From: Roger Dingledine
To: Kelly DeYoe; Ken Berman
Subject: (FWD) Draft proposal for TLS normalization
Date: Tuesday, October 09, 2007 10:10:01 PM

Hi Kelly, Ken,

Here's some reading material for your spare time. This is still an early draft, but it's a fine start I think. The next steps are to nail down exactly what this means we should *do* -- and then do it. :)

--Roger

----- Forwarded message from Steven Murdoch <[redacted] -----

From: Steven Murdoch <[redacted]
To: Tor internal list <[redacted]
Subject: Draft proposal for TLS normalization
Delivery-Date: Sat, 29 Sep 2007 17:36:28 -0400

One of the Oct 1 deliverables is a roadmap for TLS normalization. I have a draft of this for your perusal:

[Username: "[redacted] password: "[redacted] (to keep Google away)]

http://www.cl.cam.ac.uk/~sjm217/volatile/guest/xxx-tls-normalization.txt

The two goals of this are to make our funders happy, and to be useful for actually implementing the TLS normalization. If you have any suggestions on how to do either better, please let me know.

Currently this document is private, but eventually some or all of it should be public. I'll leave this discussion for a later date, but essentially my thought is that while we should not rely on secrecy, it might be a good to delay the release of anything like "this attack is bad; I hope nobody realizes it before we fix it".

NOT RELEASING KNOWN VULNARABILITY WHILE LETTING BBG KNOW ABOUT IT

Steven.

--
w: http://www.cl.cam.ac.uk/users/sjm217/

----- End forwarded message -----

From: Roger Dingledine
To: Eric Johnson; [redacted] Kelly DeYoe; Ken Berman
Cc: [redacted]
Subject: (FWD) Host security while using Tor: possible directions
Date: Sunday, September 14, 2008 5:50:50 AM

And a similar mail from Steven.

--Roger

----- Forwarded message from "Steven J. Murdoch" <[redacted] -----

From: "Steven J. Murdoch" <[redacted]
To: Tor internal list <[redacted]
Subject: Host security while using Tor: possible directions
Delivery-Date: Thu, 11 Sep 2008 07:55:10 -0400

Following up Jacob's email, I have another set of experiences from an recent project to help another non-specific organization in an non-specific country (sorry in advance for the lack of details, and please treat the content of the email as sensitive).

The situation is that this organization believes their outgoing emails are being intercepted and read. They have quite convincing evidence that this is the case, but don't know how it is happening. My suspicion is that they have some host compromises, which are either being used directly or stolen credentials have been used to escalate privilege.

I've given training courses in Kyrgyzstan and Poland, on censorship resistance as part of the OpenNet Initiative, which discussed how to use Tor and related tools. However, the security of these assumes a trustworthy host operating system, which is in many cases not true (at these courses, machines with unpatched Windows 98 were common).

So one question for Tor is whether and how to assist with training and tools on keeping users' PCs secure. Also for people who only have Internet access at Internet cafes, for some countries the situation is that they are probably safe, and in others that we should advise against using Tor (or any other security sensitive software) at all on shared PCs.

The level of attacks will also vary between countries. According to a lecture by Mikko Hypponen of F-Secure, the Tibetan movement is subject to attacks comparable to the state-of-the art in targeted malware (only major banks and defense contractors were subject to attacks of comparable sophistication). There's an example here which mentions names that many of us will be familiar with:

http://www.f-secure.com/weblog/archives/00001494.html

One way to help understand these issues is forensics. Host-based forensics (like anti-virus software) is ultimately a losing battle. A more promising approach, which I discussed with Ethan Zuckerman in 2007, was to build a little box that says who your computer is contacting. It's not foolproof, but it can help defend against certain information-theft attacks.

In the case I mentioned at the start of the email, I'm working with someone who is in the field on investigating the potential compromise. One approach I'd like to try is the network forensics approach. I'll let you know how that works out.

Steven.

--
w: http://www.cl.cam.ac.uk/users/sjm217/

----- End forwarded message -----

From: Roger Dingledine
To: [redacted] Ken Berman; Kelly DeYoe; Sho Ho
Cc: [redacted]
Subject: (FWD) Merci!
Date: Saturday, September 12, 2009 12:48:26 AM

Hi folks,

Here's a note from another happy person in Iran. (Name removed since he didn't seem to want that spread. http://translate.google.com/ will help for the non-French-speakers).

--Roger

----- Forwarded message from ... -----

From: ...
To: [redacted]
Subject: Merci!
Delivery-Date: Sun, 06 Sep 2009 14:50:44 -0400

Bonsoir,
Je vous écris juste pour vous remercier... En ce moment, et depuis 8 mois, je me trouve en Iran. Comme vous devez être au courant, il s'est passé quelques petites choses pas très agréables ici depuis quelques mois. Il se trouve que les méthodes de contrôle commençaient aussi par des choses simples : Les réseaux GSM étaient coupés, les lignes téléphoniques aussi, et internet était non seulement censuré, mais ralenti jusqu'à un débit inférieur au RTC... Alors que j'avais l'ADSL...

Grâce à TOR, je pouvais non seulement aller sur tous les sites web importants pour faire passer certains messages (twitter, facebook, youtube, dailymotion, etc...) mais en plus, j'ignore comment et pourquoi, mais le débit devenait correcte... Si bien que je ne surfe plus qu'avec TOR maintenant!

J'espère que vous êtes conscient du fait que tout un peuple, le peuple Perse se sert de votre logiciel pour communiquer avec l'extérieur, et que le TOR project est devenu pour nous le symbole d'une liberté que nous atteindrons peut être... Sachez que si nous y arrivons, vous n'y serez certainement pas pour rien!

Voilà... C'était juste pour ça! D'ici quelques semaines, je rentrerai en France, et à ce moment là, je m'empresserai d'apporter ma contribution au projet... Financièrement bien entendu (surtout que j'ai vu qu'on peut avoir un T-Shirt!!! ;-)) Et aussi... Avez vous besoin d'un traducteur en Farsi ? Je peux le faire en cas de besoin... Je serai disponible, j'ai un bon niveau aussi bien en Anglais, Français et Perse, et donc si vous avez l'INtention de traduire TOR dans la langue de ceux à qui il a le plus servi, je suis votre homme! ;-)

Encore une fois merci pour tout, et j'espère à bientôt!

Arafel. (Je vous donnerai mon vrai nom quand je serai rentré en France... Là j'avoue que malgré TOR, je sais pas du tout ce que les mollahs sont capables

de faire, et je voudrais pas me faire arrêter à l'aéroport... ;-))

----- End forwarded message -----

FBI
DOJ

From: Roger Dingledine
To: Kelly DeYoe
Cc: Ken Berman
Subject: (FWD) Notes from ITSG meeting, Oct 22-23
Date: Saturday, November 22, 2008 1:19:03 AM

And here are the more details about the FBI conference I told you about. Keeping FBI informed of (and using!) Tor contributes to project and network sustainability.

--Roger

----- Forwarded message from Roger Dingledine <[redacted] -----

Date: Mon, 3 Nov 2008 00:12:18 -0500
From: Roger Dingledine <[redacted]
To: [redacted]
Subject: Notes from ITSG meeting, Oct 22-23

[Please don't spread this document around. The conference was one of those "not for attribution, now we can talk freely" sort of gigs. I figure that means I can summarize it internally.]

On Oct 22-23, I met with about 50 DoJ/FBI agents in San Diego. The context was an "industry and government" conference series they run, which was born out of the CALEA / lawful intercept / key escrow debacles. Now they gather people from industry together twice a year to talk to them early in the process about how law enforcement is going and what capabilities they would benefit from, so industry can put in the backdoors early in the design process when they're still cheap.

I was there on a panel about anonymity with John Bashinski (of Cisco, but before that from Zero-Knowledge Systems) and Christian Grothoff (author of Gnunet, now a CS professor at Denver University). I only got about 20 minutes for my talk, so I focused on "who uses Tor and why -- all the various good uses of an anonymity system". I also put in a slide or two about bad people on the Internet, to counter the traditional "sure, I admit there are good uses, but aren't you destroying the world too?" questions.

The talk was quite well received overall. Most people recognized that Tor has good uses -- in fact, some of the agents in the audience told me they use Tor for their work already. One agent who works in the "innocent images unit" (how's that for a unit title) told me that he uses Tor every day for his work. Recall that I got the same statement from the FBI agent I met with in Indiannapolis. I wonder how we can make better use of these non-attributable quotes.

Another interesting response was "Wow, that was great. There are so many landmines in that topic here, and you managed to avoid them all." I suppose that's a good thing. :)

One of the key points here is the narrow audience they had. I heard many of them say "I'm so glad we get this opportunity to interact with the rest of industry". But the industry representatives were basically Microsoft, Google, Yahoo, AOL, Cisco, and a few others. Not really a good cross-section of the whole community doing innovation. I asked whether they had other outreach conferences (human rights, civil liberties,

hacker con audiences, etc), and the answer was that FBI as a whole probably does, but this particular piece of FBI is focused on this small segment of industry, so that's what outreach means for them.

I also noticed that pretty much all the industry talks contained the phrase "We cooperate fully with the FBI". Boy, that's a phrase we are steering clear of.

I now expect to have invitations from many FBI groups around the east coast to come talk to them in more detail. One of the downsides I'm beginning to realize is the high rate of churn of good technical people at FBI. Once they learn enough useful technical stuff, they can get higher-paying jobs elsewhere. So is my goal of training all the FBI people about Tor and anonymity a losing proposition? Some people say that FBI is really good at maintaining its institutional memory, despite the turnover rate. Need to learn more.

One of the most interesting presentations was on their "Going Dark" initiative. They realize that the amount of darkness (stuff they can't observe with their current mechanisms and plans, e.g. due to encryption or jurisdiction or uncooperative ISPs) is increasing exponentially with time. They proposed some ways to address the darkness, but the industry side of the audience rightly pointed out that each of their points would only be a linear fix -- that is, not really address the problem at all.

Some of them are coming to accept that they need radically different solutions, since trying to claw back the progress of security technology really isn't going to work long-term. Worse, they suffer from the "plus one" effect -- just because a new technology comes out doesn't mean the old one goes away, so the set of technologies they need to know how to observe just keeps going up. The "old style" pre-wiretap approaches are hideously expensive and cumbersome though -- I heard the stat that the whole Bureau can only do something like 350 physical breakin jobs a year. So our concern that a physical attack is just as reasonable as an eavesdropping attack may be off-base, at least with respect to this threat class.

They also confirmed our assumption that law enforcement below the federal level has gone pretty much entirely dark already.

The other informative talk was from the #2 guy in the Bureau. He did the usual "zip in zip out" style of keynote. His talk was full of bold demands like "we must leave no hideouts left on the Internet for bad people". Another statement that stuck in my mind was how our colleagues in the EU have recently rolled out data retention, and he expects to see that in this country "very soon".

Another point I didn't realize was significant until afterwards was his demand that they need to move forward with new monitoring initiatives, and they can't afford to keep waiting until industry standardizes them. Apparently some people in their organization are very upset that the telcom industry has been so slow at coming to standards on how to put in backdoors. One of the Microsoft people there had a fantastic response, which was "hey, we *can't* build something unless it's a standard. The DoJ guys smack us down whenever we try to do that."

Overall, the industry folks I met were pretty realistic about how hard tapping the Internet would be in practice, as well as the likelihood that taps would catch bad people vs good people. They weren't excited at all to deploy any solutions. I got the feeling that a lot of them

were the same people who went through (and won) the crypto wars.

Since I'm not "industry" I'm unlikely to be invited back for another of these conferences, unless they end up with another topic for which I'd be a good speaker. (Alas, I'm pretty much a one-trick pony when it comes to this particular area.) But I do expect to hear back from some of the agents and go talk to their groups in more detail. So if there are any questions or topics you want me to bring up next time I talk to them, please let me know.

--Roger

----- End forwarded message -----

From: Roger Dingledine
To: Ken Berman; Kelly DeYoe
Subject: (FWD) Notes from Jeremiah and CDHR
Date: Wednesday, October 29, 2008 2:15:39 AM

FYI
--Roger

----- Forwarded message from Roger Dingledine <[redacted] -----

Date: Wed, 29 Oct 2008 01:13:29 -0400
From: Roger Dingledine <[redacted]
To: [redacted]
Cc: Jeremiah Young <[redacted]
Subject: Notes from Jeremiah and CDHR

On Oct 21 I met with Jeremiah Young, a junior at UCSD studying polisci. He was a volunteer intern last year for a group in DC called CDHR (cdhr.info), which is a non-profit that focuses on democracy in Saudi Arabia. CDHR is only about five people, and they get their funding from a variety of groups. One of their main goals is to help people in-country realize that there actually are groups who are trying to help, to give them hope and give them a way to coordinate. Their exec dir, Ali, is apparently a really good networker and runs across all sorts of people who want to help. However, they've noticed recently that they have two big deficiencies:
A) They haven't learned much about how technology can help accomplish their goals. In particular, they hadn't really heard of Tor before, and didn't know how to make use of this sort of tool to let people in-country reach the cdhr website.
B) They know approximately zero technical people in-country who can help them train others, spread the word, or report back on the state of government filtering and crackdowns.

I gave Jeremiah a 4-hour tutorial on how Tor works, who uses it and why, what protections it provides and what protections it doesn't provide, and our 'arms race' roadmap including bridges, the idea of TLS network fingerprint detection, etc. He was really excited, and they want to make Tor an integral part of their solutions going forward. They also want to apply for some grants and list us as the consultants who can work with them to make sure Tor continues to work smoothly in Saudi Arabia. He didn't have any details past that, because Ali is the one who'd be doing the applications. I told him we were certainly interested in learning more, and under the right circumstances we'd be happy to be listed in some of their grants. I explained that we're pretty much full up for the next 6-12 months, but that isn't an issue because these grants move very slowly anyway.

I tried to emphasize how important it is for them to start building a network of people they know in-country. First they need this to be able to tell what constraints we'll see in terms of trying to keep Tor working well. But they'll also need it in terms of getting the word out to the right people. Extra points if they meet technical folks there who can train or advise others in the area.

Next step is that Jeremiah is going to try to explain all of this to Ali, and then I guess we'll eventually hear from one of them when they a) have questions, b) have more details about the context they want to

deploy in, or c) have a grant proposal in mind.

--Roger

----- End forwarded message -----

Google + Tor

From: Roger Dingledine
To: Kelly DeYoe
Cc: Ken Berman
Subject: (FWD) Notes from Niels, Google, Tor
Date: Saturday, November 22, 2008 1:14:55 AM

Hi Kelly,

Here's some more reading to keep you informed about the "Google makes you solve a captcha if you're using Tor" issue.

--Roger

----- Forwarded message from Roger Dingledine <[redacted] -----

Date: Wed, 29 Oct 2008 00:54:46 -0400
From: Roger Dingledine <[redacted]
To: [redacted]
Cc: Niels Provos <[redacted]
Subject: Notes from Niels, Google, Tor

Mike, Jake, and I talked to Niels Provos, Google's security guy, about how Google search can become more compatible with Tor. Google keeps giving out captchas (or worse, doesn't offer a captcha and just gives a 403 failure) when Tor users try to query google.

We theorize this problem is happening because some Tor users are scraping Google -- perhaps for competitive analysis by other search engines, perhaps by folks who've seen Johnny Long's talk too many times and want to find lists of vulnerable websites, etc.

If you load a Google page (e.g. the www.google.com frontpage), it will give you a google cookie (this is the one that doesn't expire for decades). If a) you do a search query, b) Google doesn't like your IP address, and c) you provide a google cookie, then it'll give you a captcha to solve. Once you solve the captcha, you get a captcha cookie that shows you're a human. The captcha cookie expires after like 20 minutes.

("google cookie" and "captcha cookie" are my terms, not anything official)

The first problem comes if you do your query directly from Firefox's google search box (in the top right). You never load a google page first, so you never get a google cookie. And if Google hates your IP address, and you don't present a google cookie, then it never even offers a captcha. It just gives you a 403 and that's it.

So there are a couple of problems here:

A) The captcha cookie expiration date is way too short. Niels is going to raise it to something more like 3 hours. He's been meaning to do this for a while anyway, so this change didn't need much prompting.

B) If Torbutton throws away your cookies when you toggle it, as it should, then you're going to risk a 403 with no captcha if you type your query into Firefox's widget rather than visiting www.google.com first. (As an aside, the reason I haven't been seeing this problem is that www.google.com is my Firefox's start page.)

We thought about several solutions for this part. First would be for Torbutton to do an xmlhttp request to www.google.com every time you toggle Tor on. Then you'd get a google cookie, and you would at least be offered a captcha. But this solution means informing Google whenever you toggle Tor -- and worse, you're doing it for the express purpose of having them stick a tracking device on you for the duration of your session. The second idea was to ship Torbutton with a valid google cookie that every Torbutton user would share. This is a better idea, except if one day Google wonders why there's this massive botnet around the world all using the same google cookie, and decides to cancel it. The third idea is for Torbutton to intercept your use of the search widget, check if you have a google cookie already, and if not then stall your search while it touches www.google.com and gets a google cookie for you. This isn't so bad an idea, except it may be ugly to implement.

C) But it gets worse. There are a dozen or more google domains around the world, and "www.google.com" could send a 302 redirect to any of them depending on geography. The current working theory is that each of these domains like google.ca demands its own separate google cookie. So do we ship with 30 google cookies that all users share like option two above? Do we do option three (the stall-and-fetch-cookie trick) once for each google domain for each browsing session? It seems the better answer is to pick one google domain that Torbutton uses. We could do that by intercepting the 302 and then rewriting our query to use our preferred google domain rather than the one they provide. Mike rather likes google.ca as his ideal google.

(Before we go to these lengths, Mike is going to check if a cookie valid for google.ca is also valid for google.de. If so, we could simplify things by just keeping a cookie for one google domain, and presenting it for the others too. (Cross-domain vulnerabilities, what cross-domain vulnerabilities.) Presumably this trick is fragile because Google does, or should, prevent it by including the domain in its keyed hash.)

