
<table>
<thead>
<tr>
<th>Grantee:</th>
<th>The Tor Project Inc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Title:</td>
<td>Applying Censorship Resistance Research to the Field</td>
</tr>
<tr>
<td>Grant Number:</td>
<td>S-LMAQM-14-GR-1095</td>
</tr>
<tr>
<td>Primary Point of Contact/Title:</td>
<td>Isabela Bagueros / Project Manager</td>
</tr>
<tr>
<td>Email:</td>
<td><a href="mailto:grants@torproject.org">grants@torproject.org</a></td>
</tr>
</tbody>
</table>

**Final Report project timeline (July 10, 2014 – November 30, 2016)**

**Pluggable transport integration**

**Project objectives**

**Note:**

**Project accomplishments**

**Accomplishments per Tasks**

**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.

**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.

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

**Task 4 (SponsorS):** Pluggable transport R&D (Catch-all)

**Project challenges**

**Testing and network simulation improvements**
Pluggable transport integration

Project objectives

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.

Note:

We would like to note that the list of activities for this project was reviewed in early 2015 to clarify that Task 1 was part of another grant Tor was working on. Since this work was also relevant to other tasks we had under this goal, we continue to report on it throughout the project time period, therefore we decided to include the list of accomplishments achieved under that task in this final report as well.
Project accomplishments

The best data point we can use to demonstrate the success of our work under this goal is the incredible increase of PT usage capture by our Metrics team, we had ~5k daily users back in July 2014 (when we started) and by November 2016 (when our grant ended) that number went up to ~30k daily users:

[Image of a graph showing the total pluggable transport usage growth from July 2014 to November 2016.]

1https://metrics.torproject.org/userstats-bridge-transport.html?start=2014-07-10&end=2016-12-01&transport=%21%3COR%3E
Breakdown by Pluggable Transport

Please refer to our Metrics Final Report for highlights of Internet censorship situations throughout the period of this grant that shows the direct impact of this efforts with the end user.

Accomplishments per Tasks

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 created an Evaluation Criteria for Pluggable Transports (PTs) which gave us a baseline to evaluate upcoming PTs designs:

- meek Evaluation
- obfs2 Evaluation
- obfs3 Evaluation
- obfs4 Evaluation

4 https://trac.torproject.org/projects/tor/wiki/doc/PluggableTransports/MeekEvaluation
5 https://trac.torproject.org/projects/tor/wiki/doc/PluggableTransports/Obfs2Evaluation
This work had a direct impact on:

- PTs development - not only the developers of the PTs we evaluated benefited from it but new members of our community has now a set of guidelines to follow when creating new PTs that will help them build a solution with better chances of being deployed in censorship circumvention tools.
- Direct impact on R&D of PTs - our guidelines provided clear guidance for this process, making it easier for PTs to be deployed.
- Increased awareness around PTs and how to use it to circumvent censorship through our new educational materials and remake of our wiki and web pages.

---

9 https://trac.torproject.org/projects/tor/wiki/doc/PluggableTransports/FteEvaluation
13 https://trac.torproject.org/projects/tor/wiki/doc/PluggableTransports/basket2evaluation
14 https://twitter.com/torproject/status/809792947181023232
15 https://trac.torproject.org/projects/tor/wiki/doc/PluggableTransports
16 https://www.torproject.org/docs/pluggable-transports.html.en
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.

When we started this grant (July 2014), Tor Browser had the following Pluggable Transports deployed as part of its bundle:\textsuperscript{17}:

<table>
<thead>
<tr>
<th>Pluggable Transport</th>
<th>Number of Bridges</th>
</tr>
</thead>
<tbody>
<tr>
<td>obfs3</td>
<td>7</td>
</tr>
<tr>
<td>flashproxy</td>
<td>5</td>
</tr>
<tr>
<td>FTE</td>
<td>8</td>
</tr>
<tr>
<td>scramblesuit</td>
<td>3</td>
</tr>
<tr>
<td>meek</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>23</strong></td>
</tr>
</tbody>
</table>

