From: Andrew Lewman, Executive Director
To: The Tor Community
Date: December 13, 2011

This report documents progress in November 2011.

New releases, new hires, new funding

New Releases

1. November 11th, we released new Tor Browser Bundles. The Tor Browser Bundles have been updated to Firefox 8. There was a slight delay as we adjusted to their new add-on management scheme, but everything should be working normally now.

   Tor Browser Bundle (2.2.34-2)

   ```
       - Update Firefox to 8.0
       - Update Libevent to 2.0.15-stable
       - Update NoScript to 2.1.8
       - Add extensions.autoDisableScopes to allow TBB's Firefox to launch with its extension
   ```

2. November 11th, the Tails team released the latest version of Tails, 0.9.

   Notable user-visible changes include:

   ```
   ## Tor
   - Upgrade to 0.2.2.34. This fixes CVE-2011-2768 and CVE-2011-2769 which
   prompted for manual updates for users of Tails 0.8.1.
   - Suppress Tor's warning about applications doing their own DNS
   lookups. Some users have reported concerns about these warnings, but it
   should be noted that they are completely harmless inside Tails as its
   system DNS resolver is Torified.

   - Linux 3.0.0-6, which fixed a great number of bugs and security issues.

   ## Iceweasel
   - Upgrade to 3.5.16-11 ((fixes CVE-2011-3647, CVE-2011-3648,
   CVE-2011-3650).
   - Torbutton: upgrade to 1.4.4.1-1, including support for the in-browser
   "New identity" feature.
   - FireGPG: upgrade to 0.8-1+tails2. Users are notified that the FireGPG
   ```

```
Text Editor is the only safe place for performing cryptographic
operations, and these operations has been disabled in other
places. Performing them outside of the editor opens up several severe
attacks through JavaScript (e.g. leaking plaintext when decrypting,
signing messages written by the attacker).
- Replace CS Lite with Cookie Monster for cookie management. Cookie
Monster has an arguably nicer interface, is being actively maintained
and is packaged in Debian.

## Software
- Install MAT, the Metadata Anonymisation Toolkit. Its goal is to
remove file metadata which otherwise could leak information about you
in the documents and media files you publish. This is the result of a
Tails developer's suggestion for GSoC 2011, although it ended up being
mentored by The Tor Project.
- Upgrade WhisperBack to 1.5~rc1. Users are guided how to send their bug
reports through alternative channels upon errors sending them. This will
make bug reporting easier when there's no network connection available.
- Upgrade TrueCrypt to 7.1.

## Miscellaneous
- The date and time setting system was completely reworked. This
should prevent time syncing issues that may prevent Tor from working
properly, which some users have reported. The new system will not leave
a fingerprintable network signature, like the old system did. Previously
that signature could be used to identify who is using Tails (but not
deanonymize them).
- Erase memory at shutdown: run many instances of the memory wiper. Due
to architectural limitations of i386 a process cannot access all memory
at the same time, and hence a single memory wipe instance cannot clear
all memory.
- Saner keyboard layouts for Arabic and Russian.
- Use Plymouth text-only splash screen at boot time.

Plus the usual bunch of minor bug reports and improvements. The full
technical changelog is available.

The full version of this release is available at http://tails.boum.org/news/version_0.9/.
```

3. November 14th, The Guardian Project released the latest version of orbot based on Tor 0.2.3.7-alpha. Full package available in the Android Market at https://market.android.com/details?id=org.torproject.android. The major new features are:

```
- - Nodes: exit/exclude/entrance node specification with strict is working
- - Wizard update: a new user interface process for the first-time user
- - Tor Tethering: if wifi or usb tethering is on, Orbot can route
```

```
traffic through Tor (aka "make your phone a Tor hotspot!" feature)
- - Settings for proxying Tor through another proxy is also now exposed
in Settings
- - And of course, support for all the other updates in 0.2.3.7-alpha

Has been primarily tested on Android 1.6 to 2.3.x, with some limited
testing on 3.x tablets.
```

4. November 14, we announced the availability of Tor bridge relay images in the Amazon Cloud, https://cloud.torproject.org. The Tor Cloud project gives you a user-friendly way of deploying bridges to help users access an uncensored Internet. By setting up a bridge, you donate bandwidth to the Tor network and help improve the safety and speed at which users can access the Internet.