If we get our 'intercept 302 and always send towards one google domain' design going, we could later complexify it by offering a pull-down menu in Torbutton so the user can prefer e.g. google.com.hk instead.

Lastly, Niels wants me to come give a talk at Google about Tor, including this issue, to maybe drum up more support for having Google interoperate better with Tor. I think I'm not going to try to squeeze that into my mid November trip, but rather do it a few months after that. That delay will also give us time to play around with the above solutions and get some insight into what the next roadblock will be.

--Roger

----- End forwarded message -----

FALUN GUNG / TOR / STATE DEPT

From: Roger Dingledine
To: Eric Johnson; Christopher Walker; Persephone Miel; Ken Berman; Kelly DeYoe
Cc: [redacted]
Subject: (FWD) Notes from Shiyu Zhou meeting
Date: Friday, December 12, 2008 1:55:51 PM

[I'm sending this to both Sesawe people and BBG people. Feel free to strip off whichever cc's you're nervous about when replying.]

Here's a summary of my November meeting with Shiyu.

The more interesting summary (not written below) is that he spent a short while ranting about the State Dept money and how the State Dept people are too scared to actually put the money where it would make a difference, and apparently they prefer to give it to some group that is going to maintain the status quo.

He seemed to genuinely not know that Tor was receiving some of the DRL money. My sense was that he isn't a good enough actor to be secretly aware of the details of the grant but be talking about it like that anyway.

He started the meeting thinking Tor was just some tiny volunteer project.

I followed Eric's request and didn't talk about our role in the DRL grant at all. I talked a lot about our other funders (IBB, NRL, Google, etc) and why each of them cares about Tor. Hopefully he won't later learn the details about DRL and decide to hate me for not being clear with him.

Yay politics,
--Roger

----- Forwarded message from Roger Dingledine <[redacted]> -----

Date: Fri, 12 Dec 2008 13:41:52 -0500
From: Roger Dingledine <[redacted]>
To: [redacted]
Subject: Notes from Shiyu Zhou meeting

On Nov 4 I met with Shiyu Zhou in NYC. He's a nice fellow who lives in NYC, after being a CS professor in Philly for a while. He moved to the States in '91 after experiencing the Tiananman massacre. Around that time his father, a high-ranking government official, also got really sick, and found a fine new government-approved health practice that seemed to be working for him. Until suddenly Falun Gong was outlawed and his father ended up in house arrest, with now a very limited life.

Now Shiyu lives in NYC, doing human rights work for various groups including a television station there. He works with a variety of the member groups of GIFC (Global Internet Freedom Consortium), which work on various circumvention tools to let Falun Gong members in China communicate with each other and with the outside world. They send out mass mailings into China (in fact, our friends at IBB fund them for that), and they've accumulated a lot of wisdom about how the arms race proceeds once you really catch the attention of a a well-funded adversary.

I gave him the quick version of the same talk I gave Jeremiah from CDHR a few weeks before. I tried to emphasize the many different uses that people find for Tor, and the improved sustainability that the project

gets from the diversity of users and funders. I also tried to emphasize that Tor's security and sustainability comes from transparency -- we want to explain exactly how it works to everybody, yet still remain secure.

He didn't seem to care much about the non-circumvention uses or users for Tor. Regarding our circumvention arms race plans, he said they seemed reasonable, but he really wanted us to learn from what the other members of GIFC have learned. I told him I'd already met Bill Xia in Oxford (Bill runs Dynaweb in North Carolina), but I'd love to meet with more of the technical people in their consortium, and to hear more details about how their tools work. Nothing has come of that yet; I just sent him a followup mail.

He thought the cutoff for getting really noticed by the Chinese government is around 100K users.

We concluded with a "yay more circumvention tools, the more the better" agreement.

--Roger

----- End forwarded message -----

DRP Belarus

From: Roger Dingledine
To: Ken Berman; Kelly DeYoe; Sho Ho
Cc: [redacted] [redacted]
Subject: (FWD) Re: [liberationtech] belarus opposition site hijacking
Date: Monday, December 20, 2010 2:37:43 AM

Another success for Tor. It's a shame there are so many places these days where Tor is useful, but it's good that the censors in most of these places don't know what Tor is.

--Roger

----- Forwarded message from Evgeny Morozov <[redacted]> -----

From: Evgeny Morozov <[redacted]>
To: "[redacted]" <[redacted]>
Subject: Re: [liberationtech] belarus opposition site hijacking
Delivery-Date: Sun, 19 Dec 2010 11:02:25 -0500

I'm in Belarus right now and can confirm that the redirects were, indeed, taking place for some time. It also seems that https is blocked. Tor's site is not blocked and Tor is working fine.

On Sun, Dec 19, 2010 at 3:45 PM, Hal Roberts <[redacted]> wrote:

> Hi All,
>
> I've written up a report today about opposition sites in Belarus being
> hijacked with redirects to fake (presumably government controlled) versions
> by BELPAK, the national ISP:
>
>
> http://blogs.law.harvard.edu/hroberts/2010/12/19/independent-media-sites-in-belarus-reportedly-hijacked-during-election/
>
> I'm taking the redirects on faith according to a report by a digital
> activist that I trust, but you can see the faked sites with almost identical
> domain names yourself, as well as that the fake sites are all hosted within
> IP addresses owned by BELPAK. He is also reporting some DDoS attacks and
> that international ports 443 and 465 are currently being blocked.
>
> -hal
>
> --
> Hal Roberts
> Fellow
> Berkman Center for Internet & Society
> Harvard University
> [redacted]
> [redacted]

liberationtech mailing list
[redacted]

----- End forwarded message -----

China

From: Roger Dingledine
To: Ken Berman; Kelly DeYoe; Sho Ho
Cc: [redacted]
Subject: (FWD) Re: Debugging Tor in China
Date: Friday, September 25, 2009 6:00:04 AM

The second of three mails with some more technical details.

--Roger

----- Forwarded message from Roger Dingledine <[redacted] -----

From: Roger Dingledine <[redacted]
To: [redacted]
Subject: Re: Debugging Tor in China
Delivery-Date: Thu, 24 Sep 2009 23:28:20 -0400

On Thu, Sep 24, 2009 at 06:23:48PM -0400, Roger Dingledine wrote:
> So the next step is to go through our bridge lists, and figure out how
> many of them are actually blocked from this Ubuntu box. Nick is working
> on some scripts to automate that testing.

Ok. Nick wrote up some magic scripts, and I ran them both on comcast and in Beijing, both on the bridge list and on the public relay list.

Out of the 1538 Running public Tor relays, my comcast found 1430 of them to be reachable. On the other hand, the China node found 240 of them to be reachable. My guess is that they took a snapshot of the directory a couple of days ago, and 15% of it has changed since then. Alas, while 15% in a few days seems like a good trend, most of the fast and stable relays probably will keep the same (blocked) IP address over time.

Out of the 335 Running bridges, my comcast found 321 to be reachable. China on the other hand found 208 of them to be reachable. So the good news is that 2/3 of our bridges are still unblocked.

Which leads to the next question: how did they block some but not others? Did they make a bunch of gmail accounts? Look at bridges.tp.o from a bunch of different network locations? Something else?

My early looks at our bridgedb logs (which bridges are in which buckets) show that the bridges you can get via http are mostly blocked, and the bridges you can get via gmail are not blocked. Perhaps they paid a lot of people to exhaustively fetch bridge addresses via https://bridges.torproject.org/, and then thought they were done, without realizing that we split bridge addresses up so defeating one strategy doesn't mean you learn every bridge.

So what does this mean? Use bridges, and get them via gmail, and your Tor will work fine.

Well, not totally fine. Here's another side effect we hadn't anticipated: you can't visit websites in China via Tor anymore, if the exit relay you pick is null-routed by GFW.

--Roger

----- End forwarded message -----

China 58

From:	Roger Dingledine
To:	Ken Berman; Kelly DeYoe; Sho Ho
Cc:	[redacted]
Subject:	(FWD) Re: Debugging Tor in China
Date:	Friday, September 25, 2009 6:04:59 AM

The third of three mails.

It would be great to have your advice on these strategy questions.

--Roger

----- Forwarded message from Roger Dingledine <[redacted]> -----

From: Roger Dingledine <[redacted]>
To: [redacted]
Subject: Re: Debugging Tor in China
Delivery-Date: Fri, 25 Sep 2009 04:47:52 -0400

On Thu, Sep 24, 2009 at 11:28:04PM -0400, Roger Dingledine wrote:
> So what does this mean? Use bridges, and get them via gmail, and your
> Tor will work fine.

We have a couple of strategy choices to make. Isaac, I'd love to have your input on these.

A) How loudly do we tell people that getting bridges via gmail still works? It seems clear that we should tell people like Isaac and Nathan, and let them do with the information what they will. Do we blog about it? Tell people on IRC?

B) More generally, should we scramble before Oct 1 to put out a new version of Tor that has some directory authorities at new addresses, ask the fast entry guards to get a different IP address, etc? We could show the world that we can't be stopped that easily. Or should we just let Tor be blocked for a week, and then fix things afterwards? Which approach would our users in China prefer? Which approach would get us more users in China later? If we lie low, are they more likely to remove the IP address filters later? We probably can go through the process of encouraging everybody to change IP addresses once or twice a year, but not every month.

C) Right now https://bridges.torproject.org/ is offering mostly blocked bridges. So if you ask for bridges that way, you'll probably be sad. We could go through and remove the ones that are blocked, so the remaining ones work. But that makes it easier for the censors to just clean up the few that they missed. Eventually we will want to weed out the bad ones, but how urgently should we do that? Or said another way, are the censors all done for now or will they do another round of filtering before Oct 1?

D) Mike Perry suggested that we should add some more IP:port combinations to the answers you get from https://bridges.torproject.org/ -- things like 64.4.241.45:443 (paypal) and other common ssl websites. There would be two goals: 1) raising the cost of blocking bridge addresses, since you have to check that it isn't a "real" site first. 2) Punish them if they slip up by having them block a site that they wouldn't have wanted to block. Are there such sites, or would they all just count as acceptable

collateral damage? For example, I wouldn't want to put 66.249.80.83:443 (gmail) on the list.

E) Do we want to change Tonga's address? It's our bridge authority, and it got blocked -- and probably because it was a public relay, not because it was a bridge authority. Next time we should come up with an IP address that isn't the same address that Tonga publishes to the directory. Here we have the same question as B: eventually we should do this, but now or in two weeks?

F) Nick wrote a great little Python tool called marco.py that takes in a cached-consensus file and tells you which relays are unreachable and why. We could give that out to people, and they could use it to find public relays that aren't blocked for them. Then they could configure those relays to be their bridges, and voila, their Tor works. Except, giving this script out means giving it to the bad guys too. Will it help them much, or are they already smart and technically skilled and just haven't messed with Tor yet for other reasons?

Thanks,
--Roger

----- End forwarded message -----

From: Roger Dingledine
To: [redacted] (b) (6) Kelly DeYoe; Ken Berman
Subject: (FWD) Re: tor geoip stats
Date: Friday, September 28, 2007 7:45:20 PM

Hi folks,

Here's my latest round of stat-gathering. Make of it what you will, or
let me know if you want me to dig into a particular issue more deeply. :)

--Roger

----- Forwarded message from Roger Dingledine <[redacted] (b) (6) -----

Date: Fri, 28 Sep 2007 18:34:43 -0400
From: Roger Dingledine <[redacted] (b) (6)
Subject: Re: tor geoip stats

Here are some very rough stats on current Tor usage. The algorithms for
how Tor clients pick directory mirrors have changed, so we're getting a
different sample size -- my guess is a slightly larger sample than before.
So while a sample of 58328 clients in 24 hours seems a lot larger than
the February sample of 32031, it's hard to say if this represents much
growth in the size of the overall Tor user community. It is clear that
use in China in particular has continued to increase, though, and that
Tor use has become less US-centric.

We also see the trend of 132 countries represented, compared to 125 in
February and 109 last October. But again, it's hard to make that precise
since the geoip db I used isn't good with tiny countries.

We also see a drop in Saudia Arabian and especially Arab Emirates users,
now that those countries have updated their Smartfilter to block Tor
directory requests by default. It's less clear from these numbers how
much of that is happening in Iran too.

Let me know if you have questions.

Sep 28 17:09:35.946 [notice] 58328 Total
Sep 28 17:09:35.946 [notice] 12208 US (20.930%)
Sep 28 17:09:35.946 [notice] 11107 CN (19.042%)
Sep 28 17:09:35.946 [notice] 10650 DE (18.259%)
Sep 28 17:09:35.946 [notice] 2163 IT (3.708%)
Sep 28 17:09:35.946 [notice] 2158 FR (3.700%)
Sep 28 17:09:35.946 [notice] 1850 GB (3.172%)
Sep 28 17:09:35.946 [notice] 1339 JP (2.296%)
Sep 28 17:09:35.946 [notice] 1279 PL (2.193%)
Sep 28 17:09:35.946 [notice] 1103 CA (1.891%)
Sep 28 17:09:35.946 [notice] 895 ES (1.534%)
Sep 28 17:09:35.946 [notice] 778 AU (1.334%)
Sep 28 17:09:35.946 [notice] 762 RU (1.306%)
Sep 28 17:09:35.946 [notice] 761 BR (1.305%)
Sep 28 17:09:35.946 [notice] 701 SE (1.202%)
Sep 28 17:09:35.946 [notice] 654 AT (1.121%)
Sep 28 17:09:35.946 [notice] 627 NL (1.075%)
Sep 28 17:09:35.946 [notice] 583 Unknown (1.000%) (mostly Africa)
Sep 28 17:09:35.947 [notice] 506 CH (0.868%)
Sep 28 17:09:35.947 [notice] 468 TW (0.802%)

Sep 28 17:09:35.947 [notice] 386 NO (0.662%)
Sep 28 17:09:35.947 [notice] 375 IR (0.643%)
Sep 28 17:09:35.947 [notice] 328 TR (0.562%)
Sep 28 17:09:35.947 [notice] 324 BE (0.555%)
Sep 28 17:09:35.947 [notice] 316 MX (0.542%)
Sep 28 17:09:35.947 [notice] 308 FI (0.528%)
Sep 28 17:09:35.947 [notice] 294 TH (0.504%)
Sep 28 17:09:35.947 [notice] 292 DK (0.501%)
Sep 28 17:09:35.947 [notice] 290 CZ (0.497%)
Sep 28 17:09:35.947 [notice] 275 AR (0.471%)
Sep 28 17:09:35.947 [notice] 255 RO (0.437%)
Sep 28 17:09:35.947 [notice] 255 IN (0.437%)
Sep 28 17:09:35.947 [notice] 245 IL (0.420%)
Sep 28 17:09:35.947 [notice] 237 SG (0.406%)
Sep 28 17:09:35.947 [notice] 225 PT (0.386%)
Sep 28 17:09:35.947 [notice] 210 MY (0.360%)
Sep 28 17:09:35.947 [notice] 203 HK (0.348%)
Sep 28 17:09:35.947 [notice] 168 UA (0.288%)
Sep 28 17:09:35.947 [notice] 167 HU (0.286%)
Sep 28 17:09:35.947 [notice] 165 GR (0.283%)
Sep 28 17:09:35.948 [notice] 139 CL (0.238%)
Sep 28 17:09:35.948 [notice] 130 SA (0.223%)
Sep 28 17:09:35.948 [notice] 130 VN (0.223%)
Sep 28 17:09:35.948 [notice] 130 PH (0.223%)
Sep 28 17:09:35.948 [notice] 121 NZ (0.207%)
Sep 28 17:09:35.948 [notice] 112 IE (0.192%)
Sep 28 17:09:35.948 [notice] 106 SK (0.182%)
Sep 28 17:09:35.948 [notice] 97 BG (0.166%)
Sep 28 17:09:35.948 [notice] 88 SI (0.151%)
Sep 28 17:09:35.948 [notice] 84 LT (0.144%)
Sep 28 17:09:35.948 [notice] 81 CO (0.139%)
Sep 28 17:09:35.948 [notice] 80 VE (0.137%)
Sep 28 17:09:35.948 [notice] 74 CS (0.127%)
Sep 28 17:09:35.948 [notice] 73 HR (0.125%)
Sep 28 17:09:35.948 [notice] 65 KR (0.111%)
Sep 28 17:09:35.948 [notice] 58 ID (0.099%)
Sep 28 17:09:35.948 [notice] 53 PE (0.091%)
Sep 28 17:09:35.948 [notice] 47 BY (0.081%)
Sep 28 17:09:35.948 [notice] 43 EE (0.074%)
Sep 28 17:09:35.948 [notice] 39 KW (0.067%)
Sep 28 17:09:35.948 [notice] 37 LV (0.063%)
Sep 28 17:09:35.948 [notice] 37 PK (0.063%)
Sep 28 17:09:35.949 [notice] 36 QA (0.062%)
Sep 28 17:09:35.949 [notice] 31 LU (0.053%)
Sep 28 17:09:35.949 [notice] 31 CR (0.053%)
Sep 28 17:09:35.949 [notice] 23 UY (0.039%)
Sep 28 17:09:35.949 [notice] 23 MD (0.039%)
Sep 28 17:09:35.949 [notice] 22 GT (0.038%)
Sep 28 17:09:35.949 [notice] 22 AE (0.038%)
Sep 28 17:09:35.949 [notice] 21 RS (0.036%)
Sep 28 17:09:35.949 [notice] 20 SV (0.034%)
Sep 28 17:09:35.949 [notice] 19 PR (0.033%)
Sep 28 17:09:35.949 [notice] 18 DO (0.031%)
Sep 28 17:09:35.949 [notice] 18 JO (0.031%)
Sep 28 17:09:35.949 [notice] 17 CY (0.029%)
Sep 28 17:09:35.949 [notice] 15 MT (0.026%)
Sep 28 17:09:35.949 [notice] 14 EC (0.024%)
Sep 28 17:09:35.950 [notice] 12 PY (0.021%)
Sep 28 17:09:35.950 [notice] 12 MK (0.021%)
Sep 28 17:09:35.950 [notice] 11 UZ (0.019%)