\textsuperscript{17}https://gitweb.torproject.org/builders/tor-browser-bundle.git/tree.Bundle-Data/PTConfigs/bridge_prefs.js?id=ece1766b18f94b7937ac2497d7e3fb4b5fd62965
Currently Tor Browser has the following Pluggable Transports bridges available to it’s users:

<table>
<thead>
<tr>
<th>Pluggable Transports</th>
<th>Number of Bridges</th>
</tr>
</thead>
<tbody>
<tr>
<td>obfs3</td>
<td>5</td>
</tr>
<tr>
<td>FTE</td>
<td>4</td>
</tr>
<tr>
<td>obfs4</td>
<td>20</td>
</tr>
<tr>
<td>Meek Amazon</td>
<td>1</td>
</tr>
<tr>
<td>Meek azure</td>
<td>1</td>
</tr>
<tr>
<td>Snowflake</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>32</strong></td>
</tr>
</tbody>
</table>

As part of this task we not only collaborated with the maintenance of existent Pluggable Transports but we also developed or helped deploy new ones to Tor Browser. Here are some highlights from this work that we would like to share:

**Obfs4**

The obfs4 protocol was developed in response to the vulnerability of the obfs3 protocol to detection via active probing attacks. It is expected to supersede the obfs3 protocol as the front-line Pluggable Transport used by most Tor users.

From a design standpoint, the obfs4 protocol is significantly closer to the ScrambleSuit protocol by Philipp Winter, and can be described as a direct descendant with incremental cryptographic improvements. This integration also made it easier to use obfs4 on mobile.

We created a deployment plan for obfs4 when we started this project in October 2014 and finally deployed it on Tor Browser 4.5 stable release in April 2015. Right after the launch we gained adoption really quickly and achieved our bandwidth capacity of our bridge by end of 2015:

---

[12] [https://trac.torproject.org/projects/tor/ticket/13633](https://trac.torproject.org/projects/tor/ticket/13633)
[19] [https://trac.torproject.org/projects/tor/ticket/12130](https://trac.torproject.org/projects/tor/ticket/12130)
Because of its success we worked with our community to add more bridges for obfs4, the first one was added in April 2016 as part of our 5.5.5 release, and continue to add more bridges on the following releases. You can see the immense growth in usage during all 2016 and continuing over 2017\(^2\). Right now we have 20 obfs4 bridges available to users and an average of 35,000 daily users:

\(^2\)https://metrics.torproject.org/userstats-bridge-transport.html?start=2015-04-01&end=2017-03-02&transport=obfs4
Other projects also adopted obfs4 transport as an option for people to use to connect to the Tor network like Orbot on version v15 and Tails on version 1.3 and up.

**Development basket2 (previously called obfs5)**

The basket2 transport was developed by the Tor Project in response to certain theoretical weaknesses in the obfs4 transport\(^{22}\). From a design standpoint, basket2 most closely resembles the obfs4 protocol, also incorporating ideas borrowed from the experimental and undeployed basket protocol\(^{23}\).

**Solving meek scalability problem:**

meek makes Tor traffic look like a connection to an HTTPS website. Unlike the other transports, it doesn't connect directly to a bridge. meek first connects to a real HTTPS web server (in the Amazon cloud or the Microsoft Azure cloud) and from there connects to the actual bridge. Censors cannot easily block meek connections because the HTTPS servers also provide many other useful services.

We ran into a few road bumps while trying to meet the demand for such solution. Mainly because of bandwidth latency and cost as well, after all these are cloud services we are paying the bandwidth usage for it.

First bump was meek-azure performance, at first meek-azure was the slowest transport we had available and many users didn’t like using it. In April we released a fix for it that provided a big improved on meek-azure’s performance\(^{24}\) which lead to more people to use it.

We continue to release other fixes\(^{25-26}\) that would remove unnecessary bandwidth usage in order to try to optimize bandwidth consumption. This was important to be able to have more users connected through meek while our costs for bandwidth usage would remain relative low as we pay for usage of those cloud services.

The graphic below\(^{27}\) shows the reflect of these efforts throughout the period of this grant and how we were capable to increase user adoption even within our limitations.


