From: Roger Dingledine
To: Kelly DeYoe
Subject: Re: Statement of Work draft
Date: Sunday, February 19, 2006 2:17:49 AM

On Fri, Feb 17, 2006 at 04:25:59PM -0500, Kelly DeYoe wrote:
> Roger, I've attached our proposed Statement of Work for a contract with
> you in rich text format. Please let me know if this is acceptable, and
> if you have any questions. (Or if you have problems reading it, let me
> know another document format that might work better!)

Great. It looks like we're both on the same page overall.

Who is the AR/CO -- is that you I guess?

We're not going to reach the 2 million user mark by the end of September, with our current resources. Should we perhaps say 'eventual goal', or pick an intermediate number?

The "FreeBSD documentation license" looks bad because it defines source as "the SGML docbook format". We don't ever plan to go near docbook. Probably it is best to just put all our docs under the BSD license too? But that's not an "open source documentation license", so maybe it's simplest to combine C.4.2 into C.4.1 and say "software and documentation"?

Lastly, if there's a chance that we might be able to get a second developer for the 12 month extension, would we do up a different contract then, or should the answer to the last question be "120k or 240k for 1 or 2 people"? I'm just thinking to save time down the road. But I guess there are only so many chickens we want to be counting at this point. :)

I also notice what you sent me was only Section C of the contract. Should I take a look at the other parts in parallel with the next step of paperwork, in case there are standard clauses like crazy intellectual property issues?

> Before I can get the ball rolling to get a contract awarded to you, I
> also need the name of the legal entity we'll be contracting with. I
> believe you provided a company name before, but I cannot find the email.

Moria Research Labs
1558 Massachusetts Ave #24
Cambridge, MA 02138

> Also, I need to know, has this legal entity done business with any
> other civilian agency of the Federal government before? (If yes, the
> time it will take to award the contract may be less.)

I believe the answer is no. We had a subcontract with ITT.com, and then a subcontract with Smartronix.com, when we were getting NRL money. But I think those were government contractors and not the government itself so it wouldn't count.

Thanks!
--Roger

From: Roger Dingledine
To: Kelly DeYoe
Subject: Re: Statement of Work draft
Date: Friday, February 24, 2006 2:43:07 AM

On Wed, Feb 22, 2006 at 11:07:39AM -0500, Kelly DeYoe wrote:
> >We're not going to reach the 2 million user mark by the end of September,
> >with our current resources. Should we perhaps say 'eventual goal', or
> >pick an intermediate number?
>
> I thought I'd worded this to indicate, the goal isn't to actually have 2
> million users, but just to have the network scalable to support up to 2
> million users.

Ok.

> >The "FreeBSD documentation license" looks bad because it defines source
> >as "the SGML docbook format". We don't ever plan to go near docbook.
> >Probably it is best to just put all our docs under the BSD license too?
> >But that's not an "open source documentation license", so maybe it's
> >simplest to combine C.4.2 into C.4.1 and say "software and documentation"?
>
> Ok, I'll combine and change those clauses so that everything is just
> covered by the BSD License.

Ok.

> >Lastly, if there's a chance that we might be able to get a second
> >developer for the 12 month extension, would we do up a different contract
> >then, or should the answer to the last question be "120k or 240k for 1
> >or 2 people"? I'm just thinking to save time down the road. But I guess
> >there are only so many chickens we want to be counting at this point. :)
>
> Modifying the contract to add additional resources is always possible
> down the road. The main reason for adding the option year is just to
> simplify continuing the status quo of the contract if we don't have
> additional resources or scope changes.

Sounds good.

> >I also notice what you sent me was only Section C of the contract. Should
> >I take a look at the other parts in parallel with the next step of
> >paperwork, in case there are standard clauses like crazy intellectual
> >property issues?
>
> Section C is the technical requirements and statement of work, and is
> pretty much the only negotiable section of the contract. The
> Contracting Officer will of course send you the full and complete
> contract for your acceptance, almost all of which besides Section C is
> boilerplate and written to comply with the requirements of Federal law.
> You should of course review it, but there won't be much you will be
> able to change easily, if you have any questions, you should speak to
> the Contracting Officer at that point.

Ok.

> Ok, we'll see what this does to the process, you may have to jump
> through some other hoops to satisfy various requirements for doing

> business with the Federal government.

Sounds good. When the time comes hopefully we'll know somebody who can help me with the hoops.

Thanks,
--Roger

From:	Roger Dingledine
To:	Shava Nerad
Cc:	Kelly DeYoe
Subject:	Re: statement of work, revised
Date:	Tuesday, March 20, 2007 2:03:46 AM
Attachments:	ibb2.tex mrl-ibb2.pdf

On Mon, Mar 19, 2007 at 11:29:32AM -0400, Shava Nerad wrote:
> Great! Roger, do you have a template from last year that I can use,
> or Kelly do you have a preferred format?

Attached are the tex and pdf for one of my invoices.

Somehow I don't think you'll want to use LaTeX for yours,
but that's why there's a pdf too. :)

--Roger

From:	Roger Dingledine
To:	Shava Nerad
Cc:	Shava Nerad; Kelly DeYoe; Ken Berman
Subject:	Re: statement of work, revised
Date:	Monday, March 19, 2007 5:26:43 AM

On Mon, Mar 19, 2007 at 03:53:33AM -0400, Shava Nerad wrote:
> At 03:36 AM 3/19/2007, Roger Dingledine wrote:
> >On Mon, Mar 19, 2007 at 03:25:31AM -0400, Shava Nerad wrote:
> >> Here 'tis.

Looks great. I look forward to continuing to work on the
blocking-resistance stuff with an actual contract. :)

Thanks,
--Roger

From: Shava Nerad
To: Roger Dingledine; Shava Nerad
Cc: Kelly DeYoe; Ken Berman
Subject: Re: statement of work, revised
Date: Monday, March 19, 2007 4:53:33 AM
Attachments: Statement of work Mar 16 2007.pdf

At 03:36 AM 3/19/2007, Roger Dingledine wrote:
>On Mon, Mar 19, 2007 at 03:25:31AM -0400, Shava Nerad wrote:
> > Here 'tis.
>
>It seems there's nothing attached to this mail, btw. :)

Oops.

--
Shava Nerad
[redacted]

From: Roger Dingledine
To: Shava Nerad
Cc: Kelly DeYoe; Ken Berman
Subject: Re: statement of work, revised
Date: Monday, March 19, 2007 4:36:26 AM

On Mon, Mar 19, 2007 at 03:25:31AM -0400, Shava Nerad wrote:
> Here 'tis.

It seems there's nothing attached to this mail, btw. :)

--Roger

From: Shava Nerad
To: Roger Dingledine; Shava Nerad
Cc: Kelly DeYoe
Subject: Re: statement of work, revised
Date: Tuesday, March 20, 2007 2:55:52 AM

At 01:03 AM 3/20/2007, Roger Dingledine wrote:
>On Mon, Mar 19, 2007 at 11:29:32AM -0400, Shava Nerad wrote:
> > Great! Roger, do you have a template from last year that I can use,
> > or Kelly do you have a preferred format?
>
>Attached are the tex and pdf for one of my invoices.
>
>Somehow I don't think you'll want to use LaTeX for yours,
>but that's why there's a pdf too. :)

Captured, drafted on letterhead, and ready for Friday.

Thanks!

--
Shava Nerad
[redacted]

From: Andrew Lewman
To: Kelly DeYoe
Subject: Re: status
Date: Monday, April 09, 2012 5:51:34 PM

On Mon, 9 Apr 2012 21:25:19 +0000
Kelly DeYoe <[redacted]> wrote:

> Well, sending email from an address that doesn't immediately end up
> in my Junk E-Mail folder is probably a good start... (torproject.is
> now instead of torproject.org?) I just happened to be looking there
> for something else and just saw this message now. (We're on
> Microsoft's hosted Exchange service Outlook365 now, so I have even
> less control over my mail than I used to...)

Hmm. I wonder why it was marked as junk. I've been using it for a while now.

> We're still waiting on the finalization of the additional funding,
> but I expect that to be done this week, and Diane will arrange a call
> with the 3 of us to negotiate based on price. The more options you
> have for how to price various parts of the contract and suggestions
> for requirement modifications that would reflect significant cost
> savings are probably the best things you can have ready for that call.

ok

--
Andrew
http://tpo.is/contact
pgp 0x6B4D6475

From: Andrew Lewman
To: Diane Sturgis
Cc: Kelly DeYoe
Subject: Re: Task 5
Date: Monday, June 18, 2012 5:28:36 PM

On Mon, 18 Jun 2012 19:24:34 +0000
Diane Sturgis <_____ wrote:
> Attached is copy of Task Order for your records.

Hello Diane,

Pardon my confusion, does this mean we have the contract and June 18 is the start date?

Also, this is for Tor Solutions Corp, not Tor Project, Inc, was that intentional? Tor Solutions is the for-profit small business, Tor Project, Inc is the non-profit.