Sep 28 17:09:35.950 [notice] 11 PA (0.019%)
Sep 28 17:09:35.950 [notice] 11 IS (0.019%)
Sep 28 17:09:35.950 [notice] 11 PS (0.019%)
Sep 28 17:09:35.950 [notice] 10 MO (0.017%)
Sep 28 17:09:35.950 [notice] 9 YE (0.015%)
Sep 28 17:09:35.950 [notice] 8 LB (0.014%)
Sep 28 17:09:35.950 [notice] 8 KZ (0.014%)
Sep 28 17:09:35.950 [notice] 8 AZ (0.014%)
Sep 28 17:09:35.950 [notice] 8 BD (0.014%)
Sep 28 17:09:35.950 [notice] 8 BO (0.014%)
Sep 28 17:09:35.950 [notice] 7 LK (0.012%)
Sep 28 17:09:35.950 [notice] 7 BB (0.012%)
Sep 28 17:09:35.950 [notice] 7 BH (0.012%)
Sep 28 17:09:35.950 [notice] 7 BN (0.012%)
Sep 28 17:09:35.950 [notice] 7 GE (0.012%)
Sep 28 17:09:35.951 [notice] 6 BA (0.010%)
Sep 28 17:09:35.951 [notice] 6 JM (0.010%)
Sep 28 17:09:35.951 [notice] 6 NI (0.010%)
Sep 28 17:09:35.951 [notice] 5 OM (0.009%)
Sep 28 17:09:35.951 [notice] 5 CU (0.009%)
Sep 28 17:09:35.951 [notice] 5 BS (0.009%)
Sep 28 17:09:35.951 [notice] 5 SY (0.009%)
Sep 28 17:09:35.951 [notice] 5 MC (0.009%)
Sep 28 17:09:35.951 [notice] 4 IQ (0.007%)
Sep 28 17:09:35.951 [notice] 4 LI (0.007%)
Sep 28 17:09:35.951 [notice] 4 FJ (0.007%)
Sep 28 17:09:35.951 [notice] 3 AX (0.005%)
Sep 28 17:09:35.951 [notice] 3 TT (0.005%)
Sep 28 17:09:35.951 [notice] 3 GU (0.005%)
Sep 28 17:09:35.951 [notice] 3 AM (0.005%)
Sep 28 17:09:35.951 [notice] 2 MN (0.003%)
Sep 28 17:09:35.951 [notice] 2 NG (0.003%)
Sep 28 17:09:35.951 [notice] 2 LA (0.003%)
Sep 28 17:09:35.951 [notice] 2 NP (0.003%)
Sep 28 17:09:35.951 [notice] 2 DZ (0.003%)
Sep 28 17:09:35.951 [notice] 2 AL (0.003%)
Sep 28 17:09:35.951 [notice] 2 AN (0.003%)
Sep 28 17:09:35.952 [notice] 2 AG (0.003%)
Sep 28 17:09:35.952 [notice] 2 ME (0.003%)
Sep 28 17:09:35.952 [notice] 2 SB (0.003%)
Sep 28 17:09:35.952 [notice] 1 VI (0.002%)
Sep 28 17:09:35.952 [notice] 1 MV (0.002%)
Sep 28 17:09:35.952 [notice] 1 GI (0.002%)
Sep 28 17:09:35.952 [notice] 1 BT (0.002%)
Sep 28 17:09:35.952 [notice] 1 AF (0.002%)
Sep 28 17:09:35.952 [notice] 1 PF (0.002%)
Sep 28 17:09:35.952 [notice] 1 AD (0.002%)
Sep 28 17:09:35.952 [notice] 1 KH (0.002%)
Sep 28 17:09:35.952 [notice] 1 HN (0.002%)
Sep 28 17:09:35.952 [notice] 1 KI (0.002%)
Sep 28 17:09:35.952 [notice] 1 GL (0.002%)
Sep 28 17:09:35.952 [notice] 1 UG (0.002%)
Sep 28 17:09:35.952 [notice] 1 KE (0.002%)
Sep 28 17:09:35.952 [notice] 1 MP (0.002%)
Sep 28 17:09:35.952 [notice] 1 SM (0.002%)

On Thu, Feb 08, 2007 at 04:04:40PM -0500, Roger Dingledine wrote:
> Another day in the life of a typical Tor server. I quote the
> previous data point below, for comparison.
>

> Feb 08 15:42:44.360 [notice] 32031 Total IPs seen:
> Feb 08 15:42:44.361 [notice] 8988 US (28.060%)
> Feb 08 15:42:44.361 [notice] 5415 DE (16.905%)
> Feb 08 15:42:44.361 [notice] 3054 CN (9.535%)
> Feb 08 15:42:44.361 [notice] 1461 FR (4.561%)
> Feb 08 15:42:44.361 [notice] 1229 JP (3.837%)
> Feb 08 15:42:44.361 [notice] 1142 IT (3.565%)
> Feb 08 15:42:44.361 [notice] 1089 GB (3.400%)
> Feb 08 15:42:44.361 [notice] 953 CA (2.975%)
> Feb 08 15:42:44.361 [notice] 649 PL (2.026%)
> Feb 08 15:42:44.361 [notice] 486 SE (1.517%)
> Feb 08 15:42:44.361 [notice] 468 NL (1.461%)
> Feb 08 15:42:44.361 [notice] 419 ES (1.308%)
> Feb 08 15:42:44.361 [notice] 417 AU (1.302%)
> Feb 08 15:42:44.361 [notice] 397 RU (1.239%)
> Feb 08 15:42:44.361 [notice] 390 IR (1.218%)
> Feb 08 15:42:44.361 [notice] 344 AT (1.074%)
> Feb 08 15:42:44.361 [notice] 323 CH (1.008%)
> Feb 08 15:42:44.361 [notice] 311 AE (0.971%)
> Feb 08 15:42:44.361 [notice] 309 SA (0.965%)
> Feb 08 15:42:44.361 [notice] 305 BR (0.952%)
> Feb 08 15:42:44.361 [notice] 285 TW (0.890%)
> Feb 08 15:42:44.361 [notice] 239 FI (0.746%)
> Feb 08 15:42:44.361 [notice] 185 TR (0.578%)
> Feb 08 15:42:44.361 [notice] 183 NO (0.571%)
> Feb 08 15:42:44.361 [notice] 182 Unknown (0.568%)
> Feb 08 15:42:44.361 [notice] 153 BE (0.478%)
> Feb 08 15:42:44.361 [notice] 148 IL (0.462%)
> Feb 08 15:42:44.361 [notice] 147 TH (0.459%)
> Feb 08 15:42:44.361 [notice] 124 CZ (0.387%)
> Feb 08 15:42:44.361 [notice] 118 MX (0.368%)
> Feb 08 15:42:44.361 [notice] 117 PT (0.365%)
> Feb 08 15:42:44.361 [notice] 112 DK (0.350%)
> Feb 08 15:42:44.361 [notice] 109 RO (0.340%)
> Feb 08 15:42:44.361 [notice] 108 SG (0.337%)
> Feb 08 15:42:44.361 [notice] 96 AR (0.300%)
> Feb 08 15:42:44.361 [notice] 95 GR (0.297%)
> Feb 08 15:42:44.361 [notice] 90 MY (0.281%)
> Feb 08 15:42:44.361 [notice] 90 IN (0.281%)
> Feb 08 15:42:44.361 [notice] 90 HK (0.281%)
> Feb 08 15:42:44.361 [notice] 85 HU (0.265%)
> Feb 08 15:42:44.361 [notice] 73 UA (0.228%)
> Feb 08 15:42:44.361 [notice] 73 NZ (0.228%)
> Feb 08 15:42:44.361 [notice] 69 SK (0.215%)
> Feb 08 15:42:44.361 [notice] 66 BG (0.206%)
> Feb 08 15:42:44.361 [notice] 59 SI (0.184%)
> Feb 08 15:42:44.361 [notice] 57 IE (0.178%)
> Feb 08 15:42:44.361 [notice] 51 PH (0.159%)
> Feb 08 15:42:44.361 [notice] 44 HR (0.137%)
> Feb 08 15:42:44.361 [notice] 40 QA (0.125%)
> Feb 08 15:42:44.361 [notice] 37 CL (0.116%)
> Feb 08 15:42:44.361 [notice] 37 KR (0.116%)
> Feb 08 15:42:44.361 [notice] 33 EE (0.103%)
> Feb 08 15:42:44.361 [notice] 32 VN (0.100%)
> Feb 08 15:42:44.361 [notice] 32 LT (0.100%)
> Feb 08 15:42:44.361 [notice] 27 VE (0.084%)
> Feb 08 15:42:44.361 [notice] 27 KW (0.084%)
> Feb 08 15:42:44.361 [notice] 24 CO (0.075%)
> Feb 08 15:42:44.361 [notice] 24 LV (0.075%)
> Feb 08 15:42:44.361 [notice] 20 PR (0.062%)

> Feb 08 15:42:44.361 [notice] 20 LU (0.062%)
> Feb 08 15:42:44.362 [notice] 19 PE (0.059%)
> Feb 08 15:42:44.362 [notice] 18 CS (0.056%)
> Feb 08 15:42:44.362 [notice] 17 ID (0.053%)
> Feb 08 15:42:44.362 [notice] 17 BY (0.053%)
> Feb 08 15:42:44.362 [notice] 11 CR (0.034%)
> Feb 08 15:42:44.362 [notice] 11 PK (0.034%)
> Feb 08 15:42:44.362 [notice] 10 OM (0.031%)
> Feb 08 15:42:44.362 [notice] 9 UY (0.028%)
> Feb 08 15:42:44.362 [notice] 9 GT (0.028%)
> Feb 08 15:42:44.362 [notice] 8 JO (0.025%)
> Feb 08 15:42:44.362 [notice] 8 MD (0.025%)
> Feb 08 15:42:44.362 [notice] 7 CY (0.022%)
> Feb 08 15:42:44.362 [notice] 6 EC (0.019%)
> Feb 08 15:42:44.362 [notice] 6 UZ (0.019%)
> Feb 08 15:42:44.362 [notice] 5 DO (0.016%)
> Feb 08 15:42:44.362 [notice] 5 BH (0.016%)
> Feb 08 15:42:44.362 [notice] 5 MK (0.016%)
> Feb 08 15:42:44.362 [notice] 5 IS (0.016%)
> Feb 08 15:42:44.362 [notice] 5 KZ (0.016%)
> Feb 08 15:42:44.362 [notice] 5 PA (0.016%)
> Feb 08 15:42:44.362 [notice] 5 DZ (0.016%)
> Feb 08 15:42:44.362 [notice] 4 PS (0.012%)
> Feb 08 15:42:44.362 [notice] 4 SY (0.012%)
> Feb 08 15:42:44.362 [notice] 4 SV (0.012%)
> Feb 08 15:42:44.362 [notice] 4 MC (0.012%)
> Feb 08 15:42:44.362 [notice] 4 CU (0.012%)
> Feb 08 15:42:44.362 [notice] 3 BN (0.009%)
> Feb 08 15:42:44.362 [notice] 3 BO (0.009%)
> Feb 08 15:42:44.362 [notice] 3 PF (0.009%)
> Feb 08 15:42:44.362 [notice] 3 NI (0.009%)
> Feb 08 15:42:44.362 [notice] 3 BA (0.009%)
> Feb 08 15:42:44.362 [notice] 3 NC (0.009%)
> Feb 08 15:42:44.362 [notice] 3 MO (0.009%)
> Feb 08 15:42:44.362 [notice] 3 LK (0.009%)
> Feb 08 15:42:44.362 [notice] 2 MN (0.006%)
> Feb 08 15:42:44.362 [notice] 2 AN (0.006%)
> Feb 08 15:42:44.362 [notice] 2 GU (0.006%)
> Feb 08 15:42:44.362 [notice] 2 LA (0.006%)
> Feb 08 15:42:44.362 [notice] 2 YE (0.006%)
> Feb 08 15:42:44.362 [notice] 2 GE (0.006%)
> Feb 08 15:42:44.362 [notice] 2 MT (0.006%)
> Feb 08 15:42:44.362 [notice] 2 LB (0.006%)
> Feb 08 15:42:44.362 [notice] 2 BS (0.006%)
> Feb 08 15:42:44.362 [notice] 2 VI (0.006%)
> Feb 08 15:42:44.362 [notice] 2 TD (0.006%)
> Feb 08 15:42:44.362 [notice] 2 KY (0.006%)
> Feb 08 15:42:44.362 [notice] 1 AW (0.003%)
> Feb 08 15:42:44.362 [notice] 1 RS (0.003%)
> Feb 08 15:42:44.362 [notice] 1 FJ (0.003%)
> Feb 08 15:42:44.362 [notice] 1 HN (0.003%)
> Feb 08 15:42:44.362 [notice] 1 VC (0.003%)
> Feb 08 15:42:44.362 [notice] 1 AG (0.003%)
> Feb 08 15:42:44.362 [notice] 1 UG (0.003%)
> Feb 08 15:42:44.362 [notice] 1 MV (0.003%)
> Feb 08 15:42:44.362 [notice] 1 IQ (0.003%)
> Feb 08 15:42:44.362 [notice] 1 PY (0.003%)
> Feb 08 15:42:44.362 [notice] 1 BD (0.003%)
> Feb 08 15:42:44.362 [notice] 1 AZ (0.003%)
> Feb 08 15:42:44.362 [notice] 1 LI (0.003%)

> Feb 08 15:42:44.362 [notice] 1 AL (0.003%)
> Feb 08 15:42:44.362 [notice] 1 BB (0.003%)
> Feb 08 15:42:44.362 [notice] 1 ZA (0.003%)
> Feb 08 15:42:44.362 [notice] 1 SM (0.003%)
> Feb 08 15:42:44.362 [notice] 1 MA (0.003%)
> Feb 08 15:42:44.362 [notice] 1 MQ (0.003%)
> Feb 08 15:42:44.362 [notice] 1 TT (0.003%)
> Feb 08 15:42:44.362 [notice] 1 LC (0.003%)
>
> On Sat, Oct 14, 2006 at 06:49:13AM -0400, Roger Dingledine wrote:
> > Here are some preliminary results for a day (24 hours) in the life of
> > a typical Tor server:
> >
> > Oct 14 06:30:53.339 [notice] 20430 Total IPs seen:
> > Oct 14 06:30:53.339 [notice] 6256 US (30.622%)
> > Oct 14 06:30:53.339 [notice] 3021 DE (14.787%)
> > Oct 14 06:30:53.339 [notice] 2401 CN (11.752%)
> > Oct 14 06:30:53.339 [notice] 897 JP (4.391%)
> > Oct 14 06:30:53.339 [notice] 868 FR (4.249%)
> > Oct 14 06:30:53.339 [notice] 701 GB (3.431%)
> > Oct 14 06:30:53.339 [notice] 658 CA (3.221%)
> > Oct 14 06:30:53.339 [notice] 656 IT (3.211%)
> > Oct 14 06:30:53.339 [notice] 306 SE (1.498%)
> > Oct 14 06:30:53.339 [notice] 305 AU (1.493%)
> > Oct 14 06:30:53.339 [notice] 303 NL (1.483%)
> > Oct 14 06:30:53.339 [notice] 238 RU (1.165%)
> > Oct 14 06:30:53.339 [notice] 230 AE (1.126%)
> > Oct 14 06:30:53.339 [notice] 222 ES (1.087%)
> > Oct 14 06:30:53.339 [notice] 213 AT (1.043%)
> > Oct 14 06:30:53.339 [notice] 206 PL (1.008%)
> > Oct 14 06:30:53.339 [notice] 187 CH (0.915%)
> > Oct 14 06:30:53.339 [notice] 179 IR (0.876%)
> > Oct 14 06:30:53.339 [notice] 165 FI (0.808%)
> > Oct 14 06:30:53.339 [notice] 160 BR (0.783%)
> > Oct 14 06:30:53.339 [notice] 141 SA (0.690%)
> > Oct 14 06:30:53.339 [notice] 136 TW (0.666%)
> > Oct 14 06:30:53.339 [notice] 136 TH (0.666%)
> > Oct 14 06:30:53.339 [notice] 103 IL (0.504%)
> > Oct 14 06:30:53.339 [notice] 102 BE (0.499%)
> > Oct 14 06:30:53.339 [notice] 97 NO (0.475%)
> > Oct 14 06:30:53.339 [notice] 77 DK (0.377%)
> > Oct 14 06:30:53.339 [notice] 76 CZ (0.372%)
> > Oct 14 06:30:53.339 [notice] 76 IN (0.372%)
> > Oct 14 06:30:53.339 [notice] 73 AR (0.357%)
> > Oct 14 06:30:53.339 [notice] 72 Unknown (0.352%)
> > Oct 14 06:30:53.339 [notice] 69 HK (0.338%)
> > Oct 14 06:30:53.339 [notice] 67 PT (0.328%)
> > Oct 14 06:30:53.339 [notice] 64 SG (0.313%)
> > Oct 14 06:30:53.339 [notice] 60 RO (0.294%)
> > Oct 14 06:30:53.339 [notice] 60 HU (0.294%)
> > Oct 14 06:30:53.339 [notice] 60 GR (0.294%)
> > Oct 14 06:30:53.339 [notice] 58 MY (0.284%)
> > Oct 14 06:30:53.339 [notice] 54 MX (0.264%)
> > Oct 14 06:30:53.339 [notice] 51 NZ (0.250%)
> > Oct 14 06:30:53.339 [notice] 47 TR (0.230%)
> > Oct 14 06:30:53.339 [notice] 43 IE (0.210%)
> > Oct 14 06:30:53.339 [notice] 38 SI (0.186%)
> > Oct 14 06:30:53.339 [notice] 37 UA (0.181%)
> > Oct 14 06:30:53.339 [notice] 36 BG (0.176%)
> > Oct 14 06:30:53.339 [notice] 31 SK (0.152%)

