Monthly Progress report for March 2012

The Tor Project, Inc.

Contents

1 Research

1.1 Anonymous Communications

- We fixed a variety of bugs in Shadow, Experimentor, and Tor (e.g. https://trac.torproject.org/projects/tor/ticket/5373), and we located and cleaned up the original N23 patch from the Defenestrator authors (https://trac.torproject.org/projects/tor/ticket/4488). Next steps: get some simulation results (https://trac.torproject.org/projects/tor/ticket/4486) and write a spec for N23 (https://trac.torproject.org/projects/tor/ticket/5392). It's also likely that the "static n23" design is going to be inappropriate for real deployment, and nobody has yet invented an "adaptive n23" design that improves over static (https://trac.torproject.org/projects/tor/ticket/5379).

- Steven worked on research relating to Protecting bridge operators from probing attacks.

- On March 26 we released a new alpha version of Tor.

```
Tor 0.2.3.13-alpha fixes a variety of stability and correctness bugs
in managed pluggable transports, as well as providing other cleanups
that get us closer to a release candidate.

Changes in version 0.2.3.13-alpha - 2012-03-26
  o Directory authority changes:
    - Change IP address for maatuska (v3 directory authority).

  o Security fixes:
    - Provide controllers with a safer way to implement the cookie
      authentication mechanism. With the old method, if another locally
      running program could convince a controller that it was the Tor
      process, then that program could trick the contoller into telling
      it the contents of an arbitrary 32-byte file. The new "SAFECOOKIE"
      authentication method uses a challenge-response approach to prevent
      this attack. Fixes bug 5185, implements proposal 193.
    - Never use a bridge or a controller-supplied node as an exit, even
      if its exit policy allows it. Found by wanoskarnet. Fixes bug
      5342. Bugfix on 0.1.1.15-rc (for controller-purpose descriptors)
      and 0.2.0.3-alpha (for bridge-purpose descriptors).
    - Only build circuits if we have a sufficient threshold of the total
      descriptors that are marked in the consensus with the "Exit"
      flag. This mitigates an attack proposed by wanoskarnet, in which
      all of a client's bridges collude to restrict the exit nodes that
      the client knows about. Fixes bug 5343.

  o Major bugfixes (on Tor 0.2.3.x):
    - Avoid an assert when managed proxies like obfsproxy are configured,
      and we receive HUP signals or setconf attempts too rapidly. This
      situation happens most commonly when Vidalia tries to attach to
```

Tor or tries to configure the Tor it's attached to. Fixes bug 5084; bugfix on 0.2.3.6-alpha.
- Fix a relay-side pluggable transports bug where managed proxies were unreachable from the Internet, because Tor asked them to bind on localhost. Fixes bug 4725; bugfix on 0.2.3.9-alpha.
- Stop discarding command-line arguments when TestingTorNetwork is set. Discovered by Kevin Bauer. Fixes bug 5373; bugfix on 0.2.3.9-alpha, where task 4552 added support for two layers of torrc files.
- Resume allowing the unit tests to run in gdb. This was accidentally made impossible when the DisableDebuggerAttachment option was introduced. Fixes bug 5448; bugfix on 0.2.3.9-alpha.
- Resume building with nat-pmp support. Fixes bug 4955; bugfix on 0.2.3.11-alpha. Reported by Anthony G. Basile.

