From: Andrew Lewman, Executive Director
To: The Tor Community
Date: October 7, 2011

This report documents progress in September 2011.

New releases, new hires, new funding

New Funding

Tor receives funding from the Swedish International Cooperation Development Agency to improve the Tails live system.

New Releases

1. On September 1st, we released Tor 0.2.3.3-alpha. Tor 0.2.3.3-alpha adds a new "stream isolation" feature to improve Tor's security, and provides client-side support for the microdescriptor and optimistic data features introduced earlier in the 0.2.3.x series. It also includes numerous critical bugfixes in the (optional) bufferevent-based networking backend.

```
Changes in version 0.2.3.3-alpha - 2011-09-01
  o Major features (stream isolation):
    - You can now configure Tor so that streams from different
      applications are isolated on different circuits, to prevent an
      attacker who sees your streams as they leave an exit node from
      linking your sessions to one another. To do this, choose some way
      to distinguish the applications: have them connect to different
      SocksPorts, or have one of them use SOCKS4 while the other uses
      SOCKS5, or have them pass different authentication strings to the
      SOCKS proxy. Then, use the new SocksPort syntax to configure the
      degree of isolation you need. This implements Proposal 171.
    - There's a new syntax for specifying multiple client ports (such as
      SOCKSPort, TransPort, DNSPort, NATDPort): you can now just declare
      multiple *Port entries with full addr:port syntax on each.
      The old *ListenAddress format is still supported, but you can't
      mix it with the new *Port syntax.

  o Major features (other):
    - Enable microdescriptor fetching by default for clients. This allows
      clients to download a much smaller amount of directory information.
```

```
    To disable it (and go back to the old-style consensus and
    descriptors), set "UseMicrodescriptors 0" in your torrc file.
  - Tor's firewall-helper feature, introduced in 0.2.3.1-alpha (see the
    "PortForwarding" config option), now supports Windows.
  - When using an exit relay running 0.2.3.x, clients can now
    "optimistically" send data before the exit relay reports that
    the stream has opened. This saves a round trip when starting
    connections where the client speaks first (such as web browsing).
    This behavior is controlled by a consensus parameter (currently
    disabled). To turn it on or off manually, use the "OptimisticData"
    torrc option. Implements proposal 181; code by Ian Goldberg.

o Major bugfixes (bufferevents, fixes on 0.2.3.1-alpha):
  - When using IOCP on Windows, we need to enable Libevent windows
    threading support.
  - The IOCP backend now works even when the user has not specified
    the (internal, debugging-only) _UseFilteringSSLBufferevents option.
    Fixes part of bug 3752.
  - Correctly record the bytes we've read and written when using
    bufferevents, so that we can include them in our bandwidth history
    and advertised bandwidth. Fixes bug 3803.
  - Apply rate-limiting only at the bottom of a chain of filtering
    bufferevents. This prevents us from filling up internal read
    buffers and violating rate-limits when filtering bufferevents
    are enabled. Fixes part of bug 3804.
  - Add high-watermarks to the output buffers for filtered
    bufferevents. This prevents us from filling up internal write
    buffers and wasting CPU cycles when filtering bufferevents are
    enabled. Fixes part of bug 3804.
  - Correctly notice when data has been written from a bufferevent
    without flushing it completely. Fixes bug 3805.
  - Fix a bug where server-side tunneled bufferevent-based directory
    streams would get closed prematurely. Fixes bug 3814.
  - Fix a use-after-free error with per-connection rate-limiting
    buckets. Fixes bug 3888.

o Major bugfixes (also part of 0.2.2.31-rc):
  - If we're configured to write our ControlPorts to disk, only write
    them after switching UID and creating the data directory. This way,
    we don't fail when starting up with a nonexistent DataDirectory
    and a ControlPortWriteToFile setting based on that directory. Fixes
    bug 3747; bugfix on Tor 0.2.2.26-beta.

o Minor features:
  - Added a new CONF_CHANGED event so that controllers can be notified
```

of any configuration changes made by other controllers, or by the user. Implements ticket 1692.
- Use evbuffer_copyout() in inspect_evbuffer(). This fixes a memory leak when using bufferevents, and lets Libevent worry about how to best copy data out of a buffer.
- Replace files in stats/ rather than appending to them. Now that we include statistics in extra-info descriptors, it makes no sense to keep old statistics forever. Implements ticket 2930.

