From: Andrew Lewman, Executive Director
To: the tor community
Date: June 8, 2011

This report documents progress in May 2011.

New releases, new hires, new funding

New Hires

RiseUp Labs have been contracted to enhance and improve the TAILS anonymous operating system, `http://tails.boum.org`.

New Releases

1. On May 5 we released a new highly experimental branch of Tor, 0.2.3.1-alpha. Tor 0.2.3.1-alpha adds some new experimental features, including support for an improved network IO backend, IOCP networking on Windows, microdescriptor caching, "fast-start" support for streams, and automatic home router configuration. There are also numerous internal improvements to try to make the code easier for developers to work with.

   This is the first alpha release in a new series, so expect there to be bugs. Users who would rather test out a more stable branch should stay with 0.2.2.x for now. For now, only the source has been uploaded. Our website scripts don't like for there to be three active branches at one time, so while we're getting that straightened out, you can get the source and the signature at `https://www.torproject.org/dist/tor-0.2.3.1-alpha.tar.gz` and `https://www.torproject.org/dist/tor-0.2.3.1-alpha.tar.gz.asc` respectively. Packages for Debian and expert packages for other platforms should follow. If you don't build from source, and prefer the easier-to-use packages, please stick with 0.2.2.x or 0.2.1.x until we get more bugs shaken out of this one.

```
  o Major features
    - Tor can now optionally build with the "bufferevents" buffered IO
      backend provided by Libevent 2. To use this feature, make sure you
      have the latest possible version of Libevent, and pass the
      --enable-bufferevents flag to configure when building Tor from
      source. This feature will make our networking code more flexible,
      let us stack layers on each other, and let us use more efficient
      zero-copy transports where available.
    - As an experimental feature, Tor can use IOCP for networking on Windows.
      Once this code is tuned and optimized, it promises much better
```

```
    performance than the select-based backend we've used in the past. To
    try this feature, you must build Tor with Libevent 2, configure Tor
    with the "bufferevents" buffered IO backend, and add "DisableIOCP 0" to
    your torrc. There are known bugs here: only try this if you can help
    debug it as it breaks.
  - The EntryNodes option can now include country codes like {de} or IP
    addresses or network masks. Previously we had disallowed these options
    because we didn't have an efficient way to keep the list up to
    date. Fixes bug 1982, but see bug 2798 for an unresolved issue here.
  - Exit nodes now accept and queue data on not-yet-connected streams.
    Previously, the client wasn't allowed to send data until the stream was
    connected, which slowed down all connections. This change will enable
    clients to perform a "fast-start" on streams and send data without
    having to wait for a confirmation that the stream has opened. (Patch
    from Ian Goldberg; implements the server side of Proposal 174.)
  - Tor now has initial support for automatic port mapping on the many
    home routers that support NAT-PMP or UPnP. (Not yet supported on
    Windows). To build the support code, you'll need to have libnatpnp
    library and/or the libminiupnpc library, and you'll need to enable the
    feature specifically by passing "--enable-upnp" and/or
    "--enable-natpnp" to configure. To turn it on, use the new
    PortForwarding option.
  - Caches now download, cache, and serve multiple "flavors" of the
    consensus, including a flavor that describes microdescriptors.
  - Caches now download, cache, and serve microdescriptors -- small
    summaries of router descriptors that are authenticated by all of the
    directory authorities. Once enough caches are running this code,
    clients will be able to save significant amounts of directory bandwidth
    by downloading microdescriptors instead of router descriptors.

o Minor features:
  - Make logging resolution configurable with a new LogGranularity
    option, and change the default from 1 millisecond to 1
    second. Implements enhancement 1668.
  - We log which torrc file we're using on startup. Implements ticket
    2444.
  - Ordinarily, Tor does not count traffic from private addresses (like
    127.0.0.1 or 10.0.0.1) when calculating rate limits or accounting.
    There is now a new option, CountPrivateBandwidth, to disable this
    behavior. Patch from Daniel Cagara.
  - New --enable-static-tor configure option for building Tor as
    statically as possible. Idea, general hackery and thoughts from
    Alexei Czeskis, John Gilmore, Jacob Appelbaum. Implements ticket
    2702.
  - If you set the NumCPUs option to 0, Tor will now try to detect how
```

```
    many CPUs you have. This is the new default behavior.
  - Turn on directory request statistics by default and include them in
    extra-info descriptors. Don't break if we have no GeoIP database.
  - Relays that set "ConnDirectionStatistics 1" write statistics on the
    bidirectional use of connections to disk every 24 hours.
  - Add a GeoIP file digest to the extra-info descriptor. Implements
    enhancement 1883.
  - Add a new 'Heartbeat' log message type to periodically log a message
    describing Tor's status at level Notice. This feature is meant for
    operators who log at notice, and want to make sure that their Tor
    server is still working. Implementation by George Kadianakis.

o Minor bugfixes (on 0.2.2.25-alpha):
  - When loading the microdesc journal, remember its current size.
    In 0.2.2, this helps prevent the microdesc journal from growing
    without limit on authorities (who are the only ones to use it in
    0.2.2). Fixes a part of bug 2230; bugfix on 0.2.2.6-alpha.
    Fix posted by "cypherpunks."
  - The microdesc journal is supposed to get rebuilt only if it is
    at least _half_ the length of the store, not _twice_ the length
    of the store. Bugfix on 0.2.2.6-alpha; fixes part of bug 2230.
  - If as an authority we fail to compute the identity digest of a v3
    legacy keypair, warn, and don't use a buffer-full of junk instead.
    Bugfix on 0.2.1.1-alpha; fixes bug 3106.
  - Authorities now clean their microdesc cache periodically and when
    reading from disk initially, not only when adding new descriptors.
    This prevents a bug where we could lose microdescriptors. Bugfix
    on 0.2.2.6-alpha.

o Minor features (controller)
  - Add a new SIGNAL event to the controller interface so that
    controllers can be notified when Tor handles a signal. Resolves
    issue 1955. Patch by John Brooks.
  - Add a new GETINFO option to get total bytes read and written. Patch
    from pipe, revised by atagar. Resolves ticket 2345.
  - Implement some GETINFO controller fields to provide information about
    the Tor process's pid, euid, username, and resource limits.

o Build changes
  - Our build system requires automake 1.6 or later to create the
    Makefile.in files. Previously, you could have used 1.4.
    This only affects developers and people building Tor from git;
    people who build Tor from the source distribution without changing
    the Makefile.am files should be fine.
  - Our autogen.sh script uses autoreconf to launch autoconf, automake, and
```

```
    so on. This is more robust against some of the failure modes
    associated with running the autotools pieces on their own.

  o Minor packaging issues:
    - On OpenSUSE, create the /var/run/tor directory on startup if it is not
      already created. Patch from Andreas Stieger. Fixes bug 2573.

  o Code simplifications and refactoring:
    - A major revision to our internal node-selecting and listing logic.
      Tor already had at least two major ways to look at the question of
      "which Tor servers do we know about": a list of router descriptors,
      and a list of entries in the current consensus. With
      microdescriptors, we're adding a third. Having so many systems
      without an abstraction layer over them was hurting the codebase.
      Now, we have a new "node_t" abstraction that presents a consistent
      interface to a client's view of a Tor node, and holds (nearly) all
      of the mutable state formerly in routerinfo_t and routerstatus_t.
    - The helper programs tor-gencert, tor-resolve, and tor-checkkey
      no longer link against Libevent: they never used it, but
      our library structure used to force them to link it.

  o Removed features:
    - Remove some old code to work around even older versions of Tor that
      used forked processes to handle DNS requests. Such versions of Tor
      are no longer in use as servers.

  o Documentation fixes:
    - Correct a broken faq link in the INSTALL file. Fixes bug 2307.
    - Add missing documentation for the authority-related torrc options
      RephistTrackTime, BridgePassword, and V3AuthUseLegacyKey. Resolves
      issue 2379.
```

