January 11, 2011

Proposal for BBG

Kelly and Ken,

We offer a menu of items from which you can choose to further fund Tor research, development, and deployment over the next year. Rather than write a 10-15 page document of dense, academic text more thoroughly explaining every option, we feel this menu-like set of choices is better aligned to our relationship. Of course, we're happy to expand upon, and answer questions about, any of the items listed below.

1. Implement methods to reduce Tor directory overhead for Tor servers during bootstrapping and maintenance to better support users on low bandwidth connections, by means of Tor proposal 158 ("microdescriptors") or other methods as required. R&D $75k
2. Develop and implement changes to the Tor software to reduce the impact of high data volume circuits on the performance of low data volume circuits by dynamically prioritizing writing of data for low volume circuits to the network, thus squeezing the bandwidth of high volume circuits slightly. R&D $100k
3. Enhance the existing Tor Weather service to provide better support for Tor relay operators on the status and functioning of their Tor server, with flexible levels of notification and notification time frames which can be customized by each user. Additionally, notify Tor relay operators of the availability of the Tor Weather service and advocate for its use with more prominent information, documentation, and links to the subscription service in the Tor web pages and software. R&D $30k
4. Develop and implement a new method to balance traffic over the available bandwidth as provided by the Tor relays, to overcome the problem in the current traffic balancing algorithm which causes fast Tor relays to end up with less load than slow relays. The goal of this revised traffic balancing algorithm should be to reduce latency on Tor circuits as much as possible. R&D $80k
5. Bridge relay and bridge directory authority mechanisms and generally improving Tor for the target environments. Part of this work is to turn users into bridges by default, pending them passing some reachability tests and prompting the user for approval. The full proposal, and subsequent discussion, can be read at `http://archives.seul.org/or/dev/Mar-2010/msg00028.html` R&D $100k
6. Research and document additional options for the scalability of the Tor network beyond 2 million concurrent users, including analysis of splitting the network into multiple segments, switching to datagram-based protocols, and improving the load balancing within the network. R&D $100k

7. Continue research and potential deployment of relay incentives system. Research $30k

8. Research, develop, and deploy more reliable download mechanisms for users on slow and/or unreliable network connections, by means of a split download of multiple smaller files, implementation of a lightweight download manager, reduction in software bundle file size, secure updater, network installer, or other methods as feasible. Research and deployment $60k

9. Enhance and develop Tor Browser Bundle on Windows, Apple OS X, and GNU/Linux environments. Evaluate trace footprint on all operating systems for which Tor Browser Bundle is released. Research and deployment $60k.

10. Enhance and maintain a Web-based portal to manage translations. Investigate integration with machine learning or automated translation systems to reduce the quantity of text required to be translated by a human. Research and deployment $20k. Maintenance and improvements $20k.

11. Develop and implement improvements to the bridge relay and bridge directory authority mechanisms to improve usability, performance, and reliability of the Tor network by users in countries with government-imposed Internet censorship. R&D $80k

12. Develop and deploy a customized version of Tor Browser Bundle, complete with native language translations, applicable bookmarks, and relevant start page for target audiences. $60k.

13. Research, Develop, and deploy a secured, anonymity-preserving operating system designed to run from cd-rom, dvd-rom, or usb drives. R&D $75k. Deployment & Maintenance $30k.

14. Enhance Tor Browser Bundle with free software Adobe Flash implementation called Gnash (`http://www.gnashdev.org`). This enhancement will allow for safe, anonymity-preserving viewing and using of Flash videos and applications. R&D $50k.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: July 9, 2010

This report documents progress in June 2010 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

- On June 1, we released the latest Tor Browser Bundle for Linux, version 1.0.7. This is a compatibility release to allow the bundle to work on a wider variety of Linux distributions.
- On June 2, updated the Vidalia bundle for OS X PowerPC to include Vidalia 0.2.9.
- On June 14, we released orbot 0.0.8. This is a maintenance release to fix issues discovered with Android 2.2.
- On June 17, Tor and the EFF released a Firefox extension called HTTP Everywhere. The goal is to enable encrypted website viewing by default. More about this release at `https://blog.torproject.org/blog/https-everywhere-firefox-addon-helps-you-encrypt-web-traffic`.
- Damian continues to improve and release new versions of ARM, the console-based anonymizing relay monitor, `http://www.atagar.com/arm/`. Consider it to be like the graphical control application, Vidalia, for relays without a graphical environment.

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

- We updated the geoip mapping database to the Maxmind GeoLite Country database in tor after an analysis of various geoip mapping databases. The Maxmind GeoLite Country database has more accurate mappings for many parts of the world, such as Iran, SouthEast Asia, and many African countries.
- We added an eigth directory authority called “maatuska“ hosted by NORDUNet in Sweden.
- China's Great Firewall continues blocking connections to the public Tor relays. They also updated their blocking to include bridge relays published via email and https websites. We conducted further research into the blocking mechanisms from inside China. A detailed analysis shows China GFW is blocking 90% of the published bridges in the https and smtp pools. The blocking is simply IP Address and TCP port combinations. Bridge relays that have

been seeded into various social networks in China as well as new bridge addresses continue to work well.

- In late June, we started receiving many reports that Nigerian internet providers are blocking many circumvention tools, Tor included. Data about the blocking methods implemented are sparse right now, but we're continuing to work with a few smart Nigerians to reverse-engineer the blocking regime. More details about this block at `https://blog.torproject.org/blog/dear-nigerians-help-us-help-you`.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

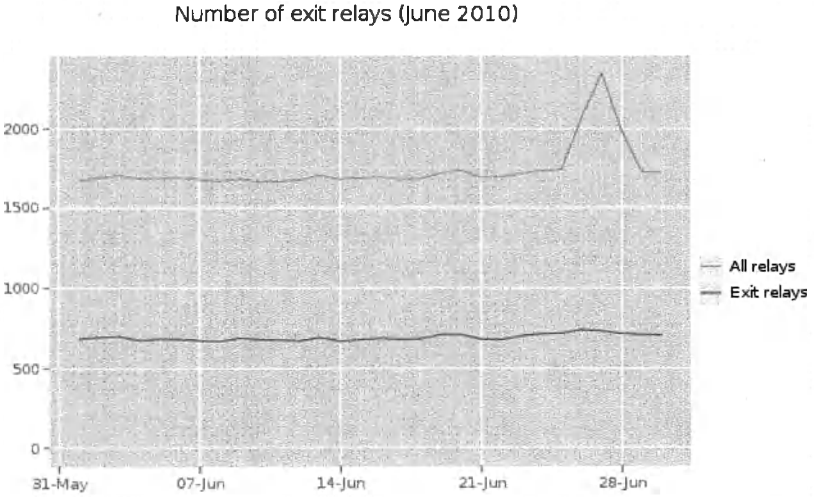
Nothing to report.

C.2.5. Hide Tor's network signature.

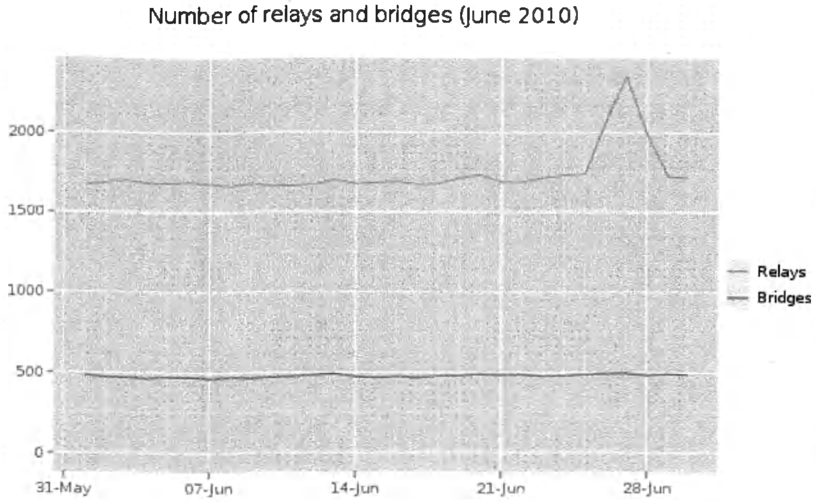
Nothing to report.

C.2.10 Grow the Tor network and user base. Outreach.

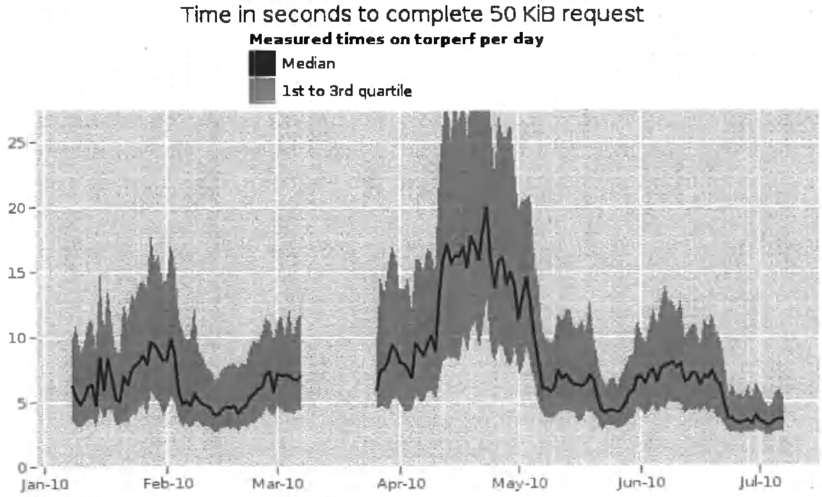
Measures of the Tor Network



This graph shows the total quantity of relays and quantity of exit relays in june 2010. Exit relay capacity is one of the potential bottlenecks that affects the overall performance of Tor. The more exit relays we have, the faster it seems to browse the open Internet. As seen in late June, a researcher using PlanetLab hooked up 512 relays to the Tor network for their research into cloud computing and scaling effects on the Tor Network. Before contacting PlanetLab, we removed all 512 nodes from the network consensus so users couldn't use the suspect relays. We contacted the researcher and the relays were subsequently disabled.



This graph shows the total quantity of relays and the total quantity of bridges in June 2010. The quantity of bridges is stable throughout the month. As seen in late June, a researcher using PlanetLab hooked up 512 relays to the Tor network for their research into cloud computing and scaling effects on the Tor Network. Before contacting PlanetLab, we removed all 512 nodes from the network consensus so users couldn't use the suspect relays. We contacted the researcher and the relays were subsequently disabled.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This measurement is from the server torperf, located in Chicago, Illinois. As you can see, latency dropped dramatically over the month for the second month in a row. We believe this is due to the fixes for relays in 0.2.1.26 allow relays to handle older clients flooding circuit requests to relays. As some relays were overloaded and dropped out of the network, the remaining relays had to handle an increasing load of users. Also, we have a budding competition between individuals looking to run the highest bandwidth relays. TorServersdotNet, `http://www.torservers.net/`, starting running some very high bandwidth relays to increase performance and provide a way for non-technical users to support tor through combined financial donations in exchange for Tor servers. We're also looking to run this measurement software on a linux client connected to a standard dial-up modem to see how Tor fares in extremely low-bandwidth environments.

Outreach and Advocacy

- Andrew met with the Wesleyan University Humantarian Free and Open Source Software (HFOSS) team working on Tor for their summer project. They are fixing up the Tor Weather application to allow for more features as requested by relay operators and attempting a start a Tor Status re-write, design, and update. `http://hfoss.wesleyan.edu/`.
- Jacob attended FooCamp 2010.
- Mike, along with Peter Eckersley from EFF, met with the Mozilla team to talk about web fingerprinting, privacy, and Torbutton. Mike's summary of their discussion is at `https://blog.torproject.org/blog/firefox-private-browsing-mode-torbutton-and-fingerprinting`.
- Sebastian and Linus gave a Tor talk to the Netherlands Privacy group, PvIB (`https://www.pvib.nl/home`). Their presentation is at `https://svn.torproject.org/svn/projects/presentations/pvib-2.pdf`.
- Runa gave a Tor talk to Electronic Frontier Norway, `http://www.efn.no/`.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

Erinn continues to work on a Tor Browser Bundle for Apple's OS X. Erinn continues to improve Tor Browser Bundle for Linux with feedback from initial users and other volunteer developers.

C.2.12 Bridge relay and bridge authority work.

Andrew published a template configuration file for tor relays to be a bridge automatically. It seems some relay operators are confused as to configuring their relay as a bridge. The configuration template is at `https://gitweb.torproject.org/tor.git/blob_plain/HEAD:/src/config/torrc.bridge.in` and will be included in future Tor releases.

Andrew created some experimental "bridge by default" bundles for Microsoft Windows. The idea is to use existing technology and see if we can get users to be bridges by default without any additional configuration. Intitial testing shows it works well if the upstream router or NAT device has Universal Plug and Play (UPNP) enabled. The largest obstacle is still the manual configuration of firewalls, routers, and NAT devices if UPNP is not enabled by default. More details about this experiment are at `https://blog.torproject.org/blog/technology-preview-bridge-default-microsoft-windows-clients`.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

Mike spent a lot of effort and research into optimizing the circuit based timing (CBT) codebase. CBT is how clients measure the performance of their tor circuits to better optimize performance. The changelog of the fixes is:

- Major bugfixes:
  - Ignore negative and large timeout values that can happen during a suspend or hibernate. These values caused various asserts to fire in the circuit build times code, crashing Tor. Bug 1245, bugfix on 0.2.2.2-alpha.
  - Alter calculation of Pareto distribution parameter 'Xm' for Circuit Build Timeout learning to use the weighted average of the top N=3 modes. This should improve the timeout calculation in some cases, and prevent extremely high timeout values. Bug 1335, bugfix on 0.2.2.2-alpha.
  - Implement a filtering step to recompute synthetic build times every time the timeout changes. Additionally, place a lower cap on synthetic build times, and allow this cap to be controlled by the consensus. This should also improve the build time calculations, and should eliminate a case where Tor was allocating an excessive amount of temporary memory during timeout calculation. Bugs 1335 and 1245, bugfix on 0.2.2.2-alpha.
- Minor bugfixes:
  - Eliminate a case where a circuit build time warning was displayed after network connectivity resumed.
- Minor features:
  - Add a

    ```
    TIMEOUT_RATE
    ```

    keyword to the

    ```
    BUILDTIMEOUT_SET
    ```

    control port event, to give information on the current rate of circuit timeouts over our stored history.
  - Add ability to disable circuit build time learning via consensus parameter and via a LearnCircuitBuildTimeout config option. Also automatically disable circuit build time calculation if we are either a AuthoritativeDirectory, or if we fail to write our state file. Bug 1296.