o Minor features (build compatibility):
- Limited, experimental support for building with nmake and MSVC.
- Provide a substitute implementation of lround() for MSVC, which apparently lacks it. Patch from Gisle Vanem.

o Minor features (also part of 0.2.2.31-rc):
- Update to the August 2 2011 Maxmind GeoLite Country database.

o Minor bugfixes (on 0.2.3.x-alpha):
- Fix a spurious warning when parsing SOCKS requests with bufferevents enabled. Fixes bug 3615; bugfix on 0.2.3.2-alpha.
- Get rid of a harmless warning that could happen on relays running with bufferevents. The warning was caused by someone doing an http request to a relay's orport. Also don't warn for a few related non-errors. Fixes bug 3700; bugfix on 0.2.3.1-alpha.

o Minor bugfixes (on 2.2.x and earlier):
- Correct the man page to explain that HashedControlPassword and CookieAuthentication can both be set, in which case either method is sufficient to authenticate to Tor. Bugfix on 0.2.0.7-alpha, when we decided to allow these config options to both be set. Issue raised by bug 3898.
- The "--quiet" and "--hush" options now apply not only to Tor's behavior before logs are configured, but also to Tor's behavior in the absense of configured logs. Fixes bug 3550; bugfix on 0.2.0.10-alpha.

o Minor bugfixes (also part of 0.2.2.31-rc):
- Write several files in text mode, on OSes that distinguish text mode from binary mode (namely, Windows). These files are: 'buffer-stats', 'dirreq-stats', and 'entry-stats' on relays that collect those statistics; 'client_keys' and 'hostname' for hidden services that use authentication; and (in the tor-gencert utility) newly generated identity and signing keys. Previously, we wouldn't specify text mode or binary mode, leading to an assertion failure. Fixes bug 3607. Bugfix on 0.2.1.1-alpha (when

```
    the DirRecordUsageByCountry option which would have triggered
    the assertion failure was added), although this assertion failure
    would have occurred in tor-gencert on Windows in 0.2.0.1-alpha.
  - Selectively disable deprecation warnings on OS X because Lion
    started deprecating the shipped copy of openssl. Fixes bug 3643.
  - Remove an extra pair of quotation marks around the error
    message in control-port STATUS_GENERAL BUG events. Bugfix on
    0.1.2.6-alpha; fixes bug 3732.
  - When unable to format an address as a string, report its value
    as "???" rather than reusing the last formatted address. Bugfix
    on 0.2.1.5-alpha.

o Code simplifications and refactoring:
  - Rewrite the listener-selection logic so that parsing which ports
    we want to listen on is now separate from binding to the ports
    we want.

o Build changes:
  - Building Tor with bufferevent support now requires Libevent
    2.0.13-stable or later. Previous versions of Libevent had bugs in
    SSL-related bufferevents and related issues that would make Tor
    work badly with bufferevents. Requiring 2.0.13-stable also allows
    Tor with bufferevents to take advantage of Libevent APIs
    introduced after 2.0.8-rc.
```

2. On September 10th, we released new Tor Browser Bundles.

```
Important note to Windows users: in the last release we enabled automatic
port selection for Tor and this had very unexpected side effects on
many Windows machines. It turns out that there are a number of consumer
firewalls that don't like things connecting on high ports, which was the
default. We're looking into smarter ways to handle this failure mode,
but until we find one, we have reverted the behavior to using the previous
static port. We're very sorry for the huge inconvenience this caused and
hope you will find these bundles more bug-free!

Tor Browser Bundle (2.2.32-4)

    Windows fixes

        Disable automatic port selection to accommodate Windows users
        with firewalls that don't allow connections or traffic on high
        ports (closes: #3952, #3945)

    Linux fixes
        Fix Makefile to allow for automatic retrieval of Qt and libpng
```

```
        (closes: #2255)
        Remove symlinks from tarball (closes: #2312)

    General fixes and updates
        New Firefox patches
            Prevent Firefox from loading all system plugins besides Flash
            (closes: #2826, #3547)
            Prevent content-preferences service from writing website
            urls and their settings to disk (closes: #3229)
        Update Torbutton to 1.4.3
            Don't let Torbutton inadvertently enable automatic updating
            in Firefox (closes: #3933)
            Fix auto-scroll on Twitter (closes: #3960)
            Allow site zoom information to be stored (closes: #3928)
            Make permissions and disk errors human-readable (closes: #3649)
```