2. On May 9, an updated Orbot, Tor for Android, was released for testing. Based on feedback from our core test group in the Guardian Project, it seems like we have a solid new version of Orbot that includes Tor 0.2.2.25, as well as improved handling of transparent proxying. This new build also includes our own version of iptables, and proactively checks if the device has netfilter/owner support in the kernel. This should lead to overall less support requests from confused users who have "root" but still can't transproxy.

   We have a few UI tweaks to make, and need to make sure all of our translations are up-to-date, but otherwise, the app feels very ready to go.

   I invite any of you with a few spare cycles and an Android device handy to try it out if you haven't already. As this is a dev build, it is not signed by the official Tor distro key, so you will have to uninstall any existing Orbot official release. The final app we release to the market will be signed by the Tor key, and users will get an automatic "updates available" message from the Android market.

The software is available at `https://guardianproject.info/downloads/0.2.2.25-orbot-alpha-1.0.5.20110508a-dev.apk` with the (.asc - signed by nathan@guardianproject.info 0xB374CBD2)

3. On May 6, we released an experimental Vidalia branch, 0.3.0. We are going to be doing a series of alpha releases in parallel with the stable 0.2.x to have a wider audience for some changes that are kind of "core" for Vidalia, or they are really big to put them on the stable before testing them for a while.

