From: Andrew Lewman, Executive Director
To: the tor community
Date: July 12, 2011

This report documents progress in June 2011.

New releases, new hires, new funding

New Funding

The US National Science Foundation funds the second year of grant number CNS-0959138. This funds research into Tor Metrics. This grant is the main driver behind `https://metrics.torproject.org`.

New Releases

1. On June 4th we released the latest in the -beta series, Tor 0.2.2.28-beta. Tor 0.2.2.28-beta makes great progress towards a new stable release: we fixed a big bug in whether relays stay in the consensus consistently, we moved closer to handling bridges and hidden services correctly, and we started the process of better handling the dreaded "my Vidalia died, and now my Tor demands a password when I try to reconnect to it" usability issue.

```
Changes in version 0.2.2.28-beta
  o Major bugfixes:
    - Don't decide to make a new descriptor when receiving a HUP signal.
      This bug has caused a lot of 0.2.2.x relays to disappear from the
      consensus periodically. Fixes the most common case of triggering
      bug 1810; bugfix on 0.2.2.7-alpha.
    - Actually allow nameservers with IPv6 addresses. Fixes bug 2574.
    - Don't try to build descriptors if "ORPort auto" is set and we
      don't know our actual ORPort yet. Fix for bug 3216; bugfix on
      0.2.2.26-beta.
    - Resolve a crash that occurred when setting BridgeRelay to 1 with
      accounting enabled. Fixes bug 3228; bugfix on 0.2.2.18-alpha.
    - Apply circuit timeouts to opened hidden-service-related circuits
      based on the correct start time. Previously, we would apply the
      circuit build timeout based on time since the circuit's creation;
      it was supposed to be applied based on time since the circuit
      entered its current state. Bugfix on 0.0.6; fixes part of bug 1297.
    - Use the same circuit timeout for client-side introduction
```

```
    circuits as for other four-hop circuits, rather than the timeout
    for single-hop directory-fetch circuits; the shorter timeout may
    have been appropriate with the static circuit build timeout in
    0.2.1.x and earlier, but caused many hidden service access attempts
    to fail with the adaptive CBT introduced in 0.2.2.2-alpha. Bugfix
    on 0.2.2.2-alpha; fixes another part of bug 1297.
  - In ticket 2511 we fixed a case where you could use an unconfigured
    bridge if you had configured it as a bridge the last time you ran
    Tor. Now fix another edge case: if you had configured it as a bridge
    but then switched to a different bridge via the controller, you
    would still be willing to use the old one. Bugfix on 0.2.0.1-alpha;
    fixes bug 3321.

o Major features:
  - Add an __OwningControllerProcess configuration option and a
    TAKEOWNERSHIP control-port command. Now a Tor controller can ensure
    that when it exits, Tor will shut down. Implements feature 3049.
  - If "UseBridges 1" is set and no bridges are configured, Tor will
    now refuse to build any circuits until some bridges are set.
    If "UseBridges auto" is set, Tor will use bridges if they are
    configured and we are not running as a server, but otherwise will
    make circuits as usual. The new default is "auto". Patch by anonym,
    so the Tails LiveCD can stop automatically revealing you as a Tor
    user on startup.

o Minor bugfixes:
  - Fix warnings from GCC 4.6's "-Wunused-but-set-variable" option.
  - Remove a trailing asterisk from "exit-policy/default" in the
    output of the control port command "GETINFO info/names". Bugfix
    on 0.1.2.5-alpha.
  - Use a wide type to hold sockets when built for 64-bit Windows builds.
    Fixes bug 3270.
  - Warn when the user configures two HiddenServiceDir lines that point
    to the same directory. Bugfix on 0.0.6 (the version introducing
    HiddenServiceDir); fixes bug 3289.
  - Remove dead code from rend_cache_lookup_v2_desc_as_dir. Fixes
    part of bug 2748; bugfix on 0.2.0.10-alpha.
  - Log malformed requests for rendezvous descriptors as protocol
    warnings, not warnings. Also, use a more informative log message
    in case someone sees it at log level warning without prior
    info-level messages. Fixes the other part of bug 2748; bugfix
    on 0.2.0.10-alpha.
  - Clear the table recording the time of the last request for each
    hidden service descriptor from each HS directory on SIGNAL NEWNYM.
    Previously, we would clear our HS descriptor cache on SIGNAL
```

```
    NEWNYM, but if we had previously retrieved a descriptor (or tried
    to) from every directory responsible for it, we would refuse to
    fetch it again for up to 15 minutes. Bugfix on 0.2.2.25-alpha;
    fixes bug 3309.
  - Fix a log message that said "bits" while displaying a value in
    bytes. Found by wanoskarnet. Fixes bug 3318; bugfix on
    0.2.0.1-alpha.
  - When checking for 1024-bit keys, check for 1024 bits, not 128
    bytes. This allows Tor to correctly discard keys of length 1017
    through 1023. Bugfix on 0.0.9pre5.

o Minor features:
  - Relays now log the reason for publishing a new relay descriptor,
    so we have a better chance of hunting down instances of bug 1810.
    Resolves ticket 3252.
  - Revise most log messages that refer to nodes by nickname to
    instead use the "$key=nickname at address" format. This should be
    more useful, especially since nicknames are less and less likely
    to be unique. Resolves ticket 3045.
  - Log (at info level) when purging pieces of hidden-service-client
    state because of SIGNAL NEWNYM.

o Removed options:
  - Remove undocumented option "-F" from tor-resolve: it hasn't done
    anything since 0.2.1.16-rc.
```