3. On September 13th we released Tor 0.2.3.4-alpha. Tor 0.2.3.4-alpha includes the fixes from 0.2.2.33, including a slight tweak to Tor's TLS handshake that makes relays and bridges that run this new version reachable from Iran again. It also fixes a few new bugs in 0.2.3.x, and teaches relays to recognize when they're not listed in the network consensus and republish.

```
Changes in version 0.2.3.4-alpha - 2011-09-13
  o Major bugfixes (also part of 0.2.2.33):
    - Avoid an assertion failure when reloading a configuration with
      TrackExitHosts changes. Found and fixed by 'laruldan'. Fixes bug
      3923; bugfix on 0.2.2.25-alpha.

  o Minor features (security, also part of 0.2.2.33):
    - Check for replays of the public-key encrypted portion of an
      INTRODUCE1 cell, in addition to the current check for replays of
      the g^x value. This prevents a possible class of active attacks
      by an attacker who controls both an introduction point and a
      rendezvous point, and who uses the malleability of AES-CTR to
      alter the encrypted g^x portion of the INTRODUCE1 cell. We think
      that these attacks is infeasible (requiring the attacker to send
      on the order of zettabytes of altered cells in a short interval),
      but we'd rather block them off in case there are any classes of
      this attack that we missed. Reported by Willem Pinckaers.

  o Minor features (also part of 0.2.2.33):
    - Adjust the expiration time on our SSL session certificates to
      better match SSL certs seen in the wild. Resolves ticket 4014.
    - Change the default required uptime for a relay to be accepted as
      a HSDir (hidden service directory) from 24 hours to 25 hours.
      Improves on 0.2.0.10-alpha; resolves ticket 2649.
    - Add a VoteOnHidServDirectoriesV2 config option to allow directory
```

```
    authorities to abstain from voting on assignment of the HSDir
    consensus flag. Related to bug 2649.
  - Update to the September 6 2011 Maxmind GeoLite Country database.

o Minor bugfixes (also part of 0.2.2.33):
  - Demote the 'replay detected' log message emitted when a hidden
    service receives the same Diffie-Hellman public key in two different
    INTRODUCE2 cells to info level. A normal Tor client can cause that
    log message during its normal operation. Bugfix on 0.2.1.6-alpha;
    fixes part of bug 2442.
  - Demote the 'INTRODUCE2 cell is too {old,new}' log message to info
    level. There is nothing that a hidden service's operator can do
    to fix its clients' clocks. Bugfix on 0.2.1.6-alpha; fixes part
    of bug 2442.
  - Clarify a log message specifying the characters permitted in
    HiddenServiceAuthorizeClient client names. Previously, the log
    message said that "[A-Za-z0-9+-_]" were permitted; that could have
    given the impression that every ASCII character between "+" and "_"
    was permitted. Now we say "[A-Za-z0-9+_-]". Bugfix on 0.2.1.5-alpha.

o Build fixes (also part of 0.2.2.33):
  - Clean up some code issues that prevented Tor from building on older
    BSDs. Fixes bug 3894; reported by "grarpamp".
  - Search for a platform-specific version of "ar" when cross-compiling.
    Should fix builds on iOS. Resolves bug 3909, found by Marco Bonetti.

o Major bugfixes:
  - Fix a bug where the SocksPort option (for example) would get
    ignored and replaced by the default if a SocksListenAddress
    option was set. Bugfix on 0.2.3.3-alpha; fixes bug 3936. Fix by
    Fabian Keil.

o Major features:
  - Relays now try regenerating and uploading their descriptor more
    frequently if they are not listed in the consensus, or if the
    version of their descriptor listed in the consensus is too
    old. This fix should prevent situations where a server declines
    to re-publish itself because it has done so too recently, even
    though the authorities decided not to list its recent-enough
    descriptor. Fix for bug 3327.

o Minor features:
  - Relays now include a reason for regenerating their descriptors
    in an HTTP header when uploading to the authorities. This will
    make it easier to debug descriptor-upload issues in the future.
```

```
    - When starting as root and then changing our UID via the User
      control option, and we have a ControlSocket configured, make sure
      that the ControlSocket is owned by the same account that Tor will
      run under. Implements ticket 3421; fix by Jérémy Bobbio.

  o Minor bugfixes:
    - Abort if tor_vasprintf fails in connection_printf_to_buf (a
      utility function used in the control-port code). This shouldn't
      ever happen unless Tor is completely out of memory, but if it did
      happen and Tor somehow recovered from it, Tor could have sent a log
      message to a control port in the middle of a reply to a controller
      command. Fixes part of bug 3428; bugfix on 0.1.2.3-alpha.
    - Make 'FetchUselessDescriptors' cause all descriptor types and
      all consensus types (including microdescriptors) to get fetched.
      Fixes bug 3851; bugfix on 0.2.3.1-alpha.

  o Code refactoring:
    - Make a new "entry connection" struct as an internal subtype of "edge
      connection", to simplify the code and make exit connections smaller.
```

