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


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

## C 2.0. New releases, new hires, new funding

1. On April 24, we released Tor 0.2.2.13-alpha. This version addresses the recent connection and memory overload problems we've been seeing on relays, especially relays with their DirPort open. If your relay has been crashing, or you turned it off because it used too many resources, give this release a try.

```
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).

o Minor features:
  - Finally get rid of the deprecated and now harmful notion of "clique
    mode", where directory authorities maintain TLS connections to
    every other relay.
  - Directory authorities now do an immediate reachability check as soon
    as they hear about a new relay. This change should slightly reduce
    the time between setting up a relay and getting listed as running
    in the consensus. It should also improve the time between setting
    up a bridge and seeing use by bridge users.
  - Directory authorities no longer launch a TLS connection to every
    relay as they startup. Now that we have 2k+ descriptors cached,
    the resulting network hiccup is becoming a burden. Besides,
    authorities already avoid voting about Running for the first half
    hour of their uptime.
```

2. On April 20, 2010 we released Tor 0.2.2.12-alpha. This release fixes a critical bug in how directory authorities handle and vote on descriptors. It was causing relays to drop out of the consensus.

```
Changes in version 0.2.2.12-alpha - 2010-04-20
  o Major bugfixes:
    - Many relays have been falling out of the consensus lately because
      not enough authorities know about their descriptor for them to get
      a majority of votes. When we deprecated the v2 directory protocol,
      we got rid of the only way that v3 authorities can hear from each
      other about other descriptors. Now authorities examine every v3
      vote for new descriptors, and fetch them from that authority. Bugfix
      on 0.2.1.23.
    - Fix two typos in tor_vasprintf() that broke the compile on Windows,
      and a warning in or.h related to bandwidth_weight_rule_t that
      prevented clean compile on OS X. Fixes bug 1363; bugfix on
      0.2.2.11-alpha.
    - Fix a segfault on relays when DirReqStatistics is enabled
      and 24 hours pass. Bug found by keb. Fixes bug 1365; bugfix on
      0.2.2.11-alpha.

  o Minor bugfixes:
    - Demote a confusing TLS warning that relay operators might get when
      someone tries to talk to their OrPort. It is neither the operator's
      fault nor can they do anything about it. Fixes bug 1364; bugfix
      on 0.2.0.14-alpha.
```

3. On April 15, we released Tor 0.2.2.11-alpha. It fixes yet another instance of broken OpenSSL libraries that was causing some relays to drop out of the consensus.

```
  o Major bugfixes:
    - 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.
    - Fix a parsing error that made every possible value of
      CircPriorityHalflifeMsec get treated as "1 msec". Bugfix
      on 0.2.2.7-alpha. Rename CircPriorityHalflifeMsec to
      CircuitPriorityHalflifeMsec, so authorities can tell newer relays
      about the option without breaking older ones.
    - 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.
```

```
  o Minor features:
    - Experiment with a more aggressive approach to preventing clients
      from making one-hop exit streams. Exit relays who want to try it
      out can set "RefuseUnknownExits 1" in their torrc, and then look
      for "Attempt by %s to open a stream" log messages. Let us know
      how it goes!
    - Add support for statically linking zlib by specifying
      --enable-static-zlib, to go with our support for statically linking
      openssl and libevent. Resolves bug 1358.

  o Minor bugfixes:
    - Fix a segfault that happens whenever a Tor client that is using
      libevent2's bufferevents gets a hup signal. Bugfix on 0.2.2.5-alpha;
      fixes bug 1341.
    - When we cleaned up the contrib/tor-exit-notice.html file, we left
      out the first line. Fixes bug 1295.
    - When building the manpage from a tarball, we required asciidoc, but
      the asciidoc -> roff/html conversion was already done for the
      tarball. Make 'make' complain only when we need asciidoc (either
      because we're compiling directly from git, or because we altered
      the asciidoc manpage in the tarball). Bugfix on 0.2.2.9-alpha.
    - When none of the directory authorities vote on any params, Tor
      segfaulted when trying to make the consensus from the votes. We
      didn't trigger the bug in practice, because authorities do include
      params in their votes. Bugfix on 0.2.2.10-alpha; fixes bug 1322.

  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.
```

4. Tor Browser Bundle for GNU/Linux was updated throughout the month, from versions 1.0.1 to 1.0.4. The details are:

```
1.0.4: Released 2010-04-24
       Update Tor to 0.2.2.13-alpha

1.0.3: Released 2010-04-20
       Update Tor to 0.2.2.12-alpha

1.0.2: Released 2010-04-18
       Update Tor to 0.2.2.10-alpha
```

```
        Update to Vidalia 0.2.8

    1.0.1: Released 2010-04-08
        Stop TBB from crashing when it tries to download files
        Update Torbutton to 1.2.5
```

5. On April 4, we released Tor Browser Bundle for Windows version 1.3.4. The changes were an update to Firefox 3.5.9 to address some security issues, and update the Torbutton Firefox extension to 1.2.5.

6. On April 8, we released the latest Torbutton Firefox Extension version, 1.2.5. This release includes a number of bugfixes and some new features. The details are:

```
* bugfix: bug 1169: Fix blank popup conflict with CoolPreviews
* bugfix: bug 1246: Fix IST and other HH:30 timezone issues.
* bugfix: bug 1219: Fix the toggle warning loop issue on settings change.
* bugfix: bug 1321: Fix a session restore bug when closing the last window
* bugfix: bug 1302: Update useragent to FF3.6.3 on WinNT6.
* bugfix: bug 1157: Add logic to handle torbutton crashed state conflicts
* bugfix: bug 1235: Improve the 'changed-state' refresh warning message
* bugfix: bug 1337: Bind alert windows to correct browser window
* bugfix: bug 1055: Make the error console the default log output location
* bugfix: bug 1032: Fix an exception in the localhost proxy filter
* misc: Always tell a website our window size is rounded even if it's not
* misc: Add some suggestions to warning about loading external content
* new: Add option to always update Torbutton via Tor. On by default
* new: Redirect Google queries elsewhere on captcha (default ixquick)
* new: Strip identifying info off of Google searchbox queries
```

7. On April 11, we released Vidalia 0.2.8. It contains updated translations, updates to the universal plug and play libraries, and better compatibility with newer versions of the Nokia Qt toolkit.

```
o Stop using our custom dock icon implementation on OS X and just use
  QSystemTrayIcon everywhere. Fixes the build on Snow Leopard.
  (Ticket #562)
o Update the bundled CA certificates to re-enable downloading bridges
  from bridges.torproject.org via SSL.
o Include a pre-configured qt.conf file in the Mac OS X bundles that
  disable Qt plugin loading from the default directories. Otherwise,
  users who have Qt installed in a system-wide location would end up
  loading the libraries twice and crashing.
o Include libgcc_s_dw2-1.dll in the Windows installers, since Qt 4.6 now
  depends on that DLL. Including the .dll is currently hardcoded, so the
  Windows installer must be built using Qt 4.6. (Ticket #555)
o Update the included version of miniupnpc to 1.4.20100407.
o Add Burmese and Thai UI translations.
```

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

Karsten did major backend processing work on the metrics.torproject.org data and website. These improvements allow for an automated process to update the various graphs and analyze the data sets. The whole system is better documented to assist someone in replicating the environment from scratch.

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

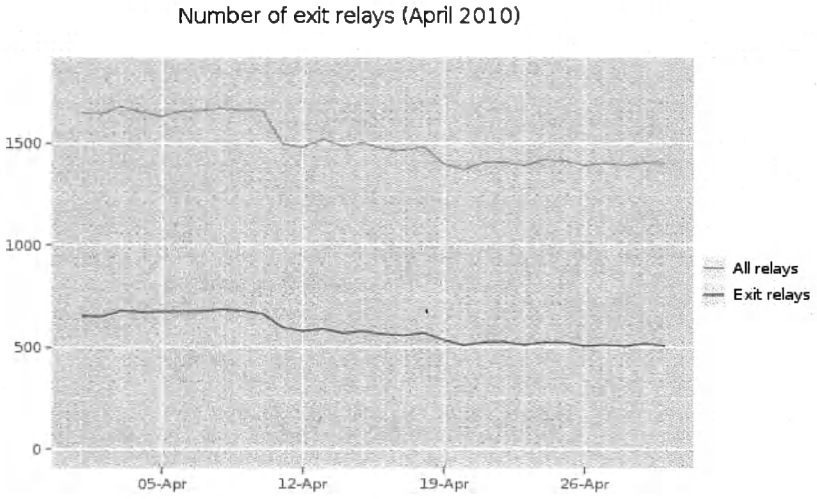
Nothing to report.

## C.2.5. Hide Tor's network signature.

Nothing to report.

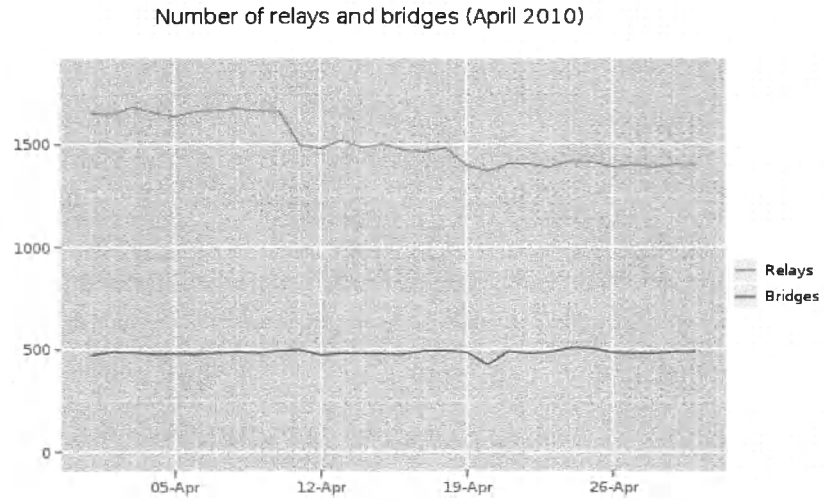
## C.2.10 Grow the Tor network and user base. Outreach.

### Measures of the Tor Network

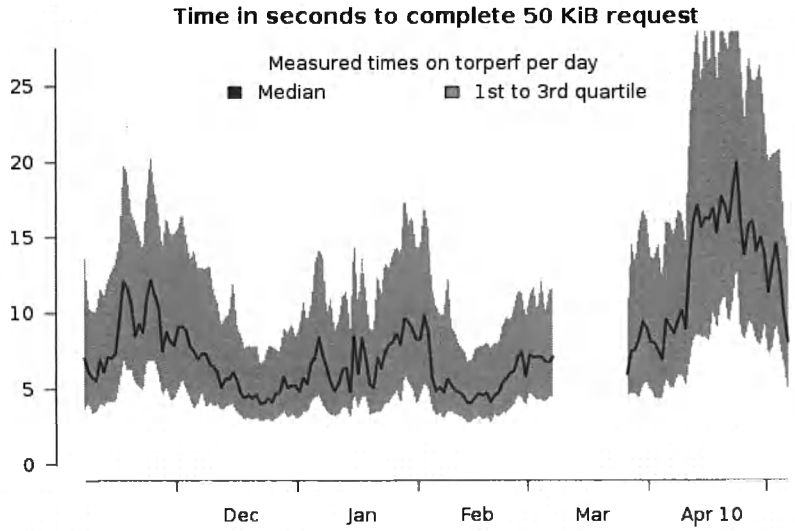



This graph shows the total quantity of relays and quantity of exit relays in April 2010. Exit relay capacity is one of the potential bottlenecks that affects the overall performance of Tor. The more exit relays we have, the faster it seems to browse the open Internet. As shown, the

quantity of relays dropped dramatically over the month.




This graph shows the total quantity of relays and the total quantity of bridges in April 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 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.

### Outreach and Advocacy

- Jacob talked at SOURCE Boston about Tor, censorship circumvention, and running relays. http://www.sourceconference.com/. Jacob's presentation can be found at https://svn.torproject.org/svn/projects/presentations/SOURCE-Boston-2010.pdf.
- Andrew lectured about anonymous communications and Tor at the Portland campus of the University of Southern Maine.
- Roger lectured about anonymous communications and Tor at the Albuquerque campus of the University of New Mexico.
- Andrew was interviewed by Radio Free Asia: Vietnam about using Tor for online privacy and anonymity. http://www.rfa.org/vietnamese/in_depth/TOR-free-anti-censorship-tool-KhA20-04262010195030.html

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

Released new versions of Tor Browser Bundle for GNU/Linux and Windows. See C.2.0 for details.