   Setting up a Tor bridge on Amazon EC2 is simple and will only take you a couple of minutes. The images have been configured with automatic package updates and port forwarding, so you do not have to worry about Tor not working or the server not getting security updates.

   To help new customers get started in the cloud, Amazon is introducing a free usage tier. The Tor Cloud images are all micro instances, and new customers will be able to run a free micro instance for a whole year.

5. November 22, we released a new -alpha version of Tor. Tor 0.2.3.8-alpha fixes some crash and assert bugs, including a socketpair-related bug that has been bothering Windows users. It adds support to serve microdescriptors to controllers, so Vidalia's network map can resume listing relays (once Vidalia implements its side), and adds better support for hardware AES acceleration. Finally, it starts the process of adjusting the bandwidth cutoff for getting the ”Fast” flag from 20KB to (currently) 32KB – preliminary results show that tiny relays harm performance more than they help network capacity.

```
Changes in version 0.2.3.8-alpha - 2011-11-22
  o Major bugfixes:
    - Initialize Libevent with the EVENT_BASE_FLAG_NOLOCK flag enabled, so
      that it doesn't attempt to allocate a socketpair. This could cause
      some problems on Windows systems with overzealous firewalls. Fix for
      bug 4457; workaround for Libevent versions 2.0.1-alpha through
      2.0.15-stable.
    - Correctly sanity-check that we don't underflow on a memory
      allocation (and then assert) for hidden service introduction
      point decryption. Bug discovered by Dan Rosenberg. Fixes bug 4410;
      bugfix on 0.2.1.5-alpha.
    - Remove the artificially low cutoff of 20KB to guarantee the Fast
      flag. In the past few years the average relay speed has picked
      up, and while the "top 7/8 of the network get the Fast flag" and
      "all relays with 20KB or more of capacity get the Fast flag" rules
      used to have the same result, now the top 7/8 of the network has
      a capacity more like 32KB. Bugfix on 0.2.1.14-rc. Fixes bug 4489.
    - Fix a rare assertion failure when checking whether a v0 hidden
      service descriptor has any usable introduction points left, and
      we don't have enough information to build a circuit to the first
      intro point named in the descriptor. The HS client code in
      0.2.3.x no longer uses v0 HS descriptors, but this assertion can
      trigger on (and crash) v0 HS authorities. Fixes bug 4411.
      Bugfix on 0.2.3.1-alpha; diagnosed by frosty_un.
    - Make bridge authorities not crash when they are asked for their own
      descriptor. Bugfix on 0.2.3.7-alpha, reported by Lucky Green.
    - When running as a client, do not print a misleading (and plain
      wrong) log message that we're collecting "directory request"
      statistics: clients don't collect statistics. Also don't create a
      useless (because empty) stats file in the stats/ directory. Fixes
      bug 4353; bugfix on 0.2.2.34 and 0.2.3.7-alpha.

  o Major features:
    - Allow Tor controllers like Vidalia to obtain the microdescriptor
      for a relay by identity digest or nickname. Previously,
      microdescriptors were only available by their own digests, so a
      controller would have to ask for and parse the whole microdescriptor
      consensus in order to look up a single relay's microdesc. Fixes
      bug 3832; bugfix on 0.2.3.1-alpha.
    - Use OpenSSL's EVP interface for AES encryption, so that all AES
      operations can use hardware acceleration (if present). Resolves
      ticket 4442.

  o Minor bugfixes (on 0.2.2.x and earlier):
    - Detect failure to initialize Libevent. This fix provides better
      detection for future instances of bug 4457.
    - Avoid frequent calls to the fairly expensive cull_wedged_cpuworkers
      function. This was eating up hideously large amounts of time on some
      busy servers. Fixes bug 4518; bugfix on 0.0.9.8.
    - Don't warn about unused log_mutex in log.c when building with
      --disable-threads using a recent GCC. Fixes bug 4437; bugfix on
      0.1.0.6-rc which introduced --disable-threads.
    - Allow manual 'authenticate' commands to the controller interface
      from netcat (nc) as well as telnet. We were rejecting them because
      they didn't come with the expected whitespace at the end of the
      command. Bugfix on 0.1.1.1-alpha; fixes bug 2893.