\(^{23}\) [https://github.com/yawning/basket](https://github.com/yawning/basket)


\(^{25}\) [https://trac.torproject.org/projects/tor/ticket/12857](https://trac.torproject.org/projects/tor/ticket/12857)

\(^{26}\) [https://trac.torproject.org/projects/tor/ticket/12778](https://trac.torproject.org/projects/tor/ticket/12778)

Better support for mobile - Migration to Golang

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 made this possible, 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.

Task 3 (Sponsor$): Tor side pluggable transport related (and other) improvements.

 Proper way to terminate processes for Pluggable Transports in different platforms.

On Linux we added a specific call to have the kernel SIGTERM pluggable transports if Tor abruptly terminates\textsuperscript{28}. We also addressed a long standing cross platform issues with the specification that results in massive amounts of pain for systems that are lacking SIGTERM e.g. Windows\textsuperscript{29,30}.

The "TOR_PT_EXIT_ON_STDIN_CLOSE" environment variable can be used by implementations to setup a valid open stdin in the child process that can be used to detect if Tor has terminated\textsuperscript{31}. This specific feature was very important for meek, as it is actually

\textsuperscript{28} \url{https://trac.torproject.org/projects/tor/ticket/15471}
\textsuperscript{29} \url{https://trac.torproject.org/projects/tor/ticket/9330}
\textsuperscript{30} \url{https://trac.torproject.org/projects/tor/ticket/15435}
\textsuperscript{31} \url{https://trac.torproject.org/projects/tor/ticket/15435}
meekclient that drives the pluggable transport negotiation with Tor, simplifying things a lot for meek to interact with Tor.

UX improvements:

Proxy and PT configuration form used to be placed together in the same screen, this is already a very confusing step for an user to go through, and placing both together was making it harder for our users. We changed the screen with a question that leads the user to the right form for them.

Merging PT patches and maintaining bridges on Core Tor and Tor Browser

We merged 26 patches into 6 Core Tor releases series (0.2.4, 0.2.5, 0.2.6, 0.2.7, 0.2.8 and 0.2.9 series) and 6 Tor Browser releases series (4.0, 4.5, 5.0, 5.5, 6.0 and 6.5 series) that fixed critical bugs related to the integration of PT into these systems, performance improvements, and transport bridges management during the period of this grant.

Launched a new bridge authority: "Bifrost"

After ten years of volunteer maintenance of Tonga, Tor's bridge Authority—a piece of critical infrastructure within the Tor network—our colleague and friend, Lucky Green, a long time cypherpunk, and free speech and privacy advocate, has decided to step down from this role.

---

32 https://trac.torproject.org/projects/tor/ticket/15145
33 https://archive.is/6OjQs
The Bridge Authority is a simple but essential piece of the Tor Network. Unlike the other directory authorities, the Bridge Authority does not get a vote in Tor's consensus protocol. Instead, it serves to aggregate relay descriptors which Tor Bridges send to it.

It then sends these descriptors to BridgeDB, which does all the deduplication, cryptographic signature verification (again), stability calculations, pluggable transport argument validation, assignment into the hashring of each Bridge distribution mechanism, and finally distributing the Bridges to Tor clients of users who are under censorship.

The Tor Project received the generous donation from Greenhost of hardware, hosting, and bandwidth which allowed us to launch Bifröst, our new Bridge Authority.

![Running bridges by bridge authority](image)

**Task 4 (SponsorS): Pluggable transport R&D (Catch-all)**

We would like to highlight the following researches which we have also collaborated with throughout the period of this grant:

<table>
<thead>
<tr>
<th>Researcher</th>
<th>University</th>
<th>Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undergraduate student under Prof. Nick Feamster</td>
<td>Princeton University</td>
<td>DNS based Pluggable Transport as a semester project (experimental, not deployable)</td>
</tr>
<tr>
<td>Kevin Dyer</td>
<td>Portland State University</td>
<td>Usenix Security paper called “Marionette: A”</td>
</tr>
<tr>
<td>Name</td>
<td>Organization</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Marc Juarez</td>
<td>KU Leuven</td>
<td>Work to improve his pluggable transport that provides a website fingerprinting defense framework for research purposes. This framework has proven useful at exploring anonymity defenses, by transforming Tor traffic to reduce timing and volume signatures.</td>
</tr>
<tr>
<td>Serene Han</td>
<td>University of California - Berkeley</td>
<td>Snowflake&lt;sup&gt;35&lt;/sup&gt; Pluggable Transport - working on adding WebRTC support to Flashproxy</td>
</tr>
<tr>
<td>Linda Naeun Lee, Serge Egelman, David Wagner, and David Fifield</td>
<td>University of California - Berkeley</td>
<td>Performing usability research on Tor Launcher flow - which is the configuration dialogue box of Tor Browser to connect it to the Tor network&lt;sup&gt;36&lt;/sup&gt;.</td>
</tr>
<tr>
<td>Michael Carl Tschantz, Sadia Afroz, Anonymous, and Vern Paxson</td>
<td>University of California - Berkeley</td>
<td>Their paper evaluated censorship techniques used over the years against Tor and how we have been addressing them. These techniques include active probing, which China has used to block Tor&lt;sup&gt;37&lt;/sup&gt;.</td>
</tr>
<tr>
<td>Frederick Douglas, Rorshach, Weiyang Pan and Matthew Caesar</td>
<td>University of Illinois Urbana Champaign</td>
<td>Paper: “Salmon: Robust Proxy Distribution for Censorship Circumvention”&lt;sup&gt;38&lt;/sup&gt;. An attempt to isolate malicious actors who are just trying to find out our bridges so they can censor them.</td>
</tr>
</tbody>
</table>

### Project challenges

As we worked to deploy more PT bridges and different ways to obfuscate a connection to Tor network and therefore bypass online censorship, our data shows a fast adoption and growth of such solution, reinforcing the point that there is a demand for such solution.

Such an important project will always carry important challenges. During the period of this grant we saw the need to be constantly evolving or building new PT designs as censors keeps trying to find ways to impede our solutions from working.

---

We also saw a big challenge related to capacity of maintaining the cost certain PTs has like meek, which uses cloud services from Amazon and Microsoft Azure, to bypass censorship. We have to pay for the bandwidth used by our users under those services. To compensate for that we encourage all users that don’t need meek specifically to pass the censorship they are facing. We deployed obfs4 and worked with our community to provide bridges/bandwidth for these users. We ended our program with 20 obfs4 bridges being offered on Tor Browser alone.

We had some team capacity challenges as well, in the middle of 2015 our Executive Director step down and our team leader, Nick Mathewson, together with our research director, Roger Dingledine, had to step in as interim and deputy interim Executive Directors (respectively). This added some load to their schedule for a few months which was an unexpected factor we had to deal with.

One of the challenges our PT community currently has is coordination. This is a challenge because it will require a lot of dedication and coordination with the community, in order to ensure that the results of developer efforts are useful for everyone (clients that want to deploy them, and end users).

We have reflected a lot about this, we know Tor plays a big role in the ecosystem and that is why we want to help solve this problem. We need a dedicated person to lead this effort and drive coordination with the rest of the community, we are working on this solution and hope to present it soon to the rest of the community.

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.

Project accomplishments

We have achieved the objectives described above by working on different areas such as test coverage (of legacy code as well as new code), to automate test suite processes as well as improving our testing tools like Chutney and Stem.

A data point we can give to show the impact of such accomplishment is the increase of test coverage shown on our reports, at first we reported around 60% of test coverage, at the time of writing this final report our coverage was around 83%.

Test coverage
Test coverage has become a mandatory feature\textsuperscript{39} for all incoming patches so we can ensure a constant high coverage of code. The Network Team also applied a new code review process that include reviewing the code tests as part of its guidelines\textsuperscript{40}.

For the legacy code in the codebase we prioritized all functions that needed test coverage and created tests for all of them.

Because of this effort we reached a very important milestone with our 0.2.7.3rc release, from September 2015, was considered the ‘most tested release of Tor to date’.

