From: Andrew Lewman, Executive Director

To: The Tor Community Date: November 8, 2011



This report documents progress in October 2011.

New releases, new hires, new funding

New Releases

1. On October 7th, we released a new version of Vidalia, version 0.2.15. The detailed changelog is below:

0.2.15 07-Oct-2011

Draw the bandwidth graph curves based on the local maximum, not the global maximum. Fixes bug 2188.

Add an option for setting up a non-exit relay to the Sharing configuration panel. This is meant to clarify what an exit policy and an exit relay are. Resolves bug 2644.

Display time statistics for bridges in UTC time, rather than local time. Fixes bug 3342.

Change the parameter for ordering the entries in the Basic Log list from currentTime to currentDateTime to avoid missplacing entries from different days.

Check the tor version and that settings are sanitized before trying to use the port autoconfiguration feature. Fixes bug 3843. Provide a way to hide Dock or System Tray icons in OSX. Resolves ticket 2163.

2. On October 12th, we released updated tor browser bundles.

The Tor Browser Bundles have been updated to Vidalia 0.2.15. The OS X and Linux bundles have Torbutton 1.4.4, but a hotfix for Windows was released with 1.4.4.1 because 1.4.4 had a minor issue that prevented the Windows bundle from going to https://check.torproject.org.

Tor Browser Bundle (2.2.33-3)

Update Vidalia to 0.2.15
Update Torbutton to 1.4.4.1
Update NoScript to 2.1.4
Remove trailing dash from Windows version number (closes: #4160)
Make Tor Browser (Aurora) fail closed when not launched with a TBB profile (closes: #4192)

3. On October 16th, the Tails Live System version 0.8.1 was released. Detailed changes are:

* Iceweasel

- Update to 3.5.16-10 (fixes DSA-2313-1).
- FireGPG: force crypto action results to appear in a new window, otherwise JavaScript can steal decrypted plaintext. Advice: always use FireGPG's text editor when writing text you want to encrypt. If you write it in a textbox the plaintext can be stolen through JavaScript before it is encrypted in the same way.
- Update HTTPS Everywhere extension to 1.0.3-1.
- Stop using the small version of the Tor check page. The small version incorrectly tells Tails users to upgrade their Torbrowser, which has confused some users.

* Software

- Update Linux to 3.0.0-2 (fixes DSA-2310-1, CVE-2011-2905, CVE-2011-2909, CVE-2011-2723, CVE-2011-2699, CVE-2011-1162, CVE-2011-1161).
- Update usb-modeswitch to 1.1.9-2~bpo60+1 and usb-modeswitch-data to 20110805-1~bpo60+1 from Debian backports. This adds support for a few devices such as Pantech UMW190 CDMA modem.
- Install libregexp-common-perl 2011041701-3 from Debian unstable. This fixes the bug: [[bugs/msva_does_not_use_configured_keyserver]].
- Install hdparm so the hard drives can be spinned down in order to save battery power.
- Install barry-util for better BlackBerry integration.
- Debian security upgrades: OpenOffice.org (DSA-2315-1), openjdk-6 (DSA-2311-1), policykit-1 (DSA-2319-1)
- * Protecting against memory recovery
- Set more appropriate Linux VM config before wiping memory. These parameters should make the wipe process more robust and efficient.
- 4. On Friday, October 28th, we released Tor 0.2.2.34. Tor 0.2.2.34 fixes a critical anonymity vulnerability where an attacker can deanonymize Tor users. Everybody should upgrade.
 - The attack relies on four components: 1) Clients reuse their TLS cert when talking to different relays, so relays can recognize a user by the identity key in her cert. 2) An attacker who knows the client's identity key can probe each guard relay to see if that identity key is connected to that guard relay right now. 3) A variety of active attacks in the literature (starting

from "Low-Cost Traffic Analysis of Tor" by Murdoch and Danezis in 2005) allow a malicious website to discover the guard relays that a Tor user visiting the website is using. 4) Clients typically pick three guards at random, so the set of guards for a given user could well be a unique fingerprint for her. This release fixes components 1 and 2, which is enough to block the attack; the other two remain as open research problems.

Special thanks to "frosty_un" for reporting the issue to us! (As far as we know, this has nothing to do with any claimed attack currently getting attention in the media.)

