From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: June 6, 2009

This report documents progress in May 2009 on contract BBGCON1807S6441 between BBG and The Tor Project.

C. New releases, new hires, new funding

On May 25, we released Tor 0.2.1.15-rc containing:

Major bugfixes (on 0.2.0.x):

- Fix a timing-dependent, allocator-dependent, DNS-related crash bug that would occur on some exit nodes when DNS failures and timeouts occurred in certain patterns. Fix for bug 957.

Minor bugfixes (on 0.2.0.x):

- Actually return -1 in the error case for read_bandwidth_usage(). Harmless bug, since we currently don't care about the return value anywhere. Bugfix on 0.2.0.9-alpha.
- Provide a more useful log message if bug 977 (related to buffer freelists) ever reappears, and do not crash right away.
- Fix an assertion failure on 64-bit platforms when we allocated memory right up to the end of a memarea, then realigned the memory one step beyond the end. Fixes a possible cause of bug 930.
- Protect the count of open sockets with a mutex, so we can't corrupt it when two threads are closing or opening sockets at once. Fix for bug 939. Bugfix on 0.2.0.1-alpha.
- Don't allow a bridge to publish its router descriptor to a non-bridge directory authority. Fixes part of bug 932.
- When we change to or from being a bridge, reset our counts of client usage by country. Fixes bug 932.
- Fix a bug that made stream bandwidth get misreported to the controller.
- Stop using malloc_usable_size() to use more area than we had actually allocated: it was safe, but made valgrind really unhappy.
- Fix a memory leak when v3 directory authorities load their keys and cert from disk. Bugfix on 0.2.0.1-alpha.

Minor bugfixes (on 0.2.1.x):

- Fix use of freed memory when deciding to mark a non-addable descriptor as never-downloadable. Bugfix on 0.2.1.9-alpha.

On May 17, we released Tor VM 0.0.2.

On May 25, we released Vidalia 0.1.13 containing:

o Remove an old warning on the relay settings page that running a bridge relay requires Tor 0.2.0.8-alpha or newer.
o Add a workaround for a bug that prevented Vidalia's tray icon from getting added to the system notification area on Gnome when Vidalia was run on system startup. Patch by Steve Tyree. (Ticket #247)
o Fix a bug that prevented the control panel from displaying when running on the Enlightenment window manager. Patch by Steve Tyree.
o Rename the CMake variables used to store the location of Qt's lupdate and lrelease executables. Recent versions of CMake decided to use the same variable name, which was stomping on mine, resulting in the wrong lupdate and lrelease executables being used.
o Use the TorProcess subclass of QProcess for launching Tor when hashing a control password so we can take advantage of its PATH+=:/usr/sbin trick on Debian there too.
o If a RouterDescriptor object is empty, don't try to display it in the router descriptor details viewer. (Ticket #479)
o Wait until Vidalia has registered for log events via the control port before ignoring Tor's output on stdout. Previously we would start ignoring Tor's stdout after successfully authenticating, but before registering for log events which, in some cases, could lead to messages not appearing in the message log.
o Update many translations and remove others than are no longer up-to-date enough to be useful.

On May 25th, we released Tor Browser Bundle 1.2.0 containing:

Switch to launching Firefox directly from Vidalia to
allow multiple instances of Firefox
Update Firefox to 3.0.10
Update to Qt 4.5.1
Update Firefox prefs.js to stop scanning for plugins
Update libevent to 1.4.11
Include the Tor geoip database
Update Vidalia to 0.1.13
Update Tor to 0.2.1.15-rc

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Matt added "fetch bridges" features to Vidalia 0.2.x. This provides a link to automatically request

bridges from https ://bridges.torproject.org for users.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

Proposal 160 aims to let authorities modify the bandwidth they put in the consensus for each relay. This step will allow us to adjust the weights we advertise for clients, once the measurements from TorFlow start giving us better weights.
https://git.torproject.org/checkout/tor/master/doc/spec/proposals/160-bandwidth-offset.txt

Proposal 161 you already note in C.2.13, but worth noting here too.
https://git.torproject.org/checkout/tor/master/doc/spec/proposals/161-computing-bandwidth-adjustments.txt

Proposal 162 describes "consensus flavors": the size of the networkstatus consensus is critical, since every user fetches it every few hours. So we need a way to add new fields -- and remove old fields -- in a way that lets old clients continue to use the consensus. The current plan is to build and distribute several different versions at once, so each client can fetch the one with the format they expect.
https://git.torproject.org/checkout/tor/master/doc/spec/proposals/162-consensus-flavors.txt

Proposal 163 starts to consider the problem of clients using relays as single-hop proxies. If many clients start doing this (say, to improve their own performance), it puts additional risk on the relays, since now an attacker can expect to discover both client origins and destinations by attacking the relay. Our current strategy for forcing clients to use more than one hop is quite fragile, and it looks like we will soon need more robust strategies.
https://git.torproject.org/checkout/tor/master/doc/spec/proposals/163-detecting-clients.txt

Proposal 164 suggests ways to make it easier for relay operators to discover why they are not listed in the networkstatus consensus. We have a handle of people each week ask us on IRC why their relay isn't listed, and currently the only way to answer is to have a competent directory authority operator go dig around in various files in his datadirectory.
https://git.torproject.org/checkout/tor/master/doc/spec/proposals/164-reporting-server-status.txt

Proposal 165 focuses on simplifying the steps required to add a new directory authority. The current approach requires manual work from every directory authority operator within a space of several hours. As the number of authorities grows, this synchronization is becoming impractical -- and that's causing us to leave the number of authorities small, which makes us vulnerable to other attacks. Once this proposal is finalized and deployed, we'll hopefully be able to add new authorities more

smoothly.
https://git.torproject.org/checkout/tor/master/doc/spec/proposals/165-simple-robust-voting.txt

C.2.5. Hide Tor's network signature.

Nothing to report.

C. 2.10 Grow the Tor network and user base. Outreach.

Jacob attended CONFidence in Krakow, Poland as a keynote speaker. http://2009.confidence.org.pl/

Andrew and Jacob attended the Soul of a New Machine conference in Berkeley, CA. http://hrc.berkeley.edu/events/newmachineconference/

Roger and Andrew attended the 7th Annual Chinese Internet Research Conference in Philadelphia, PA. http://www.global.asc.upenn.edu/index.php?page=167

Karsten attended SIGINT 09 in Cologne.

Mike gave a presentation on TorFlow at CodeCon.

Roger met with Nick, Paul Syverson and Aaron Johnson at Yale to work more on Paul's research question: if we trust some Tor relays differently than others, how should we select our paths to be safe, and how do we analyze how safe the paths are?

Roger did a talk for about 15 OSI people in Budapest, Hungary.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

Tor Browser 1.2.0 was released on May 25th. The changes were:
Switch to launching Firefox directly from Vidalia to
allow multiple instances of Firefox
Update Firefox to 3.0.10
Update to Qt 4.5.1
Update Firefox prefs.js to stop scanning for plugins
Update libevent to 1.4.11
Include the Tor geoip database
Update Vidalia to 0.1.13
Update Tor to 0.2.1.15-rc

The two large changes were the ability to run multiple instances of Firefox at once, such that a user's personal firefox shouldn't share data with the firefox from our bundle. The other change is the ability to stop TBB firefox from scanning the system for potential plugins, like Windows Media, Java, etc.

Started work on a hardened branch of Incognito live CD to help protect users from possible bugs in the programs running.

C.2.12 Bridge relay and bridge authority work.

Nothing to report.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

We documented the metrics we collect to help us determine the best ways to scale the Tor network. http://blog.torproject.org/blog/performance-measurements-and-blockingresistance-analysis-tor-network A number of nodes are now collecting this information to assist our network-wide measurements.

Much progress on torctl and torflow tools being used to measure real and potential performance of nodes in the public tor network.

Mike wrote proposal 161 describing how node bandwidth ratios are computed and how they can be produced in parallel. The proposal can be found at http://git.torproject.org/checkout/tor/master/doc/spec/proposals/161-computing-bandwidth-adjustments.txt

Karsten finished a first patch to dump statistics about local queues to disk every 15 minutes. A first impression of how these data could be evaluated can be found in http://freehaven.net/~karsten/volatile/bufferstats-2009-05-25.pdf. The goal is to see if our buffer allocation algorithms are sufficient or need tweaking.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Developed the ability to split Apple OS X bundles into 1.44MB chunks. The functionality is native to OS X versions 10.4 and newer. It will not work in versions 10.3.9 or earlier releases.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

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

From: Roger Dingledine, Tor Project Leader
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: February 10, 2008

This report documents progress in January 2009 on contract BBGCON1807S6441 between BBG and The Tor Project.

C.2.0. New releases, new hires, new funding

Tor 0.2.1.10-alpha (released January 6) fixes two major bugs in bridge relays (one that would make the bridge relay not so useful if it had DirPort set to 0, and one that could let an attacker learn a little bit of information about the bridge's users), and a bug that would cause your Tor relay to ignore a circuit create request it can't decrypt (rather than reply with an error). It also fixes a wide variety of other bugs.
http://archives.seul.org/or/talk/Jan-2009/msg00078.html

Tor 0.2.1.11-alpha (released Jan 20) finishes fixing the "if your Tor is off for a week it will take a long time to bootstrap again" bug. It also fixes an important security-related bug reported by Ilja van Sprundel. You should upgrade. (We'll send out more details about the bug once people have had some time to upgrade.)
http://archives.seul.org/or/talk/Jan-2009/msg00171.html

Tor 0.2.0.33 (released Jan 21) fixes a variety of bugs that were making relays less useful to users. It also finally fixes a bug where a relay or client that's been off for many days would take a long time to bootstrap.
http://archives.seul.org/or/announce/Jan-2009/msg00000.html

Tor Browser Bundle 1.1.8 (released Jan 22) updates Tor to 0.2.1.11-alpha (security update), updates OpenSSL to 0.9.8j (security update), updates Firefox to 3.0.5, updates Pidgin to 2.5.4, and updates libevent to 1.4.9.
https://svn.torproject.org/svn/torbrowser/trunk/README

This month we also hired three new people: Martin Peck is working on Tor VM, a new way of packaging Tor on Windows that will let people use Youtube safely again; Mike Perry is working on Torbutton maintenance and development and on Torflow, a set of scripts to do measurements on the Tor network; and Andrew Lewman is our new executive director.
C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

We continued enhancements to the Chinese and Russian Tor website translations. Our Farsi translation from this summer is slowly becoming obsolete; we should solve that at some point.

Major bugfixes in the Tor 0.2.1.10-alpha and 0.2.0.33 releases:
- If the cached networkstatus consensus is more than five days old, discard it rather than trying to use it. In theory it could be useful because it lists alternate directory mirrors, but in practice it just means we spend many minutes trying directory mirrors that are long gone from the network. Helps bug 887 a bit; bugfix on 0.2.0.x.

Tor 0.2.1.10-alpha contains cleanups that let Tor build on Google's Android phone:
- Change our header file guard macros to be less likely to conflict with system headers. Adam Langley noticed that we were conflicting with log.h on Android.

Major bugfixes in the Tor 0.2.1.11-alpha and 0.2.0.33 releases:
- Discard router descriptors as we load them if they are more than five days old. Otherwise if Tor is off for a long time and then starts with cached descriptors, it will try to use the onion keys in those obsolete descriptors when building circuits. Bugfix on 0.2.0.x. Fixes bug 887.

Security bugfixes in the Tor 0.2.1.11-alpha and 0.2.0.33 releases:
- Fix a heap-corruption bug that may be remotely triggerable on some platforms. Reported by Ilja van Sprundel.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

Proposal 158 ("Clients download consensus + microdescriptors") suggests a new way forward for reducing directory overhead for clients, and replaced part of proposal 141. Rather than modifying the circuit-building protocol to fetch a server descriptor inline at each circuit extend, we instead put all of the information that clients need either into the consensus itself, or into a new set of data about each relay called a microdescriptor.
https://svn.torproject.org/svn/tor/trunk/doc/spec/proposals/158-microdescriptors.txt

C.2.5. Hide Tor's network signature.

>From the 0.2.0.33 ChangeLog:

- Never use OpenSSL compression: it wastes RAM and CPU trying to compress cells, which are basically all encrypted, compressed, or both. It also made us stand out from other applications on the wire.

Nobody has blocked the new signature, as far as we know.

We have built a plan for how to address potential ways for people to block Tor based on its network signature. We are aiming to have an internal list of known potential vulnerabilities by early 2009, along with suggested paths to addressing each. Then we can react to actual blocking as it occurs, and periodically update our list of potential flaws and intended solutions as we get more intuition.

More on that in February.

C.2.10. Grow the Tor network and user base. Outreach.

Jillian York continued blogging for us about the good uses of Tor:
http://www.knightpulse.org/blog/tor

"Federico Heinz advocates anonymous browsing in Argentina", Jan 8
http://www.knightpulse.org/blog/09/01/08/federico-heinz-advocates-anonymous-browsing-argentina

"Human Rights Organizations in Argentina welcome anonymous browsing", Jan 25
http://www.knightpulse.org/blog/09/01/25/human-rights-organizations-argentina-welcome-anonymous-browsing

"Watch how you get around", Jan 30
http://www.knightpulse.org/blog/09/01/30/watch-how-you-get-around

[more soon]

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

Tor Browser Bundle 1.1.8 (released Jan 22) updates Tor to 0.2.1.11-alpha (security update), updates OpenSSL to 0.9.8j (security update), updates Firefox to 3.0.5, updates Pidgin to 2.5.4, and updates libevent to 1.4.9.
https://svn.torproject.org/svn/torbrowser/trunk/README

We continued work on Vidalia features to support where we want Tor Browser Bundle to go. In particular, we're changing it to be able to launch Firefox natively, rather than use the "PortableFirefox" pile of complex scripts. We hope this change will also let users run a normal

Firefox alongside TBB. More on that in February.