4. On September 21st, an updated version of the Tails Anonymous Live System was released. Major changes include an update to the base operating system, switch to the new Tor stable branch, Torbutton update, and better nickname randomization inside Pidgin.

   A detailed changelog is below:

```
  * Rebase on the Debian Squeeze 6.0.2.1 point-release.

  * Tor
    - Update to 0.2.2.33-1.
    - Disabled ControlPort in favour of ControlSocket.
    - Add port 6523 (Gobby) to Tor's LongLivedPorts list.

  * I2P
    - Update to 0.8.8.
    - Start script now depends on HTP since I2P breaks if the clock jumps or is
      too skewed during bootstrap.

  * Iceweasel
    - Update to 3.5.16-9 (fixes CVE-2011-2374, CVE-2011-2376, CVE-2011-2365,
      CVE-2011-2373, CVE-2011-2371, CVE-2011-0083, CVE-2011-2363, CVE-2011-0085,
      CVE-2011-2362, CVE-2011-2982, CVE-2011-2981, CVE-2011-2378, CVE-2011-2984,
      CVE-2011-2983).
    - Enable HTTP pipelining (like TBB).
    - Update HTTPS Everywhere extension to 1.0.1-1 from Debian unstable.
    - Suppress FoxyProxy update prompts.
```

  - Prevent FoxyProxy from "phoning home" after a detected upgrade.
  - Fixed a bunch of buggy regular expressions in FoxyProxy's configuration. See [[bugs/exploitable_typo_in_url_regex?]] for details. Note that none of these issues are critical due to the transparent proxy.
  - Add DuckDuckGo SSL search engine.

* Torbutton
  - Update to torbutton 1.4.3-1 from Debian unstable.
  - Don't show Torbutton status in the status bar as it's now displayed in the toolbar instead.

* Pidgin
  - More random looking nicks in pidgin.
  - Add IRC account on chat.wikileaks.de:9999.

* HTP
  - Upgrade htpdate script (taken from Git 7797fe9) that allows setting wget's --dns-timeout option.

* Software
  - Update Linux to 3.0.0-1. -686 is now deprecated in favour of -486 and -686-pae; the world is not ready for -pae yet, so we now ship -486.
  - Update OpenSSL to 0.9.8o-4squeeze2 (fixes CVE-2011-1945 (revoke compromised DigiNotar certificates), CVE-2011-1945).
  - Update Vidalia to 0.2.14-1+tails1 custom package.
  - Install accessibility tools:
    - gnome-mag: screen magnifier
    - gnome-orca: text-to-speech
  - Replace the onBoard virtual keyboard with Florence.
  - Install the PiTIVi non-linear audio/video editor.
  - Install ttdnsd.
  - Install tor-arm.
  - Install lzma.

* Arbitrary DNS queries
  - Tor can not handle all types of DNS queries, so if the Tor resolver fails we fallback to ttdnsd. This is now possible with Tor 0.2.2.x, since we fixed Tor bug #3369.

* Hardware support
  - Install ipheth-utils for iPhone tethering.
  - Install xserver-xorg-input-vmmouse (for mouse integration with the host OS in VMWare and KVM).
  - Install virtualbox-ose 4.x guest packages from Debian backports.

```
  * Miscellaneous
    - Switch gpg to use keys.indymedia.org's hidden service, without SSL.
      The keys.indymedia.org SSL certificate is now self-signed. The hidden
      service gives a good enough way to authenticate the server and encrypts
      the connection, and just removes the certificates management issue.
    - The squashfs is now compressed using XZ which reduces the image size quite
      drastically.
    - Remove Windows autorun.bat and autorun.inf. These files did open a static
      copy of our website, which is not accessible any longer.

  * Build system
    - Use the Git branch instead of the Debian version into the built image's
      filename.
    - Allow replacing efficient XZ compression with quicker gzip.
    - Build and install documentation into the chroot (-> filesystem.squashfs).
      Rationale: our static website cannot be copied to a FAT32 filesystem due
      to filenames being too long. This means the documentation cannot be
      browsed offline from outside Tails. However, our installer creates GPT
      hidden partitions, so the doc would not be browseable from outside Tails
      anyway. The only usecase we really break by doing so is browsing the
      documentation while running a non-Tails system, from a Tails CD.
```