> > Oct 14 06:30:53.339 [notice] 27 HR (0.132%)
> > Oct 14 06:30:53.339 [notice] 27 CL (0.132%)
> > Oct 14 06:30:53.339 [notice] 25 KR (0.122%)
> > Oct 14 06:30:53.339 [notice] 20 QA (0.098%)
> > Oct 14 06:30:53.339 [notice] 19 LT (0.093%)
> > Oct 14 06:30:53.339 [notice] 19 EE (0.093%)
> > Oct 14 06:30:53.339 [notice] 18 LV (0.088%)
> > Oct 14 06:30:53.339 [notice] 18 PH (0.088%)
> > Oct 14 06:30:53.339 [notice] 16 VE (0.078%)
> > Oct 14 06:30:53.339 [notice] 14 KW (0.069%)
> > Oct 14 06:30:53.339 [notice] 14 CO (0.069%)
> > Oct 14 06:30:53.339 [notice] 11 CS (0.054%)
> > Oct 14 06:30:53.339 [notice] 11 PE (0.054%)
> > Oct 14 06:30:53.339 [notice] 11 VN (0.054%)
> > Oct 14 06:30:53.339 [notice] 10 BY (0.049%)
> > Oct 14 06:30:53.339 [notice] 10 PK (0.049%)
> > Oct 14 06:30:53.339 [notice] 9 ID (0.044%)
> > Oct 14 06:30:53.339 [notice] 7 LU (0.034%)
> > Oct 14 06:30:53.339 [notice] 7 MD (0.034%)
> > Oct 14 06:30:53.339 [notice] 6 BH (0.029%)
> > Oct 14 06:30:53.339 [notice] 5 CR (0.024%)
> > Oct 14 06:30:53.339 [notice] 5 CY (0.024%)
> > Oct 14 06:30:53.340 [notice] 4 BA (0.020%)
> > Oct 14 06:30:53.340 [notice] 4 JO (0.020%)
> > Oct 14 06:30:53.340 [notice] 4 PA (0.020%)
> > Oct 14 06:30:53.340 [notice] 3 AZ (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 BN (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 UY (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 UZ (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 MK (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 KZ (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 IS (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 FJ (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 DO (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 EC (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 OM (0.015%)
> > Oct 14 06:30:53.340 [notice] 3 DZ (0.015%)
> > Oct 14 06:30:53.340 [notice] 2 BS (0.010%)
> > Oct 14 06:30:53.340 [notice] 2 MT (0.010%)
> > Oct 14 06:30:53.340 [notice] 2 SV (0.010%)
> > Oct 14 06:30:53.340 [notice] 2 SY (0.010%)
> > Oct 14 06:30:53.340 [notice] 2 PR (0.010%)
> > Oct 14 06:30:53.340 [notice] 2 BO (0.010%)
> > Oct 14 06:30:53.340 [notice] 2 GT (0.010%)
> > Oct 14 06:30:53.340 [notice] 2 HT (0.010%)
> > Oct 14 06:30:53.340 [notice] 2 AW (0.010%)
> > Oct 14 06:30:53.340 [notice] 1 LB (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 CU (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 AF (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 SR (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 BM (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 YE (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 BZ (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 LI (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 MG (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 LY (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 KE (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 MN (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 KY (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 AN (0.005%)

> > Oct 14 06:30:53.340 [notice] 1 AG (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 LC (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 VC (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 TT (0.005%)
> > Oct 14 06:30:53.340 [notice] 1 BW (0.005%)

----- End forwarded message -----

$$ JACOB REPORTS TO FUNDERS

From: Roger Dingledine
To: Eric Johnson; [redacted] Kelly DeYoe; Ken Berman
Cc: [redacted]
Subject: (FWD) Tor Browser Bundle success story
Date: Sunday, September 14, 2008 5:42:22 AM

Hi folks,

Chris is always asking for 'Tor success stories'. Jacob had one from August, so I asked him to write it up (minus the names).

--Roger

----- Forwarded message from Jacob Appelbaum <[redacted]> -----

From: Jacob Appelbaum <[redacted]>
To: [redacted]
Subject: A non-specific writeup for a non-specific country deployment during a non-specific event
Delivery-Date: Thu, 11 Sep 2008 01:15:58 -0400

Hi,

Roger asked me to write up a small document detailing how a group has recently deployed Tor in countries that employ active censorship and blocking of specific content. In the interest of the group, I'll not disclose the events, the countries or the groups. Please do not inquire about any of that information. If you're going to know at all, you already do. I'm sorry about being secretive but that's the trade off for this email happening at all.

I've been engaged in direct trainings for quite some time. I've been training many different kinds of people around the world for around seven years. This past summer was quite intense with direct action teams and the socio political tension was very high. A number of high profile groups requested help reaching parts of the internet from certain known internet oppressive locations. Some of their people were directly under surveillance by the country in question. I won't speak to their actions with regard to anything beyond internet communication.

Many of these groups were creating and collecting media for distribution in real time. Using laptops, video cameras and wireless networks, they were streaming video over the internet. The laptop users were connected to the internet over wifi for real time streaming. Sometimes those users used local wireless networks provided by third party companies. Without speaking to the legality of said use, they were not always able to find free wireless networks. Sometimes those users used their own wireless networks backed with a portable V-SAT or a cellular modem for their internet connection. They largely relied on Free Software for their backbone. Tor was a major component in their software tool chest.

Nearly all of the people in these countries were equipped with small video cameras. These devices provide a USB mass storage device. It behaves like a hard drive for use in any modern computer. These flash disks stored at least one but often more than one copy of the Tor Browser Bundle. Each device was hand prepped by someone that I personally trained or someone that they trained. Each Tor Browser Bundle was configured to use bridges. Not all of the bridges were public. Most

of them were private. This is an example of how public and non public bridges were configured:

```
SocksPort 0
Nickname BridgeExample
ORPort 443
BridgeRelay 1
PublishServerDescriptor bridge
Exitpolicy reject *:*
```

```
SocksPort 0
Nickname BridgeExample
ORPort 443
BridgeRelay 1
PublishServerDescriptor 0
Exitpolicy reject *:*
```

As expected, many people were arrested over the course of the summer. These people did not attempt to hide their use of Tor. If any inspection of their computer hardware was done, Tor was almost certainly found. This is an ironic counterpart of making the Tor Browser Bundle easy to use. It has become very easy to spot. We should very seriously consider a self-destruction feature, perhaps a small program that erases all of the programs and data in a single click.

As a result of these arrests as well as other media issues (such as the Freedom Stick by the CCC), it is very likely that we're on the worldwide radar even more than we were before. From my understanding, these uses of Tor were very successful. These people we able to treat their local network censorship as damage and route around it. They were able to use networks that were otherwise untrustworthy. They were able to not directly connect into the Tor network itself thanks to the bridging features.

In summary, they were able to publish their media files and stream their content. They were able to communicate. I'm very proud of this. It wouldn't have been possible without Tor.

Regards,
Jacob

----- End forwarded message -----

From:	Ken Berman
To:	Roger Dingledine
Cc:	Kelly DeYoe
Subject:	[Fwd: [Fwd: Re: Filtering]]
Date:	Thursday, December 20, 2007 2:43:02 PM

Roger - note comment on bottom of Tor speed. Ken

-------- Original Message --------
Subject:[Fwd: Re: Filtering]
Date: Thu, 20 Dec 2007 10:44:47 -0500
From: Saeed Rahmani <[redacted]>
To: Ken Berman <[redacted]>
CC: Kelly DeYoe <[redacted]>

Here is a respond from one of our users in Iran regarding Satellite and VPN.
- Saeed

-------- Original Message --------
Subject: Re: Filtering
Date: Thu, 20 Dec 2007 13:43:03 +0330
From:farhad sarreshteh <[redacted]>
To:[redacted]
References:[redacted]

Dear Sir:

Thank you for your response.

Please note that my Farsi typing is very poor & slow, this is why I write in English, and I apologize for that in advance.

I knew a trusted man who brought me a dish and an LNB, and a digital satellite receiver (SKYSTAR 2 TV), with the brand name Techni Sat- original.

They find Glob Sat by dish and through this Modem (Techni Sat), which they assembled in my PC, I had a VPN service.

When I was connecting to internet, I was connected to Glob Sat. first.

Please note that I was sending through a local server, and was receiving from satellite, of course with no filters on its way.

Unfortunately the man I knew left and have no access to a TRUSTED man to get a similar service.

If you are interested to know: the cost of Dish +LNB+Modem+assembling services totaled to 110,000.Tomans & I was paying 50,000.Tomans per month

for this service I was receiving. I do not know how much they were paying monthly.

By the way my receiving speed was around 150 Kb/s.

I hope the above information would be helpful, in guiding us how to by pass this very slow speed we are facing now.

Before, I used to spend around one hour total behind my PC. But now sometimes I get angry and leave my PC. , due to slow speed.

My access to Filtered sites is now through VOA, which is very time consuming & slow.

Also note through my Tor soft ware (Vidalia Bundle), I check the send and receive speed, which I found most of the time they are below 4kbps.

Best Regard

Farhad Sarreshteh

IRAN

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe; Matt Edman; [redacted]
Subject: [Fwd: Fw: Vidalia looking for Farsi translator]
Date: Thursday, October 26, 2006 11:47:37 AM

Roger - this is a lot bigger job than we thought and we may need to use some of our contract labor to actually get the work done due to the non-standard character sets we have. We might want a telephone contact of someone who can help walk our translator thru the process once we identify the right person.

Ken

-------- Original Message --------
Subject: Fw: Vidalia looking for Farsi translator
Date: Mon, 16 Oct 2006 22:08:52 -0400
From: Ken Berman <[redacted]
To: Ken <[redacted]

----- Original Message ---
From: [redacted]
To: [redacted]
Cc: [redacted]
Sent: [redacted]
Subject: Vidalia looking for Farsi translator

> Hi Ken, Kelly,
>
> Vidalia has a dozen translations so far, but no Farsi. I think it would
> be handy to get that started. Plus, the RSF folks we're working with
> are focusing on Iran and they'd be happy to see a translation.
>
> Do you have any Farsi translators who are at least mildly technically
> inclined and could help us out?
>
> Check out http://trac.vidalia-project.net/wiki/Translations for details of
> how it works. Just translating the ".ts" file is the right step for now --
> I hope to revise the help documents a lot in the next few months.
>
> Let me know if you know anybody interested and suitable and we'll go
> from there.
>
> Thanks!
> --Roger
>

RSF?

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe
Subject: [Fwd: Master"s Thesis Referral from Simson Garfinkel]
Date: Tuesday, October 16, 2007 8:49:18 AM

Roger - your thoughts??

Ken

-------- Original Message --------
Subject: Master's Thesis Referral from Simson Garfinkel
Date: Mon, 15 Oct 2007 12:37:28 -0700
From: Steve Bassi <[redacted (b) (6)]
To: [redacted (b) (6)]

Mr. Berman,

I'm a second year masters student at Naval Postgraduate School and I was talking with Simson the other day about a list of research topics you sent him. I'm particularly interested in looking into a method of decentralizing Tor's directory servers.
I have a diverse background in networks, exploitation, and programming so something like this feels right up my alley. Would you be interested in having someone such as myself work on this?

If so, could you expand a little bit about what it is that you want and what your [redacted] has tried already? If this is easier via voice my number is [redacted (b) (6)]

To be fair, I am considering another topic (which I'm a little less interested in) but it seems to be hung up in the bureaucracy.

Thanks,
Steve

From: Ken Berman
To: Roger Dingledine
Cc: Shava Nerad; Kelly DeYoe
Subject: [Fwd: P2P audio streaming by an international broadcaster]
Date: Wednesday, April 04, 2007 11:13:11 AM

Roger - I'm going to go out on a limb and predict the Tor would not work with this app, but if you care to contradict me, I would be fine with that.....Ken

-------- Original Message --------
Subject: P2P audio streaming by an international broadcaster
Date: Mon, 02 Apr 2007 12:52:39 -0400
From: Kim Andrew Elliott <(b) (6)
Organization: U.S. International Broadcasting Bureau
To: Ken Berman <(b) (6) John Johnson <(b) (6) Michael Messinger <(b) (6) Jose Vega <(b) (6)

This is the first example I've seen of peer-to-peer audio streaming for international radio. It's used by the Africa division of Trans World Radio, a U.S. based evangelical broadcaster.

http://infant.antfarm.co.za/twr/dialog.html

See also the FAQ...

http://infant.antfarm.co.za/twr/p2p_faq.html

I didn't try to install the plug-in, for fear of not being able to uninstall it.

They use a service in South Africa called Antfarm, whose main site is...

http://antfarm.co.za

Kim

(b) (6)

From: Ken Berman
To: Roger Dingledine
Cc: Hiu Ho; Kelly DeYoe
Subject: [Fwd: Re: [Fwd: [Fwd: VOA NEWS FEEDBACK: The Approach to Access voanews.com at China - Torpark]]]
Date: Tuesday, September 05, 2006 1:59:11 PM
Attachments: mmessing.vcf

---

fyi.... from China.....

Michael S. Messinger wrote:

Ken Bill
This is from a email to VOANews.com over the weekend
FYI if you don't already know
Michael

-------- Original Message --------
Subject: [Fwd: VOA NEWS FEEDBACK: The Approach to Access voanews.com at China - Torpark]
Date: Tue, 05 Sep 2006 12:05:56 -0400
From: VOANews.com <[redacted]>
To: Michael Messinger <[redacted]>

see http://torpark.nfshost.com/

Mollie

-------- Original Message --------
Subject: VOA NEWS FEEDBACK: The Approach to Access voanews.com at China - Torpark
Date: Sun, 03 Sep 2006 07:46:44 +0000 (GMT)
From: [redacted]
To: [redacted]

Name = G
Email = [redacted]t
Subject
Comments = Dear sir/madam,

Now I am in China. I get a convenient
approach to access voanews.com at China.
There is a free navigator, Torpark.
Using it, the firewall can be punched.
Users just need to type your URL as
usual when accessing your site. Hope you
could let all the listeners know about that.

Best wishes,
GreatFree

EUSSID

From: Roger Dingledine
To: Kelly DeYoe; Ken Berman
Subject: (FWD) Re: Tor news
Date: Wednesday, February 13, 2008 11:48:05 PM

And then here's another interesting tidbit we can make use of. This fellow seems to be the center of the security and privacy community in Russia, as far as I can tell.

--Roger

----- Forwarded message from Vlad SATtva Miller <[redacted] -----

From: Vlad SATtva Miller <[redacted]
To: Roger Dingledine <[redacted]
Subject: Re: Tor news
Delivery-Date: Wed, 13 Feb 2008 18:47:38 -0500

Roger Dingledine wrote on 13.02.2008 16:52:
> Hi Vlad,

Hi Roger!

> ygrek (the Russian translator for the Tor pages) said you'd be a good
> person to talk to.

I know ygrek, he's one of the active "openPGP in Russia" community members. I'd be glad to answer all your questions.

> One of our funders is IBB.gov, the US government agency that helps run
> Voice of America, Radio Free Europe, etc. They've been working with us
> to encourage us to deploy our "blocking resistance" design. You can read
> (and hear) more about it at item #4 on
> https://www.torproject.org/documentation#DesignDoc

Yes, I'm aware of experimental blocking resistance design and Tor bridges. (By the way, not so long ago there was a curious discussion at pgpru.com brought up by ygrek about Russian translation of the 'bridge' word in the context of the Tor network. Sadly, we didn't came up to anything useful.)

> The newest dev bundle of Tor comes with some new options in Vidalia's
> Settings -> Network page, that let you specify a proxy, specify that only
> certain outgoing ports will work, specify that you need to use encrypted
> directory requests rather than plaintext, and configure some bridges to
> use rather than connecting directly to the Tor network:
> https://www.torproject.org/download#Dev
>
> Even more recently, we've been working on a Tor Browser Bundle that
> includes Tor, Vidalia, Polipo, Firefox, and Torbutton:
> https://torbrowser.torproject.org/

This is a really promising thing for general users, as till recently many questions on Tor we had concerned proper installation and configuration procedure for the Tor client and properly binding it with the browser. Steven Murdoch did a great job.

> IBB wants us to start reaching out to real users who might need these

> tools at some point soon.
>
> We talked about rolling out in China, but we decided that it's simply
> too large a user base to handle at once quite yet. We talked about Iran,
> but decided that with our high directory overhead, we're still not a
> very fun solution for modem users.
>
> So we settled on Russia, which is increasingly on their radar as a country
> that may have a serious censorship problem in the next few years. Radio

Not currently, but could be especially considering some controversial legislation work going on in the Parliament on information copying, websites status, etc. (I can elaborate on this if you wish, however at this time many things are just too vague to discuss precisely).

The main problem in Russia at this time is not a government censorship (in the sense of The Great Firewall of China or some Arab states), but a self-censorship of many websites, especially of regional organizations. Unfortunately, this is not what Tor can entirely solve by itself... But it can prevent us rolling down to the very dark abyss.

> Free Europe has a mailing list of about 100,000 people in Russia who
> would be interested to hear about something like Tor. In the next week
> or so we're going to send an announcement to (some subset of) this list.

Daniel Nagy already shred some light on this initiative of yours (he also conveyed your greetings from FC, Cozumel to the pgpru.com project; I appreciate them very much). You have my full support for this initiative.

Also Dani mentioned that some sponsors of the Tor Project are associated with the US State Department, and this led to a relatively lengthy discussion of Tor's dependence on "Uncle Sam's" money, and pros and cons of such situation. As you pointed out above, that "associated sponsor" is in fact IBB. I understand this is an ambiguous and quite vague question, but do such sponsorship brings up any unusual issues to the Tor Project and Tor development process?

> So: please don't advertise this anywhere yet. But if you'd like to be
> involved in some way, or you have advice, please do let me know. We're
> still trying to stabilize the latest releases and bundles, and at some
> point we should write up a little announcement, but I figured I'd give
> you a bit of advance warning.

Sure, thanks. First, as pgpru.com community already has very strong and knowledgeable Tor userbase (there's even a user-translated specs doc[1]), you may direct all Russian-speaking users (and people taking interest in Tor) to our forum[2], there is a subsection dedicated specifically to anonymity questions. Second, I have contacts with a couple of russian human-rights organizations, so I can forward them any official announcements as well. Third, I can post your announcements in the news section and on the start page of pgpru.com, spreading the word even further. If myself or our resource could be somehow more helpful, please, don't hesitate to tell.

