From: Andrew Lewman, Executive Director
To: the tor community
Date: April 10, 2011

This report documents progress in January 2011.

New releases, new hires, new funding

New Releases

1. On January 4th, we released the latest in the alpha branch of torbutton, version 1.3.1. This release features a fix for the nasty pref dialog issue in 1.3.0 (bug 2011), as well as Firefox 4.0 support. Thanks to new APIs in Firefox 3.5 and better privacy options in Firefox 4, Torbutton has now been simplified as well. While we still provide a number of XPCOM components, the number of native Firefox components we replace has shrunk from 5 to just one. However, the amount of changes involved in supporting Firefox 4 were substantial, and it is likely that these changes as well as the removal of old code has introduced new bugs. We've done our best to test out operation on Firefox 3.6 and 4.0, but we have not tested Firefox 3.0, and may have missed other issues as well.

   ```
   Here is the complete changelog:
   * bugfix: bug 1894: Amnesia is now called TAILS (patch from intrigeri)
   * bugfix: bug 2315: Remove reference to TorVM (patch from intrigeri)
   * bugfix: bug 2011: Fix preference dialog issues (patch from chrisdoble)
   * bugfix: Fix some incorrect log lines in RefSpoofer
   * new: Support Firefox 4.0 (many changes)
   * new: Place button in the nav-bar (FF4 killed the status-bar)
   * misc: No longer reimplement the session store, use new APIs instead
   * misc: Simplify crash detection and startup mode settings
   ```

2. On January 7th, A new release of arm was released, including enhancements targeted at performance and cross platform compatibility. In particular, this release provides...

   (a) Vastly Better Resolver Performance. By far the most expensive thing that arm does is ps and netstat/lsof/etc lookups. While wandering around development forums I discovered psutil, an awesome library for cross platform resolution of system and process information. For OSX and BSD they're using ps and lsof lookups just like arm. However, for Linux they had a very different approach, querying proc contents directly. I adapted the functions for arm and it cut the runtime for resource and connection resolution by 90%. Many thanks to the authors of psutil (Jay Loden, Dave Daeschler, and Giampaolo Rodola')!

(b) BSD Compatibility. For a long time FreeBSD has been arm's nemesis. Its variant of netstat can't get connection pids, the ss resolving utility belongs to a spreadsheet program instead, and even pid resolution failed (breaking resource stats and numerous other things). However, thanks to patches and testing by Fabian Keil and Hans Schnehl arm now has BSD counterparts for all of these, plus autodetection for BSD Jails.

(c) Expanded Distribution. Peter and I have finished revisions for the arm deb and it's now pending feedback from the Debian FTP admins. Arm is also now available on ArchLinux thanks to Spider.007 and Fabian mentioned that he might be interested in doing a FreeBSD port.

(d) Volunteer Recruiting. Being the lone developer of arm is kinda lonely. I'd love to find other people interested in hacking on the code with me. To this end, and in anticipation of GSOC 2011, I've added a project to Tor's volunteer page ("Client Mode Use Cases for Arm").

Plus numerous other fixes and improvements (for details see the release notes). As always, screenshots and downloads are available from the project's homepage: `http://www.atagar.com/arm/`

3. On January 9th, The Tor Browser Bundles were updated with some important security fixes and it is advised that all users upgrade. Geolocation has been disabled and some prefs added as a workaround for bug 2338.

   - Linux bundles, version 1.1.2. Update Firefox preferences to be more secure and disable geolocation to address 2338
   - OS X bundle, version 1.0.9. Update Firefox preferences to be more secure and disable geolocation to address 2338
   - Windows bundles, version 1.3.16. Update Firefox preferences to be more secure and disable geolocation to address 2338

4. On January 10th, we updated the OS X PPC packages after a long hiatus due to failed hardware. They are now available in stable (0.2.1.28) and alpha (0.2.2.20-alpha) versions, both with the latest Vidalia (0.2.10).