Karsten web-enabled his ExoneraTor tool on the metrics website at `http://metrics.torproject.org/exonerator.html`. ExoneraTor tells you whether there was a Tor relay running on a given IP address at a given time. Many legal advisors, lawyers, and law enforcement ask us for data regarding if a certain IP address hosted a Tor relay at a point in time. Now this data is easily available to all.

Karsten fixed stats on estimated user numbers after we broke the calculations of users from directory request sampling at select relays. We found that we can use entry-stats for better user number estimates.

Karsten compared descriptor tarballs collected by ernie with directory-archive script and found that we're fine using ernie's data. Ernie is the code that provides the data processing and backend for the metrics.torproject.org website.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Nothing to report.

C.2.16. Footprints from Tor Browser Bundle.

Erinn continues work on footprints of the Tor Browser Bundle for Linux and Apple OS X.

C.2.17 Translation work, ultimately a browser-based approach.

- A new translator, pierre, translated the entire website, torbutton, and gettor email autoresponder into French.
- Added pashto (Pakistani) to the portal by request.
- Updated translations for the website, torbutton, orbot, tor, and tor manual pages for French, Spanish, Russian, Mandarin Chinese, Farsi, Italian, Arabic, Dutch, Serbian, Portugese, Danish, Japanese, Polish, and Turkish.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: April 12, 2010

This report documents progress in March 2010 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

1. On March 7th, we released the latest in the -alpha series, Tor 0.2.2.10-alpha. Tor 0.2.2.10-alpha fixes a regression introduced in 0.2.2.9-alpha that could prevent relays from guessing their IP address correctly. It also starts the groundwork for another client-side performance boost, since currently we're not making efficient use of relays that have both the Guard flag and the Exit flag.

```
o Major bugfixes:
  - Fix a regression from our patch for bug 1244 that caused relays
    to guess their IP address incorrectly if they didn't set Address
    in their torrc and/or their address fails to resolve. Bugfix on
    0.2.2.9-alpha; fixes bug 1269.

o Major features (performance):
  - Directory authorities now compute consensus weightings that instruct
    clients how to weight relays flagged as Guard, Exit, Guard+Exit,
    and no flag. Clients that use these weightings will distribute
    network load more evenly across these different relay types. The
    weightings are in the consensus so we can change them globally in
    the future. Extra thanks to "outofwords" for finding some nasty
    security bugs in the first implementation of this feature.

o Minor features (performance):
  - Always perform router selections using weighted relay bandwidth,
    even if we don't need a high capacity circuit at the time. Non-fast
    circuits now only differ from fast ones in that they can use relays
    not marked with the Fast flag. This "feature" could turn out to
    be a horrible bug; we should investigate more before it goes into
    a stable release.

o Minor features:
  - Allow disabling building of the manpages. Skipping the manpage
    speeds up the build considerably.

o Minor bugfixes (on 0.2.2.x):
  - Fix a memleak in the EXTENDCIRCUIT logic. Spotted by coverity.
    Bugfix on 0.2.2.9-alpha.
  - Disallow values larger than INT32_MAX for PerConnBWRate|Burst
    config option. Bugfix on 0.2.2.7-alpha.
  - Ship the asciidoc-helper file in the tarball, so that people can
    build from source if they want to, and touching the .1.txt files
    doesn't break the build. Bugfix on 0.2.2.9-alpha.

o Minor bugfixes (on 0.2.1.x or earlier):
  - Fix a dereference-then-NULL-check sequence when publishing
    descriptors. Bugfix on 0.2.1.5-alpha. Discovered by ekir; fixes
    bug 1255.
  - Fix another dereference-then-NULL-check sequence. Bugfix on
    0.2.1.14-rc. Discovered by ekir; fixes bug 1256.
  - Make sure we treat potentially not NUL-terminated strings correctly.
    Bugfix on 0.1.1.13-alpha. Discovered by rieo; fixes bug 1257.

o Code simplifications and refactoring:
  - Fix some urls in the exit notice file and make it XHTML1.1 strict
    compliant. Based on a patch from Christian Kujau.
  - Don't use sed in asciidoc-helper anymore.
  - Make the build process fail if asciidoc cannot be found and
    building with asciidoc isn't disabled.
```

2. On March 15, we released the latest in the -stable series, Tor 0.2.1.25-stable.

```
o Major bugfixes:
  - Fix a regression from our patch for bug 1244 that caused relays
    to guess their IP address incorrectly if they didn't set Address
    in their torrc and/or their address fails to resolve. Bugfix on
    0.2.1.23; fixes bug 1269.
  - When freeing a session key, zero it out completely. We only zeroed
    the first ptrsize bytes. Bugfix on 0.0.2pre8. Discovered and
    patched by ekir. Fixes bug 1254.

o Minor bugfixes:
  - Fix a dereference-then-NULL-check sequence when publishing
    descriptors. Bugfix on 0.2.1.5-alpha. Discovered by ekir; fixes
    bug 1255.
  - Fix another dereference-then-NULL-check sequence. Bugfix on
    0.2.1.14-rc. Discovered by ekir; fixes bug 1256.
  - Make sure we treat potentially not NUL-terminated strings correctly.
    Bugfix on 0.1.1.13-alpha. Discovered by rieo; fixes bug 1257.
```

3. On March 26 we released the first beta of a Tor Browser Bundle for GNU/Linux operating systems. It is now available for x86 and x86_64 architectures in 12 languages.

```
The bundle comes with the following software:
    * Tor 0.2.2.10-alpha
    * Vidalia 0.2.7 -- cross-platform controller GUI for the Tor software
    * Polipo 1.0.4.1 -- caching web proxy
    * Firefox 3.5.8 -- web browser
    * Torbutton 1.2.4 -- Firefox extension to enable or disable the browser's use of Tor
    * NoScript 1.9.9.57 -- Firefox extension to only allow scripts from trusted sites
    * BetterPrivacy 1.4.7 -- Firefox extension to protect against supercookies
```

Orbot for Android, or Tor on Android.

The Tor Project has been working very closely with Nathan Freitas and The Guardian Project to create an Android release. This is an early beta release and is not yet suitable for high security needs. The Android web browser is not protected by Torbutton and we have not yet developed an anonymous browser on the Android platform. Please be cautious with this release–it's probably pretty fragile and it's certainly not ready for serious use.

We've codenamed the Tor on Android project Orbot; Orbot is a single Android package that provides a new Tor controller, Privoxy as our trusty little HTTP proxy, libevent, and Tor itself. This Android package is using the C reference implementation of Tor. Orbot should be orders of magnitude safer than other Tor implementations on Android and it's our official release. Everything you'll need for using Tor is in the package. Orbot 0.0.4 is the first public release. Orbot includes:

```
* Tor 0.2.2.9-alpha
* A native Android control graphical interface
* Privoxy compiled for Android
```

March 11 we released Orbot 0.0.5 for Android phones. It fixes a number of bugs in the graphical control interface and updated Tor to 0.2.2.10-alpha.

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

We worked with activists in Iran and China to determine what relays were blocked, if any, by national firewall apparatus. Iran is not blocking Tor relays at all. China is blocking most public relays, and appears to have crawled the bridge address website in order to block those bridges. There were 4121 requests in a 6 hour period from seemingly unique gmail accounts for bridge addresses via email. However, we cannot attribute this to anything other than users requesting bridges. It is possible this was an attempt to enumerate all bridges available via email. Our twitter and qq distribution methods remain under utilized.

Implemented graphs of packages served by our get-tor email autoresponder. You can see them at `http://metrics.torproject.org/gettor-graphs.html`.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

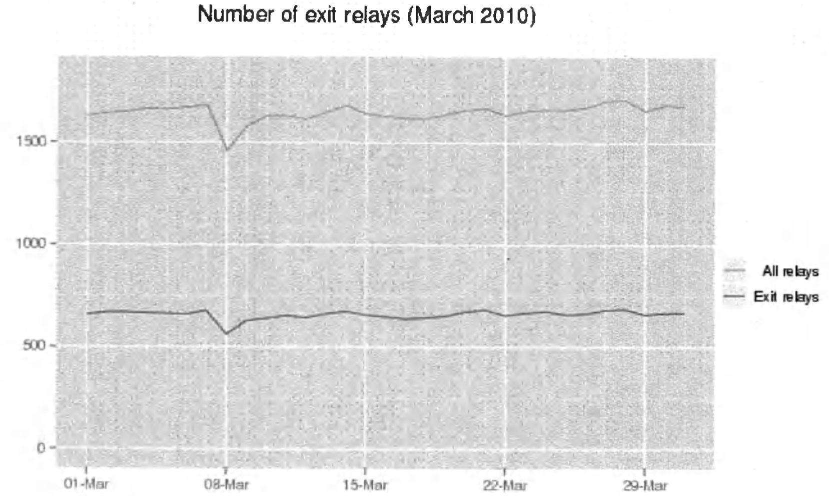
Nothing to report.

C.2.5. Hide Tor's network signature.

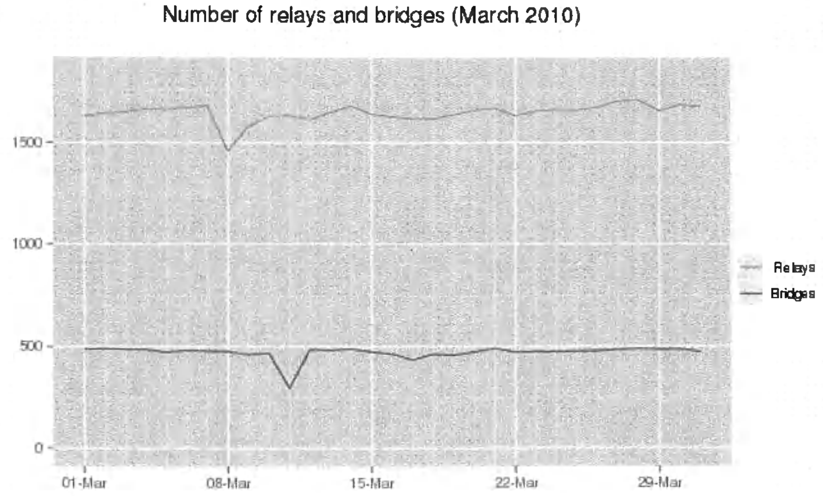
Nothing to report.

C.2.10 Grow the Tor network and user base. Outreach.

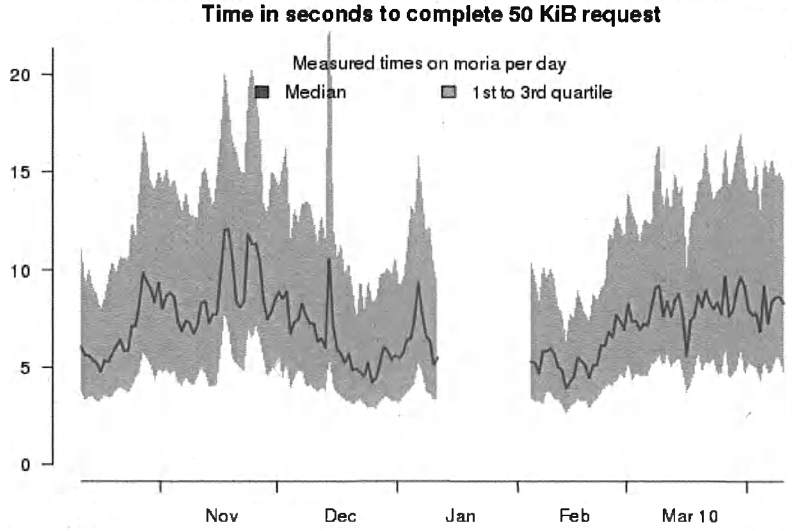
Measures of the Tor Network



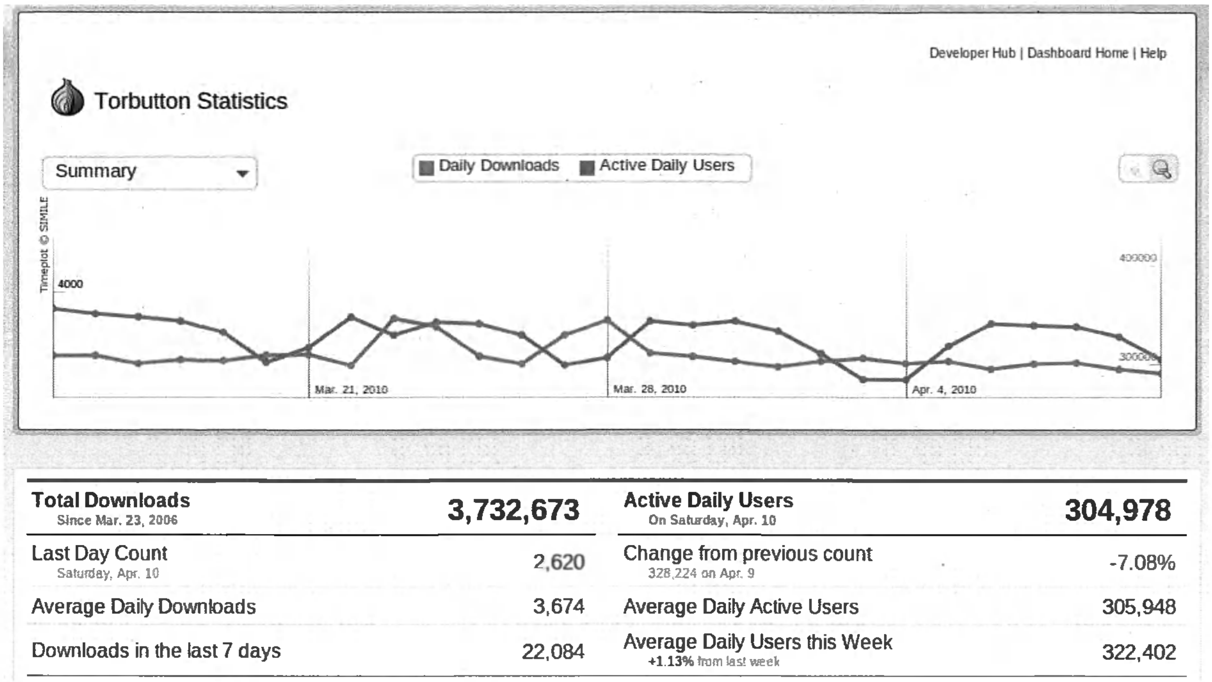
This graph shows the total quantity of relays and quantity of exit relays in March 2010. Exit relay capacity is one of the potential bottlenecks that affects the overall performance of Tor. The more exit relays we have, the faster it seems to browse the open Internet. As shown, the quantity of relays fluctuates little over the month.