    - Fix some (not actually triggerable) buffer size checks in usage of
      tor_inet_ntop. Fixes bug 4434; bugfix on Tor 0.2.0.1-alpha. Patch
      by Anders Sundman.
    - Fix parsing of some corner-cases with tor_inet_pton(). Fixes
      bug 4515; bugfix on 0.2.0.1-alpha; fix by Anders Sundman.
    - When configuring, starting, or stopping an NT service, stop
```

```
      immediately after the service configuration attempt has succeeded
      or failed. Fixes bug 3963; bugfix on 0.2.0.7-alpha.
    - When sending a NETINFO cell, include the original address
      received for the other side, not its canonical address. Found
      by "troll_un"; fixes bug 4349; bugfix on 0.2.0.10-alpha.
    - Rename the bench_{aes,dmap} functions to test_*, so that tinytest
      can pick them up when the tests aren't disabled. Bugfix on
      0.2.2.4-alpha which introduced tinytest.
    - Fix a memory leak when we check whether a hidden service
      descriptor has any usable introduction points left. Fixes bug
      4424. Bugfix on 0.2.2.25-alpha.
    - Fix a memory leak in launch_direct_bridge_descriptor_fetch() that
      occurred when a client tried to fetch a descriptor for a bridge
      in ExcludeNodes. Fixes bug 4383; bugfix on 0.2.2.25-alpha.

  o Minor bugfixes (on 0.2.3.x):
    - Make util unit tests build correctly with MSVC. Bugfix on
      0.2.3.3-alpha. Patch by Gisle Vanem.
    - Successfully detect AUTH_CHALLENGE cells with no recognized
      authentication type listed. Fixes bug 4367; bugfix on 0.2.3.6-alpha.
      Found by frosty_un.
    - If a relay receives an AUTH_CHALLENGE cell it can't answer,
      it should still send a NETINFO cell to allow the connection to
      become open. Fixes bug 4368; fix on 0.2.3.6-alpha; bug found by
      "frosty".
    - Log less loudly when we get an invalid authentication certificate
      from a source other than a directory authority: it's not unusual
      to see invalid certs because of clock skew. Fixes bug 4370; bugfix
      on 0.2.3.6-alpha.
    - Tolerate servers with more clock skew in their authentication
      certificates than previously. Fixes bug 4371; bugfix on
      0.2.3.6-alpha.
    - Fix a couple of compile warnings on Windows. Fixes bug 4469; bugfix
      on 0.2.3.4-alpha and 0.2.3.6-alpha.

  o Minor features:
    - Add two new config options for directory authorities:
      AuthDirFastGuarantee sets a bandwidth threshold for guaranteeing the
      Fast flag, and AuthDirGuardBWGuarantee sets a bandwidth threshold
      that is always sufficient to satisfy the bandwidth requirement for
      the Guard flag. Now it will be easier for researchers to simulate
      Tor networks with different values. Resolves ticket 4484.
    - When Tor ignores a hidden service specified in its configuration,
      include the hidden service's directory in the warning message.
      Previously, we would only tell the user that some hidden service
      was ignored. Bugfix on 0.0.6; fixes bug 4426.
    - When we fail to initialize Libevent, retry with IOCP disabled so we
      don't need to turn on multi-threading support in Libevent, which in
      turn requires a working socketpair(). This is a workaround for bug
      4457, which affects Libevent versions from 2.0.1-alpha through
      2.0.15-stable.
    - Detect when we try to build on a platform that doesn't define
      AF_UNSPEC to 0. We don't work there, so refuse to compile.
    - Update to the November 1 2011 Maxmind GeoLite Country database.

  o Packaging changes:
    - Make it easier to automate expert package builds on Windows,
      by removing an absolute path from makensis.exe command.

  o Code simplifications and refactoring:
    - Remove some redundant #include directives throughout the code.
      Patch from Andrea Gelmini.
    - Unconditionally use OpenSSL's AES implementation instead of our
      old built-in one. OpenSSL's AES has been better for a while, and
      relatively few servers should still be on any version of OpenSSL
      that doesn't have good optimized assembly AES.
    - Use the name "CERTS" consistently to refer to the new cell type;
      we were calling it CERT in some places and CERTS in others.

  o Testing:
    - Numerous new unit tests for functions in util.c and address.c by
      Anders Sundman.
    - The long-disabled benchmark tests are now split into their own
      ./src/test/bench binary.
    - The benchmark tests can now use more accurate timers than
      gettimeofday() when such timers are available.
```