   We need more eyes, but I want to be clear about the "alpha" part in the version. The bundles that were just announced they also have an alpha version of Tor, the latest libevent, the latest openssl, and so on, not just this Vidalia release. So be aware of this while running them.

```
0.3.0   06-May-2011
  o Vidalia has got a new GUI. Instead of separate dialogs, each
    functionality is organized in tabs arranged in a common main window.
    This new tab organization will give Vidalia a generic way of
    organizing the GUI plug-ins that will be available in later
    releases.  Resolves bug 2939.
  o When a Tor instance is already running and Vidalia doesn't know the
    control password, don't ask for the it but rather explain the
    situation and display the few possible choices the user has.
    Resolves bug 2132.
  o Add an option for setting up a non-exit relay to the Sharing
    configuration panel. This is meant to clarify what an exit policy
    and an exit relay are.  Resolves bug 2644.
  o Add a way to reload Tor's configuration without having to stop it.
    Tor can reload its configuration while it is running, Vidalia now
    provides a menu option for that, so, for example, relay operators
    won't be affected by the fact that their relay was down for a while.
    Resolves bug 2724.
  o Reintegrate Breakpad, and make available in other platforms other
    than Windows. Resolves bug 2105.
  o Fix bandwidth assigned to relays on the Network Map. A lot of relays
    are displaying an erroneous bandwidth and since they are ordered by
    that value in the Network Map, it leads to confusion. Vidalia now
    specifies the bandwidth as the minimum of the three possible values
    (burst, average and observed). Fixes bug 2744.
  o Minor change to the checkbox for starting Tor when Vidalia starts.
    It was suggested that the way the phrasing was done was missleading.
    Resolves bug 2806.
  o Add a way to bootstrap Tor's torrc file (copy the torrc to a given
    directory before Vidalia starts) so that packages such as
    Bridge-by-default portable bundles for OSX don't violate the
    directory structure of the operative system. Fixes bug 2821.
  o Add the proper CA Certificates so that the "Find Bridges" button
    works again. Fixes bug 2835.
  o Update the useful links help page. Fixes bug 2809.
```

4. On May 11, we released some experimental Vidalia bundles containing Vidalia 0.3.0-alpha and Tor 0.2.3.1-alpha.

   ```
   OS X, 10.5 and 10.6 only (untested on 10.5, please let me know if it works):
   https://archive.torproject.org/tor-package-archive/technology-preview/vidalia-bundle-0.2.3
   https://archive.torproject.org/tor-package-archive/technology-preview/vidalia-bundle-0.2.3

   Windows XP through Win7 (might work on Win2k, can someone test and confirm?):
   https://archive.torproject.org/tor-package-archive/technology-preview/vidalia-bundle-0.2.3
   https://archive.torproject.org/tor-package-archive/technology-preview/vidalia-bundle-0.2.3
   ```

5. On May 17, we released Tor 0.2.2.26-beta. Tor 0.2.2.26-beta fixes a variety of potential privacy problems. It also introduces a new "socksport auto" approach that should make it easier to run multiple Tors on the same system, and does a lot of cleanup to get us closer to a release candidate.

   ```
   o Security/privacy fixes:
     - Replace all potentially sensitive memory comparison operations
       with versions whose runtime does not depend on the data being
       compared. This will help resist a class of attacks where an
       adversary can use variations in timing information to learn
       sensitive data. Fix for one case of bug 3122. (Safe memcmp
       implementation by Robert Ransom based partially on code by DJB.)
     - When receiving a hidden service descriptor, check that it is for
       the hidden service we wanted. Previously, Tor would store any
       hidden service descriptors that a directory gave it, whether it
       wanted them or not. This wouldn't have let an attacker impersonate
       a hidden service, but it did let directories pre-seed a client
       with descriptors that it didn't want. Bugfix on 0.0.6.
     - On SIGHUP, do not clear out all TrackHostExits mappings, client
       DNS cache entries, and virtual address mappings: that's what
       NEWNYM is for. Fixes bug 1345; bugfix on 0.1.0.1-rc.

   o Major features:
     - The options SocksPort, ControlPort, and so on now all accept a
       value "auto" that opens a socket on an OS-selected port. A
       new ControlPortWriteToFile option tells Tor to write its
       actual control port or ports to a chosen file. If the option
       ControlPortFileGroupReadable is set, the file is created as
       group-readable. Now users can run two Tor clients on the same
       system without needing to manually mess with parameters. Resolves
       part of ticket 3076.
     - Set SO_REUSEADDR on all sockets, not just listeners. This should
   ```

help busy exit nodes avoid running out of useable ports just because all the ports have been used in the near past. Resolves issue 2850.

