From: Roger Dingledine
To: Kelly DeYoe
Cc: Andrew_Lewman; Ken Berman; Sami Mousa
Subject: Re: IBB Network meeting
Date: Monday, May 04, 2009 7:30:58 PM

On Mon, May 04, 2009 at 04:16:30PM -0400, Kelly DeYoe wrote:
> They were all added piecemeal to our former contractor's database, and
> we don't have access to it, so I'll have to trace back through a few
> years of email to get a good list, but will try to send it along
> sometime this week.

Great.

In other news, take a look at
http://freehaven.net/~karsten/metrics/dirreq-report-2009-04-30.pdf

It looks like data set #2 shows a much higher number of hits from Iran.

Is this a result of GIFC's pulling out of Iran? Or just a general trend?
Or a fluke? More research remains. :)

--Roger

From: Kelly DeYoe
To: Roger Dingledine
Cc: Andrew Lewman; Ken Berman; Sami Mousa
Subject: Re: IBB Network meeting
Date: Monday, May 04, 2009 5:16:30 PM

We've just been adding additional ranges to whitelists of allowed IP addresses in Iran on an ad hoc basis as we receive reports from users in Iran that they are blocked from using our existing web proxies. I can gather up the ranges for you so you can shift them around and then maybe provide us with better stats for Iran with their inclusion.

They were all added piecemeal to our former contractor's database, and we don't have access to it, so I'll have to trace back through a few years of email to get a good list, but will try to send it along sometime this week.

-k

Roger Dingledine wrote:
> Hi Kelly,
>
> It occurred to me that you folks might have a better picture of which IP
> addresses are 'in' Iran than the public geoip services do -- for example,
> I remember a few years ago services like Anonymizer gave free service
> selectively to IP addresses from Iran.
>
> If so, that would let us make more accurate graphs of which countries
> our users are coming from.
>
> Would that be interesting? :)
>
> Thanks,
> --Roger
>

From: Roger Dingledine
To: Kelly DeYoe
Cc: Andrew Lewman; Ken Berman; Sami Mousa
Subject: Re: IBB Network meeting
Date: Thursday, April 30, 2009 4:03:36 PM

Hi Kelly,

It occurred to me that you folks might have a better picture of which IP addresses are 'in' Iran than the public geoip services do -- for example, I remember a few years ago services like Anonymizer gave free service selectively to IP addresses from Iran.

If so, that would let us make more accurate graphs of which countries our users are coming from.

Would that be interesting? :)

Thanks,
--Roger

From: Andrew Lewman
To: Ken Berman
Cc: Kelly DeYoe; Roger Dingledine; Sami Mousa
Subject: Re: IBB Network meeting
Date: Monday, April 13, 2009 4:13:57 PM

On Mon, 13 Apr 2009 11:54:38 -0400
Ken Berman <[redacted] wrote:

> I'm good for the 29th, but can we make it 1:00? Ken

1:00 pm is great. Roger and I will stick to 1, not 12:30 like last time.

--
Andrew Lewman
The Tor Project
pgp 0x31B0974B
[redacted]

Website: https://torproject.org/
Blog: https://blog.torproject.org/
Identica/Twitter: torproject

From: Andrew Lewman
To: Kelly DeYoe
Cc: Ken Berman; Roger Dingledine; Sami Mousa
Subject: Re: IBB Network meeting
Date: Tuesday, April 07, 2009 5:16:38 PM

On Tue, 07 Apr 2009 15:07:36 -0400
Kelly DeYoe <[redacted] wrote:

> Ken is out of the office this week, so I'm afraid I cannot coordinate
> with him to set up a definite time. Wednesday 4/29 would be the
> better day for both Sami (who I have added to the Cc: list) and
> myself however, so let's tentatively plan for a meeting on that day.

Great. How about 2pm tentatively?

--
Andrew Lewman
The Tor Project
pgp 0x31B0974B
[redacted]

Website: https://torproject.org/
Blog: https://blog.torproject.org/
Identica/Twitter: torproject

From: Kelly DeYoe
To: Andrew Lewman
Cc: Ken Berman; Roger Dingledine; Sami Mousa
Subject: Re: IBB Network meeting
Date: Tuesday, April 07, 2009 4:07:36 PM

Ken is out of the office this week, so I'm afraid I cannot coordinate with him to set up a definite time. Wednesday 4/29 would be the better day for both Sami (who I have added to the Cc: list) and myself however, so let's tentatively plan for a meeting on that day.

-k

Andrew Lewman wrote:
> Hello Ken and Kelly,
>
> Roger and I are going to be in town early April 27-29 to meet with the
> DOJ and some other organizations. Would the 27th or 29th be good days
> to stop by and talk to your network person (Sami?) about his ideas
> regarding Tor?
>

From: Ken Berman
To: Andrew Lewman; Kelly DeYoe
Cc: Roger Dingledine; Sami Mousa
Subject: RE: IBB Network meeting
Date: Monday, April 13, 2009 12:54:38 PM

I'm good for the 29th, but can we make it 1:00? Ken

-----Original Message-----
From: Andrew Lewman [mailto:[redacted (b) (6)]
Sent: Tuesday, April 07, 2009 4:17 PM
To: Kelly DeYoe
Cc: Ken Berman; Roger Dingledine; Sami Mousa
Subject: Re: IBB Network meeting

On Tue, 07 Apr 2009 15:07:36 -0400
Kelly DeYoe <[redacted (b) (6)] wrote:

> Ken is out of the office this week, so I'm afraid I cannot coordinate
> with him to set up a definite time. Wednesday 4/29 would be the
> better day for both Sami (who I have added to the Cc: list) and myself
> however, so let's tentatively plan for a meeting on that day.

Great. How about 2pm tentatively?

--
Andrew Lewman
The Tor Project
pgp 0x31B0974B
[redacted (b) (6)]

Website: https://torproject.org/
Blog: https://blog.torproject.org/
Identica/Twitter: torproject

From: Andrew Lewman
To: Kelly DeYoe
Cc: Roger Dingledine
Subject: Re: IBB Network meeting
Date: Tuesday, May 12, 2009 4:02:48 PM

Thanks!

On Mon, 11 May 2009 17:40:39 -0400
Kelly DeYoe <_____ wrote:

> Took me a little longer to compile and clean up the list, it actually
> broke down to be pretty small once I removed everything that was
> being consistently reported as in Iran now as well as figuring out
> the larger CIDR blocks for some addresses we had only whitelisted
> smaller blocks before:
>
> 78.111.8.0/21
> 82.99.200.0/18
> 82.115.16.0/20
> 85.185.0.0/16
> 91.98.0.0/15
> 93.126.0.0/18
> 193.178.200.0/22
> 217.172.96.0/19
> 217.218.0.0/15
>
> (Some of these do report as being in Iran from some country mapping
> DBs, but others sources seem to think some are in UAE or Turkey.)
>
> I may still have some others tucked away in various places, will send
> them along as I find them.
>
> -k
>
> Roger Dingledine wrote:
> > Hi Kelly,
> >
> > It occurred to me that you folks might have a better picture of
> > which IP addresses are 'in' Iran than the public geoip services do
> > -- for example, I remember a few years ago services like Anonymizer
> > gave free service selectively to IP addresses from Iran.
> >
> > If so, that would let us make more accurate graphs of which
> > countries our users are coming from.
> >
> > Would that be interesting? :)
> >
> > Thanks,
> > --

--
Andrew Lewman
The Tor Project
pgp 0x31B0974B
[redacted]

Website: https://torproject.org/

Blog: https://blog.torproject.org/
Identica/Twitter: torproject

From: Kelly DeYoe
To: Andrew Lewman
Cc: Ken Berman; Melissa Gilroy
Subject: Re: IBB
Date: Wednesday, April 13, 2011 10:37:12 AM

Nope, it needs to be dated within the last 30 days in order to be processed. Please update and resend so we can process it.

Thanks.