5. On January 15th, we released the latest in the stable Tor series, version Tor 0.2.1.29. This continues our recent code security audit work. The main fix resolves a remote heap overflow vulnerability that can allow remote code execution. Other fixes address a variety of assert and crash bugs, most of which we think are hard to exploit remotely. All Tor users should upgrade.

```
Changes in version 0.2.1.29:
  o Major bugfixes (security):
    - Fix a heap overflow bug where an adversary could cause heap
      corruption. This bug probably allows remote code execution
      attacks. Reported by "debuger". Fixes CVE-2011-0427. Bugfix on
      0.1.2.10-rc.
    - Prevent a denial-of-service attack by disallowing any
      zlib-compressed data whose compression factor is implausibly
```

```
    high. Fixes part of bug 2324; reported by "doorss".
  - Zero out a few more keys in memory before freeing them. Fixes
    bug 2384 and part of bug 2385. These key instances found by
    "cypherpunks", based on Andrew Case's report about being able
    to find sensitive data in Tor's memory space if you have enough
    permissions. Bugfix on 0.0.2pre9.

o Major bugfixes (crashes):
  - Prevent calls to Libevent from inside Libevent log handlers.
    This had potential to cause a nasty set of crashes, especially
    if running Libevent with debug logging enabled, and running
    Tor with a controller watching for low-severity log messages.
    Bugfix on 0.1.0.2-rc. Fixes bug 2190.
  - Add a check for SIZE_T_MAX to tor_realloc() to try to avoid
    underflow errors there too. Fixes the other part of bug 2324.
  - Fix a bug where we would assert if we ever had a
    cached-descriptors.new file (or another file read directly into
    memory) of exactly SIZE_T_CEILING bytes. Fixes bug 2326; bugfix
    on 0.2.1.25. Found by doorss.
  - Fix some potential asserts and parsing issues with grossly
    malformed router caches. Fixes bug 2352; bugfix on Tor 0.2.1.27.
    Found by doorss.

o Minor bugfixes (other):
  - Fix a bug with handling misformed replies to reverse DNS lookup
    requests in DNSPort. Bugfix on Tor 0.2.0.1-alpha. Related to a
    bug reported by doorss.
  - Fix compilation on mingw when a pthreads compatibility library
    has been installed. (We don't want to use it, so we shouldn't
    be including pthread.h.) Fixes bug 2313; bugfix on 0.1.0.1-rc.
  - Fix a bug where we would declare that we had run out of virtual
    addresses when the address space was only half-exhausted. Bugfix
    on 0.1.2.1-alpha.
  - Correctly handle the case where AutomapHostsOnResolve is set but
    no virtual addresses are available. Fixes bug 2328; bugfix on
    0.1.2.1-alpha. Bug found by doorss.
  - Correctly handle wrapping around when we run out of virtual
    address space. Found by cypherpunks, bugfix on 0.2.0.5-alpha.

o Minor features:
  - Update to the January 1 2011 Maxmind GeoLite Country database.
  - Introduce output size checks on all of our decryption functions.

o Build changes:
  - Tor does not build packages correctly with Automake 1.6 and earlier;
    added a check to Makefile.am to make sure that we're building with
    Automake 1.7 or later.
  - The 0.2.1.28 tarball was missing src/common/OpenBSD_malloc_Linux.c
    because we built it with a too-old version of automake. Thus that
    release broke ./configure --enable-openbsd-malloc, which is popular
    among really fast exit relays on Linux.
```

6. On January 16, we released many updated packages.

```
- Windows expert packages (stable & alpha)
- Vidalia bundles (stable & alpha for Windows, and OS X ppc & x86)
- Tor Browser Bundles for Windows, Linux, and OS X (see below for other updates)
- RPM packages (stable & alpha)
- Debian and Ubuntu packages (stable & alpha)
- Tor Browser Bundles
-- Windows Bundles, version 1.3.17
Update Tor to 0.2.1.29
-- Linux Bundles, verson 1.1.3
Update Tor to 0.2.2.21-alpha
Update NoScript to 2.0.9.3
-- OS X Bundles, version 1.0.10
Update Tor to 0.2.2.21-alpha
Update NoScript to 2.0.9.
```