And all that followed it always had something new related to our tests. Tor's tests are now launched from a unified testing framework that ships with the Tor source distribution, which integrates with external testing tools as well. And it can now self-test using controller tests from Stem and integration tests from Chutney.

And we also created a whole new test network, simulating real ‘tor network’ scenarios that our code might encounter in the wild.

Work for the community

Great part of the ‘end user impact’ of this type of work is actually focused on those who need to ‘consume our codebase’ in order to participate of Tor project. Our ‘volunteer developer’ is also a

\textsuperscript{39} https://gitweb.torproject.org/tor.git/tree/doc/HACKING/WritingTests.md
\textsuperscript{40} https://gitweb.torproject.org/tor.git/tree/doc/HACKING/HowToReview.md
persona we must consider when thinking of ‘whose needs’ we are trying to meet as we develop Tor.

We created a special guideline for ‘Writing Tests’ for Core Tor under our ‘HACKING’ folder, which is our ‘most read’ folder for new collaborators. It’s part of Tor source code, so anyone who downloads the code sees it. We also updated our team wiki page highlighting all this documentation.

We also want to highlight ticket #17101, which was actually a contribution from a volunteer who created some tests that covers the evaluation of an exit address at the function that rewrites addresses and attaches entry connections to circuits. It is great to see our community incorporating the practices we have been promoting with efforts sponsored by this grant.

Finally we would like to highlight once more the amazing retrospective report done by Nick Mathewson, Core Tor Lead. To go back and review severe bugs to identify trends that lead to those bugs, is an important exercise to identify areas where we can improve our development process and improve the quality of what it produces.

Quoting Nick’s report:

“But many groups have found it helpful to pause periodically and look for trends in the bugs they have discovered or fixed over the course of their projects. By finding trends, we can try to identify ways to develop our software better.”

---

Mid-2016 Tor bug retrospective, with lessons for future coding

I. Introduction

Programs have bugs because developers make mistakes. Generally, when we discover a serious bug, we try to fix it as soon as we can and move on. But many groups have found it helpful to pause periodically and look for trends in the bugs they have discovered or fixed over the course of their projects. By finding trends, we can try to identify ways to develop our software better.

---

42 [https://trac.torproject.org/projects/tor/wiki/org/teams/NetworkTeam#Becomingavolunteer](https://trac.torproject.org/projects/tor/wiki/org/teams/NetworkTeam#Becomingavolunteer)
43 [https://trac.torproject.org/projects/tor/ticket/17101](https://trac.torproject.org/projects/tor/ticket/17101)
Another part of this effort that we would like to highlight is the improvements done for the tools we use to test our releases such as Chutney and Stem. As well as the sophistication of our tests through our ‘Testing Network’, being able to roll out a new release on such environment that can simulate more scenarios our code might find in the wild, such as more diversity of OSs, hardware and configurations.

Testing Network:

We created a completely private/password protected testing network, which we are calling “testnet.” It contains 16 Tor relays, and it has metrics tools like CollecTor, Atlas, Onionoo and Consensus Health set up, so we can monitor the network.

Chutney:

The first achievement on improving Chutney was to reduce the time it used to take to run it against your code to test it. Before it would take up to 20 minutes to run Chutney tests on your code, thanks to the hard work of the team it now takes a matter of seconds.

● New functionalities in Chutney:
  ● Hidden Service functionality
  ● Large networks functionality
  ● Directory Authority functionality
  ● Added single onion service tests
  ● Added IPv6 client tests
  ● Made chutney able to use the system Tor instance much more easily
  ● Added more mixed Tor version tests to chutney
  ● Made chutney more reliable and faster

Stem:

We launched a new release of Stem (1.5 645), a Python library for interacting with Tor. This is library can also be used to test Tor in different scenarios, this new release has and we were happy to have this new version that includes:

● Improved Python 3.x Performance - used to take 11420.1 seconds (190 minutes!) now it takes 14.9 seconds
● Tor Manual Information - Stem’s new stem.manual module provides programmatic access for Tor manual information.
● Fallback Directory information - Relieving load from the directory authority, Stem can retrieve information about and use tor’s fallback directory mirrors46.