Clients should upgrade so they are no longer recognizable by the TLS certs they present. Relays should upgrade so they no longer allow a remote attacker to probe them to test whether unpatched clients are currently connected to them.

This release also fixes several vulnerabilities that allow an attacker to enumerate bridge relays. Some bridge enumeration attacks still remain; see for example proposal 188.

Changes in version 0.2.2.34 - 2011-10-26

- o Privacy/anonymity fixes (clients):
 - Clients and bridges no longer send TLS certificate chains on outgoing OR connections. Previously, each client or bridge would use the same cert chain for all outgoing OR connections until its IP address changes, which allowed any relay that the client or bridge contacted to determine which entry guards it is using. Fixes CVE-2011-2768. Bugfix on 0.0.9pre5; found by "frosty_un".
 - If a relay receives a CREATE_FAST cell on a TLS connection, it no longer considers that connection as suitable for satisfying a circuit EXTEND request. Now relays can protect clients from the CVE-2011-2768 issue even if the clients haven't upgraded yet.
 - Directory authorities no longer assign the Guard flag to relays that haven't upgraded to the above "refuse EXTEND requests to client connections" fix. Now directory authorities can protect clients from the CVE-2011-2768 issue even if neither the clients nor the relays have upgraded yet. There's a new "GiveGuardFlagTo_CVE_2011_2768_VulnerableRelays" config option to let us transition smoothly, else tomorrow there would be no guard relays.
- o Privacy/anonymity fixes (bridge enumeration):
 - Bridge relays now do their directory fetches inside Tor TLS connections, like all the other clients do, rather than connecting directly to the DirPort like public relays do. Removes another avenue for enumerating bridges. Fixes bug 4115; bugfix on 0.2.0.35.
 - Bridges relays now build circuits for themselves in a more similar way to how clients build them. Removes another avenue for enumerating bridges. Fixes bug 4124; bugfix on 0.2.0.3-alpha, when bridges were introduced.
 - Bridges now refuse CREATE or CREATE_FAST cells on OR connections

that they initiated. Relays could distinguish incoming bridge connections from client connections, creating another avenue for enumerating bridges. Fixes CVE-2011-2769. Bugfix on 0.2.0.3-alpha. Found by "frosty_un".

o Major bugfixes:

- Fix a crash bug when changing node restrictions while a DNS lookup is in-progress. Fixes bug 4259; bugfix on 0.2.2.25-alpha. Bugfix by "Tey'".
- Don't launch a useless circuit after failing to use one of a hidden service's introduction points. Previously, we would launch a new introduction circuit, but not set the hidden service which that circuit was intended to connect to, so it would never actually be used. A different piece of code would then create a new introduction circuit correctly. Bug reported by katmagic and found by Sebastian Hahn. Bugfix on 0.2.1.13-alpha; fixes bug 4212.

o Minor bugfixes:

- Change an integer overflow check in the OpenBSD_Malloc code so that GCC is less likely to eliminate it as impossible. Patch from Mansour Moufid. Fixes bug 4059.
- When a hidden service turns an extra service-side introduction circuit into a general-purpose circuit, free the rend_data and intro_key fields first, so we won't leak memory if the circuit is cannibalized for use as another service-side introduction circuit. Bugfix on 0.2.1.7-alpha; fixes bug 4251.
- Bridges now skip DNS self-tests, to act a little more stealthily. Fixes bug 4201; bugfix on 0.2.0.3-alpha, which first introduced bridges. Patch by "warms0x".
- Fix internal bug-checking logic that was supposed to catch failures in digest generation so that it will fail more robustly if we ask for a nonexistent algorithm. Found by Coverity Scan. Bugfix on 0.2.2.1-alpha; fixes Coverity CID 479.
- Report any failure in init_keys() calls launched because our IP address has changed. Spotted by Coverity Scan. Bugfix on 0.1.1.4-alpha; fixes CID 484.

o Minor bugfixes (log messages and documentation):

- Remove a confusing dollar sign from the example fingerprint in the man page, and also make the example fingerprint a valid one. Fixes bug 4309; bugfix on 0.2.1.3-alpha.
- The next version of Windows will be called Windows 8, and it has a major version of 6, minor version of 2. Correctly identify that version instead of calling it "Very recent version". Resolves ticket 4153; reported by funkstar.