This graph shows the total quantity of relays and the total quantity of bridges in March 2010. The quantity of bridges is stable throughout the month.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This measurement is from the server moria, located in Cambridge, Massachusetts. As you can see, latency slightly increased over the month as more users came online. We're also looking to run this measurement software on a linux client connected to a standard dial-up modem to see how Tor fares in extremely low-bandwidth environments.



Total Downloads Since Mar. 23, 2006	3,732,673	Active Daily Users On Saturday, Apr. 10	304,978
Last Day Count Saturday, Apr. 10	2,620	Change from previous count 328,224 on Apr. 9	-7.08%
Average Daily Downloads	3,674	Average Daily Active Users	305,948
Downloads in the last 7 days	22,084	Average Daily Users this Week +1.13% from last week	322,402

This is the public dashboard as kept by Mozilla for the torbutton Firefox extension. It's located at `https://addons.mozilla.org/en-US/statistics/addon/2275`. The red line shows the number of Firefox installations with Torbutton installed. The blue line represents the number of daily downloads of the torbutton extension. As we move torbutton over to https://www.torproject.org/torbutton we expect these numbers reported by Mozilla will decrease. Mozilla is currently tracking all activity to their add-on site, and has the ability to modify the torbutton.xpi file without our approval. These two conditions are the reason we're moving to hosting downloads and updates to torbutton on our own site.

Outreach and Advocacy

- On March 1, Roger met with Sina from Access. He answered many questions about Tor, learned more about the situation in Iran now, and helped brainstorm about further collaborations.
- On March 2, Karen was a panelist at the University of Maryland Digital Media Conference.
- On March 12, Jacob spoke at Digital Security and Tactics for (and by) anti-authoritarians. https://www.noisebridge.net/wiki/Digital_Security_and_Tactics_For_(and_By)_Anti_Authoritarians
- On March 20, Andrew, Erinn, and Runa attended LibrePlanet 2010. Erinn was a panelist at a session about "Women in Technology and Free Software". Andrew spoke about Tor, Free Software, and running a non-profit business with free software. http://libreplanet.org/2010
- A Tor fan created a very quick advocacy video about using Tor for circumvention at http://media.torproject.org/video/TorQatarCensor15secs2b.ogv.
- Andrew was interviewed by ABC Australia's Future Tense program about the "Dark-Web". You can listen to the radio interview at http://media.torproject.org/video/2010-03-11-ABC-Australia-FutureTense-Interview.mp3 or read the transcript at http://www.abc.net.au/rn/futuretense/stories/2010/2837736.htm.
- Steven Murdoch was interviewed by PC Pro UK magazine about "The Dark Side of the Web", http://www.pcpro.co.uk/features/356254/the-dark-side-of-the-web.
- On March 25, we announced The Tor Store to allow users to support Tor from around the world with t-shirts, mugs, and other merchandise. https://www.torproject.org/press/2010-03-25-tor-store-press-release.html.en.
- Tor and EFF were accepted into the Google Summer of Code for the fourth year in a row. https://blog.torproject.org/blog/tor-google-summer-code-2010.
- Jacob gave a Tor talk to Twitter engineers about circumvention, anonymity, and the positive uses of both technologies.
- Erinn, Jacob, and Mike talked to Google engineers about Tor on Android and better integration with the Chrome browser.

Christian rewrote the Tor Weather web application, https://weather.torproject.org/, to increase stability, fix a number of bugs, and add some requested features. Tor Weather is a tool for relay operators to get a reminder when their relay appears to be offline.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

A beta-test of Tor Browser Bundle for GNU/Linux was released for general testing. It is released in both native 32-bit and 64-bit versions.

C.2.12 Bridge relay and bridge authority work.

Steven started work on a proposal to turn all clients into bridges by default. This proposal describes how Tor clients could determine when they have sufficient bandwidth capacity and are sufficiently reliable to become either bridges or Tor relays. When they meet this criteria, they will automatically promote themselves, based on user preferences. The proposal also defines the new controller messages and options which will control this process.

Note that for the moment, only transitions between client and bridge are being considered. Transitions to public relay will be considered at a future date, but will use the same infrastructure for measuring capacity and reliability.

The full proposal, and subsequent discussion, can be read at `http://archives.seul.org/or/dev/Mar-2010/msg00028.html`.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

Karsten continued to improve the Tor Metrics Portal, `http://metrics.torproject.org/`. More reports were automated. The entire setup and process of how we analyze the data was documented.

We added proposal 170, "Configuration options regarding circuit building". Tor's treatment of the various configuration *Nodes options was surprising to many users, and quite a few conspiracy theories have crept up. We should update our specification and code to better describe and to communicate what is going during circuit building, and how we're honoring configuration. So far, we've been tracking a bugreport about this behaviour (`https://bugs.torproject.org/flyspray/index.php?do=details&id=1090`) and Nick replied in a thread on or-talk (`http://archives.seul.org/or/talk/Feb-2010/msg00117.html`). This proposal tries to document our intention for those configuration options.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Nothing to report.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

C.2.17 Translation work, ultimately a browser-based approach.

- Language updates to the website in French, Chinese, German, Spanish, Polish, Russian, Estonian, Norwegian, Greek
- Language updates to the get-tor email autoresponder in Vietnamese, Dutch,
- Language updates to torbutton in Arabic, German, Danish, Slovakian, Swedish, Vietnamese, Russian

Runa fixed a large amount of broken html and translated files. This enabled us to push nearly all projects and languages into the codebases.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: June 9, 2010

This report documents progress in May 2010 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

1. On May 26, Tor Browser Bundle for Microsoft Windows is updated to include the newer Vidalia 0.2.9. This fixes some issues with character set handling, and adds Vietnamese as a new language.
2. On May 31, we released Tor Browser Bundle for Linux 1.0.6. It contains the following updates:
   - Add arch to tarball name so there's no collision
   - Add libpng for Arch Linux
   - Add HTTPS Everywhere extension
   - Update Qt to 4.6.2
   - Update Vidalia to 0.2.9
   - Update NoScript to 1.9.9.80
3. On June 1st, we released Tor Browser Bundle for Linux 1.0.7. It uses an older glibc for better compatibility with older linux distributions.
4. On May 20, we released Vidalia 0.2.9. Fixes include Qt 4.6.2 compatibility, new cert, and some new translations. You can download it at https://www.torproject.org/vidalia/. Packages are slowly being updated to include this version of Vidalia. The full changelog is:

```
 * Remove the GoDaddy CA certificate bundle since we changed the certificate used to authenticate
connections to geoips.vidalia-project.net for downloading GeoIP information from a commercial
GoDaddy certificate to a free CACert certificate.
 * Define -D_WIN32_WINNT=0x0501 on Windows builds so that MiniUPnPc will build with the latest
versions of MinGW.
 * Modify miniupnpc.c from MiniUPnPc's source so that it will build on Mac OS X 10.4.
 * Work around Qt's new behavior for the QT_WA macro so that Vidalia will
 * work correctly again on Windows with Qt >= 4.6.
```

5. On May 2nd, we released an updated stable version of Tor, 0.2.1.26. The detailed list of changes is:

```
o Major bugfixes:
  - Teach relays to defend themselves from connection overload. Relays
    now close idle circuits early if it looks like they were intended
    for directory fetches. Relays are also more aggressive about closing
    TLS connections that have no circuits on them. Such circuits are
    unlikely to be re-used, and tens of thousands of them were piling
    up at the fast relays, causing the relays to run out of sockets
    and memory. Bugfix on 0.2.0.22-rc (where clients started tunneling
    their directory fetches over TLS).
  - Fix SSL renegotiation behavior on OpenSSL versions like on Centos
    that claim to be earlier than 0.9.8m, but which have in reality
    backported huge swaths of 0.9.8m or 0.9.8n renegotiation
    behavior. Possible fix for some cases of bug 1346.
  - Directory mirrors were fetching relay descriptors only from v2
    directory authorities, rather than v3 authorities like they should.
    Only 2 v2 authorities remain (compared to 7 v3 authorities), leading
    to a serious bottleneck. Bugfix on 0.2.0.9-alpha. Fixes bug 1324.

o Minor bugfixes:
  - Finally get rid of the deprecated and now harmful notion of "clique
    mode", where directory authorities maintain TLS connections to
    every other relay.

o Testsuite fixes:
  - In the util/threads test, no longer free the test_mutex before all
    worker threads have finished. Bugfix on 0.2.1.6-alpha.
  - The master thread could starve the worker threads quite badly on
    certain systems, causing them to run only partially in the allowed
    window. This resulted in test failures. Now the master thread sleeps
    occasionally for a few microseconds while the two worker-threads
    compete for the mutex. Bugfix on 0.2.0.1-alpha.
```

6. On May 19, we released an updated OrBot (Tor for Android), version 0.0.6, which contains Tor 0.2.2.13-alpha.

7. On May 26, we released an updated Orbot (Tor for Android), version 0.0.7, which contains a number of usability fixes reported by users. See the bugfixes at `https://trac.torproject.org/projects/tor/query?status=closed&component=Android+(Orbot)-Backend+/+Core&order=priority&col=id&col=summary&col=status&col=type&col=priority&col=milestone&col=component&owner=`.

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

On May 4, China's Great Firewall began blocking connections to the public Tor relays. They also updated their blocking to include bridge relays published via email and https websites. Further research into the blocking mechanisms from inside China show they are simply blocking IP Address and TCP port combinations. Bridge relays that have been seeded into various social networks in China continue to work well.

Tor on the Android OS, called Orbot, continues progress. Work continues on a privacy-preserving web browser, Orweb, and other supporting applications to make Tor on Android more useful for daily users. Nathan got a Tor relay running on a Moons e-7001 "iRobot" tablet, `http://guardianproject.info/2010/05/25/tor-on-a-tablet/`.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

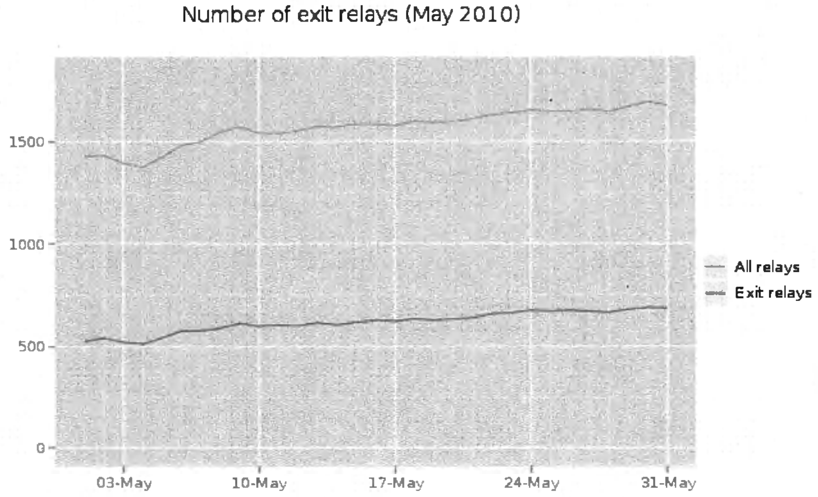
Nothing to report.

C.2.5. Hide Tor's network signature.

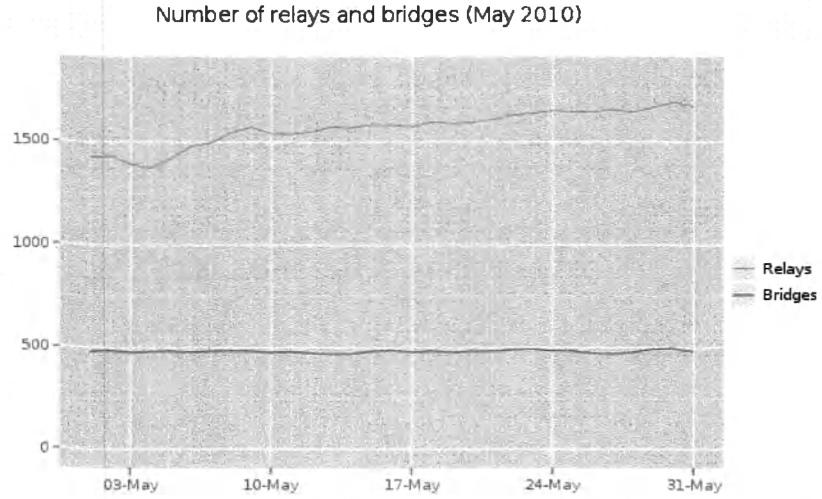
Nothing to report.

C.2.10 Grow the Tor network and user base. Outreach.

