From: Andrew Lewman, Executive Director
To: The Tor Community
Date: February 12, 2012

This report documents progress in January 2012.

New releases, new hires, new funding

New Releases

1. On January 22, we released Tor 0.2.3.11-alpha.

   Tor 0.2.3.11-alpha marks feature-freeze for the 0.2.3 tree. It deploys the last step of the plan to limit maximum circuit length, includes a wide variety of hidden service performance and correctness fixes, works around an OpenSSL security flaw if your distro is too stubborn to upgrade, and fixes a bunch of smaller issues.

   Note that the tarball and git tags are signed by Roger's newer (4096 bit) gpg key, 0x19F78451.

```
Changes in version 0.2.3.11-alpha - 2012-01-22
  o Major features:
    - Now that Tor 0.2.0.x is completely deprecated, enable the final
      part of "Proposal 110: Avoiding infinite length circuits" by
      refusing all circuit-extend requests that do not use a relay_early
      cell. This change helps Tor resist a class of denial-of-service
      attacks by limiting the maximum circuit length.
    - Adjust the number of introduction points that a hidden service
      will try to maintain based on how long its introduction points
      remain in use and how many introductions they handle. Fixes
      part of bug 3825.
    - Try to use system facilities for enumerating local interface
      addresses, before falling back to our old approach (which was
      binding a UDP socket, and calling getsockname() on it). That
      approach was scaring OS X users whose draconian firewall
      software warned about binding to UDP sockets, regardless of
      whether packets were sent. Now we try to use getifaddrs(),
      SIOCGIFCONF, or GetAdaptersAddresses(), depending on what the
      system supports. Resolves ticket 1827.

  o Major security workaround:
    - When building or running with any version of OpenSSL earlier
    than 0.9.8s or 1.0.0f, disable SSLv3 support. These OpenSSL
    versions have a bug (CVE-2011-4576) in which their block cipher
    padding includes uninitialized data, potentially leaking sensitive
    information to any peer with whom they make a SSLv3 connection. Tor
    does not use SSL v3 by default, but a hostile client or server
    could force an SSLv3 connection in order to gain information that
    they shouldn't have been able to get. The best solution here is to
    upgrade to OpenSSL 0.9.8s or 1.0.0f (or later). But when building
    or running with a non-upgraded OpenSSL, we disable SSLv3 entirely
    to make sure that the bug can't happen.

o Major bugfixes:
  - Fix the SOCKET_OK test that we use to tell when socket
    creation fails so that it works on Win64. Fixes part of bug 4533;
    bugfix on 0.2.2.29-beta. Bug found by wanoskarnet.
  - Correct our replacements for the timeradd() and timersub() functions
    on platforms that lack them (for example, Windows). The timersub()
    function is used when expiring circuits, while timeradd() is
    currently unused. Bug report and patch by Vektor. Fixes bug 4778;
    bugfix on 0.2.2.24-alpha and 0.2.3.1-alpha.
  - Do not use OpenSSL 1.0.0's counter mode: it has a critical bug
    that was fixed in OpenSSL 1.0.0a. We test for the counter mode
    bug at runtime, not compile time, because some distributions hack
    their OpenSSL to mis-report its version. Fixes bug 4779; bugfix
    on 0.2.3.9-alpha. Found by Pascal.

o Minor features (controller):
  - Use absolute path names when reporting the torrc filename in the
    control protocol, so a controller can more easily find the torrc
    file. Resolves bug 1101.
  - Extend the control protocol to report flags that control a circuit's
    path selection in CIRC events and in replies to 'GETINFO
    circuit-status'. Implements part of ticket 2411.
  - Extend the control protocol to report the hidden service address
    and current state of a hidden-service-related circuit in CIRC
    events and in replies to 'GETINFO circuit-status'. Implements part
    of ticket 2411.
  - When reporting the path to the cookie file to the controller,
    give an absolute path. Resolves ticket 4881.
  - Allow controllers to request an event notification whenever a
    circuit is cannibalized or its purpose is changed. Implements
    part of ticket 3457.
  - Include the creation time of a circuit in CIRC and CIRC2
    control-port events and the list produced by the 'GETINFO
    circuit-status' control-port command.
```

```
o Minor features (directory authorities):
  - Directory authorities now reject versions of Tor older than
    0.2.1.30, and Tor versions between 0.2.2.1-alpha and 0.2.2.20-alpha
    inclusive. These versions accounted for only a small fraction of
    the Tor network, and have numerous known security issues. Resolves
    issue 4788.
  - Authority operators can now vote for all relays in a given
    set of countries to be BadDir/BadExit/Invalid/Rejected.
  - Provide two consensus parameters (FastFlagMinThreshold and
    FastFlagMaxThreshold) to control the range of allowable bandwidths
    for the Fast directory flag. These allow authorities to run
    experiments on appropriate requirements for being a "Fast" node.
    The AuthDirFastGuarantee config value still applies.
  - Document the GiveGuardFlagTo_CVE_2011_2768_VulnerableRelays
    directory authority option (introduced in Tor 0.2.2.34).

o Minor features (other):
  - Don’t disable the DirPort when we cannot exceed our AccountingMax
    limit during this interval because the effective bandwidthrate is
    low enough. This is useful in a situation where AccountMax is only
    used as an additional safeguard or to provide statistics.
  - Prepend an informative header to generated dynamic_dh_params files.
  - If EntryNodes are given, but UseEntryGuards is set to 0, warn that
    EntryNodes will have no effect. Resolves issue 2571.
  - Log more useful messages when we fail to disable debugger
    attachment.
  - Log which authority we’re missing votes from when we go to fetch
    them from the other auths.
  - Log (at debug level) whenever a circuit’s purpose is changed.
  - Add missing documentation for the MaxClientCircuitsPending,
    UseMicrodescriptors, UserspaceIOCPBuffers, and
    _UseFilteringSSLBufferevents options, all introduced during
    the 0.2.3.x series.
  - Update to the January 3 2012 Maxmind GeoLite Country database.

o Minor bugfixes (hidden services):
  - Don’t close hidden service client circuits which have almost
    finished connecting to their destination when they reach
    the normal circuit-build timeout. Previously, we would close
    introduction circuits which are waiting for an acknowledgement
    from the introduction point, and rendezvous circuits which have
    been specified in an INTRODUCE1 cell sent to a hidden service,
    after the normal CBT. Now, we mark them as ’timed out’, and launch
    another rendezvous attempt in parallel. This behavior change can
```

