The Tor Project:

7th QUARTER OF PROJECT, Q3 OF THE YEAR: July 1, 2016 – September 30, 2016

<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>

Q3 project timeline (July 1, 2016 – September 30, 2016): activity summary

Pluggable transport integration

Project objectives

Outputs for the quarter

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

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

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

Challenges

Testing and network simulation improvements

Project objectives

Outputs for the quarter

Challenges

Enhanced outreach
Project objectives

Outputs for the quarter

Direct work with organizations

Outreach materials

Media strategy:

Social media

Community promotion:

Challenges

Press

Finalizing activities - project retrospective session - final report.

Q3 project timeline (July 1, 2016 - September 30, 2016): activity summary

Pluggable transport integration

Project objectives

The goal of this project 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 "plug in" new transports as needed; plus, 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 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 Tor frameworks to do relevant research.

Basket2: finished the documentation and remaining development tasks. We are planning for the adoption and rollout process of this new PT into our clients in 2017.

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

- Tor 0.2.8.8 - 2016-09-23
  - Fix a complicated crash bug that could affect Tor clients configured to use bridges when replacing a networkstatus consensus in which one of their bridges was mentioned. OpenBSD users saw more crashes here, but all platforms were potentially affected. Fixes bug 20103; bugfix on 0.2.8.2-alpha.

- Tor 0.2.8.6
  - Avoid reporting a spurious error when we decide that we don’t need to terminate a pluggable transport because it has already exited. Fixes bug 18686; bugfix on 0.2.5.5-alpha.

- Tor 0.2.8.7 - 2016-08-24
  - The "Tonga" bridge authority has been retired; the new bridge authority is "Bifrost". Closes tickets 19728 and 19690.

- Tor Browser 6.5a2-hardened is released
  - Bug 19714: Remove mercurius4 obfs4 bridge

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

As we mentioned last quarter, we released a new "Fallback directories" design as a big feature for Tor 0.2.8. We worked with relay operators, contacting them directly to update to this release and to collect their feedback/bug reports. This is a new feature to help fight censorship.

Challenges

Right now we are discussing internally how to move forward with this initiative in 2017. We need a dedicated person to lead this effort and drive coordination with the rest of the community. The challenge for us has been capacity. The team is stretched too thin on many fronts, which is not ideal. We need to recruit more people and delegate community organizing work in order to succeed on this initiative.

1 https://blog.torproject.org/blog/tor-0288-released-important-fixes
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.

Outputs for the quarter

Over the quarter, we continued to test new and old code, which is something we have been doing more systematically with this project. We have even seen more and more volunteers following the good practices we put in place over the last two years. This increases the quality of work overall.

This effort has been quite successful. But out of our success, we have some new challenges. Tests that we write for the code we create won't fully catch every edge case that might be encountered in the wild. Therefore, we also spent a lot of effort this quarter creating a testing network for the team, as well as a way to test our code in an environment that is closer to what it will encounter in the production environment.

Finally, we made a call for help to test our alpha releases, and we got a great response from the community. People not only tested and reported bugs, but they also gave us great feedback in the process. We plan to continue with calls every release and drive these volunteers to our tor-qa mailing list for better coordination, not only between volunteers but with our Applications and Network development teams, as well.

Test coverage:

There was a big effort in July when we merged the Shared Random subsystem into the Tor 0.2.9 release. As we added a big chunk of new code, we also added 90%+ code coverage of unit test. The screenshot below shows coverage statistics for both files: shared_random.c and shared_random_state.c

![Coverage screenshot](https://trac.torproject.org/projects/tor/ticket/16943)

![Coverage screenshot](https://people.torproject.org/%7Enickm/tor-auto/coverage/cov-full_html/or/index.html)
Another huge effort was the implementation of HSDir support\(^4\) as part of Proposal 224. Here is the test coverage statistic for this effort:

<table>
<thead>
<tr>
<th></th>
<th>Hit</th>
<th>Total</th>
<th>Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lines</td>
<td>674</td>
<td>747</td>
<td>90.2%</td>
</tr>
<tr>
<td>Functions</td>
<td>36</td>
<td>37</td>
<td>97.3%</td>
</tr>
</tbody>
</table>

**Testing Network:**

As we mentioned above, applying tests to our code alone would not cover all possible edge cases we might encounter when our code is released into production and is running on different OSs, hardware and configurations. Therefore, we decided to work on an effort to create a testing network, which we are calling “testnet.”

