From: Andrew Lewman, Executive Director
To: the tor community
Date: May 7, 2011

This report documents progress in April 2011.

New releases, new hires, new funding

New Releases

1. On April 8, we released Tor 0.2.2.24-alpha. Tor 0.2.2.24-alpha fixes a variety of bugs, including a big bug that prevented Tor clients from effectively using "multihomed" bridges, that is, bridges that listen on multiple ports or IP addresses so users can continue to use some of their addresses even if others get blocked.

```
o Major bugfixes:
  - Fix a bug where bridge users who configure the non-canonical
    address of a bridge automatically switch to its canonical
    address. If a bridge listens at more than one address, it should be
    able to advertise those addresses independently and any non-blocked
    addresses should continue to work. Bugfix on Tor 0.2.0.x. Fixes
    bug 2510.
  - If you configured Tor to use bridge A, and then quit and
    configured Tor to use bridge B instead, it would happily continue
    to use bridge A if it's still reachable. While this behavior is
    a feature if your goal is connectivity, in some scenarios it's a
    dangerous bug. Bugfix on Tor 0.2.0.1-alpha; fixes bug 2511.
  - Directory authorities now use data collected from their own
    uptime observations when choosing whether to assign the HSDir flag
    to relays, instead of trusting the uptime value the relay reports in
    its descriptor. This change helps prevent an attack where a small
    set of nodes with frequently-changing identity keys can blackhole
    a hidden service. (Only authorities need upgrade; others will be
    fine once they do.) Bugfix on 0.2.0.10-alpha; fixes bug 2709.

o Minor bugfixes:
  - When we restart our relay, we might get a successful connection
    from the outside before we've started our reachability tests,
    triggering a warning: "ORPort found reachable, but I have no
    routerinfo yet. Failing to inform controller of success." This
```

bug was harmless unless Tor is running under a controller
like Vidalia, in which case the controller would never get a
REACHABILITY_SUCCEEDED status event. Bugfix on 0.1.2.6-alpha;
fixes bug 1172.
- Make directory authorities more accurate at recording when
relays that have failed several reachability tests became
unreachable, so we can provide more accuracy at assigning Stable,
Guard, HSDir, etc flags. Bugfix on 0.2.0.6-alpha. Resolves bug 2716.
- Fix an issue that prevented static linking of libevent on
some platforms (notably Linux). Fixes bug 2698; bugfix on
versions 0.2.1.23/0.2.2.8-alpha (the versions introducing
the --with-static-libevent configure option).
- We now ask the other side of a stream (the client or the exit)
for more data on that stream when the amount of queued data on
that stream dips low enough. Previously, we wouldn't ask the
other side for more data until either it sent us more data (which
it wasn't supposed to do if it had exhausted its window!) or we
had completely flushed all our queued data. This flow control fix
should improve throughput. Fixes bug 2756; bugfix on the earliest
released versions of Tor (svn commit r152).
- Avoid a double-mark-for-free warning when failing to attach a
transparent proxy connection. (We thought we had fixed this in
0.2.2.23-alpha, but it turns out our fix was checking the wrong
connection.) Fixes bug 2757; bugfix on 0.1.2.1-alpha (the original
bug) and 0.2.2.23-alpha (the incorrect fix).
- When warning about missing zlib development packages during compile,
give the correct package names. Bugfix on 0.2.0.1-alpha.

o Minor features:
- Directory authorities now log the source of a rejected POSTed v3
networkstatus vote.
- Make compilation with clang possible when using
--enable-gcc-warnings by removing two warning options that clang
hasn't implemented yet and by fixing a few warnings. Implements
ticket 2696.
- When expiring circuits, use microsecond timers rather than
one-second timers. This can avoid an unpleasant situation where a
circuit is launched near the end of one second and expired right
near the beginning of the next, and prevent fluctuations in circuit
timeout values.
- Use computed circuit-build timeouts to decide when to launch
parallel introduction circuits for hidden services. (Previously,
we would retry after 15 seconds.)
- Update to the April 1 2011 Maxmind GeoLite Country database.

o Packaging fixes:
  - Create the /var/run/tor directory on startup on OpenSUSE if it is not already created. Patch from Andreas Stieger. Fixes bug 2573.

o Documentation changes:
  - Modernize the doxygen configuration file slightly. Fixes bug 2707.
  - Resolve all doxygen warnings except those for missing documentation. Fixes bug 2705.
  - Add doxygen documentation for more functions, fields, and types.

2. On April 29, we released Tor 0.2.25-alpha. Tor 0.2.2.25-alpha fixes many bugs: hidden service clients are more robust, routers no longer overreport their bandwidth, Win7 should crash a little less, and NEWNYM (as used by Vidalia's "new identity" button) now prevents hidden service-related activity from being linkable. It provides more information to Vidalia so you can see if your bridge is working. Also, 0.2.2.25-alpha revamps the Entry/Exit/ExcludeNodes and StrictNodes configuration options to make them more reliable, more understandable, and more regularly applied. If you use those options, please see the revised documentation for them in the manual page.

   o Major bugfixes:
     - Relays were publishing grossly inflated bandwidth values because they were writing their state files wrong--now they write the correct value. Also, resume reading bandwidth history from the state file correctly. Fixes bug 2704; bugfix on 0.2.2.23-alpha.
     - Improve hidden service robustness: When we find that we have extended a hidden service's introduction circuit to a relay not listed as an introduction point in the HS descriptor we currently have, retry with an introduction point from the current descriptor. Previously we would just give up. Fixes bugs 1024 and 1930; bugfix on 0.2.0.10-alpha.
     - Clients now stop trying to use an exit node associated with a given destination by TrackHostExits if they fail to reach that exit node. Fixes bug 2999. Bugfix on 0.2.0.20-rc.
     - Fix crash bug on platforms where gmtime and localtime can return NULL. Windows 7 users were running into this one. Fixes part of bug 2077. Bugfix on all versions of Tor. Found by boboper.