> Thanks!
> --Roger

Yours,

[1] https://www.pgpru.com/biblioteka/specifikacii/tor

[2] https://www.pgpru.com/forum

--
SATtva | security & privacy consulting
www.vladmiller.info | www.pgpru.com

----- End forwarded message -----

DARPA, TIA

From: Roger Dingledine
To: Kelly DeYoe
Cc: Ken Berman; Andrew Lewman
Subject: Helping to review BBG proposals
Date: Wednesday, July 06, 2011 3:29:46 AM

Hi Kelly,

I talked to Ken last week at the DARPA meeting, and one of the topics that came up was that I could help BBG evaluate some of the proposals you're looking at. While Ken is enjoying his hiking I realized I should send you a heads-up so you can start thinking about how to make use of me.

I imagine there are conflict-of-interest issues to consider (since Tor sent a proposal too), but I figure since Ken says he wants us to be part of the BBG family going forward, it's in our interest to make sure it's a good strong family. :)

Hope things are going well with you,
--Roger

AKAMAI + TOR

From: Ken Berman
To: Kelly DeYoe; Hiu Ho; Roger Dingledine
Cc: Betty Pruitt
Subject: [Fwd: Re: Akamai and Tor]
Date: Monday, November 13, 2006 1:19:58 PM

---

stand by.....

-------- Original Message --------
Subject: Re: Akamai and Tor
Date: Mon, 13 Nov 2006 12:15:41 -0500 (EST)
From: Avi Freedman <[redacted (b)(6)]
To:[redacted (b)(6)] (Ken Berman)

Hi, I am familiar with Tor. Sounds interesting, though I haven't used it myself. I have played with proxify.net myself and the nph-proxy code (which is slooooow) - but I was surprised at how many hundreds of people run such proxies.

Tor sounds more generally interesting, in the sense that it's even better for you guys and some other gov agencies, and even worse for law enforcement :)

I live in PA but am up in MA most weeks.

I will take a look and get back to you.

Thanks,

Avi

> Avi - hope all is well with you, it certainly is with Akamai! Gettin' too cold to wear your shorts and sandals to meetings? Anyway, we have started supporting a development product called Tor, developed by the Naval Research Lab and Roger Dingledine, as part of our Internet anti-censorship program. In the past you and I have discussed possible areas of cooperation above and beyond our formal VOA-Akamai streaming relationship. Tor might be one of those areas.
>
> Pls review their ideas, philosophy, and technical details (http://tor.eff.org/) and in this well done overview (http://tor.eff.org/overview.html) and let me know if you think some of the Akamai servers might serve as points on the Tor network. It must be something you/Akamai are comfortable with, and I can easily arrange a meeting between you and Roger, who has most of the answers you might have. He is based in MA, so he can come over to your offices (I guess you are still living in PA?) when you are there.
>
> thanks in advance for your consideration,
>
> Ken Berman
> IT Director
> BBG/IBB
>
>
>

0808 FUNDING CHINA

From: Roger Dingledine
To: Kelly DeYoe; Ken Berman
Subject: (FWD) Re: Meeting notes, Jan 11 2008
Date: Tuesday, January 15, 2008 12:31:08 AM

Hi folks,

Two questions for tomorrow's talk:

a) We added Isaac Mao, a well-known blogger from China, as one of the Tor directors for the next three years. This is part of a push to internationalize the board. We have a good fellow from Germany in mind. We'd like to add somebody from the Middle East, but we don't have very many great candidates in mind. Do you know some who would be great?

b) See Isaac's mail below. Is this something we should try to get in on? Do you know any of the right people behind the scenes?

(You can also read our Tor annual meeting minutes, quoted below, if you like. :)

Thanks!
--Roger

----- Forwarded message from Isaac Mao <[redacted (b) (6)] -----

From: Isaac Mao <[redacted (b) (6)]
To: [redacted (b) (6)]
Subject: Re: Meeting notes, Jan 11 2008
Delivery-Date: Sat, 12 Jan 2008 03:54:10 -0500

fyi. maybe you have seen this news too

http://www.defensenews.com/story.php?F=3286113&C=asiapac

* U.S. Launches Internet Anti-Censorship Effort *
By WILLIAM MATTHEWS<[redacted (b) (6)]
subject=Question%20from%20DefenseNews.com%20reader>
Posted 01/07/08 14:51
The U.S. Congress is funding a modest assault on the great firewall of China.
The newly approved budget for the U.S. State Department includes $15 million for developing "anti-censorship tools and services" which could help Internet users breach electronic firewalls set up by China, Iran and other "closed societies."
The money is part of the 2008 budget for the State Department's Bureau of Democracy, Human Rights and Labor. It is to be awarded competitively to software developers to produce "internet technology programs and protocols" that enable "widespread and secure internet use" in countries where the Internet is now heavily censored.
The funding bill says the anti-censorship effort is intended "for the advancement of information freedom in closed societies, including the Middle East and Asia."
In a report that accompanies the bill, the House Appropriations Committee singles out China as a particular target. It cites recent efforts by Chinese President Hu Jintao "to 'purify' the Internet via further monitoring and censorship," and through punishing Internet users who engage in uncensored communications.

The report also decries recent Internet crackdowns by the Cuban and Russian governments.
The $15 million for anti-censorship technology is a small part of a $164 million "Democracy Fund" that the State Department receives to promote democracy around the globe, but is a 30-fold increase over the half-million dollars provided for that purpose in 2007.
A spokeswoman said the State Department "is engaged globally promoting freedom of expression and the free flow of information on the Internet."
Lawmakers said programs they are funding"should be able to support large numbers of users simultaneously in a hostile Internet environment."
The Internet in China fits the "hostile" description.
The free-press organization Reporters Without Borders labels China "the world's most advanced country in Internet filtering."
Chinese authorities monitor Web sites, chat forums, blogs and video exchange sites, and have imprisoned more than 50 Internet users for postings deemed to be anti-government, subversive and otherwise objectionable, Reporters Without Borders reports.
The Chinese government has required companies like Google, Yahoo! and Microsoft to censor their search engines as a condition for operating in China. As a result, Internet searches for terms such as "human rights" and "Taiwan independence" have been blocked.
According to some reports, a Chinese Internet search on Google for "Tiananmen Square" produces images of buildings and smiling tourists, while the same search in the United States generates pictures of the Chinese tanks used to crush pro-democracy protestors in 1989.
Internet censorship in North Korea is worse. Government control makes North Korea "the world's worst Internet black hole," Reporters Without Borders says. "Only a few officials are able to access the Web, using connections rented from China."
Cuba is repressive as well. Virtually all Internet connections are government-controlled, and "you can get five years just for connecting to the Internet illegally," the organization says.
The Iranian government boasts that it blocks access to 10 million "immoral" Web sites, including political and religious sites.
Saudi Arabia, Syria and Egypt also make the Reporters Without Borders list of "Internet enemies."
The new funding for State Department efforts to defeat Internet censorship "is a welcome arrow" in a modest arsenal of weapons for defending Internet freedom, said Leslie Harris, president of the Center for Democracy and Technology.
Protecting the Internet from abusive governments is important to supporting democracy, she said. But accomplishing that "will require the free world to take much harder positions" against abuses such as censorship. Ultimately, the odds may favor technology.
"No matter how many restrictions are written in China, the Internet is a very hard technology to control," Harris said. "The number of users is growing exponentially ? blogs, e-mail accounts, the magnitude is extraordinary. At the end of the day, governments trying to control the Internet are going to have a very difficult time." å
E-mail: [redacted] (b) (6) (b) (6)
subject=Question%20from%20DefenseNews.com%20reader>

.

On Jan 12, 2008 3:30 AM, Roger Dingledine <[redacted] (b) (6) wrote:

> Meeting minutes: Tor annual meeting, Jan 11, 2008.
>
> Ian calls meeting to order, 11:13am EST.
> Roger, Andrew, Fred, Ian, Nick, Wendy, Rebecca present.

> Frank Rieger also here as an invited observer, with John Gilmore
> and Isaac Mao joining later as invited observers.
>
> Item 0: approve last meeting's minutes.
> No objections to approving last meeting's minutes.
> Approved.
>
> a) Treasurer's report (Andrew).
>
> Andrew gives budget overview. 2007 was a great year for us.
>
> Ian reminds us the details of the MITACS arrangement. First research
> project is Ian's grad student who wants to work on DTLS / UDP transport.
> Conclusion: we'll wait until Ian learns more; he expects to learn more
> in February, and we can decide how much money to put in then.
>
> Andrew: the final question is whether we'll get an audit. Still up in
> the air. Most likely the IRS letter will arrive in March. Andrew will
> continue to look for good auditing firms in anticipation that such a
> letter will arrive.
>
> b) The year in review, and funding prospects (Roger).
>
> 2007 public-facing features:
> - great progress on supporting apps like vidalia and torbutton
> - we made it much easier for clients to be relays
> - we launched the blocking-resistance work
>
> Wendy asks if we should be doing press releases about our progress;
> this causes Roger to add a new agenda item (g) for that question.
>
> Roger's intended 2008 focus:
> - Make it even easier for clients to be relays
> - Tolerate network scaling (see first section of roadmap-future.pdf)
> - Alternate packaging: USB images, VM-based images, LiveCD images, ...
> - More organizational depth: an exec dir, fundraising, handling press.
>
> (Isaac Mao arrives: 11:34)
>
> 2008 prospective funders:
> IBB and France continue as our main prospects.
> We submitted a proposal to Google.
> Roger is working on a funder that could fund us via ARL (the same
> funding avenue as our SRI contract).
>
> c) Broad goals over the next several years.
>
> Roger enumerates some 3-year goals:
> - 10000 servers.
> - Make it easy (back end and interface) to run an exit relay
> - More consistent funding (30-50% of our yearly funding stable)
> - Understand anonymity enough to discard our when-Tor-starts warning.
> - Outreach and education
> - With law enforcement
> - With media
>
> Nick wants us to win the "global privacy war" (a la global crypto war).
> Public opinion. Public awareness of the value of anonymity. Getting an
> exec dir who understands this will help a lot.
>

> Fred points out that we've got a good opportunity here for this war,
> because right now nobody is taking up our side in the media. So if we
> have the right person, we'll be the group that the media always calls.
>
> Frank points out that the war on crypto was won by putting ssl into
> the browser. Not just by politics and talking. Fred agrees but says we
> need both.
>
> d) Trademark update (Andrew and Wendy).
>
> Andrew and Wendy talked to our mofo lawyers. We're working towards a
> licensing document so we can license people who are using our brand.
>
> Ian wants to make sure that the people who get it licensed will put a
> little note saying 'Tor and the onion logo are trademarks of...'
>
> Roger agrees, and wants to make a list of the approved projects on the
> Tor trademark page, so everybody can know.
>
> Fred says that the Torrify trademark app has now been abandoned. That's
> good news.
>
> Andrew says that our trademark is still on track. Now that the two
> competing trademarks are withdrawn/abandoned, that goes in our favor.
>
> Roger asks if we should pick up our European trademark filing discussion,
> or just leave it alone? Andrew reminds us that the Madrid filing was
> potentially very expensive.
>
> Frank explains that there's a prohibition against registering every-day
> terms in Europe, and speculates that Tor counts.
>
> Roger asks Frank to look into doing it in Germany. Frank needs an example
> application. Andrew has one of those, and will send it to Frank.
>
> e) New directors.
>
> Frank wants to see more focus on long-term: developing the parts of Tor
> that are not dependent on exit nodes: hidden services, making exit nodes
> more dynamic so they can survive better.
>
> John wants to see bylaws and other docs. What form of protections do we
> have for directors? Andrew is still looking into this -- board insurance
> is tricky because we're in a category that most insurance companies
> don't have a category for.
>
> Isaac is excited to spread the word about Tor in many different countries.
> He's quite familiar with Web 2.0 approaches and getting word out that
> way. Along with tutorial / outreach program, we should try to simplify
> the user interface (installation, configuration) as well. Viral marketing
> plan. Isaac is ready to start right away.
>
> We delay actual elections until the end of the agenda, so Ian and Isaac
> can stay on the call.
>
> f) The exec dir hunt.
>
> Ian had a good set of questions about an exec dir. Fred had some good
> answers. Ian and Fred will assemble answers and send them back.
>

> Fred graciously relents to be the executive director search committee
> chair.
>
> Ian moves that Fred will be chair of above.
> Roger seconds.
> Further discussion? "Thanks Fred!"
> No objections. Passed.
>
> John asks if we've considered a search firm. Fred and John will talk about
> that more offline.
>
> Fred will write a few wish-list bullet points and Roger will make a web
> page out of it, so people know we're looking.
>
> g) Should we be doing press releases?
>
> Roger thinks this should be a major bullet point on the exec dir "desired
> skills" list.
>
> Rebecca says press releases are nice and all, but what we really need
> is to develop relationships with journalists. "Cultivating the media."
>
> Roger suggests that that's a great thing to do once we have the bandwidth
> for it. Let's keep this in mind, and also put it on our "3-year vision"
> list.
>
> e) Director elections
>
> (Ian, Frank, John, and Isaac hang up.)
>
> Andrew moves to reelect Ian to his director position.
> Wendy seconds.
> Nobody opposed.
> Motion Passes. Ian is a director for three more years.
>
> Roger moves to elect Isaac Mao to the director position that is currently
> Rebecca's.
> Fred seconds.
> Nobody opposed.
> Motion passes. Isaac is now a director for three years.
>
> Wendy moves to thank Rebecca for her fine work as a director.
> Roger seconds.
> General agreement.
> Motion passes.
>
> Rebecca is excited to stay as an active contributor, particularly with
> respect to educating journalists and users in Asia.
>
> Any final topics?
> No final topics.
>
> Andrew moves to adjourn.
> Adjourned at 12:38.
>
>
> -----BEGIN PGP SIGNATURE-----
> Version: GnuPG v1.4.6 (GNU/Linux)
>
> iD8DBQFHh8Pz61qJaiiYi/URAp55AKDH4g8iloOXWJvZsyt/QrJM+Q1KIgCfXTVm

> szx/E2WR4jzsGEdfx9EQLk4=
> =3hbd
> -----END PGP SIGNATURE-----
>
>

--
Isaac Mao
We Make Art Not Money
Skype: isaac.mao
Home: http://isaacmao.com
Thinking: http://twitter.com/isaac
Profile(Chinese): http://mao.wealink.com
Photos: http://flickr.com/photos/isaacmao
Subscriptons: http://anothr.com/isaac.mao
Twitter: http://twitter.com/isaac

If you travel to China or can't access some overseas web sites, please prepare to download Tor(http://tor.eff.org) to get free access to those sites, e.g. http://www.memedia.cn

----- End forwarded message -----

From:
To: (b) (6) (b) (6)
Subject: FW: Upcoming Event: Internet Circumvention Tools and Methods: Evaluation and Review
Date: Thursday, March 31, 2011 12:39:14 PM

You are invited.....

From: Freedom House [mailto: (b) (6)
Sent: Monday, March 28, 2011 12:47 PM
To: (b) (6)
Subject: Upcoming Event: Internet Circumvention Tools and Methods: Evaluation and Review

Dear Ken,

Freedom House invites you to join us on Tuesday, April 12 at the Freedom House Offices in Washington, DC for the official launch of Internet Circumvention Tools and Methods: Evaluation and Review.

As the recent shift in political landscape within the Middle East has shown, the Internet is increasingly influencing the way that citizens around the world gather and distribute information. While these changes occur, it is vital that people are aware of how to protect themselves online and how to access information, news, and facts, when the Internet is censored.

While there are sites that recognize the effectiveness of circumvention tools, there are none that assess the effectiveness of circumvention tools systematically. Freedom House has used its expertise and relationships with leading academic experts on information technology security, censorship, and software development to conduct a systematic assessment of how censorship circumvention tools perform in practice inside the countries they are designed to serve.

Freedom House's Internet Freedom Project Director, Robert Guerra, will join major report contributors Cormac Callanan, director of Ireland-based Aconite Internet Solutions with experience in international computer networks and cybercrime, and Hein Dries-Ziekenheimer, the CEO of VIGILO consult, a Netherlands based consultancy specializing in Internet enforcement, cybercrime, and IT law, to discuss the findings of the report and its implications in the world of Internet privacy and censorship circumvention.

The event will be broadcast live over the Internet. A link to the broadcast will be sent out prior to the beginning of the event. Please review the event information below:

Internet Circumvention Tools and Methods: Evaluation and Review
April 12, 2011
12:00pm - 2:00pm

Freedom House 4th Floor Conference Room
1301 Connecticut Ave NW Floor 4
Washington, DC 20036

Lunch will be provided. Please RSVP by selecting the following link:

Internet Circumvention Tools and Methods: Evaluation and Review

Sincerely,

Robert Guerra, Director, Internet Freedom Program

Freedom House

Click here to unsubscribe

From:	Andrew Lewman
To:	Ken Berman; Kelly DeYoe; Sho Ho
Cc:	Karen Reilly; Roger Dingledine
Subject:	July Monthly Report from Tor
Date:	Tuesday, August 10, 2010 6:02:44 PM
Attachments:	2010-July-Monthly-Report-BBG.pdf

Hello Kelly, Ken, and Sho,

We have a longer than usual report due to lots of projects completing or coming online in July.

We're available to answer questions about progress in July or any questions you may have about the recent press regarding Jake and Wikileaks.

Thanks!