o Minor features:
- New "GETINFO net/listeners/(type)" controller command to return a list of addresses and ports that are bound for listeners for a given connection type. This is useful when the user has configured "SocksPort auto" and the controller needs to know which port got chosen. Resolves another part of ticket 3076.
- Add a new ControlSocketsGroupWritable configuration option: when it is turned on, ControlSockets are group-writeable by the default group of the current user. Patch by JÃ©rÃ©my Bobbio; implements ticket 2972.
- Tor now refuses to create a ControlSocket in a directory that is world-readable (or group-readable if ControlSocketsGroupWritable is 0). This is necessary because some operating systems do not enforce permissions on an AF_UNIX sockets. Permissions on the directory holding the socket, however, seems to work everywhere.
- Rate-limit a warning about failures to download v2 networkstatus documents. Resolves part of bug 1352.
- Backport code from 0.2.3.x that allows directory authorities to clean their microdescriptor caches. Needed to resolve bug 2230.
- When an HTTPS proxy reports "403 Forbidden", we now explain what it means rather than calling it an unexpected status code. Closes bug 2503. Patch from Michael Yakubovich.
- Update to the May 1 2011 Maxmind GeoLite Country database.

o Minor bugfixes:
- Authorities now clean their microdesc cache periodically and when reading from disk initially, not only when adding new descriptors. This prevents a bug where we could lose microdescriptors. Bugfix on 0.2.2.6-alpha. 2230
- Do not crash when our configuration file becomes unreadable, for example due to a permissions change, between when we start up and when a controller calls SAVECONF. Fixes bug 3135; bugfix on 0.0.9pre6.
- Avoid a bug that would keep us from replacing a microdescriptor cache on Windows. (We would try to replace the file while still holding it open. That's fine on Unix, but Windows doesn't let us do that.) Bugfix on 0.2.2.6-alpha; bug found by wanoskarnet.
- Add missing explanations for the authority-related torrc options RephistTrackTime, BridgePassword, and V3AuthUseLegacyKey in the man page. Resolves issue 2379.
- As an authority, do not upload our own vote or signature set to

```
    ourself. It would tell us nothing new, and as of 0.2.2.24-alpha,
    it would get flagged as a duplicate. Resolves bug 3026.
  - Accept hidden service descriptors if we think we might be a hidden
    service directory, regardless of what our consensus says. This
    helps robustness, since clients and hidden services can sometimes
    have a more up-to-date view of the network consensus than we do,
    and if they think that the directory authorities list us a HSDir,
    we might actually be one. Related to bug 2732; bugfix on
    0.2.0.10-alpha.
  - When a controller changes TrackHostExits, remove mappings for
    hosts that should no longer have their exits tracked. Bugfix on
    0.1.0.1-rc.
  - When a controller changes VirtualAddrNetwork, remove any mappings
    for hosts that were automapped to the old network. Bugfix on
    0.1.1.19-rc.
  - When a controller changes one of the AutomapHosts* options, remove
    any mappings for hosts that should no longer be automapped. Bugfix
    on 0.2.0.1-alpha.
  - Do not reset the bridge descriptor download status every time we
    re-parse our configuration or get a configuration change. Fixes
    bug 3019; bugfix on 0.2.0.3-alpha.

o Minor bugfixes (code cleanup):
  - When loading the microdesc journal, remember its current size.
    In 0.2.2, this helps prevent the microdesc journal from growing
    without limit on authorities (who are the only ones to use it in
    0.2.2). Fixes a part of bug 2230; bugfix on 0.2.2.6-alpha.
    Fix posted by "cypherpunks."
  - The microdesc journal is supposed to get rebuilt only if it is
    at least _half_ the length of the store, not _twice_ the length
    of the store. Bugfix on 0.2.2.6-alpha; fixes part of bug 2230.
  - Fix a potential null-pointer dereference while computing a
    consensus. Bugfix on tor-0.2.0.3-alpha, found with the help of
    clang's analyzer.
  - Avoid a possible null-pointer dereference when rebuilding the mdesc
    cache without actually having any descriptors to cache. Bugfix on
    0.2.2.6-alpha. Issue discovered using clang's static analyzer.
  - If we fail to compute the identity digest of a v3 legacy keypair,
    warn, and don't use a buffer-full of junk instead. Bugfix on
    0.2.1.1-alpha; fixes bug 3106.
  - Resolve an untriggerable issue in smartlist_string_num_isin(),
    where if the function had ever in the future been used to check
    for the presence of a too-large number, it would have given an
    incorrect result. (Fortunately, we only used it for 16-bit
    values.) Fixes bug 3175; bugfix on 0.1.0.1-rc.
```

```
    - Require that introduction point keys and onion handshake keys
      have a public exponent of 65537. Starts to fix bug 3207; bugfix
      on 0.2.0.10-alpha.

  o Removed features:
    - Caches no longer download and serve v2 networkstatus documents
      unless FetchV2Networkstatus flag is set: these documents haven't
      haven't been used by clients or relays since 0.2.0.x. Resolves
      bug 3022.
```