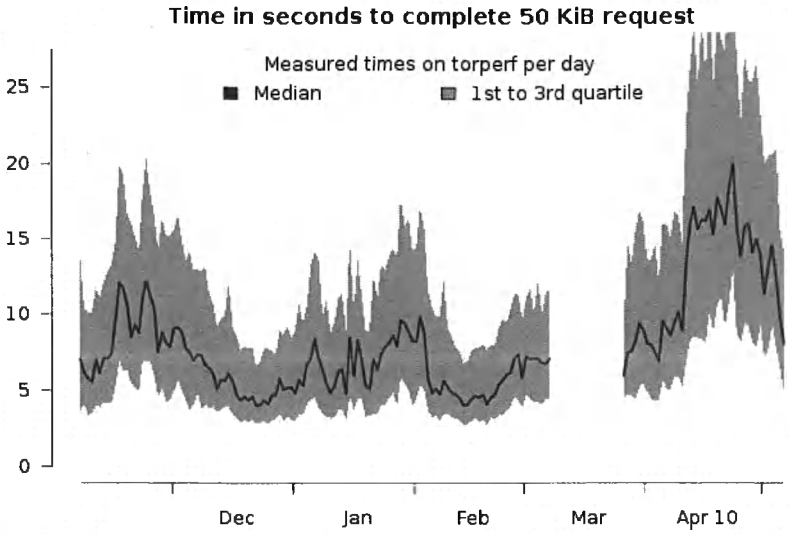
## C.2.12 Bridge relay and bridge authority work.

Nothing to report.

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

From the 0.2.2.12-alpha release notes:
Directory authorities now do an immediate reachability check as soon as they hear about a new relay. This change should slightly reduce the time between setting up a relay and getting listed as running in the consensus. It should also improve the time between setting up a bridge and seeing use by bridge users.

In March, we changed a setting on a majority of the Directory Authorities called CircPriority-HalflifeMsec. Based upon research at the University of Waterloo, changing this setting could improve the overall performance of the network by fine tuning the earned weighted mean average bit bucket for better performance. Due to a bug in the CircPriorityHalflifeMsec parsing, the average latency in the network increased dramatically. At the same time, China unblocked the list of public and bridge relays, flooding hundreds of thousands of clients back into the network. The results of the bug and Chinese clients returning to the network can be




seen in this graph:

## C.2.14. Incentives work.

Nothing to report.

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

The GNU/Linux tor browser bundle with localizations was added to the get-tor email auto-responder.

## C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

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

- Updated text strings for the get-tor email auto-responder to make it easier for translators to complete the work.
- Added new translations of Vietnamese, Greek and Serbian to all projects.
- Many updated translated strings in German, Polish, Greek, Dutch, Finnish, Russian, Japanese, Chinese, French, Burmese, Spanish, Farsi, Arabic, Swedish, Turkish, and Norwegian.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: September 13, 2010


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

## C 2.0. New releases, new hires, new funding

### New Releases

1. On August 21st we released Tor Browser Bundle 1.0.10 for GNU/Linux. It includes a number of updates, the largest one being a switch to Firefox 3.6.8. The rest of the updates are:

   - Update Tor to 0.2.2.15-alpha
   - Update Firefox to 3.6.8 (Mozilla is not doing security and stability updates for 3.5.x after August 2010)
   - Update NoScript to 2.0.2.3
   - Update BetterPrivacy to 1.48.3
   - Update HTTPS Everywhere to 0.2.2

2. On August 18, we released Tor 0.2.2.15-alpha. It fixes a big bug in hidden service availability, fixes a variety of other bugs that were preventing performance experiments from moving forward, fixes several bothersome memory leaks, and generally closes a lot of smaller bugs that have been filling up trac lately.

```
Changes in version 0.2.2.15-alpha - 2010-08-18
  o Major bugfixes:
    - Stop assigning the HSDir flag to relays that disable their
      DirPort (and thus will refuse to answer directory requests). This
      fix should dramatically improve the reachability of hidden services:
      hidden services and hidden service clients pick six HSDir relays
      to store and retrieve the hidden service descriptor, and currently
      about half of the HSDir relays will refuse to work. Bugfix on
      0.2.0.10-alpha; fixes part of bug 1693.
    - The PerConnBWRate and Burst config options, along with the
      bwconnrate and bwconnburst consensus params, initialized each conn's
      token bucket values only when the connection is established. Now we
      update them if the config options change, and update them every time
      we get a new consensus. Otherwise we can encounter an ugly edge
      case where we initialize an OR conn to client-level bandwidth,
```

```
    but then later the relay joins the consensus and we leave it
    throttled. Bugfix on 0.2.2.7-alpha; fixes bug 1830.
  - Fix a regression that caused Tor to rebind its ports if it receives
    SIGHUP while hibernating. Bugfix in 0.1.1.6-alpha; closes bug 919.

o Major features:
  - Lower the maximum weighted-fractional-uptime cutoff to 98%. This
    should give us approximately 40-50% more Guard-flagged nodes,
    improving the anonymity the Tor network can provide and also
    decreasing the dropoff in throughput that relays experience when
    they first get the Guard flag.
  - Allow enabling or disabling the *Statistics config options while
    Tor is running.

o Minor features:
  - Update to the August 1 2010 Maxmind GeoLite Country database.
  - Have the controller interface give a more useful message than
    "Internal Error" in response to failed GETINFO requests.
  - Warn when the same option is provided more than once in a torrc
    file, on the command line, or in a single SETCONF statement, and
    the option is one that only accepts a single line. Closes bug 1384.
  - Build correctly on mingw with more recent versions of OpenSSL 0.9.8.
    Patch from mingw-san.
  - Add support for the country code "{??}" in torrc options like
    ExcludeNodes, to indicate all routers of unknown country. Closes
    bug 1094.
  - Relays report the number of bytes spent on answering directory
    requests in extra-info descriptors similar to {read,write}-history.
    Implements enhancement 1790.

o Minor bugfixes (on 0.2.1.x and earlier):
  - Complain if PublishServerDescriptor is given multiple arguments that
    include 0 or 1. This configuration will be rejected in the future.
    Bugfix on 0.2.0.1-alpha; closes bug 1107.
  - Disallow BridgeRelay 1 and ORPort 0 at once in the configuration.
    Bugfix on 0.2.0.13-alpha; closes bug 928.
  - Change "Application request when we're believed to be offline."
    notice to "Application request when we haven't used client
    functionality lately.", to clarify that it's not an error. Bugfix
    on 0.0.9.3; fixes bug 1222.
  - Fix a bug in the controller interface where "GETINFO ns/asdaskljkl"
    would return "551 Internal error" rather than "552 Unrecognized key
    ns/asdaskljkl". Bugfix on 0.1.2.3-alpha.
  - Users can't configure a regular relay to be their bridge. It didn't
    work because when Tor fetched the bridge descriptor, it found
    that it already had it, and didn't realize that the purpose of the
    descriptor had changed. Now we replace routers with a purpose other
    than bridge with bridge descriptors when fetching them. Bugfix on
    0.1.1.9-alpha. Bug 1776 not yet fixed because now we immediately
    refetch the descriptor with router purpose 'general', disabling
    it as a bridge.
```

```
  - Fix a rare bug in rend_fn unit tests: we would fail a test when
    a randomly generated port is 0. Diagnosed by Matt Edman. Bugfix
    on 0.2.0.10-alpha; fixes bug 1808.
  - 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. Also update the spec to reflect this new reason. Bugfix on
    0.1.0.1-rc; fixes part of bug 1793.
  - Delay geoip stats collection by bridges for 6 hours, not 2 hours,
    when we switch from being a public relay to a bridge. Otherwise
    there will still be clients that see the relay in their consensus,
    and the stats will end up wrong. Bugfix on 0.2.1.15-rc; fixes bug
    932 even more.
  - Instead of giving an assertion failure on an internal mismatch
    on estimated freelist size, just log a BUG warning and try later.
    Mitigates but does not fix bug 1125.
  - Fix an assertion failure that could occur in 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.

o Minor bugfixes (on 0.2.2.x):
  - Alter directory authorities to always consider Exit-flagged nodes
    as potential Guard nodes in their votes. The actual decision to
    use Exits as Guards is done in the consensus bandwidth weights.
    Fixes bug 1294; bugfix on 0.2.2.10-alpha.
  - When the controller is reporting the purpose of circuits that
    didn't finish building before the circuit build timeout, it was
    printing UNKNOWN_13. Now print EXPIRED. Bugfix on 0.2.2.14-alpha.
  - Our libevent version parsing code couldn't handle versions like
    1.4.14b-stable and incorrectly warned the user about using an
    old and broken version of libevent. Treat 1.4.14b-stable like
    1.4.14-stable when parsing the version. Fixes bug 1731; bugfix
    on 0.2.2.1-alpha.
  - Don't use substitution references like $(VAR:MOD) when
    $(asciidoc_files) is empty -- make(1) on NetBSD transforms
    '$(:x)' to 'x' rather than the empty string. This bites us in
    doc/ when configured with --disable-asciidoc. Bugfix on
    0.2.2.9-alpha; fixes bug 1773.
  - Remove a spurious hidden service server-side log notice about
    "Ancient non-dirty circuits". Bugfix on 0.2.2.14-alpha; fixes
    bug 1741.
  - Fix compilation with --with-dmalloc set. Bugfix on 0.2.2.6-alpha;
    fixes bug 1832.
  - Correctly report written bytes on linked connections. Found while
    implementing 1790. Bugfix on 0.2.2.4-alpha.
  - Fix three memory leaks: one in circuit_build_times_parse_state(),
    one in dirvote_add_signatures_to_pending_consensus(), and one every
    time we parse a v3 network consensus. Bugfixes on 0.2.2.14-alpha,
    0.2.2.6-alpha, and 0.2.2.10-alpha respectively; fixes bug 1831.
```

```
  o Code simplifications and refactoring:
    - Take a first step towards making or.h smaller by splitting out
      function definitions for all source files in src/or/. Leave
      structures and defines in or.h for now.
    - Remove a bunch of unused function declarations as well as a block of
      #if 0'd code from the unit tests. Closes bug 1824.
    - New unit tests for exit-port history statistics; refactored exit
      statistics code to be more easily tested.
    - Remove the old debian/ directory from the main Tor distribution.
      The official Tor-for-debian git repository lives at the URL
      \url{https://git.torproject.org/debian/tor.git}
```

3. Released two new versions of Orbot, Tor for Android.

```
Version 1.0.2
- added "check" yes/no dialog prompt
- debugged iptables/transprox settings on Android 1.6 and 2.2
- added proxy settings help screen and fixed processSettings() NPE

Version 1.0.1
- found and fixed major bug in per-app trans proxying; list of apps was being cached and iptables
```

4. On August 6, we released Libevent 2.0.6-rc, the first release candidate of the new Libevent 2.0 series. The main new feature that we want from Libevent 2.0 is its support for buffer-based (rather than socket-based) network abstractions, which will let us support Windows the way it wants to be supported. The new Libevent includes a wide variety of other features that will make our lives easier too, ranging from making it easier to support multi-threaded crypto operations to making it easier to modularly change Tor's transport from TLS-over-TCP to other options.

```
DOCUMENTATION
 o Document a change in the semantics of event_get_struct_event_size()
   (e21f5d1)
 o Add a comment to describe our plan for library versioning (9659ece)
 o Fix sentence fragment in docs for event_get_struct_event_size() (7b259b6)

NEW FEATURES AND INTERFACE CHANGES
 o Remove the obsolete evthread interfaces (c5bab56)
 o Let evhttp_send_error infer the right error reasons (3990669)
 o Add a function to retrieve the other side of a bufferevent pair (17a8e2d)
 o Add bufferevent_lock()/bufferevent_unlock() (215e629)
 o Stop asserting when asked for a (unsupported) TCP dns port. Just
   return NULL. (7e87a59)
 o Replace (unused,always 0) is_tcp argument to evdns_add_server_port*()
   with flags (e1c1167)
 o Constify a couple of arguments to evdns_server_request_add_*_reply
   (cc2379d)
 o Add an interface to expose min_share in ratelimiting groups (6ae53d6)
```