be disabled using the new CloseHSClientCircuitsImmediatelyOnTimeout option. Fixes part of bug 1297; bugfix on 0.2.2.2-alpha.

- Don't close hidden-service-side rendezvous circuits when they reach the normal circuit-build timeout. This behaviour change can be disabled using the new CloseHSServiceRendCircuitsImmediatelyOnTimeout option. Fixes the remaining part of bug 1297; bugfix on 0.2.2.2-alpha.
- Make sure we never mark the wrong rendezvous circuit as having had its introduction cell acknowleged by the introduction-point relay. Previously, when we received an INTRODUCE_ACK cell on a client-side hidden-service introduction circuit, we might have marked a rendezvous circuit other than the one we specified in the INTRODUCE1 cell as INTRO_ACKED, which would have produced a warning message and interfered with the hidden service connection-establishment process. Fixes bug 4759; bugfix on 0.2.3.3-alpha, when we added the stream-isolation feature which might cause Tor to open multiple rendezvous circuits for the same hidden service.
- Don't trigger an assertion failure when we mark a new client-side hidden-service introduction circuit for close during the process of creating it. Fixes bug 4796; bugfix on 0.2.3.6-alpha. Reported by murb.

o Minor bugfixes (log messages):

- Correctly spell "connect" in a log message on failure to create a controlsocket. Fixes bug 4803; bugfix on 0.2.2.26-beta and 0.2.3.2-alpha.
- Fix a typo in a log message in rend_service_rendezvous_has_opened(). Fixes bug 4856; bugfix on Tor 0.0.6.
- Fix the log message describing how we work around discovering that our version is the ill-fated OpenSSL 0.9.8l. Fixes bug 4837; bugfix on 0.2.2.9-alpha.
- When logging about a disallowed .exit name, do not also call it an "invalid onion address". Fixes bug 3325; bugfix on 0.2.2.9-alpha.

o Minor bugfixes (build fixes):