   o Security and stability fixes:
     - Don't double-free a parsable, but invalid, microdescriptor, even if it is followed in the blob we're parsing by an unparsable microdescriptor. Fixes an issue reported in a comment on bug 2954. Bugfix on 0.2.2.6-alpha; fix by "cypherpunks".
     - If the Nickname configuration option isn't given, Tor would pick a nickname based on the local hostname as the nickname for a relay. Because nicknames are not very important in today's Tor and the "Unnamed" nickname has been implemented, this is now problematic

```
    behavior: It leaks information about the hostname without being
    useful at all. Fixes bug 2979; bugfix on 0.1.2.2-alpha, which
    introduced the Unnamed nickname. Reported by tagnaq.
  - Fix an uncommon assertion failure when running with DNSPort under
    heavy load. Fixes bug 2933; bugfix on 0.2.0.1-alpha.
  - Avoid linkability based on cached hidden service descriptors: forget
    all hidden service descriptors cached as a client when processing a
    SIGNAL NEWNYM command. Fixes bug 3000; bugfix on 0.0.6.

o Major features:
  - Export GeoIP information on bridge usage to controllers even if we
    have not yet been running for 24 hours. Now Vidalia bridge operators
    can get more accurate and immediate feedback about their
    contributions to the network.

o Major features and bugfixes (node selection):
  - Revise and reconcile the meaning of the ExitNodes, EntryNodes,
    ExcludeEntryNodes, ExcludeExitNodes, ExcludeNodes, and StrictNodes
    options. Previously, we had been ambiguous in describing what
    counted as an "exit" node, and what operations exactly "StrictNodes
    0" would permit. This created confusion when people saw nodes built
    through unexpected circuits, and made it hard to tell real bugs from
    surprises. Now the intended behavior is:
      . "Exit", in the context of ExitNodes and ExcludeExitNodes, means
        a node that delivers user traffic outside the Tor network.
      . "Entry", in the context of EntryNodes, means a node used as the
        first hop of a multihop circuit. It doesn't include direct
        connections to directory servers.
      . "ExcludeNodes" applies to all nodes.
      . "StrictNodes" changes the behavior of ExcludeNodes only. When
        StrictNodes is set, Tor should avoid all nodes listed in
        ExcludeNodes, even when it will make user requests fail. When
        StrictNodes is *not* set, then Tor should follow ExcludeNodes
        whenever it can, except when it must use an excluded node to
        perform self-tests, connect to a hidden service, provide a
        hidden service, fulfill a .exit request, upload directory
        information, or fetch directory information.
    Collectively, the changes to implement the behavior fix bug 1090.
  - ExcludeNodes now takes precedence over EntryNodes and ExitNodes: if
    a node is listed in both, it's treated as excluded.
  - ExcludeNodes now applies to directory nodes -- as a preference if
    StrictNodes is 0, or an absolute requirement if StrictNodes is 1.
    Don't exclude all the directory authorities and set StrictNodes to 1
    unless you really want your Tor to break.
  - ExcludeNodes and ExcludeExitNodes now override exit enclaving.
```

- ExcludeExitNodes now overrides .exit requests.
- We don't use bridges listed in ExcludeNodes.
- When StrictNodes is 1:
  . We now apply ExcludeNodes to hidden service introduction points and to rendezvous points selected by hidden service users. This can make your hidden service less reliable: use it with caution!
  . If we have used ExcludeNodes on ourself, do not try relay reachability self-tests.
  . If we have excluded all the directory authorities, we will not even try to upload our descriptor if we're a relay.
  . Do not honor .exit requests to an excluded node.
- Remove a misfeature that caused us to ignore the Fast/Stable flags when ExitNodes is set. Bugfix on 0.2.2.7-alpha.
- When the set of permitted nodes changes, we now remove any mappings introduced via TrackExitHosts to now-excluded nodes. Bugfix on 0.1.0.1-rc.
- We never cannibalize a circuit that had excluded nodes on it, even if StrictNodes is 0. Bugfix on 0.1.0.1-rc.
- Revert a change where we would be laxer about attaching streams to circuits than when building the circuits. This was meant to prevent a set of bugs where streams were never attachable, but our improved code here should make this unnecessary. Bugfix on 0.2.2.7-alpha.
- Keep track of how many times we launch a new circuit to handle a given stream. Too many launches could indicate an inconsistency between our "launch a circuit to handle this stream" logic and our "attach this stream to one of the available circuits" logic.
- Improve log messages related to excluded nodes.

o Minor bugfixes:
- Fix a spurious warning when moving from a short month to a long month on relays with month-based BandwidthAccounting. Bugfix on 0.2.2.17-alpha; fixes bug 3020.
- When a client finds that an origin circuit has run out of 16-bit stream IDs, we now mark it as unusable for new streams. Previously, we would try to close the entire circuit. Bugfix on 0.0.6.
- Add a forgotten cast that caused a compile warning on OS X 10.6. Bugfix on 0.2.2.24-alpha.
- Be more careful about reporting the correct error from a failed connect() system call. Under some circumstances, it was possible to look at an incorrect value for errno when sending the end reason. Bugfix on 0.1.0.1-rc.
- Correctly handle an "impossible" overflow cases in connection byte counting, where we write or read more than 4GB on an edge connection in a single second. Bugfix on 0.1.2.8-beta.
- Correct the warning displayed when a rendezvous descriptor exceeds

the maximum size. Fixes bug 2750; bugfix on 0.2.1.5-alpha. Found by John Brooks.
- Clients and hidden services now use HSDir-flagged relays for hidden service descriptor downloads and uploads even if the relays have no DirPort set and the client has disabled TunnelDirConns. This will eventually allow us to give the HSDir flag to relays with no DirPort. Fixes bug 2722; bugfix on 0.2.1.6-alpha.
- Downgrade "no current certificates known for authority" message from Notice to Info. Fixes bug 2899; bugfix on 0.2.0.10-alpha.
- Make the SIGNAL DUMP control-port command work on FreeBSD. Fixes bug 2917. Bugfix on 0.1.1.1-alpha.
- Only limit the lengths of single HS descriptors, even when multiple HS descriptors are published to an HSDir relay in a single POST operation. Fixes bug 2948; bugfix on 0.2.1.5-alpha. Found by hsdir.
- Write the current time into the LastWritten line in our state file, rather than the time from the previous write attempt. Also, stop trying to use a time of -1 in our log statements. Fixes bug 3039; bugfix on 0.2.2.14-alpha.
- Be more consistent in our treatment of file system paths. "~" should get expanded to the user's home directory in the Log config option. Fixes bug 2971; bugfix on 0.2.0.1-alpha, which introduced the feature for the -f and --DataDirectory options.