7. On January 15th, we released the latest in the Tor alpha series, version 0.2.2.21-alpha. It includes all the patches from Tor 0.2.1.29, which continues our recent code security audit work. The main fix resolves a remote heap overflow vulnerability that can allow remote code execution (CVE-2011-0427). Other fixes address a variety of assert and crash bugs, most of which we think are hard to exploit remotely.

```
Changes in version 0.2.2.21-alpha
  o Major bugfixes (security), also included in 0.2.1.29:
    - Fix a heap overflow bug where an adversary could cause heap
      corruption. This bug probably allows remote code execution
      attacks. Reported by "debuger". Fixes CVE-2011-0427. Bugfix on
      0.1.2.10-rc.
    - Prevent a denial-of-service attack by disallowing any
      zlib-compressed data whose compression factor is implausibly
      high. Fixes part of bug 2324; reported by "doorss".
    - Zero out a few more keys in memory before freeing them. Fixes
      bug 2384 and part of bug 2385. These key instances found by
      "cypherpunks", based on Andrew Case's report about being able
      to find sensitive data in Tor's memory space if you have enough
      permissions. Bugfix on 0.0.2pre9.

  o Major bugfixes (crashes), also included in 0.2.1.29:
    - Prevent calls to Libevent from inside Libevent log handlers.
      This had potential to cause a nasty set of crashes, especially
      if running Libevent with debug logging enabled, and running
      Tor with a controller watching for low-severity log messages.
      Bugfix on 0.1.0.2-rc. Fixes bug 2190.
    - Add a check for SIZE_T_MAX to tor_realloc() to try to avoid
      underflow errors there too. Fixes the other part of bug 2324.
    - Fix a bug where we would assert if we ever had a
      cached-descriptors.new file (or another file read directly into
      memory) of exactly SIZE_T_CEILING bytes. Fixes bug 2326; bugfix
      on 0.2.1.25. Found by doorss.
    - Fix some potential asserts and parsing issues with grossly
```

malformed router caches. Fixes bug 2352; bugfix on Tor 0.2.1.27.
Found by doorss.

o Minor bugfixes (other), also included in 0.2.1.29:
- Fix a bug with handling misformed replies to reverse DNS lookup requests in DNSPort. Bugfix on Tor 0.2.0.1-alpha. Related to a bug reported by doorss.
- Fix compilation on mingw when a pthreads compatibility library has been installed. (We don't want to use it, so we shouldn't be including pthread.h.) Fixes bug 2313; bugfix on 0.1.0.1-rc.
- Fix a bug where we would declare that we had run out of virtual addresses when the address space was only half-exhausted. Bugfix on 0.1.2.1-alpha.
- Correctly handle the case where AutomapHostsOnResolve is set but no virtual addresses are available. Fixes bug 2328; bugfix on 0.1.2.1-alpha. Bug found by doorss.
- Correctly handle wrapping around when we run out of virtual address space. Found by cypherpunks; bugfix on 0.2.0.5-alpha.

o Minor features, also included in 0.2.1.29:
- Update to the January 1 2011 Maxmind GeoLite Country database.
- Introduce output size checks on all of our decryption functions.

o Build changes, also included in 0.2.1.29:
- Tor does not build packages correctly with Automake 1.6 and earlier; added a check to Makefile.am to make sure that we're building with Automake 1.7 or later.
- The 0.2.1.28 tarball was missing src/common/OpenBSD_malloc_Linux.c because we built it with a too-old version of automake. Thus that release broke ./configure --enable-openbsd-malloc, which is popular among really fast exit relays on Linux.

o Major bugfixes, new in 0.2.2.21-alpha:
- Prevent crash/heap corruption when the cbtnummodes consensus parameter is set to 0 or large values. Fixes bug 2317; bugfix on 0.2.2.14-alpha.

o Major features, new in 0.2.2.21-alpha:
- Introduce minimum/maximum values that clients will believe from the consensus. Now we'll have a better chance to avoid crashes or worse when a consensus param has a weird value.

