From: Andrew Lewman, Executive Director
To: The Tor Community
Date: January 14, 2012

This report documents progress in December 2011.

# New releases, new hires, new funding

## New Releases

1. 2011-12-14. Torbutton 1.4.5 Released.

```
Fixes:
  * bug 4517: Disable external drag and drop (prevents proxy bypass)
  * bug 4099: Disable TLS session tickets to prevent linkability
  * bug 4603: Lower HTTP keep-alive timeout to reduce linkability
  * bug 4611: Notify user if "New Identity" fails
  * bug 4667: Close keep-alive connections on "New Identity" (TBB only)
  * bug 4453: Reset SOCKS host and port only when using "recommended settings"
  * misc: Perform versioncheck at startup regardless of session restore status
```

2. 2011-12-16. Tor 0.2.2.35 released.

   Tor 0.2.2.35 fixes a critical heap-overflow security issue in Tor's buffers code. Absolutely everybody should upgrade.

   The bug relied on an incorrect calculation when making data continuous in one of our IO buffers, if the first chunk of the buffer was misaligned by just the wrong amount. The miscalculation would allow an attacker to overflow a piece of heap-allocated memory. To mount this attack, the attacker would need to either open a SOCKS connection to Tor's SocksPort (usually restricted to localhost), or target a Tor instance configured to make its connections through a SOCKS proxy (which Tor does not do by default).

   Good security practice requires that all heap-overflow bugs should be presumed to be exploitable until proven otherwise, so we are treating this as a potential code execution attack. Please upgrade immediately! This bug does not affect bufferevents-based builds of Tor. Special thanks to "Vektor" for reporting this issue to us!

   Tor 0.2.2.35 also fixes several bugs in previous versions, including crash bugs for unusual configurations, and a long-term bug that would prevent Tor from starting on Windows machines with draconian AV software.

With this release, we remind everyone that 0.2.0.x has reached its formal end-of-life. Those Tor versions have many known flaws, and nobody should be using them. You should upgrade – ideally to the 0.2.2.x series. If you're using a Linux or BSD and its packages are obsolete, stop using those packages and upgrade anyway.

The Tor 0.2.1.x series is also approaching its end-of-life: it will no longer receive support after some time in early 2012.