I"m about to hop on a 6h flight, so I'll sync up overnight.

Thanks!

--
Andrew
http://tpo.is/contact
pgp 0x6B4D6475

From: Andrew Lewman
To: Diane Sturgis
Cc: Kelly DeYoe
Subject: Re: Task 5
Date: Monday, June 18, 2012 5:28:36 PM

On Mon, 18 Jun 2012 19:24:34 +0000
Diane Sturgis <[redacted (b)(6)] wrote:
> Attached is copy of Task Order for your records.

Hello Diane,

Pardon my confusion, does this mean we have the contract and June 18 is the start date?

Also, this is for Tor Solutions Corp, not Tor Project, Inc, was that intentional? Tor Solutions is the for-profit small business, Tor Project, Inc is the non-profit.

I"m about to hop on a 6h flight, so I'll sync up overnight.

Thanks!

--
Andrew
http://tpo.is/contact
pgp 0x6B4D6475

From: Andrew Lewman
To: Diane Sturgis
Cc: Kelly DeYoe
Subject: Re: Task order #5 - BBG50-Q-12-0015
Date: Monday, March 12, 2012 11:12:14 AM

On Tue, 6 Mar 2012 16:59:18 +0000
Diane Sturgis <[redacted] wrote:
> I will like to set-up meeting with your to discuss your proposal for
> above subject RFQ, dated 23 Feb. Are you available to meet on Friday
> at 2:00 pm, please let me know.

Thanks for taking the time on Friday. As requested, here are our thoughts on bandwidth and increasing capacity. 4-6 relays running at up to 1 gbps each, located in datacenters outside of North America and Europe. This will provide the desired 10% boost to the capacity of the Tor Network and keep it from being concentrated with current exit relays.

--
Andrew
http://tpo.is/contact
pgp 0x6B4D6475

From: Andrew Lewman
To: Diane Sturgis
Cc: Kelly DeYoe
Subject: Re: Task order #5 - BBG50-Q-12-0015
Date: Tuesday, March 06, 2012 12:28:48 PM

On Tue, 6 Mar 2012 16:59:18 +0000
Diane Sturgis <[redacted] (b) (6)> wrote:
> I will like to set-up meeting with your to discuss your proposal for
> above subject RFQ, dated 23 Feb. Are you available to meet on Friday
> at 2:00 pm, please let me know.

Friday at 2 pm sounds good. Thanks.

--
Andrew
http://tpo.is/contact
pgp 0x6B4D6475

From: Andrew Lewman
To: Diane Sturgis
Cc: Kelly DeYoe
Subject: Re: Task order #5 - BBG50-Q-12-0015
Date: Wednesday, March 21, 2012 4:15:45 PM

On Tue, 6 Mar 2012 16:59:18 +0000
Diane Sturgis <_____ wrote:
> I will like to set-up meeting with your to discuss your proposal for
> above subject RFQ, dated 23 Feb. Are you available to meet on Friday
> at 2:00 pm, please let me know.

Hello Diane and Kelly,

Just a quick follow-up note to see about timing on next steps. I believe I'm waiting for BBG to formally request a corrected proposal, correct?

--
Andrew
http://tpo.is/contact
pgp 0x6B4D6475

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe; [redacted]
Subject: RE: Telex at UMI
Date: Monday, December 12, 2011 9:37:38 AM

Thx, just what I feared, another academic "research" project with no commitment to timeline, goals, actual deployment, etc.
Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Friday, December 09, 2011 3:19 PM
To: Ken Berman
Cc: Kelly DeYoe; [redacted]
Subject: Re: Telex at UMI

On Fri, Dec 09, 2011 at 02:58:45PM -0500, Ken Berman wrote:
> Roger - do you have a connection with Haldeman at the University of
>Michigan as regards the Telex project? Any idea where he is on this?

I see Alex several times a year at security conferences, and consider him a friend. Can you give me a hint about which 'this' you mean?

I believe Alex and Ian Goldberg (the other Telex person, also a Tor director) are working on the deployment angle by talking to a) DPI vendors who should donate their hardware to do something good for a change, and b) ISPs that should put said DPI boxes on their network.

At least, that was the status in October. I haven't talked to them about it since.

Also, both Alex and Ian are professors so their main priorities are to publish and to teach their students how to do research.

Actual for-real Telex deployment is going to take a lot of effort beyond what I know they've done so far (first in terms of the logistics above, and second in terms of software usability). In my opinion their best bet for the usability side is to bundle with a popular open-source circumvention tool so a) they don't have to come up with their own user interface and b) so they don't have to "compete" with the more-established tools.

--Roger

From: Roger Dingledine
To: Ken Berman
Cc: Kelly DeYoe; [redacted]
Subject: Re: Telex at UMI
Date: Friday, December 09, 2011 3:18:41 PM

On Fri, Dec 09, 2011 at 02:58:45PM -0500, Ken Berman wrote:
> Roger - do you have a connection with Haldeman at the University of
>Michigan as regards the Telex project? Any idea where he is on this?

I see Alex several times a year at security conferences, and consider him a friend. Can you give me a hint about which 'this' you mean?

I believe Alex and Ian Goldberg (the other Telex person, also a Tor director) are working on the deployment angle by talking to a) DPI vendors who should donate their hardware to do something good for a change, and b) ISPs that should put said DPI boxes on their network.

At least, that was the status in October. I haven't talked to them about it since.

Also, both Alex and Ian are professors so their main priorities are to publish and to teach their students how to do research.

Actual for-real Telex deployment is going to take a lot of effort beyond what I know they've done so far (first in terms of the logistics above, and second in terms of software usability). In my opinion their best bet for the usability side is to bundle with a popular open-source circumvention tool so a) they don't have to come up with their own user interface and b) so they don't have to "compete" with the more-established tools.

--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Shava Nerad; Kelly DeVos; [redacted]
Subject: Re: Thanks!
Date: Thursday, August 17, 2006 11:50:15 AM

Yes

Roger Dingledine wrote:

> On Wed, Aug 16, 2006 at 09:11:32AM -0400, Ken Berman wrote:
>
> > Shava - not quite. The disbursements would be over the remaining
> > period, not 10/1. 10/1 is simply the date by which to complete the
> > action. Ken
>
> Hi Ken,
>
> This is fabulous news.
>
> Shava: the period for this contract is May 24 2006 to Dec 23 2006. But
> it took several months to "complete the action" on the first one, so we
> should get moving on this. :)
>
> Kelly (and Ken): this is going to let us get Nick back on-board starting
> October 1 if all goes well. Yay! We'll be able to do some great stuff
> in terms of getting Tor development, scalability, and documentation
> back on track. I'd like to focus most on two topics, once we get back
> up to speed: 1) usability for server operators, to expand the network
> and make it more stable; and 2) design document and code changes for a
> blocking-resistant network. These both seem like good topics. Did you
> have anything in mind that we should concentrate on too (or instead)?
>
> Ken: I don't want to make you commit to anything too early, but can
> you let me know if we are planning to add the FY07 extension to our
> contract too? If so, we can start to bite off a larger set of topics,
> and it's never too early to start thinking about that. :) A simple
> "yes / no / ask later" would be great.
>
> Thanks!
> --Roger

From: Roger Dingledine
To: Ken Berman
Cc: [redacted]
Subject: Re: Thanks!
Date: Wednesday, August 16, 2006 4:20:35 PM

On Wed, Aug 16, 2006 at 09:11:32AM -0400, Ken Berman wrote:
> Shava - not quite. The disbursements would be over the remaining
> period, not 10/1. 10/1 is simply the date by which to complete the
> action. Ken

Hi Ken,

This is fabulous news.

Shava: the period for this contract is May 24 2006 to Dec 23 2006. But it took several months to "complete the action" on the first one, so we should get moving on this. :)

Kelly (and Ken): this is going to let us get Nick back on-board starting October 1 if all goes well. Yay! We'll be able to do some great stuff in terms of getting Tor development, scalability, and documentation back on track. I'd like to focus most on two topics, once we get back up to speed: 1) usability for server operators, to expand the network and make it more stable; and 2) design document and code changes for a blocking-resistant network. These both seem like good topics. Did you have anything in mind that we should concentrate on too (or instead)?

Ken: I don't want to make you commit to anything too early, but can you let me know if we are planning to add the FY07 extension to our contract too? If so, we can start to bite off a larger set of topics, and it's never too early to start thinking about that. :) A simple "yes / no / ask later" would be great.