- During configure, detect when we're building with clang version 3.0 or lower and disable the -Wnormalized=id and -Woverride-init CFLAGS. clang doesn't support them yet.
- During configure, search for library containing cos function as libm lives in libcore on some platforms (BeOS/Haiku). Linking against libm was hard-coded before. Fixes the first part of bug 4727; bugfix on 0.2.2.2-alpha. Patch and analysis by Martin Hebnes Pedersen.
- Detect attempts to build Tor on (as yet hypothetical) versions

```
    of Windows where sizeof(intptr_t) != sizeof(SOCKET). Partial
    fix for bug 4533. Bugfix on 0.2.2.28-beta.
  - Preprocessor directives should not be put inside the arguments
    of a macro. This would break compilation with GCC releases prior
    to version 3.3. We would never recommend such an old GCC version,
    but it is apparently required for binary compatibility on some
    platforms (namely, certain builds of Haiku). Fixes the other part
    of bug 4727; bugfix on 0.2.3.3-alpha. Patch and analysis by Martin
    Hebnes Pedersen.

o Minor bugfixes (other):
  - Older Linux kernels erroneously respond to strange nmap behavior
    by having accept() return successfully with a zero-length
    socket. When this happens, just close the connection. Previously,
    we would try harder to learn the remote address: but there was
    no such remote address to learn, and our method for trying to
    learn it was incorrect. Fixes bugs 1240, 4745, and 4747. Bugfix
    on 0.1.0.3-rc. Reported and diagnosed by "r1eo".
  - Fix null-pointer access that could occur if TLS allocation failed.
    Fixes bug 4531; bugfix on 0.2.0.20-rc. Found by "troll_un". This was
    erroneously listed as fixed in 0.2.3.9-alpha, but the fix had
    accidentally been reverted.
  - Fix our implementation of crypto_random_hostname() so it can’t
    overflow on ridiculously large inputs. (No Tor version has ever
    provided this kind of bad inputs, but let’s be correct in depth.)
    Fixes bug 4413; bugfix on 0.2.2.9-alpha. Fix by Stephen Palmateer.
  - Find more places in the code that should have been testing for
    invalid sockets using the SOCKET_OK macro. Required for a fix
    for bug 4533. Bugfix on 0.2.2.28-beta.
  - Fix an assertion failure when, while running with bufferevents, a
    connection finishes connecting after it is marked for close, but
    before it is closed. Fixes bug 4697; bugfix on 0.2.3.1-alpha.
  - test_util_spawn_background_ok() hardcoded the expected value
    for ENOENT to 2. This isn’t portable as error numbers are
    platform specific, and particularly the hurd has ENOENT at
    0x40000002. Construct expected string at runtime, using the correct
    value for ENOENT. Fixes bug 4733; bugfix on 0.2.3.1-alpha.
  - Reject attempts to disable DisableDebuggerAttachment while Tor is
    running. Fixes bug 4650; bugfix on 0.2.3.9-alpha.
  - Use an appropriate-width type for sockets in tor-fw-helper on
    win64. Fixes bug 1983 at last. Bugfix on 0.2.3.9-alpha.

o Feature removal:
  - When sending or relaying a RELAY_EARLY cell, we used to convert
    it to a RELAY cell if the connection was using the v1 link
```

```
        protocol. This was a workaround for older versions of Tor, which
        didn't handle RELAY_EARLY cells properly. Now that all supported
        versions can handle RELAY_EARLY cells, and now that we're enforcing
        the "no RELAY_EXTEND commands except in RELAY_EARLY cells" rule,
        remove this workaround. Addresses bug 4786.

    o Code simplifications and refactoring:
      - Use OpenSSL's built-in SSL_state_string_long() instead of our
        own homebrewed ssl_state_to_string() replacement. Patch from
        Emile Snyder. Fixes bug 4653.
      - Use macros to indicate OpenSSL versions, so we don't need to worry
        about accidental hexadecimal bit shifts.
      - Remove some workaround code for OpenSSL 0.9.6 (which is no longer
        supported).
      - Convert more instances of tor_snprintf+tor_strdup into tor_asprintf.
      - Use the smartlist_add_asprintf() alias more consistently.
      - Use a TOR_INVALID_SOCKET macro when initializing a socket to an
        invalid value, rather than just -1.
      - Rename a handful of old identifiers, mostly related to crypto
        structures and crypto functions. By convention, our "create an
        object" functions are called "type_new()", our "free an object"
        functions are called "type_free()", and our types indicate that
        they are types only with a final "_t". But a handful of older
        types and functions broke these rules, with function names like
        "type_create" or "subsystem_op_type", or with type names like
        type_env_t.
```

2. On January 10, released a new version of Orbot, Tor for Android

```
1.0.7
- reduced data folder size by making geoip file only installed on demand
- added options for turning of persistent notification
- enabled access to localhost ports for SOCKS, HTTP, etc even when transproxy is on
- improved handling of tor and privoxy binary upgrades
- updated openssl to 1.0.0f to address recent SSLv3 threat
- check for root mode uses "which su" command and does not look for Superuser.apk
- changed tor binary res/raw storage mechanism to use the "mp3" file ext trick
```

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

- George helped people setup bridges with obfsproxy. He currently has two bridge addresses that can be used with obfsproxy/obfs2.

- George tried to push obfsproxy deployment a bit by scheduling an obfsproxy 'alpha' release, https://trac.torproject.org/projects/tor/ticket/4926, making a ticket about a Pluggable Transport Tor Bundle https://trac.torproject.org/projects/tor/ticket/4927, and wrote some implementation thoughts.