6. On May 18, we released Tor 0.2.2.27-beta. Tor 0.2.2.27-beta fixes a bridge-related stability bug in the previous release, and also adds a few more general bugfixes.

```
  o Major bugfixes:
    - Fix a crash bug when changing bridges in a running Tor process.
      Fixes bug 3213; bugfix on 0.2.2.26-beta.
    - When the controller configures a new bridge, don't wait 10 to 60
      seconds before trying to fetch its descriptor. Bugfix on
      0.2.0.3-alpha; fixes bug 3198 (suggested by 2355).

  o Minor bugfixes:
    - Require that onion keys have exponent 65537 in microdescriptors too.
      Fixes more of bug 3207; bugfix on 0.2.2.26-beta.
    - Tor used to limit HttpProxyAuthenticator values to 48 characters.
      Changed the limit to 512 characters by removing base64 newlines.
      Fixes bug 2752. Fix by Michael Yakubovich.
    - When a client starts or stops using bridges, never use a circuit
      that was built before the configuration change. This behavior could
      put at risk a user who uses bridges to ensure that her traffic
      only goes to the chosen addresses. Bugfix on 0.2.0.3-alpha; fixes
      bug 3200.
```

7. On May 23, we released updated packages for Linux, OS X, and Microsoft Windows. All of the alpha Tor Browser Bundles have been updated to the latest Tor 0.2.2.27-beta.

```
Firefox 3.6 Tor Browser Bundles
Linux bundles
1.1.9: Released 2011-05-19
Update Tor to 0.2.2.27-beta
Update NoScript to 2.1.0.5
Update BetterPrivacy to 1.50
Update HTTPS Everywhere to 0.9.9.development.5

OS X bundle
1.0.17: Released 2011-05-19
Update Tor to 0.2.2.27-beta
```

```
Update NoScript to 2.1.0.5
Update HTTPS-Everywhere to 0.9.9.development.5
Update BetterPrivacy to 1.50

Firefox 4 Tor Browser Bundles
Tor Browser Bundle (2.2.27-1)
Update Tor to 0.2.2.27-beta
Update HTTPS Everywhere to 0.9.9.development.5
Update NoScript to 2.1.0.5
```

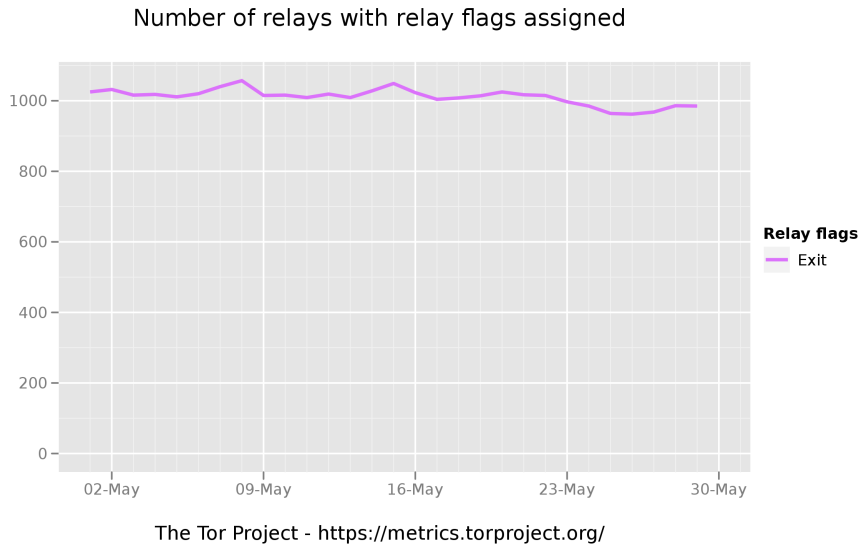
Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

- Nick spent a while chasing security issues, particularly bug 3122, `https://trac.torproject.org/projects/tor/ticket/3122`. This should make Tor more resilient to a class of timing attack. In practice, we still doubt whether there could be exploitable bugs here: we believe that getting good enough answers to mount a good timing attack would require that Tor be a lot less noisy in its current timing behavior. Nonetheless, we could be quite wrong.
- Nick and George started writing out the threat models and specification for obfsproxy, `https://gitweb.torproject.org/obfsproxy.git/tree/HEAD:/doc`.

