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


This report documents progress in July 2011.

# New releases, new hires, new funding

## New Releases

1. On July 7, we released Torbutton 1.4.0. The addon has been disabled on addons.mozilla.org. Our URL is now canonical.

   This release features support for Firefox 5.0, and has been tested against the vanilla release for basic functionality. However, it has not been audited for Network Isolation, State Separation, Tor Undiscoverability or Interoperability issues[1] due to toggling under Firefox 5.

   If you desire Torbutton functionality with Firefox 4/5, we recommend you download the Tor Browser Bundle 2.2.x alphas from https://www.torproject.org/dist/torbrowser/ or run Torbutton in its own separate Firefox profile.

   The reasons for this shift are explained here: https://blog.torproject.org/blog/toggle-or-not-toggle-end-torbutton

   If you find bugs specific to Firefox 5, toggling, and/or extension conflicts, file them under the component "Torbutton": https://trac.torproject.org/projects/tor/report/14

   Bugs that still apply to Tor Browser should be filed under component "TorBrowserButton": https://trac.torproject.org/projects/tor/report/39

   Bugs in the "Torbutton" component currently have no maintainer available to fix them. Feel free to step up.

   Here is the complete changelog:

```
 * bug 3101: Disable WebGL. Too many unknowns for now.
 * bug 3345: Make Google Captcha redirect work again.
 * bug 3399: Fix a reversed exception check found by arno.
 * bug 3177: Update torbutton to use new TorBrowser prefs.
 * bug 2843: Update proxy preferences window to support env var.
 * bug 2338: Force toggle at startup if tor is enabled
 * bug 3554: Make Cookie protections obey disk settings
 * bug 3441: Enable cookie protection UI by default.
 * bug 3446: We're Firefox 5.0, we swear.
 * bug 3506: Remove window resize event listener.
```

```
 * bug 1282: Set fixed window size for each new window.
 * bug 3508: Apply Stanford SafeCache patch (thanks Edward, Collin et
 * al).
 * bug 2361: Make about window work again on FF4+.
 * bug 3436: T(A)ILS was renamed to Tails.
 * bugfix: Fix a transparent context menu issue on Linux FF4+.
 * misc: Squelch exception from app launcher in error console.
 * misc: Make DuckDuckGo the default Google Captcha redirect
 * destination.
 * misc: Make it harder to accidentally toggle torbutton.
```

1. https://www.torproject.org/torbutton/en/design/requirements

2. On July 7th, we released the latest in the 0.2.2x release candidate branch.

   Tor 0.2.2.30-rc is the first release candidate for the Tor 0.2.2.x series. It fixes a few smaller bugs, but generally appears stable. Please test it and let us know whether it is!

```
Changes in version 0.2.2.30-rc - 2011-07-07
  o Minor bugfixes:
    - Send a SUCCEEDED stream event to the controller when a reverse
      resolve succeeded. Fixes bug 3536; bugfix on 0.0.8pre1. Issue
      discovered by katmagic.
    - Always NUL-terminate the sun_path field of a sockaddr_un before
      passing it to the kernel. (Not a security issue: kernels are
      smart enough to reject bad sockaddr_uns.) Found by Coverity;
      CID #428. Bugfix on Tor 0.2.0.3-alpha.
    - Don't stack-allocate the list of supplementary GIDs when we're
      about to log them. Stack-allocating NGROUPS_MAX gid_t elements
      could take up to 256K, which is way too much stack. Found by
      Coverity; CID #450. Bugfix on 0.2.1.7-alpha.
    - Add BUILDTIMEOUT_SET to the list returned by the 'GETINFO
      events/names' control-port command. Bugfix on 0.2.2.9-alpha;
      fixes part of bug 3465.
    - Fix a memory leak when receiving a descriptor for a hidden
      service we didn't ask for. Found by Coverity; CID #30. Bugfix
      on 0.2.2.26-beta.

  o Minor features:
    - Update to the July 1 2011 Maxmind GeoLite Country database.
```