BUGFIXES

- Avoid event_del on uninitialized event in event_base_free (6d19510)
- Add some missing includes to fix Linux build again (75701e8)
- Avoid close of uninitialized socket in evbuffer unit test (bda21e7)
- Correctly recognize .255 addresses as link-local when looking for interfaces (8c3452b)
- If no evdns request can be launched, return NULL, not a handle (b14f151)
- Use generic win32 interfaces, not ASCII-only ones, where possible. (899b0a3)
- Fix the default HTTP error template (06bd056 Felix Nawothnig)
- Close the file in evutil_read_file whether there's an error or not. (0798dd1 Pierre Phaneuf)
- Fix possible nullptr dereference in evhttp_send_reply_end() (29b2e23 Felix Nawothnig)
- never let bufferevent_rlim functions return negative (0859870)
- Make sample/hello_world work on windows (d89fdba)
- Fix a deadlock related to event-base notification. Diagnosed by Zhou Li, Avi Bab, and Scott Lamb. (17522d2)
- Possible fix to 100% cpu usage with epoll and openssl (cf249e7 Mike Smellie)
- Don't race when calling event_active/event_add on a running signal event (fc5e0a2)
- Suppress a spurious EPERM warning in epoll.c (e73cbde)
- Fix wrong size calculation of iovec buffers when exact=1 (65abdc2 niks)
- Change bufferevent_openssl::do_write so it doesn't call SSL_write with a 0 length buffer (c991317 Mike Smellie)
- Fixed compilation of sample/le-proxy.c on win32 (13b912e Trond Norbye)
- Fix rate-limit calculation on openssl bufferevents. (009f300)
- Remember to initialize timeout events for bufferevent_async (de1f5d6 Christopher Davis)

BUILD AND DISTRIBUTION CHANGES

- Test the unlocked-deferred callback case of bufferevents (dfb75ab)
- Remove the now-unusable EVTHREAD_LOCK/UNLOCK constants (fdfc3fc)
- Use -Wlogical-op on gcc 4.5 or higher (d14bb92)
- Add the libtool-generated /m4/* stuff to .gitignore (c21c663)
- Remove some automake-generated files from version control. (9b14911)
- Have autogen.sh pass --force-missing to automake (8a44062)
- Set library version for libevent_pthreads correctly (b2d7440)
- Really only add libevent_core.la to LIBADD on mingw (1425003 Sebastian Hahn)
- Build more cleanly with NetBSDs that dislike toupper(char) (42a8c71)
- Fix unit tests with -DUSE_DEBUG enabled (28f31a4)
- Fix evdns build with -DUNICODE (5fa30d2)
- Move event-config.h to include/event2 (ec347b9)

TESTING

- Add options to test-ratelim.c to check its results (2b44dcc)
- Make test-ratelim clean up after itself better. (b5bfc44)
- Remove the now-obsolete setup_test() and cleanup_test() functions (e73f1d7)
- Remove all non-error prints from test/regress.c (8bc1e3d)
- Make test.sh exit with nonzero status if tests fail (faf2a04)
- Have the unit tests report errors from test.sh (3689bd2)

```
  o Fix logic in correcting high values from FIONREAD (3467f2f)
  o Add test for behavior on remote socket close (44d57ee)
  o Unit test for event_get_struct_event_size() (7510aac)
  o Make test/test.sh call test-changelist (7c92691)
  o Fix badly-behaved subtest of dns/bufferevent_connect_hostname (840a72f
    Joachim Bauch)
  o Add option to test-ratelim to test min_share (42f6b62)
  o Fix an assertion bug in test-ratelim (b2c6202)
  o Make tests quieter on local dns resolver failure (e996b3d)
  o Increase the tolerance in our unit tests for sloppy clocks. (170ffd2)
  o Use AF_INET socketpair to test sendfile on Solaris (9b60209)
  o Make test-changelist count cpu usage right on win32 (ea1ea3d)

INTERNALS, PERFORMANCE, AND CODE CLEANUPS
  o Mark the event_err() functions as __attribute__((noreturn)) (33bbbed)
  o Do not check that event_base is set in EVBASE_ACQUIRE_LOCK (218a3c3)
  o Replace (safe) use of strcpy with memcpy to appease OpenBSD (caca2f4)
  o Remove some dead assignments (47c5dfb)
  o Fix a pedantic gcc 4.4 warning in event2/event.h (276e7ee)
  o Drain th_notify_fd[0] more bytes at a time. (a5bc15b)
  o Tidy up the code in evthread_make_base_notifiable a little (61e1eee)
  o Pass flags to fcntl(F_SETFL) and fcntl(F_SETFD) as int, not long (7c2dea1)
  o Remove unused variables in test/test-changelist.c (b00d4c0)
  o Fix whitespace. (cb927a5)
  o Improve error message for failed epoll to make debugging easier. (9e725f7)
  o Turn our socketpair() replacement into its own function (57b30cd)
```

### Funding

We finished the first year of our NSF grant, and wrote up the annual (interim) report on what metrics work we've done and what research projects we've helped with. We were then awarded the second year of the two-year grant.

Expect a blog post soon where we follow through with our transparency promises.

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

Continuing research into China's Great Firewall shows bridges are surviving for 1-2 weeks before being blocked. We're working to improve the bridge database such that it only gives out bridges that work in a requested country. Right now, we hand out a random selection of 3 bridges regardless of potential country of usage. In China, bridges and relays are still blocked by IP address and TCP port combinations.

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

We've brainstormed future tasks that need to be done for Tor, broken down into two sets by upcoming priority: `https://trac.torproject.org/projects/tor/wiki/sponsors/SponsorD/`

March2011 and https://trac.torproject.org/projects/tor/wiki/sponsors/SponsorD/June2011
We wrote up project sketches of how to tackle some of these tasks, such as:

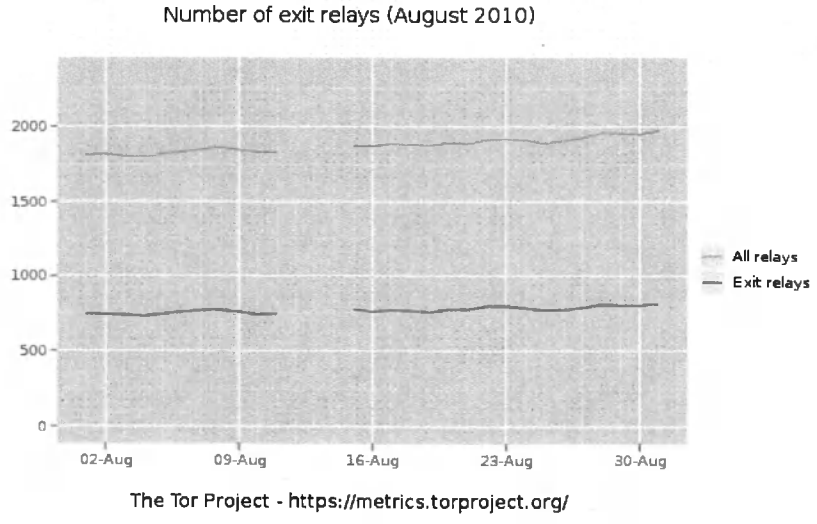
- Bridge relay images for the cloud. https://trac.torproject.org/projects/tor/ticket/1853
- Bundling the http request and headers with the initial begin cell, to save a round-trip and improve client preformance. https://trac.torproject.org/projects/tor/ticket/1849
- A performance experiment to raise the minimum bandwidth for being a relay, thus reducing the overall capacity of the network but improving the average performance of each relay. https://trac.torproject.org/projects/tor/ticket/1854
- A preliminary design for UDP transport between Tor relays. https://trac.torproject.org/projects/tor/ticket/1855
- Tor clients should remember bridge relay information and statistics across restarts. https://trac.torproject.org/projects/tor/ticket/1852
- We should have bridge relays automatically monitor whether they can reach websites like Baidu, to give us early warnings when the bridges become blocked. https://trac.torproject.org/projects/tor/ticket/1851

## C.2.5. Hide Tor's network signature.

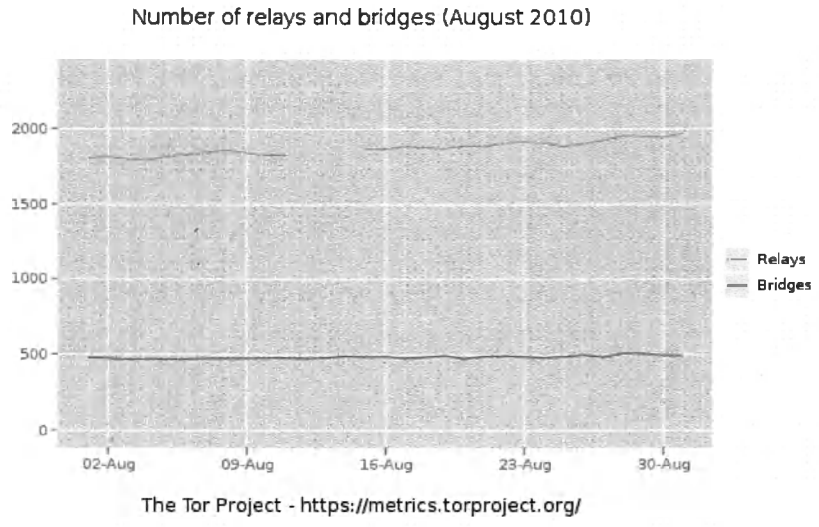
Nothing to report.

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

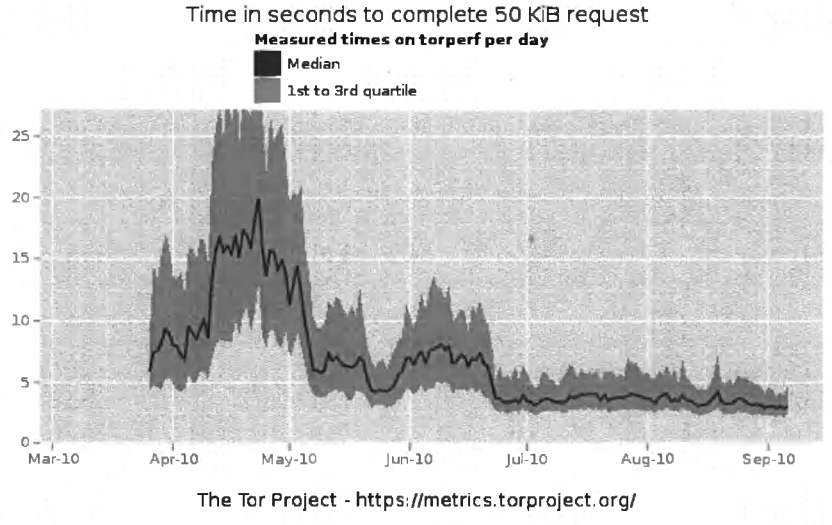
### Measures of the Tor Network



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




This graph shows the total quantity of relays and the total quantity of bridges in August 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

- Roger met with David Tian of Freegate. While interactions at the policy level between Tor and the various GIFC organizations didn't work out very well, interactions between the technical developers have gone much more smoothly. Following on an informal gathering of circumvention tool developers earlier this summer, Roger met with Alan Huang of Ultrasurf in July, and then David Tian of Freegate in August. The goal is to establish common ground of what problems need to be solved, what behavior we're seeing from the censors, and where there are shared solutions that we can collaborate on. One piece of advice we suggested was that they should look for ways to get subsidized or donated bandwidth, so they can focus their new funding to more permanent results like better software.

- Roger met with the University of California - San Diego research group to help them better understand the research challenges in Tor. The full trip report is available at `https://blog.torproject.org/blog/trip-report-ucsd`. Roger's presentation can be found at `https://svn.torproject.org/svn/projects/presentations/slides-ucsd10.pdf`.

- Roger met with a researcher from The Cooperative Association for Internet Data Analysis (CAIDA) to discuss Tor, metrics, and analyzing our growing collection of data about the Tor network.

- Roger met with Tom Heydt-Benjamin, an anonymity researcher in the NYC area, about helping us with metrics work, grant proposals, and getting a better handle on the bridge address distribution arms race.

- Roger attended the "Workshop on Cyber Security Data for Experimentation" organized by the National Science Foundation (NSF). The premise of the workshop was that many academics need real-world data sets to solve problems, whereas industry is the place with the real-world data sets and they don't have any real reason to share. By getting the academics and the industry people talking, with government funders nearby, they hoped to better understand the problems and maybe move things forward. Roger was there (and on the first panel) because of Tor's work on gathering Tor network snapshots, performance data, and user statistics. Tor's approach represents one way out of the trap where researchers never quite get the data they want, or if they do it isn't open enough (which hinders whether anybody else can reproduce their results). The full trip report is available at `https://blog.torproject.org/blog/trip-report-nsf-data-workshop`.