**Composition:**

Sixteen Tor relays, run by nine different people, collaborated on the testnet initiative. We have set up metrics tools CollecTor, Atlas, Onionoo and Consensus Health on testnet, so we can monitor the network.

This network is completely private, and all of these services are password protected. We don’t want the nodes in this network to become known, which could result in people starting to use it, which we strongly want to avoid since it’s for testing only.

We also have a private git repository on testnet that contains our torrc files and some needed internal documentation. We are in the process of creating a public git repository that would contain public tools and scripts we would use in the testnet that can be shared. The only part we won’t make public is the identity of the nodes in the testnet.

**Success stories:**

Shared random is a big success story that illustrates using this network to test how a big feature would act in production. This test exposed bugs, such as memleaks and important synchronization issues with the consensus and voting schedules. Some of these issues were entered into our ticket system,\(^5\) while some were fixed right away while the team was in a heavy development/testing phase.

We can’t emphasize how important it was to do this prior to building a release. Good practices like this can ensure better quality to the code before being released. For instance, during this heavy development/testing period, we even found a security issue on directory authorities.

---

\(^4\) [https://trac.torproject.org/projects/tor/ticket/17238](https://trac.torproject.org/projects/tor/ticket/17238)

By using our testnet, we can ensure that our users will be safer when relay operators update to a new release.

Other types of tests and/or use cases:

- Proposal 224 - use testnet to stabilize things.
- Test consensus methods 22, 23, 24, 25, and soon 26 before they were activated on the public network:
  - 22 MIN_METHOD_FOR_ED25519_ID_VOTING
  - 23 MIN_METHOD_FOR_SHAREDRANDOM
  - 24 MIN_METHOD_FOR_EXCLUDINGINVALID_NODES
  - 25 MIN_METHOD_FOR_RECOMMENDED_PROTOCOLS / MIN_METHOD_FOR_RS_PROTOCOLS
  - 26 MIN_METHOD_FOR_INIT_BW_WEIGHTS_ONE
- We're also trying to test bandwidth authorities. In both the current and proposed implementations, for instance, we are proposing modifications for upcoming contracts where we will work on features to improve low-bandwidth (i.e., mobile, etc.) user experiences. We will be able to use testnet to test those modifications, as well.
- We also started to use testnet to ramp up operators who want to become directory authorities in the real network. We have them running their nodes on testnet right now.

Chutney:

We also worked on new features for our testing tool, chutney:

- 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

Challenges

Although the team did great work over the quarter, going above and beyond in setting up testing and ensuring the quality of the code they released, the team also experienced some challenges in that many times the developers were stretched too thin.

We discussed these problems during the Tor Meeting in September, and we hosted sessions about technical hiring and discussions about what areas we could use more help with to define the roles and responsibilities of possible new additions to the team.
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.

Outputs for the quarter

Direct work with organizations

Mozilla - Tor uplifting

We are working closely with Mozilla to help them apply Tor security features to the Firefox browser. Members of the Mozilla team joined us at our Tor Meeting in Seattle last September as part of this effort to increase collaboration between both browsers. Bringing more security features from Tor Browser to Firefox will impact millions of users who are seeking a more secure way to browse the Internet.

You can track this project here:

https://wiki.mozilla.org/Security/Tor_Uplift/Tracking

Quote from GHacks.net:

"Mozilla works on uplifting privacy settings of the Tor browser project to the Firefox web browser to provide privacy conscious users with additional privacy-related options."

Tor Social Contract:

The Tor Project is home to a very diverse and complex community. Following up from our Mission Statement published last year, this quarter we published our Social Contract7, a set of principles that shows who we are and what it means to be part of this community. This contract aims to protect our users and got really great feedback from the public and from the media,8 which highlighted our “no backdoors” pledge in many articles.

---

6 http://www.ghacks.net/2016/07/04/tor-privacy-settings-coming-to-firefox/
7 https://blog.torproject.org/blog/tor-social-contract
8 http://boingboing.net/2016/08/12/the-tor-projects-social-cont.html
Outreach materials

Video and other visuals:

We finally published our video⁹ on Pluggable Transports and Bridges!