o Minor features:
- Make sure every relay writes a state file at least every 12 hours. Previously, a relay could go for weeks without writing its state file, and on a crash could lose its bandwidth history, capacity estimates, client country statistics, and so on. Addresses bug 3012.
- Send END_STREAM_REASON_NOROUTE in response to EHOSTUNREACH errors. Clients before 0.2.1.27 didn't handle NOROUTE correctly, but such clients are already deprecated because of security bugs.
- Don't allow v0 hidden service authorities to act as clients. Required by fix for bug 3000.
- Ignore SIGNAL NEWNYM commands on relay-only Tor instances. Required by fix for bug 3000.
- Ensure that no empty [dirreq-](read|write)-history lines are added to an extrainfo document. Implements ticket 2497.

o Code simplification and refactoring:
- Remove workaround code to handle directory responses from servers that had bug 539 (they would send HTTP status 503 responses _and_ send a body too). Since only server versions before 0.2.0.16-alpha/0.1.2.19 were affected, there is no longer reason to keep the workaround in place.
- Remove the old 'fuzzy time' logic. It was supposed to be used for

handling calculations where we have a known amount of clock skew and an allowed amount of unknown skew. But we only used it in three places, and we never adjusted the known/unknown skew values. This is still something we might want to do someday, but if we do, we'll want to do it differently.
- Avoid signed/unsigned comparisons by making SIZE_T_CEILING unsigned. None of the cases where we did this before were wrong, but by making this change we avoid warnings. Fixes bug 2475; bugfix on 0.2.1.28.
- Use GetTempDir to find the proper temporary directory location on Windows when generating temporary files for the unit tests. Patch by Gisle Vanem.

3. On April 10, we released Vidalia 0.2.12. We'd also like to congratulate Tomás Touceda on his first release and thank him for all his work and patience in getting this out!

o Vidalia's SVN repository has been migrated to Git. All branches but master have been archived for later review, since SVN trunk had changed significantly; they should be reviewed later to determine whether they can and should still be merged. All \version Id headers have been removed since Git does not support Id.
o As part of the move, Vidalia's Trac is now at:
  https://trac.torproject.org/
  All Trac numbers in Vidalia 0.2.12 and beyond refer to the new Trac entries. The old Trac is archived for posterity at:
  https://trac-vidalia.torproject.org/projects/vidalia
o Add support for Tor's ControlSocket as an alternative to ControlPort. It can be used for Linux maintainers to build a better default interaction between Tor and Vidalia by just setting the right permissions and file owner on the socket file for the connection. Using ControlSocket means you don't need to worry about authentication methods with ControlPort. Resolves bug 2091.
o Add a way to edit arbitrary torrc entries while Tor is running. Now Vidalia users have more flexibility for configuring Tor. This change doesn't replace editing torrc directly, because on some systems (like Debian) Tor can't write to its torrc file. Resolves bug 2083.
o Remove Vidalia's direct dependency on OpenSSL. This dependency had caused Vidalia to fail to run on FreeBSD (due to a bug in the FreeBSD ports collection) and Fedora 14 (due to an incompatibility between OpenSSL and Fedora's SELinux configuration). Resolves bug 2287 and 2611.
o Restore compatibility with Windows 2000. An update to the MiniUPnPc library had introduced an unnecessary dependency on a system library not included in Windows 2000. Fixes bug 2612.
o Fix how the advanced message log window displays message updates when messages are coming in too quickly, for example when you're listening to debug-level messages from Tor. Fixes bug 2093.

```
  o Add a what's this? link to the bridge option to explain in a more verbose
    fashion what being a bridge involves. Resolves bug 1995.
  o Prompt users to restart Tor after changing the path to torrc. Fixes bug
    2086.
  o Disable the directory port configuration field when configuring a
    bridge. A bridge does not need to operate a separate directory port,
    and operating one can make a bridge easier to detect. Fixes bug 2431.
  o When Vidalia asks Tor for a bridge's usage history before anyone has
    used it, correctly report that no clients have used the bridge recently.
    Previously, it would incorrectly warn that it was unable to retrieve the
    bridge's usage history. Fixes bug 2186.
```