- Roger did a talk to a half dozen NSF program managers, to bring them up to speed on what Tor is up to and what sort of measurement and research projects we're working on and should work on next. The presentation can be found at `https://svn.torproject.org/svn/projects/presentations/slides-nsf10.pdf`.

- Erinn discussed Tor and free software at DebConf 2010 in New York City. `http://debconf10.debconf.org/`.

- Andrew and Paul presented at The International Conference on Cyber Security. `http://www.iccs.fordham.edu/`. Andrew's presentation can be found at `https://svn.torproject.org/svn/projects/presentations/2010-iccs-tor-overview.pdf`. Paul presented the

current attacks on Tor's design from a research perspective, as well as giving a briefing on current topics of research into trusted routing within Tor.

- Ian, Roger, and others attended Usenix Security 2010, `http://www.usenix.org/events/sec10/index.html`.

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

- Torbrowser Bundle for GNU/Linux version 1.0.10 released. See section C.2.0 above for the details.
- Torbrowser Bundle for OSX works on OS X 10.4 and 10.5. 10.6 users continue to experience issues with the launching of the Firefox browser. Erinn and Steven are continuing to debug the 10.6 issues.

## C.2.12 Bridge relay and bridge authority work.

We're developing designs to better handle bridge distribution. Part of this is to enable Tor clients to become bridges and then relays by default. The other part of this is for Tor clients to always have a set of working bridges, requesting new bridges in advance, or be able to track bridge address changes and update accordingly.

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

- Accepted Proposal 174 for "Optimistic Data for Tor: Server Side" from Ian Goldberg. This change will save one OP-Exit round trip (down to one from two). There are still two SOCKS Client-OP round trips (negligible time) and two Exit-Server round trips. Depending on the ratio of the Exit-Server (Internet) RTT to the OP-Exit (Tor) RTT, this will decrease the latency by 25 to 50 percent. Experiments validate these predictions. [Goldberg, PETS 2010 rump session; see https://thunk.cs.uwaterloo.ca/optimistic-data-pets2010-rump.pdf ] The full proposal can be read at `https://gitweb.torproject.org/tor.git/blob_plain/HEAD:/doc/spec/proposals/174-optimistic-data-server.txt`.
- Mike Perry fixed a number of bugs in the bandwidth authority and exit scanner codebases. The exit scanner codebase is updated with the work of a Google Summer of Code student
- A Google Summer of Code student, Harry Bock, worked on improving the Tor DNSEL codebase. TorDNSEL is a DNSBL-style interface for querying information about Tor exit nodes, to be more thorough, more usable, and more maintainable. Out of this effort came TorBEL, a set of specifications and Python tools that try to address this problem. The full writeup on the new software can be found on our blog at `https://blog.torproject.org/blog/torbel-tor-bulk-exit-list-tools`.

## C.2.14. Incentives work.

Roger helped to shepherd a paper by Rob Jansen, Nicholas Hopper, and Yongdae Kim that will be presented in October at ACM CCS 2010. The paper is called "Recruiting New Tor Relays with BRAIDS". It is the next step after the "Building Incentives into Tor" paper from January 2010, and aims to resolve some of the vulnerabilities in that design. Expect a blog post in the next few months explaining what it solves and what it leaves unsolved. `http://www-users.cs.umn.edu/~hopper/braids_ccs.pdf`

## 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.

- Runa implemented a change to the publishing of translated website pages. We now only publish a non-English page to the website if the text is 80% translated or more. This has cleared out hundreds of older, untranslated pages from the website that were misinforming and confusing readers.
- Updated translations for all documents in Arabic, Persian, German, French, Polish, Romanian, Russian, Norwegian, Mandarin Chinese, and Turkish.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: January 10, 2011


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

## C 2.0. New releases, new hires, new funding

### New Releases

1. On December 14, we released updated Tor Browser Bundes for Windows, OSX, and Linux:

```
Linux Bundles 1.1.0: Released 2010-12-13
Important: Polipo has been removed from the Linux Tor Browser Bundle. Please read the full
changelog and report bugs if you have any problems.
Update Firefox to 3.6.13
Update NoScript to 2.0.7
Update HTTPS Everywhere to 0.9.9.development.1
This version of HTTPS-Everywhere is patched to include a fix for bug #2096 which
prevented globally installed versions of the extension from working. It also
includes better protection from Firesheep. See the changelog here:
https://www.eff.org/files/Changelog.txt
Add Chris Davis's patch
This patch improves Firefox's SOCKS support and eliminates the need for Polipo, so
Torbutton has been reconfigured to just use a SOCKS proxy. Polipo has been removed
entirely from this release of the Tor Browser Bundle. If this causes you problems,
please file a bug: https://trac.torproject.org/projects/tor
Rebuild all binaries against glibc 2.7 so they work for older distros again

OS X bundle 1.0.7: Released 2010-12-14
Update Firefox to 3.6.13
Update NoScript to 2.0.7
Update HTTPS-Everywhere to 0.9.9.development.1
This version of HTTPS-Everywhere is patched to include a fix for bug #2096 which
prevented globally installed versions of the extension from working. It also
includes better protection from Firesheep. See the changelog here:
https://www.eff.org/files/Changelog.txt

Windows bundles 1.3.14: Released 2010-12-13
Update Firefox to 3.6.13
Update HTTPS-Everywhere to 0.9.9.development.1
This version of HTTPS-Everywhere is patched to include a fix for bug #2096 which
```

```
prevented globally installed versions of the extensions from working. It also
includes better protection from Firesheep. See the changelog here:
https://www.eff.org/files/Changelog.txt
```

2. On December 17th, we released an updated -stable version of Tor, 0.2.1.28. Tor 0.2.1.28 does some code cleanup to reduce the risk of remotely exploitable bugs. Thanks to Willem Pinckaers for notifying us of the issue. The Common Vulnerabilities and Exposures project has assigned CVE-2010-1676 to this issue. We also took this opportunity to change the IP address for one of our directory authorities, and to update the geoip database we ship.

```
o Major bugfixes:
    - Fix a remotely exploitable bug that could be used to crash instances
      of Tor remotely by overflowing on the heap. Remote-code execution
      hasn't been confirmed, but can't be ruled out. Everyone should
      upgrade. Bugfix on the 0.1.1 series and later.

  o Directory authority changes:
    - Change IP address and ports for gabelmoo (v3 directory authority).

  o Minor features:
    - Update to the December 1 2010 Maxmind GeoLite Country database.
```

3. On December 17th, we released an updated -alpha version of Tor, 0.2.2.20-alpha. Tor 0.2.2.20-alpha does some code cleanup to reduce the risk of remotely exploitable bugs. We also fix a variety of other significant bugs, change the IP address for one of our directory authorities, and update the minimum version that Tor relays must run to join the network.

```
  o Major bugfixes:
    - Fix a remotely exploitable bug that could be used to crash instances
      of Tor remotely by overflowing on the heap. Remote-code execution
      hasn't been confirmed, but can't be ruled out. Everyone should
      upgrade. Bugfix on the 0.1.1 series and later.
    - Fix a bug that could break accounting on 64-bit systems with large
      time_t values, making them hibernate for impossibly long intervals.
      Fixes bug 2146. Bugfix on 0.0.9pre6; fix by boboper.
    - Fix a logic error in directory_fetches_from_authorities() that
      would cause all _non_-exits refusing single-hop-like circuits
      to fetch from authorities, when we wanted to have _exits_ fetch
      from authorities. Fixes more of 2097. Bugfix on 0.2.2.16-alpha;
      fix by boboper.
    - Fix a stream fairness bug that would cause newer streams on a given
      circuit to get preference when reading bytes from the origin or
      destination. Fixes bug 2210. Fix by Mashael AlSabah. This bug was
      introduced before the first Tor release, in svn revision r152.

  o Directory authority changes:
    - Change IP address and ports for gabelmoo (v3 directory authority).

  o Minor bugfixes:
```

```
    - Avoid crashes when AccountingMax is set on clients. Fixes bug 2235.
      Bugfix on 0.2.2.18-alpha. Diagnosed by boboper.
    - Fix an off-by-one error in calculating some controller command
      argument lengths. Fortunately, this mistake is harmless since
      the controller code does redundant NUL termination too. Found by
      boboper. Bugfix on 0.1.1.1-alpha.
    - Do not dereference NULL if a bridge fails to build its
      extra-info descriptor. Found by an anonymous commenter on
      Trac. Bugfix on 0.2.2.19-alpha.

  o Minor features:
    - Update to the December 1 2010 Maxmind GeoLite Country database.
    - Directory authorities now reject relays running any versions of
      Tor between 0.2.1.3-alpha and 0.2.1.18 inclusive; they have
      known bugs that keep RELAY_EARLY cells from working on rendezvous
      circuits. Followup to fix for bug 2081.
    - Directory authorities now reject relays running any version of Tor
      older than 0.2.0.26-rc. That version is the earliest that fetches
      current directory information correctly. Fixes bug 2156.
    - Report only the top 10 ports in exit-port stats in order not to
      exceed the maximum extra-info descriptor length of 50 KB. Implements
      task 2196.
```

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

- Mike spent the past month and a half primarily working on preparing Torbutton for Firefox 4. This was a rather difficult task, as a lot has changed in this release, and the Javascript debugger doesn't yet support Firefox 4. The new mechanism works just fine for replacing XPCOM components. He also took the opportunity to clean up the code a bit. Firefox 3.5 and Firefox 4 both added some new APIs that make our job easier. We no longer rely so heavily on reimplementing pieces of Firefox using XPCOM re-registration. In fact, the only component we still need to hook is the external app launcher, to provide our warning message.

- Mike reviewed a proposed Chrome API at: `https://groups.google.com/a/chromium.org/group/chromium-dev/browse_thread/thread/4c318fb01062678a/89a11a7cbaa48d5f`. The main goal there was to try to steer them away from declarative models and more towards blocking callback APIs that will work better for us. We'll see if it works.

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

- Steven worked on plans of how to make Tor look more like other protocols, for when Tor's HTTPS-like cloaking is broken or someone blocks Tor along with HTTPS. The proposal is to allow Tor bridges to be configured to use one or more plugins which offer translation between Tor and obfuscated-Tor. There is now a proposal draft here: `https://gitweb.torproject.org/tor.git/blob/HEAD:/doc/spec/proposals/ideas/xxx-pluggable-transport.txt`. Steven

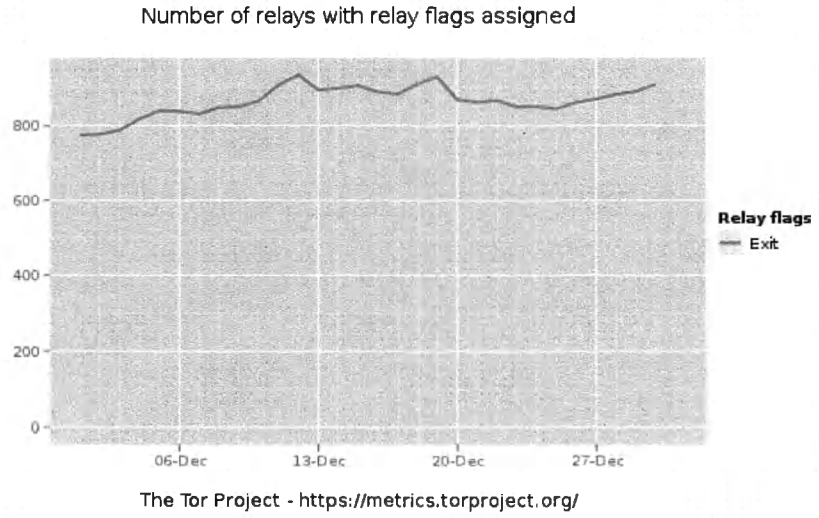
wrote a first proof-of-concept (albeit not compliant with the proposal), for a HTTP-like protocol, and put the code here: `https://gitweb.torproject.org/sjm217/pluggable-transport.git`. A screenshot of the a Wireshark dump of Steven successfully accessing check.torproject.org is at: `http://www.cl.cam.ac.uk/~sjm217/volatile/pluggable-transport.png`.