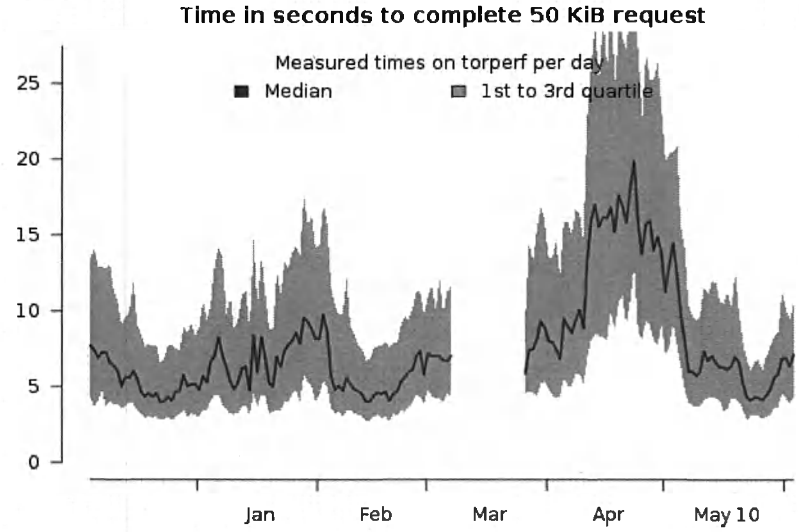
Measures of the Tor Network



This graph shows the total quantity of relays and quantity of exit relays in May 2010. Exit relay capacity is one of the potential bottlenecks that affects the overall performance of Tor. The more exit relays we have, the faster it seems to browse the open Internet. As shown, the quantity of relays inreased dramatically over the month. We believe this is due to bugfixes in 0.2.1.26 which helps relays handle connection overload from older clients.



This graph shows the total quantity of relays and the total quantity of bridges in May 2010. The quantity of bridges is stable throughout the month.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This measurement is from the server torperf, located in Chicago, Illinois. As you can see, latency dropped dramatically over the month. We believe this is due to two independent events. First, China blocked the tor network as a precaution for the June 4th Tiananmen Square Anniversary, removing 70-80,000 daily users. Second, the fixes for relays in 0.2.1.26 allow relays to handle older clients flooding circuit requests to relays. As some relays were overloaded and dropped out of the network, the remaining relays had to handle an increasing load of users. We're also looking to run this measurement software on a linux client connected to a standard dial-up modem to see how Tor fares in extremely low-bandwidth environments.

Outreach and Advocacy

- Jacob, Roger, Runa, and Linus talked to various NorduNet and SUNET people in Sweden.
- Jacob attended Internet Dagarna, http://www.internetdagarna.se/track/sakerhet/ett-slag-for-yttrandefriheten
- Erinn and Karen attended the Global Voices Summit 2010 in Santiago, Chile. There were a number of discussions about how to use Tor safely and its usage in activism. Erinn held a detailed Tor training for 5-10 activists in Spanish. `http://summit2010.globalvoicesonline.org/`
- Roger gave a few talks as AUSCERT, `http://www.auscert.org.au/`.
- Roger was interviewed by The Australian about Internet censorship and privacy. `http://www.theaustralian.com.au/australian-it/call-to-join-tor-network-to-fight-censorship/story-e6frgakx-1225870756466`
- Roger was interviewed by ComputerWorld Australia about the relationship between China and Tor. `http://www.computerworld.com.au/article/347273/auscert_2010_china_set_net_blackout_tiananmen_square_anniversary/`
- Jacob gave the keynote speech at CONFidence in Krakow, Poland, `http://2010.confidence.org.pl/`.
- Jacob, Christian, and others attended pH neutral in Berlin, Germany. `http://ph-neutral.darklab.org/`

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

Continued to work on Linux and Mac OS X tor browser bundles. The Mac version of TBB is going to use a sandboxing technology borrowed from IronFox. This should help minimize the footprint and security concerns about running TBB on OS X computers.

C.2.12 Bridge relay and bridge authority work.

Nothing to report.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

From the 0.2.1.26 release notes, teach relays to defend themselves from connection overload. Relays now close idle circuits early if it looks like they were intended for directory fetches. Relays are also more aggressive about closing TLS connections that have no circuits on them. Such circuits are unlikely to be re-used, and tens of thousands of them were piling up at the fast relays, causing the relays to run out of sockets and memory. Bugfix on 0.2.0.22-rc (where clients started tunneling their directory fetches over TLS).

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Nothing to report.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

C.2.17 Translation work, ultimately a browser-based approach.

- Added the Android orbot application to the translation portal.
- By user request, add Serbian to the available languages.
- Translation updates for the following languages: Polish, Arabic, Greek, Serbian, Russian, Swedish, Chinese, Norwegian, Japanese, German, Spanish, Portugese, French, Dutch, Romanian, and Farsi.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: December 10, 2010

This report documents progress in November 2010 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

New Releases

1. On November 16 we released the latest in the Tor -alpha series. Tor 0.2.2.18-alpha fixes several crash bugs that have been nagging us lately, makes unpublished bridge relays able to detect their IP address, and fixes a wide variety of other bugs to get us much closer to a stable release.

```
Changes in version 0.2.2.18-alpha - 2010-11-16
  o Major bugfixes:
    - Do even more to reject (and not just ignore) annotations on
      router descriptors received anywhere but from the cache. Previously
      we would ignore such annotations at first, but cache them to disk
      anyway. Bugfix on 0.2.0.8-alpha. Found by piebeer.
    - Do not log messages to the controller while shrinking buffer
      freelists. Doing so would sometimes make the controller connection
      try to allocate a buffer chunk, which would mess up the internals
      of the freelist and cause an assertion failure. Fixes bug 1125;
      fixed by Robert Ransom. Bugfix on 0.2.0.16-alpha.
    - Learn our external IP address when we're a relay or bridge, even if
      we set PublishServerDescriptor to 0. Bugfix on 0.2.0.3-alpha,
      where we introduced bridge relays that don't need to publish to
      be useful. Fixes bug 2050.
    - Maintain separate TLS contexts and certificates for incoming and
      outgoing connections in bridge relays. Previously we would use the
      same TLS contexts and certs for incoming and outgoing connections.
      Bugfix on 0.2.0.3-alpha; addresses bug 988.
    - Maintain separate identity keys for incoming and outgoing TLS
      contexts in bridge relays. Previously we would use the same
      identity keys for incoming and outgoing TLS contexts. Bugfix on
      0.2.0.3-alpha; addresses the other half of bug 988.
    - Avoid an assertion failure when we as an authority receive a
      duplicate upload of a router descriptor that we already have,
      but which we previously considered an obsolete descriptor.
      Fixes another case of bug 1776. Bugfix on 0.2.2.16-alpha.
    - Avoid a crash bug triggered by looking at a dangling pointer while
      setting the network status consensus. Found by Robert Ransom.
      Bugfix on 0.2.2.17-alpha. Fixes bug 2097.
    - Fix a logic error where servers that _didn't_ act as exits would
      try to keep their server lists more aggressively up to date than
      exits, when it was supposed to be the other way around. Bugfix
      on 0.2.2.17-alpha.

  o Minor bugfixes (on Tor 0.2.1.x and earlier):
    - When we're trying to guess whether we know our IP address as
      a relay, we would log various ways that we failed to guess
      our address, but never log that we ended up guessing it
      successfully. Now add a log line to help confused and anxious
      relay operators. Bugfix on 0.1.2.1-alpha; fixes bug 1534.
    - Bring the logic that gathers routerinfos and assesses the
      acceptability of circuits into line. This prevents a Tor OP from
      getting locked in a cycle of choosing its local OR as an exit for a
      path (due to a .exit request) and then rejecting the circuit because
      its OR is not listed yet. It also prevents Tor clients from using an
      OR running in the same instance as an exit (due to a .exit request)
      if the OR does not meet the same requirements expected of an OR
      running elsewhere. Fixes bug 1859; bugfix on 0.1.0.1-rc.
    - Correctly describe errors that occur when generating a TLS object.
      Previously we would attribute them to a failure while generating a
      TLS context. Patch by Robert Ransom. Bugfix on 0.1.0.4-rc; fixes
      bug 1994.
    - Enforce multiplicity rules when parsing annotations. Bugfix on
      0.2.0.8-alpha. Found by piebeer.
    - Fix warnings that newer versions of autoconf produced during
      ./autogen.sh. These warnings appear to be harmless in our case,
      but they were extremely verbose. Fixes bug 2020.

  o Minor bugfixes (on Tor 0.2.2.x):
    - Enable protection of small arrays whenever we build with gcc
      hardening features, not only when also building with warnings
      enabled. Fixes bug 2031; bugfix on 0.2.2.14-alpha. Reported by keb.

  o Minor features:
    - Make hidden services work better in private Tor networks by not
      requiring any uptime to join the hidden service descriptor
      DHT. Implements ticket 2088.
    - Rate-limit the "your application is giving Tor only an IP address"
      warning. Addresses bug 2000; bugfix on 0.0.8pre2.
    - When AllowSingleHopExits is set, print a warning to explain to the
      relay operator why most clients are avoiding her relay.
    - Update to the November 1 2010 Maxmind GeoLite Country database.

  o Code simplifications and refactoring:
    - When we fixed bug 1038 we had to put in a restriction not to send
      RELAY_EARLY cells on rend circuits. This was necessary as long
      as relays using Tor 0.2.1.3-alpha through 0.2.1.18-alpha were
      active. Now remove this obsolete check. Resolves bug 2081.
    - Some options used different conventions for uppercasing of acronyms
      when comparing manpage and source. Fix those in favor of the
      manpage, as it makes sense to capitalize acronyms.
    - Remove the torrc.complete file. It hasn't been kept up to date
      and users will have better luck checking out the manpage.
    - Remove the obsolete "NoPublish" option; it has been flagged
      as obsolete and has produced a warning since 0.1.1.18-rc.
    - Remove everything related to building the expert bundle for OS X.
      It has confused many users, doesn't work right on OS X 10.6,
      and is hard to get rid of once installed. Resolves bug 1274.
```

2. On November 23, we released the latest in the Tor -stable series. Tor 0.2.1.27 makes relays work with OpenSSL 0.9.8p and 1.0.0.b – yet another OpenSSL security patch broke its compatibility with Tor. We also took this opportunity to fix several crash bugs, integrate a new directory authority, and update the bundled GeoIP database.

```
Changes in version 0.2.1.27 - 2010-11-23
  o Major bugfixes:
    - Resolve an incompatibility with OpenSSL 0.9.8p and OpenSSL 1.0.0b:
      No longer set the tlsext_host_name extension on server SSL objects;
      but continue to set it on client SSL objects. Our goal in setting
      it was to imitate a browser, not a vhosting server. Fixes bug 2204;
      bugfix on 0.2.1.1-alpha.
    - Do not log messages to the controller while shrinking buffer
      freelists. Doing so would sometimes make the controller connection
      try to allocate a buffer chunk, which would mess up the internals
      of the freelist and cause an assertion failure. Fixes bug 1125;
      fixed by Robert Ransom. Bugfix on 0.2.0.16-alpha.
    - Learn our external IP address when we're a relay or bridge, even if
      we set PublishServerDescriptor to 0. Bugfix on 0.2.0.3-alpha,
      where we introduced bridge relays that don't need to publish to
      be useful. Fixes bug 2050.
    - Do even more to reject (and not just ignore) annotations on
      router descriptors received anywhere but from the cache. Previously
      we would ignore such annotations at first, but cache them to disk
      anyway. Bugfix on 0.2.0.8-alpha. Found by piebeer.
    - When you're using bridges and your network goes away and your
      bridges get marked as down, recover when you attempt a new socks
      connection (if the network is back), rather than waiting up to an
      hour to try fetching new descriptors for your bridges. Bugfix on
      0.2.0.3-alpha; fixes bug 1981.

  o Major features:
    - Move to the November 2010 Maxmind GeoLite country db (rather
      than the June 2009 ip-to-country GeoIP db) for our statistics that
      count how many users relays are seeing from each country. Now we'll
      have more accurate data, especially for many African countries.

  o New directory authorities:
    - Set up maatuska (run by Linus Nordberg) as the eighth v3 directory
```

```
      authority.

  o Minor bugfixes:
    - Fix an assertion failure that could occur in directory caches or
      bridge users when using a very short voting interval on a testing
      network. Diagnosed by Robert Hogan. Fixes bug 1141; bugfix on
      0.2.0.8-alpha.
    - Enforce multiplicity rules when parsing annotations. Bugfix on
      0.2.0.8-alpha. Found by piebeer.
    - Allow handshaking OR connections to take a full KeepalivePeriod
      seconds to handshake. Previously, we would close them after
      IDLE_OR_CONN_TIMEOUT (180) seconds, the same timeout as if they
      were open. Bugfix on 0.2.1.26; fixes bug 1840. Thanks to mingw-san
      for analysis help.
    - When building with --enable-gcc-warnings on OpenBSD, disable
      warnings in system headers. This makes --enable-gcc-warnings
      pass on OpenBSD 4.8.

  o Minor features:
    - Exit nodes didn't recognize EHOSTUNREACH as a plausible error code,
      and so sent back END_STREAM_REASON_MISC. Clients now recognize a new
      stream ending reason for this case: END_STREAM_REASON_NOROUTE.
      Servers can start sending this code when enough clients recognize
      it. Bugfix on 0.1.0.1-rc; fixes part of bug 1793.
    - Build correctly on mingw with more recent versions of OpenSSL 0.9.8.
      Patch from mingw-san.

  o Removed files:
    - Remove the old debian/ directory from the main Tor distribution.
      The official Tor-for-debian git repository lives at the URL
      https://git.torproject.org/debian/tor.git
    - Stop shipping the old doc/website/ directory in the tarball. We
      changed the website format in late 2010, and what we shipped in
      0.2.1.26 really wasn't that useful anyway.
```

3. On November 21, we released the latest in the Tor -alpha series. Yet another OpenSSL security patch broke its compatibility with Tor: Tor 0.2.2.19-alpha makes relays work with OpenSSL 0.9.8p and 1.0.0.b.

```
Changes in version 0.2.2.19-alpha - 2010-11-21
  o Major bugfixes:
    - Resolve an incompatibility with openssl 0.9.8p and openssl 1.0.0b:
      No longer set the tlsext_host_name extension on server SSL objects;
      but continue to set it on client SSL objects. Our goal in setting
      it was to imitate a browser, not a vhosting server. Fixes bug 2204;
      bugfix on 0.2.1.1-alpha.

  o Minor bugfixes:
    - Try harder not to exceed the maximum length of 50 KB when writing
      statistics to extra-info descriptors. This bug was triggered by very
      fast relays reporting exit-port, entry, and dirreq statistics.
  Reported by Olaf Selke. Bugfix on 0.2.2.1-alpha. Fixes bug 2183.
- Publish a router descriptor even if generating an extra-info
  descriptor fails. Previously we would not publish a router
  descriptor without an extra-info descriptor; this can cause fast
  exit relays collecting exit-port statistics to drop from the
  consensus. Bugfix on 0.1.2.9-rc; fixes bug 2195.
```

4. On November 26, we released updated Tor Browser Bundles. There are new browser bundles out with the updated Tor versions (0.2.2.19-alpha and 0.2.1.27) that work with the latest OpenSSL.