Thanks!
--Roger

From: Roger Dingledine
To: Kelly DeYoe
Cc: Ken Berman; Shava Nerad; [redacted]
Subject: Re: Thanks!
Date: Thursday, August 17, 2006 7:14:39 PM

On Thu, Aug 17, 2006 at 05:54:28PM -0400, Kelly DeYoe wrote:
> Yeah, we may need to get the dates on the contract fixed up, since in
> one place it lists the contract term at 6/1/2006-1/31/2007 which is
> correctly 8 months, but in another place it lists 5/24/2006-12/23/2006,
> which is in fact only 7 months.
>
> I'm going to be pessimistic and assume we cannot get the mod through
> before 8/24 (next Thursday), so that would mean if we want to keep the
> months even, the mod should go through 9/24, which means 4 months left
> on the contract, and $70,000 / 4 months = $17,500 additional per month
> for the modification.
>
> I'll keep everyone posted on this though.

Fabulous. That works for me. I've been running around as usual -- I just had a meeting with Nick to confirm that he's in now that we've got more money coming in, and he is. Great. Are there specific further things you need from me to move the contract changes forward? I'm going to be not-so-communicado this Saturday to next Saturday; I'll have cell phone and periodic net access but fax machines and such will be harder to find. So if we want actual signatures in the 8/24 timeframe, perhaps I should deputize Shava to sign for me? Or will this complicate things too much?

--Roger

From: Andrew Lewman
To: [redacted]
Cc: [redacted] Kelly DeYoe; Sho Ho; [redacted] [redacted] Ken Berman; Karen Reilly
Subject: Re: the report is already out -- Re: FW: Upcoming Event: Internet Circumvention Tools and Methods: Evaluation and Review
Date: Tuesday, April 12, 2011 10:46:56 PM

On Tue, 12 Apr 2011 15:48:48 -0400
"[redacted] <[redacted] wrote:

>
> http://freedomhouse.org/template.cfm?page=383&report=97

Yup, it is out. Congrats to DIT for your good reviews and popularity among the surveyed users.

I'm sure all of you picked up on a number of problems with the methodology of the report. Just one is that "Support and Security" are two very different things, but the report writers appeared to only have measured support, and completely glossed over security. It's not clear to me what they measured for support, either.

However, it's clear that we at Tor need to focus much more on usability for normal people. Or, we need to eschew normal users and work with the other circumvention tool providers more to provide them the results of our R&D into online privacy, circumvention, and anonymity. We're seeing a number of very sophisticated circumvention/privacy/anonymity attacks in the wild that no one else is addressing. This has us concerned for sensitive users in hostile countries.

I need more time to collect my thoughts about this report.

--
Andrew
pgp 0x74ED336B

From: Kelly DeYoe
To: Roger Dingledine
Cc: Ken Berman; Hiu Ho
Subject: Re: Tor / China plan
Date: Monday, June 19, 2006 6:54:28 PM

Hey Roger, it all sounds good to us. I'm going to work on fleshing out some more details for Phase 2 planning, and get things together to hand off to Bennett over the next couple days so that he can do much of the work in that area.

-k

Roger Dingledine wrote:
> On Mon, Jun 05, 2006 at 04:37:09PM -0400, Roger Dingledine wrote:
>
>>An outline for a design doc coming soon...
>
>
> Hi folks. Here is The Plan, broken down into three phases, which we can
> pursue in parallel. Phase one is mostly me, phase two is where Bennett
> comes in, and then we all team up to take phase two to phase three.
>
> Phase one: Core Tor development to make it easier to become a relay.
> Generally improve usability of Tor and supporting programs.
>
> [Phase one-prime: Fix the fact that Windows XP networking doesn't handle
> being a Tor server as well as we'd like. Mike Chiussi at UToronto
> is making a start at this. We can skip this step by telling Windows
> volunteers to come back later -- but that might impact the number of
> volunteer relays we end up with.]
>
> Phase two: Come up with ways to communicate some bootstrap relays to
> dissidents. Try to make China not notice despite all the media who want
> to write about us. Iterate.
>
> Phase three: Code for a separate "unlisted" Tor network, handling the
> easy/promising cases from phase two.
> a) Change directory authority code to enable a separate, parallel Tor
>   network that doesn't broadcast the addresses of all its participants.
> b) Add interfaces to Vidalia to allow a user to sign up to be one of
>   these secondary relays; document and test.
> c) Add interfaces to Vidalia for the people who are blocked; document
>   and test.
>
> To start phase two, we need to enumerate all the schemes we can
> imagine. Then we can list their pros and cons, prioritize them, and
> predict what sort of interfaces will be helpful for each in phase three.
>
> Here are a few starts that need to be fleshed out and need more thought.
> - The dir server just gives you a random IP address if you ask.
>   This is great until the dir server gets censored, or until
>   the adversary starts collecting IP addresses too.
> - To solve the blocked-dirserver problem, we could
>   - Have a way to manually enter a relay address learned out-of-band
>   (e.g. via social network).
>   - Encourage users to use open proxies or other proxies to reach

> the dir server.
> - To solve the adversary-collecting-addresses problem, we could
> - Add a captcha.
> - Require a valid email address at e.g. yahoo -- leveraging somebody
> else's captcha system.
> - Give out a single address to all queries for a given hour, so you
> need to ask every single hour for many weeks in order to learn
> the entire list.
> - Give accounts to users, let them earn trust, try to detect
> when the addresses they use get blocked, and reward when not.
> - ...
> - Send lots of spam to bootstrap relay IPs.
> - Have users scan the Internet for relay IPs (won't work while we're
> small, but we're trying to be complete here).
> - We could sneak a big pile of relay addresses into popular software,
> and have them each suddenly enabled one day.
> - ...
>

From: Roger Dingledine
To: Kelly DeYoe
Cc: Ken Berman; Hiu Ho; [redacted]
Subject: Re: Tor / China plan
Date: Monday, July 31, 2006 5:16:47 PM

Hi Kelly, folks,

I've collected some rudimentary stats about our Tor users, by running a directory cache and seeing who hits it. We should probably keep the existence of these stats quiet for now -- even though we're not watching any actual Tor traffic, it might still make users uncomfortable. We have it on our todo list to fix the fact that this information can be gathered (by having clients pick a few directory caches and stick with them, rather than picking randomly from the whole set each time), but on the other hand, we also want to be able to collect stats...

It's been running for about 6 days now, and has seen 97054 distinct IP addresses. I'm not sure what fraction of the overall Tor client population this is -- it's clearly not all of it, but I think it's maybe half. The most interesting part is the breakdown by country. I've annotated a few in case you're not familiar with two-letter country codes.

23084 US (23.785%)
19809 DE (20.410%) Germany
15505 CN (15.976%) China
4948 JP (5.098%) Japan
3814 IT (3.930%) Italy
3042 FR (3.134%) France
2966 GB (3.056%) Great Britain
2427 CA (2.501%) Canada
1357 Unknown (1.398%) My GeoIP engine didn't work for these, so they could be anything. I checked a few manually and some were US, some were Africa.
1315 SE (1.355%) Sweden
1308 AU (1.348%) Australia
1059 ES (1.091%) Spain
1027 CH (1.058%) Switzerland
986 TH (1.016%) Thailand
917 NL (0.945%) Nederlands
835 PL (0.860%) Poland
792 BR (0.816%) Brazil
784 IR (0.808%) Iran
757 AT (0.780%) Austria
756 TW (0.779%) Taiwan
607 RU (0.625%) Russia
546 SA (0.563%) Saudia Arabia
504 FI (0.519%) Finland
501 IL (0.516%) Israel
464 PT (0.478%) Portugal
464 AE (0.478%) Arab Emirates
441 BE (0.454%) Belgium
408 SG (0.420%) Singapore
366 NO (0.377%) Norway
341 AR (0.351%) Argentina
326 HK (0.336%) Hong Kong
277 DK (0.285%) Denmark
271 IN (0.279%) India

251 RO (0.259%) Romania
242 MY (0.249%) Malaysia
239 MX (0.246%)
227 TR (0.234%)
225 GR (0.232%)
211 NZ (0.217%)
195 IE (0.201%)
189 HU (0.195%)
169 SI (0.174%)
148 CZ (0.152%)
119 UA (0.123%)
114 PH (0.117%)
111 BG (0.114%)
108 LT (0.111%)
90 SK (0.093%)
83 KR (0.086%)
81 CL (0.083%)
73 LV (0.075%)
66 HR (0.068%)
63 QA (0.065%)
63 EE (0.065%)
58 VE (0.060%)
54 PE (0.056%)
54 VN (0.056%)
50 CO (0.052%)
47 ID (0.048%)
46 KW (0.047%)
38 LU (0.039%)
32 BY (0.033%)
31 PK (0.032%)
28 CS (0.029%)
27 IS (0.028%)
24 MK (0.025%)
21 DO (0.022%)
20 CR (0.021%)
19 PA (0.020%)
18 JO (0.019%)
15 UY (0.015%)
13 LI (0.013%)
13 BN (0.013%)
13 OM (0.013%)
12 CY (0.012%)
12 TT (0.012%)
12 MT (0.012%)
12 GT (0.012%)
10 GI (0.010%)
10 MD (0.010%)
10 NC (0.010%)
8 SM (0.008%)
8 SY (0.008%)
8 MC (0.008%)
8 BS (0.008%)
8 KZ (0.008%)
7 MO (0.007%)
7 BH (0.007%)
7 UZ (0.007%)
6 EC (0.006%)
6 BZ (0.006%)
6 LB (0.006%)
6 PS (0.006%)