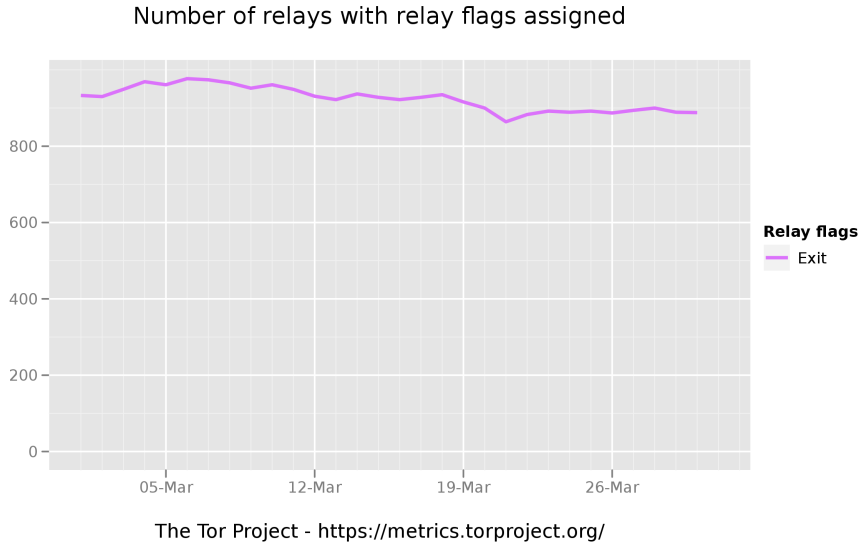
o Minor bugfixes (on 0.2.2.x and earlier):
- Ensure we don't cannibalize circuits that are longer than three hops already, so we don't end up making circuits with 5 or more hops. Patch contributed by wanoskarnet. Fixes bug 5231; bugfix on 0.1.0.1-rc which introduced cannibalization.
- Detect and reject certain misformed escape sequences in configuration values. Previously, these values would cause us to crash if received in a torrc file or over an authenticated control port. Bug found by Esteban Manchado VelÃ¡zquez, and independently by Robert Connolly from Matta Consulting who further noted that it allows a post-authentication heap overflow. Patch by Alexander Schrijver. Fixes bugs 5090 and 5402 (CVE 2012-1668); bugfix on 0.2.0.16-alpha.
- Fix a compile warning when using the --enable-openbsd-malloc configure option. Fixes bug 5340; bugfix on 0.2.0.20-rc.
- Directory caches no longer refuse to clean out descriptors because of missing v2 networkstatus documents, unless they're configured to retrieve v2 networkstatus documents. Fixes bug 4838; bugfix on 0.2.2.26-beta. Patch by Daniel Bryg.
- Update to the latest version of the tinytest unit testing framework. This includes a couple of bugfixes that can be relevant for running forked unit tests on Windows, and removes all reserved identifiers.

o Minor bugfixes (on 0.2.3.x):
- On a failed pipe() call, don't leak file descriptors. Fixes bug 4296; bugfix on 0.2.3.1-alpha.
- Spec conformance: on a v3 handshake, do not send a NETINFO cell until after we have received a CERTS cell. Fixes bug 4361; bugfix on 0.2.3.6-alpha. Patch by "frosty".

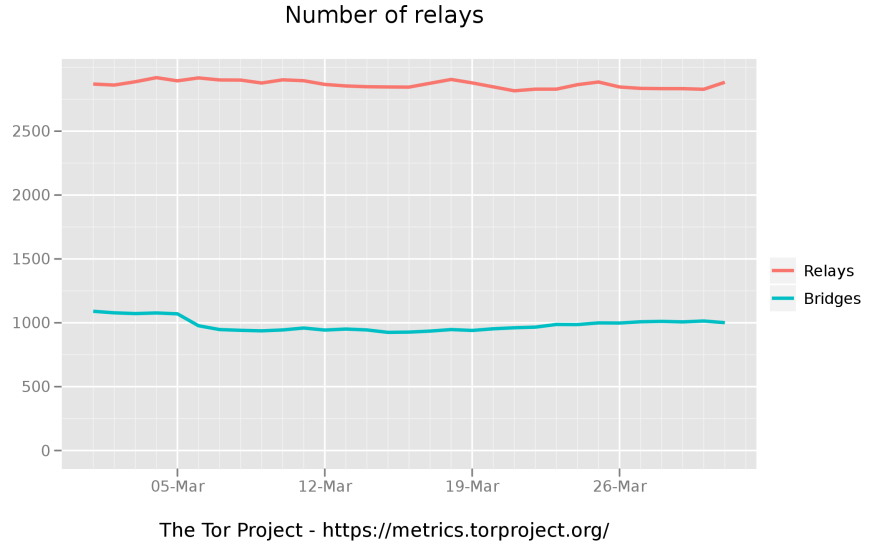
```
  - When binding to an IPv6 address, set the IPV6_V6ONLY socket
    option, so that the IP stack doesn't decide to use it for IPv4
    too. Fixes bug 4760; bugfix on 0.2.3.9-alpha.
  - Ensure that variables set in Tor's environment cannot override
    environment variables that Tor passes to a managed
    pluggable-transport proxy. Previously, Tor would pass every
    variable in its environment to managed proxies along with the new
    ones, in such a way that on many operating systems, the inherited
    environment variables would override those which Tor tried to
    explicitly set. Bugfix on 0.2.3.12-alpha for most Unixoid systems;
    bugfix on 0.2.3.9-alpha for Windows.

o Minor features:
  - A wide variety of new unit tests by Esteban Manchado Velazquez.
  - Shorten links in the tor-exit-notice file. Patch by Christian Kujau.
  - Update to the March 6 2012 Maxmind GeoLite Country database.
```