   Windows Tor Browser Bundles
   1.3.13: Released 2010-11-25 There were some controversial changes recently made to the Windows bundle, and for those I apologize. I have removed BetterPrivacy and NoScript from them pending further testing. The whole changelog:

   - update Tor to 0.2.1.27
   - update Pidgin to 2.7.5
   - update OpenSSL to 0.9.8p
   - fix Firefox extension install path so extensions show in the installed add-ons list
   - disable Firefox's ability to search the Windows registry path for system-wide plugins and extensions (closes: 2118)
   - remove NoScript and BetterPrivacy from stable bundle until they receive more testing

   OS X bundles
   1.0.6: Released 2020-11-24 Update Tor to 0.2.2.19-alpha

   Linux Bundles
   1.0.17: Released 2010-11-24 Update Tor to 0.2.2.19-alpha

5. On November 30th, we released the latest Arm relay monitor. Damian writes, "What's new since August of 2009, you ask? Lots. The project has been under very active development, continuing to add usability improvements to make relay operation nicer and less error prone. If you're really curious what I've been up to this last year then it's all available in the change log." For those unfamiliar, arm is a terminal monitor for Tor relays and, to a growing extent, end users. It provides:

   - resource usage (bandwidth, cpu, and memory usage)
   - general relaying information (nickname, fingerprint, flags, or/dir/controlports)
   - event log with optional regex filtering and deduplication
   - connections correlated against tor's consensus data (ip, connection types, relay details, etc)
   - an editor to quickly alter Tor's configuration
   - torrc configuration file with syntax highlighting and validation
   - and quite a bit more via a curses interface. For screenshots and downloads visit: `http://www.atagar.com/arm/`

We are currently working on getting this to be available via repositories for Debian and Ubuntu too. RPM builds are available

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Nothing to report.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

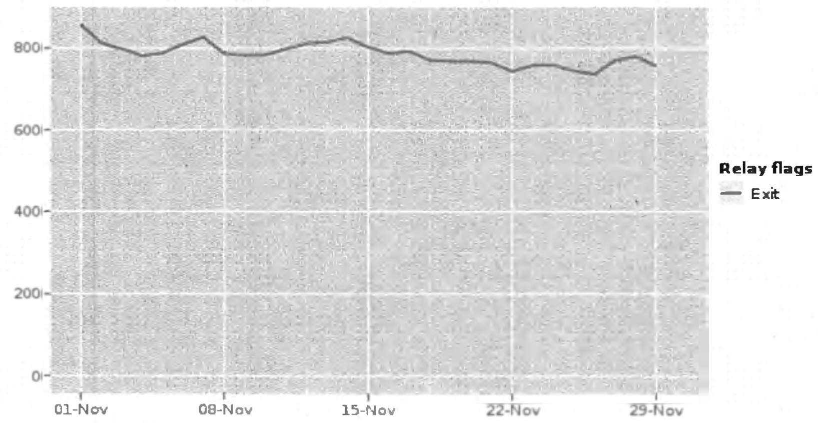
Nothing to report.

C.2.5. Hide Tor's network signature.

Nothing to report.

C.2.10 Grow the Tor network and user base. Outreach.

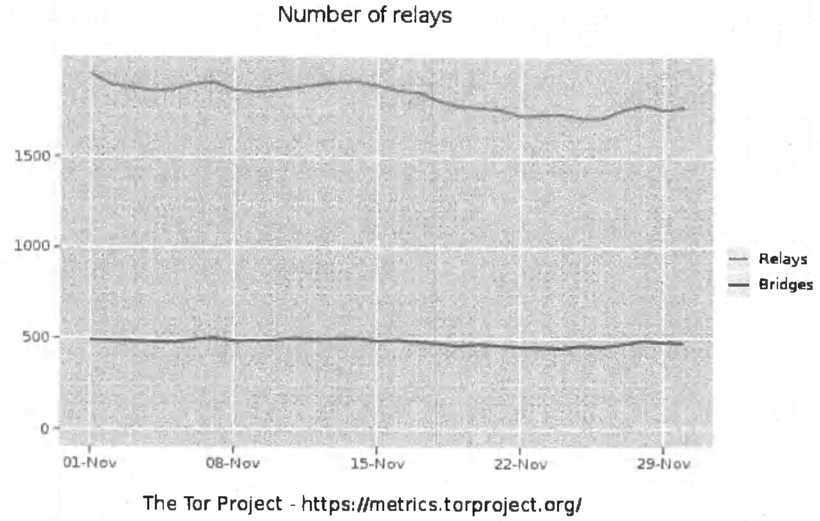
Measures of the Tor Network



Number of relays with relay flags assigned

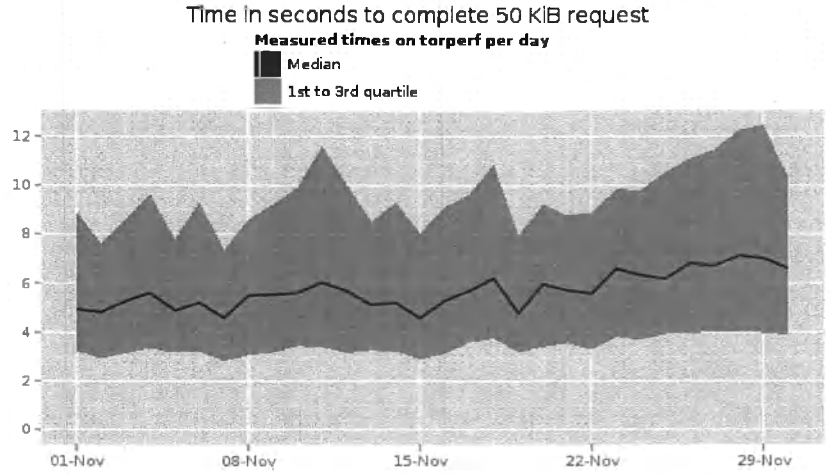
The Tor Project - https://metrics.torproject.org/

This graph shows the total quantity of relays and quantity of exit relays in November 2010.



The Tor Project - https://metrics.torproject.org/

This graph shows the total quantity of relays and the total quantity of bridges in November 2010. The quantity of bridges is declining throughout the month due to an OpenSSL issue which only broke Tor relays, not clients.



The Tor Project - https://metrics.torproject.org/

This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This measurement is from the server torperf, located in Chicago, Illinois. As you can see, latency continues to be low but increased slightly as we lost relays due to an OpenSSL issue.

Outreach and Advocacy

1. We released our first ever Annual Report for 2009. It highlights what we've accomplished in 2009. https://www.torproject.org/about/financials.html.en

2. Andrew presented to the U.S. Dept of Commerce Information Systems Technical Advisory Committee (ISTAC) about Tor and its relation to US Export Controls. More about ISTAC can be found here, http://tac.bis.doc.gov/ischart.htm. Andrew's presentation can be found at https://svn.torproject.org/svn/projects/presentations/2010-11-03-ISTAC-tor-circumvention-overview.pdf

3. Linus and Erinn attended FSCONS as a guest speaker in Sweden, http://fscons.org/. Erinn was invited back to be a main speaker next year. Linus' presentation can be found at https://svn.torproject.org/svn/projects/presentations/FSCONS-2010.pdf.

4. Erinn spoke at Codebits in Portugal about Tor, Free Software, and Anonymity, http://codebits.eu/. Her presentation can be found at https://svn.torproject.org/svn/projects/presentations/2010-11-Codebits.pdf.

5. Andrew was interviewed for Internet Evolution, http://www.internetevolution.com/radio.asp?doc_id=196479 about Tor and online anonymity.

6. Roger visited Nick Hopper's research group at UMN, http://www-users.cs.umn.edu/~hopper/. He helped with a number of areas around a Tor simulator, how to anonymously collect Tor internal statistics, effect of guard nodes on security, how to model Tor user behavior, overlaying a censorship resistant publishing system, and some ideas on how to better count tor users anonymously.

7. Jake and Karen attended a training held with Human Rights Watch and Access.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- Updated Tor Browser Bundles to fix some Firefox plugin issues in the Windows bundle and updated Tor binaries. See the C2.0 section for details.

C.2.12 Bridge relay and bridge authority work.

Mike's initial research into bridges shows that we get 700-800 new bridges a day, but around 500 of them stay online and are reliable enough to give to users. We are developing ways to create more bridges through packaging that turns users into a bridge by default, a hardware router that acts as a bridge and transparent tor proxy, and creating images for cloud computing providers such as Amazon, Rackspace, and Microsoft. We're tracking the progress of these projects at:

- Bridge-by-default bundles, https://trac.torproject.org/projects/tor/milestone/Experimental%20Bridge%20Bundles

- Karsten fixed the Python version of the VisiTor script that was contributed by Kiyoto Tamura.
- Nick did some multithreaded crypto hacking, wrote the missing code to have clients fetch microdescriptors, and spent a good while longer bughunting in Tor, particularly for issues related to brokenness in and around openssl.
- Nick also spent a while chasing down more lingering Libevent bugs that don't affect Tor directly; having Libevent useful for more people means that we get more contributors for the Libevent codebase, which in turn helps Tor indirectly. Tor is heavily dependent on libevent, therefore the better libevent becomes, the better Tor becomes.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Nothing to report.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

C.2.17 Translation work, ultimately a browser-based approach.

We are migrating all translation work over to `https://www.transifex.net/projects/p/torproject/`. Runa spent the month preparing the po/pot files for migration, committing translations still residing in pootle at translation.torproject.org.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: November 9, 2010

This report documents progress in October 2010 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

New Funding

- Tor is awarded a grant from the Swedish International Development Agency (sida.se) for an 18-month project to educate, survey, and improve Tor the software for circumvention usage in the Middle East.

- Internews Network extends $400k in funding to Tor to complete the 3-year contract through US State DRL grant. The total contract from Internews over 3 years is $1.66 million.

New Releases

1. On October 29th, we released updated Tor Browser Bundles for OS X, Linux, and Windows. This is an upgrade to Firefox 3.6.12 which fixes a critical bug and OS X users' Torbutton will now show up.

```
Tor Browser Bundle for Windows 1.3.12
 - 1.3.12: Release 2010-10-28
 - Update Firefox to 3.6.12

Tor Browser Bundle for Mac OS X 1.0.4
 - 1.0.4: Released 2010-10-28
 - Update Firefox to 3.6.12
 - Fix weird Torbutton location so users can tell it's installed

Tor Browser Bundle for GNU/Linux 1.0.15
 - 1.0.15: Released 2010-10-28
 - Update Firefox to 3.6.12
```

2. On October 28th, we released new OSX Vidalia bundles which include Tor 0.2.2.17-alpha. Vidalia 0.2.10 changed the way we deal with the geoip databases by dropping the remote geoip lookups. This caused a lot of headaches for OS X users because of the layout of the package, but it's fixed in this version.

version work. `https://www.torproject.org`. It features an entirely redesigned Information Architecture, user experience design, and codebase. Andrew, Roger, Sebastian, Runa, and many volunteers contributed to this release.

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Nick continued to work on the codebase around microdescriptors. Microdescriptors will allow clients on very low bandwidth connections to use the tor network more quickly than waiting to download the current directory information.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

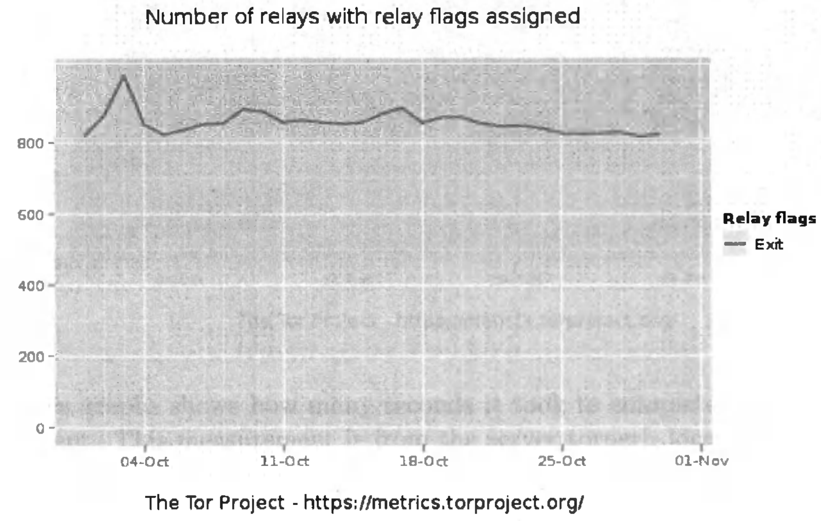
Nothing to report.

C.2.5. Hide Tor's network signature.

Nothing to report.