## C.2.5. Hide Tor's network signature.

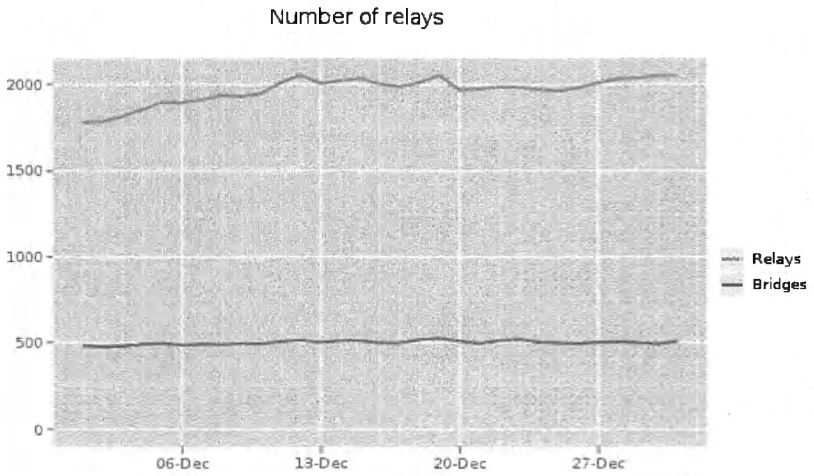
Nothing to report.

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

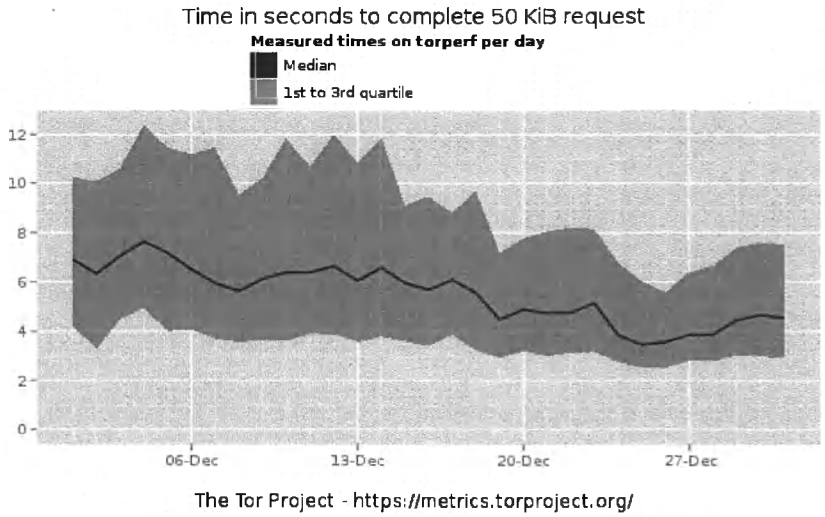
### Measures of the Tor Network




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




This graph shows the total quantity of relays and the total quantity of bridges in December 2010. The quantity of relays is increasing due to the OpenSSL fixes from last 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 as the network recovered from the OpenSSL bugs.

### Outreach and Advocacy

1. Karen spoke at the Reykjavík Digital Freedom Conference, http://www.fsfi.is/radstefna2010/.
2. Erinn spoke at Moscow State University, http://www.linux.org.ru/news/security/5624240
3. Many tor people attended the CCC's 27C3, http://events.ccc.de/congress/2010/wiki/Main_Page
4. Karen participated in "Hivos Digital Natives With a Cause?" Thinkathon, http://www.hivos.net/Hivos-Knowledge-Programme/Themes/Digital-Natives-with-a-Cause/Publications/Digital-Natives-with-a-Cause-Thinkathon-Position-Papers.

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

- See 2.0 for the updated Tor Browser Bundles for OSX, Windows, and Linux.

## C.2.12 Bridge relay and bridge authority work.

- Jacob and Runa continue work on making it easy for people to become Tor bridge relays by default. The Torouter project is very much an alpha code quality project, but making progress on OpenWRT-based wireless access points and the Excito B3 hardware. The project page is kept up-to-date at https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/Torouter.

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

- Karsten wrote a technical report with an "Overview of Statistical Data in the Tor Network". The idea is to give this report to interested researchers who want to know what statistical data we have. The report is available at https://metrics.torproject.org/papers/data-2010-12-29.pdf.
- Erinn and Sebastian worked on some Thandy Hudson hacking accomplishing: 1) Hudson and Windows finally cooperate, so now we can have a Windows autobuilder; and 2) setup a basic instance of Thandy-the secure software update platform.
- Mike did a quick modification to the TorFlow statsplitter.py script to have it output the results from the extra-info descriptors to give us breakdowns on port stats in more readable percentages, to compare the default exit policy of blutmagie to Amunet. It looks like the default exit policy causes you to write a heck of a lot more data, and over half of the read data is misc ports. Using these stats to produce new consensus weights to account for this seems like a good task to do.

## 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 fully migrated from our own Pootle-based translation system to Transifex, `https://www.transifex.net/projects/p/torproject/`. A number of translations for various products have already come through for German, Arabic, Burmese, Simplified Chinese, Dutch, Finnish, French, Indonesian, Italian, Norwegian, Persian, Polish, and Romanian.

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


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

## C 2.0. New releases, new hires, new funding

1. On February 13, we released a new stable version of Tor, 0.2.1.23. Tor 0.2.1.23 fixes a huge client-side performance bug, makes Tor work again on the latest OS X, and updates the location of a directory authority.

```
o Major bugfixes (performance):
  - We were selecting our guards uniformly at random, and then weighting
    which of our guards we'd use uniformly at random. This imbalance
    meant that Tor clients were severely limited on throughput (and
    probably latency too) by the first hop in their circuit. Now we
    select guards weighted by currently advertised bandwidth. We also
    automatically discard guards picked using the old algorithm. Fixes
    bug 1217; bugfix on 0.2.1.3-alpha. Found by Mike Perry.

o Major bugfixes:
  - Make Tor work again on the latest OS X: when deciding whether to
    use strange flags to turn TLS renegotiation on, detect the OpenSSL
    version at run-time, not compile time. We need to do this because
    Apple doesn't update its dev-tools headers when it updates its
    libraries in a security patch.
  - Fix a potential buffer overflow in lookup_last_hid_serv_request()
    that could happen on 32-bit platforms with 64-bit time_t. Also fix
    a memory leak when requesting a hidden service descriptor we've
    requested before. Fixes bug 1242, bugfix on 0.2.0.18-alpha. Found
    by aakova.

o Directory authority changes:
  - Change IP address for dannenberg (v3 directory authority), and
    remove moria2 (obsolete v1, v2 directory authority and v0 hidden
    service directory authority) from the list.

o Minor bugfixes:
  - Refactor resolve_my_address() to not use gethostbyname() anymore.
    Fixes bug 1244; bugfix on 0.0.2pre25. Reported by Mike Mestnik.
```

```
o Minor features:
  - Avoid a mad rush at the beginning of each month when each client
    rotates half of its guards. Instead we spread the rotation out
    throughout the month, but we still avoid leaving a precise timestamp
    in the state file about when we first picked the guard. Improves
    over the behavior introduced in 0.1.2.17.
```

2. On February 21st, we released an update Tor stable in 0.2.1.24. Tor 0.2.1.24 makes Tor work again on the latest OS X – this time for sure!

```
o Minor bugfixes:
  - Work correctly out-of-the-box with even more vendor-patched versions
    of OpenSSL. In particular, make it so Debian and OS X don't need
    customized patches to run/build.
```

3. On February 22, we released the latest in the -alpha series, 0.2.2.9-alpha.

```
o Directory authority changes:
  - Change IP address for dannenberg (v3 directory authority), and
    remove moria2 (obsolete v1, v2 directory authority and v0 hidden
    service directory authority) from the list.

o Major bugfixes:
  - Make Tor work again on the latest OS X: when deciding whether to
    use strange flags to turn TLS renegotiation on, detect the OpenSSL
    version at run-time, not compile time. We need to do this because
    Apple doesn't update its dev-tools headers when it updates its
    libraries in a security patch.
  - Fix a potential buffer overflow in lookup_last_hid_serv_request()
    that could happen on 32-bit platforms with 64-bit time_t. Also fix
    a memory leak when requesting a hidden service descriptor we've
    requested before. Fixes bug 1242, bugfix on 0.2.0.18-alpha. Found
    by aakova.
  - Authorities could be tricked into giving out the Exit flag to relays
    that didn't allow exiting to any ports. This bug could screw
    with load balancing and stats. Bugfix on 0.1.1.6-alpha; fixes bug
    1238. Bug discovered by Martin Kowalczyk.
  - When freeing a symmetric 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 static compilation by listing the openssl libraries in the right
    order. Bugfix on Tor 0.2.2.8-alpha; fixes bug 1237.
  - Resume handling .exit hostnames in a special way: originally we
    stripped the .exit part and used the requested exit relay. In
    0.2.2.1-alpha we stopped treating them in any special way, meaning
    if you use a .exit address then Tor will pass it on to the exit
    relay. Now we reject the .exit stream outright, since that behavior
    might be more expected by the user. Found and diagnosed by Scott
```

```
    Bennett and Downie on or-talk.
  - Don't spam the controller with events when we have no file
    descriptors available. Bugfix on 0.2.1.5-alpha. (Rate-limiting
    for log messages was already solved from bug 748.)
  - Avoid a bogus overlapped memcpy in tor_addr_copy(). Reported by
    "memcpyfail".
  - Make the DNSPort option work with libevent 2.x. Don't alter the
    behaviour for libevent 1.x. Fixes bug 1143. Found by SwissTorExit.
  - Emit a GUARD DROPPED controller event for a case we missed.
  - Make more fields in the controller protocol case-insensitive, since
    control-spec.txt said they were.
  - Refactor resolve_my_address() to not use gethostbyname() anymore.
    Fixes bug 1244; bugfix on 0.0.2pre25. Reported by Mike Mestnik.
  - Fix a spec conformance issue: the network-status-version token
    must be the first token in a v3 consensus or vote. Discovered by
    parakeep. Bugfix on 0.2.0.3-alpha.

o Code simplifications and refactoring:
  - Generate our manpage and HTML documentation using Asciidoc. This
    change should make it easier to maintain the documentation, and
    produce nicer HTML.
  - Remove the --enable-iphone option. According to reports from Marco
    Bonetti, Tor builds fine without any special tweaking on recent
    iPhone SDK versions.
  - Removed some unnecessary files from the source distribution. The
    AUTHORS file has now been merged into the people page on the
    website. The roadmaps and design doc can now be found in the
    projects directory in svn.
  - Enabled various circuit build timeout constants to be controlled
    by consensus parameters. Also set better defaults for these
    parameters based on experimentation on broadband and simulated
    high latency links.

o Minor features:
  - The 'EXTENDCIRCUIT' control port command can now be used with
    a circ id of 0 and no path. This feature will cause Tor to build
    a new 'fast' general purpose circuit using its own path selection
    algorithms.
  - Added a BUILDTIMEOUT_SET controller event to describe changes
    to the circuit build timeout.
  - Future-proof the controller protocol a bit by ignoring keyword
    arguments we do not recognize.
  - Expand homedirs passed to tor-checkkey. This should silence a
    coverity complaint about passing a user-supplied string into
    open() without checking it.
```

4. On February 15th, we released an updated Tor Browser Bundle; version 1.2.3. This new bundle contains:

```
update Vidalia to 0.2.7
```

```
update Tor to 0.2.1.23
update Qt to 4.6.2
update Polipo to 1.4.0.1
configure pidgin to not log chats by default
```

5. On February 27th, we released an updated Tor Browser Bundle, version 1.3.3. This new bundle contains:

```
update Firefox to 3.5.8
update Pidgin to 2.6.6
update Tor to 0.2.1.24
```

6. On February 18th, Tor for the Nokia Maemo mobile platform was announced. `https://blog.torproject.org/blog/tor-nokia-n900-maemo-gsm-telephone`. The announcement details are:

> We're always working on expanding the number of different devices and platforms where Tor runs. Today we've published an installation document that should help users of the Nokia N900 telephone to use the Tor network.
>
> Tor is configured as a client by default. The Tor status applet will also run privoxy and configure the system wide preferences appropriately while Tor is enabled. Transparent proxying is not possible with the default N900 kernels at this time.
>
> Please note that this is an experimental configuration. The web browser on the N900 does not have the protections that Torbutton provides.
>
> For basic circumvention needs this configuration should be usable out of the box. At the moment, we're not seriously investigating Torbutton support for the N900 mobile web browser. If there is significant user demand for a mobile Torbutton this may change.
>
> Many thanks to the fine folks at synthesize.us for their help in the production of the N900 documentation.