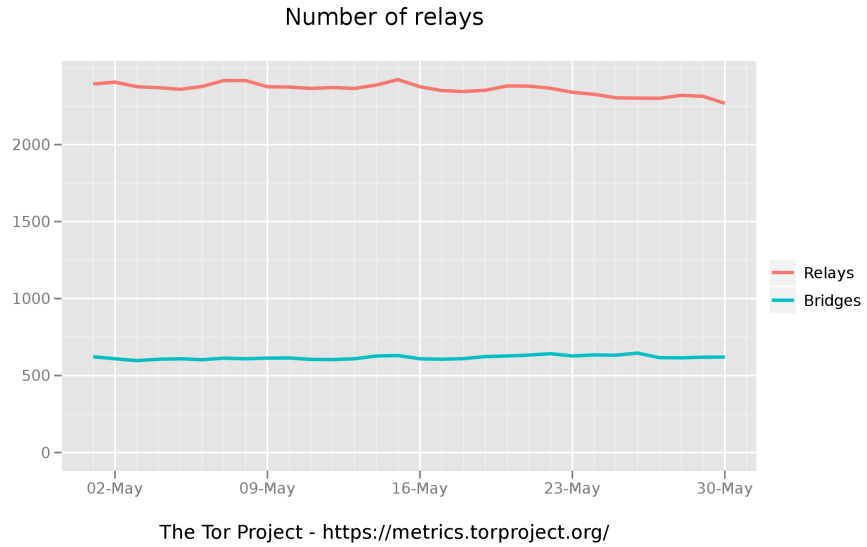
Hide Tor's network signature.

Grow the Tor network and user base. Outreach.

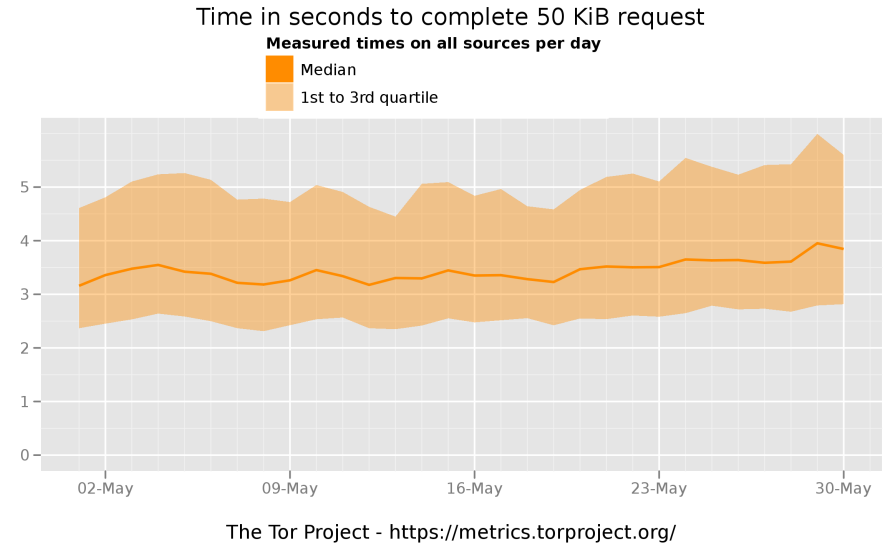
Measures of the Tor Network



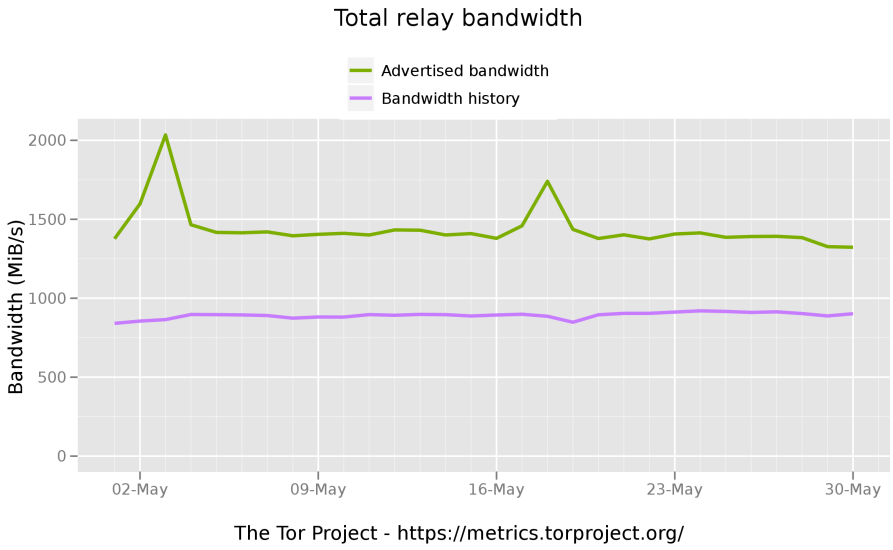
This graph shows the total quantity of exit relays in May 2011. We seem to have kept most of our relays since the bump due to Tunisia and Egypt.