45 https://blog.torproject.org/blog/stem-release-15
46 https://stem.torproject.org/api/descriptor/remote.html#stem.descriptor.remote.FallbackDirectory
Direct impact of our Testing work for the end user:

The combination of all testing resources listed above allowed us to release big features to our users with higher quality - in other words, without as many bugs in production as we would have encounter if we didn’t had the resources created with this effort.

Two main features we would like to share to help illustrate this are:

- Proposal #271\(^{47}\) - Tor’s guard selection algorithm has been redesigned from the ground up, to better support unreliable networks and restrictive sets of entry nodes, and to better resist guard-capture attacks by hostile local networks
- Proposal #220\(^{48, 49, 50}\) - Migrates server identity keys to Ed25519. Relays now use Ed25519 to prove their Ed25519 identities and to one another, and to clients. This algorithm is faster and more secure than the RSA-based handshake we’ve been doing until now.

These was a major change for Core Tor. The fact we had Chutney features to test it as well as a testing network, it allowed us to fix many bugs like memleaks and important synchronization issues with the consensus and voting schedules. Bugs that otherwise we would only learn about it once these features were already being used by our users.

We can’t emphasize how important it is to have these tests prior to building a release. For instance, it’s during this heavy development/testing period, that we have found a security issue on directory authorities. This is a super important step on Tor’s development that impacts the quality of the solution (Tor network) we are providing users who need anonymity and security online.

Project challenges

To make Chutney run faster we had to complete change it's architecture. The main challenge for such a task was the fact that while building a new architecture we still had to test Core Tor features as we were developing them. We could easily have dropped it or done a poor job with the new architecture in order to get quick solutions for the tests needs we had.

Another challenge for this goal was to make sure the quality of tests for our code. Most worryingly, it's common for contributed tests to check that the code “does exactly what it does” rather than that the code “performs its functions” and “behaves well under corner cases”.

To address this issue we invested on improving documentation, reviewing current tests and refactoring those that the quality didn’t meet our new standards. And more important, include test review on our code review process.

\(^{47}\) https://trac.torproject.org/projects/tor/ticket/19877
\(^{48}\) https://trac.torproject.org/projects/tor/ticket/15055
\(^{49}\) https://trac.torproject.org/projects/tor/ticket/15056
\(^{50}\) https://trac.torproject.org/projects/tor/ticket/15056
In order to build good practices within our team we created new routines for the developers. All the work done for this goal added more load on our developers plate as well. Not that anyone thinks this is a bad thing but now everyone is really using these testing resources to make sure their code is running on all the corner cases it can possibly cover. That means our developers are spending more time building tests, testing their code, fixing bugs and helping others in the team by reviewing their code and their tests.

At the beginning the impact of this new load of work hurt the team a little bit as people were stretched too thin. We then decided to apply some scrum techniques that would help the team better calculate its capacity while taking into account all this new load. Once we had an idea of our capacity it became easier to plan our work without overcommitting and getting overwhelmed. Because now we knew to reserve time for testing and code review into our planning.

**Enhanced outreach**

**Project objectives**

We seek to make more people aware of the benefits of Tor, especially in scenarios where censorship circumvention needs to be combined with privacy and anonymity to help civil society members work in Internet-repressive environments.

**Note:**

At first we proposed online ads as our main effort to do outreach for Tor. But later on, with the organization growth and new people coming on-board, we decided to change this strategy. We decided that Tor had to define different fronts that would help us reach out to a diverse audience. We selected 4 areas of outreach work:

- **Direct work with organizations** - this work would focus on educating organizations in order to generate a big impact on promoting Tor’s mission. This could be policies, private sector adoption, user education and security solutions adoption.
- **Outreach materials** - from t-shirts, to animations and other media materials. We decided to have a dedicated effort to generate this type of resource that could be used by anyone promoting Tor.
- **Media support** - Tor hired a Media Director for the first time. Before this project Tor never had a media strategy, with our new Media Director we could now build one and educate the media about our mission and our work.
- **Social media** - we decided was important to build our presence on social media. We rebrand our Twitter account to be more active and be a voice for Tor community.
Accomplishments

Direct work with organizations

Throughout the period of this grant we worked with over a dozen organizations, below is a summary of some of the accomplishment achieved by this work.