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

Website: https://www.torproject.org/
Blog: https://blog.torproject.org/
Identi.ca: torproject
Skype: lewmanator

From: Roger Dingledine
To: Kelly DeYoe
Cc: Ken Berman; Hiu Ho
Subject: July Tor activity
Date: Wednesday, August 02, 2006 2:47:07 PM

Hi folks,

Here's a summary of some of what I've been up to in July. Please do ask about the points that sound interesting and are too vague. :)

Conferences / meetings:
* Working with Julien at RSF for us+them to create a "Tor for Freedom" advocacy site.
* Met with Jonathan Zittrain (ONI/Berkman/Oxford) about building and deploying an overlay (perhaps via Tor) to gather statistics about which websites are blocked from which network locations.
* SOUPS conference at CMU: presented Tor GUI results, worked with Vidalia/Foxtor developers to help them decide a roadmap.
* Met with Phil Malone, Harvard law prof who is going to integrate a lot of our legal questions into his fall clinical program.
* Met with Frank Rieger, CTO of cryptophone, who wants to integrate Tor into their new secure messaging network and set up every user as a Tor hidden service.
* Met with Ethan Zuckerman, Global Voices founder and OSI representative.
* Met with Andrew Lih, blogger in Hong Kong and PRC activist. Have been talking to Rebecca McKinnon and Isaac Mao, other PRC activists.
* Led the WPES program committee (http://freehaven.net/wpes2006/) to finish reviews and decide on a program. Actual conference is Oct 30 in Alexandria.

Need to work closer with the Toronto ONI folks, because Ethan says their Psiphon plans sound similar to my Tor plans.

August plans include meeting with the Wikipedia main developers to help them with authentication/authorization on Wikipedia ("China blocks Wikipedia, Wikipedia blocks Tor, ..."), and presenting at the MIT network security conference to discuss how to let universities run Tor servers better. (Many fast Tor servers are on .edu networks.)

Money stuff:
* Sorted out the DUNS number with Demetria, which means I can start invoicing IBB. Yay.
* Looks like we've got some short-term $ from Omidyar via Bruce Schneier. I'll believe it when I see it; if so, I'm going to aim for bringing Nick back on board Oct 1.
* Got a bit of funding from RSF for new website / "message" development in late CY06.
* Next step there is to finish contract for $ for Vidalia/Foxtor developers.

Dev:
* New stable release, fixing several big security-related bugs.
* Began skeleton of blocking.tex paper.
* Geo-ip survey of Tor IP addresses. (Why is China so high on the list yet Iran is so low?)
* The Tor network reached the 700 active Tor servers mark.

* Preliminary work on a network system call wrapper to make Tor scale on Windows XP. Still not sure when that will be done, but at least there's progress.
* Built a plan for including versions in the Tor network protocol, and a way to migrate to the new protocols. This will let us fix a lot of the brokenness that we've been backward-compatibly supporting over the past few years.
* Integrated asynchronous DNS subsystem to Tor, so Tor will work better without having to create lots of new threads.
* Now Tor directory servers tell you your IP whenever you make a request, so in theory servers don't need to sign up for a DynDNS account. This is still unauthenticated though, so we're aiming for a better solution down the road.
* Moved Tor source repository from CVS to SVN.
* Started working with Vitaly Shmatikov at UTexas Austin to come up with schemes (and figure out how to test them) to improve our resistance to traffic confirmation ("end-to-end") attacks.

August/Sept plans include
* Making the Vidalia bundle work better on OS X
* Making Foxtor into a usable Firefox plugin, and integrating it into the Vidalia/Privoxy/Tor bundle
* Replacing Privoxy with Polipo eventually
* Finish page explaining the Tor rendezvous protocol -- with diagrams! (We already have the diagrams, I've just never written the text.)
* Putting out a 0.1.2.1-alpha release, to gather and document (and test ;) all our recent dev work.

From: Ken Berman
To: Andrew Lewman; Kelly DeYoe; Sho Ho
Cc: Karen Reilly; Roger Dingledine
Subject: RE: July Monthly Report from Tor
Date: Wednesday, August 11, 2010 10:21:20 AM

Great stuff, thx. Roger answered a number of questions when he met us this week in DC...

-----Original Message-----
From: Andrew Lewman [mailto:[redacted]
Sent: Tuesday, August 10, 2010 5:03 PM
To: Ken Berman; Kelly DeYoe; Sho Ho
Cc: Karen Reilly; Roger Dingledine
Subject: July Monthly Report from Tor

Hello Kelly, Ken, and Sho,

We have a longer than usual report due to lots of projects completing or coming online in July.

We're available to answer questions about progress in July or any questions you may have about the recent press regarding Jake and Wikileaks.

Thanks!

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

Website: https://www.torproject.org/
Blog: https://blog.torproject.org/
Identi.ca: torproject
Skype: lewmanator

Chose your exit node!

From: Roger Dingledine
To: [redacted]
Cc: Kelly DeYoe; Ken Berman; Bennett Haselton; Betty Pruitt
Subject: Choosing your Tor exit node
Date: Wednesday, August 02, 2006 5:08:22 PM

Hi Hiu,

Check out
http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#ChooseEntryExit
for some discussion about how to choose your Tor exit node.

Blossom is quite hard to use these days, in part because Geoff never focused on usability in the first place, and in part because Geoff just got a new job in NYC so he hasn't been maintaining it. The URL above suggests a few other fine options too.

Once you've played with it for a while, perhaps you will learn enough to clean up the FAQ entry too? :)

Thanks,
--Roger

Iran

From: Sho Ho
To: Andrew Lewman
Cc: Roger Dingledine
Subject: Current Tor Traffic from Iran
Date: Tuesday, March 12, 2013 11:30:23 AM

Hi Andrew, Roger,

Can I ask both of you a HUGE favor? can you please send me the current Tor traffic report today? Since Kelly is on sick leave today, my boss wants to find out Current Tor traffic from Iran after the IRIB implemented their VPN negating hardware.

Thanks a million!

-Sho

DARPA

From: Roger Dingledine
To: Ken Berman
Cc: Andrew Lewman; Kelly DeYoe; Sho Ho
Subject: DARPA contact
Date: Tuesday, July 06, 2010 12:29:44 PM

Hi Ken,

Have you met Drew Dean from DARPA yet? If not, I should do an introduction.

--Roger

From: Bennett Haselton
To: [redacted] Roger Dingledine; Ken Berman
Subject: data sent in cleartext during Tor initialization
Date: Thursday, July 27, 2006 2:30:39 AM
Attachments: tor-initialization-capture-data.txt
ATT00001.txt

Using the Windows freeware program SmartSniff I captured some of the data sent and received by the Tor client when it initialized and first joined the network.

It shows there are a few strings in there like "TOR1.0", "<identity>", and "client0..0" that would typically show up only in Tor traffic, and not show up anywhere else -- which we would need to make sure are removed from the future China version since otherwise those strings could be used to block all Tor traffic without affecting anything else. (Of course, that wasn't an error on the part of the original designers, since Tor wasn't designed to evade censorship in that situation. Just something to change for the future.)

-Bennett

China network

From: Roger Dingledine
To: Jed Crandall
Cc: Ken Berman; Kelly DeYoe; Sho Ho
Subject: Detecting keywords filtered by GFW
Date: Tuesday, October 20, 2009 6:56:04 PM

Hi Jed, Ken/Kelly/Sho,

Here's an introduction. Jed is working on automated machine learning techniques to come up with keywords that are "likely" to be filtered, so you can come up with a list of filtered keywords much faster than just by walking through a dictionary.

Ken et al are looking for better ways to get the Voice of America website to people all around the world, including people in China.

So Jed, next time you're in the DC area, consider dropping by their office to teach them more about what you're up to. (It's not clear that it will be immediately useful for them, but giving them a sense of what options might be on the horizon could come in handy down the road.)

--Roger

Arab Spring

From: Andrew Lewman
To: Ken Berman; Kelly DeYoe
Subject: Egypt, Satellite, BGAN, thoughts
Date: Monday, January 31, 2011 5:27:40 PM

Hello Kelly and Ken,

I'm sure you are aware of the situation in Egypt all too well. I'll keep this short. The last ISP in Egypt, Noor, has just gone offline. Activists are telling us that landlines are going down too.

Do you have any experience, or spare equipment, with Tor over BGAN/Satellite?

Thanks!

--
Andrew
pgp 0x74ED336B
[redacted]

From: Andrew Lewman
To: Kelly DeYoe; Roger Dingledine
Subject: EPIC, BBC, Tor, and FOIA
Date: Tuesday, September 10, 2013 7:23:40 AM

Hello Kelly,

I assume you've seen https://epic.org/foia/tor.html?

I approved the full release of everything to your privacy office when they asked.

What can we do to clear up EPICs misunderstanding of how Tor works, how the contracts between us were arranged, and from them turning this into some sort of circus?

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

BBG/EFF

From: Roger Dingledine
To: Kelly DeYoe
Cc: Shava Nerad; Ken Berman; Hiu Ho
Subject: First draft of blocking-resistance design
Date: Monday, November 20, 2006 8:17:03 AM

Hi Kelly, Ken, Hiu,

Take a look at
http://tor.eff.org/svn/trunk/doc/design-paper/blocking.pdf
for our first draft on how to adapt Tor to have a blocking-resistance component.

Please don't publicize it widely yet (we want to go through a few more iterations first). Comments and thoughts appreciated -- on which parts don't make sense and need more explanation, on which parts claim wrong things or make bad assumptions, on which parts need better solutions, etc.

Should we bring Bennett back in at this point?

A roadmap for how to start building-and-deploying this in 2007 will follow soon, hopefully sometime this week.

Thanks!
--Roger

From: Roger Dingledine
To: Kelly DeYoe; Ken Berman
Cc: [redacted]
Subject: Followup from last week"s meeting
Date: Tuesday, September 23, 2008 9:40:37 PM

Hi folks,

Hope everything is going well with you. Great to see you last week.

Let me know if you have any questions or comments about the roadmap, when you get around to looking at it.

Also, give me a holler when you want me to show up again in person. I'm not so far away, it turns out.

I mailed Ali, and will hopefully connect with Jeremiah.

iFree is in fact focusing on Saudi Arabia as one of its first six countries.

I have a note here that Ken wanted me to meet "James Mulvenon", from CIRA.

Thanks,
--Roger

From:	Ken Berman
To:	Andrew Lewman
Cc:	Kelly DeYoe; Kyle Noori
Subject:	FW: Tor + Iran - HELPDESK
Date:	Wednesday, September 07, 2011 2:54:40 PM

Andrew – any idea whose these people are, soliciting funding for Tor!? I remember the message below, but what's the connection with you?
Ken

Ken

From: SiNA [mailto:[redacted (b) (6)]
Sent: Wednesday, September 07, 2011 1:37 PM
To: Ken Berman
Cc: Andrew Lewman; Kim Pham; Kelly DeYoe
Subject: Tor + Iran - HELPDESK

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Dear Ken,

Hope all is well!

We have been working on introducing the Tor project to the Iranian users for the past 6 months. As a result of our efforts and others including VOA...
Iran has become the 3rd largest user of Tor and it's growing by they day:
https://metrics.torproject.org/users.html?graph=direct-users&start=2011-01-09&end=2011-09-07&country=ir&dpi=72#direct-users

We are a small team with limited funding and resources, when VOA did a special program on Tor, our support lines ([redacted (b) (6)] was flooded with emails and questions.
Iran and the Tor Project as a whole is in need of a help desk. There are mostly volunteers and a few paid staff available to reply to these questions and help people connect properly.

The reason I wrote this email, is because I am very well aware that if there is any hope for the people of Iran, these last lines of communication must stay open. This is a an opportunity to do something great here. If you know anyone interested in helping in any shape, please refer them to us.

All the best,
SiNA

On 02/22/2011 01:16 PM, Ken Berman wrote:

> Thanks, Andrew!

>

> -----Original Message----- From: Andrew Lewman

> [mailto:[redacted] 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.

>

- --
SiNA
PGP: 0x0B47D56D

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

iQIcBAEBAgAGBQJOZ6ujAAoJEJPBwXYLR9VtfOIP/jZSCh/E5TictA32ziOtyeso
PxK1ykpzJIJmxHOAkr+MiyTpSqB1AyWzBX409+nWVcteLM2JPNrvX9BldBpNesKG
qb/gwCXcoUbY/ZGMn980eqiBni9QeAUxTWWIBCyd8i7aCjA1Tvu9+nUhqM41Y8cu
AGW7xODSKAERtj2eiiOuvwmWqeacLTa+MjszQ4pdfXPRZv2HNyhWFmCUMsN7xvqt
sRI9dX1I1JG9mtuq6BZ2RG6MmycvmRh46/hIyM5KA/rk6qK61/6Vypa0CVN6isMy
kbhAYBD/UzOKuX9Hm3LC2smmW17RszpNhXtWXkXI/rEJH9rMaqEoQwCObwu6+DaR
+nN7Pr7xTQFV+ULzZGLaPmNXXBDD5JgWhx8jOkF70PrcutIG30i1QP5HfmVNT9p4
uF4dWJtZUItisRKw0OrSEmhsnahWlCZWB/zi78n4vuAencB8OXzws+xiT74SK09R
e5gOjF2nNMGWt2qnMM+cv0g2gnRlq+oBy+YUhYJAoiVU9HDaJr9OaVfuSAXjR7Ww
BRWzzjDpOOH+2TfeUIr2iSNAS/T4mQRioXu/h/IixGFGbJYS/n1xR1gU+jQI3Yk1
vVMVIyd2WCCzi171j5okTN5sfcfMbl2q0tvDDAgzTlYAhbiZYXIUzQaro59dYNKx
SIgDUQ0LFHJr4f+XnkOC
=X7Tr
-----END PGP SIGNATURE-----

From: Ken Berman
To: Andrew Lewman; Roger Dingledine
Cc: Kelly DeYoe; Sho Ho
Subject: FW: Solicitation
Date: Monday, June 06, 2011 8:40:06 AM

---

https://www.fbo.gov/index?s=opportunity&mode=form&id=34602c22a64a1fea109c520936ccf000&tab=core&_cview=0

From: Ken Berman
To: Roger Dingledine; Andrew Lewman
Cc: Kelly DeYoe; Kim Elliott; Sho Ho
Subject: hot boot CDs/sticks
Date: Monday, April 19, 2010 2:10:59 PM

Roger/Andrew – would you give us a little more info on the Tor/Firefox bundle on it bootable CD or USB stick? Kim is one of our researchers, and we are playing with the idea of how to give it wider distribution.

Thx,
Ken

From: Roger Dingledine
To: dmitri vitaliev; Chris Walker; Ethan Zuckerman; Nart Villeneuve; Kelly DeYoe; Ken Berman; Cory Doctorow
Subject: I met the Smartfilter CTO; any questions for him?
Date: Tuesday, October 16, 2007 3:19:35 AM

Hello diverse group of friends,

At the MIT Emtech conference a few weeks ago, I met a very nice man named Paul Q. Judge, who is the CTO for Secure Computing, Inc -- the company that makes Smartfilter. Paul worked at a startup on encrypting email in a usable way, and his company got bought by Secure Computing a few years ago. Now he is CTO over such groups as Smartfilter.

Either he's an extremely good actor, or he really is unaware of how the rest of the (at least our) world views Smartfilter.

He lives in Atlanta, and I periodically visit my parents there. I plan to go to dinner with him in December and see if I can find any weaknesses we can exploit. :) Alas, it's way more complex than that -- even if Smartfilter backed off, Websense would eagerly jump into the void.

But it's worth continuing to talk -- once we got talking in depth, he speculated that Smartfilter and Websense were our only real adversaries, since companies like Cisco don't have 100+ person R&D teams working on blocking patterns. One hope would be to find a way to make the arms race diverge, so blocking-by-companies and blocking-by-governments have different incentives and different requirements -- if American corporations don't find it worthwhile to pursue the arms race against blocking Tor, some of Smartfilter's motivation to pursue the arms race disappears (Saudi Arabia et al are a small fraction of their customers).

In any case, I figured that some of you might want the chance to chat with him too. I don't want to overload him with fanatics, but I'd be happy to introduce you one at a time over the next while. Let me know if you're interested.

--Roger

DOJ

From: Andrew Lewman
To: [redacted] Roger Dingledine
Subject: IBB Network meeting
Date: Monday, April 06, 2009 11:08:44 PM

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?

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

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

CIA,

From: Roger Dingledine
To: (b) (6)
Cc: Kelly DeYoe
Subject: IBB notes for Sept
Date: Wednesday, October 10, 2007 4:14:30 AM

Hi Shava,

Here are the notes for the Sept IBB blurb. Feel free to fix up as you see fit. I'm cc'ing Kelly so he can get an advance skim if he's interested. :)

--Roger

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

Continuing enhancements have been made to the Tor website Chinese translation.

Tor 0.2.0.7-alpha (released Sep 21) makes bridges work again, makes bridge authorities work for the first time, fixes two huge performance flaws in hidden services, and fixes a variety of minor issues.

The Windows bundle also includes the new development Torbutton version 1.1.7 (released Sep 21), which clears cookies and disables a lot of other dangerous web behavior. A lot more stability and usability work remains on this development branch of Torbutton.

We began investigating whether to replace Privoxy with Polipo in the default Windows and OS X bundles. Preliminary results are that Polipo offers no actual performance advantages, but it offers some improvements in other respects. More research remains.

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

We now have a graphical draft of a bridge interface (along with other firewall and proxy settings) in Vidalia:
http://freehaven.net/~arma/vidalia-bridge-screenshot.png

In October we plan to attach the interface to the actual code so clicking the buttons actually produces results.

C.2.3. Let Tor users opt to become bridge relays.

We fixed a major bug that was causing bridges running recent alpha versions of Tor to not function properly:

From the 0.2.0.7-alpha ChangeLog:
- Fix a bug that made servers send a "404 Not found" in response to attempts to fetch their server descriptor. This caused Tor servers to take many minutes to establish reachability for their DirPort, and it totally crippled bridges. Bugfix on 0.2.0.5-alpha.

C.2.4. bridge directory authority mechanism

We implemented another step in making bridge authorities actually useful. Now Tor clients can configure themselves to bootstrap by getting bridge descriptor updates only from the bridge authority:

From the 0.2.0.7-alpha ChangeLog:

- Make "UpdateBridgesFromAuthority" torrc option work: when bridge users configure that and specify a bridge with an identity fingerprint, now they will lookup the bridge descriptor at the default bridge authority via a one-hop tunnel, but once circuits are established they will switch to a three-hop tunnel for later connections to the bridge authority. Bugfix in 0.2.0.3-alpha.