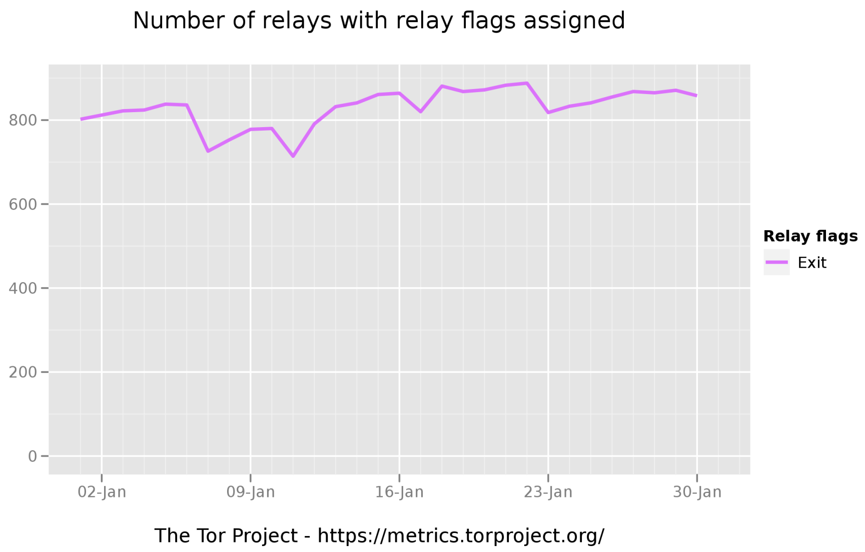
- George and Roger wrote a website for obfsproxy, https://www.torproject.org/projects/obfsproxy.html.en.
- George made a small python script which geographically visualized Chinese probers using their IP and a GeoIP database, https://gitorious.org/prober_visualization. Unfortunately, he hasn't had the time to analyze whether the concentration points in the map are caused by the GeoIP database being non-robust/bad/lying.

Hide Tor's network signature.

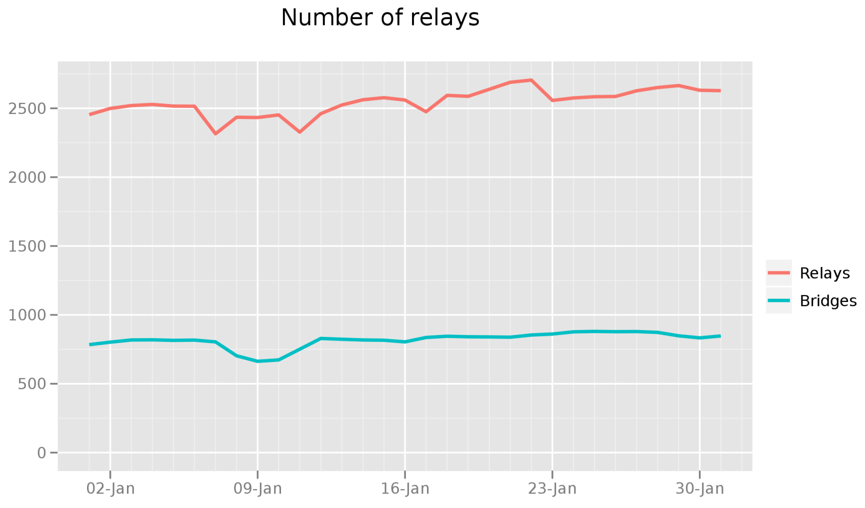
George spent some time talking to the authors of the morpher paper.

Grow the Tor network and user base. Outreach.

Measures of the Tor Network

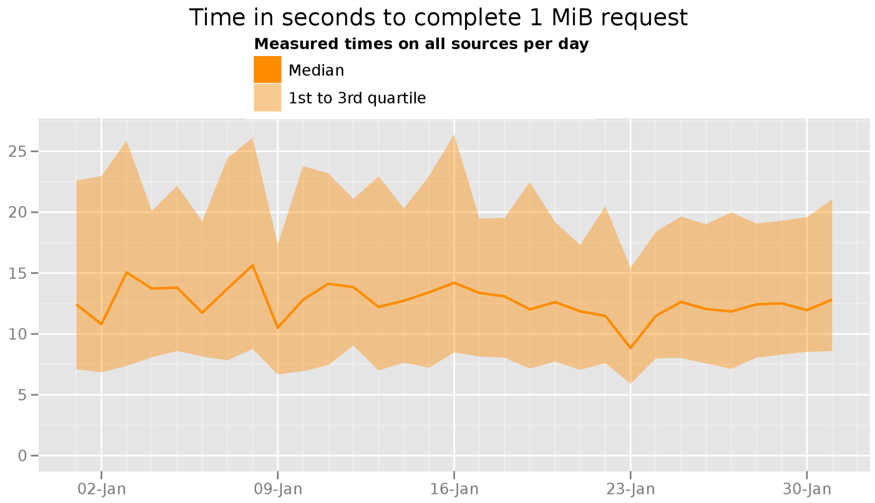


This graph shows the total quantity of exit relays in January 2012.