3. On July 17th, we released the latest in the Arm relay controller, 1.4.3. This completes the codebase refactoring project that's been a year in the works and provides numerous performance, usability, and stability improvements...

```
* Relay Setup Wizard
Setting up a relay can be tricky for new users. In headless
```

```
environments this means navigating Tor's massive, user unfriendly man
page and even when Vidalia's an option it makes relatively poor exit
configurations. Starting arm before Tor now provides instructions for
auto-generating a good relay setup...

  a. Selection for what you'd like to be
      http://www.atagar.com/transfer/tmp/arm_wizard1.png
  b. Picking your relay options
      http://www.atagar.com/transfer/tmp/arm_wizard2.png
  c. Confirmation for the configuration it's making
      http://www.atagar.com/transfer/tmp/arm_wizard3.png

* Menu Interface
All of arm's capabilities are now available via a simple menu interface.
http://www.atagar.com/transfer/tmp/arm_menu.png

* Arm Gui Prototype
Over this summer Kamran Khan has been working on a GTK frontend for
arm as part of Google Summer of Code. The initial prototype is ready!
http://inspirated.com/2011/06/28/summer-of-code-progress-graphs-logs-and-acid

* Performance Improvements
Several arm and TorCtl performance fixes providing a 83% faster
startup time, 12% lower memory usage, and instantaneous shutdown.

* Improved Platform Support
Vastly better support for Mac OSX. Arm has also been backported to
Debian Squeeze and Ubuntu Lucid / Maverick.
http://packages.debian.org/squeeze-backports/tor-arm
https://bugs.launchpad.net/maverick-backports/+bug/721886

* ... etc
Options for requesting a new identity, shutting down Tor, reconnecting
if Tor's been restarted and many, many bugfixes.
http://www.atagar.com/arm/releaseNotes.php#1.4.3
```