The next step (scheduled for October) is to let bridge authorities write out a list of descriptors that are annotated by "purpose", so we can distinguish bridge descriptors from ordinary Tor server descriptors. Then we can start giving out these bridge descriptors using the variety of distribution methods described in the blocking.pdf document.

C.2.5. Hide Tor's network signature.

Began work on a draft strategy for making our TLS handshake look more normal. Early draft at http://www.cl.cam.ac.uk/~sjm217/volatile/guest/xxx-tls-normalization.txt

C.2.6. Design a better cell-based protocol for people with poor network connectivity. (the follow-up mails refine this to "produce a design for fetching fewer descriptors")

We continued to make progress on the "v3" directory voting protocol. The Tor 0.2.0.7-alpha release sets up moria1 and tor26 as the first v3 directory authorities. See https://tor.eff.org/svn/trunk/doc/spec/dir-spec.txt for details on the new directory design.

We also completed the last step in separating the "bandwidth usage reporting" lines out of the normal router descriptor format. All Tor servers running 0.2.0.7-alpha and later will omit these bandwidth lines and only publish them in a separate "extra info" descriptor. This will shrink ordinary router descriptors by as much as 60%. https://tor.eff.org/svn/trunk/doc/spec/proposals/104-short-descriptors.txt

//C.2.7. Let the Tor network scale better.

//C.2.8. Identify tasks IBB can help with.

//C.2.9. Monitor and coordinate work performed by IBB, and integrate into Tor.

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

Roger Dingledine presented on a panel at the MIT Technology Review conference (Sept 27). We also met a variety of other interested attendees, including a business person from Intel, the CTO of Secure Computing (the company that sells Smartfilter), and a fellow who works with CIA and State Dept and is working on human rights.

We also started moving closer to switching to the torproject.org domain. This move will let us put much more detailed documentation and guides on our website, since the pages will no longer need to be vetted by EFF folks first.

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

The new Incognito 20070824.1 LiveCD (released on Sep 5) upgrades to Tor 0.1.2.17, adds a bunch of new software plus configurations, and fixes a variety of bugs.

The new Incognito 20070824.2 LiveCD (released on Sep 29) allows Incognito to be run in a virtual PC via qemu (qemu is like vmware but free), so ordinary Windows users can launch Incognito in a virtual window. It also includes the new version of Vidalia, a variety of upgrades, and is more tolerant of old and unusual hardware.

Additional news:

Steven Murdoch joined us starting this month.

Tor adventure in the news:
Storm botnet:
http://www.boingboing.net/2007/09/06/beware-wolf-dressed.html
http://www.links.org/?p=251

Embassy password story:
http://www.pcworld.com/article/id,137004-page,1/article.html

DUTCH, DRL
+ IIPB O JACOBS

From: Roger Dingledine
To: Ken Berman; Kelly DeYoe
Cc: [redacted]
Subject: IBB/Tor notes for April
Date: Monday, May 12, 2008 5:55:28 AM

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

NETWORK

From: Andrew Lewman
To: Ken Berman; Adam Fisk; Kelly DeYoe
Subject: Introduction to Lantern and BBG
Date: Saturday, February 05, 2011 8:39:31 AM

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

From: Andrew Lewman
To: Kelly DeYoe; Kelley Misata
Subject: Introductions
Date: Wednesday, January 16, 2013 1:48:47 PM

Hello Kelly and Kelley,

Please consider this an introduction to one another.

Kelly,

Meet Kelley. She's our new marketing and communications person working to improve Tor's image in the world. She's been hacking away on our soon-to-be-released Annual Report. She has tons of tech company experience and is full of ideas for Tor's future.

Kelley,

Meet Kelly. Kelly is responsible for a huge number of tech projects at BBG. He's been a consistent ally and funder of Tor since 2006.

I'll let you two take it from here.

Thanks!

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

PR, BAO

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe; Jill Moss
Subject: Fwd: MEDIA Query - TOR - other uses
Date: Thursday, February 23, 2012 6:22:35 PM

Roger,
Suggestions for a response?
Ken

A Boston Globe reporter is inviting our comment on a story she is doing related to TOR. She understands we work with them in our web anti-censorship program. Her piece focuses on the fact that there are reports that the TOR anonymizing technology is used for other purposes (including the silk road drug trade and child pornography).

She asked if we were aware of those reports and if we had a comment. She'd like to hear from us **by NOON tomorrow, Friday, Feb. 24.**

How about this as a possible statement:

Our work with TOR focuses on international audiences that face Internet censorship and lack press freedom to a degree that protecting one's identity can be a matter of life-or-death. We are providing news seekers online access to reliable news and information that they might not otherwise get.

Optional – do we want to say anything?
Clearly, it is unfortunate that some individuals might use such tools for nefarious purposes.

Welcome your thoughts and guidance on the subject:

- Tish

Letitia King
Director, Office of Public Affairs
Broadcasting Board of Governors
330 Indepedence Ave, SW
Washington, DC 20237
Office [redacted]
Mobile: [redacted]
[redacted]
www.bbg.gov
Twitter: @LetitiaKing

Iran National Science Found $

From: Roger Dingledine
To: Kelly DeYoe; Sho Ho; Ken Berman
Cc: [redacted] (b) (6)
Subject: Getting together Oct 7?
Date: Wednesday, September 23, 2009 8:18:36 AM

Hi folks,

A) I'm going to be in town Oct 5-6 for an NSF grant review panel. Any interest in getting together on Oct 7?

B) We've been hearing rumors of massive crackdowns in Iran in the past week -- the "all ssl is blocked again" sort of rumors. We're having difficulty finding clueful people on the inside who have tested, though. Do you have any useful rumors on your side?

--Roger

From: Kelly DeYoe
To: Andrew Lewman
Cc: Ken Berman
Subject: Invitation to attend Hill briefing on BBG Internet Anti-Censorship program
Date: Friday, July 01, 2011 4:27:33 PM

Andrew, on behalf of Ken, I'd like to invite you to participate in a briefing here on Capitol Hill in Washington DC on Wednesday July 20th and Thursday July 21st. We will be briefing staffers from both the Senate and House of Representatives, as well as the National Security Council, on the BBG Internet Anti-Censorship program, and would like to offer you the opportunity to discuss the role Tor plays in the success of our program as well as provide a demonstration.

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,

Kelly

From: Roger Dingledine
To: Kelly DeYoe
Cc: Ken Berman; Steven J. Murdoch
Subject: Kelly, meet Steven
Date: Friday, December 14, 2007 1:40:41 PM

Hi Kelly,

Here's an introduction to Steven Murdoch, who's working on the new Tor USB image. We've been building a list of questions -- mostly of the "should we configure it this way or that way" variety -- and we're hoping your area experts in China and Iran can provide some guidance. Steven can take it from here.

Steven: other good people to ask would probably be Chris Walker, Dmitri Vitaliev, and Ethan Zuckerman. Heck, you could involve them all in one big email thread. :)

Thanks!
--Roger

From: Roger Dingledine
To: [redacted]; Ethan Zuckerman
Subject: Ken and Kelly should meet Ethan
Date: Monday, November 06, 2006 11:04:33 PM

Hi Ken, Kelly, Ethan,

I should introduce you to each other.

Ken and Kelly work at the International Broadcasting Bureau, which helps support Voice of America, Radio Free foo and bar, etc. Their goal is to work on freedom of access so people around the world can reach IBB's Internet resources. They have a particular focus on China and Iran. They're also one of the major funders of Tor now (yay).

Ethan is a fellow at the Berkman Center, is a blogger and helps lead Global Voices Online (http://www.globalvoicesonline.org/), and also works with OSI to help direct some of their funding. Some URLs related to Tor-and-Ethan:
http://www.ethanzuckerman.com/blog/?p=1019
http://www.ethanzuckerman.com/blog/?p=1015
http://www.ethanzuckerman.com/blog/?p=473

I thought that you would find each other to be good resources. So here you go.

--Roger

SUDAN

From: Roger Dingledine
To: Kelly DeYoe
Cc: Ken Berman
Subject: List of some Tor projects
Date: Tuesday, August 22, 2006 5:49:13 PM

Hi Kelly, Ken,

Here's the list of potential Tor projects I talked about. I wrote it in June, so it could use a bit of updating, but pretty much all of the topics are still outstanding and could really use some attention. Let me know if you want elaboration on any of them, and we'll go from there.

On first glance through them, I would say that the 70k would have us start work on your favorites out of A, C, D, E, F, G, and J. Then the 120k extension would continue work on those plus maybe some of H, I, K, L. Of course, we won't be able to tackle every piece of each of these, even in the 2007 timeframe. But here is a lot of material to work with for the contract. :)

Thanks!
--Roger

A) Reduce the bandwidth load from network-status and server descriptor updates. This is important because the bandwidth overhead from directory updates is quite high for ordinary users, and unbearably high for modem users -- downloading a few extra megabytes per hour is crazy for them. This is easy to do on first thought -- we simply reduce the frequency of fetching updates. This is a fine stop-gap measure, but it is probably not smart as a real solution. The reason here is that when people are getting updates less frequently, they are more quickly and more easily partitioned. So what we want to do is find a way to decrease the update frequency while keeping them synchronized, either all together or in batches, without any coordination between them. I believe this can be done, but it will require some careful thought (i.e. research).
Difficulty: Medium. Effectiveness: High.

B) Reduce the bandwidth load from cell overhead -- all Tor cells are 512 bytes, even if their payload isn't full. This would be challenging to do, since we need to make Tor servers understand multiple cell sizes, and it might actually be a bad idea, since one day we plan to get security against end-to-end confirmation attacks and uniform cell size will play a key role. Also, since cells are typically full when we have a lot to say, I don't think this should be first in line.
Difficulty: High. Effectiveness: Low.

C) Pick good entry guard nodes. Dialup users are already in a better position, because they are already used to high latency. Since most of Tor's latency comes from inside the Tor network, it's conceivable that dialup users wouldn't see much slowdown at all. On the other hand, if they're connecting from Iran to Alaska as their first hop, they may have some problems. We need to investigate whether choosing the first hop from a constrained set (e.g. nearby geographically or network-wise) can improve things, and if so how much.
Difficulty: variable. Effectiveness: variable.

D) Blocking resistance. We have a scheme in mind that can be deployed in Iran and China to let them continue to reach the Tor network even

after their government firewall has decided to block connections to the public Tor servers. IBB is funding Tor enough to keep Tor alive, but I would love to actually get to building this.
Difficulty: High. Effectiveness: High.

E) Steganography. We're not going to actually solve this, but we can get better than we currently are. This will make it less possible to identify that a given TCP stream is Tor traffic, rather than simply SSL traffic. Part of this is normalizing the elements in the SSL handshake and headers, and part of it is making sure that Tor directory communications go via Tor circuits. This item only really makes sense if we're tackling item D also.

F) General Tor speed.
Bigger network:
- Gathering more servers
- Keeping current servers happy
- Making it easier to run (and keep running) your server
- Solve the Windows XP Tor bug.
- Incentives to run a server

Scalability:
- How to partition the network so the directory overhead can scale better.

G) A portable Tor+Firefox that can be run without installing any components. Two options:
1) a LiveCD that people can boot that takes care of everything.
Pro: we can make a more secure solution. This is the better approach long-term for a lot of dissidents in risky places.
Con: Hard to do in settings where you can't boot your own media?

2) a package you can fetch and run on Windows that tries to be safe.
Pro: Pretty easy to set up. People seem to like the concept.
Con: You're still running Windows; it's hard to really clean up the evidence and other stuff that Windows leaves around.

3) A combination. Maybe a VM image that people can boot or run as they see fit?

H) Ethan's dilemma: we can't tell a person in the Sudan to use Tor to post her blog entry, because she's the only person there who is using Tor. Somebody watching the Sudanese blogs will correlate, based on timing, topic, and so on. The long-term solution is to get more people in every place using Tor. The short term solution is to look at the software and blog posting tools they want to use, and figure out if some tweaks (e.g. "don't post until") can make a large improvement in security.

I) Write good guides. How should you set up your Tor client to be safe? What should you keep in mind if you need to do various activities, and various protocols? Are some applications safer than others? "How to secure your online behavior if you're a blogger/corporation/whistleblower/etc."
I') Write good FAQs and good user support pages. Maintain them, help users, etc.

J) Localization. Step one here is to get some words that we think are useful. Step two is to get them into lots of languages. This applies for Vidalia/Torbutton/etc, for the Tor website and installation instructions, and for the guides above.

K) Vidalia development. Make it more portable; figure out how to let it launch Tor correctly on more platforms, and to let users become servers via Vidalia clicks. The two Vidalia student developers are doing it for free right now, and presumably they won't keep that up indefinitely.

L) Research questions.

L1) Defenses against the end-to-end correlation attack. Are there some padding or delaying or batching or mixing techniques that can help improve security against somebody watching both ends of the Tor circuit? What about if we make assumptions like having both endpoints running Tor? The SRI contract wants to explore this question. Nick wants to expand our simulations to show that it can't be done in many situations.

L2) The website fingerprinting attack. Read more about this and the others at http://tor.eff.org/volunteer#Research

L3) The routing-zones attack.

L4) Mixing traffic latencies to let people choose their security.

L5) Figure out partitioning / partial network knowledge.

L6) Tor over UDP.

M) Make hidden services not suck. We need a new format and spec, and we need to revamp how it all works to remove the bottlenecks. We could also add authentication and authorization in. A previous NRL contract wanted that but didn't have the money for doing it -- perhaps a future one will. Cryptophone (a German company) wants to use Tor to set up a hidden service for each phone, which would let people maintain an identity that is contactable without even the phone company needing to know where they are.

From: Roger Dingledine
To: Ken Berman
Cc: Andrew Lewman; Kelly DeYoe; Sho Ho
Subject: Meet with Roger, Aug 24?
Date: Tuesday, August 02, 2011 5:23:35 PM

Hi Ken et al,

I'm coming to DC Aug 23 to meet with a SAFER team. Are you around the day after for me to drop by and catch up on things?

If the timing works I'll also plan to bring Chris Soghoian, an IU grad student who has done Tor-related research and now works with the FTC in the DC area trying to teach legislators about the Internet and technology in general. Hopefully it will be good that you two know about each other.

--Roger

From: Ken Berman
To: Roger Dingledine; Kelly DeYoe
Subject: nice job
Date: Friday, December 07, 2007 3:24:40 PM

Roger - just wanted to say what a well written paper the Bldg Incentives into Tor was. Do I have any questions - no...tho I know I should...

What has been the reaction to it?

Ken

7

From: Bennett Haselton
To: roger dingledine; Ken Berman; hiu ho; Kelly DeYoe; [redacted] simson garfinkel
Subject: patent lawyer question: Triangle-Boy algorithm?
Date: Wednesday, December 28, 2005 10:09:30 PM

I believe SafeWeb, which was later bought by Symantec, had a patent on the following algorithm:

- A user in China X connects with a free-world node Y, requesting the contents of a banned Web site. Y is assumed to be an average home DSL user.
- Node Y forwards the request to node Z, a central server.
- Z sends packets back to X that are spoofed to appear as if they came from Y. These packets appear to X as the "response" from Y, and X sees the contents of the banned web site he requested.

This algorithm addresses the question: What if Y, in the free world, wants to be a circumventor node but doesn't want to incur the bandwidth toll? With the T-Boy algorithm, the major bandwidth hog (serving the contents of the banned site) is handled by Z, the central server. (You still need a way to distribute the locations of circumvention nodes like Y to users in China like X, but that's a separate problem.)

The question for a patent lawyer would be: is this patent enforceable, in the event that Symantec decides to block other people from using it? It seems like a pretty simple, almost obvious, idea. It would be worth incorporating into other programs like TOR if it didn't get us in a lot of legal trouble.

The web site http://www.safeweb.com/ appears to have been all but abandoned by Symantec, with content at least two years old. But just because they're no longer interested in SafeWeb's products doesn't mean they'd give away the patents for free :)

-Bennett

[redacted]
http://www.peacefire.org

From: Bennett Haselton
To: Ken Berman; Simson Garfinkel; Roger Dingledine; [redacted] Kelly DeYoe; [redacted]
Subject: places to stay in D.C.?
Date: Thursday, December 29, 2005 2:29:36 PM

I found a $200 round-trip flight from here to D.C. so I figured I could make it to the meeting as well -- flying into BWI Jan 12th and out Jan 14th. Is anybody else going to be staying in a hotel in D.C. the night of the 12th and 13th? If you are, we could split a room. Otherwise, are there any good, reasonably-priced places to stay that are convenient to IBB?

-Bennett

[redacted] http://www.peacefire.org

Help State

From: Ken Berman
To: Roger Dingledine
Cc: [redacted] Kelly DeYoe; Sho Ho; Labowitz, Sarah
Subject: pls offer your guidance
Date: Wednesday, December 16, 2009 9:13:26 AM

Roger – Pls help us out on something. Sarah at State is trying to do some good things in our arena and is receiving some pushback from some of the policy types at State re some of the so-called dual use nature of our tools: good for circumvention, bad for allowing the bad guys to do their thing.

I told Sarah you had addressed both the FBI and members of the IC on this very same issue, and you had some cogent talking points to address these fears.

Would you mind giving her a call tomorrow or Friday (today she is wrapped up in a big conference) and talk her thru some of these issues?

Her number is [redacted]

Thanks very much,

Ken

From: Ken Berman
To: Andrew Lewman
Cc: Kelly DeYoe; Sho Ho; Jill Moss; Roger Dingledine
Subject: Possible Hill Briefing
Date: Monday, June 13, 2011 2:50:07 PM

Andrew - We may be called to a Hill briefing for House and Senate appropriations and authorizers. I have been asked to include Tor, so pls consider joining us. Possible date is week of July 11. Further details coming.