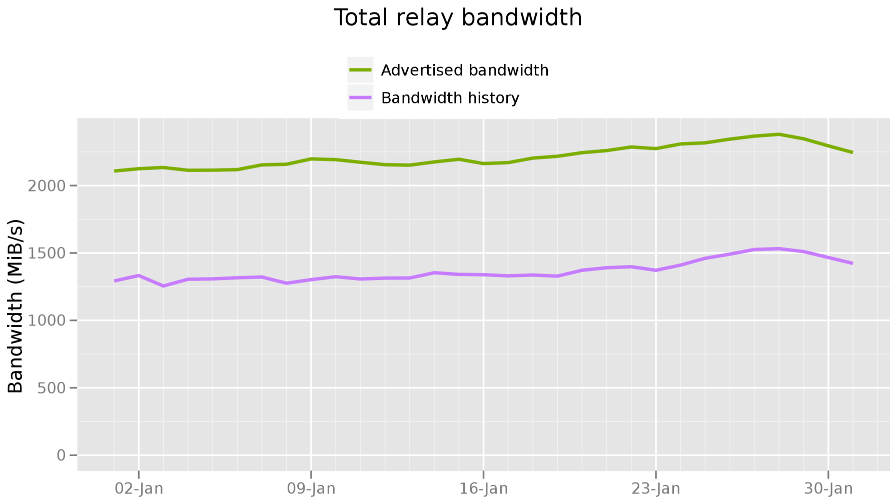
The Tor Project - https://metrics.torproject.org/

This graph shows the total quantity of relays and the total quantity of bridges in January 2012.



The Tor Project - https://metrics.torproject.org/

This graphs shows how many seconds it took to complete a 1 megabyte download from a standard Tor client. We changed from the 50KB download metric to 1 MB because this better reflects real-world web browsing and rich media currently seen on the Internet. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden.



The Tor Project - https://metrics.torproject.org/

This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. Maintaining a capacity of 2.6 GBps (21.0 Gbps) available with 1.47 GBps (11.8 Gbps) used.

Outreach and Advocacy

1. Jake gave a talk at LCA 2012 in Australia. A video of his talk is available, https://www.youtube.com/watch?v=GMN236OLM_U.

2. Andrew summarized some real-time support experiences over the past few months. The original email can be found at https://lists.torproject.org/pipermail/tor-talk/2012-January/022893.html. The full email is below.

   ”It’s been a while since I relayed phone support experiences. Six months ago we listed our phone number on the ’contact us’ page. See the experiences of the first month or so at ’talking to users’, https://lists.torproject.org/pipermail/tor-talk/2011-July/020838.html

   There have been a few tweaks and changes to the live/phone support. It is still free, but it is clear there is a demand for paid support and consulting. The notable changes are adding jitsi for supporting otr and zrtp-encrypted voip and video chats. Jitsi also works for anything xmpp-based, such as google chat and voice. Also, publishing ’office hours’ for the world concentrates the calls to predictable hours.

   We also setup a ticketing system to track email support requests.

   tl;dr, users call, have questions, some calls are short, some calls are long. maybe we should offer a paid support option.

   First, the phone support FAQ list:

   1. What is Aurora? 2. Why is Tor slower than x (vpn, proxy, native internet, psiphon, etc)? 3. Why is running a bridge/relay so complex? I want to help people, not get a degree

in computer science. 4. I want watch videos on the internet, how do I do this? 4a. Ok, not in tbb. How do I configure safari/chrome/ie/opera to use tor so I can watch videos on the internet? 4b. why is this self-configuration so complex? 5. My anti-virus/anti-malware/spyware-detector tells me tor.exe and vidalia.exe are unknown and unsafe. what do I do? 6. Can you explain to me online privacy and anonymity and how tor helps make these happen?

Second, there are three calls that stand out over the past six months.

The first is actually not a single call, but a series of them.

'I'm an (animal rights or religious rights) supporter going to a repressive Asian country to spread my message and take some actions. Can you help me be anonymous online while traveling?'

There are apparently some organized groups going somewhere in Asia to do something. They eventually find Tor through search engines and their fellow members and want to learn more. These calls are generally 30-50 minutes long and generally wind up talking about how the Internet works more than tor itself. There have been eight of these calls so far.

The second was a series of calls from one woman. She called out of desperation. She figured tor is 'technical and computery' and may be able to help, since the local computer stores and police dept were useless. She said her computer would randomly do things she didn't tell it to do, like move the cursor, turn the webcam light on, and one of her coworkers in another country seemed to know far more about her than she remembers telling him over the years.