Tor Project met with David Kaye to help him understand Tor’s role within the Internet Freedom community in helping those who seek privacy and protection to freely express their thoughts in hostile environments. We can say that this outreach work helped with the fact his report highlighted the importance of encryption to guarantee such rights.

Amnesty International - Tanya O’Carroll

We worked with Tanya O’Carroll to integrate Tor into their curriculum and for internal use within their organization. We trained their Washington D.C. staff as well as helped them better understand how Tor works and how it can be used to guarantee human rights in hostile environments.

UK Parliament - Parliamentary Office of Science and Technology

Worked with the Parliamentary Office of Science and Technology during their research process to publish a paper about online anonymity for the UK Parliament.

---

51 https://blog.torproject.org/blog/un-special-rapporteur-anonymity-gateway-free-expression
53 https://www.opentech.fund/advisory-council/tanya-o-carroll
56 http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-488
Mozilla

Our Tor Browser team has been working with Mozilla on uplifting our patches into Firefox, this work has impacted a whole new group of users that are not necessary using Tor but is benefiting from other security work we have done, because they are not available for them.

A big way to demonstrate the impact of this work was patch that fixed a zero-day that could affect both, Tor Browser and Firefox users. In 12 hours the Tor Browser team had a patch for it that Mozilla team upstreamed and both browsers released the fix to their users57.

Facebook

Tor Project has worked with Facebook employees helping them with implementing support for their users to access Facebook using Tor. Facebook created Tor integration to their Android app making it easier for the user to have it working with Orbot (vpn app for Android that makes the connection with Tor network). Facebook also offers a .onion version of their website.

According to Facebook this works can impact around 1 million people. Their conducted a research internally and announced that 1 million users were connecting to Facebook via Tor every month.58

---

**Library Freedom Project**

During this program we partner with Library Freedom Project in many projects, from training, to user support and outreach. We would like to highlight one of the programs we partner with them and the amazing impact of it in New Hampshire community.

Library Freedom Project have an outreach program to librarians to teach about privacy online and one of the tools they suggest them to use is Tor. They also have advocate for libraries to host Tor relays and collaborate with the network bandwidth. One of the libraries they worked with, in New Hampshire, received some intimidation from law enforcement because they announced they were going to host a Tor relay.

At the end the whole community showed up at the library board meeting to speak out in favor of Tor, leading to the board vote for keeping the relay running. Another outcome of this was a bill presented59 by New Hampshire State Rep. Keith Ammon (R), with six bipartisan cosponsors. The NH HB 150835 bill60 would explicitly permit public libraries to "allow the installation and use of cryptographic privacy platforms on public library computers for library patrons use"

---

58 [https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648/](https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648/)
59 [http://boingboing.net/2016/02/20/nh-bill-would-explicitly-allow.html](http://boingboing.net/2016/02/20/nh-bill-would-explicitly-allow.html)
Outreach materials

T-shirts

The Tor Project used to have a program to send t-shirts to relay operators as a ‘thank you’ gift for being part of the Tor network. We re-organized this program and sent t-shirts to a long backlog of relay operators (over 500 t-shirts!) that were really happy when they got their ‘thank you’ gift:

We also created new swags for our ‘end of year’ crowdfunding campaigns (2015 and 2016):
Outreach videos:

Bridge and Pluggable Transports animation (over 3.7k views):
https://www.youtube.com/watch?v=DkEqWGF3cvg

Tactical Tech ‘Support Tor’ video (over 38k views):
https://www.youtube.com/watch?v=h114LK71GOo
Tor Browser User Manual

After months of hard work reviewing and updating the Tor Browser Manual, our Community Team published a new version of it61! This new version includes new screenshots, new features information and a complete revision of the language to ensure it was inclusive for all users.

Media support:

The Tor Project never had a dedicated person working with the media. In 2015 we hired our first Media Director which allowed us to develop a media strategy and build media support interaction with journalists.