C.2.10 Grow the Tor network and user base. Outreach.

Measures of the Tor Network



This graph shows the total quantity of relays and quantity of exit relays in October 2010.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

- Karsten incorporated Kevin Berry's Google Summer of Code work into the metrics portal, https://blog.torproject.org/blog/tor-metrics-google-summer-code-2010. This enables all graphs to be dynamically generated with minimal load to the server.
- Karsten and Sebastian continue to research an alternate way to more accurately count Tor users while still preserving their anonymity by design. They expect to have a report out in December 2010.
- Mike fixed some bugs relating to Bandwidth and Exit Authorities. These fixes are for code stability.
- Mike began investigating the odd reality that we seem to have only 500 bridges available at any point in time. Hundreds to thousands of people become bridges each week, but only around 500 are reported as being available at any point in time. This seems an odd coincidence to Mike and others. Research continues.
- Update to the October 1 2010 Maxmind GeoLite Country database. This updates the mapping of IP Address to Geolocation of relays.
- Nick commits a huge number of bug fixes, code refactoring, and general logic corrections as discovered through code audits, buffer events integration, and volunteer reviews.
- Karsten extended total relay bandwidth graph https://metrics.torproject.org/network.html#bandwidth by bandwidth history as reported by relays and added new graph on directory bytes written by relays https://metrics.torproject.org/network.html#dirbytes.
- Karsten changed most servlets to JSPs, added database connection pool, made the Tomcat application generate CSV files upon request, etc. These changes are not visible to most people, but they were necessary to clean up the grown metrics website. As a result, it's much easier now to add new graphs to the website.
- Karsten helped a volunteer to write a Python version of the VisiTor script https://metrics.torproject.org/tools.html#visitor and wrote a spec for the exit list file format https://trac.torproject.org/projects/tor/ticket/2064#comment:1.
- Karsten found a new approach for combining directory request statistics from multiple relays to estimate total user numbers. The result is a much more reliable metric than the one we're using right now, https://metrics.torproject.org/users.html#direct-users. Asked Olaf Selke (operator of blugmagie), Teun Nijssen (operator of TORy), and a few more to turn on directory request statistics on their relays. Updated tech report on Privacy-preserving Ways to Estimate the Number of Tor Users with new results, https://gitweb.torproject.org/karsten/metrics.git/blob_plain/refs/heads/counting-users:/report/counting-users/countingusers.pdf.

C.2.14. Incentives work.

Nothing to report.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: October 5, 2010

This report documents progress in September 2010 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

New Hires

- Tom Heydt-Benjamin is contracted full-time to work on NSF-related research through December 2010.
- Erinn Clark is contracted full-time to work on improving packaging, secure updater, tor browser bundles, and continuous integration systems through December 2010. Previously, Erinn was part-time.

New Funding

- We are one of 4 finalists for a likely Swedish Kronor 4M grant from the Swedish International Development Agency.
- Internews obligated funding of $1.2M since September 2008 has been finished. Internews promises $400K additional in FY2011.

New Releases

1. Tor Browser Bundle for Mac OS X is now available for the i386 architecture in 11 languages. This is an alpha release to let the community test functionality. The bundle comes with the following software:

   - Tor 0.2.2.15-alpha
   - Vidalia 0.2.10 – cross-platform controller GUI for the Tor software
   - Polipo 1.0.4.1 – caching web proxy
   - Firefox/Namoroka 3.6.9 – web browser
   - Torbutton 1.2.5 – Firefox extension to enable or disable the browser's use of Tor
   - NoScript 2.0.2.3 – Firefox extension to only allow scripts from trusted sites
   - HTTPS-Everywhere 0.2.2 – Firefox extension to provide encryption to a major number of websites

2. Orbot, Tor for Android, was released into the Android Market. Android users can now officially download and install Orbot on their devices. `https://guardianproject.info/apps/orbot/`

3. Version 0.2.10 of the graphical controller for tor, Vidalia, is now available. The main change is the use of Tor's native geoip database to map relay IP addresses to country. This removes the remote geoip resolution that occurred over Tor in previous versions of Vidalia. The full changelog is:

   - Drop remote GeoIP lookups. Instead, the default behavior now is to use the country-level GeoIP database that ships with Tor to map an IP address to a country code, and then map the country code to latitude and longitude with a separate database built into Vidalia.
   - Add a -DUSE_GEOIP build option to enable building with MaxMind's GeoIP C library for using a local city-level or country-level database instead of Tor's database. See README.geoip for details on use.
   - Only update a stream's displayed target address in the network map if no hostname was given in the stream's NEW status event. Fix suggested by Robert Hogan. (Ticket 608)
   - Update the menubar icon at the same time as the dock icon on OS X. Previously, we had a blank icon in the menubar. (Ticket 610)
   - Updated several translations.

4. Tor 0.2.2.16-alpha fixes a variety of old stream fairness bugs (most evident at exit relays), and also continues to resolve all the little bugs that have been filling up trac lately.

   Packages will be appearing over the next few days or weeks (except on Windows, which apparently doesn't build – stay tuned for an 0.2.2.17-alpha in that case).

```
Changes in version 0.2.2.16-alpha - 2010-09-17
  o Major bugfixes (stream-level fairness):
    - When receiving a circuit-level SENDME for a blocked circuit, try
      to package cells fairly from all the streams that had previously
      been blocked on that circuit. Previously, we had started with the
      oldest stream, and allowed each stream to potentially exhaust
      the circuit's package window. This gave older streams on any
      given circuit priority over newer ones. Fixes bug 1937. Detected
      originally by Camilo Viecco. This bug was introduced before the
      first Tor release, in svn commit r152: it is the new winner of
      the longest-lived bug prize.
    - When the exit relay got a circuit-level sendme cell, it started
      reading on the exit streams, even if had 500 cells queued in the
      circuit queue already, so the circuit queue just grew and grew in
      some cases. We fix this by not re-enabling reading on receipt of a
      sendme cell when the cell queue is blocked. Fixes bug 1653. Bugfix
      on 0.2.0.1-alpha. Detected by Mashael AlSabah. Original patch by
      "yetonetime".
    - Newly created streams were allowed to read cells onto circuits,
      even if the circuit's cell queue was blocked and waiting to drain.
    This created potential unfairness, as older streams would be
    blocked, but newer streams would gladly fill the queue completely.
    We add code to detect this situation and prevent any stream from
    getting more than one free cell. Bugfix on 0.2.0.1-alpha. Partially
    fixes bug 1298.

  o Minor features:
    - Update to the September 1 2010 Maxmind GeoLite Country database.
    - Warn when CookieAuthFileGroupReadable is set but CookieAuthFile is
      not. This would lead to a cookie that is still not group readable.
      Closes bug 1843. Suggested by katmagic.
    - When logging a rate-limited warning, we now mention how many messages
      got suppressed since the last warning.
    - Add new "perconnbwrate" and "perconnbwburst" consensus params to
      do individual connection-level rate limiting of clients. The torrc
      config options with the same names trump the consensus params, if
      both are present. Replaces the old "bwconnrate" and "bwconnburst"
      consensus params which were broken from 0.2.2.7-alpha through
      0.2.2.14-alpha. Closes bug 1947.
    - When a router changes IP address or port, authorities now launch
      a new reachability test for it. Implements ticket 1899.
    - Make the formerly ugly "2 unknown, 7 missing key, 0 good, 0 bad,
      2 no signature, 4 required" messages about consensus signatures
      easier to read, and make sure they get logged at the same severity
      as the messages explaining which keys are which. Fixes bug 1290.
    - Don't warn when we have a consensus that we can't verify because
      of missing certificates, unless those certificates are ones
      that we have been trying and failing to download. Fixes bug 1145.
    - If you configure your bridge with a known identity fingerprint,
      and the bridge authority is unreachable (as it is in at least
      one country now), fall back to directly requesting the descriptor
      from the bridge. Finishes the feature started in 0.2.0.10-alpha;
      closes bug 1138.
    - When building with --enable-gcc-warnings on OpenBSD, disable
      warnings in system headers. This makes --enable-gcc-warnings
      pass on OpenBSD 4.8.

  o Minor bugfixes (on 0.2.1.x and earlier):
    - Authorities will now attempt to download consensuses if their
      own efforts to make a live consensus have failed. This change
      means authorities that restart will fetch a valid consensus, and
      it means authorities that didn't agree with the current consensus
      will still fetch and serve it if it has enough signatures. Bugfix
      on 0.2.0.9-alpha; fixes bug 1300.
    - Ensure DNS requests launched by "RESOLVE" commands from the
      controller respect the __LeaveStreamsUnattached setconf options. The
      same goes for requests launched via DNSPort or transparent
      proxying. Bugfix on 0.2.0.1-alpha; fixes bug 1525.
    - Allow handshaking OR connections to take a full KeepalivePeriod
      seconds to handshake. Previously, we would close them after
      IDLE_OR_CONN_TIMEOUT (180) seconds, the same timeout as if they
```

- new: Add DuckDuckGo.com as a Google captcha redirect destination (patch from aiden tighe)
- bugfix: bug 1911: Fix broken useragent locale string on debian (patch from lunar)
- bugfix: Fix captcha detection for encrypted.google.com

6. Tor 0.2.2.17-alpha introduces a feature to make it harder for clients to use one-hop circuits (which can put the exit relays at higher risk, plus unbalance the network); fixes a big bug in bandwidth accounting for relays that want to limit their monthly bandwidth use; fixes a big pile of bugs in how clients tolerate temporary network failure; and makes our adaptive circuit build timeout feature (which improves client performance if your network is fast while not breaking things if your network is slow) better handle bad networks.

```
Changes in version 0.2.2.17-alpha - 2010-09-30
  o Major features:
    - Exit relays now try harder to block exit attempts from unknown
      relays, to make it harder for people to use them as one-hop proxies
      a la tortunnel. Controlled by the refuseunknownexits consensus
      parameter (currently enabled), or you can override it on your
      relay with the RefuseUnknownExits torrc option. Resolves bug 1751.

  o Major bugfixes (0.2.1.x and earlier):
    - Fix a bug in bandwidth accounting that could make us use twice
      the intended bandwidth when our interval start changes due to
      daylight saving time. Now we tolerate skew in stored vs computed
      interval starts: if the start of the period changes by no more than
      50% of the period's duration, we remember bytes that we transferred
      in the old period. Fixes bug 1511; bugfix on 0.0.9pre5.
    - Always search the Windows system directory for system DLLs, and
      nowhere else. Bugfix on 0.1.1.23; fixes bug 1954.
    - When you're using bridges and your network goes away and your
      bridges get marked as down, recover when you attempt a new socks
      connection (if the network is back), rather than waiting up to an
      hour to try fetching new descriptors for your bridges. Bugfix on
      0.2.0.3-alpha; fixes bug 1981.

  o Major bugfixes (on 0.2.2.x):
    - Fix compilation on Windows. Bugfix on 0.2.2.16-alpha; related to
      bug 1797.
    - Fix a segfault that could happen when operating a bridge relay with
      no GeoIP database set. Fixes bug 1964; bugfix on 0.2.2.15-alpha.
    - The consensus bandwidth-weights (used by clients to choose fast
      relays) entered an unexpected edge case in September where
      Exits were much scarcer than Guards, resulting in bad weight
      recommendations. Now we compute them using new constraints that
      should succeed in all cases. Also alter directory authorities to
      not include the bandwidth-weights line if they fail to produce
      valid values. Fixes bug 1952; bugfix on 0.2.2.10-alpha.
    - When weighting bridges during path selection, we used to trust
      the bandwidths they provided in their descriptor, only capping them
      at 10MB/s. This turned out to be problematic for two reasons:
```

```
    Bridges could claim to handle a lot more traffic then they
    actually would, thus making more clients pick them and have a
    pretty effective DoS attack. The other issue is that new bridges
    that might not have a good estimate for their bw capacity yet
    would not get used at all unless no other bridges are available
    to a client. Fixes bug 1912; bugfix on 0.2.2.7-alpha.

o Major bugfixes (on the circuit build timeout feature, 0.2.2.x):
  - Ignore cannibalized circuits when recording circuit build times.
    This should provide for a minor performance improvement for hidden
    service users using 0.2.2.14-alpha, and should remove two spurious
    notice log messages. Bugfix on 0.2.2.14-alpha; fixes bug 1740.
  - Simplify the logic that causes us to decide if the network is
    unavailable for purposes of recording circuit build times. If we
    receive no cells whatsoever for the entire duration of a circuit's
    full measured lifetime, the network is probably down. Also ignore
    one-hop directory fetching circuit timeouts when calculating our
    circuit build times. These changes should hopefully reduce the
    cases where we see ridiculous circuit build timeouts for people
    with spotty wireless connections. Fixes part of bug 1772; bugfix
    on 0.2.2.2-alpha.
  - Prevent the circuit build timeout from becoming larger than
    the maximum build time we have ever seen. Also, prevent the time
    period for measurement circuits from becoming larger than twice that
    value. Fixes the other part of bug 1772; bugfix on 0.2.2.2-alpha.

o Minor features:
  - When we run out of directory information such that we can't build
    circuits, but then get enough that we can build circuits, log when
    we actually construct a circuit, so the user has a better chance of
    knowing what's going on. Fixes bug 1362.
  - Be more generous with how much bandwidth we'd use up (with
    accounting enabled) before entering "soft hibernation". Previously,
    we'd refuse new connections and circuits once we'd used up 95% of
    our allotment. Now, we use up 95% of our allotment, AND make sure
    that we have no more than 500MB (or 3 hours of expected traffic,
    whichever is lower) remaining before we enter soft hibernation.
  - If we've configured EntryNodes and our network goes away and/or all
    our entrynodes get marked down, optimistically retry them all when
    a new socks application request appears. Fixes bug 1882.
  - Add some more defensive programming for architectures that can't
    handle unaligned integer accesses. We don't know of any actual bugs
    right now, but that's the best time to fix them. Fixes bug 1943.
  - Support line continuations in the torrc config file. If a line
    ends with a single backslash character, the newline is ignored, and
    the configuration value is treated as continuing on the next line.
    Resolves bug 1929.

o Minor bugfixes (on 0.2.1.x and earlier):
  - For bandwidth accounting, calculate our expected bandwidth rate
    based on the time during which we were active and not in
```

```
      soft-hibernation during the last interval. Previously, we were
      also considering the time spent in soft-hibernation. If this
      was a long time, we would wind up underestimating our bandwidth
      by a lot, and skewing our wakeup time towards the start of the
      accounting interval. Fixes bug 1789. Bugfix on 0.0.9pre5.

  o Minor bugfixes (on 0.2.2.x):
    - Resume generating CIRC FAILED REASON=TIMEOUT control port messages,
      which were disabled by the circuit build timeout changes in
      0.2.2.14-alpha. Bugfix on 0.2.2.14-alpha; fixes bug 1739.
    - Make sure we don't warn about missing bandwidth weights when
      choosing bridges or other relays not in the consensus. Bugfix on
      0.2.2.10-alpha; fixes bug 1805.
    - In our logs, do not double-report signatures from unrecognized
      authorities both as "from unknown authority" and "not
      present". Fixes bug 1956, bugfix on 0.2.2.16-alpha.
```

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Mike wrote up the current state of progress on a torbutton extension for Google's Chrome web browser, https://blog.torproject.org/blog/google-chrome-incognito-mode-tor-and-fingerprinting.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

Steven submitted a proposal to automatically promote nodes to bridges. This proposal describes how Tor clients could determine when they have sufficient bandwidth capacity and are sufficiently reliable to become either bridges or Tor relays. When they meet this criteria, they will automatically promote themselves, based on user preferences. The proposal also defines the new controller messages and options which will control this process.https://gitweb.torproject.org/tor.git/blob_plain/HEAD:/doc/spec/proposals/175-automatic-node-promotion.txt.