This graph shows the total quantity of relays and the total quantity of bridges in May 2011. We seem to have kept most of our relays since the bump due to Tunisia and Egypt.



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



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

Outreach and Advocacy

1. Andrew spoke at World Press Freedom Day, `http://www.wpfd2011.org/`. His presentation is available here `https://svn.torproject.org/svn/projects/presentations/2011-WorldPressFreedomDa`

pdf.

2. Jacob attended Google I/O, http://www.google.com/events/io/2011/.

3. Andrew traveled to Iceland to meet with the International Modern Media Institute, National Police of Iceland, and Hakkavélin. His trip report was published as a blog post, https://blog.torproject.org/blog/visit-iceland.

4. Andrew, Runa, Sebastian, George, and Linus worked with IIS.se to hold a successful hackfest in Stockholm, https://blog.torproject.org/blog/2011-stockholm-hackfest-thanks. IIS further published the event in Swedish at https://www.iis.se/blogg/hackare-intar-se and their follow-up, https://www.iis.se/internet-for-alla/reportage/teknikreportage/hackare-intog-se.

5. Andrew and Runa met with University College of London Information Security Research Group, http://sec.cs.ucl.ac.uk/. Andrew presented about usability, humans, and Tor with this presentation, https://svn.torproject.org/svn/projects/presentations/2011-anonymity-us pdf.

6. Andrew and Dr. Angela Sasse from UCL were interviewed by the BBC Click program about why Internet Anonymity is important and valuable in a modern, networked society. http://news.bbc.co.uk/2/hi/programmes/click_online/default.stm

7. Mike spoke at W3C Identity, http://www.w3.org/2011/identity-ws/Overview.html and presented this paper, https://svn.torproject.org/svn/projects/articles/browser-privacy/.

8. Mike attended Web 2.0 Security and Privacy, http://w2spconf.com/2011/.

9. Roger attended the IEEE Symposium on Security and Privacy, http://www.ieee-security.org/TC/SP2011/index.html.

10. Runa attended the Youth Congress on Digital Citizenship in London, http://www.cybersummit2011.com/.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

Bridge relay and bridge authority work.

- Runa continued to work on the Excito web interface, and sent Excito the text for the help page. The current iteration of the interface looks like this http://forum.excito.net/download/file.php?id=91.

- Runa went to Malmö, Sweden to meet and work with developers at Excito. The trip was successful in getting the Tor parts of the web interface integrated into the rest of the B3 management interface.

- Runa received a DreamPlug from GlobalScale Technologies. The idea was that this plug could be used for the Torouter project. It may not be as user friendly as first thought. See "The Torouter and the DreamPlug" on tor-dev for more info., https://lists.torproject.org/pipermail/tor-dev/2011-May/002686.html.

- Roger put up a 'need more bridge addresses' blog post, and managed some of the comments: https://blog.torproject.org/blog/strategies-getting-more-bridge-addresses

Scalability, load balancing, directory overhead, efficiency.

- Nick had some pretty good discussions about possibilities for faster ECC-based handshakes on or-dev, turning Goldberg Stebila and Ustaoglu's design into a spec proposal idea draft. We'd like to see about getting this into a release; it seems like it would make circuit crypto much faster.

- From the 0.2.3.0 release notes: As an experimental feature, Tor can use IOCP for networking on Windows. Once this code is tuned and optimized, it promises much better performance than the select-based backend we've used in the past. To try this feature, you must build Tor with Libevent 2, configure Tor with the "bufferevents" buffered IO backend, and add "DisableIOCP 0" to your torrc. There are known bugs here: only try this if you can help debug it as it breaks.

- From the 0.2.3.0 release notes: Exit nodes now accept and queue data on not-yet-connected streams.Previously, the client wasn't allowed to send data until the stream was connected, which slowed down all connections. This change will enable clients to perform a "fast-start" on streams and send data without having to wait for a confirmation that the stream has opened. (Patch from Ian Goldberg; implements the server side of Proposal 174.)