4. On April 6, TAILS 0.7 anonymous operating system was released.

```
  * Hardware support
  - Install foomatic-filters-ppds to support more printers.
  - Give the default user the right to manage printers.

  * Software
  - Deinstall unwanted packages newly pulled by recent live-build.

 -- Tails developers <amnesia@boum.org>  Wed, 06 Apr 2011 22:58:51 +0200

tails (0.7~rc2) unstable; urgency=low

  ** SNAPSHOT build @824f39248a08f9e190146980fb1eb0e55d483d71 **

  * Rebase on Debian Squeeze 6.0.1 point-release.

  * Vidalia: new 0.2.10-3+tails5 custom package..

  * Hardware support
  - Install usb-modeswitch and modemmanager to support mobile broadband
    devices such as 3G USB dongles. Thanks to Marco A. Calamari for the
    suggestion.

  * Misc
  - Website relocated to https://tails.boum.org/ => adapt various places.
  - Configure keyboard layout accordingly to the chosen language for
    Italian and Portuguese.

 -- Tails developers <amnesia@boum.org>  Fri, 25 Mar 2011 15:44:25 +0100

tails (0.7~rc1) UNRELEASED; urgency=low

  ** SNAPSHOT build @98987f111fc097a699b526eeaef46bc75be5290a **
```

```
* Rebase on Debian Squeeze.

* T(A)ILS has been renamed to Tails.

* Protecting against memory recovery
  New, safer way to wipe memory on shutdown which is now also used when
  the boot media is physically removed.

* Tor
- Update to 0.2.1.30-1.

* Iceweasel
- Add HTTPS Everywhere 0.9.4 extension.
- Better preserve Anonymity Set: spoof US English Browser and timezone
  the same way as the Tor Browser Bundle, disable favicons and picture
  iconification.
- Install AdBlock Plus extension from Debian.
- Add Tor-related bookmarks.
- Support FTP, thanks to FoxyProxy.
- Update AdBlock patterns.
- Disable geolocation and the offline cache.

* Software
- Update Vidalia to 0.2.10-3+tails4.
- Install gnome-disk-utility (Palimpsest) and Seahorse plugins.
- Add opt-in i2p support with Iceweasel integration through FoxyProxy.
- onBoard: fix "really quits when clicking the close window icon" bug.
- Optionally install TrueCrypt at boot time.
- Install laptop-mode-tools for better use of battery-powered hardware.
- Replace xsane with simple-scan which is part of GNOME and way easier
  to use.
- Upgrade WhisperBack to 1.3.1 (bugfixes, French translation).
- Install scribus-ng instead of scribus. It is far less buggy in Squeeze.

* Firewall
- Drop incoming packets by default.
- Forbid queries to DNS resolvers on the LAN.
- Set output policy to drop (defense-in-depth).

* Hardware support
- Install Atheros and Broadcom wireless firmwares.
- Install libsane-hpaio and sane-utils, respectively needed for
  multi-function peripherals and some SCSI scanners.
```

```
  * live-boot 2.0.15-1+tails1.35f1a14
  - Cherry-pick our fromiso= bugfixes from upstream 3.x branch.

  * Miscellaneous
  - Many tiny user interface improvements.
  - More robust HTP time synchronization wrt. network failures.
    Also, display the logs when the clock synchronization fails.
  - Disable GNOME automatic media mounting and opening to protect against
    a class of attacks that was recently put under the spotlights.
    Also, this feature was breaking the "no trace is left on local
    storage devices unless explicitly asked" part of Tails specification.
  - Make configuration more similar to the Tor Browser Bundle's one.
  - GnuPG: default to stronger digest algorithms.
  - Many more or less proper hacks to get the built image size under 700MB.
  - Compress the initramfs using LZMA for faster boot.

  * Build system
  - Run lb build inside eatmydata fsync-less environment to greatly improve
    build time.

 -- Tails developers <amnesia@boum.org>  Fri, 11 Mar 2011 15:52:19 +0100
```

5. On April 30, TAILS 0.7.1 anonymous operating system was released.

```
Vidalia: new 0.2.12-2+tails1 custom package.

  * Iceweasel
  - Don't show Foxyproxy's status / icon in FF statusbar to prevent users
    from accidentaly / unconsciously put their anonymity at risk.
  - "amnesia branding" extension: bump Iceweasel compatibility to 4.0 to ease
    development of future releases.

  * Software
  - Upgrade Linux kernel to Debian's 2.6.32-33: fixes tons of bugs,
    including the infamous missing mouse cursor one. Oh, and it closes
    a few security holes at well.
  - Install unrar-free.
  - Do not install pppoeconf (superseeded by NetworkManager).
  - Upgrade macchanger to Debian testing package to ease development of
    future Tails releases.
  - Debian security upgrades: x11-xserver-utils (DSA-2213-1), isc-dhcp
    (DSA-2216-1), libmodplug (DSA-2226-1), openjdk-6 (DSA-2224-1).

  * Protecting against memory recovery
  - Add Italian translation for tails-kexec. Thanks to Marco A. Calamari.
```

```
  - Make it clear what it may mean if the system does not power off
    automatically.
  - Use kexec's --reset-vga option that might fix display corruption issues
    on some hardware.

  * WhisperBack (encrypted bug reporting software)
  - Upgrade WhisperBack to 1.4.1:
    localizes the documentation wiki's URL,
    uses WebKit to display the bug reporting help page,
    now is usable on really small screens.
  - Extract wiki's supported languages at build time, save this
    information to /etc/amnesia/environment, source this file into the
    Live user's environment so that WhisperBack 1.4+ can make good use
    of it.

  * Miscellaneous
  - Fix boot in Chinese.
  - Install mobile-broadband-provider-info for better 3G support.
  - Add back GNOME system icons to menus.
  - tails-security-check: avoid generating double-slashes in the Atom
    feeds URL.
  - Remove "vga=788" boot parameter which breaks the boot on some hardware.
  - Remove now useless "splash" boot parameter.
  - Fix a bunch of i386-isms.
  - Pass the noswap option to the kernel. This does not change actual Tails
    behaviour but prevents users from unnecessarily worrying because of
    the "Activating swap" boot message.
  - Make use of check.torproject.org's Arabic version.

  * Build system
  - Enable squeeze-backports. It is now ready and will be used soon.
  - Install eatmydata in the chroot.
  - Convert ikiwiki setup files to YAML.
```

6. On April 12, Tor Browser Bundle for Windows, version 1.3.22 released.

```
   Update Vidalia to 0.2.12
```

7. On April 13, Tor Browser Bundle for Windows, version 1.3.23 released.

```
   Fix langpack mistake that made Firefox only use English
```

8. On April 30, Tor Browser Bundle for Windows, version 1.3.24 released.

```
   Update Firefox to 3.6.17
   Update Libevent to 2.0.10-stable
```

```
Update zlib to 1.2.5
Update OpenSSL to 1.0.0d
```

9. On April 12, Tor Browser Bundle for Linux, version 1.1.7 released.

```
Update Tor to 0.2.2.24-alpha
Update Vidalia to 0.2.12
Update NoScript to 2.1.0.1
```

10. On April 30, Tor Browser Bundle for Linux, version 1.1.8 released.

```
Update Tor to 0.2.2.25-alpha
Update Firefox to 3.6.17
```

11. On April 11, Tor Browser Bunde for OSX, version 1.0.15 released.

```
Update Tor to 0.2.2.24-alpha
Update Vidalia to 0.2.12
Update NoScript to 2.1.0.1
```