2. On June 20th, we released the latest in the -beta series, Tor 0.2.2.29-beta. Tor 0.2.2.29-beta reverts an accidental behavior change for users who have bridge lines in their torrc but don't want to use them; gets us closer to having the control socket feature working on Debian; and fixes a variety of smaller bugs.

```
Changes in version 0.2.2.29-beta
  o Major bugfixes:
    - Revert the UseBridges option to its behavior before 0.2.2.28-beta.
      When we changed the default behavior to "use bridges if any
      are listed in the torrc", we surprised users who had bridges
      in their torrc files but who didn't actually want to use them.
      Partial resolution for bug 3354.

  o Privacy fixes:
    - Don't attach new streams to old rendezvous circuits after SIGNAL
      NEWNYM. Previously, we would keep using an existing rendezvous
      circuit if it remained open (i.e. if it were kept open by a
      long-lived stream, or if a new stream were attached to it before
      Tor could notice that it was old and no longer in use). Bugfix on
```

```
    0.1.1.15-rc; fixes bug 3375.

  o Minor bugfixes:
    - Fix a bug when using ControlSocketsGroupWritable with User. The
      directory's group would be checked against the current group, not
      the configured group. Patch by Jérémy Bobbio. Fixes bug 3393;
      bugfix on 0.2.2.26-beta.
    - Make connection_printf_to_buf()'s behaviour sane. Its callers
      expect it to emit a CRLF iff the format string ends with CRLF;
      it actually emitted a CRLF iff (a) the format string ended with
      CRLF or (b) the resulting string was over 1023 characters long or
      (c) the format string did not end with CRLF *and* the resulting
      string was 1021 characters long or longer. Bugfix on 0.1.1.9-alpha;
      fixes part of bug 3407.
    - Make send_control_event_impl()'s behaviour sane. Its callers
      expect it to always emit a CRLF at the end of the string; it
      might have emitted extra control characters as well. Bugfix on
      0.1.1.9-alpha; fixes another part of bug 3407.
    - Make crypto_rand_int() check the value of its input correctly.
      Previously, it accepted values up to UINT_MAX, but could return a
      negative number if given a value above INT_MAX+1. Found by George
      Kadianakis. Fixes bug 3306; bugfix on 0.2.2pre14.
    - Avoid a segfault when reading a malformed circuit build state
      with more than INT_MAX entries. Found by wanoskarnet. Bugfix on
      0.2.2.4-alpha.
    - When asked about a DNS record type we don't support via a
      client DNSPort, reply with NOTIMPL rather than an empty
      reply. Patch by intrigeri. Fixes bug 3369; bugfix on 2.0.1-alpha.
    - Fix a rare memory leak during stats writing. Found by coverity.

  o Minor features:
    - Update to the June 1 2011 Maxmind GeoLite Country database.

  o Code simplifications and refactoring:
    - Remove some dead code as indicated by coverity.
    - Remove a few dead assignments during router parsing. Found by
      coverity.
    - Add some forgotten return value checks during unit tests. Found
      by coverity.
    - Don't use 1-bit wide signed bit fields. Found by coverity.
```