-k

Andrew Lewman wrote:
> On Tue, 12 Apr 2011 15:40:01 -0400
> Kelly DeYoe <[redacted] wrote:
>
>> Also, please send an updated version of invoice #32 with today's date
>> as we will not be able to process it dated from December!
>
> Attached. It was actually sent in January, does this help because it's
> in the same calendar year?
>

From: Andrew Lewman
To: Kelly DeYoe
Cc: Ken Berman; Melissa Gilroy
Subject: Re: IBB
Date: Tuesday, April 12, 2011 10:41:39 PM

On Tue, 12 Apr 2011 15:38:21 -0400
Kelly DeYoe <[redacted] (b) (6)> wrote:

> Andrew, based on my own review and the review of our admin. officer
> who processes the payments, Malita Dyson, we have no record of
> receiving invoice #32 (12/2010) from Tor. We have processed invoices
> #31, #33, #34, but #32 was skipped. If you can please submit it to
> us, it will be processed for payment.
>
> When submitting invoices, you may wish include both Malita and myself
> on the email in the future, as I don't have any email trail of
> invoices since they have been sent to Malita exclusively, and she
> just presents me with the hardcopy to approve and sign.

Going forward, I will cc you Kelly. Thanks for investigating!

--
Andrew
pgp 0x74ED336B

From: Andrew Lewman
To: Kelly DeYoe
Cc: Ken Berman; Melissa Gilroy
Subject: Re: IBB
Date: Tuesday, April 12, 2011 10:41:05 PM
Attachments: 2011-01-11-32nd-Invoice.pdf

On Tue, 12 Apr 2011 15:40:01 -0400
Kelly DeYoe <[redacted] wrote:

> Also, please send an updated version of invoice #32 with today's date
> as we will not be able to process it dated from December!

Attached. It was actually sent in January, does this help because it's
in the same calendar year?

--
Andrew
pgp 0x74ED336B

From: Andrew Lewman
To: Kelly DeYoe
Cc: Ken Berman; Melissa Gilroy
Subject: Re: IBB
Date: Wednesday, April 13, 2011 12:02:28 PM
Attachments: 2011-01-11-32nd-Invoice.pdf

On Wed, 13 Apr 2011 09:37:12 -0400
Kelly DeYoe <[redacted (b) (6)] wrote:

> Nope, it needs to be dated within the last 30 days in order to be
> processed. Please update and resend so we can process it.

Attached, thanks!

--
Andrew
pgp 0x74ED336B

From: Ken Berman
To: Roger Dingledine; Kelly DeYoe
Cc: [redacted]
Subject: RE: IBB/Tor notes for April
Date: Wednesday, May 21, 2008 10:25:36 AM

" Berman Center's proposal to DRL".....I am so glad to have a center named after me....

Kelly -do we need to press the Russian Service to mod the web page for the Tor info?

Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Monday, May 12, 2008 4:55 AM
To: Ken Berman; Kelly DeYoe
Cc: [redacted]
Subject: IBB/Tor notes for April

Hi folks,

Here are my notes for the April report. I'm afraid they're not in a doc file yet; I'll aim to do that in the next few days. But I figured you might be interested to see them in their current form.

I'm in Europe til May 21, so assuming we want a call for this month, doing it after that would be best. :)

Thanks!
--Roger

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

Tor 0.2.0.24-rc (released Apr 22) adds dizum (run by Alex de Joode) as the new sixth v3 directory authority, makes relays with dynamic IP addresses and no DirPort notice more quickly when their IP address changes, fixes a few rare crashes and memory leaks, and fixes a few other miscellaneous bugs. Tor 0.2.0.25-rc (released Apr 23) makes Tor work again on OS X and certain BSDs.
http://archives.seul.org/or/talk/May-2008/msg00014.html

Torbutton 1.1.18 (released Apr 17) fix many usability and interoperability items, in an attempt to make the new Torbutton not so obnoxious in its zeal to protect the user. It also includes new translations for French, Russian, Farsi, Italian, and Spanish.

We hired Jacob Appelbaum as a full-time contractor in mid April. He will be working on a translation portal, auto update for Tor on Windows and OS X, an email autoresponder for sending Tor clients to users who can't reach our website, and other projects down the road.

We will be hiring Matt Edman as a part-time employee at the beginning of May. He will be working on Vidalia maintenance, bugfixes, and new features --- for example, providing a GUI interface for the above auto update feature, letting users change their preferred language in Vidalia without requiring an application restart, and providing a better GUI

for showing Tor's start-up progress.

We worked on a funding proposal to the State Dept's DRL grant in cooperation with Internews and Psiphon. We'll hear about that one... sometime.

We have been awarded two grants by NLNet (http://www.nlnet.nl), a Dutch NGO that emphasizes free-software development and is focusing this year on privacy software. One grant is to work harder on lowering the overhead of directory requests, especially during bootstrap, and should directly improve the experience for Tor users on modems or cell phones; it will allow us to bring Peter Palfrader on half-time from mid-May to January to accelerate our scalability work. The other grant is to work on making hidden service rendezvous and interaction faster, with the goal of making it easier to set up and advertise a hidden service even for short periods of time; it will allow us to bring Karsten Loesing on quarter-time from mid-May to January so we can work harder in this direction.

The additions of Jacob, Matt, Peter, and Karsten will move Tor from 3 FTE developers to 5 FTE developers.

We gave $5k to the research group of Ian Goldberg, a professor at Waterloo in Canada, to fund his graduate student to work on a UDP design for Tor. Our funding was matched 4x by MITACS, a Canadian research organization similar to NSF.

And that's not all! Google is funding seven students to work on Tor projects over the summer as part of the "Google Summer of Code": https://blog.torproject.org/blog/congrats-2008-google-summer-code-students%21

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.

We did a complete overhaul of the https://check.torproject.org/ page. Now it accepts a language choice, e.g. https://check.torproject.org/?lang=fa-IR Available languages are German, English, Spanish, Italian, Farsi, Japanese, Polish, Portugese, Russian, and Chinese. The Tor Browser Bundle automatically uses the appropriate language as its home page, based on which language of the Browser Bundle was downloaded.

Started on a documentation page to explain to users what bridges are, how they can decide whether they need one, and how to configure their Tor client to use them: https://www.torproject.org/bridges.html

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

We've started working on a design proposal for letting the v3 directory authorities produce a consensus networkstatus even when they disagree about who is a valid authority. As we add more v3 authorities, it becomes more and more of a hassle to coordinate getting a majority of authorities to upgrade immediately. https://www.torproject.org/svn/trunk/doc/spec/proposals/134-robust-voting.txt

We've also started working on a design proposal for making it easier

to set up a private or testing Tor network. With the advent of the v3 directory protocol, it currently takes up to 30 minutes before a test network will produce a useful networkstatus consensus. Also, there are a dozen different config options that need to be set correctly for a Tor network running on a single IP address to not trigger various security defenses. This approach should let more people set up their own Tor networks, either for testing or because they can't reach the main Tor network.
https://www.torproject.org/svn/trunk/doc/spec/proposals/135-private-tor-networks.txt

We have the beginnings of a grand plan for how to successfully scale the Tor network to orders of magnitude more relays than we have currently. Much more work and thinking remain.
https://www.torproject.org/svn/trunk/doc/spec/proposals/ideas/xxx-grand-scaling-plan.txt

We also did a retrospective on currently open but not finished design proposals, so we don't have as many "open" proposals in the pipeline but not getting attention:
http://archives.seul.org/or/dev/Apr-2008/msg00009.html

C.2.5. Hide Tor's network signature.

As far as we know, nobody's put any effort into blocking our current protocol as it stands, since it no longer says "TOR" in the TLS certificates or "/tor/" in the directory fetch requests.

The next two steps in the arms race will make it harder for an attacker to catch up:

1) Spoof Firefox's ciphersuites in our TLS handshake. That is, extend or adapt OpenSSL internals so that the list of advertised ciphersuites from Tor matches the list that Firefox advertises. This will require advertising ciphers that OpenSSL doesn't actually support, failing safely if those ciphers are actually selected.

2) Spoof Firefox's extensions list in our TLS handshake. Turn on extensions in OpenSSL to match those advertised in Firefox. If any don't exist (we currently think they all do), then find a way to make OpenSSL advertise them without actually supporting them.

We hope to get a first cut at these deployed in June.