6. November 24, we updated the Tor Browser Bundle. The Tor Browser Bundles have been updated to Firefox 8.0.1 along with a new Libevent and some extension updates.

```
Tor Browser Bundle (2.2.34-3)
    - Update Firefox to 8.0.1
    - Update Libevent to 2.0.16-stable
    - Update NoScript to 2.2
    - Update HTTPS Everywhere to 1.2.1
    - Begin building Tor with --enable-gcc-warnings
```

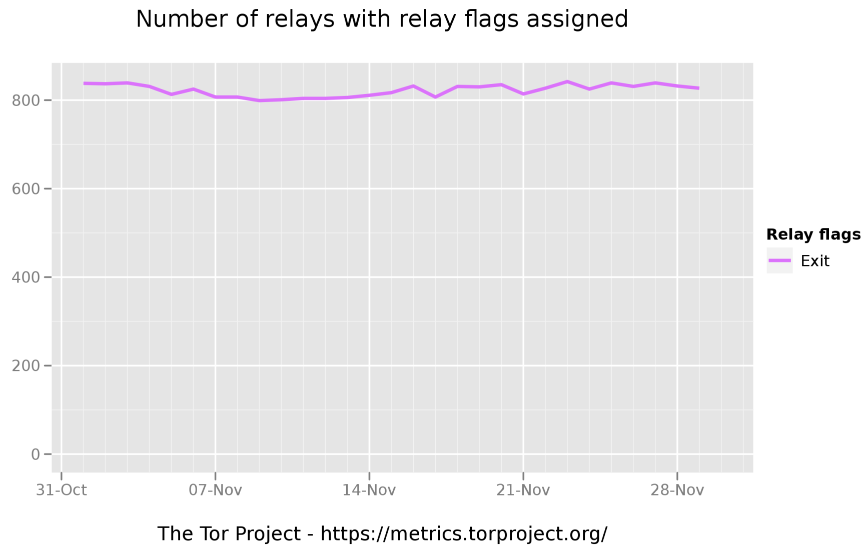
Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

- Aaron helped Sebastian track down some bugs in TorBEL (tickets, 4503, 4500, 4447)
- Integrated redesign of check.tpo into TorBEL. The check.torproject.org redesign is now a separate project with TorBEL as a dependency
- TorBEL will include DuckDuckGo search and TBB 'update available' features.
- Robert wrote some small Tor patches, most notably GETINFO items to fetch microdescriptors from Tor, (see ticket 3832), so the relay list in Vidalia's 'Network Map' can be updated to work with Tor 0.2.3.x.

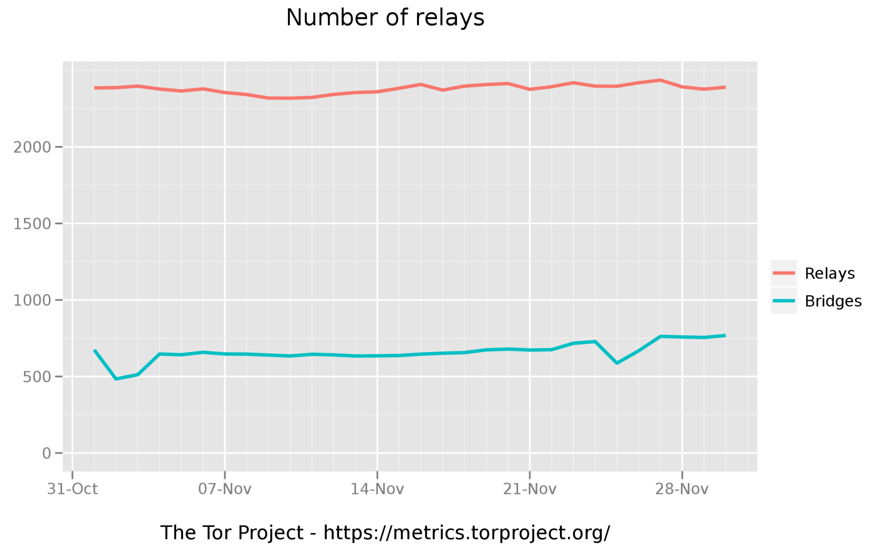
Hide Tor's network signature.

Grow the Tor network and user base. Outreach.