- We added two new architectures to the build system, armel and armhf, for Debian packages. This should enable Tor to work on more hardware.
- Finished larger and smaller tickets like 4561, 5151, 5529, 4875. The IPv6 work comes with some refactoring of code which is interesting.
- Managed to finish phase 1 of xxx-ipv6-roadmap.txt.
- Finally made some progress on ticket 4345 "Bug: closing wedged cpuworker". More to do here.

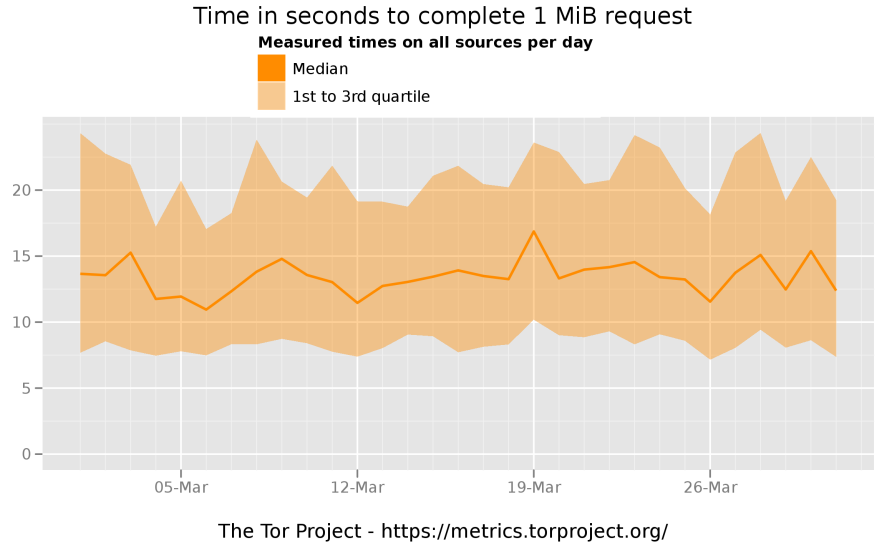
1.2 Metrics



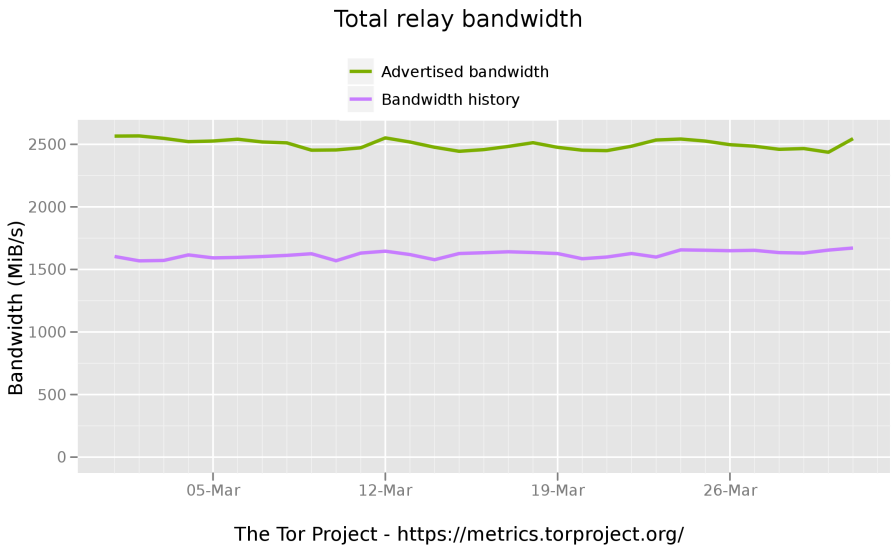
This graph shows the total quantity of exit relays in March 2012.