- From the 0.2.3.0 release notes: Tor now has initial support for automatic port mapping on the many home routers that support NAT-PMP or UPnP. (Not yet supported on Windows). To build the support code, you'll need to have libnatpnp library and/or the libminiupnpc library, and you'll need to enable the feature specifically by passing "–enable-upnp" and/or "–enable-natpnp" to configure. To turn it on, use the new PortForwarding option.

- Steven is writing a comparison of datagram protocols for Tor. Current draft of the comparison is available at https://gitweb.torproject.org/sjm217/torspec.git/tree/refs/heads/datagram_comparison:/proposals/ideas/xxx-datagram-comparison. Updated progress at https://trac.torproject.org/projects/tor/ticket/1855.

- Tor 0.2.3.1-alpha was released which includes full microdescriptor client and relay support. Progress is being tracked at https://trac.torproject.org/projects/tor/ticket/1748. Specific changelog entries available at https://lists.torproject.org/pipermail/tor-talk/2011-May/020313.html. Relevant entries are:

```
  - Caches now download, cache, and serve microdescriptors -- small
    summaries of router descriptors that are authenticated by all of the
    directory authorities. Once enough caches are running this code,
    clients will be able to save significant amounts of directory bandwidth
    by downloading microdescriptors instead of router descriptors.

  o Minor bugfixes (on 0.2.2.25-alpha):
  - When loading the microdesc journal, remember its current size.
```

```
  In 0.2.2, this helps prevent the microdesc journal from growing
  without limit on authorities (who are the only ones to use it in
  0.2.2). Fixes a part of bug 2230; bugfix on 0.2.2.6-alpha.
  Fix posted by "cypherpunks."
- The microdesc journal is supposed to get rebuilt only if it is
  at least _half_ the length of the store, not _twice_ the length
  of the store. Bugfix on 0.2.2.6-alpha; fixes part of bug 2230.
- If as an authority we fail to compute the identity digest of a v3
  legacy keypair, warn, and don't use a buffer-full of junk instead.
  Bugfix on 0.2.1.1-alpha; fixes bug 3106.
- Authorities now clean their microdesc cache periodically and when
  reading from disk initially, not only when adding new descriptors.
  This prevents a bug where we could lose microdescriptors. Bugfix
  on 0.2.2.6-alpha.
```

- Bandwidth authority improvements.
  - ticket 2391 'upgrade to use new sqlalchemy and elixir:' completed. `https://trac.torproject.org/projects/tor/ticket/2391`
  - ticket 2392 'support postgres/mysql backend': completed, but fix for 2947 conflicts. Seeking resolution. `https://trac.torproject.org/projects/tor/ticket/2392`
  - ticket 2550 'bwauth should reschedule quicker bandwidth test when bandwidthrate changes?' - part a. implemented. Waiting on feedback from Mike to determine if we are proceeding with parts b. and c. `https://trac.torproject.org/projects/tor/ticket/2550`
  - ticket 2568 'IOError: file name too long' - completed. implemented a fix, but unable to reproduce the bug – possibly an OS bug. (see ticket for details: `https://trac.torproject.org/projects/tor/ticket/2568`)
  - ticket 2947 - 'bwscanner does not clear stream data between slices' Fixed but hasn't had the impact that Mike I were hoping for. 2 weeks of testing show improvement in memory usage but usage continues to grow. The sqlite database is only about 5MB in size, so it looks like the memory leak is elsewhere. `https://trac.torproject.org/projects/tor/ticket/2947`

Incentives work.

Nothing to report.

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

To great effect the world over, Mike blogged about ending torbutton as a separate entity and forking Firefox. `https://blog.torproject.org/blog/toggle-or-not-toggle-end-torbutton`. This story was reported upon by at least 30 different media outlets around the world.

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

- updated the translation template for Orbot and pushed/pulled new translations: `https://trac.torproject.org/projects/tor/ticket/3104`.
- pulled and validated translations for Vidalia, Vidalia Installer, the Vidalia help files and the website.
- created a Vidalia-alpha resource on Transifex and added the translations we have right now (they are currently the same as for the stable version of Vidalia): `https://trac.torproject.org/projects/tor/ticket/3092`.
- The German translation of overview.html contained wml code. Fixed it by closing a couple of tags: `https://trac.torproject.org/projects/tor/ticket/3102`.
- The Russian translation of overview.html didn't include the sidenav. Fixed by removing extra space before one of the include lines: `https://trac.torproject.org/projects/tor/ticket/3120`.