We also continued work on Tor VM, a new way of packaging Tor on Windows that will (among other things) let people use Youtube safely again. Hopefully we'll have some simple instructions up about that in February too.

C. Bridge relay and bridge authority work.

Major bugfixes in the Tor 0.2.1.10-alpha and 0.2.0.33 releases:
- Bridge relays that had DirPort set to 0 would stop fetching descriptors shortly after startup, and then briefly resume after a new bandwidth test and/or after publishing a new bridge descriptor. Bridge users that try to bootstrap from them would get a recent networkstatus but would get descriptors from up to 18 hours earlier, meaning most of the descriptors were obsolete already. Reported by Tas; bugfix on 0.2.0.13-alpha.
- Prevent bridge relays from serving their 'extrainfo' document to anybody who asks, now that extrainfo docs include potentially sensitive aggregated client geoip summaries. Bugfix on 0.2.0.13-alpha.

Bugfixes in the Tor 0.2.1.10-alpha release:
- When we made bridge authorities stop serving bridge descriptors over unencrypted links, we also broke DirPort reachability testing for bridges. So bridges with a non-zero DirPort were printing spurious warns to their logs. Bugfix on 0.2.0.16-alpha. Fixes bug 709.

New feature in Tor 0.2.1.10-alpha:
- New controller event "clients_seen" to report a geoip-based summary of which countries we've seen clients from recently. Now controllers like Vidalia can show bridge operators that they're actually making a difference.

Vidalia will add support for this feature in February.

Karsten began to crunch the numbers on all our historical bridge relay information, to look for trends, and to start being able to display the database more graphically. We sent some graphs about this in January, but we're aiming to have improved graphs in February.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

Circuit-building speedups in Tor 0.2.1.10-alpha:

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: April 7, 2009

This report documents progress in March 2009 on contract BBGCON1807S6441 between BBG and The Tor Project.

C. New releases, new hires, new funding

On March 9, we released Tor 0.2.1.13-alpha. It includes the following fixes and enhancements:

o Major bugfixes:
- Correctly update the list of which countries we exclude as exits, when the GeoIP file is loaded or reloaded. Diagnosed by lark. Bugfix on 0.2.1.6-alpha.

o Minor bugfixes (on 0.2.0.x and earlier):
- Automatically detect MacOSX versions earlier than 10.4.0, and disable kqueue from inside Tor when running with these versions. We previously did this from the startup script, but that was no help to people who didn't use the startup script. Resolves bug 863.
- When we had picked an exit node for a connection, but marked it as "optional", and it turned out we had no onion key for the exit, stop wanting that exit and try again. This situation may not be possible now, but will probably become feasible with proposal 158. Spotted by rovv. Fixes another case of bug 752.
- Clients no longer cache certificates for authorities they do not recognize. Bugfix on 0.2.0.9-alpha.
- When we can't transmit a DNS request due to a network error, retry it after a while, and eventually transmit a failing response to the RESOLVED cell. Bugfix on 0.1.2.5-alpha.
- If the controller claimed responsibility for a stream, but that stream never finished making its connection, it would live forever in circuit_wait state. Now we close it after SocksTimeout seconds. Bugfix on 0.1.2.7-alpha; reported by Mike Perry.
- Drop begin cells to a hidden service if they come from the middle of a circuit. Patch from lark.
- When we erroneously receive two EXTEND cells for the same circuit ID on the same connection, drop the second. Patch from lark.
- Fix a crash that occurs on exit nodes when a nameserver request

timed out. Bugfix on 0.1.2.1-alpha; our CLEAR debugging code had been suppressing the bug since 0.1.2.10-alpha. Partial fix for bug 929.
- Do not assume that a stack-allocated character array will be 64-bit aligned on platforms that demand that uint64_t access is aligned. Possible fix for bug 604.
- Parse dates and IPv4 addresses in a locale- and libc-independent manner, to avoid platform-dependent behavior on malformed input.
- Build correctly when configured to build outside the main source path. Patch from Michael Gold.
- We were already rejecting relay begin cells with destination port of 0. Now also reject extend cells with destination port or address of 0. Suggested by lark.

o Minor bugfixes (on 0.2.1.x):
- Don't re-extend introduction circuits if we ran out of RELAY_EARLY cells. Bugfix on 0.2.1.3-alpha. Fixes more of bug 878.
- If we're an exit node, scrub the IP address to which we are exiting in the logs. Bugfix on 0.2.1.8-alpha.

o Minor features:
- On Linux, use the prctl call to re-enable core dumps when the user is option is set.
- New controller event NEWCONSENSUS that lists the networkstatus lines for every recommended relay. Now controllers like Torflow can keep up-to-date on which relays they should be using.
- Update to the "February 26 2009" ip-to-country file.

On March 10, we released Tor Browser Bundle 1.1.10. It includes:
- Update Tor to 0.2.1.13-alpha
- Update Firefox to 3.0.7
- Update Pidgin to 2.5.5

On March 31, we released Tor Browser Bundle 1.1.11. It includes:
- Update Firefox to 3.0.8
- Add Italian language bundles
- Update Torbutton to 1.2.1
- Update Vidalia to 0.1.12

On March 21, we released Torbutton 1.2.1, it includes:

- bugfix: bug 773: Fixed Noscript conflict issue.
- bugfix: bug 866: Fixed conflict with ZoTero
- bugfix: bug 908: Make UserAgentSwitcher's 'default' button restore Torbutton's spoofed user agent if Tor is enabled.
- bugfix: bug 909: Get Torbutton to "properly" react to users changing their Firefox cookie lifetime settings as opposed to using the Torbutton interface.
- bugfix: bug 834: Fix session saving and startup issues
- bugfix: bug 875: Removed docShell == null popup during toggle for some users
- bugfix: bug 910: fixed a locale spoofing issue in navigator.appVersion
- bugfix: bug 747: Attempt to fix 'fullscreen' resizing issues.
- bugfix: Stop-gap timezone spoofing fix for Linux and Mac for FF3. Requires a one-line patch to Firefox for Windows to work.
- bugfix: Clear SSL Session IDs on toggle. (See FF Bug 448747)
- misc: bug 931: Added a socks v4 vs v5 version choice to custom prefs.
- misc: bug 836: redesign startup preference window to make it more understandable
- misc: Torbutton now presents itself as Windows FF3.0.7.

On March 16, we released TorVM 0.0.1 as a testing release for user feedback and testing. More about TorVM can be read at https://www.torproject.org/torvm/

Vidalia 0.1.12 16-Mar-2009
o Fix a bug in the hidden service settings configuration class that could lead to compile errors in Visual Studio and on IRIX.
o Fix a build error that occurred on IRIX when using the MIPSPro compiler. Patch from Matthew Saunier.
o Remove two duplicated strings in the Spanish translation of Qt's internal strings (qt_es.po). The duplicated strings caused build errors when building with Qt 4.5. (Ticket #469)
o Remove the code that altered PublishServerDescriptor when becoming a bridge, since Tor handles that itself now, and ensure that BridgeRelay is reset when going from bridge to just-a-client mode.
o Remove an unnecessary #include from helpbrowser.cpp.
o Add an application icon based on Tor's logo to the vidalia.desktop file.

Vidalia 0.2.0 19-Mar-2009
o Add support for changing UI languages without having to restart Vidalia.
o Add preliminary support for using the KDE Marble widget for the network map. It's currently a compile-time option and is disabled by default.
o Add support for displaying Tor's plaintext port warnings. Also gives

the user the option to disable future warnings.
o Add an interface for displaying the geographic distribution of clients who have recently used a bridge operator's relay.
o Add tooltips to tree items in the help browser's table of contents. Some of the help topic labels are a bit long.
o Switch to a simpler About dialog and move the license information to a separate HTML-formatted display.
o Switch to a simpler drag-and-drop installer in the OS X bundles.
o Switch to an MSI-based installer on Windows.
o Clear the list of default CA certificates used by QSslSocket before adding the only one we care about. Suggested by coderman.
o Support building with Visual Studio again.
o Add a Debian package structure from dererk.
o Updated Albanian, Czech, Finnish, Polish, Portuguese, Romanian, Swedish, Turkish and many other translations.

The Vidalia 0.2.0 release was also posted to the blog,
https://blog.torproject.org/blog/technology-preview-marble-and-vidalia020

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

The Torbutton 1.2.1 update fixes a number of bugs that protect users in censored countries. Continued work on TorVM for easier and safer usage of Tor. Continued development of the secure updater client for Tor.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

Nick wrote up a blog entry describing our current plans for making libevent (and ultimately) Tor work well on Windows:
https://blog.torproject.org/blog/some-notes-progress-iocp-and-libevent

C.2.5. Hide Tor's network signature.

No progress.

C. 2.10 Grow the Tor network and user base. Outreach.

Andrew attended the LibrePlanet 2009 conference,
http://www.fsf.org/associate/meetings/2009/. Discussed Tor, free network services, and free software.

Karsten, Sebastian, and others helped organize and then attended Pet-Con 2009, http://www.pet-con.org/index.php/PET_Convention_2009.1.

Nick wrote a blog post about the secure updater for Tor, codenamed Thandy, for Google's Open Source blog: http://google-opensource.blogspot.com/2009/03/thandy-secure-update-for-tor.html

Finished analyzing directory archives from February 2006 to February 2009. This analysis gives a slightly better picture of the Tor network than the analysis of the 2008 data. The analysis shows that there is a clear trend reversal in the number of German relays in 2008, , but for other countries the number of relays has continued to increase.

http://freehaven.net/~karsten/metrics/dirarch-2009-03-31.pdf

On March 17, Roger attended a hearing at the US Sentencing Commission, where Seth Schoen from EFF was testifying in opposition to a new "if you use a proxy when committing a crime, it's a sophisticated crime so you get more jail-time" clause they were considering. It turned out one of the commissioners is an avid Tor user, so they were sympathetic to his testimony.

On March 24-25, Roger and Andrew met with the Psiphon team in Toronto. We taught them about Tor's perspective on blocking-resistance, and about our bridges design. We also helped review their future design plans. We still have concerns that their closed design and implementation will ultimately mean they are less effective than they could be, but it's good to have alternate circumvention approaches available.

Tor (in combination with EFF) got accepted to Google Summer of Code 2009. Google will be funding roughly 5 students to work on Tor-related development projects over this coming summer:
https://blog.torproject.org/blog/eff-and-tor-google-summer-code-2009
Our current thoughts are to focus on porting Polipo to Windows; improving usability and features for Torbutton; working harder to get WML support into Pootle, so people can translate our website with a browser; and further work on Thandy to make it scale better when 100000 users all try to upgrade in the same day.

Hal Roberts released his Berkman Center report on the "landscape of circumvention technologies" as of 2007, which recommends Tor and Psiphon:

https://blog.torproject.org/blog/berkman-2007-circumvention-landscape-and-progress

Roger and Nick participated in the Codecon program committee, and helped to choose a variety of good development projects to showcase in April. Two of these turned out to be libevent (including the new Windows work), and Torflow:
http://www.codecon.org/2009/program.html

Roger had lunch on March 4 with Micah Sherr, a PhD student at Penn who is working on a new path selection algorithm for Tor, that tries to minimize path latency rather than maximize bandwidth. Roger poked some holes in his design, and hopefully will help him over the next few months to fix them. You can read more about Micah's design in Section 4.3 of the "performance.pdf" document.

We worked with Global Voices to help them update their "guide to blogging anonymously":
https://blog.torproject.org/blog/updated-guide-blogging-anonymously
In particular, we updated it to include recommendations for using Tor Browser Bundle, since TBB didn't exist when the guide was first written.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

On March 10, we released Tor Browser Bundle 1.1.10. It includes:

- Update Tor to 0.2.1.13-alpha
- Update Firefox to 3.0.7
- Update Pidgin to 2.5.5

On March 31, we released Tor Browser Bundle 1.1.11. It includes:

- Update Firefox to 3.0.8
- Add Italian language bundles
- Update Torbutton to 1.2.1
- Update Vidalia to 0.1.12

C.2.12 Bridge relay and bridge authority work.

From the changelog item from Vidalia 0.1.12:

o Remove the code that altered PublishServerDescriptor when becoming a bridge, since Tor handles that itself now, and ensure that BridgeRelay is reset when going from bridge to just-a-client mode.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

Roger and Steven wrote the Performance Roadmap as published at
https://www.torproject.org/press/2009-03-12-performance-roadmap-press-release.html.en

Karsten analyzed client requests to three directories run on non-authority IP addresses. The results are pretty interesting:
We found that directory mirrors with smaller bandwidth (128 KB/s) don't answer version 2 status requests at all, but reply with 503 Busy. Also, we realized that guards only see 1/3 as many directory requests as compared to normal relays (which is actually a forgotten design feature). We need a fourth round of measurements, this time limiting bandwidth by setting MaxAdvertisedBandwidth.

http://freehaven.net/~karsten/metrics/directory-requests-2009-03-31.pdf

C.2.14. Incentives work.