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

o Minor features:

- Turn on directory request statistics by default and include them in extra-info descriptors. Don't break if we have no GeoIP database. Backported from 0.2.3.1-alpha; implements ticket 3951.
- Update to the October 4 2011 Maxmind GeoLite Country database.
- 5. On Friday October 28th, we released Tor 0.2.3.6-alpha. Tor 0.2.3.6-alpha includes the fix from 0.2.2.34 for a critical anonymity vulnerability where an attacker can deanonymize Tor users: https://lists.torproject.org/pipermail/tor-announce/2011-October/000082.html.

Everybody should upgrade.

This release also features support for a new v3 connection handshake protocol, and fixes to make hidden service connections more robust.

Changes in version 0.2.3.6-alpha - 2011-10-26

o Major features:

- Implement a new handshake protocol (v3) for authenticating Tors to each other over TLS. It should be more resistant to fingerprinting than previous protocols, and should require less TLS hacking for future Tor implementations. Implements proposal 185.
- Allow variable-length padding cells to disguise the length of Tor's TLS records. Implements part of proposal 184.

o Privacy/anonymity fixes (clients):

- Clients and bridges no longer send TLS certificate chains on outgoing OR connections. Previously, each client or bridge would use the same cert chain for all outgoing OR connections until its IP address changes, which allowed any relay that the client or bridge contacted to determine which entry guards it is using. Fixes CVE-2011-2768. Bugfix on 0.0.9pre5; found by "frosty_un".
- If a relay receives a CREATE_FAST cell on a TLS connection, it no longer considers that connection as suitable for satisfying a circuit EXTEND request. Now relays can protect clients from the CVE-2011-2768 issue even if the clients haven't upgraded yet.
- Directory authorities no longer assign the Guard flag to relays that haven't upgraded to the above "refuse EXTEND requests to client connections" fix. Now directory authorities can protect clients from the CVE-2011-2768 issue even if neither the clients nor the relays have upgraded yet. There's a new "GiveGuardFlagTo_CVE_2011_2768_VulnerableRelays" config option to let us transition smoothly, else tomorrow there would be no

guard relays.

o Major bugfixes (hidden services):

- Improve hidden service robustness: when an attempt to connect to a hidden service ends, be willing to refetch its hidden service descriptors from each of the HSDir relays responsible for them immediately. Previously, we would not consider refetching the service's descriptors from each HSDir for 15 minutes after the last fetch, which was inconvenient if the hidden service was not running during the first attempt. Bugfix on 0.2.0.18-alpha; fixes bug 3335.
- When one of a hidden service's introduction points appears to be unreachable, stop trying it. Previously, we would keep trying to build circuits to the introduction point until we lost the descriptor, usually because the user gave up and restarted Tor. Partly fixes bug 3825.
- Don't launch a useless circuit after failing to use one of a hidden service's introduction points. Previously, we would launch a new introduction circuit, but not set the hidden service which that circuit was intended to connect to, so it would never actually be used. A different piece of code would then create a new introduction circuit correctly. Bug reported by katmagic and found by Sebastian Hahn. Bugfix on 0.2.1.13-alpha; fixes bug 4212.

o Major bugfixes (other):

- Bridges now refuse CREATE or CREATE_FAST cells on OR connections that they initiated. Relays could distinguish incoming bridge connections from client connections, creating another avenue for enumerating bridges. Fixes CVE-2011-2769. Bugfix on 0.2.0.3-alpha. Found by "frosty_un".
- Don't update the AccountingSoftLimitHitAt state file entry whenever tor gets started. This prevents a wrong average bandwidth estimate, which would cause relays to always start a new accounting interval at the earliest possible moment. Fixes bug 2003; bugfix on 0.2.2.7-alpha. Reported by BryonEldridge, who also helped immensely in tracking this bug down.
- Fix a crash bug when changing node restrictions while a DNS lookup is in-progress. Fixes bug 4259; bugfix on 0.2.2.25-alpha. Bugfix by "Tey'".

o Minor bugfixes (on 0.2.2.x and earlier):

- When a hidden service turns an extra service-side introduction circuit into a general-purpose circuit, free the rend_data and intro_key fields first, so we won't leak memory if the circuit is cannibalized for use as another service-side introduction circuit. Bugfix on 0.2.1.7-alpha; fixes bug 4251.