---

⁹ https://www.youtube.com/watch?v=DkEqWGF3cvg
The accompanying blog post\textsuperscript{10} also shares other education materials (mentioned in last quarter’s report). This post is a great explanation of how to bypass censorship against Tor. Most recently, it was highlighted in an article related to online censorship in Turkey\textsuperscript{11}:

\textbf{Turks Are Flocking to Tor After Government Orders Block of Anti-Censorship Tools}

November 7, 2016 // 03:03 PM EST

\textbf{Rapid response program:}

\textsuperscript{10} https://blog.torproject.org/blog/breaking-through-censorship-barriers-even-when-tor-blocked
On our Community Team wiki, we documented our new rapid response program, which organizes visual materials, call to action phrases, and translations in an effort to be prepared for cases of censorship online. Our rapid response program will enable us to respond to threats and reach out to people in their own language with educational materials that teach them how to use our tools to bypass censorship.

Once this work is finalized, our goal is to share information we collect with other rapid response programs, so they can leverage this resource, as well. We also plan to join these other initiatives to share information on censorship actions we might detect to alert them so they can take action.

Media strategy:

This quarter we tried to work with different media to promote information about different use cases of the Tor Network, its components and its clients. We want to popularize Tor and the idea of privacy and security, and the best way to do that is by exposing the many use cases for our tools. For this quarter we want to highlight articles that talk about them such as:

**The Guardian** - Tor is suggested in The Guardian’s guide for digital privacy.

Quote:

"*For the ultimate in security, consider using the Tor web browser*"

---

13 [https://pad.riseup.net/p/RapidResponseProgram](https://pad.riseup.net/p/RapidResponseProgram)
The Intercept highlighted a prototype created by Nathan Freitas from the Guardian Project. Nathan was able to create a baby monitor that uses .onion services by using a raspberry PI, an Android client, and Home Assistant, an open source platform built on Python.

Slides from the Guardian Project

DIRECT CONNECT (BAD)

You connect to Your Thing via Direct Internet Address Through Open Firewall Port (usually without encryption and often with default passwords)

CLOUD SYNC (MORE SECURE, LESS PRIVATE)

You connect to Your Thing through a Cloud Service (which then knows all, remembers all, and happily shares and/or monetizes all)
TechCrunch\textsuperscript{15} - TechCrunch mentioned Tor in its guide on “How to circumvent Turkey’s social media block.”

\textsuperscript{15} https://techcrunch.com/2016/07/15/circumvent-social-media-block/
Social media

Promotion of use cases for Tor:

We tweeted and publicized\(^{16}\) the Guardian Project's work on: “Simple Guide to Tor and the Internet of Things,” which garnered a lot of attention from the media and the industry:

\(^{16}\) [https://twitter.com/torproject/status/755926833401507840](https://twitter.com/torproject/status/755926833401507840)
[https://twitter.com/torproject/status/75588215058336960](https://twitter.com/torproject/status/75588215058336960)
[https://twitter.com/torproject/status/755930620312719360](https://twitter.com/torproject/status/755930620312719360)
[https://twitter.com/torproject/status/755938384166653953](https://twitter.com/torproject/status/755938384166653953)
We tweeted and publicized our new educational materials on how to bypass censorship against Tor. Here is a tweet with our animated gif:\footnote{https://twitter.com/torproject/status/754035172350144512}:
We tweeted about an article in Motherboard about how a Department of Justice official told federal judges to use Tor\textsuperscript{18}.

\textsuperscript{18} https://twitter.com/torproject/status/762002127115911169

Rapid response:
We sent tweets targeting people in Turkey\textsuperscript{19} when they were under heavy Internet censorship attacks\textsuperscript{20} by their government.