No progress

C.2.15. More reliable (e.g. split) download mechanism.

No progress.

C.2.16. Footprints from Tor Browser Bundle.

March 17, updated research on traces left behind by the Tor Browser Bundle. The current document can be found at https://svn.torproject.org/svn/torbrowser/trunk/docs/traces.txt.

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

21 Polish website translations
20 French website translations
53 Italian website translations
25 German website translations
5 Chinese website translations
5 Updates from the translation portal for torbutton, in French, Italian, and Bokmål (Norwegian)

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: July 6, 2009

This report documents progress in June 2009 on contract BBGCON1807S6441 between BBG and The Tor Project.

C. New releases, new hires, new funding

On June 20th we released Tor 0.2.1.16-rc. This release contains:

Security fixes:

- Fix an edge case where a malicious exit relay could convince a controller that the client's DNS question resolves to an internal IP address. Bug found and fixed by "optimist"; bugfix on 0.1.2.8-beta.

Major performance improvements (on 0.2.0.x):

- Disable and refactor some debugging checks that forced a linear scan over the whole server-side DNS cache. These accounted for over 50% of CPU time on a relatively busy exit node's gprof profile. Found by Jacob.
- Disable some debugging checks that appeared in exit node profile data.

Minor features:

- Update to the "June 3 2009" ip-to-country file.
- Do not have tor-resolve automatically refuse all .onion addresses; if AutomapHostsOnResolve is set in your torrc, this will work fine.

Minor bugfixes (on 0.2.0.x):

- Log correct error messages for DNS-related network errors on Windows.
- Fix a race condition that could cause crashes or memory corruption when running as a server with a controller listening for log messages.
- Avoid crashing when we have a policy specified in a DirPolicy or SocksPolicy or ReachableAddresses option with ports set on it, and we re-load the policy. May fix bug 996.
- Hidden service clients didn't use a cached service descriptor that

was older than 15 minutes, but wouldn't fetch a new one either, because there was already one in the cache. Now, fetch a v2 descriptor unless the same descriptor was added to the cache within the last 15 minutes. Fixes bug 997; reported by Marcus Griep.

Minor bugfixes (on 0.2.1.x):

- Don't warn users about low port and hibernation mix when they provide a *ListenAddress directive to fix that. Bugfix on 0.2.1.15-rc.
- When switching back and forth between bridge mode, do not start gathering GeoIP data until two hours have passed.
- Do not complain that the user has requested an excluded node as an exit when the node is not really an exit. This could happen because the circuit was for testing, or an introduction point. Fix for bug 984.

One of the packaging changes that started with 0.2.1.16-rc rpms is the static inclusion of libevent 1.4.11-stable. The various linux distributions are very out of date on their versions of libevent. This change makes the rpm packages consistent with every other binary package we produce, as they all contain libevent compiled into the Tor binary.

On June 21st, we released Tor Browser Bundle 1.2.1. This releases contains:

- Better updates to Firefox to stop scanning for plugins on start
- Update Pidgin to 2.5.6r2
- Update Firefox to 3.0.11
- Include OpenSSL 0.9.8k DLL and stop using the system ssl dll

On June 23rd, we released Tor Browser Bundle 1.2.2. This release contains an update to Pidgin 2.5.7. Yahoo changed the way 3rd party clients can connect to Yahoo Instant Messenging. Pidgin 2.5.7 is compatible with these changes. Yahoo Instant Messaging is very popular in Iran. Users in Iran requested an update.

On June 24th, we released Tor 0.2.0.35-stable. We expect that this release is the last of the 0.2.0.x -stable series, soon to be replaced with the 0.2.1.x series. This release contains:

Security fix:

- Avoid crashing in the presence of certain malformed descriptors. Found by lark, and by automated fuzzing.
- Fix an edge case where a malicious exit relay could convince a controller that the client's DNS question resolves to an internal IP address. Bug found and fixed by "optimist"; bugfix on 0.1.2.8-beta.

Major bugfixes:

- Finally fix the bug where dynamic-IP relays disappear when their IP address changes: directory mirrors were mistakenly telling them their old address if they asked via begin_dir, so they never got an accurate answer about their new address, so they just vanished after a day. For belt-and-suspenders, relays that don't set Address in their config now avoid using begin_dir for all direct connections. Should fix bugs 827, 883, and 900.
- Fix a timing-dependent, allocator-dependent, DNS-related crash bug that would occur on some exit nodes when DNS failures and timeouts occurred in certain patterns. Fix for bug 957.

Minor bugfixes:

- When starting with a cache over a few days old, do not leak memory for the obsolete router descriptors in it. Bugfix on 0.2.0.33; fixes bug 672.
- Hidden service clients didn't use a cached service descriptor that was older than 15 minutes, but wouldn't fetch a new one either, because there was already one in the cache. Now, fetch a v2 descriptor unless the same descriptor was added to the cache within the last 15 minutes. Fixes bug 997; reported by Marcus Griep.

On June 30th, we released Vidalia 0.1.14. It contains:

- Close the TorProcess more quickly after registering for log events, so we avoid displaying duplicate log messages received over Tor's control port and Tor's stdout log. (Ticket #484)
- Explicitly set CMAKE_OSX_SYSROOT to the 10.4 SDK rather than expecting the packager to do so when building a Universal binary.
- Include Tor's geoip file in the Windows bundles.

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Packaged rpms for Red Flag Linux version 6. Red Flag Linux is reported to be the new operating system for all Internet cafe's in China. So far, no one has seen this conversion actually happen, but now we're ready if it does.

Our email autoresponder, gettor , received a number of patches to deal with dkim issues, including finding a dkim bug that prevented yahoo email users from fetching Tor. This bug has been fixed. Additionally, we've whitelisted some domains where we see we're having lots of use but dkim isn't always configured properly. We've had thousands of users from China using gettor.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

C.2.5. Hide Tor's network signature.

Nothing to report.

C. 2.10 Grow the Tor network and user base. Outreach.

Andrew, Roger, and Wendy attended Computers, Freedom, and Privacy 2009 Conference (http ://www.cfp2009.org). Andrew presented a "quicktake" talk on "Who uses Tor?". Andrew and Roger, along with Paul Syverson, and a North African blogger, hosted a panel on "It Takes A Village To Be Anonymous". Due to the sensitive situation surrounding the blogger, this panel was not recorded.

Andrew talked with the Committee to Protect Journalists (http://cpj.org) about online security and circumvention tools.

Jillian C. York blogged at KnightPulse about "Average citizens browse anonymously "; http://www.knightpulse.org/blog/09/06/04/average-citizens-browse-anonymously

Due to Iranian's usage of Tor during the recent election, the general press/media conducted a few interviews with Andrew:

1. Computer World, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134471&intsrc=news_ts_head
2. Cnet News, http://news.cnet.com/8301-13578_3-10267287-38.html
3. Deutche Welle, http://www.dw-world.de/dw/article/0,,4400882.00.html
4. Technology Review, http://www.technologyreview.com/web/22893/
5. Origo, in Hungary, http://www.origo.hu/techbazis/internet/20090618-a-kiberforradalmarok-fegyverei-eszkozok-anonim-netezeshez.html

6. O'Reilly, http://radar.oreilly.com/2009/06/tor-and-the-legality-of-runnin.html
7. Washington Times, http://www.washingtontimes.com/news/2009/jun/26/protesters-use-navy-technology-to-avoid-censorship/?feat=home_headlines
8. Arte TV video interview, the 30-minute video interview can't be put online, but will be shown to their viewers in late June/early July 2009. http://www.arte.tv
9. EFF, http://www.eff.org/deeplinks/2009/06/help-protesters-iran-run-tor-relays-bridges
10. A Houston Radio station did an on-air interview, but didn't put the interview online.
11. A Romanian newspaper did an interview, but didn't put the story online.
12. Public Rado International did a more in-depth interview. They expect it to be on PBS Radio and BBC Radio 4 in early July 2009.

A number of blogs and other media picked up these original interviews and spread the word even further:

1. Wall Street Journal, http://blogs.wsj.com/digits/2009/06/18/iranians-using-tor-to-anonymize-web-use/
2. CBS News, http://www.cbsnews.com/blogs/2009/06/17/politics/politicalhotsheet/entry5094825.shtml
3. http://curtisschweitzer.net/blog/?p=2995
4. http://voices.allthingsd.com/20090618/iranians-using-tor-to-anonymize-web-use/
5. http://www.dailyfinance.com/2009/06/24/nokia-and-siemens-in-iran-controversy/
6. http://www.muslimnews.co.uk/news/news.php?article=16360

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

Tor Browser Bundle 1.2.1 and 1.2.2 released in June. Planning a migration of the base operating system for the Incognito LiveCD to switch from Gentoo to an Ubuntu variant.

C.2.12 Bridge relay and bridge authority work.

Nothing to report.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

June was spent documenting, stabilizing, and streamlining the bandwidth authority scanner, which has been runningfor a while on the Directory Authority named ides.

It is good enough to start running on multiple authorities now to produce actual results for clients to use.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Our email autoresponder, gettor , received a number of patches to deal with dkim issues, including finding a dkim bug that prevented yahoo email users from fetching Tor. This bug has been fixed. Additionally, we've whitelisted some domains where we see we're having lots of use but dkim isn't always configured properly. We've had thousands of users from China using gettor.

The Tor Check website (check.torproject.org) had a few bugs and we've fixed all but two. We sometimes still have false negatives (because the Tor client doesn't know to fetch the consensus at any specific time) and we also still sometimes barf python exceptions because mod_python has some weird exception from time to time. We also accepted a patch from Marcus Greip that extends the TorBulkExitList to allow arbitrary ports rather than just port 80.

C.2.16. Footprints from Tor Browser Bundle.

Reduced the scanning for plugins Portable Firefox can do on launch of the application. There is still an issue where Firefox displays other plugins to users, but they aren't actually valid plugins and won't run on command. Firefox acquires the names through queries to the Windows Registry.

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

16 Polish website updates
8 Italian website updates
3 German website updates

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: August 2, 2009

This report documents progress in July 2009 on contract BBGCON1807S6441 between BBG and The Tor Project.

C. New releases, new hires, new funding

On July 8th, we released Vidalia 0.1.15. It contains:

- Bump the minimum required Qt version to 4.3.0.
- Remove USE_QSSLSOCKET as a build option. If your Qt doesn't support ! OpenSSL, then you don't get GeoIP lookups.
- Fix the TorPostFlight portion of the OS X bundle installer so it doesn't fail when installing Torbutton.
- Include libeay32.dll in the Windows installers.

On July 8th, we updated the Tor 0.2.0.35-stable bundles with the new Vidalia to fix an ssl issue and the Firefox Torbutton extension installation for OS X users.

On July 8th, we released Tor 0.2.1.17-rc. It contains:
Tor 0.2.1.17-rc marks the fourth -- and hopefully last -- release candidate for the 0.2.1.x series. It lays the groundwork for further client performance improvements, and also fixes a big bug with directory authorities that were causing them to assign Guard and Stable flags poorly.

The Windows bundles also finally include the geoip database that we thought we'd been shipping since 0.2.0.x (oops), and the OS X bundles should actually install Torbutton rather than giving you a cryptic failure message (oops).

This is a release candidate! That means that we don't know of any remaining show-stopping bugs, and 0.2.1.18 will be the new stable if there are no problems.

Major features:

- Clients now use the bandwidth values in the consensus, rather than the bandwidth values in each relay descriptor. This approach opens the door to more accurate bandwidth estimates once the directory

authorities start doing active measurements. Implements more of proposal 141.

Major bugfixes:

- When Tor clients restart after 1-5 days, they discard all their cached descriptors as too old, but they still use the cached consensus document. This approach is good for robustness, but bad for performance: since they don't know any bandwidths, they end up choosing at random rather than weighting their choice by speed. Fixed by the above feature of putting bandwidths in the consensus. Bugfix on 0.2.0.x.
- Directory authorities were neglecting to mark relays down in their internal histories if the relays fall off the routerlist without ever being found unreachable. So there were relays in the histories that haven't been seen for eight months, and are listed as being up for eight months. This wreaked havoc on the "median wfu" and "median mtbf" calculations, in turn making Guard and Stable flags very wrong, hurting network performance. Fixes bugs 696 and 969. Bugfix on 0.2.0.6-alpha.

Minor bugfixes:

- Serve the DirPortFrontPage page even when we have been approaching our quotas recently. Fixes bug 1013; bugfix on 0.2.1.8-alpha.
- The control port would close the connection before flushing long replies, such as the network consensus, if a QUIT command was issued before the reply had completed. Now, the control port flushes all pending replies before closing the connection. Also fixed a spurious warning when a QUIT command is issued after a malformed or rejected AUTHENTICATE command, but before the connection was closed. Patch by Marcus Griep. Bugfix on 0.2.0.x; fixes bugs 1015 and 1016.
- When we can't find an intro key for a v2 hidden service descriptor, fall back to the v0 hidden service descriptor and log a bug message. Workaround for bug 1024.

Minor features:

- If we're a relay and we change our IP address, be more verbose about the reason that made us change. Should help track down further bugs for relays on dynamic IP addresses.