Throughout the period of this grant we worked on pitching stories to journalists. We created an internal support system to prepare different members from our communities to give interviews and helped coordinate those with journalists. This effort helped diversify Tor’s public representation.

We also coordinated our own Q&A with developers6263 to explain in depth features we are building, with human rights activists that uses Tor64. And helped prepare fact sheets to help educate journalists on matters such as Tor network security or the real amount of malicious activity in the network that researchers have identified65.

---

63. https://blog.torproject.org/blog/q-and-yawning-angel
The accomplishments of this work could be seen in the articles reported over the quarters, including some from international media.

Social media

We completely revamped our social media presence. Twitter is a fast paced media and is all about the moment. We used that to engage with our supports and broader audience on topics such as:

- User education about Tor’s technology

-- ![Image](https://twitter.com/torproject/status/577889039216410625)

- Announce new features coming from Tor and other projects from the Internet Freedom community

-- ![Image](https://twitter.com/torproject/status/773862801253212160)

--- ![Image](https://twitter.com/torproject/status/236882080406073345)
Reach out to people under censorship events, letting them know how to use Tor to bypass those.

@ https://twitter.com/torproject/status/638346887230152704
Australia? Please download the Tor browser.
torproject.org

Matthew Green @matthew_d_green
Australia decides to retain all metadata at the ISP level, give it to law enforcement without a warrant. m.smh.com.au/technology/tec...

RETWEETS: 210  LIKES: 89

2https://twitter.com/torproject/status/730514181468893184
Use Orbot’s free #VPN to reach social media on Android: guardianproject.info/apps/orbot/
@enamara @frankmugisha #Uganda

- Spread information related to Tor, Internet Freedom, privacy, security and other issues that are related to Tor’s mission

71 https://twitter.com/torproject/status/786229910918475776
@Fahrenthold, the @washingtonpost reporter doing landmark journalism about Donald Trump--uses @SecureDrop, which is based on #Tor.

David Fahrenthold @Fahrenthold
There is!!! The @washingtonpost homepage has a "secure DropBox" function on the lower right. It works. I know. twitter.com/bzosiad/status…

- Live tweet events Tor’s members were participating on²²

²² https://twitter.com/torproject/status/756132428419305472
Tor’s @nickm_tor is livetweeting privacy /#anonymity research meeting #pets16 --check it out!

Nick Mathewson @nickm_tor
Now Tariq and Ryan talk about trademark infringement. They may be trolling. #pets16

- Publish statements about news events related to Tor\textsuperscript{73}

\textsuperscript{73} https://twitter.com/torproject/status/618303411071655936
Over the two years of this project we gained over 50k new Twitter followers (went from 98k to 184k). Our tweets get millions of impressions and many of them have received hundreds of engagement (retweet or likes).

We also verified both of our accounts (official English one and a Farsi focused account):
Challenges

As we changed the work proposed under this objective to something more holistic that cover outreach to our users, media education and partnership with organizations.

In order to do that we created a Community Team to focus on building outreach materials such as t-shirts, educational videos and manuals to our users.

Some of the challenges faced by this team was to re-engage our relay operators volunteers with the Tor Community. To do that they resurrected our t-shirts program, a reward to our volunteers that they really appreciate.

On user education one of our big challenges was to re-engage users who have tried to download and use Tor unsuccessfully in the past, as well as teach new users about Tor. To do that they created educational videos and Tor Browser manual. They also used our Twitter presence to promote these materials and reach out to users, specially during censorship events which are the moments our users needs our tools the most.

Since this was a relative new team, they faced the challenge of doing all this work while building the team. One could say that they had “to sail while building the boat”. But they overcome it very well and now we have a very strong Community Team that is in full engagement with our users and volunteers.
For media support part, we faced the challenge to educate reporters on the complexity of Tor’s technologies and solutions as well as the diversity of its usage around the world. In order to solve this problem we decided to: use our blog as a tool to help journalists understand new features we are working on by publishing Q&A with developers that covered questions the media would not have asked if they just saw the announcement for the feature. We also built a relationship with journalists and acted more pro-active with them by pitching them stories and presenting them members of our community that they might be interest in interviewing or writing a story about their work.