5 JM (0.005%)
5 HN (0.005%)
5 CU (0.005%)
5 BO (0.005%)
4 PF (0.004%)
4 PY (0.004%)
4 SV (0.004%)
3 BD (0.003%)
3 DZ (0.003%)
3 AG (0.003%)
3 AZ (0.003%)
3 BM (0.003%)
3 GH (0.003%)
3 NG (0.003%)
3 TZ (0.003%)
3 BA (0.003%)
2 IQ (0.002%)
2 VI (0.002%)
2 VU (0.002%)
2 FJ (0.002%)
2 YE (0.002%)
2 AL (0.002%)
2 NI (0.002%)
2 PR (0.002%)
1 AD (0.001%)
1 GE (0.001%)
1 AN (0.001%)
1 ZW (0.001%)
1 GP (0.001%)
1 KE (0.001%)
1 FO (0.001%)
1 KH (0.001%)
1 LK (0.001%)
1 GU (0.001%)
1 MV (0.001%)
1 UG (0.001%)
1 TM (0.001%)

From: Roger Dingledine
To: Hiu Ho
Cc: Ken Berman; [redacted] Kelly DeYoe; Betty Pruitt
Subject: Re: Tor + IBB: moving forward
Date: Friday, March 17, 2006 3:26:22 PM

On Fri, Mar 17, 2006 at 01:24:01PM -0500, Hiu Ho wrote:
> I agree with Ken that the translation of the whole Tor website involes
> tremendous amount of work. I suggest we should first create a
> trimmed-down Chinese (or whatever language) Tor site, which covers the
> basic such as what Tor is, how to set up Tor, and where to download Tor.
> Then, from that basis, we can continue to add new sections to the
> translated Tor site if there's a demand.
>
> >>Our translation guidelines are here:
> >>http://tor.eff.org/translation

Right, I agree. I didn't mean to suggest that we translate everything in sight -- the main reason other than workload being that many of these pages change quite often. The Tor website translation guidelines give a list of which pages we think would be useful to do first.

I don't think translation is high priority though. So far we've just waited for people to come along and volunteer some translations, and we could stick with that plan if that's simplest.

--Roger

From: Ken Berman
To: Roger Dingledine
Cc: [redacted] Kelly DeYoe; Betty Pruitt
Subject: Re: Tor + IBB: moving forward
Date: Friday, March 17, 2006 10:25:25 AM

Roger, I think we can help on the Chinese translation, but somehow I need to bound it, When I go to the pages, they keep linking deeper and deeper, often ending at wiki sites. Is there some way to get a hierarchy? The translation guide lists the .wml files as being of top priority, but the overall doc sites lists many more. I did not see any Chinese mentioned in the bottom link on the home page, so I would assume everything need translating, but for German, only your home page is translated, every second link is back to English.

Ken

Roger Dingledine wrote:

> On Fri, Feb 24, 2006 at 10:34:20AM -0500, Ken Berman wrote:
>
> > As for translations, we can help with the Russian and
> > Chinese language
> > sites.
>
> Great. You can see our Russian translation here:
> http://tor.eff.org/index.html.ru
>
> Some pages are already translated, and probably the ones that
> most still want translation are listed in this section:
> http://tor.eff.org/documentation#RunningTor
> (and the actual files to be translated are in
> http://tor.eff.org/cvs/website/docs/en/)
>
> Our translation guidelines are here:
> http://tor.eff.org/translation
>
> We have no Chinese-language translations currently.
>
> What are the next steps to help move this forward?
>
> Thanks,
> --Roger

From: Bennett Haselton
To: Roger Dingledine; (b) (6) Kelly DeYoe
Cc: (b) (6)
Subject: Re: Tor + IBB: moving forward
Date: Thursday, March 16, 2006 1:51:46 AM

I can definitely work on the incentives problem since that's something I've thought about too.

I was also looking at the Windows networking error that Roger discussed which causes crashes on lots of TOR servers, but as far as I could tell from searching on it, this appears to be a limit of Windows networking -- however, it only happens in cases when a program opens a large number of sockets. My understanding is that if we set up an incentives system, that will encourage lots of different users to configure their nodes to provide services that right now only a handful of servers are providing, so that will lessen the problem with servers crashing because of a huge number of open sockets.

-Bennett

At 05:05 PM 3/15/2006 -0500, Roger Dingledine wrote:
>Hi Bennett, Hiu,
>
>How are these going?
>
>I know we're a bit disorganized over here since there's too much work to
>be done and nobody to manage other people, so I'm hoping to find tasks
>which will make you self-motivated. :)
>
>If there's something you'd rather be looking at, please let me know that
>too.
>
>Thanks,
>--Roger
>
>On Thu, Feb 16, 2006 at 05:19:02PM -0500, Roger Dingledine wrote:
> > Hiu is going to learn about the Tor controller protocol:
> > http://tor.eff.org/cvs/tor/doc/control-spec.txt
> > http://tor.eff.org/cvs/control/doc/howto.txt
> > http://tor.eff.org/cvs/control/
> > http://tor.eff.org/gui/
> > and think about what features are missing and how he might
> > want to design an interface for censored Tor users that a) has a
> > GUI for people to know that something is happening, configure it,
> > etc, and b) can handle a variety of ways of hearing about relay
> > addresses. Check out http://freehaven.net/edmanm/torcp/ for what's
> > probably the most common Windows Tor controller currently (but it
> > has many usability problems). Be sure to use the latest development
> > release of Tor when trying things.
> >
> > Bennett is going to go through the previous email's text (quoted
> below),
> > plus his previous documents, and sketch out a concise-but-detailed :)
> > roadmap of the design issues and tradeoffs we'll need to tackle to
> deploy
> > a censorship solution.
> > See http://tor.eff.org/cvs/tor/doc/incentives.txt for a

> work-in-progress
> > example or http://tor.eff.org/cvs/tor/doc/dir-spec.txt for a more
> > polished example if needed.
> >
> > Hiu and Bennett should also skim the Blossom page at
> > http://afs.eecs.harvard.edu/~goodell/blossom/ for another example
> > of a Tor controller that uses more of the protocol's features,
> > and demonstrates how Tor's path-building can be separated from
> > its network-discovery. Blossom's developer is amenable to helping
> > to adapt it for use in the censorship context.
> >
> > And again, let me know if you have any questions about anything, and
> > feel free to tackle anything else you want:
> > http://tor.eff.org/volunteer lists some more issues.
> >
> > Lastly, if you folks are into IRC, you are welcome to listen in on the
> > user support channel at #tor on irc.oftc.net, or the secret
> undocumented
> > internal developer's channel at #tor-dev on irc.seul.org.

From: Roger Dingledine
To: Ken Berman
Cc: [redacted] (b)(6) [redacted] Kelly DeYoe; Betty Pruitt
Subject: Re: Tor + IBB: moving forward
Date: Wednesday, March 15, 2006 10:42:03 PM

On Fri, Feb 24, 2006 at 10:34:20AM -0500, Ken Berman wrote:
> As for translations, we can help with the Russian and Chinese language
> sites.

Great. You can see our Russian translation here:
http://tor.eff.org/index.html.ru

Some pages are already translated, and probably the ones that
most still want translation are listed in this section:
http://tor.eff.org/documentation#RunningTor
(and the actual files to be translated are in
http://tor.eff.org/cvs/website/docs/en/)

Our translation guidelines are here:
http://tor.eff.org/translation

We have no Chinese-language translations currently.

What are the next steps to help move this forward?

Thanks,
--Roger

From: Roger Dingledine
To: [redacted] Kelly DeYoe
Cc: [redacted]
Subject: Re: Tor + IBB: moving forward
Date: Wednesday, March 15, 2006 6:05:26 PM

Hi Bennett, Hiu,

How are these going?

I know we're a bit disorganized over here since there's too much work to be done and nobody to manage other people, so I'm hoping to find tasks which will make you self-motivated. :)

If there's something you'd rather be looking at, please let me know that too.