o Minor features, new in 0.2.2.21-alpha:
- Make sure to disable DirPort if running as a bridge. DirPorts aren't used on bridges, and it makes bridge scanning somewhat easier.
- If writing the state file to disk fails, wait up to an hour before retrying again, rather than trying again each second. Fixes bug 2346; bugfix on Tor 0.1.1.3-alpha.
- Make Libevent log messages get delivered to controllers later, and not from inside the Libevent log handler. This prevents unsafe reentrant Libevent calls while still letting the log messages

```
    get through.
  - Detect platforms that brokenly use a signed size_t, and refuse to
    build there. Found and analyzed by doorss and rransom.
  - Fix a bunch of compile warnings revealed by mingw with gcc 4.5.
    Resolves bug 2314.

o Minor bugfixes, new in 0.2.2.21-alpha:
  - Handle SOCKS messages longer than 128 bytes long correctly, rather
    than waiting forever for them to finish. Fixes bug 2330; bugfix
    on 0.2.0.16-alpha. Found by doorss.
  - Add assertions to check for overflow in arguments to
    base32_encode() and base32_decode(); fix a signed-unsigned
    comparison there too. These bugs are not actually reachable in Tor,
    but it's good to prevent future errors too. Found by doorss.
  - Correctly detect failures to create DNS requests when using Libevent
    versions before v2. (Before Libevent 2, we used our own evdns
    implementation. Its return values for Libevent's evdns_resolve_*()
    functions are not consistent with those from Libevent.) Fixes bug
    2363; bugfix on 0.2.2.6-alpha. Found by "lodger".

o Documentation, new in 0.2.2.21-alpha:
  - Document the default socks host and port (127.0.0.1:9050) for
    tor-resolve.
```

8. On January 20th, the TAILS LiveCD/USB team released an updated version, 0.6.2. It is available at `http://amnesia.boum.org/news/version_0.6.2/`. It contains:

```
* Tor: upgrade to 0.2.1.29 (fixes CVE-2011-0427).
* Software
- Upgrade Linux kernel, dpkg, libc6, NSS, OpenSSL, libxml2 (fixes various
  security issues).
- Upgrade Claws Mail to 3.7.6 (new backport).
- Install Liferea, tcpdump and tcpflow.
* Seahorse: use hkp:// transport as it does not support hkps://.
* FireGPG: use hkps:// to connect to the configured keyserver.
* Build system: take note of the Debian Live tools versions being used
  to make next point-release process faster.
* APT: don't ship package indices.
```

9. On January 25th, we released Tor 0.2.2.22-alpha. It fixes a few more less-critical security issues. The main other change is a slight tweak to Tor's TLS handshake that makes relays and bridges that run this new version reachable from Iran again. We don't expect this tweak will win the arms race long-term, but it will buy us a bit more time until we roll out a better solution. Anybody running a relay or bridge who wants it to work for Iran should upgrade.

```
Changes in version 0.2.2.22-alpha
  o Major bugfixes:
    - Fix a bounds-checking error that could allow an attacker to
      remotely crash a directory authority. Bugfix on 0.2.1.5-alpha.
```

```
    Found by "piebeer".
  - Don't assert when changing from bridge to relay or vice versa
    via the controller. The assert happened because we didn't properly
    initialize our keys in this case. Bugfix on 0.2.2.18-alpha; fixes
    bug 2433. Reported by bastik.

o Minor features:
  - Adjust our TLS Diffie-Hellman parameters to match those used by
    Apache's mod_ssl.
  - Provide a log message stating which geoip file we're parsing
    instead of just stating that we're parsing the geoip file.
    Implements ticket 2432.

o Minor bugfixes:
  - Check for and reject overly long directory certificates and
    directory tokens before they have a chance to hit any assertions.
    Bugfix on 0.2.1.28 / 0.2.2.20-alpha. Found by "doorss".
```

10. Released new VisiTor version 0.0.4 that contains a Python version of the weblog-parsing script contributed by Kiyoto Tamura and two minor fixes.

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

- From the 0.2.2.22-alpha release notes, Adjust our TLS Diffie-Hellman parameters to match those used by Apache's $\mathrm{mod}_{s}sl.Thisisaslighttweaktoo Tor's TLS handshake that makes relays and bridges that r$

- Started discussion of TLS normalization. The developer discussion is at `http://archives.seul.org/or/dev/Jan-2011/msg00029.html`
- Continued discussions of pluggable transports. The draft specification can be found at `https://gitweb.torproject.org/tor.git/blob/HEAD:/doc/spec/proposals/ideas/xxx-pluggable-transport.txt`. The start of the discussion can be found on the or-dev mailing list at `http://archives.seul.org/or/dev/Jan-2011/msg00018.html`.
- Started discussion of Proposal 176 to change the version 3 handshake to not use TLS renegotiation. Proposal 176 is at `https://gitweb.torproject.org/tor.git/blob/HEAD:/doc/spec/proposals/176-revising-handshake.txt`. The developer discussion starts at `http://archives.seul.org/or/dev/Jan-2011/msg00052.html`.
- Andrew and Roger documented the features in the Tor -alpha software that allow users to use a SOCKS proxy as a circumvention method should Tor be blocked in some manner. `https://www.torproject.org/docs/proxychain.html.en`.