Tor Browser Bundle 1.2.3 was released on July 8, 2009. It contains the following changes:

- Update Vidalia to 0.1.14

- Update Tor to 0.2.1.17-rc
- Update Pidgin to 2.5.8

TBB 1.2.3 was replaced by 1.2.4 on July 11, 2009 to include:

- Include libeay32.dll from OpenSSL 0.9.8k to make QT happy
- Update Vidalia to 0.1.15

TBB 1.2.5 was released on July 25th. It solely included an update to Tor 0.2.1.18 .

TBB 1.2.6 was released on July 28th. It solely included an update to Tor 0.2.1.19.

On July 24th, we released Tor 0.2.1.18. It contains:

Build fixes:

- Add LIBS=-lrt to Makefile.am so the Tor RPMs use a static libevent.

On July 28th, we released Tor 0.2.1.19. It contains:

o Major bugfixes:

- Make accessing hidden services on 0.2.1.x work right again. Bugfix on 0.2.1.3-alpha; workaround for bug 1038.

o Minor features:

- When a relay/bridge is writing out its identity key fingerprint to the "fingerprint" file and to its logs, write it without spaces. Now it will look like the fingerprints in our bridges documentation, and confuse fewer users.

o Minor bugfixes:

- Relays no longer publish a new server descriptor if they change their MaxAdvertisedBandwidth config option but it doesn't end up changing their advertised bandwidth numbers. Bugfix on 0.2.0.28-rc; fixes bug 1026. Patch from Sebastian.
- Avoid leaking memory every time we get a create cell but we have so many already queued that we refuse it. Bugfix on 0.2.0.19-alpha; fixes bug 1034. Reported by BarkerJr.

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Tor 0.2.1.18 is our new stable. That is, this is the first stable release of the 0.2.1.x branch. The 0.2.0.x branch went stable in July of 2008.

From the 0.2.1.18 release:

If the bridge config line doesn't specify a port, assume 443.
This makes bridge lines a bit smaller and easier for users to understand.

If we're using bridges and our network goes away, be more willing to forgive our bridges and try again when we get an application request.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

Proposal 166 details four steps we're taking to safely collect data about Tor's network performance and network usage: 1) directory client counts by country, 2) entry guard client counts by country, 3) relay cell statistics, and 4) exit traffic by port and volume.
https://git.torproject.org/checkout/tor/master/doc/spec/proposals/166-statistics-extra-info-docs.txt

C.2.5. Hide Tor's network signature.

Part of the reason why Tor might be especially slow in Iran could be that they're doing deep packet inspection (DPI) to throttle SSL connections. Tor's strategy of looking like SSL might turn out to be a bad move in this case. It's hard to tell whether the SSL throttling is actually happening, of course, because we get plenty of mixed information from our sources in Iran. But if it ***is*** happening, we should start investigating traffic obfuscation approaches that a) don't look like SSL, but b) don't look recognizably like any other protocol.

Some other Iran circumvention developers have come up with a patch to obfuscate ssh traffic:
http://github.com/brl/obfuscated-openssh/tree/master

http://c-skills.blogspot.com/2008/12/sshv2-trickery.html

Sometime soon we should start looking at designs to super-encrypt the Tor link traffic in this way.

C. 2.10 Grow the Tor network and user base. Outreach.

On July 1st, Andrew gave a detailed Tor talk at the National Cyber Forensics and Training Alliance. Andrew's blog about the event is at https://blog.torproject.org/blog/visit-ncfta.

On July 7th, Andrew was a panelist for the CIMA/NED discussion on Iran and the Role of New Media, http://cima.ned.org/events/new-media-in-iran.html. Andrew's blog about the event is at https://blog.torproject.org/blog/cimaned-panel-iran-and-new-media.

On July 15th, Andrew presented Tor at Webinno22, http://www.webinnovatorsgroup.com/2009/07/06/the-webinno22-demo-companies/. Further discussions about online privacy startups and business deals with various venture capitalists are continuing since this event.

More press interviews and articles:

Iran activists work to elude crackdown on Internet, http://www.google.com/hostednews/ap/article/ALeqM5hTf-p6Iv3sWHK8BRR58npGosLC3AD99L01OO0

http://blog.taragana.com/n/iran-government-builds-internet-walls-but-activists-still-slip-around-in-political-turmoil-119968/

Twitter and Facebook Help Protestors Connect, http://www.outloud.com/2009/issue96/protest.html

US set to hike aid aimed at Iranians. http://www.boston.com/news/nation/washington/articles/2009/07/26/us_to_increase_funding_for_hackivists_aiding_iranians/

Senate OKs funds to thwart Iran Web censors , http://www.washingtontimes.com/news/2009/jul/26/senate-help-iran-dodge-internet-censorship/

We wrote a follow-up blog post about the number of people using Tor

from Iran and China in June:
https://blog.torproject.org/blog/measuring-tor-and-iran-part-two

On July 1-5, Roger, Jake, Mike, and Damian attended Toorcamp in rural Washington State. Roger did a talk on current attacks and vulnerabilities in Tor.
http://www.toorcamp.org/content/B4

Roger attended a conference in DC (Jul 7-9) which was funded by NSF and France to encourage collaboration, and did a keynote on Tor and Iran:
http://freehaven.net/~arma/slides-yess09.pdf
The conference was mostly a failure with respect to the collaboration-with-France part, but Roger got to talk to several good security profs while there, and also got connected to some NSF funders who are interested to help make Tor metrics and measurement research happen.

On July 21-23, Roger attended a workshop in DC at the National Academy of Sciences. The workshop focused on the combination of Usability, Privacy, and Security, and where future funding should concentrate.

On July 31, Roger gave a Defcon talk on the current state of Tor's performance challenges and how we're addressing them:
http://defcon.org/html/defcon-17/dc-17-speakers.html#Dingledine
http://freehaven.net/~arma/slides-dc09.pdf

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

Tor Browser Bundle 1.2.3 was released on July 8, 2009. It contains the following changes:

- Update Vidalia to 0.1.14
- Update Tor to 0.2.1.17-rc
- Update Pidgin to 2.5.8

TBB 1.2.3 was replaced by 1.2.4 on July 11, 2009 to include:

- Include libeay32.dll from OpenSSL 0.9.8k to make QT happy
- Update Vidalia to 0.1.15

TBB 1.2.5 was released on July 25th. It solely included an update to Tor 0.2.1.18 .

TBB 1.2.6 was released on July 28th. It solely included an update to Tor 0.2.1.19.

Upgraded many programs in Incognito to address security concerns and general bugfixes.

C.2.12 Bridge relay and bridge authority work.

Updated geoip database. From the 0.2.1.18 release:

If the bridge config line doesn't specify a port, assume 443.
This makes bridge lines a bit smaller and easier for users to
understand.

If we're using bridges and our network goes away, be more willing
to forgive our bridges and try again when we get an application
request.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

From the 0.2.1.18 release:

Network status consensus documents and votes now contain bandwidth
information for each relay. Clients use the bandwidth values
in the consensus, rather than the bandwidth values in each
relay descriptor. This approach opens the door to more accurate
bandwidth estimates once the directory authorities start doing
active measurements. Implements part of proposal 141.

When building a consensus, do not include routers that are down.
This cuts down 30% to 40% on consensus size. Implements proposal
138.

Authorities now vote for the Stable flag for any router whose
weighted mean time between failure (MTBF) is at least 5 days, regardless of the
mean MTBF.

The main 2009 remaining performance changes are, in order of importance:
- Get the bwauthority scripts into place so authorities are voting on
  more accurate bandwidths.
- Write a proposal for capping the circuit window much lower, and
  implement it, and backport it to 0.2.1.x.
- Proposal 151: Mike's plan to track circuit build times and give up on
  the slow ones.
- Write a proposal for refilling our bandwidth buckets intra-second.

Consider deploying in 0.2.2.x.
- Figure out what we can do for a less fair round-robin between active circuits. My intuition is heading towards "we don't know what effect each possible change will make, and our other changes are going to have big effects, so we shouldn't deploy anything here quite yet."
- Get enough authorities upgraded that our bug 969 fixes ("voting wrong on wfu and mtbf") take effect.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

We have a new Volunteer, Jon, working on maintaining and expanding the list of tor mirrors. Jon has contacted all mirror maintainers and updated the mirrors list. Three were removed, two added, and seven updated with new information. There are 39 active mirrors.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

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

10 Polish website updates
7 French website updates
1 Chinese website updates
German torbutton translations updated
Finnish torbutton translations updated
Generate translation infrastructure for our email auto-responder.
Ukrainian torbutton translation started
Start of a Thai torbutton translation
Spanish torbutton translation
Ukrainian check.torproject.org translation
Thai check.torproject.org translation

Our Google Summer of Code student, Runa, created a set of scripts to allow translators to translate our website content through the translation web portal. This will greatly simplify the process used to translate the website.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, Program Officer, BBG
RE: contract BBGCON1807S6441
Date: October 6, 2009

This report documents progress in September 2009 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

New Hires

- Carolyn Anhalt is our new Translation and Community Manager. Carolyn has years of experience managing and growing content translation, as well as wrangling online communities and developing volunteer moderators and support roles from the community. She's fluent or conversant in a number of languages, such as: Russian, French, English, German, Italian, and Welsh. Carolyn's initial goals are to grow the translator community to keep everything Tor translated, work out better translation tools for translators, and to generally assist translators.

- Melissa Gilroy is our new Chief Financial Officer. Melissa has years of experience in non-profit accounting and auditing. Melissa's initial goal is to arrange Tor's finances to be compliant with US Government accounting standards such as A-133 and A-110.

- Karen Reilly joins us as our volunteer Development Director. Karen has years of experience in growing both community-based and foundation-based funding, as well as helping to fulfill the mission of organizations through outreach and community-building. Karen's initial goals are to further develop community funding, work with our current donors, help create an annual report, and expand Tor's outreach efforts.

New Funding

- Tor and Drexel University receive a grant from the National Science Foundation to research "Privacy-preserving measurements of the Tor network to improve performance and anonymity".

- Tor and ITT receive a grant from the Naval Research Laboratory to research "Tor Networks Trust-Based Routing Research & Design Support".

New Releases

- On September 21, we released version 0.2.2.2-alpha.
  Major features:
  - Tor now tracks how long it takes to build client-side circuits over time, and adapts its timeout to local network performance. Since a circuit that takes a long time to build will also provide bad performance, we get significant latency improvements by discarding the slowest 20% of circuits. Specifically, Tor creates circuits more aggressively than usual until it has enough data points for a good timeout estimate. Implements proposal 151. We are especially looking for reports (good and bad) from users with both EDGE and broadband connections that can move from broadband to EDGE and find out if the build-time data in the .tor/state gets reset without loss of Tor usability. You should also see a notice log message telling you that Tor has reset its timeout.
  - Directory authorities can now vote on arbitary integer values as part of the consensus process. This is designed to help set network-wide parameters. Implements proposal 167.
  - Tor now reads the "circwindow" parameter out of the consensus, and uses that value for its circuit package window rather than the default of 1000 cells. Begins the implementation of proposal 168.

  Major bugfixes:
  - Fix a remotely triggerable memory leak when a consensus document contains more than one signature from the same voter. Bugfix on 0.2.0.3-alpha.

  Minor bugfixes:
  - Fix an extremely rare infinite recursion bug that could occur if we tried to log a message after shutting down the log subsystem. Found by Matt Edman. Bugfix on 0.2.0.16-alpha.
  - Fix parsing for memory or time units given without a space between the number and the unit. Bugfix on 0.2.2.1-alpha; fixes bug 1076.
  - A networkstatus vote must contain exactly one signature. Spec conformance issue. Bugfix on 0.2.0.3-alpha.
  - Fix an obscure bug where hidden services on 64-bit big-endian systems might mis-read the timestamp in v3 introduce cells, and refuse to connect back to the client. Discovered by "rotor". Bugfix on 0.2.1.6-alpha.
  - We were triggering a CLOCK_SKEW controller status event whenever we connect via the v2 connection protocol to any relay that has a wrong clock. Instead, we should only inform the controller when it's a trusted authority that claims our clock is wrong. Bugfix on 0.2.0.20-rc; starts to fix bug 1074. Reported by "SwissTorExit".
  - We were telling the controller about CHECKING_REACHABILITY and REACHABILITY_FAILED status events whenever we launch a testing circuit or notice that one has failed. Instead, only tell the controller when we want to inform the user of overall success or overall failure. Bugfix on 0.1.2.6-alpha. Fixes bug 1075. Reported by SwissTorExit.

- Don't warn when we're using a circuit that ends with a node excluded in ExcludeExitNodes, but the circuit is not used to access the outside world. This should help fix bug 1090, but more problems remain. Bugfix on 0.2.1.6-alpha.
- Work around a small memory leak in some versions of OpenSSL that stopped the memory used by the hostname TLS extension from being freed.
- Make our 'torify' script more portable; if we have only one of 'torsocks' or 'tsocks' installed, don't complain to the user; and explain our warning about tsocks better.

Minor features:

- Add a "getinfo status/accepted-server-descriptor" controller command, which is the recommended way for controllers to learn whether our server descriptor has been successfully received by at least on directory authority. Un-recommend good-server-descriptor getinfo and status events until we have a better design for them.
- Update to the "September 4 2009" ip-to-country file.

- On September 23, we released version 0.2.2.3-alpha.
  Major bugfixes:
  - Fix an overzealous assert in our new circuit build timeout code. Bugfix on 0.2.2.2-alpha; fixes bug 1103.