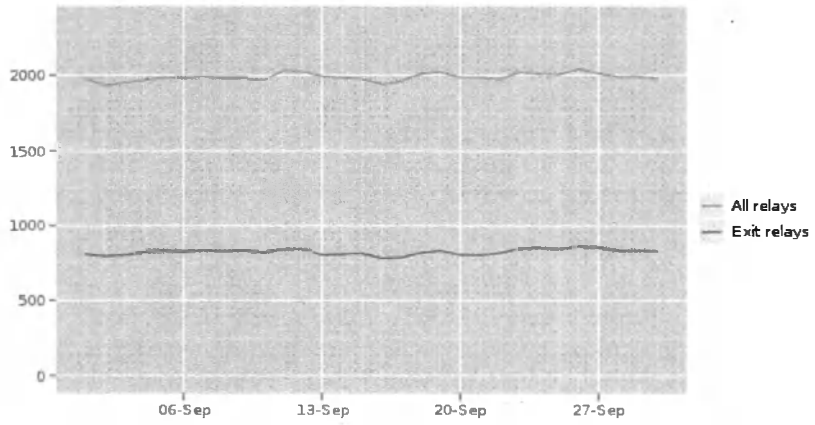
C.2.5. Hide Tor's network signature.

Nothing to report.

C.2.10 Grow the Tor network and user base. Outreach.

Measures of the Tor Network

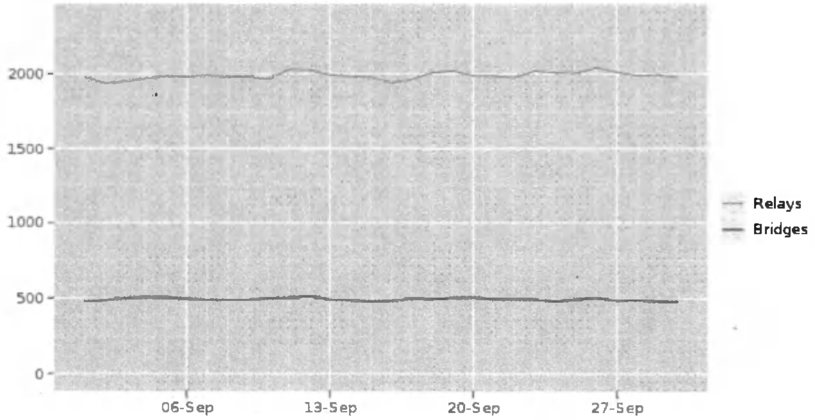
Number of exit relays (September 2010)



The Tor Project - https://metrics.torproject.org/

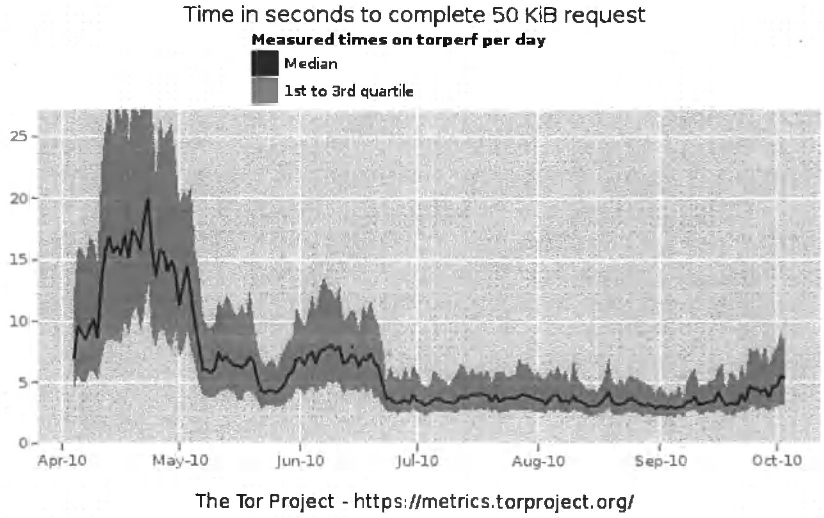
This graph shows the total quantity of relays and quantity of exit relays in September 2010.

Number of relays and bridges (September 2010)



The Tor Project - https://metrics.torproject.org/

This graph shows the total quantity of relays and the total quantity of bridges in September 2010. The quantity of bridges is stable throughout the month.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This measurement is from the server torperf, located in Chicago, Illinois. As you can see, latency continues to be low for the third month in a row.

Outreach and Advocacy

1. We released an article about the "Ten Things to Look for in a Circumvention Tool". As more countries crack down on Internet use, people around the world are turning to anti-censorship software that lets them reach blocked websites. Many types of software, also known as circumvention tools, have been created to answer the threat to freedom online. These tools provide different features and levels of security, and it's important for users to understand the tradeoffs. This article lays out ten features you should consider when evaluating a circumvention tool. The goal isn't to advocate for any specific tool, but to point out what kind of tools are useful for different situations. Full details at `https://www.torproject.org/press/2010-09-16-ten-things-circumvention-tools.html.en`

2. Karen attended a meeting of the United Nations Internet Governance Forum in Vilnius, Lithuania. `http://igf2010.lt/`.

3. Karen attended Ars Electronica in Linz, Austria. Tor received an Honorable Mention for Digital Communities. `http://aec.at`

4. Karen attended InternetLiberty in Budapest, Hungary. `https://sites.google.com/a/pressatgoogle.com/internet-at-liberty-2010/` and `http://jilliancyork.com/tag/ial2010/` for Jillian's summary.

5. Sebastian gave a talk at SourceBarcelona about Anonymity, Privacy, and the real world. `http://www.sourceconference.com/index.php/barcelona-2010/bcn2010-schedule#Jacob`

6. Nick and Andrew held a Boston Hackfest to explain Tor's internals, hack on some Tor simulator code, and generally be available for questions and help on topics relating to Tor. https://blog.torproject.org/blog/boston-tor-hackers-join-us-sunday-september-19th.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- Erinn synchronized the Windows, OS X, and Linux tor browser bundles to use the same configurations and included software.
- The TAILS team continues to improve and update their LiveCD available at https://amnesia.boum.org.
- Jacob began an audit of the TAILS LiveCD to help assess the safety and security of the software for users in highly-volatile situations.

C.2.12 Bridge relay and bridge authority work.

Steven submitted a proposal to automatically promote nodes to bridges. This proposal describes how Tor clients could determine when they have sufficient bandwidth capacity and are sufficiently reliable to become either bridges or Tor relays. When they meet this criteria, they will automatically promote themselves, based on user preferences. The proposal also defines the new controller messages and options which will control this process.https://gitweb.torproject.org/tor.git/blob_plain/HEAD:/doc/spec/proposals/175-automatic-node-promotion.txt.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

Created Tor 0.2.3 branch and started work on integrated bufferevents and microdescriptors. Bufferevents are the proper way to manage heavy network i/o in Microsoft Windows. Microdescriptors are a way to let clients on extremely low-bandwidth connections bootstrap into the Tor network. Proposal 158, https://gitweb.torproject.org/tor.git/blob_plain/HEAD:/doc/spec/proposals/158-microdescriptors.txt, defines microdescriptors.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Nothing to report.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

- Hardware bridge/router, https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/Torouter.
- Cloud computing images, https://trac.torproject.org/projects/tor/wiki/sponsors/SponsorE/PhaseOne.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

- Sebastian and Nick spent some time debugging and resolving the issues with the OpenSSL changes to address a security announcement. The results of this work is included in the Tor 0.2.1.27 and 0.2.2.19-alpha releases. Initially, we did not see any direct relevance to Tor:

  There's a new buffer overflow vulnerability in versions of OpenSSL from 0.9.8f through 0.9.8o, and 1.0.0 through 1.0.0a. You can read the security advisory for the whole story. So far as we can tell from our current analysis, Tor is not affected. Here's why: 'The advisory says: Any OpenSSL based TLS server is vulnerable if it is multi-threaded and uses OpenSSL's internal caching mechanism. Servers that are multi-process and/or disable internal session caching are NOT affected. Tor qualifies for both of the safe cases: Tor does disable OpenSSL's internal session caching. This happens in the file src/common/tortls.c, when we call

  ```
  SSL_CTX_set_session_cache_mode(result->ctx,SSL_SESS_CACHE_OFF).
  ```

  Tor has done this since since version 0.0.2pre6 back in 2003. Also, though Tor is multi-threaded, Tor only calls SSL functionality from a single thread. Thus, no thread other than the main thread will examine or alter the TLS session cache, or any TLS session at all. So it would appear that Tor itself is in the clear. Nonetheless, your other applications might not be. If you're running other SSL services that might be affected, be sure to apply patches from your OS and/or your application to stay safe.'

  This was posted at https://blog.torproject.org/blog/new-openssl-vulnerability-tor-not-affecte as well.

- Karsten implemented the new user number estimate based on directory requests to many directory mirrors in the metrics portal, https://metrics.torproject.org/users.html.
- Karsten finished tech report on estimating user numbers together with Sebastian and with very helpful comments from Roger and Thomas. The report is available on the metrics website, https://metrics.torproject.org/papers.html#techreports and the specific report is at https://metrics.torproject.org/papers/countingusers-2010-11-30.pdf.
- Karsten implemented a few Tor patches, most of them related to metrics, that were kindly reviewed and merged by Nick: made log granularity configurable (1668, 0.2.3.x); included GeoIP database identifier in extra-info descriptors (1883, 0.2.3.x); turned on dirreq-stats by default (2174, 0.2.3.x); fixed a bug where fast relays exceeded the 50K limit for extra-info descriptors (2183, 0.2.2.x); reduced exit-stats to top 10 ports (2196, 0.2.2.x).
- Karsten implemented a few metrics website improvements: all servlets use a database connection pool for their queries; ExoneraTor uses the database tables instead of files; we upgraded to R 2.11.1 after finding out that the reshape package has a problem with large POSIXlt vectors.

version work. https://www.torproject.org. It features an entirely redesigned Information Architecture, user experience design, and codebase. Andrew, Roger, Sebastian, Runa, and many volunteers contributed to this release.

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Nick continued to work on the codebase around microdescriptors. Microdescriptors will allow clients on very low bandwidth connections to use the tor network more quickly than waiting to download the current directory information.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

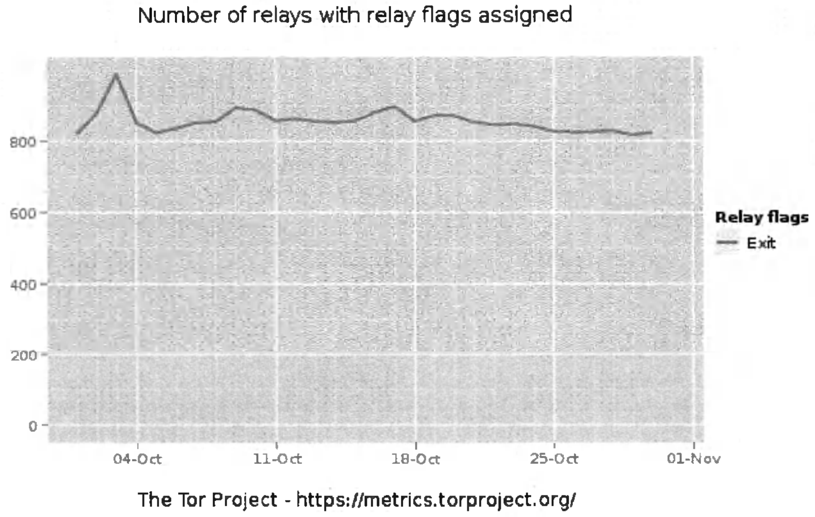
Nothing to report.

C.2.5. Hide Tor's network signature.

Nothing to report.