5. On September 25th, the latest Arm was released. A new release of arm (http://www.atagar.com/arm/) is now available. Besides the normal batch of bug fixes and minor features this includes an interactive interpretor for raw control port access...

   http://www.atagar.com/arm/images/screenshot_interpretor_full.png

   http://www.atagar.com/arm/releaseNotes.php#1.4.4

   ```
   This is intended to be a tool for developers, highly knowledgeable
   operators, and anyone that would like to learn about Tor's control
   protocol. It provides usability improvements like tab completion and
   history scroll-back, along with IRC style interpretor commands...

   * /help - provides usage information for all of the tor/interpretor
   commands and tor's configuration options
   * /info - queries relay information via fingerprint, nickname, or IP
   * address
   * /find - searches the backlog for the given regex
   * /events - displays any events that we've listened for
   * /write - dumps the interpretor backlog to a file

   This can both be used via a new page in the curses interface and as a
   standalone prompt by running "arm --prompt"...
   ```

6. On September 28th, we released Tor 0.2.3.5-alpha. Tor 0.2.3.5-alpha fixes two bugs that make it possible to enumerate bridge relays; fixes an assertion error that many users started hitting

today; and adds the ability to refill token buckets more often than once per second, allowing significant performance improvements.

```
Changes in version 0.2.3.5-alpha - 2011-09-28
  o Security fixes:
    - Bridge relays now do their directory fetches inside Tor TLS
      connections, like all the other clients do, rather than connecting
      directly to the DirPort like public relays do. Removes another
      avenue for enumerating bridges. Fixes bug 4115; bugfix on 0.2.0.35.
    - Bridges relays now build circuits for themselves in a more similar
      way to how clients build them. Removes another avenue for
      enumerating bridges. Fixes bug 4124; bugfix on 0.2.0.3-alpha,
      when bridges were introduced.

  o Major bugfixes:
    - Fix an "Assertion md->held_by_node == 1 failed" error that could
      occur when the same microdescriptor was referenced by two node_t
      objects at once. Fix for bug 4118; bugfix on Tor 0.2.3.1-alpha.

  o Major features (networking):
    - Add a new TokenBucketRefillInterval option to refill token buckets
      more frequently than once per second. This should improve network
      performance, alleviate queueing problems, and make traffic less
      bursty. Implements proposal 183; closes ticket 3630. Design by
      Florian Tschorsch and Björn Scheuermann; implementation by
      Florian Tschorsch.

  o Minor bugfixes:
    - Change an integer overflow check in the OpenBSD_Malloc code so
      that GCC is less likely to eliminate it as impossible. Patch
      from Mansour Moufid. Fixes bug 4059.

  o Minor bugfixes (usability):
    - Downgrade log messages about circuit timeout calibration from
      "notice" to "info": they don't require or suggest any human
      intervention. Patch from Tom Lowenthal. Fixes bug 4063;
      bugfix on 0.2.2.14-alpha.

  o Minor features (diagnostics):
    - When the system call to create a listener socket fails, log the
      error message explaining why. This may help diagnose bug 4027.
```

7. On September 30th, we released update Tor Browser Bundles which include Firefox 7.0.1 and Tor 0.2.2.33.

```
The bundles were originally uploaded with Firefox 7.0, but a fix was
```

```
quickly released, so the two changelogs have been merged in this post.

Tor Browser Bundle (2.2.33-2)

Windows fixes

    Begin building Vidalia with DEP/ASLR

OS X fixes

    Stop TBB from logging so much information to the system by only
    allowing dyld log library loads to syslog when it is in debug mode
    (closes: #4093)

General fixes and updates

    Update Firefox to 7.0.1
    Update OpenSSL to 1.0.0e (closes: #3996) (except for OS X)
    Update Tor to 0.2.2.33
    Update NoScript to 2.1.2.8
    Downgrade HTTPS Everywhere to 1.0.3, because we don't want stable
    TBBs to use development versions of extensions (closes: #4050)
```