  Minor bugfixes:
  - If the networkstatus consensus tells us that we should use a negative circuit package window, ignore it. Otherwise we'll believe it and then trigger an assert. Bugfix on 0.2.2.2-alpha.

- On September 7, we released Vidalia 0.2.4. Included changes are:
  - Split the message log into "Basic" and "Advanced" views. The "Advanced" view contains standard log messages from Tor, while the new experimental "Basic" view displays status events received from Tor. (Ticket 265)
  - Apply an application-global stylesheet on OS X that forces all tree widgets in Vidalia to use the 12pt font recommended by Apple's human interface guidelines.
  - Add an OSX_FORCE_32BIT CMake option that can be used to force a 32-bit build on Mac OS X versions that default to 64-bit builds (e.g., Snow Leopard), if only 32-bit versions of the Qt libraries are available.
  - Fix a bug introduced in 0.2.3 that prevented Vidalia from correctly responding to ADDRMAP events from Tor. The result was that users would sometimes see IP addresses in the connection list shown under the network map rather than hostnames.
  - Fix a bug in the default "bootstrap" vidalia.conf file included in the OS X drag-and-drop bundles that pointed to a non-existent Polipo configuration file, causing Polipo to fail on startup.

- On August 27th, we released Vidalia 0.2.3. This fixes some more bugs with "Who has used my bridge" functionality and switches to Qt signals for event handling.
  The changes are:

- Create the data directory before trying to copy over the default Vidalia configuration file from inside the application bundle on Mac OS X. Affects only OS X drag-and-drop installer users without a previous Vidalia installation.
- Change all Tor event handling to use Qt's signals and slots mechanism instead of custom QEvent subclasses.
- Fix another bug that resulted in the "Who has used my bridge?" link initially being visible when the user clicks "Setup Relaying" from the control panel if they are running a non-bridge relay. (Ticket 509, reported by "vrapp")
- Always hide the "Who has used my bridge?" link when Tor isn't running, since clicking it won't return useful information until Tor actually is running.

- On September 11, we released Tor Browser Bundle version 1.2.9. It updates Firefox and Pidgin Instant Messaging client to address the security issues in the older versions, and includes the latest and greatest Vidalia.
  Detailed changes are:
  - update Vidalia to 0.2.4
  - update Qt to 4.5.2
  - update Pidgin to 2.6.2
  - update Firefox to 3.0.14

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Jacob Appelbaum and Nathan Frietas developed a fully functional Tor for the Android mobile operating system. It is currently being tested before being released to the Android Marketplace. This Android application uses mainline Tor as written in C, rather than porting/creating a Tor client in Java. Others have started discussions and coding around using Java to create a Tor-compatible client.

Damian Johnson further developed arm, `https://svn.torproject.org/svn/arm/trunk/`. Arm is a command line application for monitoring Tor relays, providing real time status information such as the current configuration, bandwidth usage, message log, connections, etc. This uses a curses interface much like 'top' does for system usage. The application is intended for command-line aficionados, ssh connections, and anyone stuck with a tty terminal for checking their relay's status.

Added two new Tor website and software distribution mirrors. Update list of current mirrors to reflect their current status of how current the mirrors are compared to the main torproject.org website.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

A paper entitled, "On the risks of serving whenever you surf: Vulnerabilities in Tor's blocking resistance design", discussing risks in running a bridge is to be relased at Workshop on Privacy in

the Electronic Society (WPES 2009), http://freehaven.net/anonbib/#wpes09-bridge-attack.

Started development of "marco" to quickly scan for Tor relay and brige reachability from a client machine. This utility was used successfully by volunteers inside Iran and China to determine how much of the Tor network is blocked and how such blocking is occurring.

C.2.5. Hide Tor's network signature.

Nothing to report.

C.2.10 Grow the Tor network and user base. Outreach.

Roger, Paul Syverson, and Andrew gave a Tor lecture to the US Federal Bureau of Investigation Operational Technology Division as part of their quarterly series of talks on new technology. Had a follow-on conversation with a Supervisory Special Agent about how to use Tor tools safely in the field.

Roger and Andrew had a meeting with the US Department of Justice Child Exploitation and Obscenity Section to present what Tor is and how it works. We also discussed issues and challenges in their usage of, and prosecuting criminals using, Tor.

Roger and Andrew met with a Senior Policy Advisor from Senator Harry Reid's office to discuss online privacy and anonymity.

Roger is working with a freshman class at KAIST in South Korea to develop Tor bridge relay distribution strategies. More information can be found at https://blog.torproject.org/blog/bridge-distribution-strategies.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

On September 11, we released Tor Browser Bundle version 1.2.9. It updates Firefox and Pidgin Instant Messaging client to address the security issues in the older versions, and includes the latest and greatest Vidalia. Detailed changes are:

- update Vidalia to 0.2.4
- update Qt to 4.5.2
- update Pidgin to 2.6.2
- update Firefox to 3.0.14

C.2.12. Bridge relay and bridge authority work.

Deployed a temporary workaround for a vidalia/tor bug where bridges don't work if you provide a fingerprint and the bridge authority is unreachable. Discovered this bug on September 25 when China blocked the bridge authority.

Started fixing bridge statistics that have been broken in all 0.2.2.x versions. Plan to test the fixes in the next few days and include the changes in 0.2.2.5-alpha.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

A research paper on scaling our directory design, "Scalable onion routing with Torsk" was is to be presented at CCS 2009, http://freehaven.net/anonbib/#ccs09-torsk.

Deployed Mike Perry's Bandwidth Authority code to the Directory Authorities. The bandwidth authorities are now voting on measured bandwidth from relays and giving out this information in extra-info fields to Tor clients. Tor 0.2.1 and 0.2.2 clients make routing decisions based on these extra-info data. This should spread traffic across relays and improve overall performance of the Tor network.

Included the results of Mike's bandwidth scanner in the votes of gabelmoo. Helped evaluating the (impressive) performance improvements as seen by torperf, https://git.torproject.org/checkout/metrics/master/report/performance/torperf-2009-09-22.pdf. Initial results imply a 30-50% increase in performance.

Evaluated how the reduction of circuit windows from 1000 to 101 cells affects performance. The last report includes 40 KiB, 50 KiB, and 1 MiB downloads, https://git.torproject.org/checkout/metrics/master/report/circwindow/circwindow-2009-09-20.pdf.

Evaluated how Mike's buildtimes patch influences Tor performance, https://git.torproject.org/checkout/metrics/master/report/buildtimes/buildtimes-2009-09-22.pdf.

Wrote a script that parses descriptor archives to tell whether an IP address was a Tor relay at a given time, https://svn.torproject.org/svn/projects/archives/trunk/exonerator/HOWTO.

Restarted the autonaming script on September 20, so that gabelmoo will be naming relays again soon.

Fixed the remaining bugs in the proposal 166 implementation. Relays can now include their statistics in extra-info descriptors. Further testing this on select relays for a few more days. Soon will ask people on or-dev to turn on statistics as soon as tests are successful and 0.2.2.4-alpha is out.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Nothing to report.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

C.2.17. Translation work, ultimately a browser-based approach.

Released Runa's code to allow website translation from our Translation Portal, https://translation.torproject.org. Runa wrote up her ideas and Google Summer of Code experiences at http://blog.torproject.org/blog/website-translation-support-translationtorprojectorg.

- Continued work on website to translation portal code.
- 17 Polish website updates.
- 27 Italian website updates.
- Romanian and Chinese updates to the check.torproject.org website.
- 1 update to German torbutton translation.
- 23 updates to Romanian torbutton translation.
- 115 updates to Polish torbutton translation.
- 115 updates to Mandarin Chinese torbutton translation.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: December 9, 2009

This report documents progress in November 2009 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

Bruce Leidl joins to work on developing Tor in Java. Bruce will write a fully functional Tor in Java in order to provide a solid foundation for other java-based projects; such as Tor on mobile platforms like Maemo and Android.

On November 2nd we released Vidalia 0.2.6. It contains fixes for:

- Remove the erroneous comma in the default vidalia.conf in the Mac OS X drag-and-drop bundle, since we now dump whatever the user types into a QString rather than parsing it into a QStringList.
- Updated the Arabic, Russian and Slovenian translations.

On November 20th, we released Tor Browser Bundle 1.2.10. It contains updates for:

- updated Vidalia to 0.2.6
- updated Pidgin to 2.6.3
- updated Tor to 0.2.1.20
- updated Firefox to 3.0.15
- updated OpenSSL to 0.9.8l
- updated libevent to 1.4.13

On November 19th, we released Tor 0.2.2.6-alpha. It contains fixes and updates for:
Major features:

- Directory authorities can now create, vote on, and serve multiple parallel formats of directory data as part of their voting process. Partially implements Proposal 162: "Publish the consensus in multiple flavors".

- Directory authorities can now agree on and publish small summaries of router information that clients can use in place of regular server descriptors. This transition will eventually allow clients to use far less bandwidth for downloading information about the network. Begins the implementation of Proposal 158: "Clients download consensus + microdescriptors".
- The directory voting system is now extensible to use multiple hash algorithms for signatures and resource selection. Newer formats are signed with SHA256, with a possibility for moving to a better hash algorithm in the future.
- New DisableAllSwap option. If set to 1, Tor will attempt to lock all current and future memory pages via mlockall(). On supported platforms (modern Linux and probably BSD but not Windows or OS X), this should effectively disable any and all attempts to page out memory. This option requires that you start your Tor as root – if you use DisableAllSwap, please consider using the User option to properly reduce the privileges of your Tor.
- Numerous changes, bugfixes, and workarounds from Nathan Freitas to help Tor build correctly for Android phones.

Major bugfixes:

- Work around a security feature in OpenSSL 0.9.8l that prevents our handshake from working unless we explicitly tell OpenSSL that we are using SSL renegotiation safely. We are, but OpenSSL 0.9.8l won't work unless we say we are.

Minor bugfixes:

- Fix a crash bug when trying to initialize the evdns module in Libevent 2. Bugfix on 0.2.1.16-rc.
- Stop logging at severity 'warn' when some other Tor client tries to establish a circuit with us using weak DH keys. It's a protocol violation, but that doesn't mean ordinary users need to hear about it. Fixes the bug part of bug 1114. Bugfix on 0.1.0.13.
- Do not refuse to learn about authority certs and v2 networkstatus documents that are older than the latest consensus. This bug might have degraded client bootstrapping. Bugfix on 0.2.0.10-alpha. Spotted and fixed by xmux.
- Fix numerous small code-flaws found by Coverity Scan Rung 3.
- If all authorities restart at once right before a consensus vote, nobody will vote about "Running", and clients will get a consensus with no usable relays. Instead, authorities refuse to build a consensus if this happens. Bugfix on 0.2.0.10-alpha; fixes bug 1066.
- If your relay can't keep up with the number of incoming create cells, it would log one warning per failure into your logs. Limit warnings to 1 per minute. Bugfix on 0.0.2pre10; fixes bug 1042.
- Bridges now use "reject *:*" as their default exit policy. Bugfix on 0.2.0.3-alpha; fixes bug 1113.
- Fix a memory leak on directory authorities during voting that was introduced in 0.2.2.1-alpha. Found via valgrind.

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Roger met with his class at KAIST working on bridge deployment strategies. A few teams developed some creative strategies. Roger is continuing to work with the leading teams to further refine their ideas before publishing.

Improved our email autoresponder, get-tor, to handle non-english character sets. Implemented gettor+(language)@ addressing to allow users to request tor browser bundle packages in their native language. Added support for languages with a right to left orientation, such as farsi.

C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

Nothing to report.

C.2.5. Hide Tor's network signature.

Nothing to report.

C.2.10 Grow the Tor network and user base. Outreach.

- Andrew spoke at CASCON 2009 about Tor and its research. A few researchers from IBM and University of Waterloo were interested in furthering research. `https://www-927.ibm.com/ibm/cas/cascon/`
- Andrew and Roger attended Blogfest Asia 2009, HK BloggerCon, and the Privacy and Security Workshop series in Hong Kong and met with many bloggers, activists, and media people from all over Asia. Andrew wrote up his experiences at `https://blog.torproject.org/blog/blogfest-asia-2009`.
- Jacob spoke at Internet Dagarma 2009 in Stockholm, Sweden. `http://www.internetdagarna.se/`
- Jacob spoke at the NorduNet Annual Conference in Stockholm, Sweden.
- Jacob helped organize and run Hackers Conference in California. `http://www.think.org/conference/`
- Karen met with National Iranian-American Council, `http://www.niacouncil.org/`, to discuss ways Tor can help NIAC succeed in helping improve Human Rights and Democracy in Iran.
- Andrew had a conversation with Freedom House which resulted in some instructional videos being produced to help users install and configure Tor. The videos are:
  - Install and Use Tor, `http://tinyvid.tv/show/3lejztnthk2tm`

- Install and Use Tor Browser Bundle, http://tinyvid.tv/show/b0e2hzylie8r
- Using a Bridge Relay to Access Tor, http://tinyvid.tv/show/3uiwckrlqynqv

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

On November 20th, we released Tor Browser Bundle 1.2.10. It contains updates for:

- updated Vidalia to 0.2.6
- updated Pidgin to 2.6.3
- updated Tor to 0.2.1.20
- updated Firefox to 3.0.15
- updated OpenSSL to 0.9.8l
- updated libevent to 1.4.13

C.2.12 Bridge relay and bridge authority work.