- Rephrase the log message emitted if the TestSocks check is successful. Patch from Fabian Keil; fixes bug 4094.
- Bridges now skip DNS self-tests, to act a little more stealthily. Fixes bug 4201; bugfix on 0.2.0.3-alpha, which first introduced bridges. Patch by "warms0x".
- Remove a confusing dollar sign from the example fingerprint in the man page, and also make the example fingerprint a valid one. Fixes bug 4309; bugfix on 0.2.1.3-alpha.
- Fix internal bug-checking logic that was supposed to catch failures in digest generation so that it will fail more robustly if we ask for a nonexistent algorithm. Found by Coverity Scan. Bugfix on 0.2.2.1-alpha; fixes Coverity CID 479.
- Report any failure in init_keys() calls launched because our IP address has changed. Spotted by Coverity Scan. Bugfix on 0.1.1.4-alpha; fixes CID 484.

o Minor bugfixes (on 0.2.3.x):

- Fix a bug in configure.in that kept it from building a configure script with autoconf versions earlier than 2.61. Fixes bug 2430; bugfix on 0.2.3.1-alpha.
- Don't warn users that they are exposing a client port to the Internet if they have specified an RFC1918 address. Previously, we would warn if the user had specified any non-loopback address. Bugfix on 0.2.3.3-alpha. Fixes bug 4018; reported by Tas.
- Fix memory leaks in the failing cases of the new SocksPort and ControlPort code. Found by Coverity Scan. Bugfix on 0.2.3.3-alpha; fixes coverity CIDs 485, 486, and 487.

o Minor features:

- When a hidden service's introduction point times out, consider trying it again during the next attempt to connect to the HS. Previously, we would not try it again unless a newly fetched descriptor contained it. Required by fixes for bugs 1297 and 3825.
- The next version of Windows will be called Windows 8, and it has a major version of 6, minor version of 2. Correctly identify that version instead of calling it "Very recent version". Resolves ticket 4153; reported by funkstar.
- The Bridge Authority now writes statistics on how many bridge descriptors it gave out in total, and how many unique descriptors it gave out. It also lists how often the most and least commonly fetched descriptors were given out, as well as the median and 25th/75th percentile. Implements tickets 4200 and 4294.
- Update to the October 4 2011 Maxmind GeoLite Country database.
- o Code simplifications and refactoring:

- Remove some old code to remember statistics about which descriptors we've served as a directory mirror. The feature wasn't used and is outdated now that microdescriptors are around.
- Rename Tor functions that turn strings into addresses, so that "parse" indicates that no hostname resolution occurs, and "lookup" indicates that hostname resolution may occur. This should help prevent mistakes in the future. Fixes bug 3512.
- 6. On October 30th, we released Tor 0.2.3.7-alpha. Tor 0.2.3.7-alpha fixes a crash bug in 0.2.3.6-alpha introduced by the new v3 handshake. It also resolves yet another bridge address enumeration issue.

Changes in version 0.2.3.7-alpha - 2011-10-30

- o Major bugfixes:
 - 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.
 - Fix a double-free bug that would occur when we received an invalid certificate in a CERT cell in the new v3 handshake. Fixes bug 4343; bugfix on 0.2.3.6-alpha.
 - Bridges no longer include their address in NETINFO cells on outgoing OR connections, to allow them to blend in better with clients. Removes another avenue for enumerating bridges. Reported by "troll_un". Fixes bug 4348; bugfix on 0.2.0.10-alpha, when NETINFO cells were introduced.
- o Trivial fixes:
 - Fixed a typo in a hibernation-related log message. Fixes bug 4331; bugfix on 0.2.2.23-alpha; found by "tmpname0901".

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

- Developed short user manual to ship with get-tor email autoresponses, and for a single page reference guide to Tor. See https://torproject.org/docs/short-user-manual.html.en.
- Tor users requesting packages too large for their email provider to accept now get a nice and polite note from GetTor. Part of https://trac.torproject.org/projects/tor/ticket/ 3920, https://trac.torproject.org/projects/tor/ticket/4166, and https://trac.torproject.org/projects/tor/ticket/2520.
- Added GetTor package updates to cron so we don't need to run the package fetching and updating mechanism by hand.