Thanks,
--Roger

On Thu, Feb 16, 2006 at 05:19:02PM -0500, Roger Dingledine wrote:
> Hiu is going to learn about the Tor controller protocol:
> http://tor.eff.org/cvs/tor/doc/control-spec.txt
> http://tor.eff.org/cvs/control/doc/howto.txt
> http://tor.eff.org/cvs/control/
> http://tor.eff.org/gui/
> and think about what features are missing and how he might
> want to design an interface for censored Tor users that a) has a
> GUI for people to know that something is happening, configure it,
> etc, and b) can handle a variety of ways of hearing about relay
> addresses. Check out http://freehaven.net/edmanm/torcp/ for what's
> probably the most common Windows Tor controller currently (but it
> has many usability problems). Be sure to use the latest development
> release of Tor when trying things.
>
> Bennett is going to go through the previous email's text (quoted below),
> plus his previous documents, and sketch out a concise-but-detailed :)
> roadmap of the design issues and tradeoffs we'll need to tackle to deploy
> a censorship solution.
> See http://tor.eff.org/cvs/tor/doc/incentives.txt for a work-in-progress
> example or http://tor.eff.org/cvs/tor/doc/dir-spec.txt for a more
> polished example if needed.
>
> Hiu and Bennett should also skim the Blossom page at
> http://afs.eecs.harvard.edu/~goodell/blossom/ for another example
> of a Tor controller that uses more of the protocol's features,
> and demonstrates how Tor's path-building can be separated from
> its network-discovery. Blossom's developer is amenable to helping
> to adapt it for use in the censorship context.
>
> And again, let me know if you have any questions about anything, and
> feel free to tackle anything else you want:
> http://tor.eff.org/volunteer lists some more issues.
>
> Lastly, if you folks are into IRC, you are welcome to listen in on the
> user support channel at #tor on irc.oftc.net, or the secret undocumented
> internal developer's channel at #tor-dev on irc.seul.org.

From: Bennett Haselton
To: Ken Berman; Roger Dingledine
Cc: [redacted] Kelly DeYoe; [redacted] Betty Pruitt
Subject: Re: Tor + IBB: moving forward
Date: Wednesday, March 01, 2006 12:37:27 AM

When I announced that Peacefire was getting funding from Voice of America to work on the Circumventor, I expected much more of a backlash than I actually got -- being as I was part of a civil libertarian community where some people were very hostile to governments. All that happened was I got one (1) self-righteous e-mail from a guy who said he was "withdrawing all of his support" since he "understood that government is the cause of the problem, not the solution". I replied that (a) since the government in this case was helping solve the problem, didn't that contradict his statement and (b) what did he mean by "withdrawing his support", seeing as he'd never done anything to help anyway?

I think most people, especially the smart people who count, understand that government can be good or bad, and governments offices, like puppies, should be encouraged when they do the right thing.

-Bennett

At 10:34 AM 2/24/2006 -0500, Ken Berman wrote:

>We also need to think about a strategy for how to spin this move in terms
>of Tor's overall direction. I would guess that we don't want to loudly
>declare war on China, since this only harms our goals? But we also don't
>want to hide the existence of funding from IBB, since "they're getting
>paid off by the feds and they didn't tell anyone" sounds like a bad
>Slashdot title for a security project. Is it sufficient just to always
>talk about Iran, or is that not subtle enough?
>
>Roger - we will do any spin you want to do to help preserve the
>independence of TOR. We can't (nor should we) hide it for the reasons you
>have
>outlined below, but we also don't want to shout if from the rafters,
>either I guess I would say that the "feds" in this case are supporting
>the Office of Global Internet Freedom and this is another way to allow the
>kind of uncensored news access that were outlined in the recent
>Congressional hearings, and endorsed by HRIC, RSF, etc.
>
>As for translations, we can help with the Russian and Chinese language
>sites.
>
>Ken
>
>
>
>Roger Dingledine wrote:
>>
>>Hi Bennett, Hiu, Kelly,
>>
>>Here's a mail that has been queueing until I learned more details
>>about our plan. I'd still like to hear from Ken what vision and
>>goals he's hoping for (maybe Kelly can learn this and include it
>>in our upcoming conference call?), but in the meantime, here's an
>>overview of some of the tasks that need to be tackled.

>>
>>My goal here is to see if any of these paragraphs catch your eye. My
>>experience is that people do their best work when they're excited about
>>it, so -- does any of this excite you in particular? We have a lot of
>>different tasks to work on, so whatever you're most interested in is
>>clearly the right thing to work on. Or are there other related things
>>that you think need attention too? I'm open to suggestions.
>>
>>
>>My focus for the next little while is to get the Tor 0.1.1.x release
>>candidate ready. This new Tor version includes a more scalable and secure
>>directory system, and we'll need it in order for the Tor network to grow
>>much larger.
>>
>>After that, my plan is to start focusing on server usability -- how to
>>make all the internals of Tor work correctly if we have a button to
>>sign yourself up as a relay for our alternate Tor network. In addition,
>>we could really use some good simple documentation for how to forward
>>a port through some typical home routers, how to set Tor up, etc. We
>>could also use some help on the Tor GUI that lets people choose to
>>become servers. It's pretty far from having the 'help China' button on
>>it. (In fact, we have no front-end at all for OS X, Linux, etc.)
>>
>>We also need to think about a strategy for how to spin this move in terms
>>of Tor's overall direction. I would guess that we don't want to loudly
>>declare war on China, since this only harms our goals? But we also don't
>>want to hide the existence of funding from IBB, since "they're getting
>>paid off by the feds and they didn't tell anyone" sounds like a bad
>>Slashdot title for a security project. Is it sufficient just to always
>>talk about Iran, or is that not subtle enough?
>>
>>Somewhere in this, we need to keep processing volunteer mail such as the
>>nice people who just translated the Tor site into Chinese and Russian,
>>and keep trying to support server operator questions, and keep trying to
>>find somebody to help with Windows stability, docs, faqs, user support,
>>and so forth.
>>
>>In parallel to this, we're going to need somebody to design a GUI
>>controller for the people who want to be Tor clients but can't make it
>>to the main Tor network directly. The actual back-end talking to the Tor
>>client is pretty easy, but it's probably not good enough to have it in
>>English, and there are a lot of design issues to work out too:
>>
>>We need to enumerate some ways for clients to bootstrap relay IP
>>addresses
>>-- a couple of default addresses just in case they work, a way to
>>manually
>>enter them, the instant-messaging account that Bennett was talking about,
>>receiving them in the mass-mailing spams, and so forth. Once the Tor
>>client knows a few relay IP addresses, it can automatically build the
>>connection and reach the main directory server.
>>
>>...Which also needs to be figured out. I had originally envisioned this
>>as just a little cgi script on a web page somewhere, but now that I think
>>about it more, we probably want some features like being able to check
>>whether a relay is actually working right now. All of that is already
>>working if we use a normal Tor directory server, and we can modify it
>>to not answer requests for the whole directory, and to answer with our
>>special algorithm.
>>

>>...Which brings us to the algorithm for disbursing backup relay
>>addresses. This could vary widely from Bennett's "if they already know
>>the
>>public key then they can lookup the current server descriptor for that
>>key but nothing more" to "we'll give them a couple of random addresses
>>every time they ask for some" to "everybody who asks this hour gets
>>this IP address, and next hour we'll switch to giving out a new one" to
>>"ask them to register pseudonymous accounts and try to build a system
>>to detect which accounts defect". We need to enumerate these options
>>and make a concise list of pros and cons. Remember that we're not just
>>targetting one country, so it may be reasonable to deploy different
>>strategies simultaneously.
>>
>>We'll want to build a plan for bootstrapping the whole thing (if we
>>make it too locked down originally, then we'll end up with no users,
>>and there will be no point). I think it's fine to assume that when we
>>first start out nobody will care, but we need to consider and anticipate
>>some of the transition problems, for example so we avoid letting them
>>enumerate the whole set of relays and destroy the progress we've made
>>once they do start to care.
>>
>>There's clearly more to plan and more to lay out, but hopefully this will
>>get us moving in the right direction. Another topic for the conference
>>call is integrating this discussion into the normal Tor mailing lists
>>so we can do more design out in the open (or at least with a broader
>>set of developers).
>>
>>Thanks,
>>--Roger
>>
>>

From: Roger Dingledine
To: Ken Berman
Cc: (b) (6) Kelly DeYoe
Subject: Re: Tor + IBB: moving forward
Date: Sunday, February 26, 2006 3:04:51 AM

On Fri, Feb 24, 2006 at 10:25:10AM -0500, Ken Berman wrote:
> Roger -we are starting the paperwork for the agreed upon amount. I have
> signed off (that was the easy part) and now it goes to our Office of
> Contracts, for which we will, basically, have to answer the questions:
> Who the hell is Roger Dingledine and What the hecht is this TOR thing.

Great. Let me know if you need any more help answering those.

> As for my vision, I think there is congruence between yours and mine at
> this point in time relative to this subject matter.....

I agree. Now I just need to unbury myself from all the people sending me mail about Tor (we have even more users now than a few weeks ago), and start moving forward again. :) First step for that is getting the 0.1.1.x tree stable so we can release.

I've also been chatting with several people at the State department who want to take advantage of the recent hubbub to start their own anti-censorship movements in the government, and they like Tor as a starting point.

Thanks,
--Roger

From: Roger Dingledine
To: Kelly DeYoe
Subject: Re: Tor + IBB: moving forward
Date: Sunday, February 26, 2006 2:56:08 AM

On Thu, Feb 16, 2006 at 05:19:02PM -0500, Roger Dingledine wrote:
> Kelly, can you
> forward this mail to Gail(?) too so I have her email address and name?