We distributed bridge addresses to networks of people in China and Iran to let Tor users continue to work without issues.

Karsten worked to remove sensitive data from collected meta-data about bridges. We can publish our bridge data archives to http://archive.torproject.org soon. This data could help understand bridge quantity, usage of bridges around the world, and other information from possible data analysis.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

Included in the Tor 0.2.2.6-alpha release is the beginning of microdescriptors. "Directory authorities can now agree on and publish small summaries of router information that clients can use in place of regular server descriptors. This transition will eventually allow clients to use far less bandwidth for downloading information about the network. Begins the implementation of Proposal 158: "Clients download consensus + microdescriptors"."

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

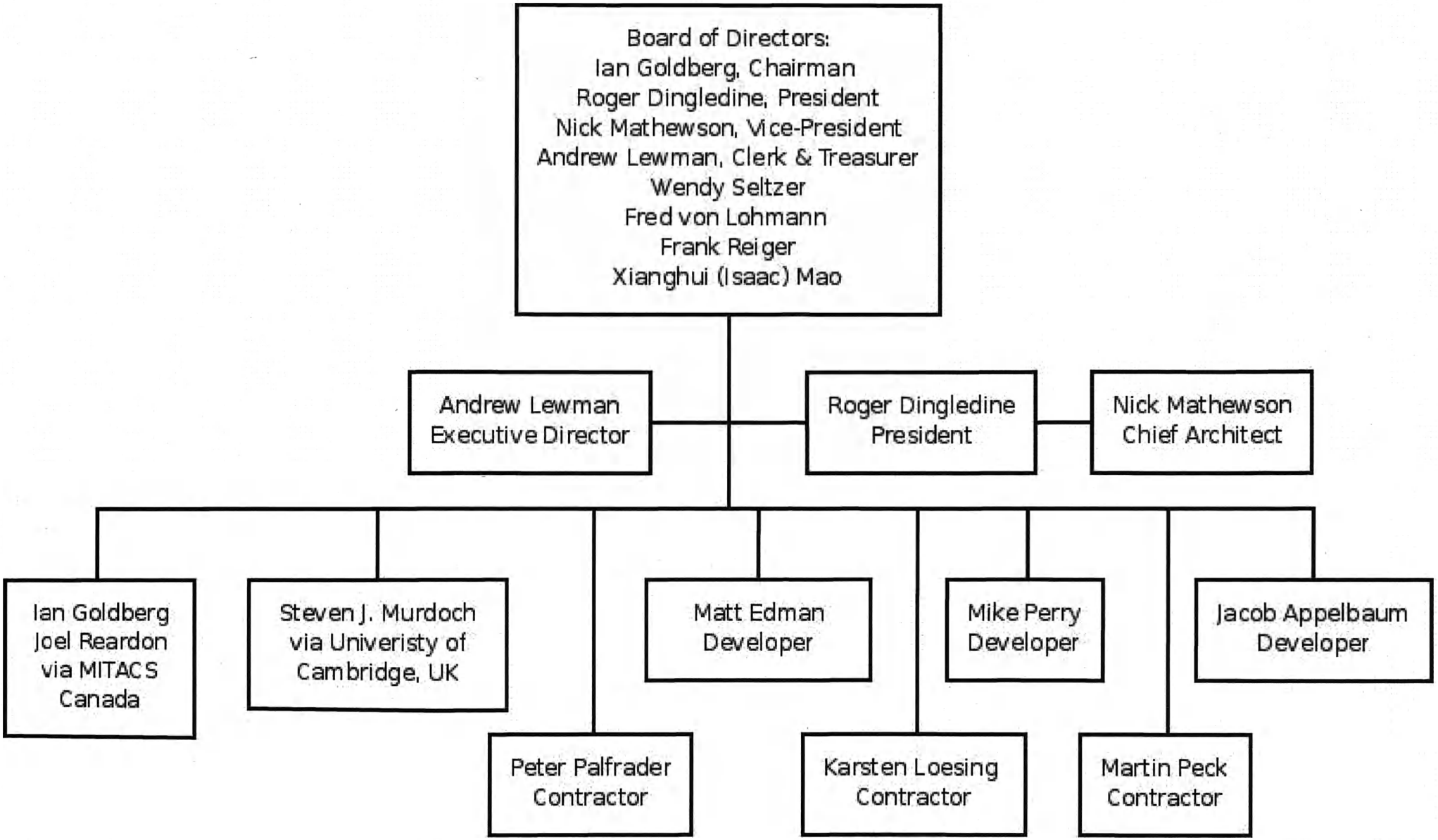
Continuing to update the email autoresponder, get-tor, to handle split downloads on request. Split Tor Browser Bundles work well. Creation and maintenance of Mac OS X split dmgs is due in December 2009.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

C.2.17 Translation work, ultimately a browser-based approach.

- Pushed live Runa's work on integrating the website to our translation portal, `https://translation.torproject.org/`.
- Runa fine tuned the translation portal to website scripts.
- Runa updated the documentation for translators to reflect these tor translation portal updates.
- Added our email autoresponder, get-tor, to the translation portal.
- Began live testing of website translations through the Tor Translation Portal.
- 28 updated Polish website translations.
- 15 updated Chinese website translations.
- 11 updated Italian website translations.
- 1 French translation of get-tor.
- Full Norwegian translation of tor browser bundle.
- Full Norwegian translation of the website.
- Full Burmese translation of the website.
- Full Burmese translation of torcheck.
- Updated Spanish torbutton translations.
- Updated Chinese torbutton translations.
- Updated Chinese torcheck translations.
- 18 updated German website translations.


Board of Directors:
Ian Goldberg, Chairman
Roger Dingledine, President
Nick Mathewson, Vice-President
Andrew Lewman, Clerk & Treasurer
Wendy Seltzer
Fred von Lohmann
Frank Reiger
Xianghui (Isaac) Mao
Andrew Lewman
Executive Director
Roger Dingledine
President
Nick Mathewson
Chief Architect
Ian Goldberg
Joel Reardon
via MITACS
Canada
Steven J. Murdoch
via Univeristy of
Cambridge, UK
Matt Edman
Developer
Mike Perry
Developer
Jacob Appelbaum
Developer
Peter Palfrader
Contractor
Karsten Loesing
Contractor
Martin Peck
Contractor

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: January 10, 2010

This report documents progress in December 2009 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

Erinn Clark joins Tor to develop, enhance, and upgrade our package build system. Her initial goals are to configure, maintain, and automate builds of tor and vidalia for Windows, OS X, ubuntu, debian, centos, fedora, and opensuse systems. Secondary goals are to develop a builtbot system that includes as many disparate operating systems as possible, including Apple OS X and Microsoft Windows flavors.

On December 2, 2009, we released torbutton 1.2.3. This is the first release that addresses the Firefox 3.5.x codebase. It contains the following changes:

- bugfix: bug 950: Preserve useragent and download settings across toggle
- bugfix: bug 1014: Fix XML Parsing Error on XHTML sites in Tor mode
- bugfix: bug 1041: Preserve tab history in FF3.5
- bugfix: bug 1047: Fix spurious user agent change notice
- bugfix: bug 1053: Partial fix for 'TypeError: browser is undefined' error
- bugfix: bug 1084: Preserve HTTP accept language for Non-Tor usage
- bugfix: bug 1085: Fix test settings issues with dead privoxy
- bugfix: bug 1088: Clean up some namespace issues in the main chrome window
- bugfix: bug 1091: Fix a lockup when 'Ask Every Time' cookie pref is set
- bugfix: bug 1093: Fix cert acceptance dialogs in Firefox 3.5
- bugfix: bug 1146: Fixes for properly handling tab restore in FF3.5
- bugfix: bug 1152: Close tabs on toggle prevents toggling in FF3.5"
- bugfix: bug 1154: Clarify "Last Tor test failed" message

- misc: Disable geolocation in FF3.5 during Tor mode
- misc: Disable DNS prefetch in FF3.5 in Tor mode and for Tor-loaded tabs
- misc: Disable offline app cache during Tor mode
- misc: Disable specific site zoom settings during Tor mode
- new: Transfer Google cookies between country-code domains. This should make it such that captchas only need to be solved once per Tor session, as opposed to for each country.

On December 16, 2009, we released Torbutton 1.2.4. This fixes a number of bugs found after two weeks of live testing by users. It contains the following changes:

- bugfix: bug 1169: Fix blank popup conflict with Google Toolbar
- bugfix: bug 1171: Properly store and set network.dns.disablePrefetch
- bugfix: bug 1165: Fix an exception on toggle in FF3.6
- bugfix: bug 1163: Fix history loss in FF3.6
- bugfix: Fix a typo error during logging
- bugfix: Properly handle session restore in FF3.6
- misc: Kill a warning message about missing properties in window-mapper.js
- new: Add a new pref to disable Livemark updates during Tor usage (FF3.5+)

On December 21, 2009, we released an update to the -stable Tor branch, Tor 0.2.1.21. It fixes compatibility with newer OpenSSL libraries that work around the renegotiation bug. The full changelog is:

Tor 0.2.1.21 fixes an incompatibility with the most recent OpenSSL library. If you use Tor on Linux / Unix and you're getting SSL renegotiation errors, upgrading should help. We also recommend an upgrade if you're an exit relay.

Major bugfixes:

- Work around a security feature in OpenSSL 0.9.8l that prevents our handshake from working unless we explicitly tell OpenSSL that we are using SSL renegotiation safely. We are, of course, but OpenSSL 0.9.8l won't work unless we say we are.
- Avoid crashing if the client is trying to upload many bytes and the circuit gets torn down at the same time, or if the flip side happens on the exit relay. Bugfix on 0.2.0.1-alpha; fixes bug 1150.

Minor bugfixes:

- Do not refuse to learn about authority certs and v2 networkstatus documents that are older than the latest consensus. This bug might have degraded client bootstrapping. Bugfix on 0.2.0.10-alpha. Spotted and fixed by xmux.

- Fix a couple of very-hard-to-trigger memory leaks, and one hard-to- trigger platform-specific option misparsing case found by Coverity Scan.
- Fix a compilation warning on Fedora 12 by removing an impossible-to- trigger assert. Fixes bug 1173.

On December 31, 2009, we released Tor Browser Bundle 1.3.0. The major change was the upgrade of Firefox to the 3.5 branch. The full changelog is:

- upgrade Firefox to 3.5.6
- update Pidgin to 2.6.4
- update Torbutton to 1.2.4
- upgrade Tor to 0.2.1.21

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

- Updated the get-tor email autoresponder to better handle translations into non-English languages. Also updated to better handle split downloads of torbrowser bundle and mac os x vidalia bundles.
- Mike finished his six week analysis of the Firefox 3.5 code base for privacy and anonymity leaks. The notes from the audit are documented in `https://www.torproject.org/torbutton/design/FF35_AUDIT`.

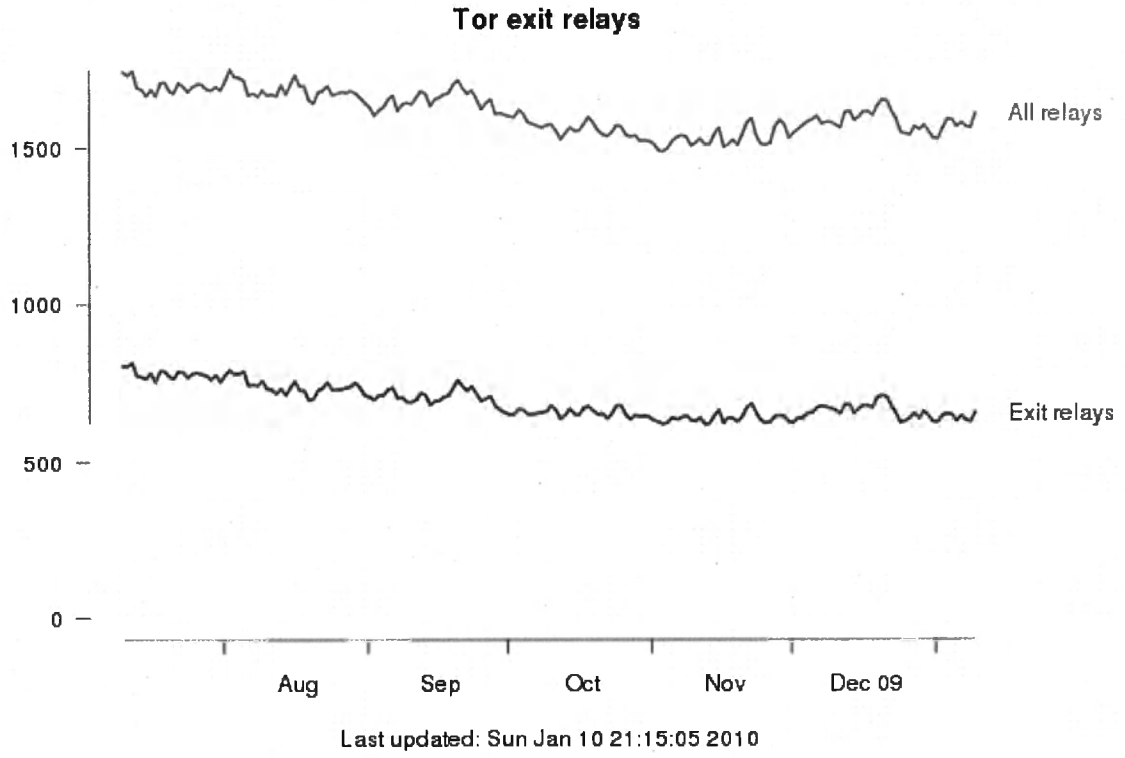
C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

Nothing to report.