12. On April 30, Tor Browser Bundle for OSX, version 1.0.16 released.

```
Update Tor to 0.2.2.25-alpha
Update Firefox to 3.6.17
```

13. On April 4, arm 1.4.2 was released. This one was focused on a full rewrite of the connection panel, improving its maintainability, performance, and (best of all) features. When rendered, the panel's baseline cpu usage is less than half of its previous incarnation, along with providing far more information... http://www.atagar.com/transfer/tmp/armScreenshot-1.4.2.png

```
- Full paths for your currently active Tor circuits
- Identification of the applications attached to your socks, hidden
  service, and control ports
- Identifying exit connections and the common uses for ports they're
  attached to
- Much better accuracy in identifying client and directory connections
- Expanded path information when there's space available (thanks to
  Fabian Keil)
... and many, many more enhancements and fixes. For the full list see:
http://www.atagar.com/arm/releaseNotes.php#1.4.2
Also, thanks to pyllyukko arm is now on slackbuilds.org so there's simple
install options available for:
Debian, Ubuntu, Gentoo, Arch Linux, and Slackware
As always, screenshots and downloads are available from the project's
homepage:
http://www.atagar.com/arm/
```

14. On April 28th, released libevent 2.0.11.

```
BUGFIXES:
 o Fix evport handling of POLLHUP and POLLERR (b42ce4b)
 o Fix compilation on Windows with NDEBUG (cb8059d)
 o Check for POLLERR, POLLHUP and POLLNVAL for Solaris event ports (0144886 Trond Norbye)
 o Detect and handle more allocation failures. (666b096 Jardel Weyrich)
 o Use event_err() only if the failure is truly unrecoverable. (3f8d22a Jardel Weyrich)
 o Handle resize failures in the select backend better. (83e805a)
 o Correctly free selectop fields when select_resize fails in select_init (0c0ec0b)
 o Make --enable-gcc-warnings a no-op if not using gcc (3267703)
 o Fix a type error in our (unused) arc4random_stir() (f736198)
 o Correctly detect and stop non-chunked http requests when the body is too long (63a715e)
 o Have event_base_gettimeofday_cached() always return wall-clock time (a459ef7)
 o Workaround for http crash bug 3078187 (5dc5662 Tomash Brechko)
 o Fix incorrect assertions and possible use-after-free in evrpc_free() (4b8f02f Christoph
 o Reset outgoing http connection when read data in idle state. (272823f Tomash Brechko)
 o Fix subtle recursion in evhttp_connection_cb_cleanup(). (218cf19 Tomash Brechko)
 o Fix the case when failed evhttp_make_request() leaved request in the queue. (0d6622e To
 o Fix a crash bug in evdns server circular list code (00e91b3)
 o Handle calloc failure in evdns. (Found by Dave Hart) (364291e)
 o Fix a memory leak on win32 socket->event map. (b4f89f0)
 o Add a forgotten NULL check to evhttp_parse_headers (12311ff Sebastian Hahn)
 o Fix possible NULL-deref in evdns_cancel_request (5208544 Sebastian Hahn)

PORTABILITY:
 o Fall back to sscanf if we have no other way to implement strtoll (453317b)
 o Build correctly on platforms without sockaddr_storage (9184563)
 o Try to build correctly on platforms with no IPv6 support (713c254)
 o Build on systems without AI_PASSIVE (cb92113)
 o Fix http unit test on non-windows platforms without getaddrinfo (6092f12)
 o Do not check for gethostbyname_r versions if we have getaddrinfo (c1260b0)
 o Include arpa/inet.h as needed on HPUX (10c834c Harlan Stenn)
 o Include util-internal.h as needed to build on platforms with no sockaddr_storage (bbf55
 o Check for getservbyname even if not on win32. (af08a94 Harlan Stenn)
 o Add -D_OSF_SOURCE to fix hpux builds (0b33479 Harlan Stenn)
 o Check for allocation failures in apply_socktype_protocol_hack (637d17a)
 o Fix the check for multicast or broadcast addresses in evutil_check_interfaces (1a21d7b)
 o Avoid a free(NULL) if out-of-memory in evdns_getaddrinfo. Found by Dave Hart (3417f68)

DEFENSIVE PROGRAMMING:
 o Add compile-time check for AF_UNSPEC==PF_UNSPEC (3c8f4e7)

BUGS IN TESTS:
 o Fix test.sh output on solaris (b4f89b6 Dave Hart)
 o Make test-eof fail with a timeout if we never get an eof. (05a2c22 Harlan Stenn)
```

```
 o Use %s with printf in test.sh (039b9bd)
 o Add an assert to appease clang's static analyzer (b0ff7eb Sebastian Hahn)
 o Add a forgotten return value check in the unit tests (3819b62 Sebastian Hahn)
 o Actually send NULL request in http_bad_request_test (b693c32 Sebastian Hahn)
 o add some (void) casts for unused variables (65707d7 Sebastian Hahn)
 o Refactor test_getaddrinfo_async_cancel_stress() (48c44a6 Sebastian Hahn)
 o Be nice and "handle" error return values in sample code (4bac793 Sebastian Hahn)
 o Check return value of evbuffer_add_cb in tests (93a1abb Sebastian Hahn)
 o Remote some dead code from dns-example.c (744c745 Sebastian Hahn)
 o Zero a struct sockaddr_in before using it (646f9fe Sebastian Hahn)

BUILD FIXES:
 o Fix warnings about AC_LANG_PROGRAM usage (f663112 Sebastian Hahn)
 o Skip check for zlib if we have no zlib.h (a317c06 Harlan Stenn)
 o Fix autoconf bracket issues; make check for getaddrinfo include netdb.h (833e5e9 Harlar
 o Correct an AM_CFLAGS to an AM_CPPFLAGS in test/Makefile.am (9c469db Dave Hart)
 o Fix make distcheck & installation of libevent 1 headers (b5a1f9f Dave Hart)
 o Fix compilation under LLVM/clang with --enable-gcc-warnings (ad9ff58 Sebastian Hahn)

FEATURES:
 o Make URI parser able to tolerate nonconformant URIs. (95060b5)

DOCUMENTATION:
 o Clarify event_set_mem_functions doc (926f816)
 o Correct evhttp_del_accept_socket documentation on whether socket is closed (f665924)
 o fix spelling mistake in whatsnew-2.0.txt (deb2f73)
 o Fix sample/http-server ipv6 fixes (eb692be)
 o Comment internal headers used in sample code. (4eb281c)
 o Be explicit about how long event loops run in event.h documentation (f95bafb)
 o Add comment to configure.in to explain gc-sections test logic (c621359)
 o Fix a couple of memory leaks in samples/http-server.c. Found by Dave Hart. (2e9f665)

BUILD IMPROVEMENTS:
 o Use the gcc -ffunction-segments feature to allow gc when linking with static libevent (
 o Add configure options to disable installation, regression tests (49e9bb7 Dave Hart)
```