The local computer stores ran anti-virus/anti-malware and found nothing. One suggested she see a doctor for dementia (she's older). The local police told her to take classes to learn how to use her computer and even if her coworker was stalking her, he's in a different country and therefore out of their jurisdiction. I was the first to tell her she's not crazy and yes, infected computers can do exactly what she's experiencing. After about 5 calls over two weeks, I eventually handed her off to a local domestic violence organization who can also help with internet stalking. It's surprisingly hard to find an anti-abuse org that also knows how to handle the Internet. Comically, the first two orgs I called pointed me at NNEDV.org, who then point people at Tor for help with privacy online.

And the final call was my first video support chat. This person is an adult video performer, and as she put it, 'there are fans, super fans, creepy fans, and stalkers. I love the first three types of fans.' The local police detective basically told her that because of what she does for a living, there is nothing they can do about her stalker and that she brought this on herself. She found tor through internet searches. She talked to other companies who just wanted to sell her software, but not actually answer her questions. She had a lot of questions.

We covered online privacy, how the internet works, how to un-infect her work computer, and how to keep her personal computer safer than the work computer. Generally helped her setup tails on a usb drive, tbb, and what happens when you login to google, twitter, and facebook over tor (who does that provide privacy from, what does it protect, etc). She wanted to know how to keep, in her words, 'the public me separate from the private me' on the Internet and from her non-stalker fans. In the end, she said the internet was far more complex than she thought, and wishes she could just buy something that 'just worked' without her thinking about it. She realized it's unlikely that will ever happen.

In summary, there are the usual 5-10 minute calls/chats about technical operations of tor, and then the far longer 'explain to me online privacy and anonymity' calls.

And yes, there are still the random crazy people that call and insist they are being stalked by the Illuminati, The Greys, and other intergalactic networks asking if tor can provide planetary anonymity or anonymity on space networks. Thankfully, these are few and far between."

3. Andrew met with students at University College London in London, UK to run a IRSG seminar about anonymity, usability and security. A number of students are interested in studying more about Tor's usability and security properties under the direction of Dr. Angela Sasse, `http://sec.cs.ucl.ac.uk/people/m_angela_sasse/`. Further discussions about crypto challenges for students under Dr. Nicolas Courtois, `http://www.cs.ucl.ac.uk/staff/N.Courtois/`.

4. Andrew and Runa met with Privacy International, `https://www.privacyinternational.org/`, to discuss their growing database of surveillance technology, the capabilities, and methods to help normal people combat such pervasive, sophisticated surveillance apparatus globally.

5. Karen spoke at the Yahoo! Change Your World! Cairo 2012 Summit, `http://ycorpblog.com/2012/01/18/change-your-world/`.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

1. Sebastian began working on TBB with Erinn and they tried making the Makefiles a little easier to use. Currently, they don't really do dependency tracking very much, so you have to be really careful in which order to execute them, otherwise some of your progress could get lost. Sebastian hopes this will both help the buildbot integration as well as make it easier for random people to reproduce our TBB builds. OS X appears especially painful here, as you need different options to build the same software on different versions of it, and some of the software (hello firefox) just doesn't build in some cases. Firefox 10 (released yesterday or so) is supposed to build on recent OS X again, so we'll see. The first steps look promising, and hopefully we can get this finished, tested, and merged soon so others can poke at it too.

2. On January 5, released Tor Browser Bundle 2.2.35-4.

   ```
   The Tor Browser Bundles and other packages have been updated to OpenSSL 1.0.0f and 0.9.8s.

   Tor Browser Bundle (2.2.35-4)

       Update OpenSSL to 1.0.0f
       Update NoScript to 2.2.5
   ```