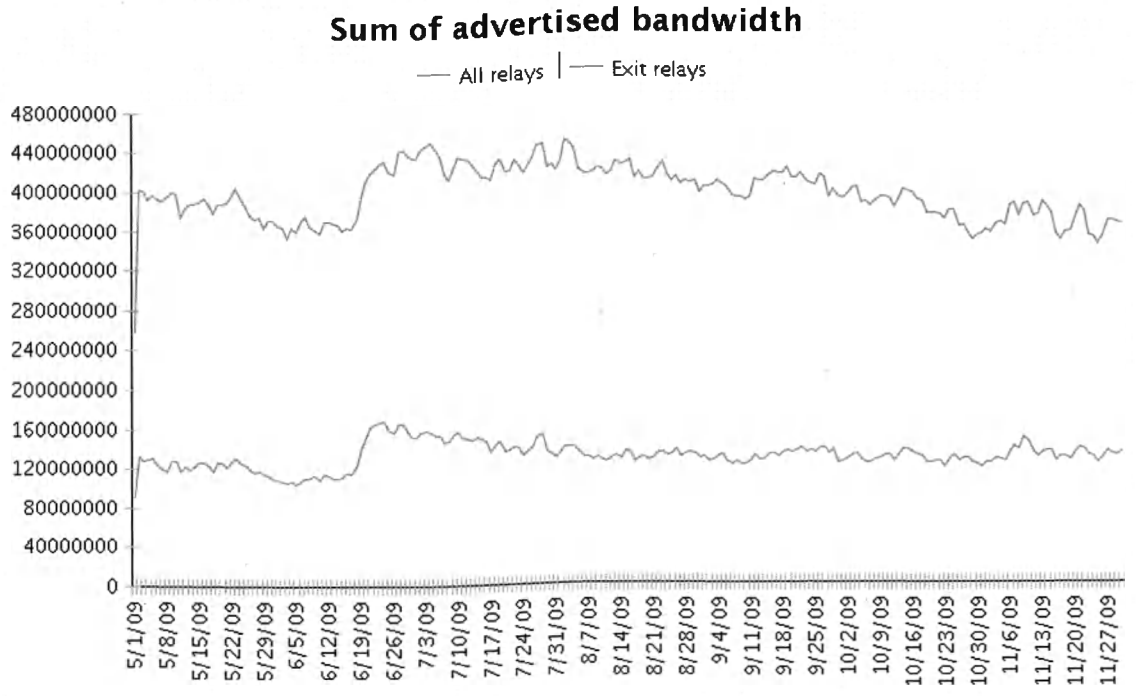
C.2.5. Hide Tor's network signature.

Nothing to report.

C.2.10 Grow the Tor network and user base. Outreach.



Graph: current size of the Tor Network



- Jacob presented at the Arab Bloggers Conference in Beirut, Lebanon. `http://www.arabloggers.com/`
- Jacob met with Al Jazeera in Doha, Qatar. `http://www.aljazeera.net/`
- Jacob met with Rainbow House in Amman, Jordan.
- Andrew and Roger attended a circumvention technology workshop in California.
- Jacob, Roger, Karsten, Steven, and others attended 26C3 in Berlin, Germany. `http://events.ccc.de/congress/2009/wiki/index.php/Main_Page`. Jacob and Roger presented on "Tor and censorship: lessons learned", `http://events.ccc.de/congress/2009/Fahrplan/events/3554.en.html`. We mirrored the video and slides at `https://blog.torproject.org/blog/tor-and-censorship-lessons-learned`.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

On December 31, 2009, we released Tor Browser Bundle 1.3.0. The major change was the upgrade of Firefox to the 3.5 branch. The full changelog is:

- upgrade Firefox to 3.5.6
- update Pidgin to 2.6.4

- update Torbutton to 1.2.4
- upgrade Tor to 0.2.1.21

Mike, Roger, and Andrew met with the Chrome team at Google to discuss integration of Tor into Chrome's "incognito mode". We need some APIs to make the integration smoother, and to be able to scale the Tor Network to handle the expected traffic from Chrome users.

C.2.12 Bridge relay and bridge authority work.

Nothing to report.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

- We did a one weekend test of the performance impact of changing circuit package window from 1000 cells to 101. The test and numbers are based on research by Csaba Kiraly. "Effect of Tor window size on performance. Email to [redacted] (b) (6) February 2009. `http://archives.seul.org/or/dev/Feb-2009/msg00000.html`". The test appeared to be a null operation, it didn't help nor hurt performance of the network as a whole.
- Karsten continues to work on metrics about the Tor Network. We have a new metrics portal, `http://metrics.torproject.org/` that shows the output, raw data, process for the collection, and the statistical analysis performed. Currently, our basic process is to collect, collate, and transform the data into graphs with R. Two organizations have offered to take the raw data from `http://archives.torproject.org/` and import it into their data analysis products. We're continuing to work on both tactics at this time.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

OS X split dmg files will be available with each release going forward. The split dmg files are a native format for OS X 10.3 (Panther) and above; so users on low bandwidth connections should easily be able to work with these.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

C.2.17 Translation work, ultimately a browser-based approach.

- Hundreds of updated translations for torbutton, tor website, vidalia, torcheck, and get-tor in the following languages: Swedish, Brazillian Portugese, Polish, Russian, Spanish, Norwegian, Burmese, Chinese, Farsi, Arabic, Portugese, Ukranian, German, Spanish, French, Finnish, Italian, Dutch, and Turkish.
- Runa applied updates to the process of syncing between the translation portal and live website. And she continues to maintain the translation portal.
- Carolyn found translators for Russian, Ukrainian, and Burmese languages. She's currently working on finding translators for Arabic, Farsi, and Spanish languages.

From: Andrew Lewman, Executive Director
To: Kelly DeYoe, program officer, BBG
RE: contract BBGCON1807S6441
Date: February 9, 2010

This report documents progress in January 2010 on contract BBGCON1807S6441 between BBG and The Tor Project.

C 2.0. New releases, new hires, new funding

1. On January 19, 2010 we released the latest in the -stable series, Tor 0.2.1.22-stable.

```
Tor 0.2.1.22 fixes a critical privacy problem in bridge directory
  authorities -- it would tell you its whole history of bridge descriptors
  if you make the right directory request. This stable update also
  rotates two of the seven v3 directory authority keys and locations.

  o Directory authority changes:
    - Rotate keys (both v3 identity and relay identity) for moria1
      and gabelmoo.

  o Major bugfixes:
    - Stop bridge directory authorities from answering dbg-stability.txt
      directory queries, which would let people fetch a list of all
      bridge identities they track. Bugfix on 0.2.1.6-alpha.
```

2. On January 19, 2010, we released the latest in the -alpha series, Tor 0.2.2.7-alpha.

```
Tor 0.2.2.7-alpha fixes a huge client-side performance bug, as well
as laying the groundwork for further relay-side performance fixes. It
also starts cleaning up client behavior with respect to the EntryNodes,
ExitNodes, and StrictNodes config options.

This release also rotates two directory authority keys, due to a
security breach of some of the Torproject servers.

  o Directory authority changes:
    - Rotate keys (both v3 identity and relay identity) for moria1
      and gabelmoo.

  o Major features (performance):
    - We were selecting our guards uniformly at random, and then weighting
      which of our guards we'd use uniformly at random. This imbalance
```

meant that Tor clients were severely limited on throughput (and probably latency too) by the first hop in their circuit. Now we select guards weighted by currently advertised bandwidth. We also automatically discard guards picked using the old algorithm. Fixes bug 1217; bugfix on 0.2.1.3-alpha. Found by Mike Perry.
- When choosing which cells to relay first, relays can now favor circuits that have been quiet recently, to provide lower latency for low-volume circuits. By default, relays enable or disable this feature based on a setting in the consensus. You can override this default by using the new "CircuitPriorityHalflife" config option. Design and code by Ian Goldberg, Can Tang, and Chris Alexander.
- Add separate per-conn write limiting to go with the per-conn read limiting. We added a global write limit in Tor 0.1.2.5-alpha, but never per-conn write limits.
- New consensus params "bwconnrate" and "bwconnburst" to let us rate-limit client connections as they enter the network. It's controlled in the consensus so we can turn it on and off for experiments. It's starting out off. Based on proposal 163.

o Major features (relay selection options):
- Switch to a StrictNodes config option, rather than the previous "StrictEntryNodes" / "StrictExitNodes" separation that was missing a "StrictExcludeNodes" option.
- If EntryNodes, ExitNodes, ExcludeNodes, or ExcludeExitNodes change during a config reload, mark and discard all our origin circuits. This fix should address edge cases where we change the config options and but then choose a circuit that we created before the change.
- If EntryNodes or ExitNodes are set, be more willing to use an unsuitable (e.g. slow or unstable) circuit. The user asked for it, they get it.
- Make EntryNodes config option much more aggressive even when StrictNodes is not set. Before it would prepend your requested entrynodes to your list of guard nodes, but feel free to use others after that. Now it chooses only from your EntryNodes if any of those are available, and only falls back to others if a) they're all down and b) StrictNodes is not set.
- Now we refresh your entry guards from EntryNodes at each consensus fetch -- rather than just at startup and then they slowly rot as the network changes.

o Major bugfixes:
- Stop bridge directory authorities from answering dbg-stability.txt directory queries, which would let people fetch a list of all bridge identities they track. Bugfix on 0.2.1.6-alpha.

o Minor features:
- Log a notice when we get a new control connection. Now it's easier for security-conscious users to recognize when a local application is knocking on their controller door. Suggested by bug 1196.

```
  - New config option "CircuitStreamTimeout" to override our internal
    timeout schedule for how many seconds until we detach a stream from
    a circuit and try a new circuit. If your network is particularly
    slow, you might want to set this to a number like 60.
  - New controller command "getinfo config-text". It returns the
    contents that Tor would write if you send it a SAVECONF command,
    so the controller can write the file to disk itself.
  - New options for SafeLogging to allow scrubbing only log messages
    generated while acting as a relay.
  - Ship the bridges spec file in the tarball too.
  - Avoid a mad rush at the beginning of each month when each client
    rotates half of its guards. Instead we spread the rotation out
    throughout the month, but we still avoid leaving a precise timestamp
    in the state file about when we first picked the guard. Improves
    over the behavior introduced in 0.1.2.17.

o Minor bugfixes (compiling):
  - Fix compilation on OS X 10.3, which has a stub mlockall() but
    hides it. Bugfix on 0.2.2.6-alpha.
  - Fix compilation on Solaris by removing support for the
    DisableAllSwap config option. Solaris doesn't have an rlimit for
    mlockall, so we cannot use it safely. Fixes bug 1198; bugfix on
    0.2.2.6-alpha.

o Minor bugfixes (crashes):
  - Do not segfault when writing buffer stats when we haven't observed
    a single circuit to report about. Found by Fabian Lanze. Bugfix on
    0.2.2.1-alpha.
  - If we're in the pathological case where there's no exit bandwidth
    but there is non-exit bandwidth, or no guard bandwidth but there
    is non-guard bandwidth, don't crash during path selection. Bugfix
    on 0.2.0.3-alpha.
  - Fix an impossible-to-actually-trigger buffer overflow in relay
    descriptor generation. Bugfix on 0.1.0.15.

o Minor bugfixes (privacy):
  - Fix an instance where a Tor directory mirror might accidentally
    log the IP address of a misbehaving Tor client. Bugfix on
    0.1.0.1-rc.
  - Don't list Windows capabilities in relay descriptors. We never made
    use of them, and maybe it's a bad idea to publish them. Bugfix
    on 0.1.1.8-alpha.

o Minor bugfixes (other):
  - Resolve an edge case in path weighting that could make us misweight
    our relay selection. Fixes bug 1203; bugfix on 0.0.8rc1.
  - Fix statistics on client numbers by country as seen by bridges that
    were broken in 0.2.2.1-alpha. Also switch to reporting full 24-hour
    intervals instead of variable 12-to-48-hour intervals.
  - After we free an internal connection structure, overwrite it
    with a different memory value than we use for overwriting a freed
```

```
    internal circuit structure. Should help with debugging. Suggested
    by bug 1055.
  - Update our OpenSSL 0.9.8l fix so that it works with OpenSSL 0.9.8m
    too.

o Removed features:
  - Remove the HSAuthorityRecordStats option that version 0 hidden
    service authorities could have used to track statistics of overall
    hidden service usage.
```

3. On January 19, 2010, we released an updated Tor Browser Bundle, version 1.3.1.

```
update Firefox to 3.5.7
update Pidgin to 2.6.5
update Tor to 0.2.1.22
```

4. On January 25, 2010, we released Vidalia 0.2.7.

```
o Remove the explicit palette set for the configuration dialog that
    prevented the dialog from inheriting colors from the user's current
    system theme. (Ticket #485. Patch from mkirk.)
o Correct the path to the badge pixmap used in time skew warning
    messages. (Ticket #537. Patch from mkirk.)
o Fix compilation on Debian GNU/kFreeBSD. Patch from dererk.
o Clean up a couple status event messages related to dangerous port
    warnings.
o Change the vidalia_ru.nsh output encoding from KOI8-R to Windows-1251.
    (Ticket #527)
o Add an option for building an OS X 10.4 compatible binary.
```

5. On January 26, 2010, we released an updated -alpha, Tor 0.2.2.8-alpha.

```
o Major bugfixes:
  - Fix a memory corruption bug on bridges that occured during the
    inclusion of stats data in extra-info descriptors. Also fix the
    interface for geoip_get_bridge_stats* to prevent similar bugs in
    the future. Diagnosis by Tas, patch by Karsten and Sebastian.
    Fixes bug 1208; bugfix on 0.2.2.7-alpha.

o Minor bugfixes:
  - Ignore OutboundBindAddress when connecting to localhost.
    Connections to localhost need to come _from_ localhost, or else
    local servers (like DNS and outgoing HTTP/SOCKS proxies) will often
    refuse to listen.
```

C.2.1. Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

Submitted Proposal 169. A backward-compatible change to the Tor connection establishment protocol to avoid the use of TLS renegotiation. In response to others using TLS renegotiation incorrectly,

vendors are pulling support for TLS renegotiation. As TLS renegotiation disappears from the Internet, Tor's use of it will stand out. In order to blend in with the crowd, we need to remove TLS renegotiation from the Tor protocol. The full spec can be found at `http://gitweb.torproject.org//tor.git?a=blob;f=doc/spec/proposals/169-eliminating-renegotiation.txt;hb=HEAD`.