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

- Karsten helped Christian fix BridgeDB that depended on a working exit list which we didn't have for a week or two. Helped fix GetTor statistics together with Christian and changed the graph parameter on metrics-web from 'bundle' to 'language'.
- George from Microsoft Research came up with a second model for a censorship detector that we need to look at and maybe deploy as a second beta on the metrics website. https://lists.torproject.org/pipermail/tor-dev/2011-September/002923.html
- Nick spent about a day evaluating Rizzo and Duong's sexy new SSL attack, BEAST, and writing a blog post about my findings, https://blog.torproject.org/blog/tor-and-beast-ssl-attack
- Tomas made some progress on Vidalia:
  - Backported the ServerPage new layout to the stable branch.
  - Improved Vidalia's authentication to Tor, so that it tries CookieAuth, and HashedAuth afterwards if the former fails.
  - Merged several branches that were for review for a while, although I didn't have any reviews.

  - Put tarballs for 0.2.15-rc and 0.3.1-rc in two tickets to get some testing before the actual release, so that we don't have those quick releases because I didn't catch a particular bug.
  - Started doing changes files, otherwise it's really hard to keep track of everything.

- Tomas worked on Thandy. Improved the Thp package implementation so that it's almost ready for a nice interface with Vidalia or whatever controller that uses it.

- Mike wrote up our analysis and deployed a patch for website fingerprinting. Website fingerprinting is the act of recognizing web traffic through surveillance despite the use of encryption or anonymizing software. The general idea is to leverage the fact that many web sites have specific fixed request patterns and response byte counts that are known beforehand. This information can be used to recognize your web traffic despite attempts at encryption or tunneling. Websites that have an abundance of static content and a fixed request structure tend to be vulnerable to this type of surveillance. Unfortunately, there is enough static content on most websites for this to be the case.

  The full post can be read at https://blog.torproject.org/blog/experimental-defense-website-traff

Hide Tor's network signature.

- Nick implemented proposal 176 – the 'new handshake' one that is supposed to make our protocol a little harder to fingerprint and make it require a little less in the way of crazy SSL hacking. It's going to take a little more poking to make it as good as I'd like, and it DEFINITELY needs more review, but at the moment it seems to work for me. https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/176-revising-handshake.txt

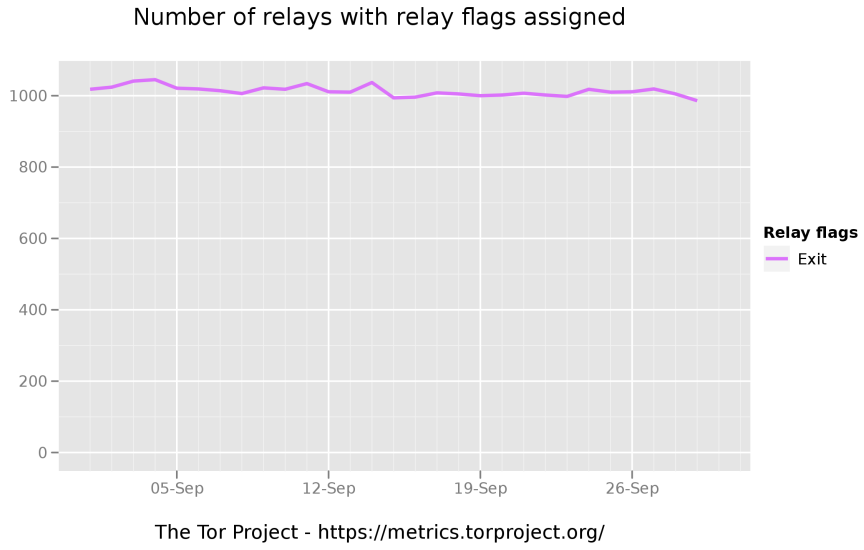
- On September 13th, Iran added a filter rule to their border routers that recognized Tor traffic and blocked it. Thanks to help from a variety of friends around the world, we quickly discovered how they were blocking it and released a new version of Tor that isn't blocked. Fortunately, the fix is on the relay side: that means once enough relays and bridges upgrade, the many tens of thousands of Tor users in Iran will resume being able to reach the Tor network, without needing to change their software.

