T-shirt program is now back up and running.

Social Media

Our Twitter account has become more influential on the network, and our statistics show an increase in popularity and impact following our efforts to make Tor’s Twitter communications clearer and more accessible.

Media Support

We would like to highlight a few strategies that had great success with the media:

• Our “How we work” post, covering the relationship between our funding and development processes was a great way to promote our voice and therefore influence the conversation in a positive way.
• Our new “attack triage” team ensures that the Director of Communications and the Press team have a solid technical foundation on which to make decisions about press releases and requests for comment.
• Our efforts to pitch stories, and our educational work with members of the press, continue to pay dividends in the quality of the articles we see coming out.

Press:

<table>
<thead>
<tr>
<th>Date</th>
<th>Media Outlet</th>
<th>Title</th>
</tr>
</thead>
</table>

34
<table>
<thead>
<tr>
<th>Date</th>
<th>Source</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 June 18</td>
<td>Medium</td>
<td>Tor’s “Summer of Privacy” (interview by Kate Krauss)</td>
</tr>
<tr>
<td>2015 June 18</td>
<td>Libération</td>
<td>Tor: Mails-toi de tes oignons</td>
</tr>
<tr>
<td>2015 June 18</td>
<td>Wired</td>
<td>The Dark Web as You Know It Is a Myth</td>
</tr>
<tr>
<td>2015 June 2</td>
<td>New York Times</td>
<td>The Art of Dissent</td>
</tr>
<tr>
<td>2015 June 2</td>
<td>Global Voices Online</td>
<td>Tor Use in Russia Spiking in Response to Kremlin's Censorship Efforts</td>
</tr>
<tr>
<td>2015 June 1</td>
<td>SC Magazine</td>
<td>Who goes there?: Tor Project</td>
</tr>
<tr>
<td>2015 May 28</td>
<td>Global Voices Advocacy</td>
<td>Advocers Talk About Tech, Privacy, and Security with Tor</td>
</tr>
<tr>
<td>2015 May 28</td>
<td>The Intercept</td>
<td>U.N. Report Asserts Encryption as a Human Right in the Digital Age</td>
</tr>
<tr>
<td>2015 May 28</td>
<td>Washington Post</td>
<td>U.N. report: Encryption is important to human rights — and backdoors undermine it</td>
</tr>
<tr>
<td>2015 May 26</td>
<td>ITWeb</td>
<td>Govt snooping highlights need for Tor</td>
</tr>
</tbody>
</table>

63 https://medium.com/@torproject/tor-s-summer-of-privacy-2a090016f8b2
64 http://www.liberation.fr/economie/2015/06/18/tor-mails-toi-de-tes-oignons_1332660
65 http://www.wired.com/2015/06/dark-web-know-myth/
68 http://www.scmagazine.com/who-goes-there-tor-project/article/414299/
70 https://firstlook.org/theintercept/2015/05/28/u-n-report-asserts-encryption-human-right-digital-age/
Next Quarter’s Planned Activities:

Pluggable Transport Integration

The following are indications from our Pluggable Transport team lead regarding the work that will be done over the coming quarter.

- The documentation/evaluation/etc work that falls under the SponsorT extension.
- Finally start approaching the Bridge Guards little-t tor code.
- Give more thought to the open OR port problem.


78 http://tecnologia.elpais.com/tecnologia/2015/04/04/actualidad/1428169979_196077.html
• Various little-t tor side PT cleanups, particularly logging and the teardown process. This stuff should/needs to happen for 0.2.7.x, so it's relatively high on my priority list.
• obfs5 work (I really want to do something UDP, but it'll be a huge timesink).
• The DNS thing that the student did might have potential, though it'll be relatively easy to detect/block, needs further investigation. Reliability and the potential for harm to the public DNS infrastructure are my primary concerns here.
• Help the UC Berkeley people as needed with their eval work etc.
• Continue to fix things as they catch on fire, though so far obfs4proxy appears to "just work".
• Someone pointed me at a potential issue in my C++ Elligator2 code, which is a port of the Go code by agl used by obfs4proxy. I need to double check the math/code in more depth but at this point I know that if my C++ code is wrong so is agl's Go code.

Testing and network simulation improvements

• We will continue to expand our test coverage of the Tor code with both unit and integration tests, and to reduce the size of the hard-to-test "blob" in the code by removing key code dependencies. Our simulation tools will also be developed, with improved Chutney tests to handle cases involving multiple versions of Tor (in order to test compatibility between old and new releases), and an alpha framework for imitating an ill-behaved client (in order to test error functionality). Finally, we also hope to build an alpha module-isolation mechanism to improve our code safety.

Enhanced Outreach

Direct working with organizations

• Our informal organizational partnership with the Library Freedom Project, already successfully launched in this quarter, will continue; a now-published blog post79 describes our current joint activities.

• We will solicit and organize information from our Community team regarding upcoming trainings and other activities, and we will deploy our survey for trainers (see above) and collect 20 sets of results, using them to develop a list of recommendations for Tor trainings.

Outreach materials

79 https://blog.torproject.org/blog/tor-exit-nodes-libraries-pilot-phase-one
• We will be making an active effort to encourage, regroup, and connect those who are reaching out to users in their communities and educating them about Tor, with the goal of growing the set of people around the world who are comfortable, empowered, and prepared to speak to others about Tor. A tor-teachers mailing list will serve as the main channel for these educators to communicate with each other and with the Tor Project itself.

• We are tabling at the National Network to End Domestic Violence Tech Summit\textsuperscript{80} — last year we hosted the keynote at this conference, and they have invited us to exhibit this year, which is a great opportunity for outreach.

• We will also be focusing on outreach materials for Farsi-speaking users, with a Farsi-language video about Tor already in production, and Farsi versions of Tor’s popular stickers. Other videos we hope to produce will deal with hidden services or bridges.

**Social Media**

• We will continue to tweet strategically, focusing on Tor’s Twitter rebranding as smart, friendly and more diverse, which has already borne fruit over the past quarter. We will use it to promote our new mission statement, giving our social media followers a clearer idea of Tor’s values and objectives.

**Media Support**

• We have developed a new procedure for creating collective blog posts, to ensure that the content is both technically accurate and clear enough for a non-specialist readership. We hope to publish seven such posts per month using this process, along with several guest blog posts from relevant groups or individuals within our community or further afield. One such post, explaining Tor’s approach to reported security issues or research papers, and how these should be treated by members of the press and public, will be published shortly.

• Tor’s Press team has also assembled a group of technical specialists who can help assess incoming reports of attacks and help decide what kind of response is needed; we expect to test this process over the next quarter. More generally, we will be continuing to coordinate and strategize our response to incoming media opportunities (including negative stories), of which we receive about one per day.

As well as responding to incoming requests, we will also be pursuing an active media strategy of pitching positive stories about Tor to news outlets: for example, Kate Krauss’ interview with Nick Mathewson will be pitched to the Christian Science Monitor for an op-ed. We hope to run at least three such stories over the quarter. We will also continue to build relationships with individual reporters and ensure they have an accurate understanding of Tor’s work. Finally, we will also be gathering and publishing information about the role of Tor software in users’ lives: a fact-sheet listing positive uses of Tor hidden services is already complete, and we hope to gather several testimonials from real Tor users about the things they do with our software, to be used in press and crowdfunding material.