4. On July 18th, we released the latest in the experimental branch of Tor 0.2.3.x-alpha.

   Tor 0.2.3.2-alpha introduces two new experimental features: microdescriptors and pluggable transports. It also continues cleaning up a variety of recently introduced features. We are not producing packages for the 0.2.3.x branch until 0.2.2.x is the new -stable. Three sets of packages is beyond our capabilities to create and display right now.

```
Changes in version 0.2.3.2-alpha - 2011-07-18
  o Major features:
    - Clients can now use microdescriptors instead of regular
```

```
      descriptors
      to build circuits. Microdescriptors are authority-generated
      summaries of regular descriptors' contents, designed to change
      very rarely (see proposal 158 for details). This feature is
      designed to save bandwidth, especially for clients on slow
internet
      connections. It's off by default for now, since nearly no caches
      support it, but it will be on-by-default for clients in a future
      version. You can use the UseMicrodescriptors option to turn it on.
    - Tor clients using bridges can now be configured to use a separate
      'transport' proxy for each bridge. This approach helps to resist
      censorship by allowing bridges to use protocol obfuscation
      plugins. It implements part of proposal 180. Implements ticket
2841.
    - While we're trying to bootstrap, record how many TLS connections
      fail in each state, and report which states saw the most failures
      in response to any bootstrap failures. This feature may speed up
      diagnosis of censorship events. Implements ticket 3116.

  o Major bugfixes (on 0.2.3.1-alpha):
    - When configuring a large set of nodes in EntryNodes (as with
      'EntryNodes {cc}' or 'EntryNodes 1.1.1.1/16'), choose only a
      random subset to be guards, and choose them in random
      order. Fixes bug 2798.
    - Tor could crash when remembering a consensus in a non-used
      consensus
      flavor without having a current consensus set. Fixes bug 3361.
    - Comparing an unknown address to a microdescriptor's shortened exit
      policy would always give a "rejected" result. Fixes bug 3599.
    - Using microdescriptors as a client no longer prevents Tor from
      uploading and downloading hidden service descriptors. Fixes
      bug 3601.

  o Minor features:
    - Allow nameservers with IPv6 address. Resolves bug 2574.
    - Accept attempts to include a password authenticator in the
      handshake, as supported by SOCKS5. This handles SOCKS clients that
      don't know how to omit a password when authenticating. Resolves
      bug 1666.
    - When configuring a large set of nodes in EntryNodes, and there are
      enough of them listed as Guard so that we don't need to consider
      the non-guard entries, prefer the ones listed with the Guard flag.
    - Check for and recover from inconsistency in the microdescriptor
      cache. This will make it harder for us to accidentally free a
      microdescriptor without removing it from the appropriate data
```

```
    structures. Fixes issue 3135; issue noted by "wanoskarnet".
  - Log SSL state transitions at log level DEBUG, log domain
    HANDSHAKE. This can be useful for debugging censorship events.
    Implements ticket 3264.
  - Add port 6523 (Gobby) to LongLivedPorts. Patch by intrigeri;
    implements ticket 3439.

o Minor bugfixes (on 0.2.3.1-alpha):
  - Do not free all general-purpose regular descriptors just
    because microdescriptor use is enabled. Fixes bug 3113.
  - Correctly link libevent_openssl when --enable-static-libevent
    is passed to configure. Fixes bug 3118.
  - Bridges should not complain during their heartbeat log messages
    that
    they are unlisted in the consensus: that's more or less the point
    of being a bridge. Fixes bug 3183.
  - Report a SIGNAL event to controllers when acting on a delayed
    SIGNAL NEWNYM command. Previously, we would report a SIGNAL
    event to the controller if we acted on a SIGNAL NEWNYM command
    immediately, and otherwise not report a SIGNAL event for the
    command at all. Fixes bug 3349.
  - Fix a crash when handling the SIGNAL controller command or
    reporting ERR-level status events with bufferevents enabled. Found
    by Robert Ransom. Fixes bug 3367.
  - Always ship the tor-fw-helper manpage in our release tarballs.
    Fixes bug 3389. Reported by Stephen Walker.
  - Fix a class of double-mark-for-close bugs when bufferevents
    are enabled. Fixes bug 3403.
  - Update tor-fw-helper to support libnatpmp-20110618. Fixes bug
    3434.
  - Add SIGNAL to the list returned by the 'GETINFO events/names'
    control-port command. Fixes part of bug 3465.
  - Prevent using negative indices during unit test runs when
    read_all()
    fails. Spotted by coverity.
  - Fix a rare memory leak when checking the nodelist without it being
    present. Found by coverity.
  - Only try to download a microdescriptor-flavored consensus from
    a directory cache that provides them.

o Minor bugfixes (on 0.2.2.x and earlier):
  - Assert that hidden-service-related operations are not performed
    using single-hop circuits. Previously, Tor would assert that
    client-side streams are not attached to single-hop circuits,
    but not that other sensitive operations on the client and service
```

```
    side are not performed using single-hop circuits. Fixes bug 3332;
    bugfix on 0.0.6.
  - Don't publish a new relay descriptor when we reload our onion key,
    unless the onion key has actually changed. Fixes bug 3263 and
    resolves another cause of bug 1810. Bugfix on 0.1.1.11-alpha.
  - Allow GETINFO fingerprint to return a fingerprint even when
    we have not yet built a router descriptor. Fixes bug 3577;
    bugfix on 0.2.0.1-alpha.
  - Make 'tor --digests' list hashes of all Tor source files. Bugfix
    on 0.2.2.4-alpha; fixes bug 3427.

o Code simplification and refactoring:
  - Use tor_sscanf() in place of scanf() in more places through the
    code. This makes us a little more locale-independent, and
    should help shut up code-analysis tools that can't tell
    a safe sscanf string from a dangerous one.
  - Use tt_assert(), not tor_assert(), for checking for test failures.
    This makes the unit tests more able to go on in the event that
    one of them fails.
  - Split connection_about_to_close() into separate functions for each
    connection type.

o Build changes:
  - On Windows, we now define the _WIN32_WINNT macros only if they
    are not already defined. This lets the person building Tor decide,
    if they want, to require a later version of Windows.
```

5. On July 28th, we released an updated Orweb for Android devices. The big news is that you can use this on any Android device without root. Just install Orbot, connect to Tor, then install this, and you are ready to browse like an onion.

   The main issue we are concerned about tracking down is DNS leaks with how we are proxying. We have to use HTTP/S proxy support for now, but it does seem to be resolving names via Tor, since .onion addresses do work. From here, I'll be talking more with mikeperry about all of the possible things we can do to further lockdown webkit, which is the basis for rweb.