I guess "forward this to her" is not sufficient for me to learn her
name and email address. So I should ask more directly. :)

Who was the other person on the phone with us during the call?

Thanks,
--Roger

From: Ken Berman
To: Roger Dingledine
Cc: [redacted] Kelly DeYoe; [redacted] Betty Pruitt
Subject: Re: Tor + IBB: moving forward
Date: Friday, February 24, 2006 10:34:20 AM

We also need to think about a strategy for how to spin this move in terms of Tor's overall direction. I would guess that we don't want to loudly declare war on China, since this only harms our goals? But we also don't want to hide the existence of funding from IBB, since "they're getting paid off by the feds and they didn't tell anyone" sounds like a bad Slashdot title for a security project. Is it sufficient just to always talk about Iran, or is that not subtle enough?

Roger - we will do any spin you want to do to help preserve the independence of TOR. We can't (nor should we) hide it for the reasons you have outlined below, but we also don't want to shout if from the rafters, either I guess I would say that the "feds" in this case are supporting the Office of Global Internet Freedom and this is another way to allow the kind of uncensored news access that were outlined in the recent Congressional hearings, and endorsed by HRIC, RSF, etc.

As for translations, we can help with the Russian and Chinese language sites.

Ken

Roger Dingledine wrote:

> Hi Bennett, Hiu, Kelly,
>
> Here's a mail that has been queueing until I learned more details about our plan. I'd still like to hear from Ken what vision and goals he's hoping for (maybe Kelly can learn this and include it in our upcoming conference call?), but in the meantime, here's an overview of some of the tasks that need to be tackled.
>
> My goal here is to see if any of these paragraphs catch your eye. My experience is that people do their best work when they're excited about it, so -- does any of this excite you in particular? We have a lot of different tasks to work on, so whatever you're most interested in is clearly the right thing to work on. Or are there other related things that you think need attention too? I'm open to suggestions.
>
> My focus for the next little while is to get the Tor 0.1.1.x release candidate ready. This new Tor version includes a more scalable and secure directory system, and we'll need it in order for the Tor network to grow much larger.
>
> After that, my plan is to start focusing on server usability -- how to make all the internals of Tor work correctly if we have a button to sign yourself up as a relay for our alternate Tor network. In addition,

we could really use some good simple documentation for how to forward
a port through some typical home routers, how to set Tor up, etc. We
could also use some help on the Tor GUI that lets people choose to
become servers. It's pretty far from having the 'help China' button on
it. (In fact, we have no front-end at all for OS X, Linux, etc.)

We also need to think about a strategy for how to spin this move in terms
of Tor's overall direction. I would guess that we don't want to loudly
declare war on China, since this only harms our goals? But we also don't
want to hide the existence of funding from IBB, since "they're getting
paid off by the feds and they didn't tell anyone" sounds like a bad
Slashdot title for a security project. Is it sufficient just to always
talk about Iran, or is that not subtle enough?

Somewhere in this, we need to keep processing volunteer mail such as the
nice people who just translated the Tor site into Chinese and Russian,
and keep trying to support server operator questions, and keep trying to
find somebody to help with Windows stability, docs, faqs, user support,
and so forth.

In parallel to this, we're going to need somebody to design a GUI
controller for the people who want to be Tor clients but can't make it
to the main Tor network directly. The actual back-end talking to the Tor
client is pretty easy, but it's probably not good enough to have it in
English, and there are a lot of design issues to work out too:

We need to enumerate some ways for clients to bootstrap relay IP addresses
-- a couple of default addresses just in case they work, a way to manually
enter them, the instant-messaging account that Bennett was talking about,
receiving them in the mass-mailing spams, and so forth. Once the Tor
client knows a few relay IP addresses, it can automatically build the
connection and reach the main directory server.

...Which also needs to be figured out. I had originally envisioned this
as just a little cgi script on a web page somewhere, but now that I think
about it more, we probably want some features like being able to check
whether a relay is actually working right now. All of that is already
working if we use a normal Tor directory server, and we can modify it
to not answer requests for the whole directory, and to answer with our
special algorithm.

...Which brings us to the algorithm for disbursing backup relay
addresses. This could vary widely from Bennett's "if they already know the
public key then they can lookup the current server descriptor for that
key but nothing more" to "we'll give them a couple of random addresses

every time they ask for some" to "everybody who asks this hour gets this IP address, and next hour we'll switch to giving out a new one" to "ask them to register pseudonymous accounts and try to build a system to detect which accounts defect". We need to enumerate these options and make a concise list of pros and cons. Remember that we're not just targetting one country, so it may be reasonable to deploy different strategies simultaneously.

We'll want to build a plan for bootstrapping the whole thing (if we make it too locked down originally, then we'll end up with no users, and there will be no point). I think it's fine to assume that when we first start out nobody will care, but we need to consider and anticipate some of the transition problems, for example so we avoid letting them enumerate the whole set of relays and destroy the progress we've made once they do start to care.

There's clearly more to plan and more to lay out, but hopefully this will get us moving in the right direction. Another topic for the conference call is integrating this discussion into the normal Tor mailing lists so we can do more design out in the open (or at least with a broader set of developers).

Thanks,
--Roger

From: Ken Berman
To: Roger Dingledine
Cc: [redacted] Kelly DeYoe
Subject: Re: Tor + IBB: moving forward
Date: Friday, February 24, 2006 10:25:10 AM

Roger -we are starting the paperwork for the agreed upon amount. I have signed off (that was the easy part) and now it goes to our Office of Contracts, for which we will, basically, have to answer the questions: Who the hell is Roger Dingledine and What the hecht is this TOR thing. As for my vision, I think there is congruence between yours and mine at this point in time relative to this subject matter.....

Ken

Roger Dingledine wrote:

>Hi Bennett, Hiu, Kelly,
>
>Here's a mail that has been queueing until I learned more details
>about our plan. I'd still like to hear from Ken what vision and
>goals he's hoping for (maybe Kelly can learn this and include it
>in our upcoming conference call?), but in the meantime, here's an
>overview of some of the tasks that need to be tackled.
>
>My goal here is to see if any of these paragraphs catch your eye. My
>experience is that people do their best work when they're excited about
>it, so -- does any of this excite you in particular? We have a lot of
>different tasks to work on, so whatever you're most interested in is
>clearly the right thing to work on. Or are there other related things
>that you think need attention too? I'm open to suggestions.
>
>
>My focus for the next little while is to get the Tor 0.1.1.x release
>candidate ready. This new Tor version includes a more scalable and secure
>directory system, and we'll need it in order for the Tor network to grow
>much larger.
>
>After that, my plan is to start focusing on server usability -- how to
>make all the internals of Tor work correctly if we have a button to
>sign yourself up as a relay for our alternate Tor network. In addition,
>we could really use some good simple documentation for how to forward
>a port through some typical home routers, how to set Tor up, etc. We
>could also use some help on the Tor GUI that lets people choose to
>become servers. It's pretty far from having the 'help China' button on
>it. (In fact, we have no front-end at all for OS X, Linux, etc.)
>
>We also need to think about a strategy for how to spin this move in terms
>of Tor's overall direction. I would guess that we don't want to loudly
>declare war on China, since this only harms our goals? But we also don't
>want to hide the existence of funding from IBB, since "they're getting
>paid off by the feds and they didn't tell anyone" sounds like a bad
>Slashdot title for a security project. Is it sufficient just to always
>talk about Iran, or is that not subtle enough?
>
>Somewhere in this, we need to keep processing volunteer mail such as the

>nice people who just translated the Tor site into Chinese and Russian,
>and keep trying to support server operator questions, and keep trying to
>find somebody to help with Windows stability, docs, faqs, user support,
>and so forth.
>
>In parallel to this, we're going to need somebody to design a GUI
>controller for the people who want to be Tor clients but can't make it
>to the main Tor network directly. The actual back-end talking to the Tor
>client is pretty easy, but it's probably not good enough to have it in
>English, and there are a lot of design issues to work out too:
>
>We need to enumerate some ways for clients to bootstrap relay IP addresses
>-- a couple of default addresses just in case they work, a way to manually
>enter them, the instant-messaging account that Bennett was talking about,
>receiving them in the mass-mailing spams, and so forth. Once the Tor
>client knows a few relay IP addresses, it can automatically build the
>connection and reach the main directory server.
>
>...Which also needs to be figured out. I had originally envisioned this
>as just a little cgi script on a web page somewhere, but now that I think
>about it more, we probably want some features like being able to check
>whether a relay is actually working right now. All of that is already
>working if we use a normal Tor directory server, and we can modify it
>to not answer requests for the whole directory, and to answer with our
>special algorithm.
>
>...Which brings us to the algorithm for disbursing backup relay
>addresses. This could vary widely from Bennett's "if they already know the
>public key then they can lookup the current server descriptor for that
>key but nothing more" to "we'll give them a couple of random addresses
>every time they ask for some" to "everybody who asks this hour gets
>this IP address, and next hour we'll switch to giving out a new one" to
>"ask them to register pseudonymous accounts and try to build a system
>to detect which accounts defect". We need to enumerate these options
>and make a concise list of pros and cons. Remember that we're not just
>targetting one country, so it may be reasonable to deploy different
>strategies simultaneously.
>
>We'll want to build a plan for bootstrapping the whole thing (if we
>make it too locked down originally, then we'll end up with no users,
>and there will be no point). I think it's fine to assume that when we
>first start out nobody will care, but we need to consider and anticipate
>some of the transition problems, for example so we avoid letting them
>enumerate the whole set of relays and destroy the progress we've made
>once they do start to care.
>
>There's clearly more to plan and more to lay out, but hopefully this will
>get us moving in the right direction. Another topic for the conference
>call is integrating this discussion into the normal Tor mailing lists
>so we can do more design out in the open (or at least with a broader
>set of developers).
>
>Thanks,
>--Roger
>
>
>