3. On January 4, the Tails team released version 0.10

   ```
   * Tor: upgrade to 0.2.2.35-1.
   ```

```
* Iceweasel
- Install Iceweasel 9.0 from the Debian Mozilla team's APT repository.
- Update Torbutton to 1.4.5.1-1.
- Support viewing any YouTube video that is available in HTML5 format:
  install xul-ext-greasemonkey and the "Permanently Enable HTML5 on
  YouTube" GreaseMonkey script.
- Stop using Polipo in Iceweasel. Its SOCKS support was fixed.
- Install from Debian sid the iceweasel extensions we ship,
  for compatibility with FF9.
- Use Scroogle (any languages) instead of Scroogle (English only) when
  booted in English. Many users choose English because their own
  language is not supported yet; let's not hide them search results in
  their own language.
- Install Iceweasel language packs from Debian unstable:
  unfortunately they are not shipped on the mozilla.debian.net repository.
- Install the NoScript Firefox extension; configure it the same way as
  the TBB does.
- Disable third-party cookies.
  They can be used to track users, which is bad. Besides, this is what
  TBB has been doing for years.
- FoxyProxy: allow direct connections to RFC1918 IPs.

* Do not transparent proxy outgoing Internet connections through Tor.
- Torify the SSH client using connect-proxy to all IPs but RFC1918 ones.
- Torify APT using Polipo HTTP.
- Torify wget in wgetrc.
- Torify gobby clients using torsocks. It does not support proxies yet.
- Torify tails-security-check using LWP::UserAgent's SOCKS proxy support.
- Fix enabling of GNOME's HTTP proxy.

* Software
- Upgrade Vidalia to 0.2.15-1+tails1.
  Â· New upstream release.
  Â· Do not warn about Tor version.
- Upgrade MAT to 0.2.2-1~bpo60+1.
- Upgrade VirtualBox guest software to 4.1.6-dfsg-2~bpo60+1,
  built against the ABI of X.Org backports.
- Upgrade I2P to 0.8.11 using KillYourTV's Squeeze packages;
  additionally, fix its start script that was broken by the tordate merge.
- Install unar (The Unarchiver) instead of the non-free unrar.
- Install Nautilus Wipe instead of custom Nautilus scripts.

* Hardware support
- Upgrade Linux kernel to 3.1.6-1.
- Upgrade to X.Org from squeeze-backports.
- Install more, and more recent b43 firmwares.
- Upgrade barry to 0.15-1.2~bpo60+1.

* Internationalization
- Add basic language support for Russian, Farsi and Vietnamese.
- Install some Indic fonts.
- Install some Russian fonts.
- Add Alt+Shift shortcut to switch keyboard layout.

* Miscellaneous
- Support booting in "Windows XP -like camouflage mode":
  Â· Install homebrewn local .debs for a Windows XP look-alike Gnome theme.
  Â· Add the "Windows XP Bliss" desktop wallpaper.
  Â· Added a script that's sets up Gnome to look like Microsoft Windows XP.
  Â· Add Windows XP "camouflage" icons for some programs.
  Â· Make Iceweasel use the IE icon when Windows XP camouflage is enabled.
  Â· Add special launcher icons for the Windows XP theme so that they're
    not too big.
- Decrease Florence focus zoom to 1.2.
- Do not fetch APT translation files. Running apt-get update is heavy enough.
- Add MSN support thanks to msn-pecan.
- Add custom SSH client configuration:
  Â· Prefer strong ciphers and MACs.
  Â· Enable maximum compression level.
  â¯Â· Explicitly disable X11 forwarding.
  Â· Connect as root by default, to prevent fingerprinting when username
    was not specified.
- Replace flawed FireGPG with a home-made GnuPG encryption applet;
  install a feature-stripped FireGPG that redirects users to
  the documentation, and don't run Seahorse applet anymore.
- Enable Seahorse's GnuPG agent.
- Blank screen when lid is closed, rather than shutting down the system.
  The shutdown "feature" has caused data losses for too many people, it seems.
  There are many other ways a Tails system can be shut down in a hurry
  these days.
- Import Tails signing key into the keyring.
- Fix bug in the Pidgin nick generation that resulted in the nick
  "XXX_NICK_XXX" once out of twenty.
- Pre-configure the #tor IRC discussion channel in Pidgin.
- Fix "technology preview" of bridge support: it was broken by tordate merge.
- Install dependencies of our USB installer to ease its development.
- Make vidalia NM hook sleep only if Vidalia is already running.
- Reintroduce the htpdate notification, telling users when it's safe
  to use Tor Hidden Services.
  - htpdate: omit -f argument to not download full pages.
  - htpdate: write success file even when not within {min,max}adjust.
    Otherwise htpdate will not "succeed" when the time diff is 0 (i.e.
    the clock was already correct) so the success file cannot be used
    as an indicator that the system time now is correct, which arguably
    is its most important purpose.

  * Build system
  - Name built images according to git tag.
```

4. On January 28, the Tails team released version 0.10.1.

```
tails (0.10.1) unstable; urgency=low

  * Iceweasel
  - Make Startpage the default web search engine. Scroogle does not look
    reliable enough these days.

  * Software
  - Upgrade WhisperBack to 1.5.1 (update link to bug reporting documentation).
  - Update MAT to 0.2.2-2~bpo60+1 (fixes a critical bug in the GUI).

  * Hardware support
  - Upgrade Linux kernel to 3.2.1-2

  * Time synchronization
    Serious rework that should fix most, if not all, of the infamous
    time-sync’ related bugs some Tails users have experienced recently.
    - Make htpdate more resilient by using three server pools, and
      allowing some failure ratio.
    - Set time from Tor’s unverified-consensus if needed.
    - Set time to middle of [valid-after, fresh-until] from consensus.
    - Many robustness, performance and fingerprinting-resistance improvements.
    - Display time-sync’ notification much earlier.

  * Miscellaneous
  - Fix access to "dumb" git:// protocol by using a connect-socks wrapper
    as GIT_PROXY_COMMAND.
  - SSH client: fix access to SSH servers on the Internet by correcting
    Host / ProxyCommand usage.
  - Pidgin: use OFTC hidden service to workaround Tor blocking.
  - Claws Mail: disable draft autosaving.
    When composing PGP encrypted email, drafts are saved back to
    the server in plaintext. This includes both autosaved and manually
    saved drafts.
  - tails-security-check-wrapper: avoid eating all memory when offline.
```

Bridge relay and bridge authority work.