   You can grab the direct binary and sig from: https://github.com/guardianproject/Orweb/downloads

   Orweb v2 (0.2.1) - now supports Android 2.x and 3.x

   Use with Orbot on any Android device without any complex configuration. It just works right out of the box.. err, market! Also blocks flash and optionally javascript, and other malicious downloads. Integrates directly with DuckDuckGo.com's search hidden service for private, anonymous searching.

   updated market page: https://market.android.com/details?id=info.guardianproject.browserfeature=search$_r$

Directly binary download: https://github.com/guardianproject/Orweb/Orwebv2-280711-0.2.1.b.apk/qr$_c$*ode*

Source and project: https://github.com/guardianproject/Orweb/tree/v0.2.1

Orweb is a privacy enhanced web browser that support proxies. When used with the Orbot (Tor on Android) app, this web browser provides enhanced privacy features. Through Tor, it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked. It also blocks cookies, keeps no local history, disables Flash, and requires only Internet permissions, keeping you safe from malicious content. Finally, beyond Tor, it can support any HTTP proxy server.

```
What's in this version:
- added Android 2.x and 3.x support
- new localization / languages
- integrated DuckDuckGo.com search engine
- new icon!
```

6. On July 13th, all of the alpha Tor Browser Bundles have been updated to the latest Tor 0.2.2.30-rc, and the Windows stable bundle has been updated with the latest Firefox 3.6.19.

   The experimental bundles also now contain Firefox 5 and Polipo has been removed from all of them.

```
Firefox 3.6 Tor Browser Bundles

Windows bundle
1.3.26: Released 2011-07-13

    Update Firefox to 3.6.19
    Update HTTPS-Everywhere to 1.0.0development.4
    Update Libevent to 2.0.12-stable

OS X bundle
1.1.22: Released 2011-07-13

    Update Tor to 0.2.2.30-rc
    Update Firefox to 3.6.19
    Update HTTPS-Everywhere to 1.0.0development.4
    Update NoScript to 2.1.1.2

Linux bundles
1.1.12: Released 2011-07-13

    Update Tor to 0.2.2.30-rc
    Update Firefox to 3.6.19
    Update HTTPS-Everywhere to 1.0.0development.4
    Update NoScript to 2.1.1.2

Firefox 4 Tor Browser Bundles
```

```
Tor Browser Bundle (2.2.30-1)

    Update Tor to 0.2.2.30-rc
    Update Firefox to 5.0.1
    Update Torbutton to 1.4.0
    Update Libevent to 2.0.12-stable
    Update HTTPS-Everywhere to 1.0.0development.4
    Update NoScript to 2.1.1.2
```

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

- The beta censorship detector is deployed. The current BETA version of the censorship detector analyzes the estimated daily user numbers from all countries and from a given country to calculate an estimated range of daily users from that country. Whenever the user number of a country falls outside this range, the censorship detector marks the event either as downturn, which is a possible censorship event, or upturn, which is a potential end of censorship. The BETA version of the algorithm still needs some fine-tuning to reduce the number of false positives." The next step will be to add a tech report or short description about how the detector works. Here's an example graph that contains upturns in blue and downturns in red: https://metrics.torproject.org/users.html?graph=direct-users&start=2011-01-01&end=2011-08-04&country=ly&events=on&dpi=72#direct-users

- Started reviewing patches to the bridge database infrastructure. A big change will be supporting reCAPTCHA for bridge address distribution. A challenge is to use reCAPTCHA technology without giving Google all of the IP addresses of users looking for bridges.

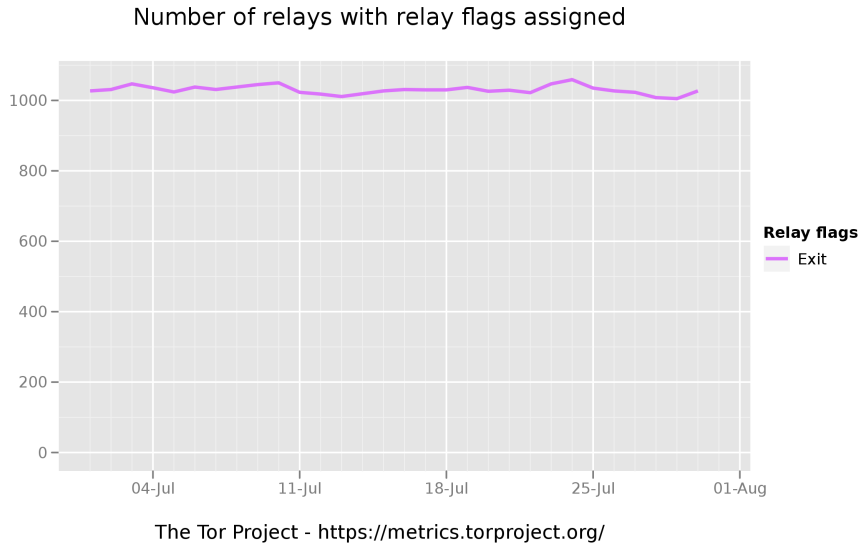
- bridges.torproject.org is accessible via IPv6 directly.