3. On June 12th, the anonymous operating system, Tails, version 0.7.2 was released. This release fixes some critical bugs in the included software.

```
   * Iceweasel
```

```
  - Disable Torbutton's external application launch warning.
    ... which advises using Tails. Tails *is* running Tails.
  - FoxyProxy: install from Debian instead of the older one we previously
    shipped.

  * Software
  - haveged: install an official Debian backport instead of a custom backport.
  - unrar: install the version from Debian's non-free repository.
    Users report unrar-free does not work well enough.
```

4. On June 25th, we released new Tor Browser Bundles. All of the alpha Tor Browser Bundles have been updated to the latest Tor 0.2.2.29-beta.

   Firefox 5 has recently been released and our next set of Firefox alpha bundles will come with that instead of Firefox 4. For users who want to use Firefox 5 now, Torbutton 1.3.3-alpha is compatible.

   We're also going to begin phasing out the Firefox 3.6 bundles within the next month. Mike Perry is focusing his attention on the new Firefox releases and we feel this is the best path to keep our users safe. You can also see his current Firefox patches in the Tor Browser Bundle git repository.

   The following changelogs encompass the would-be Tor 0.2.2.28-beta packages as well as the changes made for Tor 0.2.2.29-beta.

```
Firefox 3.6 Tor Browser Bundles

OS X bundle
1.1.19: Released 2011-06-21

    * Update Tor to 0.2.2.29-beta
    * Update NoScript to 2.1.1.1
    * Update HTTPS-Everywhere to 0.9.9.development.6

1.0.18: Released 2011-06-05

    * Update Tor to 0.2.2.28-beta
    * Update Libevent to 2.0.12-stable
    * Update zlib to 1.2.5
    * Update NoScript to 2.1.1
    * Update BetterPrivacy to 1.51

Linux bundles
1.1.11: Released 2011-06-21

    * Update Tor to 0.2.2.29-beta
    * Update NoScript to 2.1.1.1
```

```
    * Update HTTPS-Everywhere to 0.9.9.development.6

1.1.10: Released 2011-06-05

    * Update Tor to 0.2.2.28-beta
    * Update Libevent to 2.0.12-stable
    * Update zlib to 1.2.5
    * Update NoScript to 2.1.1
    * Update BetterPrivacy to 1.51

Firefox 4 Tor Browser Bundles

Tor Browser Bundle (2.2.29-1)

    * Update Tor to 0.2.2.29-beta
    * Update Libevent to 2.0.12-stable
    * Update HTTPS Everywhere to 0.9.9.development.6
    * Update NoScript to 2.1.1.1
    * Update BetterPrivacy to 1.51
```