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

Tomás

- Started working on Vidalia-0.3.0-alpha:

```
- Re-integrate breakpad and add support for Linux/OSX, along with a
basic change on what to do with the memdumps.
```

```
- "Finish" the new GUI that is flexible enough to support the plug-in
interface that I plan to start working on pretty soon.
- Change the control password problem approach to something more user
friendly.
- Other changes in the sharing setting to allow explicitly setting a non-exit
relay and other minor changes.
```

- Work on a bootstrap option so that Erinn can build bridge-only portable packages for OSX.
- Fix some certificate problems with "Find Bridges".

Mike

- The blocking request redirect APIs for Google Chrome's WebRequest API landed in the experimental API set just prior to this iteration, so I decided to churn out a prototype of HTTPS-Everywhere for Chrome (2956). This was amazingly simple compared to the Firefox effort.
- Recategorized the Torbutton bugs into two groups: those for the toggle model, and those for the browser model (2952). If you have no idea what this means, read the blog post I wrote about moving towards proving Tor Browser Bundle as our only client software (2960).

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

Karsten

- Extended metrics-db to extract v3 certificates from v3 votes which is necessary to verify the signatures on v3 consensuses without downloading the huge v3 vote tarballs (2786).
- Improved metrics-db to download all server and extra-info descriptors from the directory authorities once per day (2763). Turns out this didn't solve the problem that we're missing rejected descriptors or those that are not referenced in the consensus.
- Added GeoIP database to metrics-web to provide relay snapshots with geo data for Moritz Bartl (2512). Also used the data to add graphs on the number of relays by country.
- Improved the metrics website graph interface to show graphs on estimated user numbers for all countries in the GeoIP database (1636).
- Added a graph on bandwidth by relay flags to the metrics website (1634).
- Worked on the R code to process Torperf's new .mergedata format together with Tom (2687). Looks like we'll have to switch to Python for parsing the new .mergedata format.
- Measured Tor performance with custom circuit build timeouts and guard node selections together with Mike (2686).
- Wrote the first half of a bandwidth scanner specification (2861).
- Finished a first draft of the BridgeDB specification together with Nick (1606).

Roger

- Reviewed proposal 180 (modular transport), and helped push asn and nickm to get obfsproxy into git with a howto: `https://gitweb.torproject.org/obfsproxy.git/blob/HEAD:/doc/tor-obfs-howto.txt`

Nick

- Nick wrote up the status of IPv6 and Tor. `https://blog.torproject.org/blog/ipv6-future-i-hear`.
- Worked with George K (asn) to get obfsproxy refactored and testable. (Now it's testable! You can pull it from git, read its instructions, and go!)
- Roger and nick finished and merged the bug 1090 fix. This is a big deal: it resolves long-standing issues in our node selection logic and gives a sensible, consistent, and not-too-hard-to-explain meaning to the various *Nodes options. We've been working on this for a while, and it's a great relief to finally be done with it.

Christian

- Deployed a new version if BridgeDB. Most importantly, we now serve a Chinese translation via

  `bridges+zh_CN@torproject.org`

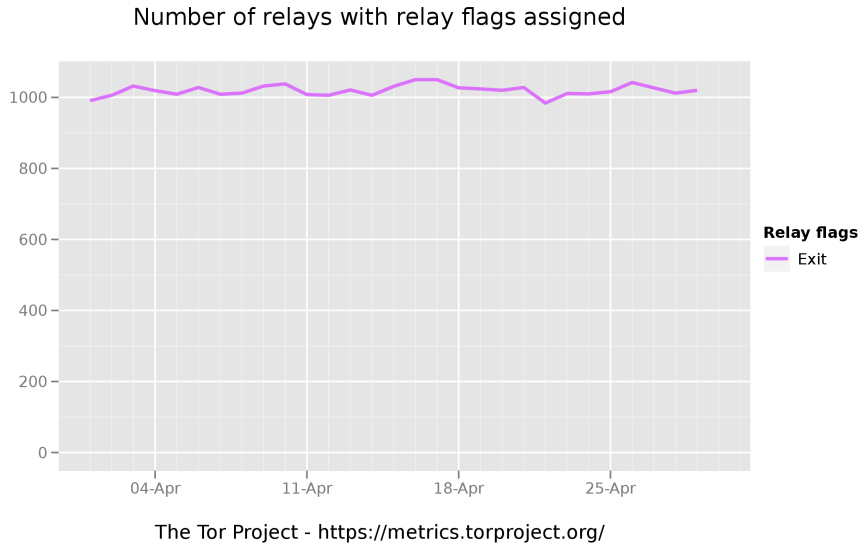
  and `https://bridges.torproject.org/zh_CN/`
- Wrote a script that emails unallocated Bridges to Chinese activists daily.

Hide Tor's network signature.