7. On February 7th, volunteers released a new beta of the Amnesia LiveCD, version 0.4.2. Amnesia is the merging of two projects, one of which is the Incognito LiveCD.

```
New release, mainly aimed at fixing live-initramfs security issue
(Debian bug #568750), with an additional set of small enhancements as
a bonus.

* live-initramfs: new custom package built from our own live-initramfs
  Git repository (commit 8b96e5a6cf8abc)
- based on new 1.173.1-1 upstream release
- fixed live-media=removable behaviour so that filesystem images found
  on non-removable storage are really never used (Debian bug #568750)

* Vidalia: bring back our UI customizations (0.2.7-1~lenny+amnesia1)
```

```
* APT: consistently use the GeoIP-powered cdn.debian.net

* Software: make room so that {alpha, future} Squeeze images fit on
  700MB CD-ROM
- only install OpenOffice.org's calc, draw, impress, math and writer components
- removed OpenOffice.org's English hyphenation and thesaurus
- removed hunspell, wonder why it was ever added

* Boot
- explicitly disable persistence, better safe than sorry
- removed compulsory 15s timeout, live-initramfs knows how to wait for
  the Live media to be ready

* Build system: don't cache rootfs anymore
```

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

Work continues to improve the Tor ports for Android, Maemo, and iPhone.

We worked with Ian Goldberg at University of Waterloo to come up with a plan for one of his grad students to continue working on "Nymbler", which is a framework they're working on that will allow Tor users to remain anonymous yet prove to websites like Wikipedia and Slashdot that they are not jerks (or at least, not yet known to be jerks). This *anonymous authentication* approach will hopefully be a step toward letting Tor users post to Wikipedia again; but it is still in its very early stages.

Along these same lines, the Freenode IRC channel has been experimenting with a new way to allow Tor users to interact in their chat rooms while still being able to contain the abuse potential: `http://blog.freenode.net/2010/01/connecting-to-freenode-using-tor-sasl/`.

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

Roger, Karsten, Steven met with Paul Syverson and Aaron Johnson at UT Austin to continue basic research on designs to let Tor users take advantage of local knowledge of how safe various Tor relays are in order to build safer paths through the network. The first goal is to answer questions like "If I believe that these relays are monitored by the Chinese government, then avoiding them will improve my security, but avoiding them could also stand out because I behave differently than other Tor users; what's the right balance?" The second goal is to figure out how path selection should work when the user runs one of the relays herself, and thus knows it's more trusted. The third goal is to come up with intuitive interfaces for letting users specify which parts of the network they trust more, while at the same time explaining the security implications of each choice.

Roger and Karsten also met with Vitaly Shmatikov to learn more about his recent work on "differential privacy", which is an academic approach to making sure that numbers in databases

do not leak too much identifying information. This question needs more attention because of the way Tor is computing and publishing "sanitized" user statistics on its metrics portal.

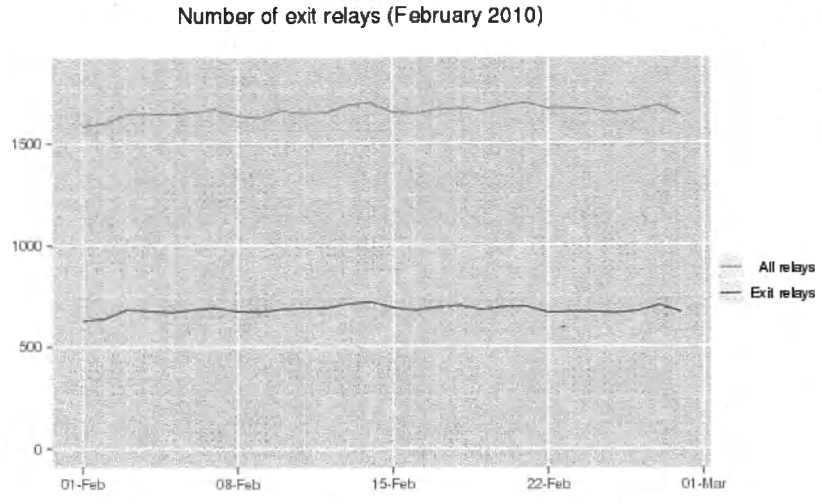
Roger also finished the first draft of his "Ten things to look for in tools that circumvent Internet censorship" document that we hope will eventually be a useful primer for policy people getting involved in this space: `https://svn.torproject.org/svn/projects/articles/circumvention-features.html`

## C.2.5. Hide Tor's network signature.

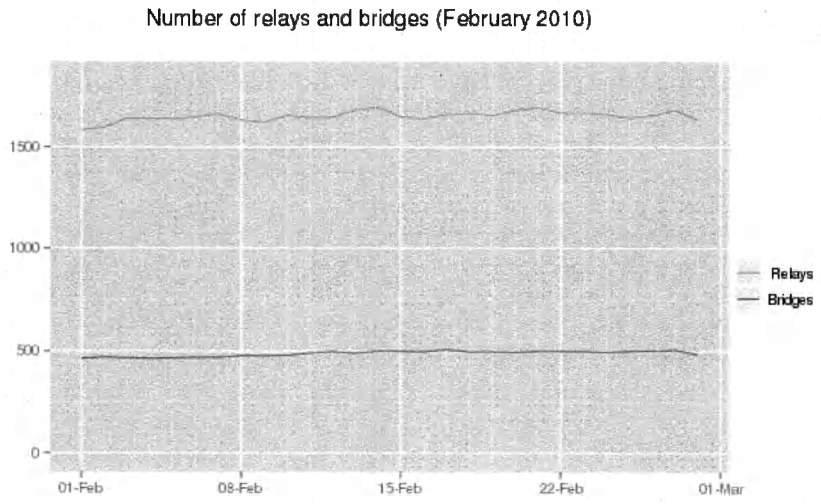
Nothing to report.

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

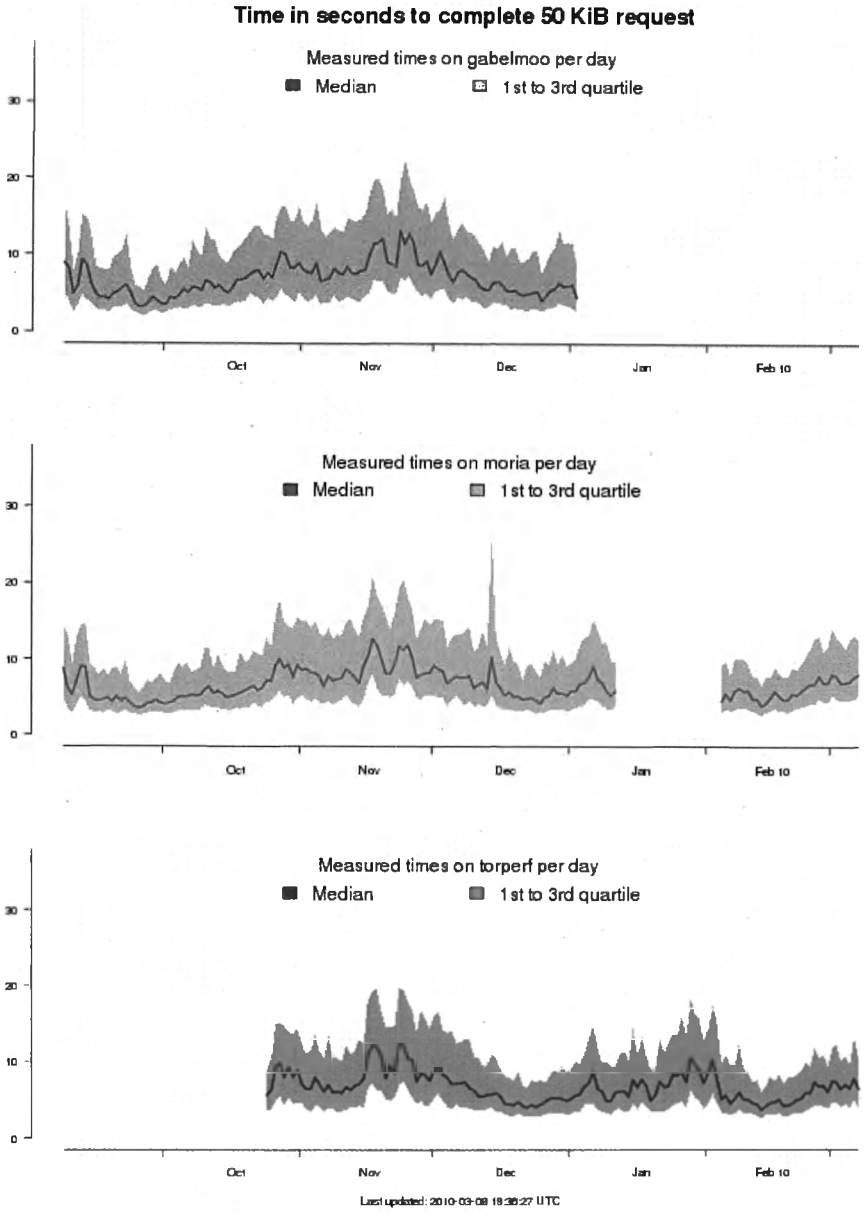
### Measures of the Tor Network




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

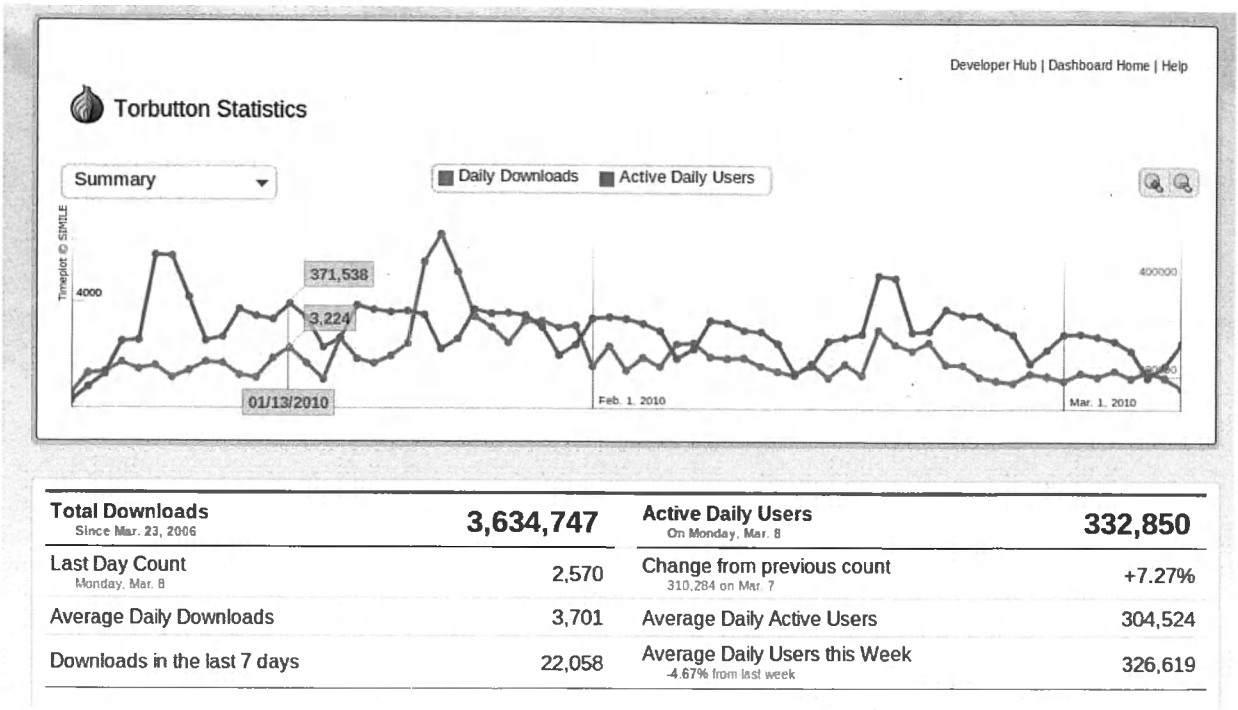



This graph shows the total quantity of relays and the total quantity of bridges in February 2010. The quantity of bridges is slowly increasing throughout the month.