From: Ken Berman
To: Roger Dingledine
Cc: (b) (6) (b) (6) Kelly DeYoe; (b) (6)
Subject: Re: Tor + IBB: moving forward
Date: Thursday, February 23, 2006 8:26:27 AM

Roger - no doubt you are aware of Oxblood's work:

Ken wrote: Can you tell me about it?

> *Tonight I'm just back from a planning session where we decided on the technical requirements for an anonymous blog publishing system.*
>
> The idea behind anonymous blog publishing system – currently known as Soapbox – is to enable democracy and human rights activists, religious minorities, private citizens, etc., to publish information freely and without fear of being censored.
>
> Rather than trying to get information into firewalled regimes, we're attempting to get it out. Call it data escape. The cut and paste job below is from our working requirements document which needs a bit of tuning up - then a thorough security audit before we move into production.
>
> >>>
> We propose to establish a system that uses The Onion Routing's feature called "Location Hidden Service". Such a hidden service does not run on any public location (no associated IP address or hostname, and while it runs on a normal Internet host, that host's address and where abouts may and should be kept secret), but a pseudonymous address, consisting of a random hash
> ending in .onion, e.g.: http://af923nrna292.onion
>
> TOR clients will understand this URL, which includes any browser using TOR as a web proxy. In this case, the request will internally be re-routed through the TOR network to the location-hidden destination, with neither the client, middle-men or anyone else being able to reliably predict where that destination actually is, due to a cryptographically-enabled protocol feature detailed here [3]. Additionally, the hidden server will not and cannot know the real identity and whereabouts of the client connecting it, due to the nature of this protocol, which additionally protects the client, who will not have to trust the server.
>
> On the technical side, our proposal involves setting up TOR infrastructure nodes and web servers providing blogging and other information distribution services, accessible only as such location-hidden "dot onion" URLs instead of a classical location. The clients will then be provided with a discreet, zero-configuration browser solution, and only need to communicate the URL of the hidden service, even just by word of mouth, to be able to anonymously and discretely publish information to the provided servers who are immune to attack, legal action and filtering or censorship, because their location cannot be pinpointed.
> <<<

From: Ken Berman
To: Roger Dingledine
Cc: [redacted] Kelly DeYoe; [redacted]
Subject: Re: Tor + IBB: moving forward
Date: Friday, February 17, 2006 4:35:05 PM

Looks good, everyone. Ken

Roger Dingledine wrote:

>Results of phone conversation:
>
>Kelly is going to look into what languages we should keep official website
>translations for (Persian, Mandarin, other?). He's also going to keep
>shepherding the statement-of-work and contract forward. Kelly, can you
>forward this mail to Gail(?) too so I have her email address and name?
>
>Hiu and Bennett are going to take a look at
>http://wiki.noreply.org/noreply/TheOnionRouter/WindowsBufferProblems
>and poke at it a bit. This is the number one critical bug in Tor right
>now, and none of the Tor developers use Windows so it's harder to solve.
>If you know anybody who would be good at solving it, please ask them too,
>or try to figure out what else we need to figure out to move forward
>on it.
>
>Hiu is going to learn about the Tor controller protocol:
>http://tor.eff.org/cvs/tor/doc/control-spec.txt
>http://tor.eff.org/cvs/control/doc/howto.txt
>http://tor.eff.org/cvs/control/
>http://tor.eff.org/gui/
>and think about what features are missing and how he might
>want to design an interface for censored Tor users that a) has a
>GUI for people to know that something is happening, configure it,
>etc, and b) can handle a variety of ways of hearing about relay
>addresses. Check out http://freehaven.net/edmanm/torcp/ for what's
>probably the most common Windows Tor controller currently (but it
>has many usability problems). Be sure to use the latest development
>release of Tor when trying things.
>
>Bennett is going to go through the previous email's text (quoted below),
>plus his previous documents, and sketch out a concise-but-detailed :)
>roadmap of the design issues and tradeoffs we'll need to tackle to deploy
>a censorship solution.
>See http://tor.eff.org/cvs/tor/doc/incentives.txt for a work-in-progress
>example or http://tor.eff.org/cvs/tor/doc/dir-spec.txt for a more
>polished example if needed.
>
>Hiu and Bennett should also skim the Blossom page at
>http://afs.eecs.harvard.edu/~goodell/blossom/ for another example
>of a Tor controller that uses more of the protocol's features,
>and demonstrates how Tor's path-building can be separated from
>its network-discovery. Blossom's developer is amenable to helping
>to adapt it for use in the censorship context.
>
>And again, let me know if you have any questions about anything, and
>feel free to tackle anything else you want:
>http://tor.eff.org/volunteer lists some more issues.
>

>Lastly, if you folks are into IRC, you are welcome to listen in on the
>user support channel at #tor on irc.oftc.net, or the secret undocumented
>internal developer's channel at #tor-dev on irc.seul.org.
>
>Thanks,
>--Roger
>
>
>
>On Mon, Feb 13, 2006 at 10:52:19AM -0500, Roger Dingledine wrote:
>
>
>>Hi Bennett, Hiu, Kelly,
>>
>>Here's a mail that has been queueing until I learned more details
>>about our plan. I'd still like to hear from Ken what vision and
>>goals he's hoping for (maybe Kelly can learn this and include it
>>in our upcoming conference call?), but in the meantime, here's an
>>overview of some of the tasks that need to be tackled.
>>
>>My goal here is to see if any of these paragraphs catch your eye. My
>>experience is that people do their best work when they're excited about
>>it, so -- does any of this excite you in particular? We have a lot of
>>different tasks to work on, so whatever you're most interested in is
>>clearly the right thing to work on. Or are there other related things
>>that you think need attention too? I'm open to suggestions.
>>
>>
>>My focus for the next little while is to get the Tor 0.1.1.x release
>>candidate ready. This new Tor version includes a more scalable and secure
>>directory system, and we'll need it in order for the Tor network to grow
>>much larger.
>>
>>After that, my plan is to start focusing on server usability -- how to
>>make all the internals of Tor work correctly if we have a button to
>>sign yourself up as a relay for our alternate Tor network. In addition,
>>we could really use some good simple documentation for how to forward
>>a port through some typical home routers, how to set Tor up, etc. We
>>could also use some help on the Tor GUI that lets people choose to
>>become servers. It's pretty far from having the 'help China' button on
>>it. (In fact, we have no front-end at all for OS X, Linux, etc.)
>>
>>We also need to think about a strategy for how to spin this move in terms
>>of Tor's overall direction. I would guess that we don't want to loudly
>>declare war on China, since this only harms our goals? But we also don't
>>want to hide the existence of funding from IBB, since "they're getting
>>paid off by the feds and they didn't tell anyone" sounds like a bad
>>Slashdot title for a security project. Is it sufficient just to always
>>talk about Iran, or is that not subtle enough?
>>
>>Somewhere in this, we need to keep processing volunteer mail such as the
>>nice people who just translated the Tor site into Chinese and Russian,
>>and keep trying to support server operator questions, and keep trying to
>>find somebody to help with Windows stability, docs, faqs, user support,
>>and so forth.
>>
>>In parallel to this, we're going to need somebody to design a GUI
>>controller for the people who want to be Tor clients but can't make it
>>to the main Tor network directly. The actual back-end talking to the Tor
>>client is pretty easy, but it's probably not good enough to have it in