## Hide Tor's network signature.

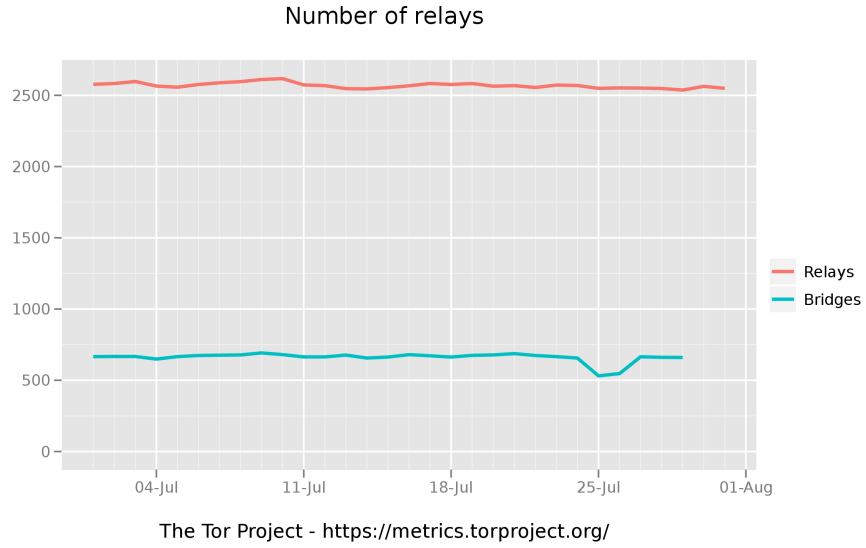
- Progress on obfsproxy continues. It's now more portable, compiling on OS X, linuxes, and MS Windows. Signal handling matches the proposed 180 Pluggable Transport spec, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/180-pluggable-transport.txt. Updated the HOWTO document for users, https://gitweb.torproject.org/obfsproxy.git/blob/HEAD:/doc/tor-obfs-howto.txt.