Note that the tarball and git tags are signed by Nick Mathewson (gpg key 165733EA) this time around.

```
Changes in version 0.2.2.35 - 2011-12-16
  o Major bugfixes:
    - Fix a heap overflow bug that could occur when trying to pull
      data into the first chunk of a buffer, when that chunk had
      already had some data drained from it. Fixes CVE-2011-2778;
      bugfix on 0.2.0.16-alpha. Reported by "Vektor".
    - Initialize Libevent with the EVENT_BASE_FLAG_NOLOCK flag enabled, so
      that it doesn't attempt to allocate a socketpair. This could cause
      some problems on Windows systems with overzealous firewalls. Fix for
      bug 4457; workaround for Libevent versions 2.0.1-alpha through
      2.0.15-stable.
    - If we mark an OR connection for close based on a cell we process,
      don't process any further cells on it. We already avoid further
      reads on marked-for-close connections, but now we also discard the
      cells we'd already read. Fixes bug 4299; bugfix on 0.2.0.10-alpha,
      which was the first version where we might mark a connection for
      close based on processing a cell on it.
    - Correctly sanity-check that we don't underflow on a memory
      allocation (and then assert) for hidden service introduction
      point decryption. Bug discovered by Dan Rosenberg. Fixes bug 4410;
      bugfix on 0.2.1.5-alpha.
    - Fix a memory leak when we check whether a hidden service
      descriptor has any usable introduction points left. Fixes bug
      4424. Bugfix on 0.2.2.25-alpha.
    - Don't crash when we're running as a relay and don't have a GeoIP
      file. Bugfix on 0.2.2.34; fixes bug 4340. This backports a fix
      we've had in the 0.2.3.x branch already.
    - When running as a client, do not print a misleading (and plain
      wrong) log message that we're collecting "directory request"
      statistics: clients don't collect statistics. Also don't create a
      useless (because empty) stats file in the stats/ directory. Fixes
      bug 4353; bugfix on 0.2.2.34.

  o Minor bugfixes:
    - Detect failure to initialize Libevent. This fix provides better
      detection for future instances of bug 4457.
  - Avoid frequent calls to the fairly expensive cull_wedged_cpuworkers
    function. This was eating up hideously large amounts of time on some
    busy servers. Fixes bug 4518; bugfix on 0.0.9.8.
  - Resolve an integer overflow bug in smartlist_ensure_capacity().
    Fixes bug 4230; bugfix on Tor 0.1.0.1-rc. Based on a patch by
    Mansour Moufid.
  - Don't warn about unused log_mutex in log.c when building with
    --disable-threads using a recent GCC. Fixes bug 4437; bugfix on
    0.1.0.6-rc which introduced --disable-threads.
  - When configuring, starting, or stopping an NT service, stop
    immediately after the service configuration attempt has succeeded
    or failed. Fixes bug 3963; bugfix on 0.2.0.7-alpha.
  - When sending a NETINFO cell, include the original address
    received for the other side, not its canonical address. Found
    by "troll_un"; fixes bug 4349; bugfix on 0.2.0.10-alpha.
  - Fix a typo in a hibernation-related log message. Fixes bug 4331;
    bugfix on 0.2.2.23-alpha; found by "tmpname0901".
  - Fix a memory leak in launch_direct_bridge_descriptor_fetch() that
    occurred when a client tried to fetch a descriptor for a bridge
    in ExcludeNodes. Fixes bug 4383; bugfix on 0.2.2.25-alpha.
  - Backport fixes for a pair of compilation warnings on Windows.
    Fixes bug 4521; bugfix on 0.2.2.28-beta and on 0.2.2.29-beta.
  - If we had ever tried to call tor_addr_to_str on an address of
    unknown type, we would have done a strdup on an uninitialized
    buffer. Now we won't. Fixes bug 4529; bugfix on 0.2.1.3-alpha.
    Reported by "troll_un".
  - Correctly detect and handle transient lookup failures from
    tor_addr_lookup. Fixes bug 4530; bugfix on 0.2.1.5-alpha.
    Reported by "troll_un".
  - 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".
  - Use tor_socket_t type for listener argument to accept(). Fixes bug
    4535; bugfix on 0.2.2.28-beta. Found by "troll_un".

o Minor features:
  - Add two new config options for directory authorities:
    AuthDirFastGuarantee sets a bandwidth threshold for guaranteeing the
    Fast flag, and AuthDirGuardBWGuarantee sets a bandwidth threshold
    that is always sufficient to satisfy the bandwidth requirement for
    the Guard flag. Now it will be easier for researchers to simulate
    Tor networks with different values. Resolves ticket 4484.
  - When Tor ignores a hidden service specified in its configuration,
    include the hidden service's directory in the warning message.
    Previously, we would only tell the user that some hidden service
    was ignored. Bugfix on 0.0.6; fixes bug 4426.
    - Update to the December 6 2011 Maxmind GeoLite Country database.

  o Packaging changes:
    - Make it easier to automate expert package builds on Windows,
      by removing an absolute path from makensis.exe command.
```

3. 2011-12-16. Tor 0.2.3.10-alpha released.

   Changes in version 0.2.3.10-alpha - 2011-12-16 Tor 0.2.3.10-alpha fixes a critical heap-overflow security issue in Tor's buffers code. Absolutely everybody should upgrade.

   The bug relied on an incorrect calculation when making data continuous in one of our IO buffers, if the first chunk of the buffer was misaligned by just the wrong amount. The miscalculation would allow an attacker to overflow a piece of heap-allocated memory. To mount this attack, the attacker would need to either open a SOCKS connection to Tor's SocksPort (usually restricted to localhost), or target a Tor instance configured to make its connections through a SOCKS proxy (which Tor does not do by default).

   Good security practice requires that all heap-overflow bugs should be presumed to be exploitable until proven otherwise, so we are treating this as a potential code execution attack. Please upgrade immediately! This bug does not affect bufferevents-based builds of Tor. Special thanks to "Vektor" for reporting this issue to us!

   This release also contains a few minor bugfixes for issues discovered in 0.2.3.9-alpha.

```
  o Major bugfixes:
    - Fix a heap overflow bug that could occur when trying to pull
      data into the first chunk of a buffer, when that chunk had
      already had some data drained from it. Fixes CVE-2011-2778;
      bugfix on 0.2.0.16-alpha. Reported by "Vektor".

  o Minor bugfixes:
    - If we can't attach streams to a rendezvous circuit when we
      finish connecting to a hidden service, clear the rendezvous
      circuit's stream-isolation state and try to attach streams
      again. Previously, we cleared rendezvous circuits' isolation
      state either too early (if they were freshly built) or not at all
      (if they had been built earlier and were cannibalized). Bugfix on
      0.2.3.3-alpha; fixes bug 4655.
    - Fix compilation of the libnatpmp helper on non-Windows. Bugfix on
      0.2.3.9-alpha; fixes bug 4691. Reported by Anthony G. Basile.
    - Fix an assertion failure when a relay with accounting enabled
      starts up while dormant. Fixes bug 4702; bugfix on 0.2.3.9-alpha.

  o Minor features:
    - Update to the December 6 2011 Maxmind GeoLite Country database.
```