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

Roger and Nick talked to Apu Kapadia at Dartmouth about his plans to open-source Nymble, which is their web-based scheme to let services like Wikipedia blacklist Tor users without needing to (or being able to) learn their location/identity. We're going to continue encouraging them discuss Nymble on or-talk / or-dev, and hopefully sometime in 2008 we will have a first version ready for testing:
http://www.cs.dartmouth.edu/~nymble/

Roger also talked to Robert Guerra about his DRL proposal as head of a new group at Freedom House. We concluded that we weren't in a position to give him an official letter of endorsement, but that we would be happy to work together if either of us get funded. I asked him to keep me in mind if he has any trainings where I could be useful, since putting me in front of users has been a good move in the past for both me and the users.

Along those lines, Roger also talked to Ethan Zuckerman about the Berman

Center's proposal to DRL. They are hoping to get some funding to do more thorough and periodic analyses of the available circumvention tools; they have Hal Roberts on board, the fellow who did the earlier report that the earlier funders then quashed. Ethan explained that they will continue to emphasize open-source and open-design as critical criteria, so Tor will likely be in good shape going forward if they end up being the ones to do the analyses.

Roger talked to Valer Mischenko at NLNet about some of his plans to make a Privacy CD. Pointed him to Tactical Tech's NGO-in-a-Box project. Valer is the director for NLNet, so it seems smart to keep him happy.

Roger collected a new set of stats for GeoIP-based breakdown of Tor clients. It looks like the overall Tor population has grown by 50% in the past four months, with a particular increase in Germany (our #1 country by user base). We pondered a little bit how to get a more accurate and comprehensive answer; we're hoping to finish a design proposal draft in this direction in May.

Roger went to Beansec, which is a monthly gathering of security professionals in the Boston area, and met a nice fellow from SiteAdvisor, who independently discovered Tor last week and had been thinking of using it to audit websites in a way that the sites don't realize they're being audited. I gave him my card but haven't followed up with him yet.

We added several more research papers that we'd like to see written to the https://www.torproject.org/volunteer#Research page. In May we'll add a few more and then start pointing academic professors at the new list.

Kevin Bauer and Damon McCoy have an upcoming PETS paper on measuring Tor users and usage. We looked through it to give suggestions on how to make their measurements more accurate and their conclusions more useful.

Roger visited Gari Clifford's group at the MIT Media Lab. They're working on citizen journalism in e.g. Bolivia, and want to get something like Tor working for cell phones. I'll meet with them again at the end of May, and see what they've come up with.

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

The development version of Vidalia now has GUI boxes to configure an http proxy that Vidalia should launch when it starts. (The Tor Browser Bundle already uses these config options internally to launch Polipo when it starts.) The next steps are to make sure that Polipo (our preferred new http proxy) is stable enough on Windows, and then start shipping some new standard bundles with Polipo rather than Privoxy.

We cleaned up the Torbutton install in the OS X bundles so it installs Torbutton for the local user, rather than global. Hopefully this will make OS X users happier.

C.2.12. Bridge relay and bridge authority work

No work on this item this month.

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

We removed the Tor relay "lefkada" as a v3 directory authority, since it has been down for several months; and set up the Tor relay "dizum" (run by Alex de Joode) as the replacement sixth v3 directory authority.

From the Tor 0.2.0.24-rc ChangeLog:
Detect address changes more quickly on non-directory mirror relays. Bugfix on 0.2.0.18-alpha; fixes bug 652.

We started work on a patch for OpenSSL that will make it keep less buffer space around. Currently fast Tor relays use (waste) as much as 100M of memory in OpenSSL's buffers.

We made a lot of progress on the 0.2.1.x development tree at reducing our memory overhead. The first 0.2.1.x alpha release will come out in May or June. (It depends when 0.2.0.x finally stabilizes.)

We're making progress on integrating a UPnP library into Vidalia. This feature will allow users who want to set up a Tor relay but don't want to muck with manual port forwarding on their router/firewall to just click a button and have Vidalia interact with their router/firewall automatically. This approach won't work in all cases, but it should work in at least some. We hope to land the first version of this in May.

Steven Murdoch and Robert Watson worked towards a final version of their PETS 2008 paper called "Metrics for Security and Performance in Low-Latency Anonymity Systems." The final version will be available in May at:
http://www.cl.cam.ac.uk/~sjm217/papers/pets08metrics.pdf

C.2.14. Incentives work.

Mike Perry found a major flaw in our earlier "gold star" incentives design: by passing the priority of the client along the entire circuit, we let the exit node correlate the times of certain actions with whether certain relays are on-line at those times. Over time, an attacker can learn which relays are often online when target actions happen. One approach to address this would be to give out e-cash digital coins for good service, and then these coins can be used later even when the relay isn't online. Many issues remain before this alternate design can be considered better, though.

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

So far there appear to be no free-software zip splitters that work on Windows and produce self-contained exe files for automatically reconstructing the file. Rather than using a closed-source shareware application (as it seems a shame to put a trust gap in our build process when we don't need to), the current plan is to write some instructions for users to fetch the 7zip program, and then fetch a set of blocks, and run a batch file to reconstruct them. We're in the process of trying to learn how large the blocks can be -- preliminary guess is 2MB.

We also started exploring whether we can mail the entire Tor Browser Bundle exe as a gmail attachment. The answer appears to be yes, but we need to zip it first so gmail doesn't complain about an executable attachment. In May we're hoping to set up an email autoresponder to see if the users consider this approach practical also.

C.2.16. Footprints from Tor Browser Bundle.

No work on this item yet. We're planning to get to it in June.

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

We have a first draft of a translation portal up here:
https://www.torproject.org/translation-portal

The Vidalia GUI now has (manual) translation instructions:
http://trac.vidalia-project.net/wiki/Translations

We've registered the Vidalia project on "LaunchPad", which is a
web-based translation site that is compatible with Vidalia's string
format:
https://translations.launchpad.net/vidalia/trunk/+pots/vidalia
We're currently working to try to upload our current translations into
the LaunchPad interface.

We've registered the Torbutton project on "BabelZilla", which is a
web-based translation site designed specifically for Firefox extensions.
We've uploaded the current translation strings:
http://www.babelzilla.org/index.php?option=com_wts&Itemid=88&extension=3510&type=lang

Lastly, we've begun developer-oriented documentation for how to manage
and maintain these various translation web-interfaces:
https://www.torproject.org/svn/trunk/doc/translations.txt

From: Roger Dingledine
To: Ken Berman
Cc: [redacted]
Subject: Re: IBB/Tor notes for April
Date: Saturday, May 24, 2008 1:45:30 AM

On Wed, May 21, 2008 at 09:25:36AM -0400, Ken Berman wrote:
> " Berman Center's proposal to DRL".....I am so glad to have a center
>named after me....

Uhm, erm, yeah. :)

Hey, speaking of DRL proposals, I finally learned last week why you thought we had made up a UDP plan for our State Dept proposal -- it turns out that Eric Johnson et al did in fact propose this on our behalf. They just didn't bother telling us until long after. This will be one of the many details that we sort out, if the funding shows up, as we all learn what the funders actually wanted to fund. But for now, nothing to do there but ignore it and make some actual progress in the meantime.

> Kelly -do we need to press the Russian Service to mod the web page
>for the Tor info?

Let me know if I can do anything to help here. Even better, let me know if you have detailed enough plans that you can share them. (For example, which web page are you planning to mod?)

Thanks,
--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe; [redacted]
Subject: Re: IBB"s web-based translation system?
Date: Monday, February 04, 2008 5:07:08 PM

Roger - We do? I think you misunderstood Kelly, or maybe not and this is something new to me! Ken

Roger Dingledine wrote:

>Hi Kelly,
>
>We talked earlier about how IBB has a proprietary web-based translation
>system that makes it easier for the non-technical translators. Can you
>send me a few screenshots (or at least a description) to give me an idea
>of how the interface works?
>
>We've been looking at https://translations.launchpad.net/ but all
>the web-based translation paradigms I've seen so far are designed for
>short phrases like in dialog boxes, where context doesn't matter much.
>Translating a tutorial or a webpage one sentence at a time without regard
>for context seems like a recipe for disaster. So does it break it up
>into sentences on a single page and give you a series of "sentence and
>translation box for that sentence"? Or is there a better way?
>
>Thanks!
>--Roger
>
>
>

From: Kyle Noori
To: Andrew Lewman
Cc: Ken Berman; Kelly DeYoe; Sho Ho; Roger Dingledine
Subject: Re: idea
Date: Thursday, February 24, 2011 2:42:15 PM

-As for Packet sniffers, WireShark program is what I think it is good to use

-Overall Tor performance is good. The problem there is not really absolute anonymity but just passing through the internet blockage set up by the regime. So an intricate circuit of tunnels all encrypted and secured separately is just too much of an overhead for an internet that is already slow over there to begin with.