# Grow the Tor network and user base. Outreach.

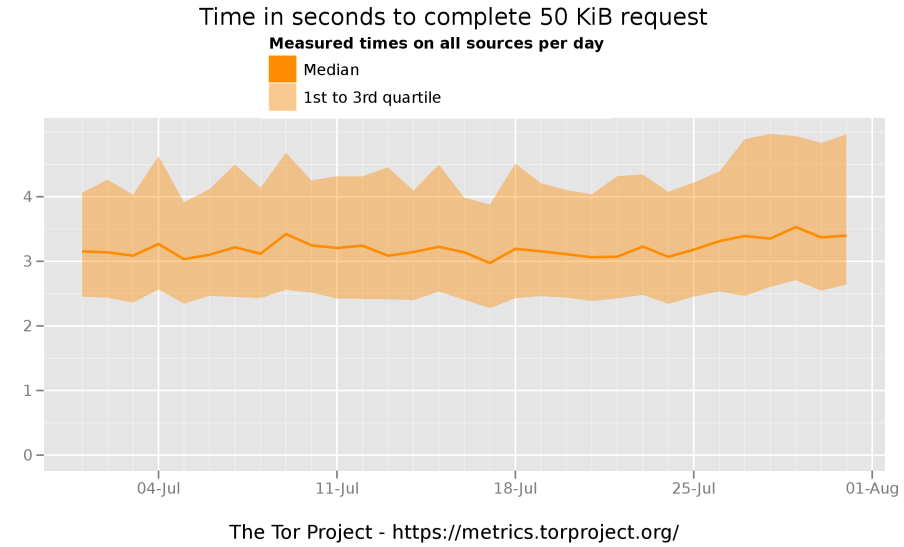
## Measures of the Tor Network



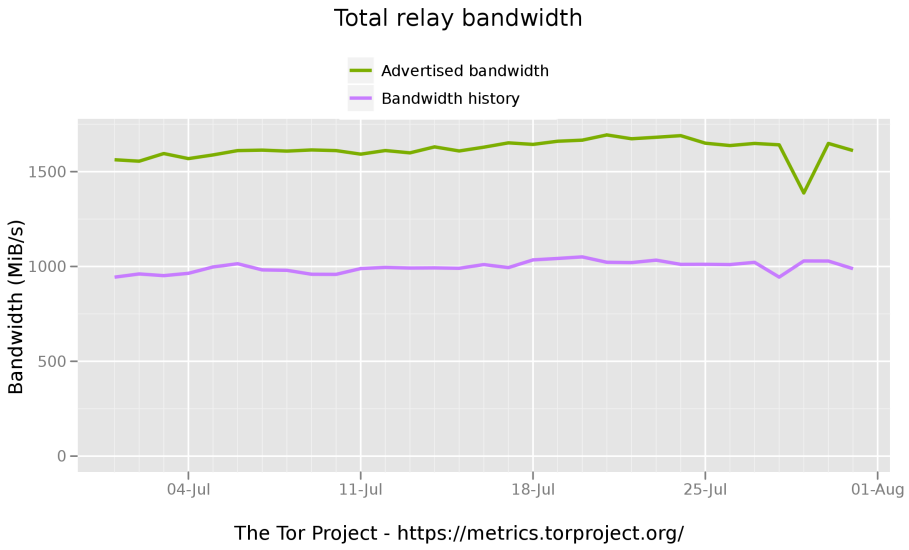

This graph shows the total quantity of exit relays in July 2011. We seem to have kept most of our relays since the bump due to the EFF Tor challenge started in May 2011.




This graph shows the total quantity of relays and the total quantity of bridges in July 2011. We seem to have kept most of our relays since the bump due to the EFF Tor Challenge started in May 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. 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 1.6GBps (12.8 Gbps) of bandwidth available.

## Outreach and Advocacy

1. Jacob attended Recon in Montreal.

2. Jacob spoke at something
3. Tor held the annual dev meeting, this year sponsored by the University of Waterloo.
4. Many members of Tor attended the Privacy Enhancing Technology Symposium at the University of Waterloo, http://petsymposium.org/2011/.
5. Andrew and Karen spoke to staffers from Senators Casey, Menendez, and Kirk about Internet circumvention and privacy.
6. Andrew and Karen spoke at Radio Liberty's office to a number of press, foundations, and think tanks about Internet censorship and privacy.
7. Andrew and Karen spoke to the Helsinki Commission about Internet censorship and privacy.
8. Runa gave a talk about Tor at the University College of London's School of Oriental and African Studies, http://www.soas.ac.uk/.
9. Roger was a panelist on the PETS 'ethics of Tor research' panel.

## Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- See the Tor Browser Bundle updates in the first section. These include new bundles based on Firefox 5.

## Bridge relay and bridge authority work.

Started a design for bridges should pick their own guard hop to address some potential risks to clients of bridges.

## Scalability, load balancing, directory overhead, efficiency.

- Thanks to an updated Coverity scan, fixed a number of bugs. These are seen in the tor release notes as attributed to Coverity.
- Fixed a number of microdescriptor bugs. Microdescriptors in the master branch are now on-by-default for clients.

## Incentives work.

Nothing to report.

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

Nothing to report.

## Footprints from Tor Browser Bundle.

Nothing to report.

## Translation work, ultimately a browser-based approach.

- Had a conf call with a group of translators in DC who are working on both Arabic and Persian translations of the website. We believe they will finish translating the website by the end of August.
- Fixed a problem with the German .wmi files (3526), included updated docs/de/sidenav.wmi (3538), included a German video on tor-doc-windows.html.de (3532), decided to include the English video as well (3581), included pt_BR translations of two .wmi files (3568), updated Makefile.common to include pt-br when building the website (3579), updated Makefile.common and include/perl-globals.wmi to include more languages when building the website (3625).
- Configured stunnel to work with the transifex-client (3576). This means that we can connect to the Transifex server using HTTPS, while also verifying the certificate.
- Updated translations for German, Arabic, Farsi, Russian, Italian, French, Finnish, Vietnamese, and Chinese.