4. 2011-12-17. Torbutton 1.4.5.1 released.

```
Fixes:
  * bug 4722: Fix ability to drag tabs on Windows (due to #4517)
```

5. 2011-12-25. Tor Ramdisk version 20111225 released.

```
    - tor updated to 0.2.2.35
    - libevent updated to 2.0.16
    - kernel updated to 2.6.32.50 + Gentoo's hardened-patches-2.6.32-83.extras
    Learn more about Tor Ramdisk and download at http://opensource.dyc.edu/tor-ramdisk
```

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

- More research into the censorship apparatus in China, ticket 4744, https://trac.torproject.org/projects/tor/ticket/4744 has more details of what we're seeing.

- From George's Google Summer of Code 2011 project, his pluggable transport proxy implementation got merged in Tor 0.2.3.9-alpha. Some of his ideas were included in some parts of proposal 179, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/178-param-voting.txt, like the dynamic DH modulus, https://trac.torproject.org/projects/tor/ticket/4548 and the not-so-fingerprintable SSL certificate serial numbers, https://trac.torproject.org/projects/tor/ticket/4584.

- George rewrote the threat model of obfs2 and an architecture overview of obfsproxy, then Nick improved them some more.

- George converted parts of obfsproxy's documentation to Doxygen.

- George started a draft of user documentation on how to setup obfsproxy.

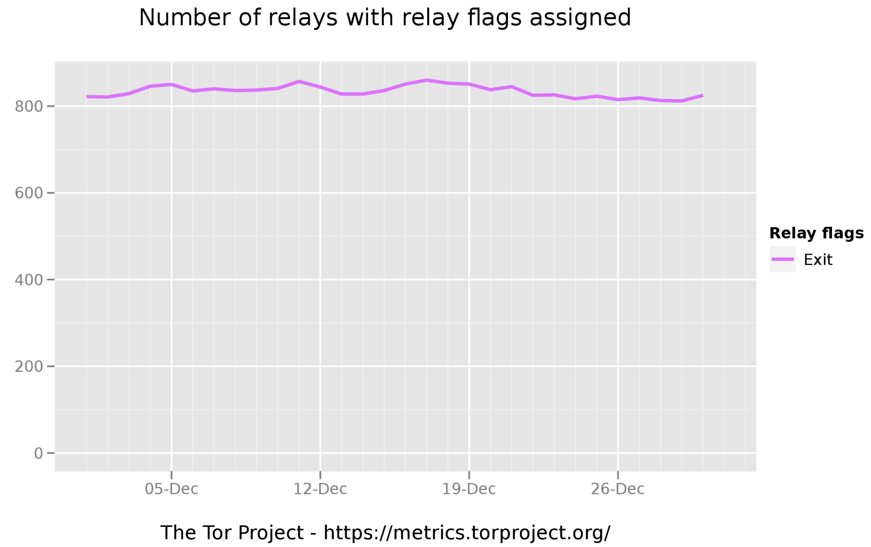
- Linus helped a few testers of private bridges on IPv6 with various results.

## Hide Tor's network signature.

Nothing to report.

# Grow the Tor network and user base. Outreach.

## Measures of the Tor Network

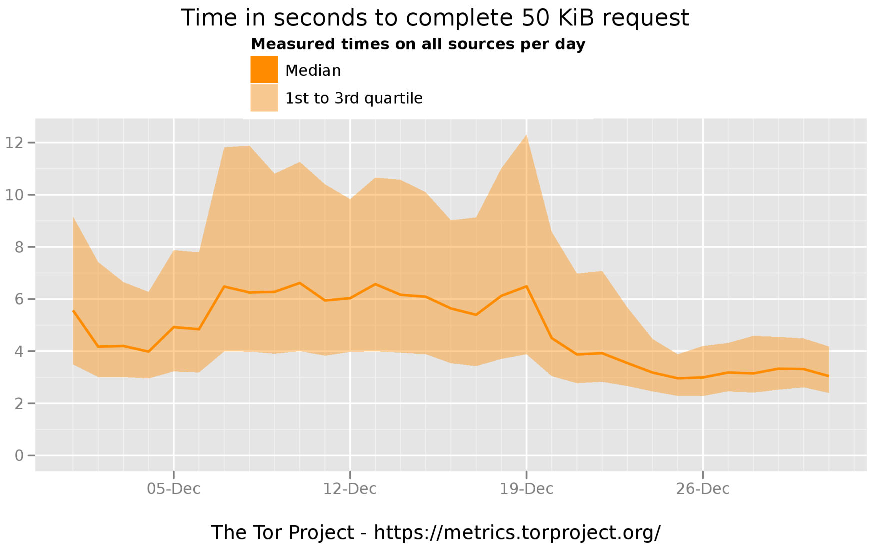


Number of relays with relay flags assigned

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

This graph shows the total quantity of exit relays in December 2011.