- Added five new website and distribution mirrors, https://www.torproject.org/getinvolved/mirrors.html.en.
- Researching some new blocking mechanisms seen in China regarding Tor bridges. Tracked at https://trac.torproject.org/projects/tor/ticket/4185. Need to collect more data. Others unrelated to Tor may be seeing something similar, http://www.nsc.liu.se/~nixon/sshprobes.html.

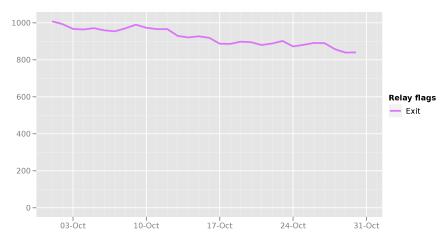
Hide Tor's network signature.

- Modular transports are a way to decouple protocol-level obfuscation from the core Tor protocol in order to better resist client-bridge censorship. Our approach is to specify a means to add pluggable transport implementations to Tor clients and bridges so that they can negotiate a superencipherment for the Tor protocol. We described the necessary changes to Tor in proposal 180, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/180-pluggable-transport.txt. The implementation is mostly done, but not merged yet, which should be done by the end of November.
- We built obfsproxy, https://gitweb.torproject.org/obfsproxy.git/blob/HEAD:/doc/protocol-spec.txt, which is a protocol obfuscation layer for TCP protocols. obfsproxy does not provide authentication or data integrity and does not hide data lengths. It is more suitable for providing a layer of obfuscation for an existing authenticated protocol, like SSH or TLS.
- Tor 0.2.3.6 is the first version to contain a new handshake protocol (v3) for authenticating Tors to each other over TLS. The v3 protocol should allow us to become more resistant to fingerprinting than previous protocols, and should require less TLS hacking for future Tor implementations. Implements proposal 176, https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/176-revising-handshake.txt. The v3 protocol gets used between any two Tors that both are running Tor version 0.2.3.6 or later. There are still bugs in the v3 handshake code, the most significant of which are fixed in Tor 0.2.3.7.

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/

Number of relays

This graph shows the total quantity of exit relays in October 2011. There is a reduction of 200 exit relays over the month for unknown reasons. Possibly a number of relays switched from exit to non-exit roles.

2500 - 2000 - 1500 - Relays - Bridges

17-Oct

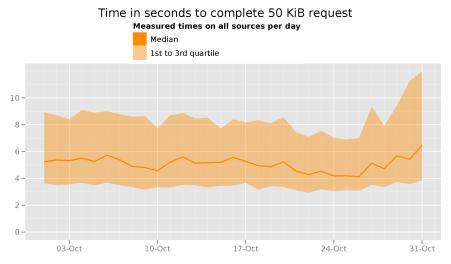
The Tor Project - https://metrics.torproject.org/

10-Oct

03-Oct

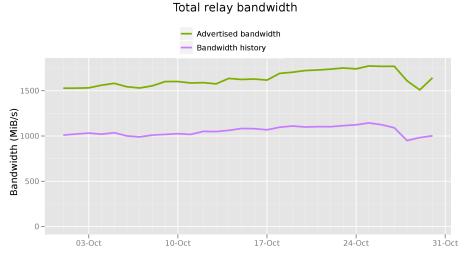
This graph shows the total quantity of relays and the total quantity of bridges in October 2011.

31-Oct



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. Average latency has increased slightly to 6 seconds at the end of the month. This is likely due to the loss of a number of exit relays throughout the month.



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. The decrease in relays overall reduces the available bandwidth. We're still at a capacity of 1.6 GBps (12.8 Gbps) available with 1 GBps (8 Gbps) used.