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



This graphs shows how many seconds it took to complete a 1 megabyte download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month.

- Identified a problem with our pbzip2-compressed descriptor tarballs and the Java decompression library that we use, and re-compressed all our tarballs with bzip2.
- Fixed a problem with Onionoo not being available via HTTPS by moving it to yatei.
- Investigated a problem in Onionoo with missing server descriptors and updating details files.
- Fixed non-working metrics-db import of tor26's collected descriptors.
- Fixed caching in Onionoo.
- Looked into corrupt bandwidth history lines in extra-info descriptors (ticket 1926) again, without success.
- Commented on Onionoo being unable to provide historical bandwidth data to Atlas (ticket 5389).
- Fixed drops in versions/platforms/bandwidth graphs (ticket 5497).
- Investigated an out-of-memory bug in metrics-lib when parsing large relay descriptor numbers.
- Looked into a bug with Atlas handling null values in bandwidth graphs.
- Looked into problem with DocTor processes not terminating sometimes, resulting from a bug in metrics-lib.
- Prepared metrics-db for 'opt' being removed from bridge descriptors.
- Started archiving consensuses published at :30 of an hour (ticket 5504).

- Fixed censorship detector script which was broken by enforcing HTTPS on metrics.
- Discussed descriptor-parsing support in stem and how it compares to metrics-lib.
- Learned client speed trends by evaluating directory request download times (ticket 3260).
- Made metrics-web use metrics-lib instead of implementing its own descriptor parsing.
- Extended Torperf to truncate its output files.
- Extended metrics-lib and wrote a server descriptor verifier that compares signing keys to fingerprints and signatures (ticket 2768).
- Updated metrics-db to handle truncated Torperf files.
- Looked at fraction of exit relays exiting from different IP (ticket 4147).
- Reviewed and commented on patches to extend bridge statistics to IPv6 by adding a GeoIP v6 database (ticket 5053) and reporting v4 vs v6 usage (ticket 5055).
- Optimized R object caching on metrics website, so that tables don't delay page loading anymore (ticket 3878).
- Extended metrics-web to export metrics graph data in JSON format.
- Implemented accepting hashed relay fingerprints and hashed hashed bridge fingerprints in Onionoo (ticket 5368).
- Added descriptor digests to metrics-lib which are used by metrics-web.
- Deployed ExoneraTor Beta, replacing the existing ExoneraTor page.
- Removed deprecated parts from Onionoo protocol, fixed a few upcoming bugs.
- Finished a first version of extending dir-spec.txt to specify microdescriptors.
- Removed mostly unused functionality from metrics website.
- Discussed an API extension in Onionoo for exporting top-10 relays by bandwidth.
- Made graph generation on metrics-web thread-safe.
- Started a wiki page with tech reports (ticket 5405).
- Wrote an Onionoo project page (ticket 5189).
- Looked into potentially adding a graph on top-10 countries by connecting clients (ticket 3624).
- Cleaned up unused parts in metrics-web.
- Implemented a check in metrics-db whether torperf source files are becoming stale.
- Updated metrics-db to parse incompletely copied assignments files.

- Visualized missing consensuses in 2011 and 2012 (ticket 1890).
- Discussed obfsproxy statistics in Tor.
- Tried scheduling Onionoo update job inside Tomcat, which needs more work.
- Commented on ooni-probe/bridget using Onionoo to check if bridges are public relays (ticket 5272).
- Removed irrelevant bandwidth graphs from Onionoo's bandwidth documents.