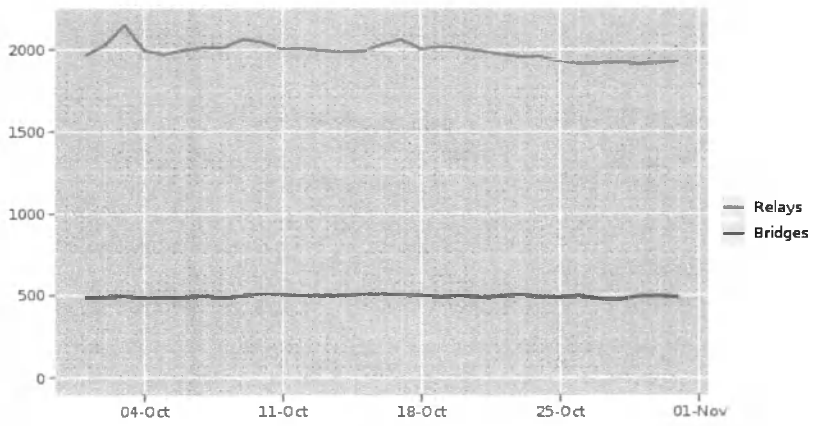
C.2.10 Grow the Tor network and user base. Outreach.

Measures of the Tor Network



This graph shows the total quantity of relays and quantity of exit relays in October 2010.

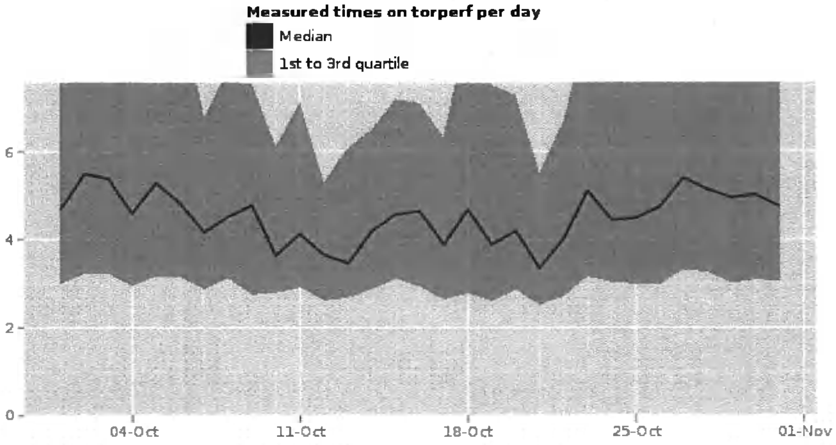
Number of relays



The Tor Project - https://metrics.torproject.org/

This graph shows the total quantity of relays and the total quantity of bridges in October 2010. The quantity of bridges is stable throughout the month.

Time in seconds to complete 50 KiB request



The Tor Project - https://metrics.torproject.org/

This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This measurement is from the server torperf, located in Chicago, Illinois. As you can see, latency continues to be low.

Outreach and Advocacy

1. Roger speaks at Internet Dagarna in Sweden, `http://www.internetdagarna.se/`. The video of his talk is provided by the Internet Foundation at `http://www.youtube.com/watch?v=35156KjTCb8&p=5BE29144D1FD2779`.

2. Roger, Ian, and others attended WPES2010, Workshop on Privacy in the Electronic Society, `http://wpes10.csi.muohio.edu/`.

3. Roger, Ian, and others attended 17th ACM Conference on Computer and Communications Security, `http://www.sigsac.org/ccs/CCS2010/`.

4. Roger, Paul, and Andrew attended the Information Technology Study Group (ITSG).

5. Jacob attended Bluehat, `http://technet.microsoft.com/en-us/security/cc261637.aspx`.

6. Roger gave a lecture at the State University of New York - Stonybrook.

7. Jacob attended the Workshop on Elliptic Curve Cryptography, `http://2010.eccworkshop.org/`.

8. Roger, Mike, Jacob, Erinn represented Tor at the Google Summer of Code Mentor Summit.

9. Roger gave a lecture at Stanford University, `http://crypto.stanford.edu/seclab/sem.html`.

10. Andrew, Karen, and Linus met with the Swedish Foreign Ministry, Swedish International Development Agency `http://www.sida.se/`, and NorduNet `http://www.nordu.net/`.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- A number of tor browser bundle releases in October.
- Working with the TA(I)LS LiveCD/LiveUSB team to get architecture designs, specifications, and goals written down and published. The desired state is to be able to analyze the live system for a number of security and anonymity properties through security and code audits.

C.2.12 Bridge relay and bridge authority work.

Mike began investigating the odd reality that we only report 500 bridges available at any point in time. Hundreds to thousands of people become bridges each week, but only around 500 are reported as being available at any point in time. This seems an odd coincidence to Mike and others. Research continues.

```
    were open. Bugfix on 0.2.1.26; fixes bug 1840. Thanks to mingw-san
    for analysis help.
  - Rate-limit "Failed to hand off onionskin" warnings.
  - Never relay a cell for a circuit we have already destroyed.
    Between marking a circuit as closeable and finally closing it,
    it may have been possible for a few queued cells to get relayed,
    even though they would have been immediately dropped by the next
    OR in the circuit. Fixes bug 1184; bugfix on 0.2.0.1-alpha.
  - Never queue a cell for a circuit that's already been marked
    for close.
  - Never vote for a server as "Running" if we have a descriptor for
    it claiming to be hibernating, and that descriptor was published
    more recently than our last contact with the server. Bugfix on
    0.2.0.3-alpha; fixes bug 911.
  - Squash a compile warning on OpenBSD. Reported by Tas; fixes
    bug 1848.

o Minor bugfixes (on 0.2.2.x):
  - Fix a regression introduced in 0.2.2.7-alpha that marked relays
    down if a directory fetch fails and you've configured either
    bridges or EntryNodes. The intent was to mark the relay as down
    _unless_ you're using bridges or EntryNodes, since if you are
    then you could quickly run out of entry points.
  - Fix the Windows directory-listing code. A bug introduced in
    0.2.2.14-alpha could make Windows directory servers forget to load
    some of their cached v2 networkstatus files.
  - Really allow clients to use relays as bridges. Fixes bug 1776;
    bugfix on 0.2.2.15-alpha.
  - Demote a warn to info that happens when the CellStatistics option
    was just enabled. Bugfix on 0.2.2.15-alpha; fixes bug 1921.
    Reported by Moritz Bartl.
  - On Windows, build correctly either with or without Unicode support.
    This is necessary so that Tor can support fringe platforms like
    Windows 98 (which has no Unicode), or Windows CE (which has no
    non-Unicode). Bugfix on 0.2.2.14-alpha; fixes bug 1797.

o Testing
  - Add a unit test for cross-platform directory-listing code.
```

5. We released Torbutton 1.3.0-alpha. Torbutton 1.3.0-alpha is the first release of Torbutton where most of the code has come from our community members! The full announcement is available at `http://archives.seul.org/or/talk/Sep-2010/msg00140.html`. The complete changelog is:

   - new: Support for transparent proxies in settings (patch from Jacob Appelbaum and Kory Kirk)
   - new: tor:// and tors:// url support to auto-toggle into tor mode (patch from Kory Kirk)
   - new: Cookie manager to allow individual Cookie protection (patch from Kory Kirk)
   - new: Add referrer spoofing based on modified same origin policy (patch from Kory Kirk)

C.2.17 Translation work, ultimately a browser-based approach.

- We began the migration from our Pootle-based translation portal to Transifex after a discussion with their developers. Transifex provides free hosting of their translation software for free software projects and access to thousands of translators shared between hosted projects. All of our translations will be completed through Transifex going forward. `https://www.transifex.net/projects/p/torproject/`.
- Updated translations for Russian, Arabic, Persian, Greek, Burmese, French, Italian, Swedish, Dutch, German, Spanish, Polish, and Simplified Chinese.

February 7, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-third invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b) (6) if there are any questions.

Invoice 33:

Period	Months	Rate	Cost
01/01/2011 - 01/31/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG02072011

January 11, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-second invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b)(6) if there are any questions.

Invoice 32:

Period	Months	Rate	Cost
12/01/2010 - 12/31/2010	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG01112011

March 15, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-fourth invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b) (6) if there are any questions.

Invoice 34:

Period	Months	Rate	Cost
02/01/2011 - 02/28/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG03152011

April 8, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-fifth invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b) (6) if there are any questions.

Invoice 35:

Period	Months	Rate	Cost
03/01/2011 - 03/31/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG04082011

May 31, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-sixth invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b) (6) if there are any questions.

Invoice 36:

Period	Months	Rate	Cost
03/17/2011 - 04/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG05312011

June 14, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-seventh invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b) (6) if there are any questions.

Invoice 37:

Period	Months	Rate	Cost
04/17/2011 - 05/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG06142011

December 14, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-eighth invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b)(6) if there are any questions.

Invoice 38:

Period	Months	Rate	Cost
05/17/2011 - 06/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG07112011

August 10, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our thirty-ninth invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b)(6) if there are any questions.

Invoice 39:

Period	Months	Rate	Cost
06/17/2011 - 07/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG08102011

September 15, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our fortieth invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b)(6) if there are any questions.

Invoice 40:

Period	Months	Rate	Cost
07/17/2011 - 08/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG09152011

October 17, 2011

Broadcasting Board of Governors
International Broadcasting Bureau
Office of Engineering
Cohen Building, Room 4300
330 Independence Avenue, SW
Washington, DC 20237
Attn: Malita Dyson

Dear Ms. Dyson,

Below is our 41st invoice for contract number BBGCON1808C6700, Accounting Appropriation Data 9568-08-0206-E009701048A.

There are no travel costs. Services rendered include blocking resistance architecture and testing, scalability and promotion and advocacy for the Tor network, and other detailed tasks under 0001 of our contract as confirmed in our status reports to BBG.

Please do not hesitate to email me at andrew@torproject.org or call me at (b)(6) if there are any questions.

Invoice 41:

Period	Months	Rate	Cost
08/17/2011 - 09/17/2011	1	$15,000	$15,000

Thank you.
Sincerely,

Andrew Lewman
Executive Director

TorProject Invoice BBG10172011

F.1. The contractor shall improve client software usability through technical development. Topics to be considered (depending on level of funding) include customizing Tor Browser Bundle's start page and other configuration options like bookmarks; automated regular TBB builds and updates (for Windows, Mac OS X, and Linux) that track updates in included software components; continued work on Torbutton to keep TBB users safe at the application layer, and to better support streaming media in TBB; launching a "bug bounty" project to crowd-source security and usability improvements in our software; adding a security sandbox around TBB and integrating Flash into the sandbox so users can safely use Flash; maintenance, support, and development of the Tails Live System; forensics work to identify and resolve fingerprints left by TBB and its components; and improving integration and usability for the "HTTPS Everywhere" Firefox extension.

F.2. The contractor shall provide an improved user experience through better user support. Topics to be considered (depending on level of funding) include full-time dedicated user support staff; dedicated "quality assurance" engineers to write automated tests, maintain an experimental Tor network for testing, reproduce bug reports and gather logs, etc; funding new translations, and keeping translations up-to-date, to track software updates and to target new languages; developing and translating new user support documentation including videos; and deploying and maintaining localized portals to help grow communities that can help themselves.

F.3. The contractor shall improve the diversity and capacity of the Tor network, leading to better safety and better performance. Topics to be considered (depending on level of funding) include sponsoring the bandwidth and/or maintenance costs for high-capacity Tor relays; operating more Tor relays in clouds like the Amazon cloud; technical improvements to the Tor design to better handle relays on dynamic IP addresses; and technical improvements to Tor that allow suitable clients to smoothly become promoted to being relays.

F.4. The contractor shall improve the diversity and capacity of Tor bridges, leading to more avenues for blocked users to reach the Tor network and better performance while doing so. Topics to be considered (depending on level of funding) include development and deployment of a small "Tor router" hardware device that will automatically run a bridge, including work on a graphical interface for configuring the Tor router; regular Tor package builds that are preconfigured to be a bridge relay; software glue and coordination plans for running an entire Internet subnet as a single bridge, allowing us to choose which addresses will be available as Tor bridges at any given time while making sure the rest don't look like bridges; and more experimental bridge deployment strategies such as "Flash bridges" that make use of short-term browser-donated resources from volunteers.

F.5. The contractor shall collect, publish, and analyze network usage and performance data. Network usage statistics include per-country daily aggregated user counts for both direct Tor connections and bridge connections. Performance statistics include tracking the size (number, capacity, and load) of relays and bridges, as well as tracking the latency offered by the network over time.

F.6. The contractor shall provide technical expertise in Internet censorship circumvention to further the BBG's other Internet anti-censorship initiatives. Depending on level of funding, work in this area includes evaluating, improving, and coordinating with other circumvention and security tools and projects, including other projects funded by or under consideration of funding by BBG; explanations of details or broader implications of censorship-related events or attacks such as Certificate Authority compromises; investigation of operation or deployment of commercial censorship equipment; helping to explain and understand the methodology used in various censorship measurement or usage studies; helping target users and organizations assess and understand risks to online communications and capabilities of possible adversaries; and producing technical documentation and data or reports on the current state of Internet censorship in target countries.

Client software:
* custom start page for tbb, plus tbb updates, 100k
* torbutton work for tbb, 100k
  - make streaming work better, 150k
- bug bounties, 50k
- flash-enabled tbb:
  - sandboxing for 175k
  - integrate flash for 100k
- tails, 200k
- forensics, 150k
- https everywhere, 50k

= 1075k (200k if only funding the critical subset)

User support:
* actual user support, 150k
* QA person for consistent package releases, 150k
* do and maintain translations, 75k
- videos (and translated), 75k
- localized portals, 100k

= 550k (375k if only funding the critical subset)

More relays:
* funding traditional tor relays, 125k
* tor relays in cloud, 75k
- better handle relays with dynamic IP, 75k
- everybody-a-relay, 250k

= 525k (200k if only funding the critical subset)

More bridges:
* torouter, 100k
  - plus gui, 100k
- bridge-by-default bundles, 25k
- redirect address blocks into tor, 250k
- flash proxy design, 100k plus 50k for promotion

= 625k (100k if only funding the critical subset)

Metrics:
* metrics, 125k

= 125k (125k)

Task 5:
* Help evaluate/coordinate other BBG projects, 200k

= 200k (200k)

Totals 3100k (1200k if only funding the critical subset)