5. On June 4th, released the latest in the libevent -stable series, 2.0.12.

```
BUGFIXES
 o Fix a warn-and-fail bug in kqueue by providing kevent() room to report
 errors (28317a0)
 o Fix an assert-inducing fencepost bug in the select backend (d90149d)
 o Fix failing http assertion introducd in commit 0d6622e (0848814
 Kevin Ko)
 o Fix a bug that prevented us from configuring IPv6 nameservers. (74760f1)
 o Prevent size_t overflow in evhttp_htmlescape. (06c51cd Mansour Moufid)
 o Added several checks for under/overflow conditions in
 evhttp_handle_chunked_read (a279272 Mark Ellzey)
 o Added overflow checks in evhttp_read_body and evhttp_get_body (84560fc
 Mark Ellzey)

DOCUMENTATION:
 o Add missing words to EVLOOP_NONBLOCK documentation (9556a7d)

BUILD FIXES
 o libssl depends on libcrypto, not the other way around. (274dd03
 Peter Rosin)
 o Libtool brings in the dependencies of libevent_openssl.la automatically
 (7b819f2 Peter Rosin)
 o Use OPENSSL_LIBS in Makefile.am (292092e Sebastian Hahn)
 o Move the win32 detection in configure.in (ceb03b9 Sebastian Hahn)
```

```
o Correctly detect openssl on windows (6619385 Sebastian Hahn)
o Fix a compile warning with zlib 1.2.4 and 1.2.5 (5786b91 Sebastian
Hahn)
o Fix compilation with GCC 2, which had no __builtin_expect (09d39a1
Dave Hart)
o Fix new warnings from GCC 4.6 (06a714f)
o Link with -lshell32 and -ladvapi32 on Win32. (86090ee Peter Rosin)
o Make the tests build when OpenSSL is not available. (07c41be Peter
Rosin)
o Bring in the compile script from automake, if needed. (f3c7a4c
Peter Rosin)
o MSVC does not provide S_ISDIR, so provide it manually. (70be7d1
Peter Rosin)
o unistd.h and sys/time.h might not exist. (fe93022 Peter Rosin)
o Make sure TINYTEST_LOCAL is defined when building tinytest.c (8fa030c
Peter Rosin)
o Fix winsock2.h #include issues with MSVC (3d768dc Peter Rosin)
o Use evutil_gettimeofday instead of relying on the system
gettimeofday. (0de87fe Peter Rosin)
o Always use evutil_snprintf, even if OS provides it (d1b2d11 Sebastian
Hahn)
o InitializeCriticalSectionAndSpinCount requires _WIN32_WINNT >=
0x0403. (816115a Peter Rosin)
o cygwin: make it possible to build DLLs (d54d3fc)
```

6. On June 30th, we released the latest stable version of torbutton, 1.4.0.

```
The addon has been disabled on addons.mozilla.org. Our URL is now
canonical.

This release features support for Firefox 5.0, and has been tested
against the vanilla release for basic functionality. However, it has
not been audited for Network Isolation, State Separation, Tor
Undiscoverability or Interoperability issues[1] due to toggling under
Firefox 5.

If you desire Torbutton functionality with Firefox 4/5, we recommend
you download the Tor Browser Bundle 2.2.x alphas from
https://www.torproject.org/dist/torbrowser/ or run Torbutton in its
own separate Firefox profile.

The reasons for this shift are explained here:
https://blog.torproject.org/blog/toggle-or-not-toggle-end-torbutton

If you find bugs specific to Firefox 5, toggling, and/or extension
```

```
conflicts, file them under the component "Torbutton":
https://trac.torproject.org/projects/tor/report/14

Bugs that still apply to Tor Browser should be filed under component
"TorBrowserButton":
https://trac.torproject.org/projects/tor/report/39

Bugs in the "Torbutton" component currently have no maintainer
available to fix them. Feel free to step up.

Here is the complete changelog:
* bug 3101: Disable WebGL. Too many unknowns for now.
* bug 3345: Make Google Captcha redirect work again.
* bug 3399: Fix a reversed exception check found by arno.
* bug 3177: Update torbutton to use new TorBrowser prefs.
* bug 2843: Update proxy preferences window to support env var.
* bug 2338: Force toggle at startup if tor is enabled
* bug 3554: Make Cookie protections obey disk settings
* bug 3441: Enable cookie protection UI by default.
* bug 3446: We're Firefox 5.0, we swear.
* bug 3506: Remove window resize event listener.
* bug 1282: Set fixed window size for each new window.
* bug 3508: Apply Stanford SafeCache patch (thanks Edward, Collin et al).
* bug 2361: Make about window work again on FF4+.
* bug 3436: T(A)ILS was renamed to Tails.
* bugfix: Fix a transparent context menu issue on Linux FF4+.
* misc: Squelch exception from app launcher in error console.
* misc: Make DuckDuckGo the default Google Captcha redirect destination.
* misc: Make it harder to accidentally toggle torbutton.

1. https://www.torproject.org/torbutton/en/design/#requirements
```