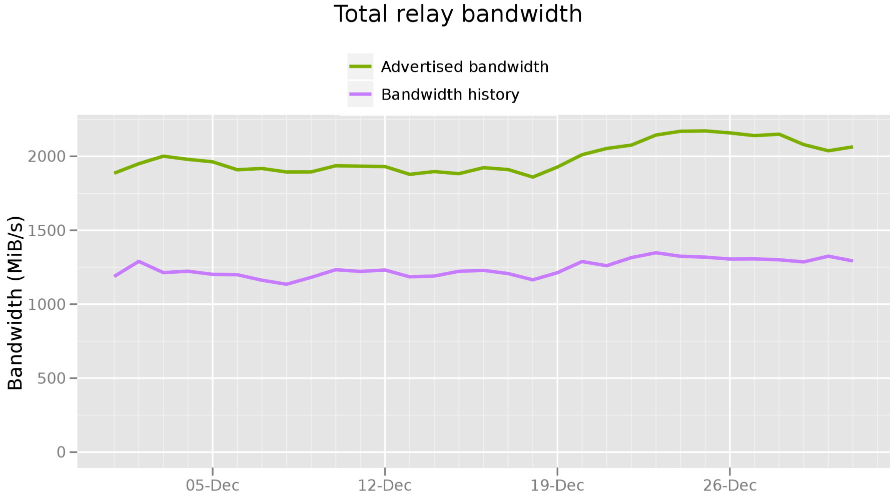
This graph shows the total quantity of relays and the total quantity of bridges in December 2011.



Time in seconds to complete 50 KiB request

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

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.



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 1.8 GBps (14.4 Gbps) available with 1.1 GBps (8.8 Gbps) used.

## Outreach and Advocacy

1. Jake talked at ”Internet and Democratic Change - Net activism, empowerment and emancipation” hosted by Sida.se, Internet and Democratic Change, http://www.sida.se/Net_activism_outcome.

2. We announced the Farsi blog https://blog.torproject.org/blog/announcing-tor-farsi-blog.

3. Roger and Jacob presented at the CCC 28C3 conference in Berlin, Germany. Slides, https://svn.torproject.org/svn/projects/presentations/slides-28c3.pdf and Video, https://media.torproject.org/video/28c3-4800-en-how_governments_have_tried_to_block_tor_h264.mp4.

4. Steven and Jacob spoke at a press-conference regarding surveillance technology, https://www.privacyinternational.org/article/wikileaks-release-shows-terrifying-power-todays-surv

5. Andrew trained some Russian activists on how to safely transport information across borders, communicate with sensitive people in and out of the country, and what level of sophistication to expect if targeted by the opposition.

6. Andrew worked with two domestic abuse/stalking survivors who were pointed at Tor and who are trying to get the anti-abuse/survivor organizations to pay attention to the Internet. The proposals for a fully identified Internet in the USA scared them into action. They want to know how technology can help them stay anonymous, even in the face of breaking future

laws that may exist. They are also interested in setting up an anonymous support forum for other survivors. One of them was swept up in an anti-terrorism operation for the steps she took to become anonymous. She wants to find a way to help others, anonymously.

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

Nothing to report.

## Bridge relay and bridge authority work.

Nothing to report.

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

- George found two remotely-triggerable memory leaks and a DoS amplifier, in the SSL part of OpenSSL. He also noticed how OpenSSL uses memcmp() to compare sensitive data. He notified the Openssl Devs who prepared fixes that will be shipped in OpenSSL 1.0.0g.
- Robert fixed the remaining part of ticket 1297, https://trac.torproject.org/projects/tor/ticket/1297 (to allow clients to connect to hidden services whose CBTs are higher than the clients').
- In the process of fixing ticket 1297, https://trac.torproject.org/projects/tor/ticket/1297, Robert found and fixed ticket 4759, https://trac.torproject.org/projects/tor/ticket/4759, which was probably made triggerable by the stream-isolation change earlier in 0.2.3.x.
- Nick coded a feature to finally implement proposal 110, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/110-avoid-infinite-circuits.txt to make certain kinds of denial of service attack harder.
- Nick wrote some compatibility code to learn our address without making fascist anti-virus programs decide that we're evil.
- We rejected all relays running Tor 0.2.0 or earlier from the consensus.
- Nick wrote up an IPv6 roadmap document based on notes from Karsten and Linus.

## 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.

Updated translations for Vidalia, Vidalia Help, gettor, short user manual, and torbutton in Farsi, Greek, Arabic, Mandarin, Italian, Dutch, and Brazilian Portugese