1.3 Censorship & Circumvention

- The 2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI '12) seeks to bring together researchers and practitioners from technology, law, and policy who are working on means to study, detect, or circumvent practices that inhibit free and open communications on the Internet. Learn more at the Call for papers: Free and Open Communications on the Internet (FOCI) Workshop
- We developed a tool for scans of bridge lists which attempts to either open a simple TCP connection to the bridge's OR port or that will perform a full Tor handshake to the bridge. We tested the scanner by running a scan from Germany, https://trac.torproject.org/projects/tor/ticket/5028#comment:35 and comparing results to bridge reachability information obtained from the bridge authority in The Netherlands. We also performed a scan from China, https://trac.torproject.org/projects/tor/ticket/5028#comment:45, and found that over 80% of bridges were unreachable. We compared active scan results to passive usage statistics, https://trac.torproject.org/projects/tor/ticket/5028#comment:48, and confirmed that bridges that were found as unreachable in the scan also reported significantly fewer connections from China than other bridges.
- We have a design sketch in https://trac.torproject.org/projects/tor/ticket/5011 that has been reviewed and approved by everyone. We wrote a proposal that seeks to create a means for inter-controller communication using the Tor Control Port and another proposal, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/199-bridgefinder-integratio txt, that describes how the Tor client software can interact with an external program that performs bridge discovery.
- We wrote proposal 195, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/195-TLS-normalization-for-024.txt, which discusses TLS certificate normalization for Tor 0.2.4.x. We have also finalized plans plans for normalizing our declared cipher lists (https://trac.torproject.org/projects/tor/ticket/4744), and renegotiation identifier position (https://trac.torproject.org/projects/tor/ticket/5390).

2 Relay

2.1 Tor Network

- Aaron immplemented option 1 of the proposal for ticket 5027, and a step towards ticket 5484.

- Added log rotation ticket 5331 and configurable SMTP settings ticket 5258 to BridgeDB.
- Discussed BridgeDB scalability in ticket 4499 and ticket 5232.
- Kicked off a relays landing page, https://www.torproject.org/relays.

2.2 Console Client

- Damian continued developing stem. His time was almost entirely dedicated to writing a python counterpart for metrics-lib. Most of the effort here went into reader concurrency, server descriptor validation, and lots of testing. This project has the following goals:

  – provide the server descriptor, network status, and microdescriptor parsing needed by the controller
  – validate that new tor versions comply with the spec and don't break our parsing
  – replace the java metrics-lib so we have a single codebase with multiple maintainers (in other words, persuade Karsten to hack on stem)
  – allow applications that just need descriptor data (such as the consensus tracker script) to use cached descriptor data so they don't require an open control port

  At present stem's implementation just handles server descriptors. A lot more work will be needed to cover the rest of what metrics-lib does.

  Implementation:
  https://gitweb.torproject.org/stem.git/tree/HEAD:/stem/descriptor

  Testing:

- https://gitweb.torproject.org/stem.git/tree/HEAD:/test/unit/descriptor

- https://gitweb.torproject.org/stem.git/tree/HEAD:/test/integ/descriptor

- Damian reviewed meejah's txtorcon, a python controller lib using twisted. It's impressive that he got this up so quickly and it's neat to see what a twisted implementation looks like. However, it is missing large and very basic controller functionality (such as parsing controller replies), and what parsing it does do is hacky (if "COOKIE" in protocolinfo_reply: do cookie auth which will obviously fail with SAFECOOKIE). With work though this could be a nice alternative implementation. Meejah is obviously very capable and it'll be interesting to see where he goes with it.
- Sathyanarayanan also took the first stab at porting arm's ExitPolicy class to stem, though more work is still needed there, see ticket 5454 for more details.

2.3 Tor router

- Runa conducted a 20 user beta test of a web interface and sample hardware. Initial feed back in ticket 3646.
- Andrew wrote up the current state of the Torouter/onionbox project on the tor-talk mailing list.

3 Client

3.1 Tor Browser

1. On March 17, we released updated Tor Browser Bundles. The Tor Browser Bundles have all been updated to the latest Firefox 11.0 as well as a number of bugfixes.

```
Tor Browser Bundle (2.2.35-8)

    Update Firefox to 11.0
    Update OpenSSL to 1.0.0h
    Update NoScript to 2.3.4
    Update HTTPS Everywhere to 2.0.1

    Always build to with warnings enabled (closes:
    https://trac.torproject.org/projects/tor/ticket/4470)

    Disable HTTPS Everywhere SSL Observatory screen (closes:
    https://trac.torproject.org/projects/tor/ticket/5300)

Windows

    Remove tor-resolve from the Windows bundle (closes:
    https://trac.torproject.org/projects/tor/ticket/5403)

Mac OS X

    Give OS X users below 10.5 an incompatibility message (closes:
    https://trac.torproject.org/projects/tor/ticket/4356)

Linux

    Don't attempt to load the default KDE 4 theme from Vidalia,
    because that fails when the Qt versions don't match (closes:
    https://trac.torproject.org/projects/tor/ticket/5214)
```