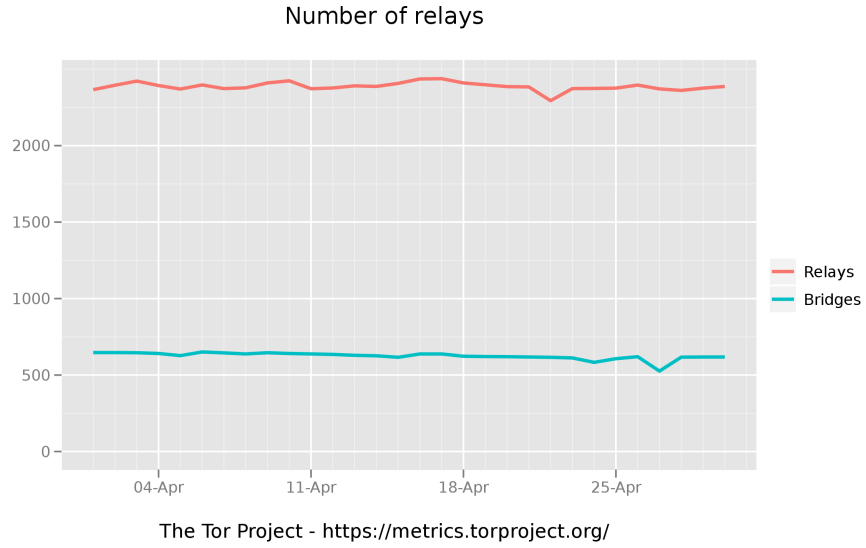
See the updates for pluggable transport and obsproxy in the section above.

Grow the Tor network and user base. Outreach.

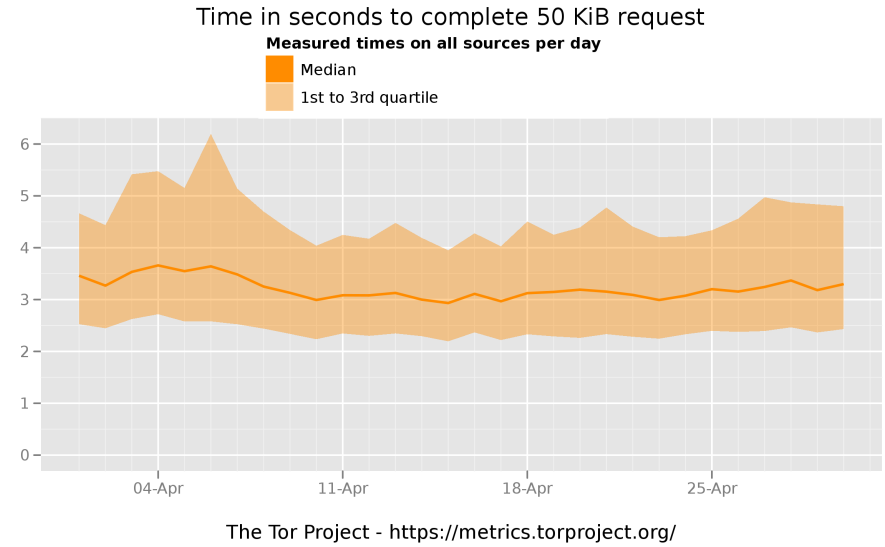
Measures of the Tor Network



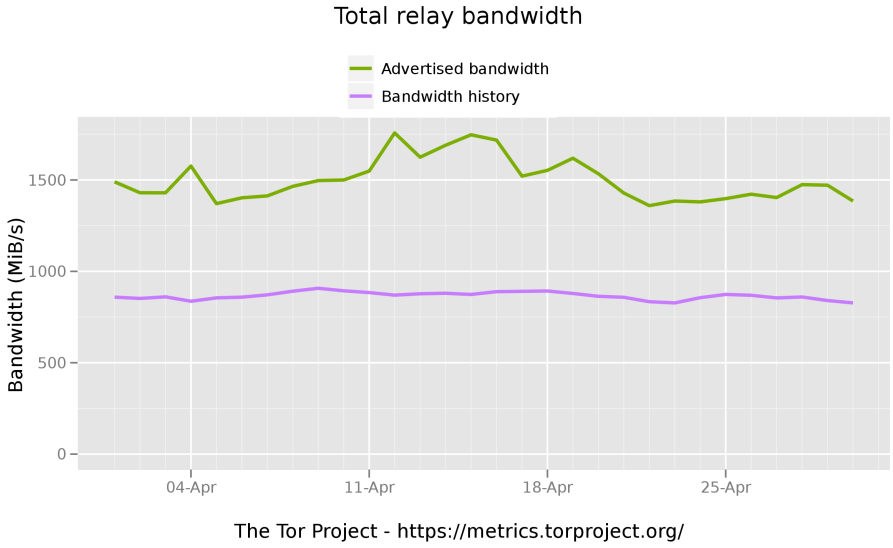
This graph shows the total quantity of exit relays in April 2011. We seem to have kept most of our relays since the bump due to Tunisia and Egypt.



This graph shows the total quantity of relays and the total quantity of bridges in April 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. Tomas Participated in the Build It! initiative, `https://openhatch.org/wiki/Build_it`. It went really well. We may have picked up a new OS X contributor for Vidalia.

2. Runa attended Security BSides London.

3. Jacob spoke on a panel at "The Future of Internet Freedom: Promoting Abroad...but Losing at Home?", https://www12.georgetown.edu/sfs/rsvp/index.cfm?Action=View&EventID=3324

4. Roger lectured at Berkeley, http://www.ischool.berkeley.edu/newsandevents/events/20110418dingledine.

5. Roger lectured at Stanford for Dan Boneh, http://crypto.stanford.edu/cs294s/.

6. Andrew spoke at the 1st Software And Usable Security Aligned for Good Engineering (SAUSAGE) Workshop, http://www.thei3p.org/events/sausage2011.html.

7. Andrew spoke at "Internet, Dissent and Authoritarianism: Control and Resistance in an Era of Social Media", http://chrchristensen.wordpress.com/2011/04/12/101/.

8. Jacob spoke at LinuxFest Northwest, http://www.linuxfestnorthwest.org/.

9. Jacob spoke at the SHARE conference in Belgrade, Serbia. http://www.shareconference.net/en/

10. Jacob responded to the Freedom House "Leaping over the Firewall" report with "Over the firewall and into the fire", http://advocacy.globalvoicesonline.org/2011/04/14/over-the-firewall-and-into-the-fire/

11. Karen talked to a government agency writing a report for Congress on companies that sell censorship and surveillance technology to Iran.