- 304,958 people risk to be on Parazit's FaceBook page and I am one of them!

thanks

Andrew Lewman wrote:
> On Wed, 23 Feb 2011 16:12:06 -0500
> Kyle Noori < (b) (6) wrote:
>
>> -Another way flooding Iran with
>> Tor knowledge and software is PNN prazit page on FaceBook
>> "Facebook recorded more than 20 million impressions on Parazit's page"
>> show has 304,958 fans
>> If you would like, I can post the manual and do translation into
>> Farsi as well.
>>
>
> That would be great. However, I'm concerned that the Iranian
> authorities are also watching facebook. Anyone that friends or joins
> that group is going to be put onto a list, their family members in
> country watched, and should they travel home, questioned at the border
> about their facebook activities.
>
>
>> An interesting feedback from a friend:
>> {
>> OK I just installed the 0.2.2.22-alpha and it worked fine. Still very
>> slow but the time it took to finish and establish a
>> circuit was much better. Interestingly
>> it connects more quickly without the bridge than
>> it does with the bridge I have set up in the U.S.
>>
>
> The -alpha series right now has a ton of performance fixes. The longer
> you leave it running, the faster it should get, to a point. As for the
> bridge vs. non-bridge, if the bridge is slow, then everything is going
> to be slow. Tor is only as fast as the slowest link between two
> relays.
>
>
>> I read the articles and the analysis based on the volume
>> of traffic. It could very well be due to the blocking of IP's of the
>> directory servers or a sheer drop in speed inside Iran (it happens

>> sometimes).
>>
>
> Yes, this is part of it. One of the ISPs in country was definitely
> doing protocol analysis and filtering. We have data that shows this is
> the case for tor. We heard that this is also true for ultrasurf,
> freegate, vpns based on pptp or ipsec, and some popular https proxies.
> Interestingly, using the SOCKS5 options to point tor at a socks proxy
> works well to bypass the filtering. It seems iran's filter at that ISP
> was only "SSL or not?" and if not ssl, it was sent to the normal IP
> block lists.
>
>
>> I think a more conclusive way of
>> finding out if they are indeed looking inside packets for specific
>> patterns (regardless of the port) is to set up a two way link between
>> Iran and US and run packet sniffers on both sides.
>>
>
> Yes, this will work. If you can run a bridge/relay and record the
> traffic from Iran, and have someone inside record their traffc, you can
> correlate the flows and censorship. If you want help analyzing the
> packets, let me know. Remember that this data is like asking
> someone for their DNA. It will give them away and let you see
> everything about their local machine and network as well.
>
> Attached are two traffic flows from somewhere in Iran to somewhere
> outside of Iran. What's different about the https flows vs. the ip
> blocking flows is that there is an added hop for anything that looked
> like ssl. It was there every time, and added between 40-500 ms of
> latency depending upon which ssl-like protocol (tor, freegate, vpns)
> was fired across the network. Iran's real-time protocol analysis is
> more sophisticated than more corporate firewalls at this point. This
> should scare the heck out of anyone.
>
>

From: Andrew Lewman
To: Kyle Noori
Cc: Ken Berman; Kelly DeYoe; Sho Ho; Roger Dingledine
Subject: Re: idea
Date: Wednesday, February 23, 2011 10:50:21 PM
Attachments: https-traffic-flow.txt
ip-blocking.txt

On Wed, 23 Feb 2011 16:12:06 -0500
Kyle Noori <[redacted] (b)(6)> wrote:
> -Another way flooding Iran with
> Tor knowledge and software is PNN prazit page on FaceBook
> "Facebook recorded more than 20 million impressions on Parazit's page"
> show has 304,958 fans
> If you would like, I can post the manual and do translation into
> Farsi as well.

That would be great. However, I'm concerned that the Iranian authorities are also watching facebook. Anyone that friends or joins that group is going to be put onto a list, their family members in country watched, and should they travel home, questioned at the border about their facebook activities.

> An interesting feedback from a friend:
> {
> OK I just installed the 0.2.2.22-alpha and it worked fine. Still very
> slow but the time it took to finish and establish a
> circuit was much better. Interestingly
> it connects more quickly without the bridge than
> it does with the bridge I have set up in the U.S.

The -alpha series right now has a ton of performance fixes. The longer you leave it running, the faster it should get, to a point. As for the bridge vs. non-bridge, if the bridge is slow, then everything is going to be slow. Tor is only as fast as the slowest link between two relays.

> I read the articles and the analysis based on the volume
> of traffic. It could very well be due to the blocking of IP's of the
> directory servers or a sheer drop in speed inside Iran (it happens
> sometimes).

Yes, this is part of it. One of the ISPs in country was definitely doing protocol analysis and filtering. We have data that shows this is the case for tor. We heard that this is also true for ultrasurf, freegate, vpns based on pptp or ipsec, and some popular https proxies. Interestingly, using the SOCKS5 options to point tor at a socks proxy works well to bypass the filtering. It seems iran's filter at that ISP was only "SSL or not?" and if not ssl, it was sent to the normal IP block lists.

> I think a more conclusive way of
> finding out if they are indeed looking inside packets for specific
> patterns (regardless of the port) is to set up a two way link between
> Iran and US and run packet sniffers on both sides.

Yes, this will work. If you can run a bridge/relay and record the traffic from Iran, and have someone inside record their traffc, you can correlate the flows and censorship. If you want help analyzing the

packets, let me know. Remember that this data is like asking someone for their DNA. It will give them away and let you see everything about their local machine and network as well.

Attached are two traffic flows from somewhere in Iran to somewhere outside of Iran. What's different about the https flows vs. the ip blocking flows is that there is an added hop for anything that looked like ssl. It was there every time, and added between 40-500 ms of latency depending upon which ssl-like protocol (tor, freegate, vpns) was fired across the network. Iran's real-time protocol analysis is more sophisticated than more corporate firewalls at this point. This should scare the heck out of anyone.

--
Andrew
pgp 0x74ED336B

From: Andrew Lewman
To: Kyle Noori
Cc: Ken Berman; Kelly DeYoe; Sho Ho; Roger Dingledine
Subject: Re: idea
Date: Wednesday, February 23, 2011 5:40:28 PM

You guys should talk to Sina, he can fill you in on the details. For fear of violating US Laws, Tor can only do so much, or only say so much over unencrypted email to a govt agency ;)

Now if we had an ITAR/Export license.....

On Wed, Feb 23, 2011 at 04:12:06PM -0500, [redacted] wrote 3.1K bytes in 83 lines about:
: Good information Andrew
:
: -Another way flooding Iran with
: Tor knowledge and software is PNN prazit page on FaceBook
: "Facebook recorded more than 20 million impressions on Parazit's page"
: show has 304,958 fans
: If you would like, I can post the manual and do translation into
: Farsi as well.
:
: An interesting feedback from a friend:
: {
: OK I just installed the 0.2.2.22-alpha and it worked fine. Still very slow
: but the time it took to finish and establish a
: circuit was much better. Interestingly
: it connects more quickly without the bridge than
: it does with the bridge I have set up in the U.S.
:
: I read the articles and the analysis based on the volume
: of traffic. It could very well be due to the blocking of IP's of the
: directory servers or a sheer drop in speed inside Iran (it happens
: sometimes).
:
: I think a more conclusive way of
: finding out if they are indeed looking inside packets for specific
: patterns (regardless of the port) is to set up a two way link
: between Iran and US and run packet sniffers on both sides.
:
: I will see what I can do on that.
:
: Thanks for the help.
:
: Cheers,
: }
:
: I will work with him on packet sniffer thing, if we come up with
: some info I will update you all
:
: Thanks
: K Noori
:
: Andrew Lewman wrote:
: >On Tue, 22 Feb 2011 11:42:36 -0500
: >Ken Berman <[redacted] wrote:
: >>[Comment : during last week street demonstration, Tor connection
: >>was blocked]//