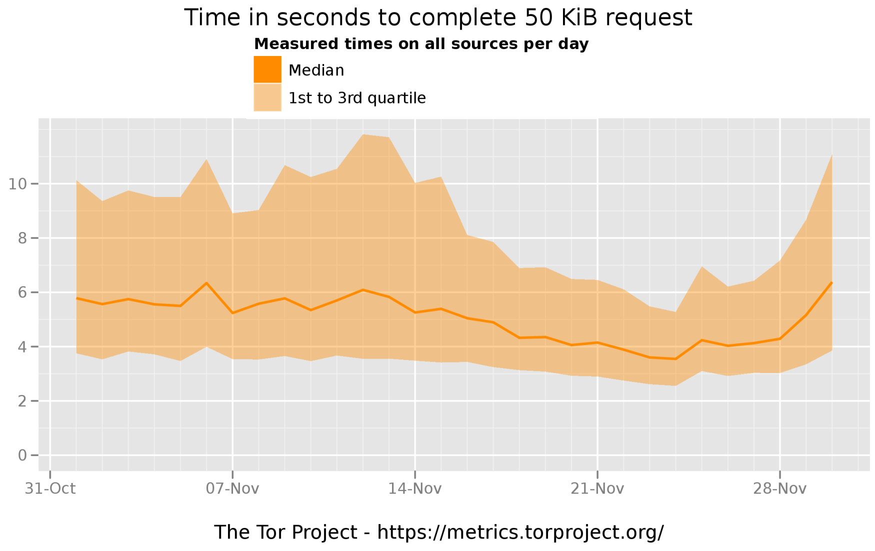
Measures of the Tor Network



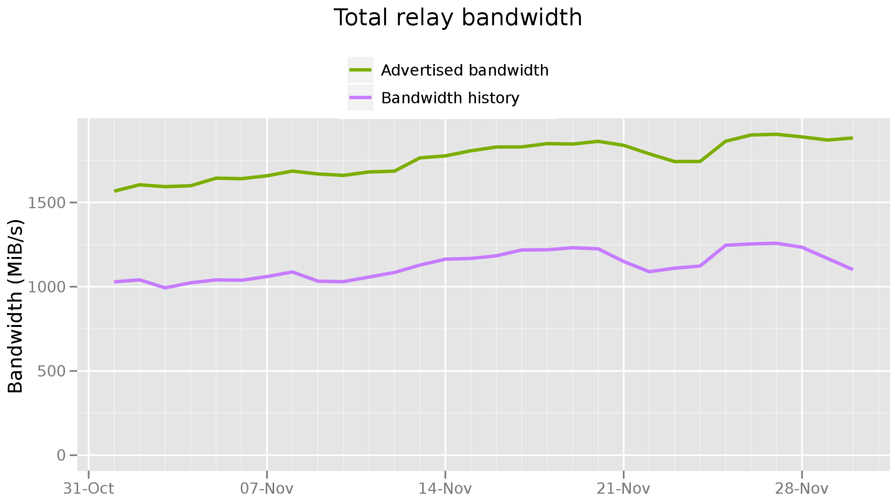
This graph shows the total quantity of exit relays in November 2011.



This graph shows the total quantity of relays and the total quantity of bridges in November 2011.



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



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

This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. Maintaining a capacity of 1.8 GBps (14.4 Gbps) available with 1.1 GBps (8.8 Gbps) used.

Outreach and Advocacy

1. Fabio Pietrosanti got Tor working on a WDTV, https://lists.torproject.org/pipermail/tor-dev/2011-November/003081.html.

2. Andrew spoke at the International Institute of Communications Conference in Ottawa, Canada, http://www.iic-canada.ca/english/2011conference/program.cfm.

3. We received some press based on the Tor Cloud launch, https://www.torproject.org/press/inthemedia.html.en.

4. Forbes picked up the story about odd probes from China, http://www.forbes.com/sites/andygreenberg/2011/11/17/chinas-great-firewall-tests-mysterious-scans-on-encrypted-connec related to this ticket, https://trac.torproject.org/projects/tor/ticket/4185.

5. Andrew talked to a homeless person assistance organization which wanted to put TorBrowser on their forthcoming internet cafe computers. Walked through how to set it up and keep it updated. The organization has asked to remain anonymous.

6. Added three new website mirrors and removed one non-responsive mirror.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- We launched the Tor Cloud, https://cloud.torproject.org. The Tor Cloud project gives you a user-friendly way of deploying bridges to help users access an uncensored Internet. By setting up a bridge, you donate bandwidth to the Tor network and help improve the safety and speed at which users can access the Internet.

This project runs on the Amazon EC2 cloud computing platform, which powers Amazon.com and other major websites. Amazon EC2 allows users to launch their own virtual machines and computing resources with flexible and cost-effective terms.