3.2 Obfsproxy

- We implemented a packet-morphing prototype and wrote down our findings in a report, https://trac.torproject.org/projects/tor/attachment/ticket/5023/morpher.2.pdf. The report explains why we decided that traffic morphing, in its current technology state, is not the definite way to go.
- Of the currently available pluggable transports, obfs2 is a good default due to its efficiency and resistance to blocking. Suggestions for future development are listed in this report, https://www.cl.cam.ac.uk/~sjm217/papers/tor12pluggableroadmap.pdf.

3.3 Anonymous Computing

No releases this month.

3.4 Mobile

We work closely with The Guardian Project to keep tor working on Android and related devices. Learn more about Guardian at https://guardianproject.info.

Nothing to report.

4 Community

4.1 Support

A total of 498 tickets were created in the Tor help desk system this month: 432 tickets are in the queue called help, 23 tickets are in the queue called help-fa, and 43 tickets have been marked as spam.

4.1.1 The help queue

432 tickets were created in the help queue this month. 273 of them have been marked as resolved, 159 are currently open and waiting on a reply from a support assistant.

4.1.2 The help-fa queue

23 tickets were created in the help-fa queue this month. 1 has been marked as resolved, 22 are currently open and waiting on a reply from a support assistant.

4.1.3 The support assistants

Ardeshir: 3 tickets resolved, 0 new, 0 open Runa: 271 tickets resolved, 0 new, 9 open Nobody: 0 tickets resolved, 172 new, 0 open

The user "Nobody" is some kind of default RT user. You can't log on to the system with this user, but all tickets are assigned to this user by default. The fact that the user has resolved tickets just means that someone forgot to take the ticket before they marked it as resolved.

4.1.4 The support requests and other things

A few users reported that the "Find Bridges Now"-button in Vidalia stopped working. This seems to be due to the addition of IPv6 bridges on `https://bridges.torproject.org/` (ticket 5370).

A number of OS X 10.5 users emailed saying they got the upgrade message, downloaded the latest TBB, and now can't get Tor to work at all. We put up a message stating we're working on the problem at Tor Browser Bundle, Mac OSX and 10.5.8.

4.2 Education & Training

- We helped with an analysis of Syrian Malware as found in the wild. See our report on Activists in Iran and Syria targeted with malicious computer software.

4.3 Outreach

1. Runa and Karen spoke at the ArabNet Digital Summit in Beirut, Lebanon.
2. Karen spoke at the Breaking through Internet Censorship in New York City.
3. Andrew spoke at the IEEE Boston, Social Implications of Technology meeting.
4. Aaron spoke at the TechCamp: Bangkok.
5. Andrew attended the reception for 101 Photos for Press Freedom: 25th Anniversary of Reporters without Borders.
6. Tor was accepted into Google Summer of Code 2012.
7. Wendy attended Open Rights Group's ORGcon. VisionOnTV did a 5-min interview about Tor with Wendy.
8. Roger and Wendy spoke at the Global Censorship Conference at the Yale Law School
9. Tor was featured in the Edmonton Journal as a privacy solution, `http://blogs.edmontonjournal.com/2012/03/01/get-your-privacy-on-with-tor/`.
10. Tor was mentioned in Ars Technica to address concerns with Google's Privacy Policy consolidation, `http://arstechnica.com/tech-policy/news/2012/03/googles-new-privacy-policy-what-has-ars`.
11. Tor was the front page of the Boston Globe about privacy software, `http://articles.boston.com/2012-03-08/business/31136655_1_law-enforcement-free-speech-technology`.
12. Tor helped Reuters with their investigation into technology used by the Iranian Government, `http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322`
13. Tor commented on the plans of the UK government to surveil the nation, `http://www.guardian.co.uk/media/2012/apr/02/internet-companies-warn-government-email-surveillance`.