Outreach and Advocacy

- 1. Jacob, Roger, and Arturo traveled to Tunisia for the 2011 Arab Blogger Conference. Roger wrote up a detailed trip report at https://blog.torproject.org/blog/trip-report-arab-bloggers-mee
- 2. The Persian News Network did a 14 minute segment on Tor, censorship circumvention, and empowering citizens to gain access to information. A copy of the video segment is available at https://media.torproject.org/video/PERSIAN_2_0.mp4.
- 3. Damian represented Tor at the Google Summer of Code 2011 Mentor Summit, http://gsoc-wiki.osuosl.org/index.php/2011.
- 4. Karen, Runa, and Mike attended the Silicon Valley Human Rights Conference, https://www.rightscon.org/.
- 5. Jacob spoke at the Julia Group/Sida Internet and Democratic Change conference, http://juliagruppen.se/lang/en/2011/09/internet-och-demokratisk-forandringinternet-and-democrati
- 6. Andrew, Roger, Nick, and Runa produced a public response to various rumors of Tor's global compromise, https://blog.torproject.org/blog/rumors-tors-compromise-are-greatly-exaggerate-
- 7. Jacob attended ISS World in Washington DC to learn about the current state of the art in detecting Tor, http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques Jacob was asked to leave on the second day of the conference.
- 8. Jacob and others found evidence that Blue Coat Systems devices are being used in Syria, furthermore to possibly track and filter Tor connections to public relays. http://motherjones.com/mojo/2011/10/blue-coat-admits-syria-connection.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

- We publicly announced our intention to reconfigure our software into Tor Browser Bundle, and various relay/bridge/exit-relay by default bundles for easier client configuration and usage, https://blog.torproject.org/blog/plain-vidalia-bundles-be-discontinued-dont-panic.
- Started a draft of the Tor Browser Design, https://www.torproject.org/projects/torbrowser/design/. This document describes the adversary model, design requirements, implementation, packaging and testing procedures of the Tor Browser. It is current as of Tor Browser 2.2.33-3.

This document is also meant to serve as a set of design requirements and to describe a reference implementation of a Private Browsing Mode that defends against active network adversaries, in addition to the passive forensic local adversary currently addressed by the major browsers.

Bridge relay and bridge authority work.

• Karsten analyzed what fraction of bridges does not report statistics (https://trac.torproject.org/projects/tor/ticket/3261). Next step will be to investigate reasons why bridges don't report statistics (less than 24 hours uptime, delayed descriptor publication, old versions, etc.).

• Karsten finished a bridge stability analysis (https://trac.torproject.org/projects/tor/ticket/4255). The focus is how BridgeDB can track bridge stability and give out at least one stable bridge per user https://metrics.torproject.org/papers/bridge-stability-2011-10-31.pdf.

Scalability, load balancing, directory overhead, efficiency.

- Setup a new bandwidth authority in Sweden. We now have five bandwidth authorities measuring and load balancing the Tor network.
- Replaced a bandwidth authority with new dedicated hardware for more reliable measurements and performance. A snowstorm promptly took out its Internet connection for two days. The authority is backonline and operating within acceptable parameters.
- Nick finished and merged his implementation of proposal 176 to provide the v3 handshake protocol. This removes the need for TLS renegotiation from the Tor handshake protocol. See https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/176-revising-handshake.txt for details.
- Nick wrote proposal 186 to describe how to give multiple ORPorts and addresses to a Tor node so as to make IPv6 migration plausible. This may be over-engineered; more discussion needed. Proposal 186 can be found at https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/186-multiple-orports.txt.
- Nick wrote proposal 187 to specify a way to allow a future cell type for a client authorization step. Proposal 187 can be found at https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/187-allow-client-auth.txt.
- Nick wrote proposal 188 to explain bridge guards, a fairly versatile (though not absolutely comprehensive) anti-enumeration mechanism. Proposal 188 can be found at https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/188-bridge-guards.txt.
- Nick wrote a long but important document explaining (ok, guessing) where we should take our crypto over the next year or so. More insight and thoughts are needed. Join the conversation at https://lists.torproject.org/pipermail/tor-dev/2011-November/002999.html.

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.

- Translation updates for get-tor, vidalia, vidalia-help, vidalia-installer, short user manual, bridge db, torbutton, and orbot.
- Language translation updates in Hebrew, Arabic, Catalan, Danish, German, Greek, Spanish, Persian, French, Hindi, Hungarian, Macedonian, Norwegian, Dutch, Polish, Slovenian, Serbian, Swedish, and Mandarin Chinese.
- Find all of the supported languages and their current translation status at https://www.transifex.net/projects/p/torproject/r/all-resources/.