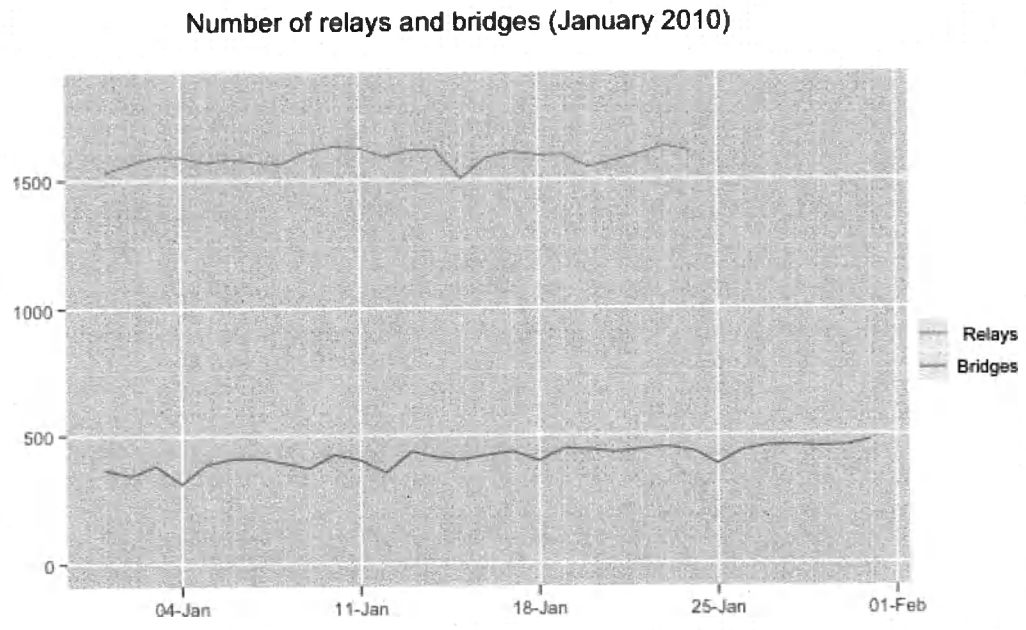
C.2.2. Architecture and technical design docs for Tor enhancements related to blocking-resistance.

Submitted Proposal 169. A backward-compatible change to the Tor connection establishment protocol to avoid the use of TLS renegotiation. In response to others using TLS renegotiation incorrectly, vendors are pulling support for TLS renegotiation. As TLS renegotiation disappears from the Internet, Tor's use of it will stand out. In order to blend in with the crowd, we need to remove TLS renegotiation from the Tor protocol. The full spec can be found at `http://gitweb.torproject.org//tor.git?a=blob;f=doc/spec/proposals/169-eliminating-renegotiation.txt;hb=HEAD`.

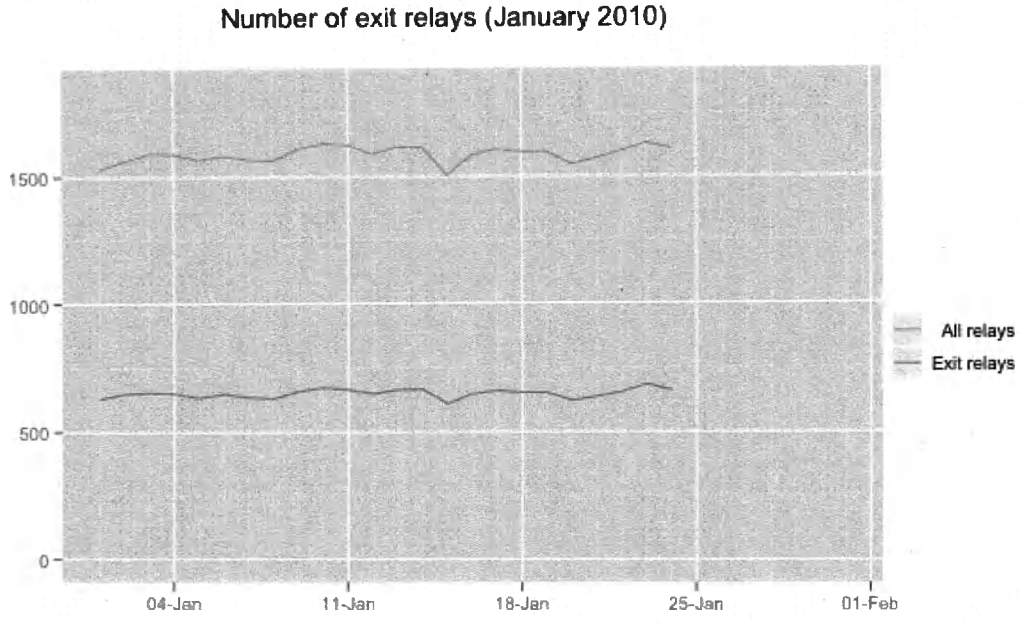
C.2.5. Hide Tor's network signature.

Submitted Proposal 169. A backward-compatible change to the Tor connection establishment protocol to avoid the use of TLS renegotiation. In response to others using TLS renegotiation incorrectly, vendors are pulling support for TLS renegotiation. As TLS renegotiation disappears from the Internet, Tor's use of it will stand out. In order to blend in with the crowd, we need to remove TLS renegotiation from the Tor protocol. The full spec can be found at `http://gitweb.torproject.org//tor.git?a=blob;f=doc/spec/proposals/169-eliminating-renegotiation.txt;hb=HEAD`.

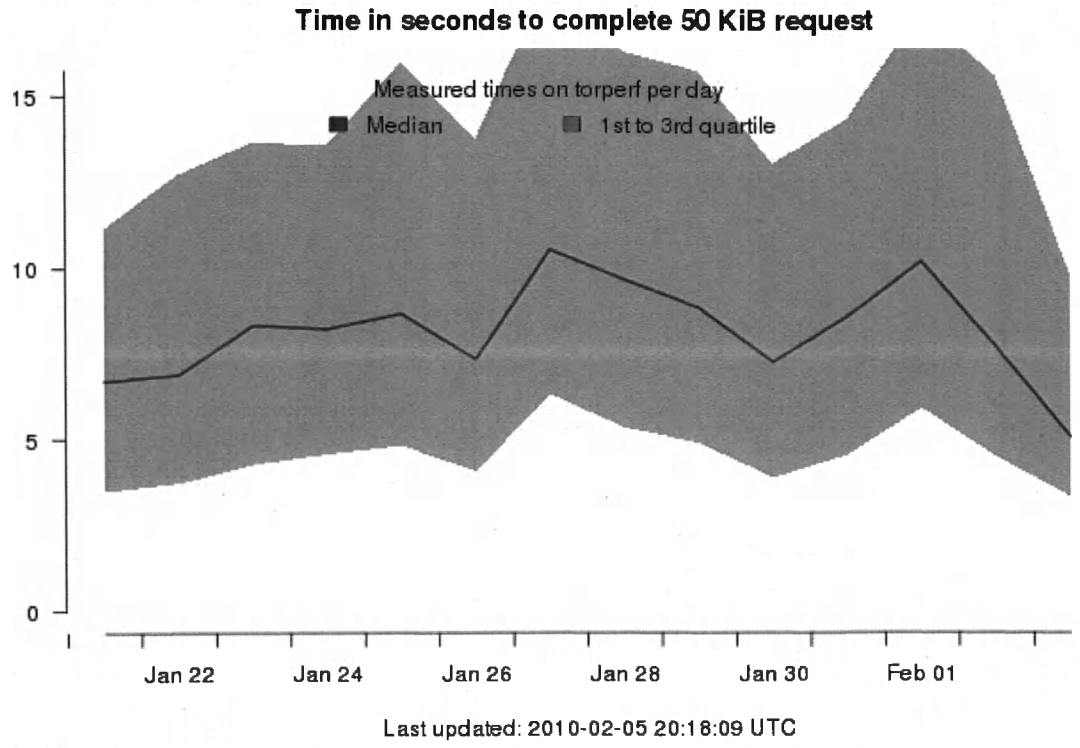
C.2.10 Grow the Tor network and user base. Outreach.



Graph: current size of the Tor Network



Graph: Breakdown of exit and non-exit relays in the Tor Network



Outreach and Advocacy

- Paul, Karsten, and Roger attended Financial Cryptography and Data Security 2010 Conference. Roger Dingledine presented a paper he had written with Tsuen-Wan Ngan and Dan Wallach on "Building Incentives into Tor". This paper won Best Paper Award at the conference. Learn more at `http://fc10.ifca.ai/`.
- Karsten and Roger attended the Workshop on Ethics in Computer Security Research, `http://www.cs.stevens.edu/~spock/wecsr2010/`. They presented "A Case Study on Measuring Statistical Data in the Tor Anonymity Network."
- Andrew attended the Internet Freedom speech by Secretary of State Clinton, `http://www.state.gov/secretary/rm/2010/01/135519.htm`.
- Roger and Jacob discussed Tor with the Pirate Party of Sweden.
- Jacob met with NorduNet to discuss their bandwidth authority and how to help Tor grow in the NorduNet, `http://www.nordu.net`.
- Jacob and Wikileaks people met with policymakers in Iceland to discuss freedom of speech, freedom of press, and that online privacy should be a fundamental right.
- Roger, Karen, and Andrew met with CDT, Internews, and BBG to discuss various topics.

- Andrew was interviewed for 90 minutes by vbs.tv about Tor, online anonymity and privacy, and the increasing usage of Tor as a censorship circumvention tool. vbs.tv will release the interview in 2010.

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

On January 19, 2010, we released an updated Tor Browser Bundle, version 1.3.1.

```
update Firefox to 3.5.7
update Pidgin to 2.6.5
update Tor to 0.2.1.22
```

C.2.12 Bridge relay and bridge authority work.

From the Tor 0.2.2.8-alpha release notes;
Fix a memory corruption bug on bridges that occurred during the inclusion of stats data in extra-info descriptors. Also fix the interface for geoip_get_bridge_stats to prevent similar bugs in the future. Diagnosis by Tas, patch by Karsten and Sebastian. Fixes bug 1208; bugfix on 0.2.2.7-alpha.

Roger and Christian defined a roadmap for bridgedb updates, scalability, and bugfixes. The plan can be found at `http://gitweb.torproject.org//bridgedb.git?a=blob_plain;f=TODO;hb=HEAD`

C.2.13. Scalability, load balancing, directory overhead, efficiency.

From the 0.2.2.7-alpha release notes:
We were selecting our guards uniformly at random, and then weighting which of our guards we'd use uniformly at random. This imbalance meant that Tor clients were severely limited on throughput (and probably latency too) by the first hop in their circuit. Now we select guards weighted by currently advertised bandwidth. We also automatically discard guards picked using the old algorithm. Fixes bug 1217; bugfix on 0.2.1.3-alpha. Found by Mike Perry.

When choosing which cells to relay first, relays can now favor circuits that have been quiet recently, to provide lower latency for low-volume circuits. By default, relays enable or disable this feature based on a setting in the consensus. You can override this default by using the new "CircuitPriorityHalflife" configuration option. Design and code by Ian Goldberg, Can Tang, and Chris Alexander.

Mike Perry implemented consensus parameters for the Circuit Build Times constants and found good defaults based on experimentation on a few simulated links. The simulations seem to indicate that tor does really poorly on links with greater than 1 second of latency. Mike wrote up his findings at `http://archives.seul.org/or/dev/Jan-2010/msg00012.html`. Mike's work on circuit build times should improve tor client performance as the clients pick new guard nodes and learn better circuit build times.

C.2.14. Incentives work.

Nothing to report.

C.2.15. More reliable (e.g. split) download mechanism.

Enhanced get-tor to handle Apple OS X split files.

C.2.16. Footprints from Tor Browser Bundle.

Nothing to report.

C.2.17 Translation work, ultimately a browser-based approach.

Updated translations via the translation portal for Chinese, Norwegian, Russian, Dutch, French, Polish, Swedish, Italian, German, Spanish, Burmese, and Turkish languages.