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

- Continued discussions of pluggable transports. The draft specification can be found at `https://gitweb.torproject.org/tor.git/blob/HEAD:/doc/spec/proposals/ideas/xxx-pluggable-transport.txt`. The start of the discussion can be found on the or-dev mailing list at `http://archives.seul.org/or/dev/Jan-2011/msg00018.html`.

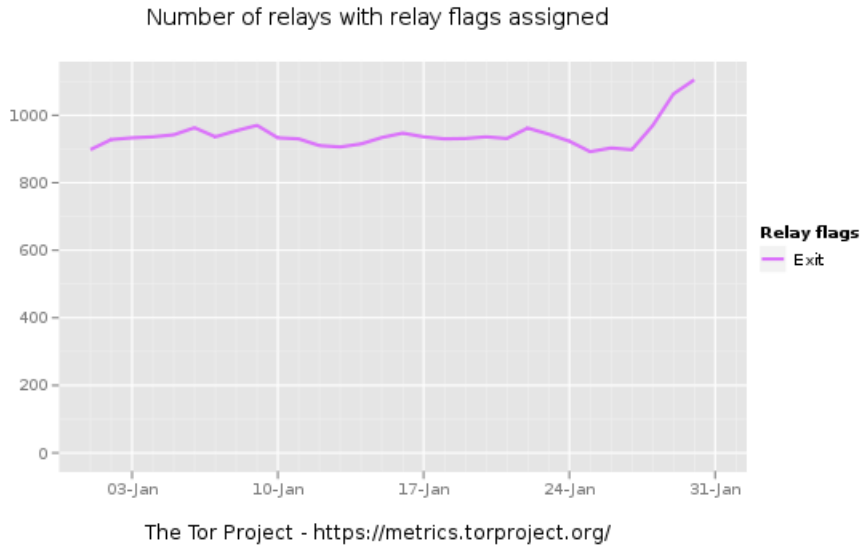
Hide Tor's network signature.

- From the 0.2.2.22-alpha release notes, Adjust our TLS Diffie-Hellman parameters to match those used by Apache's $mod_ssl. This is a slight tweak to Tor's TLS handshake that makes relays and bridges that r$

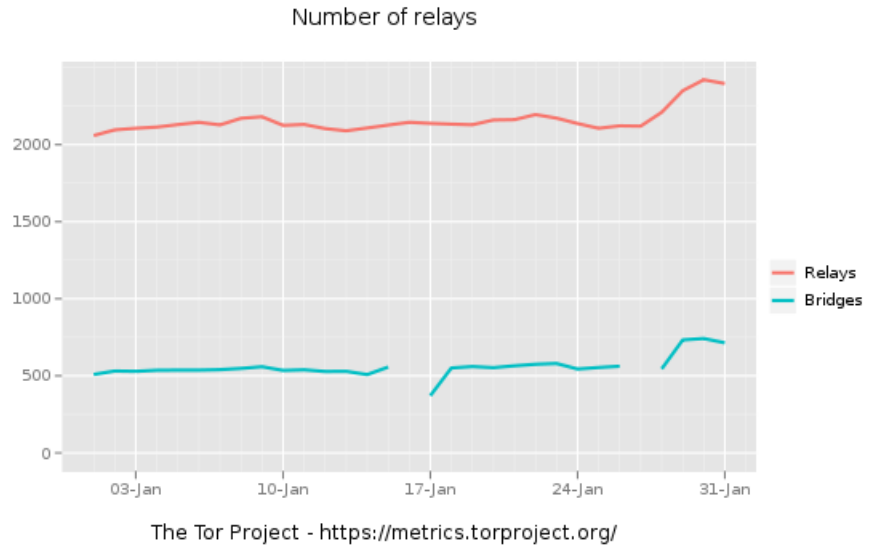
- Started discussion of TLS normalization. The developer discussion is at `http://archives.seul.org/or/dev/Jan-2011/msg00029.html`
- Continued discussions of pluggable transports. The draft specification can be found at `https://gitweb.torproject.org/tor.git/blob/HEAD:/doc/spec/proposals/ideas/xxx-pluggable-transport.txt`. The start of the discussion can be found on the or-dev mailing list at `http://archives.seul.org/or/dev/Jan-2011/msg00018.html`.
- Started discussion of Proposal 176 to change the version 3 handshake to not use TLS renegotiation. Proposal 176 is at `https://gitweb.torproject.org/tor.git/blob/HEAD:/doc/spec/proposals/176-revising-handshake.txt`. The developer discussion starts at `http://archives.seul.org/or/dev/Jan-2011/msg00052.html`.