- Tails 0.9 anonymous live system is released, see the update in the first section, or read more in our announcement, https://blog.torproject.org/blog/tails-09-released.

Bridge relay and bridge authority work.

- George wrote Proposal 189, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/189-authorize-cell.txt. Proposal 187 introduced the concept of the AUTHORIZE cell, a cell whose purpose is to make Tor bridges resistant to scanning attacks.

  This is achieved by having the bridge and the client share a secret out-of-band and then use AUTHORIZE cells to validate that the client indeed knows that secret before proceeding with the Tor protocol.

  This proposal specifies the format of the AUTHORIZE cell and also introduces the AUTHORIZED cell, a way for bridges to announce to clients that the authorization process is complete and successful.

- George wrote Proposal 190, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/190-password-bridge-authorization.txt. Proposals 187 and 189 introduced the AUTHORIZE and AUTHORIZED cells.

  Their purpose is to make bridge relays scanning resistant against censoring adversaries capable of probing hosts to observe whether they speak the Tor protocol.

  This proposal specifies a bridge client authorization scheme based on a shared password between the bridge user and bridge operator.

- George wrote Proposal 191, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/191-mitm-bridge-detection-resistance.txt. Proposals 187, 189 and 190 make the first steps toward scanning resistant bridges. They attempt to block attacks from censoring adversaries who provoke bridges into speaking the Tor protocol.

  An attack vector that hasn't been explored in those previous proposals is that of an adversary capable of performing Man In The Middle attacks to Tor clients. At the moment, Tor clients using the v3 link protocol have no way to detect such an MITM attack, and will gladly send an VERSIONS or an AUTHORIZE cell to the MITMed connection, thereby revealing the Tor protocol and thus the bridge.

  This proposal introduces a way for clients to detect an MITMed SSL connection, allowing them to protect against the above attack.

- Sebastian wrote Proposal 192, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/192-store-bridge-information.txt. Currently, tor already stores some information about the bridges it is configured to use locally, but doesn't make great use of the stored data. This data is the Tor configuration information about the bridge (IP address, port, and optionally fingerprint) and the bridge descriptor which gets stored along with the other descriptors a Tor client fetches, as well as an ”EntryGuard” line in the state file. That line includes the Tor version we used to add the bridge, and a slightly randomized timestamp (up to a month in the past of the real date). The descriptor data also includes some more accurate timestamps about when the descriptor was fetched.

The information we give out about bridges via bridgedb currently only includes the IP address and port, because giving out the fingerprint as well might mean that Tor clients make direct connections to the bridge authority, since we didn't design Tor's UpdateBridgesFromAuthority behaviour correctly.

- Aaron started evaluating changes to BridgeDB in order to support proposal 186, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/186-multiple-orports.txt.

Scalability, load balancing, directory overhead, efficiency.

- Nick started a discussion on tor-dev about future cryptography operations in Tor, https://lists.torproject.org/pipermail/tor-dev/2011-November/002999.html.
- Damian continues to make great progress on stem, a tor control library for python. This should make integrating Tor into the larger world easier. The git repo for stem is at https://gitweb.torproject.org/stem.git.
- Many updates to the bandwidth authority codebase.
- Mike ran an experiment to test new methods of load balancing the network traffic. More details can be found in this post to the tor-relays mailing list, https://lists.torproject.org/pipermail/tor-relays/2011-December/001039.html.
- Robert found a memory leak which had severely affected tor26 (ticket 4424), mostly because frosty_un traced a tor26 crash to code near that leak.

Incentives work.

Nothing to report.

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

Nothing to report.

Footprints from Tor Browser Bundle.

- Thanks to lot of work by Erinn, 'shondoit', 'weasel', and others, the Windows TBBs are now building nightly, and all of the main components (tor, vidalia, libevent, and firefox) build when commits trigger buildbot. We can finally stop focusing on build issues and work on improving the functionality, branding, and footprint of TBB.

Translation work, ultimately a browser-based approach.

- Updated translations for the short user manual, vidalia, vidalia-help, orbot, gettor, bridgedb, and vidalia installer in Spanish, Farsi, Arabic, French, German, Greek, Hungarian, Italian, Mandarin Chinese, Turkish, Portugese, and Russian.
- Automated the merge of translations into the code repo/branches, https://gitweb.torproject.org/translation.git.