>>English, and there are a lot of design issues to work out too:
>>
>>We need to enumerate some ways for clients to bootstrap relay IP addresses
>>-- a couple of default addresses just in case they work, a way to manually
>>enter them, the instant-messaging account that Bennett was talking about,
>>receiving them in the mass-mailing spams, and so forth. Once the Tor
>>client knows a few relay IP addresses, it can automatically build the
>>connection and reach the main directory server.
>>
>>...Which also needs to be figured out. I had originally envisioned this
>>as just a little cgi script on a web page somewhere, but now that I think
>>about it more, we probably want some features like being able to check
>>whether a relay is actually working right now. All of that is already
>>working if we use a normal Tor directory server, and we can modify it
>>to not answer requests for the whole directory, and to answer with our
>>special algorithm.
>>
>>...Which brings us to the algorithm for disbursing backup relay
>>addresses. This could vary widely from Bennett's "if they already know the
>>public key then they can lookup the current server descriptor for that
>>key but nothing more" to "we'll give them a couple of random addresses
>>every time they ask for some" to "everybody who asks this hour gets
>>this IP address, and next hour we'll switch to giving out a new one" to
>>"ask them to register pseudonymous accounts and try to build a system
>>to detect which accounts defect". We need to enumerate these options
>>and make a concise list of pros and cons. Remember that we're not just
>>targetting one country, so it may be reasonable to deploy different
>>strategies simultaneously.
>>
>>We'll want to build a plan for bootstrapping the whole thing (if we
>>make it too locked down originally, then we'll end up with no users,
>>and there will be no point). I think it's fine to assume that when we
>>first start out nobody will care, but we need to consider and anticipate
>>some of the transition problems, for example so we avoid letting them
>>enumerate the whole set of relays and destroy the progress we've made
>>once they do start to care.
>>
>>There's clearly more to plan and more to lay out, but hopefully this will
>>get us moving in the right direction. Another topic for the conference
>>call is integrating this discussion into the normal Tor mailing lists
>>so we can do more design out in the open (or at least with a broader
>>set of developers).
>>
>>Thanks,
>>--Roger
>>
>>
>>

From: Roger Dingledine
To: [redacted] Kelly DeYoe
Cc: Ken Berman; [redacted]
Subject: Re: Tor + IBB: moving forward
Date: Thursday, February 16, 2006 5:19:02 PM

Results of phone conversation:

Kelly is going to look into what languages we should keep official website translations for (Persian, Mandarin, other?). He's also going to keep shepherding the statement-of-work and contract forward. Kelly, can you forward this mail to Gail(?) too so I have her email address and name?

Hiu and Bennett are going to take a look at
http://wiki.noreply.org/noreply/TheOnionRouter/WindowsBufferProblems
and poke at it a bit. This is the number one critical bug in Tor right now, and none of the Tor developers use Windows so it's harder to solve. If you know anybody who would be good at solving it, please ask them too, or try to figure out what else we need to figure out to move forward on it.

Hiu is going to learn about the Tor controller protocol:
http://tor.eff.org/cvs/tor/doc/control-spec.txt
http://tor.eff.org/cvs/control/doc/howto.txt
http://tor.eff.org/cvs/control/
http://tor.eff.org/gui/
and think about what features are missing and how he might want to design an interface for censored Tor users that a) has a GUI for people to know that something is happening, configure it, etc, and b) can handle a variety of ways of hearing about relay addresses. Check out http://freehaven.net/edmanm/torcp/ for what's probably the most common Windows Tor controller currently (but it has many usability problems). Be sure to use the latest development release of Tor when trying things.

Bennett is going to go through the previous email's text (quoted below), plus his previous documents, and sketch out a concise-but-detailed :) roadmap of the design issues and tradeoffs we'll need to tackle to deploy a censorship solution.
See http://tor.eff.org/cvs/tor/doc/incentives.txt for a work-in-progress example or http://tor.eff.org/cvs/tor/doc/dir-spec.txt for a more polished example if needed.

Hiu and Bennett should also skim the Blossom page at
http://afs.eecs.harvard.edu/~goodell/blossom/ for another example of a Tor controller that uses more of the protocol's features, and demonstrates how Tor's path-building can be separated from its network-discovery. Blossom's developer is amenable to helping to adapt it for use in the censorship context.

And again, let me know if you have any questions about anything, and feel free to tackle anything else you want:
http://tor.eff.org/volunteer lists some more issues.

Lastly, if you folks are into IRC, you are welcome to listen in on the user support channel at #tor on irc.oftc.net, or the secret undocumented internal developer's channel at #tor-dev on irc.seul.org.

Thanks,
--Roger

On Mon, Feb 13, 2006 at 10:52:19AM -0500, Roger Dingledine wrote:
> Hi Bennett, Hiu, Kelly,
>
> Here's a mail that has been queueing until I learned more details
> about our plan. I'd still like to hear from Ken what vision and
> goals he's hoping for (maybe Kelly can learn this and include it
> in our upcoming conference call?), but in the meantime, here's an
> overview of some of the tasks that need to be tackled.
>
> My goal here is to see if any of these paragraphs catch your eye. My
> experience is that people do their best work when they're excited about
> it, so -- does any of this excite you in particular? We have a lot of
> different tasks to work on, so whatever you're most interested in is
> clearly the right thing to work on. Or are there other related things
> that you think need attention too? I'm open to suggestions.
>
>
> My focus for the next little while is to get the Tor 0.1.1.x release
> candidate ready. This new Tor version includes a more scalable and secure
> directory system, and we'll need it in order for the Tor network to grow
> much larger.
>
> After that, my plan is to start focusing on server usability -- how to
> make all the internals of Tor work correctly if we have a button to
> sign yourself up as a relay for our alternate Tor network. In addition,
> we could really use some good simple documentation for how to forward
> a port through some typical home routers, how to set Tor up, etc. We
> could also use some help on the Tor GUI that lets people choose to
> become servers. It's pretty far from having the 'help China' button on
> it. (In fact, we have no front-end at all for OS X, Linux, etc.)
>
> We also need to think about a strategy for how to spin this move in terms
> of Tor's overall direction. I would guess that we don't want to loudly
> declare war on China, since this only harms our goals? But we also don't
> want to hide the existence of funding from IBB, since "they're getting
> paid off by the feds and they didn't tell anyone" sounds like a bad
> Slashdot title for a security project. Is it sufficient just to always
> talk about Iran, or is that not subtle enough?
>
> Somewhere in this, we need to keep processing volunteer mail such as the
> nice people who just translated the Tor site into Chinese and Russian,
> and keep trying to support server operator questions, and keep trying to
> find somebody to help with Windows stability, docs, faqs, user support,
> and so forth.
>
> In parallel to this, we're going to need somebody to design a GUI
> controller for the people who want to be Tor clients but can't make it
> to the main Tor network directly. The actual back-end talking to the Tor
> client is pretty easy, but it's probably not good enough to have it in
> English, and there are a lot of design issues to work out too:
>
> We need to enumerate some ways for clients to bootstrap relay IP addresses
> -- a couple of default addresses just in case they work, a way to manually
> enter them, the instant-messaging account that Bennett was talking about,
> receiving them in the mass-mailing spams, and so forth. Once the Tor

> client knows a few relay IP addresses, it can automatically build the
> connection and reach the main directory server.
>
> ...Which also needs to be figured out. I had originally envisioned this
> as just a little cgi script on a web page somewhere, but now that I think
> about it more, we probably want some features like being able to check
> whether a relay is actually working right now. All of that is already
> working if we use a normal Tor directory server, and we can modify it
> to not answer requests for the whole directory, and to answer with our
> special algorithm.
>
> ...Which brings us to the algorithm for disbursing backup relay
> addresses. This could vary widely from Bennett's "if they already know the
> public key then they can lookup the current server descriptor for that
> key but nothing more" to "we'll give them a couple of random addresses
> every time they ask for some" to "everybody who asks this hour gets
> this IP address, and next hour we'll switch to giving out a new one" to
> "ask them to register pseudonymous accounts and try to build a system
> to detect which accounts defect". We need to enumerate these options
> and make a concise list of pros and cons. Remember that we're not just
> targetting one country, so it may be reasonable to deploy different
> strategies simultaneously.
>
> We'll want to build a plan for bootstrapping the whole thing (if we
> make it too locked down originally, then we'll end up with no users,
> and there will be no point). I think it's fine to assume that when we
> first start out nobody will care, but we need to consider and anticipate
> some of the transition problems, for example so we avoid letting them
> enumerate the whole set of relays and destroy the progress we've made
> once they do start to care.
>
> There's clearly more to plan and more to lay out, but hopefully this will
> get us moving in the right direction. Another topic for the conference
> call is integrating this discussion into the normal Tor mailing lists
> so we can do more design out in the open (or at least with a broader
> set of developers).
>
> Thanks,
> --Roger
>

From: Roger Dingledine
To: Ken Berman
Cc: [redacted] Kelly DeYoe; Betty Pruitt
Subject: Re: Tor + IBB: moving forward
Date: Friday, March 17, 2006 3:28:53 PM

On Fri, Mar 17, 2006 at 09:25:25AM -0500, Ken Berman wrote:
> but for German, only your home page
> is translated, every second link is back to English.

Really? Much of the site is translated for German. Clicking on things works for me too, e.g. most of the pages on http://tor.eff.org/index.html.de

If you get sent back to English pages from all of these links, can you describe your browser set-up more so I can look into it?

Thanks,
--Roger