Grow the Tor network and user base. Outreach.

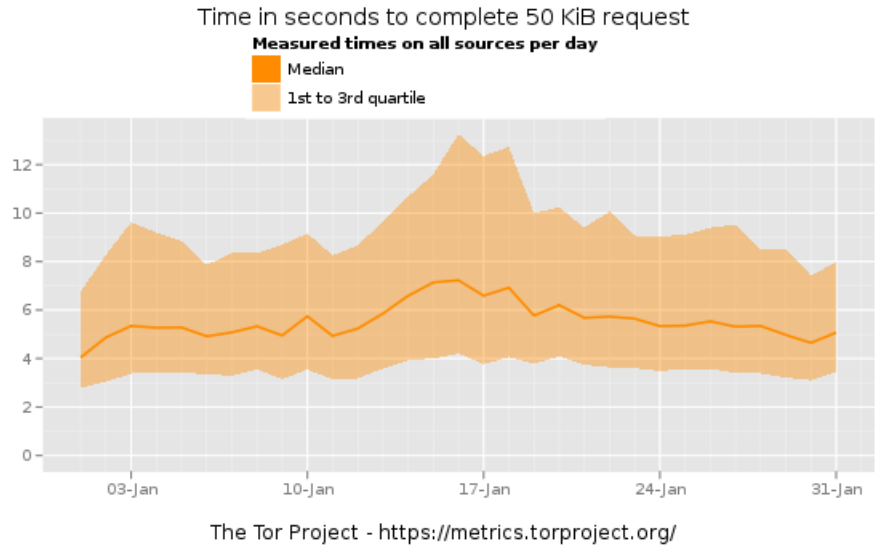
Measures of the Tor Network



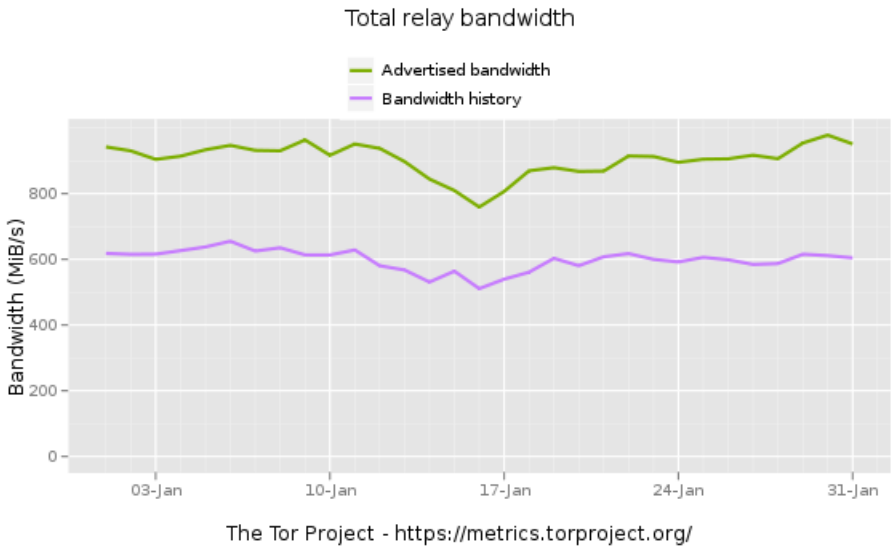
This graph shows the total quantity of exit relays in January 2011. Due to events in Egypt, we had a marked increase in exit relays joining the network.