Celebrating our community:

We tweeted about Iran Free Software Day & Tor support\textsuperscript{21}:

\begin{itemize}
\item \url{https://twitter.com/torproject/status/754060068069318658}
\item \url{https://twitter.com/torproject/status/754259071629426688}
\item \url{https://twitter.com/torproject/status/781505588597362688}
\end{itemize}
We tweeted appreciation for our relay operators!\(^{22}\)

\(^{22}\) [Link to Twitter tweet](https://twitter.com/torproject/status/779139674363142144)
Challenges

The team conducting this work was also quite busy dealing with internal changes at The Tor Project. During this quarter, we had to balance our workload while ensuring internal support for the community. In general, the team did a great job of remaining organized and focused while overcoming these challenges.

Press

<table>
<thead>
<tr>
<th>Date Published</th>
<th>Media Outlet</th>
<th>Article Title</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/16/2016</td>
<td>CNN</td>
<td>This African country is taking an unprecedented step in internet censorship</td>
<td>Suggests Tor as a tool to use to bypass Internet censorship during Gabon’s elections.</td>
</tr>
<tr>
<td>09/10/2016</td>
<td>The Merkle</td>
<td>Tor Developers Are Preparing For The Next Generation of Cyberattacks</td>
<td>Talks about challenges faced by Tor to ensure user security.</td>
</tr>
<tr>
<td>09/19/2016</td>
<td>The Guardian</td>
<td>How to contact the Guardian securely</td>
<td>The Guardian newspaper published a help guide for sources who want to contact</td>
</tr>
<tr>
<td>Date</td>
<td>Source</td>
<td>Title/Content</td>
<td>Summary</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>08/31/2016</td>
<td>ArsTechnica</td>
<td>Building a new Tor that can resist next-generation state surveillance</td>
<td>Talks about our plans to build the next generation of .onion services.</td>
</tr>
<tr>
<td>08/26/2016</td>
<td>The Merkle</td>
<td>DOJ’s Ovie Carroll: “Tor Helps Protect Sensitive User Information”</td>
<td>Talks about the recommendation from DOJ for judges to use Tor.</td>
</tr>
<tr>
<td>08/10/2016</td>
<td>TechCrunch</td>
<td>Tor’s new social contract includes ‘no backdoors’ pledge</td>
<td>Talks about our social contract, highlighting our ‘no-backdoors pledge’.</td>
</tr>
<tr>
<td>08/11/2016</td>
<td>The Inquirer</td>
<td>Tor creates ‘social contract’ promising never to harm users</td>
<td>Another article highlighting our social contract and our pledge to protect our users.</td>
</tr>
<tr>
<td>08/12/2016</td>
<td>BoingBoing</td>
<td>Tor Project Social Contract</td>
<td>Talks about our social contract and how it protects users.</td>
</tr>
<tr>
<td>08/04/2016</td>
<td>Softpedia</td>
<td>Tor Project 0.2.8.6 Improves Client Bootstrapping Performance, Linux Security</td>
<td>Talks about our new release and improvements on client bootstrapping.</td>
</tr>
<tr>
<td>08/06/2016</td>
<td>MotherBoard</td>
<td>Department of Justice Official Tells Hundred Federal Judges to Use Tor</td>
<td>Quote: Ovie Carroll, director for the Cybercrime Lab at the Department of Justice, urged the judges to “use the TOR [sic] network to protect their personal information on their computers, like work or home computers, against data breaches, and the like,”</td>
</tr>
<tr>
<td>07/07/2016</td>
<td><a href="http://www.htxt.co.za/">http://www.htxt.co.za/</a></td>
<td>Make it harder for the gov’t to track your #ShutdownZimbabwe2016 messages</td>
<td>Article mentions Tor Browser and Orbot as tools activists should use while participating in the #ShutDownZimbabwe2016 campaign</td>
</tr>
<tr>
<td>07/05/2016</td>
<td>The Inquirer</td>
<td>Mozilla ups Firefox privacy ante with Tor injection</td>
<td>Reports on collaboration between Mozilla and Tor to bring Tor Browser features to Firefox</td>
</tr>
</tbody>
</table>
## Finalizing activities - project retrospective session - final report.

During this last month, we plan to focus on finalizing the activities in these three areas of work:

- Pluggable Transport integration
- Testing and network simulation improvements
- Enhanced outreach

Once we have finalized all activities, we hope to conduct a retrospective with the teams that worked on the project to assess the overall performance while executing the project, including our difficulties, our successes, our mistakes, etc., so we can use what we’ve learned in future projects.