: >
: >The -stable version of tor was probably blocked, but the -alpha version
: >of tor was flooded into the country and was working well.
: >
: >Iran is doing a few things to block various tools, see
: >https://blog.torproject.org/blog/update-internet-censorship-iran for
: >the general overview. Specifically, Iran has some sophisticated
: >technology that could identify various ssl fingerprints; tor vs.
: >ultrasurf/freegate vs. vpns vs. normal https. We changed our ssl
: >fingerprint in 0.2.2.22-alpha to look more like normal https traffic on
: >the wire. See https://blog.torproject.org/blog/tor-02222-alpha-out,
: >specifically, "Adjust our TLS Diffie-Hellman parameters to match those
: >used by Apache's mod_ssl."
: >
: >It seems Iran has gotten tired of the game of "whack a mole" with IP
: >addresses, and is now able to identify and selectively block protocols
: >on the wire. This is a new step in the arms race, and frankly Iran has
: >leap-frogged ahead of any other country and nearly all commercial
: >companies to which we've spoken. From an engineering perspective, the
: >fact that Iran can do this in real-time wth 17 million people is
: >impressive. It's also depressing to realize that either Iran's IT
: >staff is vastly smarter than they were even a few months ago, or they
: >are getting help from abroad.
: >
: >Running 0.2.2.22-alpha bridges on random ports is a fine solution.
: >I've been running two on my personal machines and seeing Iran as the
: >primary country connecting to them.
: >
: >We are working with an organization who is flooding the country with
: >tor knowledge and software. They are very, very happy as to how it has
: >all worked so far. I've asked them if I can introduce you to each
: >other. I'll let you know either way.
: >
: >Thanks for the email.
: >

--
Andrew
pgp key: 0x74ED336B

From: Kyle Noori
To: Andrew Lewman
Cc: Ken Berman; Kelly DeYoe; Sho Ho; Roger Dingledine
Subject: Re: idea
Date: Wednesday, February 23, 2011 4:12:06 PM

Good information Andrew

-Another way flooding Iran with
Tor knowledge and software is PNN prazit page on FaceBook
"Facebook recorded more than 20 million impressions on Parazit's page"
show has 304,958 fans
If you would like, I can post the manual and do translation into Farsi
as well.

An interesting feedback from a friend:
{
OK I just installed the 0.2.2.22-alpha and it worked fine. Still very slow
but the time it took to finish and establish a
circuit was much better. Interestingly
it connects more quickly without the bridge than
it does with the bridge I have set up in the U.S.

I read the articles and the analysis based on the volume
of traffic. It could very well be due to the blocking of IP's of the
directory servers or a sheer drop in speed inside Iran (it happens
sometimes).

I think a more conclusive way of
finding out if they are indeed looking inside packets for specific
patterns (regardless of the port) is to set up a two way link between
Iran and US and run packet sniffers on both sides.

I will see what I can do on that.

Thanks for the help.

Cheers,
}

I will work with him on packet sniffer thing, if we come up with some
info I will update you all

Thanks
K Noori

Andrew Lewman wrote:
> On Tue, 22 Feb 2011 11:42:36 -0500
> Ken Berman <[redacted] wrote:
>
>> [Comment : during last week street demonstration, Tor connection was
>> blocked]//
>>
>
> The -stable version of tor was probably blocked, but the -alpha version
> of tor was flooded into the country and was working well.
>
> Iran is doing a few things to block various tools, see

> https://blog.torproject.org/blog/update-internet-censorship-iran for
> the general overview. Specifically, Iran has some sophisticated
> technology that could identify various ssl fingerprints; tor vs.
> ultrasurf/freegate vs. vpns vs. normal https. We changed our ssl
> fingerprint in 0.2.2.22-alpha to look more like normal https traffic on
> the wire. See https://blog.torproject.org/blog/tor-02222-alpha-out,
> specifically, "Adjust our TLS Diffie-Hellman parameters to match those
> used by Apache's mod_ssl."
>
> It seems Iran has gotten tired of the game of "whack a mole" with IP
> addresses, and is now able to identify and selectively block protocols
> on the wire. This is a new step in the arms race, and frankly Iran has
> leap-frogged ahead of any other country and nearly all commercial
> companies to which we've spoken. From an engineering perspective, the
> fact that Iran can do this in real-time wth 17 million people is
> impressive. It's also depressing to realize that either Iran's IT
> staff is vastly smarter than they were even a few months ago, or they
> are getting help from abroad.
>
> Running 0.2.2.22-alpha bridges on random ports is a fine solution.
> I've been running two on my personal machines and seeing Iran as the
> primary country connecting to them.
>
> We are working with an organization who is flooding the country with
> tor knowledge and software. They are very, very happy as to how it has
> all worked so far. I've asked them if I can introduce you to each
> other. I'll let you know either way.
>
> Thanks for the email.
>
>

From: Andrew Lewman
To: Ken Berman
Cc: Kyle Noori; Kelly.DeYoe; Sho Ho; Roger Dingledine
Subject: Re: idea
Date: Tuesday, February 22, 2011 12:05:22 PM

On Tue, 22 Feb 2011 11:42:36 -0500
Ken Berman <[redacted] (b) (6)> wrote:
> [Comment : during last week street demonstration, Tor connection was
> blocked]//

The -stable version of tor was probably blocked, but the -alpha version of tor was flooded into the country and was working well.

Iran is doing a few things to block various tools, see https://blog.torproject.org/blog/update-internet-censorship-iran for the general overview. Specifically, Iran has some sophisticated technology that could identify various ssl fingerprints; tor vs. ultrasurf/freegate vs. vpns vs. normal https. We changed our ssl fingerprint in 0.2.2.22-alpha to look more like normal https traffic on the wire. See https://blog.torproject.org/blog/tor-02222-alpha-out, specifically, "Adjust our TLS Diffie-Hellman parameters to match those used by Apache's mod_ssl."

It seems Iran has gotten tired of the game of "whack a mole" with IP addresses, and is now able to identify and selectively block protocols on the wire. This is a new step in the arms race, and frankly Iran has leap-frogged ahead of any other country and nearly all commercial companies to which we've spoken. From an engineering perspective, the fact that Iran can do this in real-time wth 17 million people is impressive. It's also depressing to realize that either Iran's IT staff is vastly smarter than they were even a few months ago, or they are getting help from abroad.

Running 0.2.2.22-alpha bridges on random ports is a fine solution. I've been running two on my personal machines and seeing Iran as the primary country connecting to them.

We are working with an organization who is flooding the country with tor knowledge and software. They are very, very happy as to how it has all worked so far. I've asked them if I can introduce you to each other. I'll let you know either way.

Thanks for the email.

--
Andrew
pgp 0x74ED336B

From: Ken Berman
To: Andrew Lewman; Kyle Noori
Cc: Kelly DeYoe; Sho Ho; Roger Dingledine
Subject: RE: idea
Date: Thursday, February 24, 2011 7:36:26 AM

We're reaching out to the mysterious SiNa.....

-----Original Message-----
From: Andrew Lewman [mailto:[redacted (b) (6)]
Sent: Wednesday, February 23, 2011 5:40 PM
To: Kyle Noori
Cc: Ken Berman; Kelly DeYoe; Sho Ho; Roger Dingledine
Subject: Re: idea

You guys should talk to Sina, he can fill you in on the details. For
fear of violating US Laws, Tor can only do so much, or only say so much
over unencrypted email to a govt agency ;)

Now if we had an ITAR/Export license.....