7. We released two new updates to tordnsel to address a number of bugs and add new features.

```
version 0.1.1 - 2011-06-28
  - Correctly label the release version and Changelog.
  - Add updated website and maintainers in tordnsel.cabal.
  - Document the tordnsel init script for Debian.

version 0.1.0 - 2011-06-28
  o Deployment:
    - Add support for logging messages to stdout, stderr, syslog, or to a file.
      Syslog logging should be useful for running in a chroot.
    - Display better error messages for config file parsing, directory parsing,
      Tor controller errors, I/O errors, and almost every error condition.
    - Add a man page fully documenting config options, signals, files, sockets,
```

```
    and exit codes.
  - Add support for reloading the configuration by reloading the config file
    when we receive SIGHUP, or by listening for the contents of the config
    file on a Unix domain socket. The latter is useful for running in a
    chroot, where the process can't access its own config file.
  - Implement the reload command in the sample init.d script using the new
    --reconfigure command-line option, which reloads the config file through
    a Unix domain socket for chroot-friendliness.
  - Exit gracefully when we receive SIGINT or SIGTERM.
  - Add a --verify-config command-line option for checking whether the config
    file is well-formed without starting TorDNSEL. Apply it in the sample
    init.d script.
  - Add --help and --version command-line options.

o Reliability:
  - Implement Erlang-style thread links and monitors for error handling.
  - Refactor every thread to support a start/reconfigure/terminate API.
  - Each thread now runs in a fault-tolerant supervision hierarchy in which
    the thread is responsible for handling errors in its children, and its
    supervisor handles errors in it. If a thread dies unexpectedly, the reason
    it died is logged and its supervisor attempts to restart it when possible.

o New required options:
  - Create a new required RuntimeDirectory option for the statistics and
    reconfigure sockets.
  - Rename the AuthoritativeZone option to ZoneOfAuthority, since name servers
    are authoritative, not zones.

o Performance:
  - Share copies of exit policy rules and exit policies with a hash table of
    weak pointers. According to nickm, only 5% of them are distinct.
  - Squash some space leaks in network state updates.

o Standards conformance:
  - Stop requiring that reserved bits in the DNS header be 0.

o Active tests:
  - Replace the ConcurrentExitTests option with EnableActiveTesting, since we
    now automatically detect limits imposed on open file descriptors by
    FD_SETSIZE and resource limits.
  - Refactor the exit test initiator to keep a history of scheduled exit tests
    and dynamically adjust the rate at which tests are initiated. This should
    smooth out the pubkey crypto demands on Tor that were maxing out CPU
    utilization.
  - Make a better effort to avoid redundant testing by storing pending tests
```

```
    in a distinct queue.
  - Stop testing every node periodically between descriptor publications.
    Instead, every hour attempt to test through any exit nodes that haven't
    been successfully tested since they last published a descriptor. This
    should have a similar effect of catching nodes that slipped through an
    earlier attempted test.
  - Regenerate the exit-addresses store every time a new network status
    consensus is received instead of every 15 minutes.
  - Reduce the maximum relay age from 48 hours to 24 hours.  This should
    cut down the length of time a relay is listed in the exitlist after
    it has been disabled or changed to a non-exit relay.

o Controller:
  - Close controller connections cleanly with the QUIT command.
  - Add support for authenticating with PROTOCOLINFO.
  - Set the new FetchDirInfoEarly option to enable fetching dir info on the
    mirror schedule, preferably from authorities.
  - Ensure that config options we set are rolled back to their previous state
    when a controller connection is closed cleanly.
```

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

- Vidalia improvements:

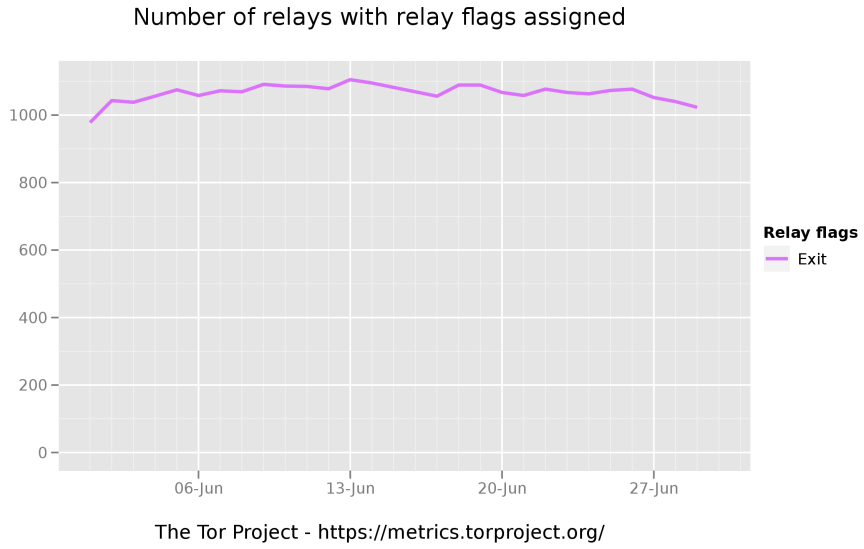
```
Regarding Vidalia:
- worked in the plugin framework. This involved writing the spec,
  working on the engine itself, and then building the interfaces to Qt
  and Vidalia/TorControl. I used qtscriptgenerator to interface Qt,
  which worked really nice and almost out of the box.
- spent a while discussing the problem of the tri-state UseBridges
  feature and preparing a 0.2.13 emergency release, but it never got
  through, and the fixes for this particular case are on stall for now.
- implemented detachable tabs to give more flexibility to plugins, and
  the basice GUI.
- implemented the Vidalia side of the *Port auto feature.

Regarding Vidalia Plugins:
- created a test plugin to implement a testing GUI to
  obfsproxy.
- migrated the TBB code to a plugin, and removed those parts from
  Vidalia.

Regarding Thandy:
- spent some time getting to know the code and discussing different
```

```
    parts of the thp spec with Nick, Robert, and Sebastian.
  - implemented the thp spec, we are about to start testing it with real
    packages. The idea (or at least my idea) is to release this with
    Vidalia-0.3.1, along with the corresponding plugin to control it.
```

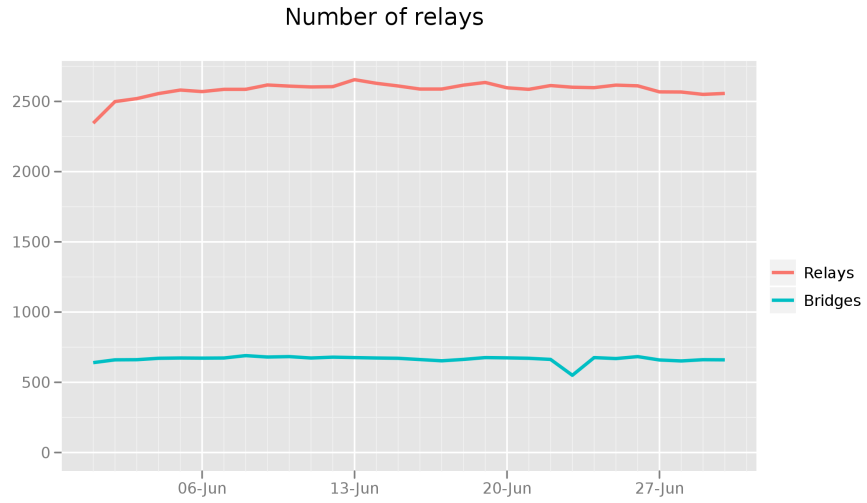
Hide Tor's network signature.

Grow the Tor network and user base. Outreach.