12. Nick spoke at the usenix LEET workshop about Tor's arms-race with censors. http://www.usenix.org/event/leet11/

13. Erinn gave a talk at the University of Split in Croatia.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

1. We suspended development and releases of the Tor Instant Messaging Browser Bundle due to security and privacy concerns with the included multi-protocol client called Pidgin. Thankfully the Pidgin team has responded with a number of fixes, http://developer.pidgin.im/ticket/11110, http://developer.pidgin.im/ticket/13928, http://developer.pidgin.im/ticket/13879.

2. Jacob did some investigation into the libpurple leaks in Adium, the Mac OS X chat client: http://trac.adium.im/ticket/15161

Bridge relay and bridge authority work.

1. Runa made some progress on the Tor web interface for the Excito B3 (2791). Getting started was a PITA due to lack of documentation and lots of trying and failing. However, I now have the following: a Tor page that has been added to the main menu, a button to disable or enable Tor, and three text fields that read and display the nickname, contact information and relay port from /etc/tor/torrc.

Scalability, load balancing, directory overhead, efficiency.

Sebastian

- Mostly worked on trying to get 0.2.2.x-blocking bugs fixed or at least reviewed so that others could fix them. The most notorious bugs were 1090, 2704 and 3000.
- Worked on getting Tor tested with more static analysis software, and found the clang analyzer. It is not totally mature yet, but found a couple of issues including real bugs for some configurations. I used it to scan libevent, and provided a few patches to fix them in time for the 2.0.11-stable release. The Tor fixes didn't go in to 0.2.2.x yet, but I hope that they soon will.
- I also ported Tor's configure enhancements for hardening etc over to libevent, which wasn't taken for 2.0.x so I will reroll it for 2.1.x.

Mike

- Worked on some Torperf experiments with Karsten (2958), and reviewed some Firefox source for future patches of Tor Browser (2951). A typo in the Torbutton install.rdf forced me to do a last-minute Torbutton release, which ended up taking 2 days of wall clock time instead of the last-minute that was allocated (3065).

Robert

- Investigated 2401, and determined that the client code's behaviour was correct. The only actual problem that led to that bug report was that the set of relays with the HSDir flag is not sufficiently stable; we need to release a fix for 2649 in a 0.2.2.x release in order to get it running on the non-developer-operated DAs and find out whether it helps.
- While investigating 2401, I found a serious security issue in the hidden service code which made the fact that the client-side hidden service descriptor cache is never cleared (3000) easy to exploit. All users who use a web browser through Tor should upgrade to Tor 0.2.2.25-alpha for the 3000 fix.
- Fixed 1930 (a long-standing reliability bug in the v2 hidden service directory code).
- Designed a way for Tor controllers that want to 'own' a Tor process (ensure that the Tor process ends when its controller does) to do so quite reliably. See 3049.

Nick

- Wrote up a couple of strawman designs for improved onionskin handshakes.
- Did some performance and feasibility testing and research with respect to ECC implementations. Curve25519-donna is looking pretty sweet.
- Did a big chunk of work to clean up Tor's internal Doxygen documentation.
- Finished the pluggable transport proposal and sent it to tor-dev. See `https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/180-pluggable-transport.txt` for the full spec.
- Started getting Chutney ready include a network test framework in addition to a test network framework. Chutney is a tool that lets you configure and test a tor network for monitoring and testing. `https://gitweb.torproject.org/nickm/chutney.git/blob/HEAD:/README`.

Incentives work.

Nothing to report.

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

Nick and Erinn worked to get a thandy package format design finished.

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

1. Sebastian, Tomás, and Runa worked on a patch to make the transifex-client verify SSL certificates. The patch works on Debian, but the Transifex developers want to find a solution that works on all systems, including Windows. Sebastian and Runa had a short discussion about the possibility of including the patch ourselves, rather than wait for Transifex to implement and roll out a solution. Once this problem is fixed, it will no longer block 2643.
2. #2811: Runa decided to drop translated manual pages.
3. #2713: Updated translation priorities for resources on Transifex.
4. #2894: Got my own Git repository and fixed translations for Vidalia.
5. #2932: Fixed a bug in the German translation of Vidalia.
6. #2896: Renamed the list of resources on Transifex to make it seem less messy.
7. #2898: Updated the path to gettor.pot on Transifex.

8. #2892: Added and fixed German .wmi files.

9. #2904: Added and fixed German .wmi files.

10. Update translations. (in translation/trunk/projects/torbutton-alpha/po: .tx af ak am arn ast az be bg bn bn_IN bo br bs csb cy da de dz eo eu fa fi fil fo fur fy ga gl gun ha he hi ht hu hy is ja jv ka km kn ko ku kw ky lb ln lo lt lv mg mi mk ml mn mr ms mt nah nap ne nn nso oc or pa pap pms ps sco sk sl so son sq sr st su sv sw ta te templates tg th ti tk uk ur ve wa wo zh_HK zu)

11. pulled updated .po files for Orbot from Transifex (in translation/trunk/projects/orbot/po: af ak am ar arn ast az be bg bn bn_IN ca cs csb cy da dz el eo es et eu fil fr fur ga gl gu gun ha he hi hr ht id is it kn kw lb ln lo lt lv mg mi mk ml mn mr ms mt my nap nb ne nl nn nso oc pa pap pl pms ps pt pt_BR ro ru sco son sw ta te tg th ti tk tr uk ve vi wa zh_CN zh_HK zh_TW zu)

12. updated Orbot translations (in projects/android/trunk/Orbot/res: values-ar values-ca values-de values-es values-fa values-mk values-nl values-pl values-ru values-zh)

13. new and updated translations for the website (in translation/trunk/projects/website/po: ar ar/about ar/docs ar/donate ar/download ar/getinvolved ar/press ar/projects ar/torbutton de de/about de/docs de/getinvolved es/about es/docs es/press es/projects fa/about fa/docs fa/download fa/projects it/about it/docs it/press it/projects my pl_PL/about pl_PL/docs pl_PL/projects ru/about ru/docs ru/press ru/projects zh_CN/about)