This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. The server gabelmoo, the blue graph, is no longer running this measurement, but is shown for historical purposes. Due to our security incident in January, moria stopped running the test for a month or so. The server "torperf", the green graph, has been running the measurements continuously. As you can see performance slightly decreased over the month as more users came online, but overall performance was less variable than in months past. Moria is located in Cambridge, Massachusetts. torperf is located in Chicago, Illinois. We're bringing up another tor performance measurement client in Sweden in March 2010. 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-banwidth environments.




| Total Downloads<br>Since Mar. 23, 2006 | 3,634,747 | Active Daily Users<br>On Monday, Mar. 8 | 332,850 |
|---|---|---|---|
| Last Day Count<br>Monday, Mar. 8 | 2,570 | Change from previous count<br>310,284 on Mar. 7 | +7.27% |
| Average Daily Downloads | 3,701 | Average Daily Active Users | 304,524 |
| Downloads in the last 7 days | 22,058 | Average Daily Users this Week<br>-4.67% from last week | 326,619 |

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

- Roger spoke to the Philadelphia Linux Users' Group about Tor and censorship. Several of the members are now looking at volunteering on Tor development. Roger also did a talk on Tor for undergraduates in Drexel University's security class.
- Andrew joined EDRI, `http://www.edri.org`, in a discussion with Members of European Parliament. and their staff along with senior staff from the European Commission Directorate-General - Justice, Freedom, Security about censorship, data retention, and online privacy.
- Andrew gave a Tor talk to around 500 people at FOSDEM, `http://www.fosdem.org`.
- Andrew, Roger, and Karen met with Access, `http://accessnow.org`, to discuss a bridges4tor campaign to increase the number of Tor Bridges, `https://www.torproject.org/bridges`, for users in censored countries.

- Steven spoke to around 80 people at Secure Application Development 2010, `http://secappdev.org/`, in Groot Begijnhof, Leuven, Belgium.
- We worked with Susan Landau to help her better understand Tor in the context of freedom, privacy, and circumvention tools, so that her upcoming book on the subject can be more accurate.
- We worked with Dave Dittrich and other researchers in the botnet community to investigate a set of suspicious Tor relays that appeared to be associated with a bot network the researchers were tracking. We eventually decided to cut these suspicious relays out of the Tor network.
- We talked a little bit with the fellow writing a circumvention tool called Puff. On the one hand, it looks like yet another centralized proxy where the operator could screw the users but promises not to. On the other hand, he seems technically savvy and he seems to really care about doing the right thing. We should talk with him more to help him improve the safety that his service can provide.

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

On February 15th, we released an updated Tor Browser Bundle; version 1.2.3. This new bundle contains:

```
update Vidalia to 0.2.7
update Tor to 0.2.1.23
update Qt to 4.6.2
update Polipo to 1.4.0.1
configure pidgin to not log chats by default
```

On February 27th, we released an updated Tor Browser Bundle, version 1.3.3. This new bundle contains:

```
update Firefox to 3.5.8
update Pidgin to 2.6.6
update Tor to 0.2.1.24
```

On February 7th, volunteers released a new beta of the Amnesia LiveCD, version 0.4.2. Amnesia is the merging of two projects, one of which is the Incognito LiveCD. We've included the release notes in section C.2.0 above.

## C.2.12 Bridge relay and bridge authority work.

We're currently researching how to turn every tor client into a bridge by default, if the client finds itself reachable externally. This will dramatically increase the available bridges. There are some new attacks and challenges to overcome before this can be deployed as part of a -stable release, but we expect by Q3 2010 to have this into -alpha releases.

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

From the 0.2.2.9-alpha changelog:

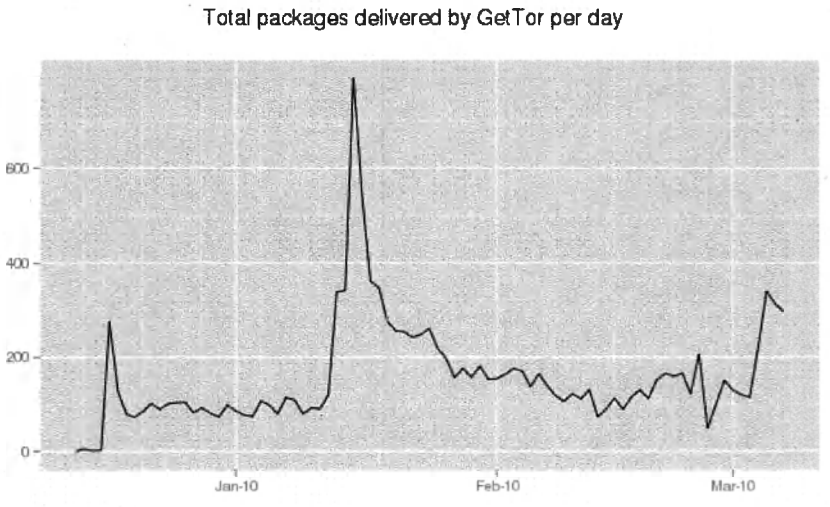
> We were selecting our guards uniformly at random, and then weighting which of our guards we'd use uniformly at random. This imbalance meant that Tor clients were severely limited on throughput (and probably latency too) by the first hop in their circuit. Now we select guards weighted by currently advertised bandwidth. We also automatically discard guards picked using the old algorithm. Fixes bug 1217; bugfix on 0.2.1.3-alpha. Found by Mike Perry.

## C.2.14. Incentives work.

Nothing to report.

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

Enhanced the metrics portal with numbers from the get-tor email autoresponder, `http://metrics.torproject.org/gettor-graphs.html`.




## C.2.16. Footprints from Tor Browser Bundle.

We've picked up the work towards a Tor Browser Bundle for OS X and Linux, and hope to have experimental bundles for at least one of those platforms ready in March. Soon after they're ready for testing, we'll want to start looking at how footprints from running the bundle differ on each platform.

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

Translated content updates for Torbutton, Tor Browser, Website, General Documentation, Vidalia interface, and TorCheck in Chinese, German, French, Italian, Dutch, Norwegian, Polish, Russian, Arabic, Farsi, Burmese, Spanish, Swedish, and Turkish.

## Upcoming plans, conferences, and schedules.

Roger meets with Sina from Access Now, March 1

Karen does her panel at UMD, March n

Andrew, Erinn, Runa will speak at LibrePlanet in Boston, March 19-21: `http://groups.fsf.org/wiki/LibrePlanet2010`

Roger does a talk for University of New Mexico, April 12

Andrew and Paul are on panel at ITSG, Apr 14-15

We're doing a talk for CDT on Apr 16

Roger does a talk for ETH Zurich and Google Zurich, Apr 20-21

Roger, Jake, and Linus meet with Swedish law enforcement, May 4

Andrew is speaking at Yahoo's Human Rights Summit on May 5

Roger and Jake do a talk for Trefpunkt in Sweden, May 5-6

Karen and Erinn attend Global Voices Summit in Chile, May 6-7

Roger, Jake, and Linus attend Amnesty International meeting in Stockholm, May 8-9

Roger talks at AUSCert in Brisbane, mid to late May

Most Tor developers will be at PETS in Berlin, July 21-23

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


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

## C 2.0. New releases, new hires, new funding

- On July 4th, we released Tor Browser Bundle 1.3.7 for Microsoft Windows. This is a security update for Firefox and Pidgin. The changes are: update to Firefox 3.5.10 and Pidgin Instant Messenger 2.7.1r2 to fix some security issues.

- On July 6th, we released Tor Browser Bundle 1.0.8 for GNU/Linux distributions. This fixes a number of security issues with included software. The updates include:

```
Update libpng to 1.4.3 (see CVE-2010-1205)
    Update Firefox to 3.5.10
    Update HTTPS Everywhere to 0.2.1
```

- On July 12th, we released the Tor 0.2.2.14-alpha. This latest -alpha greatly improves client-side handling of circuit build timeouts, which are used to estimate speed and improve performance. We also move to a much better GeoIP database, port Tor to Windows CE, introduce new compile flags that improve code security, add an eighth v3 directory authority, and address a lot of more minor issues.

```
o Major bugfixes:
    - Tor directory authorities no longer crash when started with a
      cached-microdesc-consensus file in their data directory. Bugfix
      on 0.2.2.6-alpha; fixes bug 1532.
    - Treat an unset $HOME like an empty $HOME rather than triggering an
      assert. Bugfix on 0.0.8pre1; fixes bug 1522.
    - Ignore negative and large circuit build timeout values that can
      happen during a suspend or hibernate. These values caused various
      asserts to fire. Bugfix on 0.2.2.2-alpha; fixes bug 1245.
    - Alter calculation of Pareto distribution parameter 'Xm' for
      Circuit Build Timeout learning to use the weighted average of the
      top N=3 modes (because we have three entry guards). Considering
      multiple modes should improve the timeout calculation in some cases,
      and prevent extremely high timeout values. Bugfix on 0.2.2.2-alpha;
      fixes bug 1335.
    - Alter calculation of Pareto distribution parameter 'Alpha' to use a
```

right censored distribution model. This approach improves over the synthetic timeout generation approach that was producing insanely high timeout values. Now we calculate build timeouts using truncated times. Bugfix on 0.2.2.2-alpha; fixes bugs 1245 and 1335.
- Do not close circuits that are under construction when they reach the circuit build timeout. Instead, leave them building (but do not use them) for up until the time corresponding to the 95th percentile on the Pareto CDF or 60 seconds, whichever is greater. This is done to provide better data for the new Pareto model. This percentile can be controlled by the consensus.

o Major features:
- Move to the June 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 have more accurate data for many African countries.
- Port Tor to build and run correctly on Windows CE systems, using the wcecompat library. Contributed by Valerio Lupi.
- New "--enable-gcc-hardening" ./configure flag (off by default) to turn on gcc compile time hardening options. It ensures that signed ints have defined behavior (-fwrapv), enables -D_FORTIFY_SOURCE=2 (requiring -O2), adds stack smashing protection with canaries (-fstack-protector-all), turns on ASLR protection if supported by the kernel (-fPIE, -pie), and adds additional security related warnings. Verified to work on Mac OS X and Debian Lenny.
- New "--enable-linker-hardening" ./configure flag (off by default) to turn on ELF specific hardening features (relro, now). This does not work with Mac OS X or any other non-ELF binary format.

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

o Minor features:
- New config option "WarnUnsafeSocks 0" disables the warning that occurs whenever Tor receives only an IP address instead of a hostname. Setups that do DNS locally over Tor are fine, and we shouldn't spam the logs in that case.
- Convert the HACKING file to asciidoc, and add a few new sections to it, explaining how we use Git, how we make changelogs, and what should go in a patch.
- 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. Fixes bug 1296.
- More gracefully handle corrupt state files, removing asserts in favor of saving a backup and resetting state.

```
    - Rename the "log.h" header to "torlog.h" so as to conflict with fewer
      system headers.

  o Minor bugfixes:
    - Build correctly on OSX with zlib 1.2.4 and higher with all warnings
      enabled.
    - When a2x fails, mention that the user could disable manpages instead
      of trying to fix their asciidoc installation.
    - Where available, use Libevent 2.0's periodic timers so that our
      once-per-second cleanup code gets called even more closely to
      once per second than it would otherwise. Fixes bug 943.
    - If you run a bridge that listens on multiple IP addresses, and
      some user configures a bridge address that uses a different IP
      address than your bridge writes in its router descriptor, and the
      user doesn't specify an identity key, their Tor would discard the
      descriptor because "it isn't one of our configured bridges", and
      fail to bootstrap. Now believe the descriptor and bootstrap anyway.
      Bugfix on 0.2.0.3-alpha.
    - If OpenSSL fails to make a duplicate of a private or public key, log
      an error message and try to exit cleanly. May help with debugging
      if bug 1209 ever remanifests.
    - Save a couple bytes in memory allocation every time we escape
      certain characters in a string. Patch from Florian Zumbiehl.
    - Make it explicit that we don't cannibalize one-hop circuits. This
      happens in the wild, but doesn't turn out to be a problem because
      we fortunately don't use those circuits. Many thanks to outofwords
      for the initial analysis and to swissknife who confirmed that
      two-hop circuits are actually created.
    - Make directory mirrors report non-zero dirreq-v[23]-shares again.
      Fixes bug 1564; bugfix on 0.2.2.9-alpha.
    - Eliminate a case where a circuit build time warning was displayed
      after network connectivity resumed. Bugfix on 0.2.2.2-alpha.
```

- On July 15th, we released the latest version of OrBot, tor for the Android operating system, version 0.0.8. Fixes include:

```
- Updated Settings & App configuration screens
- Changed progress dialog display
- Significant application re-arch
- Fixed force stop crash on install
- Integrated Tor 0.2.2.13-alpha-dev binary
- Fixed su shell cmd error handling & root perms issue
- #1570: Added new setup wizard on install to clarify root / non-root capabilities
- #1716: Per-app traffic routing prefs not persisted
- #1509: Help window is too big for the screen on android 1.6
- #1513: Orbot can't be told to exit <-- added 'Exit' menu option
- #1530: Capture sh cmd stout for debugging errors <-- updated debug log screen
- #1531: Don't loop ad infinitum in Orbot fails <-- only retries 3 times now
- #1272: Orbot should store Tor files in the cache
- #1273: Info should mention anonymity problems with ProxySurf
```

- On July 22nd, we released updated Tor Browser Bundles for Windows. Versions 1.3.8 and 1.3.9 are upgrades to fix security issues with Firefox and Pidgin. Firefox is updated to 3.5.11. Pidgin Instant Messenger client is updated to 2.7.2.