- Some discussion and progress on bridge scanning and reachability, https://trac.torproject.org/projects/tor/ticket/5028. Merged two different efforts into one ticket for progress, former effort was https://trac.torproject.org/projects/tor/ticket/4075.

- Reallocate bridges from a blocked country to others that do not block, https://trac.torproject.org/projects/tor/ticket/5027.

- Updated the tor cloud bridge configuration, https://trac.torproject.org/projects/tor/ticket/5004.

- Discussion and migration of the bridge database, currently run by a volunteer, to Tor's infrastructure, https://trac.torproject.org/projects/tor/ticket/2301

Scalability, load balancing, directory overhead, efficiency.

- Damian spent time writing a proper mocking module for stem, https://gitweb.torproject.org/stem.git/blob/HEAD:/test/mocking.py, and re-factoring the tests to use it. This will greatly improve the maintainability and ease of writing new tests going forward. Originally this began with the humble goal of 'remove a built-in mocking hack from the system module', then went down the rabbit hole of larger scale testing improvements.

- Sathyanarayanan took on some development tasks for stem including integration tests for chroot setups, https://trac.torproject.org/projects/tor/ticket/4896, saving configurations, https://trac.torproject.org/projects/tor/ticket/4913, and troubleshooting test failures on OSX.

- A large part of the stem discussions centered around making stem more developer friendly, both in terms of its utility APIs and easier collaboration. The stem TODO moved to a development wiki, https://trac.torproject.org/projects/tor/wiki/doc/stem.

- Karsten implemented quite a bit more of metrics-lib, the Java library that facilitates downloading, importing, and parsing various Tor descriptors from https://metrics.torproject.org

- Karsten improved DocTor, our friendly consensus-health checker. Added a warning about expiring directory certificates three months in advance, not just two weeks. Added severities to warning messages, because there are so many of them https://trac.torproject.org/projects/tor/ticket/4878. Added a check to learn when relays with the Authority flag are missing from the consensus. Fixed the consensus-health checker a couple of times when running into different edge cases when downloading consensuses and votes from the authorities.

- Karsten improved relay-search performance together with Sebastian. The first attempt was to do two subsequent queries for searching a relay, one covering only the last 4 days and one covering a full month, which improves performance sometimes, but not in all cases. The second, far more successful attempt was to partition the table containing network status entries https://trac.torproject.org/projects/tor/ticket/4673. Sebastian and Karsten used PostgreSQL's table partitioning feature that is based on table inheritance, tested the changes on SEbastian's laptop and external hard drive, did the migration on the live metrics server, adapted the aggregation and import scripts, and fixed a few problems resulting from PostgreSQL's poor table partitioning implementation. All in all, we experienced a speed-up by a factor of roughly 100.

- Changed country names on the metrics website to be less political, https://trac.torproject.org/projects/tor/ticket/4809. Now, we're using the Wikipedia country names.
- Made metrics data of the last three days available via rsync https://trac.torproject.org/projects/tor/ticket/4687. This is crucial for others to run their own metrics websites or build similar services. Now they can.
- Implemented sanitizing IPv6 addresses in bridge descriptors and processed all bridge descriptors since October 2011 once again. Now, sanitized descriptors contain sanitized bridge IP addresses of the form [fd9f:2e19:3bcf::f8:2444], where fd9f:2e19:3bcf is the same for all sanitized bridge descriptors and f8:2444 is the SHA-1 hash that is based on the bridge's original IPv6 address, among other things.
- Looked at a problem with relays publishing too many descriptors and directory authorities accepting them https://trac.torproject.org/projects/tor/ticket/3265. It seems this problem doesn't exist anymore.
- Sebastian discussed a new voting method with Roger, which would hopefully reduce the impact of a single almost-failing dirauth on the network. Currently, such an authority can prevent us from generating a consensus even if all other dirauths are fully operational, because we have an even number of dirauths. In the case where not all other dirauths are fully operational, this gets worse. See https://trac.torproject.org/projects/tor/ticket/4826 for the description. Sebastian suspects we'll need a proposal here, but the implementation should not be too difficult.

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.

Updated translations for Vidalia, Vidalia Help files, torbutton, torbrowser, orbot, short user manual, gettor in Arabic, Korean, Farsi, Greek, Dutch, Finnish, Polish, Spanish, and Italian.