This graph shows the total quantity of relays and the total quantity of bridges in January 2011. Due to events in Egypt, we had a marked increase in relays and bridges joining the network.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Performance remains relatively steady at 5 seconds.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. The influx of relays at the end of the month creates almost 1GBps (8 Gbps) of bandwidth available.

Outreach and Advocacy

1. Held a successful public hackfest at MIT's Center for Future Civic Media, https://blog.torproject.org/blog/boston-tor-hackers-join-us-saturday-january-15th.

2. Due to the events in Egypt, Tor usage by activists, and human rights organizations requesting our technical help, we were featured in over 30 news stories, interviews, and articles. The master list of the media highlights is at https://www.torproject.org/press/inthemedia.html.en.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

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

- The TAILS live CD/USB project continued to document their security model, designs, and overall software configuration.

Bridge relay and bridge authority work.

- Karsten did some work to publish sanitized bridge pool assignments. We're going to publish the information which distribution pool a bridge is assigned to. The distribution pool defines whether we're giving out bridges via HTTP, via email, or not at all (reserved pool). The plan is to remove all sensitive information from bridge pool assignments before making them available on https://metrics.torproject.org/data.html. The discussion was started on the or-dev list at http://archives.seul.org/or/dev/Jan-2011/msg00033.html.

Scalability, load balancing, directory overhead, efficiency.

- We released an updated version of Tor Weather, https://weather.torproject.org. Tor Weather is a web application used to allow tor relay operators to sign up for notices when their relay is offline, drops below a threshold of bandwidth served, and receive notifications when a new version of tor is released. This version of the web application was written by the Wesleyan University Humantarian Free and Open Source Software (HFOSS) team working on Tor for their summer project, http://hfoss.wesleyan.edu/.

- Karsten started improving metrics-db performance, so that it can scale to five years of data with 10K relays and 5K bridges. This included a few tricks to avoid parsing the same data twice. Also changed the database schema to use SQL arrays to store bandwidth histories, which is apparently a less used part of PostgreSQL, because he found a confirmed bug in PostgreSQL 8.2 (released 2006-12-05).

- Karsten found two major, if not blocking, bugs in Torouter when run on the suggested Buffalo hardware. The Excito hardware does not have these problems. The bug numbers are 2334, https://trac.torproject.org/projects/tor/ticket/2334, and 2376, https://trac.torproject.org/projects/tor/ticket/2376.

- Karsten found and fixed a problematic bridge sanitizer bug that made us keep original IP addresses in reject lines. Updated metrics-db and sanitized all bridge descriptors since May 2008 once again. The latter kept two of our computers busy for 2.5 weeks.
- Karsten started with exporting bridge pool assignments and restarted discussion about preserving hashed IP addresses in bridge descriptors.
- Karsten upgraded Torperfs to output information about which circuits they used for measuring download times. Made data available on metrics website. Added new graphs combining all Torperf sources and showing the fraction of timeouts and failures. Started Torperfs with custom entry guard selection strategies.
- Karsten talked to Björn Scheuermann and Florian Tschorsch about performance improvements in Tor. Working on a patch with them to be included in Tor 0.2.3.x.
- Karsten improved graphs on metrics-web by adding more countries and by allowing users to customize the graph image resolution.

Incentives work.

Nothing to report.

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

- Sebastian and Erinn started to tackle Thandy and Hudson work. They solved the Hudson issue on Windows and made a good deal of progress on getting Thandy set up, understanding the different roles and responsibilities of each in the Thandy system. Installing files by copying into the right place works, but the packaging db that would be required for TBB is not yet working.

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

- Updated translations for the following languages: af ak am arn ast be bg bn bn_IN csb cy dz eo eu fil fur ga gl gun ha he hi ht hu is it km kn kw lb ln lo lt lv mg mi mk ml mn mr ms mt nah nap ne nn nso oc pa pap pms ps sco son sw ta te tg th ti tk uk ur ve wa zh_HK zu.