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

- We worked with some Nigerians to determine that the Nigerian government is not mandating Internet censorship. Rather, a few ISPs in Nigeria have closed loopholes that allowed some people to obtain Internet access without paying for an account. The blog post, subsequent comments, and research results are at `https://blog.torproject.org/blog/dear-nigerians-help-us-help-you`.

- Jacob, Robert Hogan, and Damian McCoy submitted a proposal to separate streams by port or host from the Tor client. The full proposal can be read at `http://archives.seul.org/or/dev/Jul-2010/msg00021.html`. The motivation for this proposal is as follows:

  "Streams are currently attached to circuits without regard to their content, destination host, or destination port. We propose two options, IsolateStreamsByPort and IsolateStreamsByHost to change the default behavior.

  The contents of some streams will always have revealing plain text information; these streams should be treated differently than other streams that may or may not have unencrypted PII content. DNS, with the exception of DNSCurve, is always unencrypted. It is reasonable to assume that other protocols may exist that have a similar issue and may cause user concern. It is also the case that we must balance network load issues and stream privacy. The Tor network will not currently scale to one circuit per connection nor should it anytime soon.

  Circuits are currently created with a few constraints and are rotated within a reasonable time window. This allows a rogue exit nodes to correlate all streams on a given circuit."

- Continuing research into how the Chinese firewall is currently able to block 90% of the Tor relays and bridges. It seems the firewall is configured to block specific IP Address and TCP Port combinations, as changing combinations on individual IP addresses results in updates to the blocking scheme. The blocking updates in the firewall are possibly updated every two weeks. An interesting area of research would be to do a technical analysis of blocking methods around the world on both landline and mobile Internet connections.

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

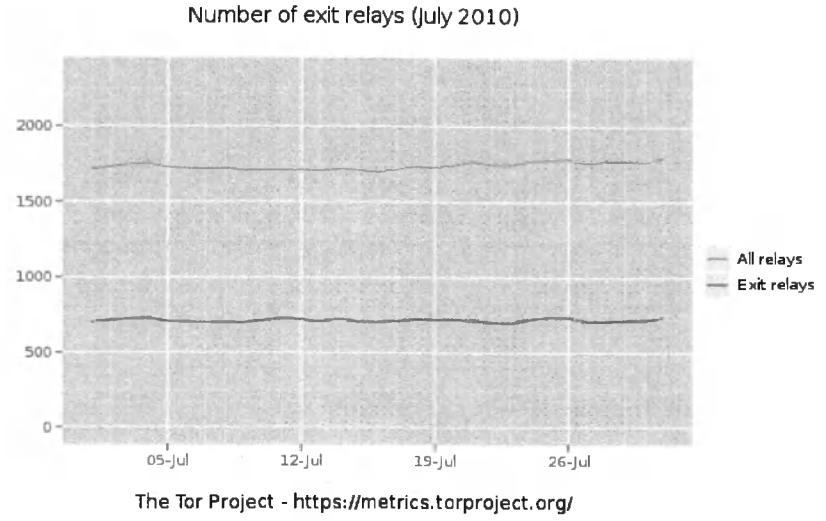
Nothing to report.

## C.2.5. Hide Tor's network signature.

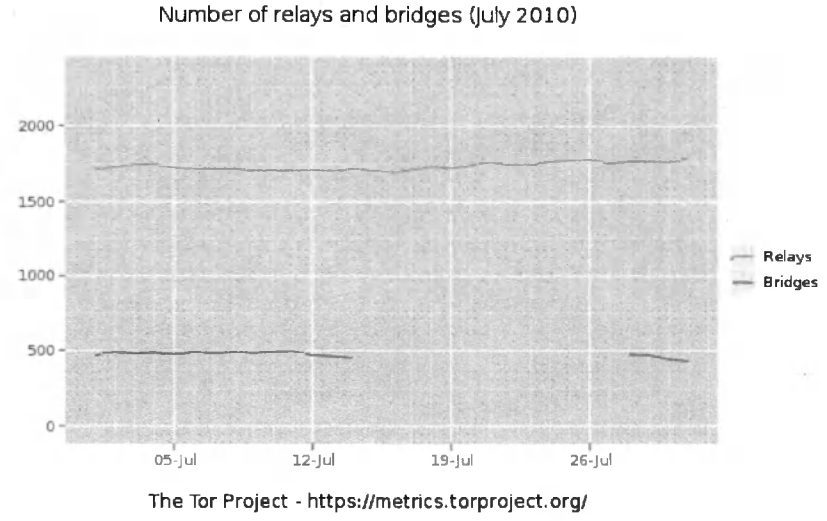
Nothing to report.

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

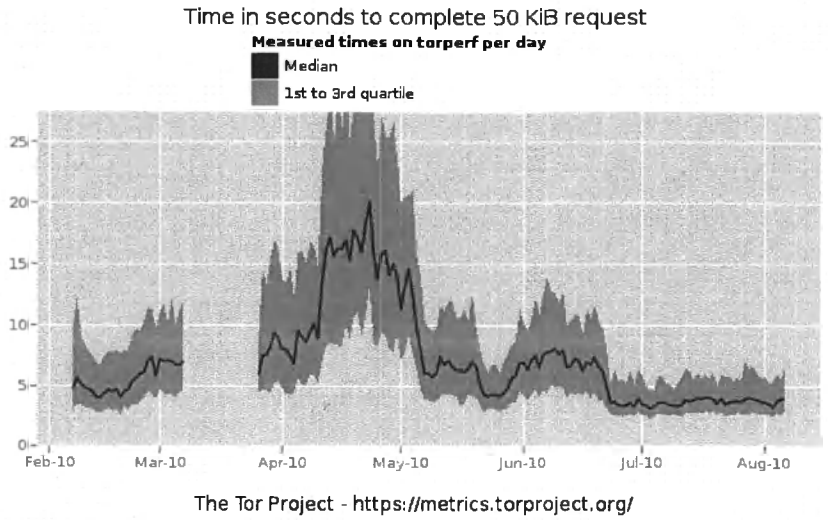
### Measures of the Tor Network




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




This graph shows the total quantity of relays and the total quantity of bridges in July 2010. The quantity of bridges is declining 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 stayed low for the second month in a row.

## Outreach and Advocacy

- Roger trained more Internews staff on what Tor is and how to use it.
- Tor held its second annual developer meeting in Potsdam, Germany. 24 committed employees, contractors, and volunteers were invited to the "un-conference". It was held over two days at the Hasso Plattner Institute at the University of Potsdam. The developers picked the topics and led the discussions over the two days. Topics ranged from an itemization and ownership of all 24 products tor produces to fundraising and financial details of our successful A-133 compliance audit. The current list of products and owners is at `https://trac.torproject.org/projects/tor/wiki/projects/ProductsandAssignments`. We also rolled out a new project management system and methodolgy to keep track of our growing ecosystem of software, advocacy, and related projects. See `https://trac.torproject.org/projects/tor/wiki/projects/HowWeDoProjectManagement` for the details.
- Andrew, Ian, Paul, Karsten, and Steven presented at the 2010 Privacy Enhancing Technologies Symposium in Berlin, Germany. `http://petsymposium.org/2010/`. Proceedings of the symposium are online through Springer at `http://www.springerlink.com/content/978-3-642-14526-1/`.
  - Ian's current research was presented by a co-author, Ryan Henry, on "Making a Nymbler Nymble Using VERBS". The abstract is available at `http://www.springerlink.com/content/3818173868g05737/`.
  - Ian's other current research topic was presented at HotPETS as a paper in progress on speeding up the Tor handshake. This will be turned into a formal proposal to Tor in

August 2010. Ian has actual code and results from live testing on the Tor network as well.

  - Paul's current research was presented by a co-author, Aaron Johnson, on "Preventing Active Timing Attacks in Low-Latency Anonymous Communication". The abstract is available at `http://www.springerlink.com/content/l8r648rr30187115/`.
  - Karsten presented on the vast quantities of data available to researchers at `http://metrics.torproject.org`. We're soon going to put all of this into a queryable database for easier access and research. This data is licensed under a Creative Commons Zero license, as defined at `http://creativecommons.org/publicdomain/zero/1.0/`. This material is supported in part by the National Science Foundation under Grant No. CNS-0959138.
  - Steven's current research was presented by a co-author, Claudia Diaz, on "Impact of Network Topology on Anonymity and Overhead in Low-Latency Anonymity Networks". The abstract is available at `http://www.springerlink.com/content/53535522423n2v68/`.

- Jacob and Seth Shoen of the EFF gave a talk about Tor and Internet Circumvention at The Next HOPE conference in New York City. Their talk is listed at `http://c2047862.cdn.cloudfiles.rackspacecloud.com/tnha08.mp3` or the full talks from the conference are online at `http://thenexthope.org/talks-list/`.

- Jacob gave a talk about Tor and Internet Circumvention at DEF CON 18 in Las Vegas, `http://defcon.org/html/defcon-18/dc-18-index.html`.

- Roger's advice on choosing a circumvention system was translated and published in Volume 2 of the China Rights Forum, `http://www.hrichina.org/public/contents/category?cid=175033`.

## 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. The Apple TBB is turning into a very tricky item to produce. Even with proper sandboxing support, the TBB leaves a large number of modified files behind due to the way Apple handles dmgs, and running binaries. Compounding progress is the way Firefox integrates into the system, resulting in code patches to the Firefox source.

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.

Tor now has another developer working on bridge authority and bridge database work. The goal is to be able to work down the list of items at `https://trac.torproject.org/projects/tor/wiki/projects/BridgeDB` over the next three months.

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

- Mike continues to tune the code for Bandwidth Authorities to better measure and load-balance the Tor network.
- Karsten completed his research into alternative GeoIP databases to more accurately asesss from where Tor clients connect. The original research started in April 2010, and was published at `http://archives.seul.org/or/dev/Apr-2010/msg00021.html`. From the 0.2.2.14-alpha change log, we chose to move to the June 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 have more accurate data for many African countries. This will be reflected in more accurate country graphs at `http://metrics.torproject.org/`.
- Karsten is conducting research into how to more accurately count tor clients than our current methods. The goal here is to get more accurate counts per country than the current sampling method without being able to de-anonymize any individual or group of Tor users.
- Karsten is rolling out new passive performance metrics about Tor. The goal is to better measure the Tor performance to gather more data to make better decisions. The start of the topic is at `http://archives.seul.org/or/dev/Jul-2010/msg00016.html`.
- We completed the first four of seven milestones on our National Science Foundation Grant No. CNS-0959138. The completed milestones are:
  1. Establish a preliminary metrics website to automatically publish daily graphs of collected data. Start with a) estimated user counts for China and Iran, and b) the results of our "torperf" performance scans.
  2. Technical report: Document our current approaches to measuring statistical data in the Tor anonymity network, and the legal/ethical/technical/social constraints around safe measurements.
  3. Publish a summary of what data and tools we have already, and what data and tools we hope to have. Then begin collaborating (ongoing) with the other researchers in the Anonymous Communications field to integrate our data and tools into their work so they can solve the problems we're actually seeing rather than the problems they speculate we might have.
  4. Instrument Tor relays to track resource load, including queue sizes, average cell latency, and number of active connections. Safely aggregate these results, then publish ongoing snapshots in our public dataset, and integrate them into our metrics website.

## C.2.14. Incentives work.

Nothing to report.

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

Erinn and Steven are working on an automated building system for packages. This will enable quicker, more reliable releases. The build system will also enable us to produce nightly packages of

the current working codebases for Tor and related software.

## 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.

- Updates to documentation and website in German, Russian, Polish, Swedish, Farsi, Turkish, Norwegian, French, Italian, Spanish, and Albanian.