  How did the filter work technically? Tor tries to make its traffic look like a web browser talking to an https web server, but if you look carefully enough you can tell some differences. In this case, the characteristic of Tor's SSL handshake they looked at was the expiry time for our SSL session certificates: we rotate the session certificates every two hours, whereas normal SSL certificates you get from a certificate authority typically last a year or more. The fix was to simply write a larger expiration time on the certificates, so our certs have more plausible expiry times.

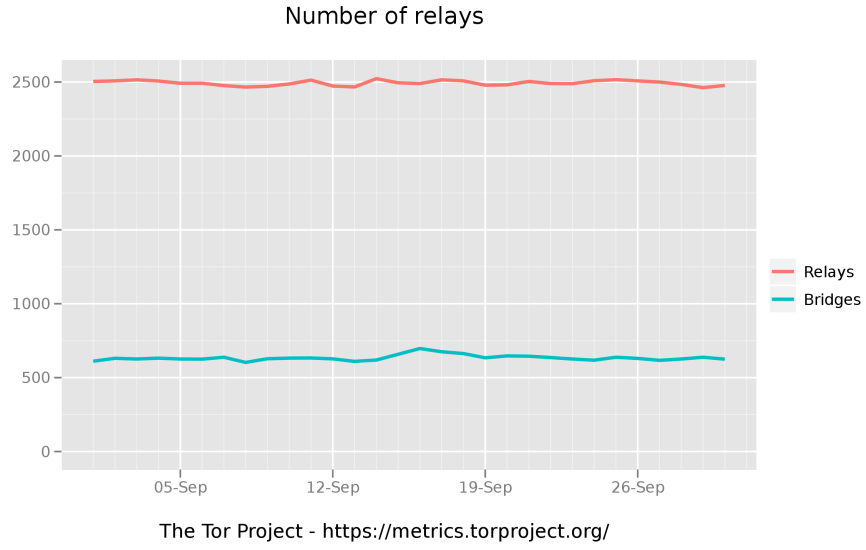
  See the full post at https://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fi

Grow the Tor network and user base. Outreach.

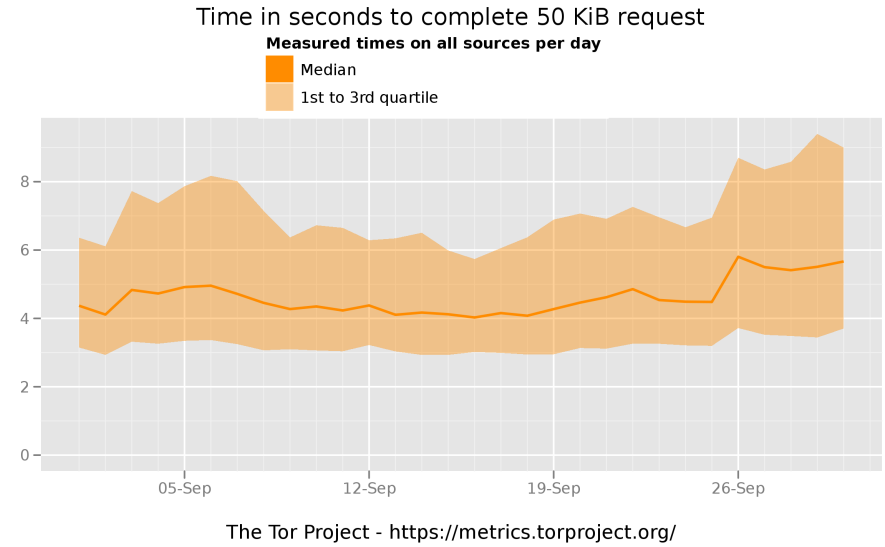
Measures of the Tor Network



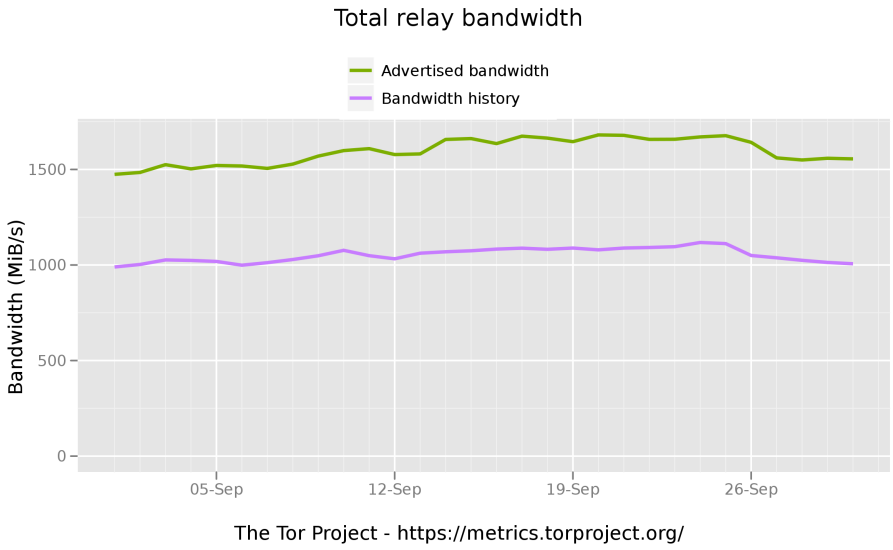
This graph shows the total quantity of exit relays in September 2011. There is a very slight reduction in relays over the month.