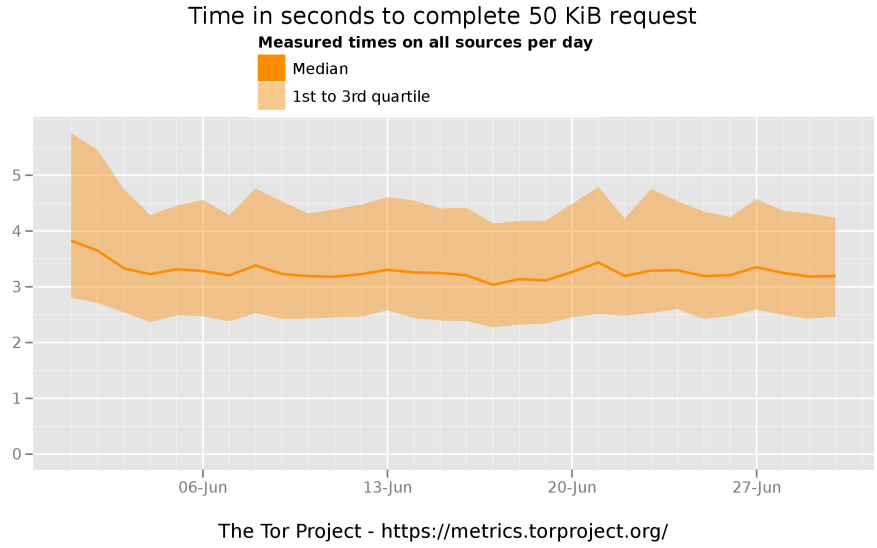
Measures of the Tor Network



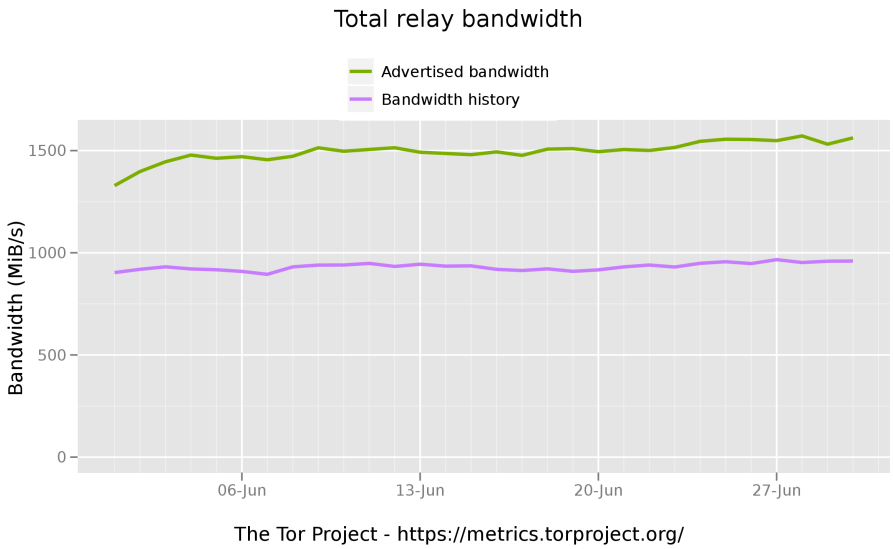
This graph shows the total quantity of exit relays in June 2011. We seem to have kept most of our relays since the bump due to the EFF Tor challenge started in May 2011.



This graph shows the total quantity of relays and the total quantity of bridges in June 2011. We seem to have kept most of our relays since the bump due to the EFF Tor Challenge started in May 2011.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Performance remains relatively steady at just under 4 seconds.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. The steady-state of relays creates almost 1.5GBps (12.0 Gbps) of bandwidth available.

Outreach and Advocacy

1. Runa attended the London CyberSecurity Summit, `http://www.cybersummit2011.com/`.
2. Jacob and Linus spoke at the NORDUnet conference, `https://portal.nordu.net/display/ndn2011web/index`.
3. Andrew spoke at the Allied Media conference, `http://alliedmedia.org/`.
4. Jacob spoke at FISL12 in Porto Allegre, Brazil, `http://softwarelivre.org/fisl12`.
5. Tor was featured by CNN for protecting whistleblower's anonymity, `http://www.cnn.com/2011/TECH/web/06/11/hiding.online.identity/index.html`.
6. Tor was featured by CNN for its role in the Arab Spring, `http://www.cnn.com/2011/TECH/innovation/06/17/mesh.technology.revolution/index.html`.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- Mike wrote up his thoughts on improving private browsing modes, `https://blog.torproject.org/blog/improving-private-browsing-modes-do-not-track-vs-real-privacy-design`.
- See the new bundles as released in the "New Releases" section.
- ARM is making tremendous progress over the past month.