On Wed, Feb 23, 2011 at 04:12:06PM -0500, [redacted (b) (6)] wrote 3.1K bytes in 83 lines about:
: Good information Andrew
:
: -Another way flooding Iran with
: Tor knowledge and software is PNN prazit page on FaceBook
: "Facebook recorded more than 20 million impressions on Parazit's page"
: show has 304,958 fans
: If you would like, I can post the manual and do translation into
: Farsi as well.
:
: An interesting feedback from a friend:
: {
: OK I just installed the 0.2.2.22-alpha and it worked fine. Still very slow
: but the time it took to finish and establish a
: circuit was much better. Interestingly
: it connects more quickly without the bridge than
: it does with the bridge I have set up in the U.S.
:
: I read the articles and the analysis based on the volume
: of traffic. It could very well be due to the blocking of IP's of the
: directory servers or a sheer drop in speed inside Iran (it happens
: sometimes).
:
: I think a more conclusive way of
: finding out if they are indeed looking inside packets for specific
: patterns (regardless of the port) is to set up a two way link
: between Iran and US and run packet sniffers on both sides.
:
: I will see what I can do on that.
:
: Thanks for the help.
:
: Cheers,
: }
:
: I will work with him on packet sniffer thing, if we come up with
: some info I will update you all

:
: Thanks
: K Noori
:
: Andrew Lewman wrote:
: >On Tue, 22 Feb 2011 11:42:36 -0500
: >Ken Berman <[redacted] (b) (6)> wrote:
: >>[Comment : during last week street demonstration, Tor connection
: >>was blocked]//
: >
: >The -stable version of tor was probably blocked, but the -alpha version
: >of tor was flooded into the country and was working well.
: >
: >Iran is doing a few things to block various tools, see
: >https://blog.torproject.org/blog/update-internet-censorship-iran for
: >the general overview. Specifically, Iran has some sophisticated
: >technology that could identify various ssl fingerprints; tor vs.
: >ultrasurf/freegate vs. vpns vs. normal https. We changed our ssl
: >fingerprint in 0.2.2.22-alpha to look more like normal https traffic on
: >the wire. See https://blog.torproject.org/blog/tor-02222-alpha-out,
: >specifically, "Adjust our TLS Diffie-Hellman parameters to match those
: >used by Apache's mod_ssl."
: >
: >It seems Iran has gotten tired of the game of "whack a mole" with IP
: >addresses, and is now able to identify and selectively block protocols
: >on the wire. This is a new step in the arms race, and frankly Iran has
: >leap-frogged ahead of any other country and nearly all commercial
: >companies to which we've spoken. From an engineering perspective, the
: >fact that Iran can do this in real-time wth 17 million people is
: >impressive. It's also depressing to realize that either Iran's IT
: >staff is vastly smarter than they were even a few months ago, or they
: >are getting help from abroad.
: >
: >Running 0.2.2.22-alpha bridges on random ports is a fine solution.
: >I've been running two on my personal machines and seeing Iran as the
: >primary country connecting to them.
: >
: >We are working with an organization who is flooding the country with
: >tor knowledge and software. They are very, very happy as to how it has
: >all worked so far. I've asked them if I can introduce you to each
: >other. I'll let you know either way.
: >
: >Thanks for the email.
: >

--
Andrew
pgp key: 0x74ED336B

From: Andrew Lewman
To: Kyle Noori
Cc: Ken Berman; Kelly DeYoe; Sho Ho; Roger Dingledine
Subject: Re: idea
Date: Thursday, February 24, 2011 4:39:51 PM

On Thu, Feb 24, 2011 at 02:42:15PM -0500, [redacted] (b) (6) wrote 3.7K bytes in 88 lines about:
: -As for Packet sniffers, WireShark program is what I think it is good to use

Yes, wireshark or tcpdump are fine packet captures.

: -Overall Tor performance is good. The problem there is not really
: absolute anonymity but just passing through the internet blockage
: set up by the regime. So an intricate circuit of tunnels all
: encrypted and secured separately is just too much of an overhead for
: an internet that is already slow over there to begin with.

The risk of not using Tor means your source and destination can be discovered trivially. The process is called website fingerprinting. When watching the network, facebook.com traffic looks different than twitter.com, which looks different than ministry.ir. While we haven't seen Iran do this yet, we have seen Iran govt run http, https, and socks proxies to record all traffic going through them.

: - 304,958 people risk to be on Parazit's FaceBook page and I am one
: of them!

Yes. Given the govt's capabilities, they can record all of those members and wait for them to cross a border. Conversely, so can the USA and EU govts. They can put people on watch lists for being in the same social circle as suspicious Iranians.

Isn't security fun?

--
Andrew
pgp key: 0x74ED336B

From: Roger Dingledine
To: Eric Johnson
Cc: Andrew Lewman [redacted] Chris Walker; Ken Berman; Kelly DeYoe
Subject: Re: IFree sub paperwork, round 1
Date: Thursday, August 28, 2008 7:25:52 PM

[In the grand tradition of expanding cc lists until they contain every organization being discussed, I am adding Ken and Kelly to the cc list here so they can keep in the loop.]

On Wed, Aug 27, 2008 at 01:35:17AM -0700, Eric Johnson wrote:
> Hi Roger,
>
> > Speaking of which, is it ok to talk to Ken Berman and the rest of the
> > BBG gang about this? I assume they know or will know soon enough, but
> > I figure you'll appreciate that we're using the caution you asked for.
>
> :-) Thanks.
> I've been in touch with Ken since well before the DRL RFA came
>out, and he was on the DRL review committee, and I let him know last week
>that the grant was cut, so he's "au courant." So, okay to talk with him.

Great.

> > (We need to coordinate with them to see if they plan to have room in
> > their budget for us next year, and to make sure that both sides are ok
> > with two different funding groups caring about Tor and circumvention.)
>
> Yes. Well, we're definitely "okay" with it, and I think he is too--Ken
>and I met to talk about that in early July. I think both we and BBG
>would be very happy to see a sort of "Tor master plan," if there is one,
>i.e. what the "strategy" is for Tor development, what the priorities are,
>how "our" circumvention-skewed resources contribute to that strategy,

Tor's overall goals are, roughly speaking,
- Develop and deploy free-software tools that promote free speech, free expression, civic engagement, and privacy rights online;
- Do research to figure out how the above tools should actually work;
- Educate the whole world about why they need the above issues solved and how to go about solving them.

Our usual funding model is that we have a huge pile of development and research tasks we'd like to do, and whoever comes along with funding gets to direct our priorities. We want to do all of them, they all need to get done, and we're not really picky about the order of tackling them.

Now, some of the research and development items *do* have dependencies. As we talked earlier, if you focus only on speed, you won't get safe or happy Tor users. And if you focus only on circumvention features, then you won't end up with a network that can handle the load from the new users, or a tool that circumventing users consider usable.

That's why, even for projects like BBG and iFree, some of the work goes to making sure the core parts of Tor can keep up with the new features. Fortunately, in practice both groups have been very understanding that in fact you need to move core R&D issues along at the same time you focus on the new features you want.

So to answer your "circumvention-skewed resources" question: Tor needs to make sure that new projects have a good balance of circumvention-specific and more-Tor-in-general work; and the funders need to keep being ok with funding both halves of the picture. If we both keep these in mind, I think we'll all be happy at the end.

>whether there are opportunities to do more, and whether/how those
>opportunities are being exploited. (Or are "our" resources already maxing
>out what can be done to improve Tor for circumvention?)

Well, assuming we can also look forward to another round of funding from BBG, we're planning to ramp up development work quite a bit in 2009 -- we have three great volunteers we've been meaning to turn into full-time developers, and it looks like we're going to finally be able to hire Andrew as our exec dir, meaning I can spend a bit more time on actual development and usability work. (I will have to negotiate with Chris how I balance that time between doing work and keeping him informed of our progress. :)

We haven't finished sorting out the draft 2010 budget yet, but it looks like we'll be ramping up even more then; plus that will be the right time to diversify our funding so we can maintain our momentum into and past 2011.

We've also been keeping an eye out the past year for other groups that want to fund Tor -- we have some basic-research projects with NRL we've been applying for, and Google has been increasingly wanting to give us money since we write good free software and the world needs more of that. These were going to be among our main funding sources if iFree didn't come through, but now we should keep them going "on a light simmer" so they're ready for us in 2011.

So are we pretty close to flat-out growth for circumvention work on Tor in 2009? In terms of the core Tor group and how many developers we can handle at once, yes. But there are still some good ways that we could spend more money.

1) A lot of the hard research questions around scaling and speed are looming as potential bottlenecks in the future, and there are some good university research groups we could fund to help us answer those questions. For example, we've been helping fund one of Ian Goldberg's grad students at the University of Waterloo. He has a deal with the Canadian govt where they match our funding 4x. His current student is working on a design for switching Tor's transport over to UDP. Ian is now looking for another good grad student who can focus on the "make Tor tolerate file-sharing better" question, and if he finds one we plan to help fund him/her.