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



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Average latency has increased slightly to 6 seconds at the end of the month. This is likely due to the loss of the four very-high bandwidth blutmagie exit relays.



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. Jacob worked on the DigiNotar CA issues, https://blog.torproject.org/blog/diginotar-damage-discl You can see all of the issues related to DigiNotar at this url, https://blog.torproject.org/category/tags/ohdiginotaryoudidnt.
2. Jacob presented at a conference hosted by the Committee to Project Journalists, https://www.cpj.org/internet/2011/09/when-a-bug-fix-can-save-a-journalists-life.php#more.
3. Runa traveled to Ann Arbor to talk to Univerisity of Michigan about Telex and Tor.
4. Runa traveled to Los Angeles to help with a Persian News Network campaign to promote Tor.
5. Runa gave a talk about usability, security and Tor at Middlesex University in London.
6. Runa went to Hacks/Hackers London.
7. Andrew talked to the Florida Coalition Against Domestic Violence about data, network, and Internet security in the shelters. http://www.fcadv.org/.
8. Karen attended the United Nations Internet Governance Forum in Nairobi, Kenya. http://igf.or.ke/.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- Runa worked with some developers on finishing up an Amazon EC2/Cloud-based Tor relay image. http://torcloudservers.com/. This allows someone to simply use their AWS account to start up any number of Tor relay or bridge images.

Bridge relay and bridge authority work.

- Wrote a "Case study: Learning whether a Tor bridge is blocked by looking at its aggregate usage statistics, Part one." This was difficult to write, because we're lacking the data to say whether a bridge was in fact blocked or not. https://metrics.torproject.org/papers/blocking-2011-09-15.pdf

Scalability, load balancing, directory overhead, efficiency.

- Started reviewing the TorStatus code so that we can run it on yatei soon. We should take out some functionality that copies stuff that ExoneraTor and Metrics do better. Also, we need to fix a few bugs. Once that's done, we can deploy the new TorStatus as status.tpo.
- Rewrote large parts of ExoneraTor by creating a distinct database for it. The goal is to remove old non-aggregate data from the Metrics database. The new ExoneraTor allows searching for full days, not just timestamps, includes exit lists in its results, and can be extended to IPv6 quite easily once Tor supports it. Once I have some feedback saying the beta works for other people, I'll make it the new default. https://metrics.torproject.org/exonerator-beta.html

- Damian fixed some authentication bugs in TorCtl and arm, https://trac.torproject.org/projects/tor/ticket/3958.
- Juan Alcaine is helping with the arm RPMs, providing much needed testing and splitting arm from its dependencies. Next step is to get help from Erinn for uploading the arm/torctl rpms to the deb.tpo repos.
- Kamran has been working on a patch for exit locale selection in arm. It's functional, but not quite done yet.

Incentives work.

Nothing to report.

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

- Gettor updates to fix a number of bugs, updated text, and deployed the patches to production.

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

- Google Android's format is natively supported in Transifex, so we don't have to push and pull .po files for Orbot anymore (3987).
- Updated translations for the bridge db, gettor email system, vidalia, vidalia help files, vidalia installer, torbutton, and orbot.
- Updated translations in Arabic, German, Farsi, Hungarian, Spanish, French, Italian, Japanese, Korean, Swedish, Vietnamese, Polish, and Mandarin Chinese.
- At the end of September, after much discussion, we removed translated pages from the website. A full description of the change is available at https://blog.torproject.org/blog/whither-website-translations. We're working on a user manual that can be translated and included in documentation shipped with our software bundles.Of course, all of the software and related documentation will continue to be translated.