Several new features and is now tantalizingly
close to its 1.4.3 release. Improvements include...
* Menu interface (thanks to Kamran for implementing its first version)
* TorCtl fixes for 2412, 2812, 2065, 1329, 2580, 3406, and 3409 [1-7]
* Newnym option
* Dependency auto-fetching via mirrors with signature checks (issue
spotted by Sebastian and Robert)
* Relay setup wizard. This is still in the works and about a week away
from completion, but it's turning out very nicely.

Kamran has made some progress with the arm gui, porting the bandwidth
graphs and nearly finishing the log panel. This has slipped quite a
bit due to illness and family issues, though the parts that are done
look great. For a description and screenshot of his work see his blog
posting [8].

Finally, dug into arm's resource consumption and performance. Reduced its
memory usage by 12% and the shutdown time's now instantaneous. However,
besides this arm's about as lean as one can reasonably make it...

17.9 MB total memory usage
3.0 MB (16.8%) is from the idle python interpretor
7.5 MB (41.9%) is from importing the codebase
7.4 MB (41.3%) is consumed at runtime, contribution from individual
panels being negligible

Startup time is 0.142 seconds. 0.103 is the baseline startup, with
graphing contributing an extra 0.02 seconds (probably from reading the
state file for bandwidth prepopulation). On the first startup there's
around an extra second, probably for importing the libraries.

As for cpu usage, there's spikes from connection and resource usage
fetches but otherwise it's flat (very little curses or controller
activity due to caching and being smart with redraws). Individual
panels don't contribute noticeably to the baseline.

[1] https://trac.torproject.org/projects/tor/ticket/2412
[2] https://trac.torproject.org/projects/tor/ticket/2812
[3] https://trac.torproject.org/projects/tor/ticket/2065
[4] https://trac.torproject.org/projects/tor/ticket/1329
[5] https://trac.torproject.org/projects/tor/ticket/2580
[6] https://trac.torproject.org/projects/tor/ticket/3406
[7] https://trac.torproject.org/projects/tor/ticket/3409
[8] http://inspirated.com/2011/06/28/summer-of-code-progress-graphs-logs-and-acid

Bridge relay and bridge authority work.

Nothing to report.

Scalability, load balancing, directory overhead, efficiency.

- Worked on code to work on the more compact geoip format of bug2506.
- Finished up the implementation for "FooPort auto", which allows Tor to pick which port to use for a given listener.
- Wrote some code for feature3116, which notes where TLS connections are when they fail so that we can more easily diagnose censorship. Still needs merge and review.
- tweaked Robert Hogan's bug1666 branch to receive and handle socks authentication. Still needs merge and review.
- Received and reviewed a patch to enable Tor to work over IPv6. Patch needs work, but progress is being made.
- Got a start on proposal 171 (stream isolation). `https://gitweb.torproject.org/torspec.git/blob/master:/proposals/171-separate-streams.txt`.
- Spent a little while working on agl's curve25519-donna.c implementation, and shaved about 10-25% off its run time.
- Fixed a number of bugs in the torflow codebase related to Bandwidth Authorities. This results in less memory utilization and a few fixes for measurement accuracy. Tickets `https://trac.torproject.org/projects/tor/ticket/1976`, `https://trac.torproject.org/projects/tor/ticket/2391`, and `https://trac.torproject.org/projects/tor/ticket/2861`.

Incentives work.

Nothing to report.

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

```
Regarding Thandy:
- spent some time getting to know the code and discussing different
  parts of the thp spec with Nick, Robert, and Sebastian.
- implemented the thp spec, we are about to start testing it with real
  packages. The idea (or at least my idea) is to release this with
  Vidalia-0.3.1, along with the corresponding plugin to control it.
```

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

- Updated translations in Arabic, German, French, Spanish, Farsi, Russian, Italian, and Polish.