2) There are many many non-development pieces of Tor that need more attention. These include advocacy for running more relays, documentation and explanations of how and when to use Tor, figuring out recommended configurations for various apps and figuring out which apps in each category to recommend, figuring out how to phrase all this for the media so they understand Tor and describe it well in their articles, making our website more usable and useful, more available in blocked countries, coordinating the community of people running mirrors, sorting out how to deploy USB keys with Tor Browser Bundle on them, doing trainings, etc. I'm hoping that the Internews side of iFree will be able to help a lot with these pieces, including finding and managing the people working

on them. It's on my todo list to provide more details on each idea above, and brainstorm about what else should go on the list. Then we all need to be sure to work together through the process, so both a) things get done and b) the things that get done get done well.

In my ideal world, the 2009 growth will go smoothly and we'll be ready to take on even more core dev work in 2010. I look forward to seeing how that goes in reality.

> Do you sometimes feel Tor's original goal of being a tool for anonymous
>internet access is being undermined or "taken over" by the circumvention
>interest? Or are the circumvention goals identical enough with the
>anonymous-isation goals that everyone's happy?

As long as the people with the circumvention interest continue to recognize that they need to help Tor work on getting faster, more usable, stay secure, etc, then I don't think there's a contradiction. Many of the things you want most out of the iFree project boil down to "make Tor work better". And we want that too.

Now, there are a few areas where circumvention and security/anonymity/privacy can point in different directions. One that keeps surfacing is "why don't you make Tor faster for blocked users by just putting people over one or two hops? Surely they don't need the anonymity given by a full three hops."

Another example is Isaac Mao's Foxyproxy configuration: he has configured his Firefox to only use Tor for 40 or 50 sites, and to use the direct Internet for the rest. So from his perspective the whole Internet now works from inside China -- some sites are slow, but those are the ones that would be entirely gone otherwise. But if you use Foxyproxy in this "whitelist" mode and you want anonymity too, you're at serious risk: any destination website that wants to uncover your location can send you a css or iframe or other web component that causes you to do a non-Tor lookup, and bam you lose.

We've argued that people who want circumvention should also want anonymity, since we've all seen so many cases of users getting busted in surprising ways, and we can see more cases like this on the horizon with current circumvention approaches. And one of Tor's major "value-adds" in the circumvention space is that we come with good anonymity built-in.

But the flip side of that is: shouldn't we trust the users to know what they want? If they want "make it really fast and screw the security", should we tell them to go use some other option instead, even if they find Tor more convenient and more usable than the other options?

This is complicated by the fact that "anonymity loves company". Tor's anonymity comes in part because its users are behaving in the same way based on the same information. So users that choose two hops rather than three hops may be hurting the other users, because they behave in a way that's distinguishable from the other users, meaning some attackers can focus on a specific target profile and ignore users that don't fit that profile. Do two-hop users actually hurt the anonymity of the three-hop users, or do they simply not help them? These are hard open research questions, and we're reluctant to open that can of worms until we have clearer answers.

So as to whether Tor's original anonymity goal is being undermined or "taken over" by the circumvention interest? No, I think we've got a good

balance right now. But we want to do even better on both sides (after all, a lot of Tor's value comes from being useful to many different communities), and it turns out that involves a lot of work. Good thing we have a full three years of funding. :)

--Roger

From: Ken Berman
To: Roger Dingledine; Dean, Richard
Cc: Kelly DeYoe; Sho Ho
Subject: RE: Introduction for Ken Berman and Drew Dean
Date: Wednesday, July 07, 2010 8:29:21 AM

Thanks, Roger.
Hi, Drew.
Ken

-----Original Message-----
From: Roger Dingledine [mailto:(b) (6)
Sent: Wednesday, July 07, 2010 12:09 AM
To: Ken Berman; Dean, Richard
Cc: (b) (6) (b) (6)
Subject: Introduction for Ken Berman and Drew Dean

Hi Ken, Drew,

Here's an introduction.

Drew is a new DARPA program manager who is launching a new program on circumvention and anonymity. He's going to be funding some groups to research new ideas and mechanisms for safely circumventing firewalls.

Ken works for the International Broadcasting Bureau (you may know the name 'Voice of America' better). He's been funding circumvention designs and thinking about the circumvention side of this problem for close to a decade now.

You two should clearly meet. :)

--Roger

From: Ken Berman
To: Dean, Richard; Roger Dingledine
Cc: Kelly DeYoe; Sho Ho
Subject: RE: Introduction for Ken Berman and Drew Dean
Date: Wednesday, July 28, 2010 10:21:21 AM

Dean - just back from leave. How about next week for a telcon, say Wed, 8/4 at 10:00? Ken

-----Original Message-----
From: Dean, Richard [mailto:[redacted]
Sent: Monday, July 12, 2010 10:24 PM
To: Ken Berman; Roger Dingledine
Cc: [redacted] [redacted]
Subject: Re: Introduction for Ken Berman and Drew Dean

Ken --
Sorry for the delay getting back to you. We should definitely talk, but the next couple weeks are fairly impacted for me. Later next week might be the best shot.

Thanks,
Drew

On 7/7/10 7:29 AM, "Ken Berman" <[redacted] wrote:

Thanks, Roger.
Hi, Drew.
Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Wednesday, July 07, 2010 12:09 AM
To: Ken Berman; Dean, Richard
Cc: [redacted] [redacted]
Subject: Introduction for Ken Berman and Drew Dean

Hi Ken, Drew,

Here's an introduction.

Drew is a new DARPA program manager who is launching a new program on circumvention and anonymity. He's going to be funding some groups to research new ideas and mechanisms for safely circumventing firewalls.

Ken works for the International Broadcasting Bureau (you may know the name 'Voice of America' better). He's been funding circumvention designs and thinking about the circumvention side of this problem for close to a decade now.

You two should clearly meet. :)

--Roger

From: Dean, Richard
To: Ken Berman; Roger Dingledine
Cc: Kelly DeYoe; Sho Ho
Subject: Re: Introduction for Ken Berman and Drew Dean
Date: Monday, July 12, 2010 11:24:09 PM

Ken --
Sorry for the delay getting back to you. We should definitely talk, but the next couple weeks are fairly impacted for me. Later next week might be the best shot.

Thanks,
Drew

On 7/7/10 7:29 AM, "Ken Berman" <[redacted] wrote:

Thanks, Roger.
Hi, Drew.
Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Wednesday, July 07, 2010 12:09 AM
To: Ken Berman; Dean, Richard
Cc: [redacted] [redacted]
Subject: Introduction for Ken Berman and Drew Dean

Hi Ken, Drew,

Here's an introduction.

Drew is a new DARPA program manager who is launching a new program on circumvention and anonymity. He's going to be funding some groups to research new ideas and mechanisms for safely circumventing firewalls.

Ken works for the International Broadcasting Bureau (you may know the name 'Voice of America' better). He's been funding circumvention designs and thinking about the circumvention side of this problem for close to a decade now.

You two should clearly meet. :)

--Roger

From: Ken Berman
To: Adam Fisk; Andrew Lewman
Cc: Kelly DeYoe; Sho Ho; Kyle Noori
Subject: RE: Introduction to Lantern and BBG
Date: Monday, February 07, 2011 9:00:29 AM
Attachments: Directions.doc

Adam - looking forward to it! Let's make it the 16th, that way we can meet with you and Chris.

Mind coming to our building (directions attached). 10:00 OK?

Ken

-----Original Message-----
From: Adam Fisk [mailto:[redacted (b) (6)]
Sent: Sunday, February 06, 2011 2:08 PM
To: Andrew Lewman
Cc: Ken Berman; Kelly DeYoe
Subject: Re: Introduction to Lantern and BBG

Thanks a million, Andrew, and it's a pleasure to meet you Ken and Kelly. I'll be in DC from Feb 9-Feb 16. Would either of you have a chance to meet? Chris Holmes, a director at OpenPlans who I'm working closely with, is available on the 16th if you're free then, but otherwise I'd love to touch base on my own.

I'm at [redacted (b) (6)] and please feel free to reach out any time.
Thanks again, Andrew, and hopefully I'll see you guys in person soon.

-Adam

On Sat, Feb 5, 2011 at 5:39 AM, Andrew Lewman <[redacted (b) (6)] wrote:
> Hello Ken, Kelly and Adam,
>
> Please consider this a virtual introduction to each other. Ken and
> Kelly, Adam is working on a xmpp/gchat/google-based tool called Lantern.
> I believe you've heard of it.
>
> And Adam, Ken and Kelly have been great to work with over the years.
> They are technical, understand the issues, and don't jump on
> bandwagons.
>
> Consider yourselves introduced. Good luck!
>
> --
> Andrew
> pgp 0x74ED336B
>

--
Adam Fisk
http://www.littleshoot.org | http://adamfisk.wordpress.com |
http://twitter.com/adamfisk

From: Adam Fisk
To: Andrew Lewman
Cc: Ken Berman; Kelly DeYoe
Subject: Re: Introduction to Lantern and BBG
Date: Sunday, February 06, 2011 2:07:36 PM

Thanks a million, Andrew, and it's a pleasure to meet you Ken and Kelly. I'll be in DC from Feb 9-Feb 16. Would either of you have a chance to meet? Chris Holmes, a director at OpenPlans who I'm working closely with, is available on the 16th if you're free then, but otherwise I'd love to touch base on my own.

I'm at [redacted] and please feel free to reach out any time. Thanks again, Andrew, and hopefully I'll see you guys in person soon.

-Adam

On Sat, Feb 5, 2011 at 5:39 AM, Andrew Lewman <[redacted] wrote:
> Hello Ken, Kelly and Adam,
>
> Please consider this a virtual introduction to each other. Ken and
> Kelly, Adam is working on a xmpp/gchat/google-based tool called Lantern.
> I believe you've heard of it.
>
> And Adam, Ken and Kelly have been great to work with over the years.
> They are technical, understand the issues, and don't jump on
> bandwagons.
>
> Consider yourselves introduced. Good luck!
>
> --
> Andrew
> pgp 0x74ED336B
>

--
Adam Fisk
http://www.littleshoot.org | http://adamfisk.wordpress.com |
http://twitter.com/adamfisk

From: Ken Berman
To: Andrew Lewman; sina; Kelly DeYoe
Subject: RE: Introductions
Date: Tuesday, February 22, 2011 4:16:02 PM

Thanks, Andrew!

-----Original Message-----
From: Andrew Lewman [mailto:[redacted (b) (6)]
Sent: Tuesday, February 22, 2011 2:57 PM
To: sina; Ken Berman; Kelly DeYoe
Subject: Introductions

Hello Ken, Kelly, and Sina,

Please consider this your introduction to one another.

Sina, Ken and Kelly help run bbg.gov, which also covers Voice of America and Radio Farda among other things. They have been fans of Tor for a while and great sponsors.

Ken and Kelly, Sina is part of Ninja Hosting which has had great success in using a mix of Tor, trainings, and outreach to help Iranian citizens bypass the great potato wall.

I will let you two converse from here. Good luck.

--
Andrew
pgp 0x74ED336B

From: Ken Berman
To: Andrew Lewman; Kim Pham
Cc: sina; Kelly DeYoe; Jill Moss
Subject: RE: Introductions
Date: Monday, September 19, 2011 10:26:13 AM

Thanks, Andrew.

Sina and Kim - are either of you in the DC area and, if so, care to come by for a chat. Meet the tech folks here as well as our PNN staffers?

Ken

-----Original Message-----
From: Andrew Lewman [mailto:[redacted (b) (6)]
Sent: Thursday, September 15, 2011 4:35 PM
To: Ken Berman; Kim Pham
Cc: sina; Kelly DeYoe
Subject: Re: Introductions

Hello Ken, Kelly, Sina, and Kim,

Did you four ever have a chance to talk more? It seems now that PNN has turned the great 'Eye of Sauron' in the Iranian government on Tor, you four should talk more.

See, https://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fix

Our blog is currently hammered with traffic and attacks right now, so it might be slow.

On Tuesday, February 22, 2011 16:16:02 Ken Berman wrote:
> Thanks, Andrew!
>
> -----Original Message-----
> From: Andrew Lewman [mailto:[redacted (b) (6)]
> Sent: Tuesday, February 22, 2011 2:57 PM
> To: sina; Ken Berman; Kelly DeYoe
> Subject: Introductions
>
> Hello Ken, Kelly, and Sina,
>
> Please consider this your introduction to one another.
>
> Sina, Ken and Kelly help run bbg.gov, which also covers Voice of
> America and Radio Farda among other things. They have been fans of Tor
> for a while and great sponsors.
>
> Ken and Kelly, Sina is part of Ninja Hosting which has had great
> success in using a mix of Tor, trainings, and outreach to help Iranian
> citizens bypass the great potato wall.
>
> I will let you two converse from here. Good luck.

--
Andrew
pgp 0x74ED336B

From: Andrew Lewman
To: Ken Berman; Kim Pham
Cc: sina; Kelly DeYoe
Subject: Re: Introductions
Date: Thursday, September 15, 2011 5:34:42 PM

Hello Ken, Kelly, Sina, and Kim,

Did you four ever have a chance to talk more? It seems now that PNN has turned the great 'Eye of Sauron' in the Iranian government on Tor, you four should talk more.

See, https://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fix

Our blog is currently hammered with traffic and attacks right now, so it might be slow.

On Tuesday, February 22, 2011 16:16:02 Ken Berman wrote:
> Thanks, Andrew!
>
> -----Original Message-----
> From: Andrew Lewman [mailto:[redacted (b) (6)]
> Sent: Tuesday, February 22, 2011 2:57 PM
> To: sina; Ken Berman; Kelly DeYoe
> Subject: Introductions
>
> Hello Ken, Kelly, and Sina,
>
> Please consider this your introduction to one another.
>
> Sina, Ken and Kelly help run bbg.gov, which also covers Voice of
> America and Radio Farda among other things. They have been fans of Tor
> for a while and great sponsors.
>
> Ken and Kelly, Sina is part of Ninja Hosting which has had great
> success in using a mix of Tor, trainings, and outreach to help Iranian
> citizens bypass the great potato wall.
>
> I will let you two converse from here. Good luck.

--
Andrew
pgp 0x74ED336B

From: Andrew Lewman
To: Kelly DeYoe
Cc: Ken Berman
Subject: Re: Invitation to attend Hill briefing on BBG Internet Anti-Censorship program
Date: Friday, July 01, 2011 4:40:40 PM

On Fri, Jul 01, 2011 at 03:27:33PM -0400, [redacted] wrote 0.7K bytes in 15 lines about:
: Details are still being worked out, and we will provide additional
: information once things start to come together, but would appreciate
: a response as to whether you'll be able to attend as soon as
: possible.

Thanks for the invite. I can attend. Please let me know what I should prepare, if anything. Can I also invite Karen and/or Roger to come with me?

--
Andrew
pgp key: 0x74ED336B

From:	Andrew Lewman
To:	Kelly DeYoe
Cc:	Ken Berman
Subject:	Re: Invitation to attend Hill briefing on BBG Internet Anti-Censorship program
Date:	Wednesday, July 13, 2011 10:19:50 PM

On Tuesday, July 05, 2011 05:44:58 PM Kelly DeYoe wrote:
> We're still working out the details, and will pass more information
> along as soon as we have things finalized.

Any more details on this? At a minimum, the suggested itinerary? I need to schedule travel.

--
Andrew
pgp 0x74ED336B

From: Ken Berman
To: Andrew Lewman; Kelly DeYoe
Subject: RE: Invitation to attend Hill briefing on BBG Internet Anti-Censorship program
Date: Thursday, July 14, 2011 3:47:16 PM

Info coming today, pls stand by...

-----Original Message-----
From: Andrew Lewman [mailto:[redacted (b) (6)]
Sent: Wednesday, July 13, 2011 9:20 PM
To: Kelly DeYoe
Cc: Ken Berman
Subject: Re: Invitation to attend Hill briefing on BBG Internet Anti-Censorship program

On Tuesday, July 05, 2011 05:44:58 PM Kelly DeYoe wrote:
> We're still working out the details, and will pass more information
> along as soon as we have things finalized.

Any more details on this? At a minimum, the suggested itinerary? I need to schedule travel.

--
Andrew
pgp 0x74ED336B