Ken

Chin

From: Bennett Haselton
To: simson l. garfinkel; Ken Berman; [redacted] Kelly DeYoe; [redacted] roger dingledine
Subject: are there any character sequences that identify TOR traffic?
Date: Thursday, December 15, 2005 4:25:39 PM

Are there any headers that are sent back and forth at the beginning if a TOR connection, that would uniquely identify the traffic as TOR traffic?

If so, then that would make it easy for the Chinese to block it at their firewall, without even having to do anything hard like install the software over and over on multiple machines. They already have the capability to add strings to their firewall such that any traffic containing that string is blocked, as they have done for Falun Dafa / Falun Gong etc.

One thing about the Circumventor is that the HTTPS certificates that it generates for each new node, are filled with random strings every time, so that there is no one fixed string that could be used to differentiate Circumventor traffic from any other type of HTTPS traffic.

-Bennett

[redacted]
http://www.peacefire.org

From: Andrew Lewman
To: [redacted]; Roger Dingledine; Karen Reilly
Subject: BBG and Tor
Date: Tuesday, March 09, 2010 11:29:26 AM

Hello Ken and Kelly,

Our contract is coming up for renewal in April. I'd like to put together a contract that better matches what you'd like to see happen with Tor over the next year. In our last meeting, you mentioned mobile, video, and continued circumvention work. Are there others?

Shall we set up a time to meet in a few weeks to discuss the contract?

Thanks!

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

Website: https://www.torproject.org/
Blog: https://blog.torproject.org/
Identi.ca: torproject

From: Toy, Debbie
To: Toy, Debbie; Ken Berman; Danny Bilson; David Dagon; Kelly DeYoe; Flint Dille; Roger Dingledine; Lance James; Paul Syverson; Rob Thomas
Cc: Shultis, John
Subject: CENTRA conference Sept. 20-21, 2006
Date: Friday, September 15, 2006 5:59:08 PM
Attachments: DRAFT AGENDA.doc

To all consultants,
Attached is a copy of the agenda for next week's conference "Esoteric Uses of the Internet," running from Wednesday, Sept. 20 – Thursday, Sept. 21, 2006 at the Hyatt Regency in Reston. (The link to the discussion site is in my previous email below. Please call if you have trouble logging in.)

For those who will be here in time, Rachel has organized a no-host dinner gathering for the 19th (see agenda for information), and a second dinner for all who wish to participate on Wednesday evening.

I look forward to meeting everyone next week.

Debbie

From: Toy, Debbie
Sent: Tuesday, September 12, 2006 11:43 AM
Subject: CENTRA conference Sept. 20-21, 2006

September 12, 2006

To all conference consultants:
The website for the upcoming conference "**Esoteric Uses of the Internet**" (Sept. 20-21, 2006) is now up and running. On this site, you will find the key questions for the conference, organized in a discussion board, which we would like you to participate in prior to the event. You will also find bios of non-government attendees, an agenda, many background articles, and hotel information.

The website is at http://www.stratgroup.org
I or my colleague Sunny Kangarloo will be calling you today to give you a user ID and password.

In addition to participating in the discussion board for both the conference questions and the articles section, please feel free to call or email me with any details you feel have been omitted, or if you have articles you feel would be helpful to the group. I will see that they are added to the site.

Again, I look forward to seeing everyone on the 20th,

Debbie

CENTRA Technology, Inc.
4121 Wilson Blvd. Suite 800
Arlington, VA 22203
Ph: (b) (6)
Fax: (b) (6)
Email: (b) (6)

From: Ken Berman
To: Andrew Lewman; Roger Dingledine
Cc: Kelly DeYoe; Sho Ho
Subject: CFO sign off
Date: Wednesday, May 05, 2010 8:50:00 AM

Andrew - the Agency Chief Financial Officer has signed off on the renewal package and it is with Contracts for execution.
Ken

From: Bennett Haselton
To: Roger Dingledine; Ben Berman; [redacted] Kelly DeYoe
Subject: Chinese "killer app", and reaching the "apathetic Chinese"
Date: Monday, February 20, 2006 8:00:01 PM

In the past we've mentioned that a big problem with the circumvention techniques is that they only reach those users who make the effort to circumvent the firewall -- they don't reach the "apathetic Chinese". Even the circumvention methods that have had large number of users, have reached so few people compared to the population as a whole, that the Chinese don't even consider it worth the effort to block them.

I'd wondered about writing some sort of killer app that we could distribute in China, and then unveil at some point in the future that it contained a secret feature that could be used to circumvent the firewall, but we had considered that writing our own "killer app" might be a bit of a big undertaking.

But consider an alternative. What if we contact a company which makes a popular e-mail program, Web browser, RSS newsreader, file sharing program, or whatever, and ask them about making a Chinese version that not only has circumvention functionality built into it, but has the capability to display content to the users in a place where advertisement-like content would normally go -- so that even the "apathetic Chinese" would see it? And then if they click to view more, their connection is routed through our circumvention system?

This could break us out of the trap of only preaching to the converted, and give us a way for the circumvention app to reach the 'apathetic Chinese'!

Suppose the default home page of Firefox China were to show a generic news page, hosted in the U.S., with innocuous news in Chinese (that doesn't offend the Chinese government, at least at first). So millions of users download and install the Firefox browser. Then suddenly the Chinese news page starts displaying news in Chinese that the Chinese government doesn't like, but on further investigation it turns out that the way Firefox loads the default home page, the page is loaded through our circumvention protocol, and the censors can't block it.

The ideal app for this purpose would be:
- one where it would be unobtrusive for some VoA-controlled content to be the first thing the user sees -- for example, a browser home page, or those "Today on AOL!" pop-ups that come up each time you run AOL Instant Messenger.
- one where the Chinese cannot block the application itself once they realize what we're doing. For example, if this were built into a chat program like Yahoo Messenger, once the Chinese figured it out, they could just block the chat servers, people would stop running the chat program when they realized it was no longer working, and nobody would see our ads.

Could this be something worth pursing together with our other efforts? We could first find out what applications are the most popular ones in China (or, perhaps, where there are deficiencies in that there is not yet any Chinese application to fill a particular need -- e.g. are there Chinese file sharing apps), and I could try reaching out to some of the companies in question.

-Bennett

(b) (6)
(b) (6)

http://www.peacefire.org

From: Ken Berman
To: Roger Dingledine; Shava Nerad; Kelly DeYoe
Subject: [Fwd: Tor schneir]
Date: Friday, March 02, 2007 1:53:56 PM

I hear there was a man in the middle vulnerabilty identified on Tor last week; anyone have the details? Kenb

-------- Original Message --------
Subject: Tor schneir
Date: Fri, 02 Mar 2007 18:31:08 +0000 (GMT)
From: (b) (6)
To: (b) (6)

Tor schneir

From:	Ken Berman
To:	[redacted]; Roger Dingledine; Andrew Lewman
Cc:	[redacted]; Shio Ho
Subject:	alkasir.com
Date:	Thursday, September 30, 2010 10:48:01 AM

Roger and Andrew, meet Walid. He is the designer, owner, manager and general authority on Middle East circumvention issues.

www.alkasir.com

One item of special interest for him, based on our chat yesterday, is how one in his (and your) business fends off potential legal entanglements. Specifically, if the authorities (in Sweden, in his case, where he is operating from) determine that certain types of content run against certain norms, and attempt to take some kind of legal action, what might be compelling arguments in his defence?

No need to go into the details in this email, but a chat might be useful to all!

Ken

From: Bennett Haselton
To: Ken Berman; Hiu Ho; Kelly DeYoe; roger dingledine
Subject: algorithm for TOR to use non-discoverable redundant nodes
Date: Tuesday, December 13, 2005 5:09:36 PM

Here's a simple description of how, if you had multiple redundant connections to circumvention nodes outside of China, you could use the nodes to keep track of each other, without allowing an attacker to exploit weaknesses in the system enabling them to discover nodes that they didn't already know about:

PROBLEM:
If you are in China and you want to access blocked Web sites, you could ask one or more friends outside of China to install a conventional Circumventor program from Peacefire.org that would let you access blocked sites. The problem is that if one or more Circumventors changes IP address, you have no automated way of finding out the new URL, and if only some of the Circumventors are online at any given moment, you would have to try each URL by trial and error to find a working one. We try to find an improvement on this system.

GOALS:
- The system should not allow a user in China who is really an agent of the Chinese censors, to discover a large number of nodes by connecting to the system for any length of time.
- The system should not allow someone outside China, who is really an agent of the Chinese censors, to install a node and use it to discover a large number of other nodes.

NON-GOALS:
- The system assumes that a user "Bob" in China has a way to establish initial contact with two or more people outside China who can install nodes and then give those node locations to Bob.
- If Bob knows about N nodes outside of China and one of those nodes goes *permanently* offline, this solution does not provide an automated way for Bob to find a replacement node; Bob would have to do the "bootstrap" work again to make contact with someone outside China who can install another one and give him the location.
- If one of the circumvention nodes that Bob is using, is really a hostile node, and the operators of that node want to configure it so that it refuses to help Bob maintain contact with the other two nodes, then there is no way to avoid this. All we can do is limit the damage that the hostile nodes are able to do -- to prevent them from discovering other legitimate nodes, for example.

HOW IT WORKS:

When users in the "free world" set up new nodes, those nodes are registered with a central server run by VOA or some other entity. When they are registered, they are assigned a unique identifying string like '9134'. (These IDs can be short because they are generated by the VOA server handing them out, so the VOA server can ensure that each ID handed out is unique.)

Bob in China installs the client, and the client generates a unique ID for itself that also functions as a public encryption key, 'FHGIAHIUHSIDAKXJGHADFG'. This client ID should be long and random enough that it will not collide with the same ID being used by any other

client. (Because these clients do not talk to each other when generating their IDs, that is why the IDs have to be long, so that two clients don't generate the same one.)

Bob in China "bootstraps" himself by getting friends on the outside to install nodes A, B, and C and tell him their locations. When he establishes contact with each node, he also gets the unique identifying string for that node. He also sends each of them his own unique ID, 'FHGIAHIUHSIDAKXJGHADFG'. Each node then tells the central VOA server, "Client node 'FHGIAHIUHSIDAKXJGHADFG' knows about me, circumvention node '9134'."

So at this point, the VOA server knows about Bob's client, and it knows that Bob's client already knows the locations of A, B, and C. Note that at this point, A, B and C do not necessarily know each other's location.

So then, say that C changes IP address. When it comes back online at its new IP address, it tells the VOA server, "I am circumvention node '9134' and I've changed location". The VOA server checks its database and sees that client node 'FHGIAHIUHSIDAKXJGHADFG' (who we know as "Bob") is one of the client nodes that knew about circumvention node '9134' before that circumventor node changed location. The VOA server also knows that circumvention nodes A and B were the other two nodes that Bob knows about. So the VOA server encrypts a message in Bob's public key saying "Circumventor node '9134' has changed to location X". Then it pushes this message to nodes A and B and says "I have a message for user 'FHGIAHIUHSIDAKXJGHADFG' encrypted in his public key." The next time Bob connects to nodes A or B, he retrieves the message, decrypts it, and gets the new location of node '9134'.

Because the updated location of node C is encrypted in Bob's public key before being sent to Bob, that means that nodes A and B cannot find out C's location by snooping on the message before relaying it to Bob, so a hostile circumvention node outside of China cannot use this algorithm to find the location of other circumvention nodes and block them.

(b) (6)
(b) (6)
http://www.peacefire.org

From: Ken Berman
To: [redacted]; Roger Dingledine
Cc: [redacted] Ho
Subject: <No Subject>
Date: Friday, February 18, 2011 2:58:42 PM

Roger/Andrew -

Well, after over ten years, they are not yet at release 1.0.

Do you guys have an opinion on Freenet and how it might be different than Tor? During my Hill briefing, one of the Freenet guys ame out of the back of the room to talk to me.

Ken

http://freenetproject.org/index.html

From: Ken Berman
To: Roger Dingledine
Subject: Re: A roadmap for Tor + IBB
Date: Wednesday, February 08, 2006 9:30:50 AM

OK - we want to move forward on this, Roger. We would like to offer some funding, and also offer the resources of Hiu and Bennett to be used as you see fit for some fixed time per week. For this first effort, we were going to offer $80,000 to you, with more possibly depending on how things evolve.

Give us the particulars for how to establish a contractual relationship with you, name business contact information. [Keep in mind that all this is subject to approval by our Contracting Officer to ensure the expenditures are in line with contract law.]

Ken.

Roger Dingledine wrote:

> On Mon, Jan 23, 2006 at 03:52:41AM -0500, Roger Dingledine wrote:
>
> > On Thu, Jan 19, 2006 at 01:38:07PM -0500, Ken Berman wrote:
> >
> > > Roger - can you say how much funding you were getting from EFF?
> >
> > We got 240k for the two of us for the year. In that time (11/04 to 11/05)
> > we made Win32, OS X, and RPM installers, overhauled the website and docs,
> > added the GUI controller interface and launched the GUI competition,
> > and generally improved the usability, performance, and scalability of the
> > system. We moved from about 40 Tor servers to about 250 servers. Before
> > that, we were getting similar levels of funding through NRL.
>
> Hi Ken,
>
> Here's a follow-up from our meeting last week. I'm glad we got the chance
> to talk face-to-face so we could start to clear up some confusions. The
> high caliber of every Tor developer is what has brought Tor to where it
> is today.
>
> I can imagine three ways for how IBB can help move Tor forward.
>
> A) We need to help keep Tor on track for the six directions listed here:
> http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#Funding
> It makes sense for me to play this role, since I've been juggling
> them all already, and currently I'm trying to do it unfunded while
> hunting for sponsors. Each of these items is a full-time job by itself,
> so spreading myself between all of them will mean that we don't fall

behind on them, and that we can make slow progress on one or two at a time. This is really a necessary first step to keep Tor from suffocating on its popularity.
Plausible milestones: several new Tor releases; reaching 750 Tor servers; milestones on design and research from above list.

B) We get somebody to work on usability and stability for Windows. This comes in two flavors: first, we need to make the Tor server work well on Windows -- this is the number one reason Tor hasn't scaled currently.
Second, we need to make the Tor client usable on Windows -- give it a good GUI, with intuitive controls and intuitive docs. I have some people in mind for this, and it should be done either as one full-time position or two half-time positions.
Plausible milestones: 200 stable Tor servers running on XP; a good package for Windows that includes all the software we need and an intuitive GUI program.

C) We get somebody to work on design, implementation, and deployment for censorship resistance. We already have tens of thousands of users in Iran and China and similar countries, but once we get more popular, we're going to need to be prepared to start the arms race: we need to build the system described in http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#China
This is a full-time job too, because it involves figuring out the requirements, building the Tor components, and making everything usable for this other context too.
Plausible milestones: 1000 volunteers signed up as relays; others?

Based on these, I can imagine four combinations:

1) Just fund A. This will help Tor stay on its feet, but I'll still be partly distracted trying to find funding for the other pieces. Therefore this choice is most suitable as joint funding with some other group.
$120k

2) Fund A and B. This is the best approach if we want to make Tor itself sustainable -- we will end up with a large network of happy users whom we can use to relay traffic from Iran, China, etc. Then we'll be in a great position to tackle the next problem, which is censorship resistance.
$240k

3) Fund A and C. We keep the Tor network afloat, and we roll out some solutions for Iran and China within the next 3-6 months. Then we learn from that and repeat.
$240k

4) Fund all three. We can tackle both at once -- making Tor usable and scalable, and deploying several solutions for blocked countries.
$360k

A multi-year approach will let us get the most work done so we don't have to start wondering about funding again part-way through. If we

can't
fund all three directions at once, I believe that the best way to
move
forward is to fund A+B for the first year, and A+C for the second
year.

I hope this helps to explain some approaches for supporting Tor.
I'm
certainly happy to think about other combinations or other topics
that
you want covered. Please let me know!

--Roger

BBG employees working for for

From: Kelly DeYoe
To: Roger Dingledine
Subject: Re: Contract status update
Date: Tuesday, March 21, 2006 11:35:09 AM

I left a voicemail to check on the contract status this morning, hopefully I'll get an answer back soon and will let you know as soon as I do.

As far as the nature of Bennett and Hiu and working "for" you, I've been mostly deferring on all TOR-related stuff and direction until we have a contract in place with you. Hiu is obviously a full-time employee, and so he is working on projects under his own direction. Bennett is also back under contract with us (renewals go through faster than new contracts), so he is working on a variety of projects for us, you're just only seeing his thoughts more related to TOR. I haven't really been steering him towards the TOR-related projects yet just because we don't have you under contract yet.

Once we actually have a signed contract with you and can begin working with you, I will be trying to provide greater direction on where we're going, and with focusing both Hiu and Bennett's work when it comes to TOR. I'd like us to actually then start having periodic phone calls, and hopefully we can then set some actual goals and milestones for your own work, as well as the work that Hiu and Bennett will do as well.

So for the most part I'm just sort of letting things run as they go right now, as I don't want to get us into any trouble for working with you directly before we actually have a contract with you.

-k

Roger Dingledine wrote:
> On Fri, Mar 17, 2006 at 05:43:04PM -0500, Kelly DeYoe wrote:
>
>>I haven't yet heard anything else either, I'll get an update for you
>>early next week.
>
>
> Ok, sounds good.
>
> In the meantime, is it currently the case that Bennett and Hiu are working
> "for" me?
>
> We never specified details like amount of time per week, or when that
> would start. Bennett has since gone off on his "assuming the hard problems
> we're supposed to be working on are solved, what then?" direction, and
> I've not heard a peep from Hiu. Once we start moving forward, it looks
> like I might need some help from you in organizing them.
>
> Thanks,
> --Roger
>

BBG recommends Tor director ☆

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe
Subject: Re: (FWD) Re: Meeting notes, Jan 11 2008
Date: Tuesday, January 15, 2008 8:07:05 AM

The main Persian blogger Hoder? Kelly, what do you think?
Yes, try for a piece of the DoS $15M! Good luck, but don't hold your breath.....

Roger Dingledine wrote:

> Hi folks,
>
> Two questions for tomorrow's talk:
>
> a) We added Isaac Mao, a well-known blogger from China, as one of the
> Tor directors for the next three years. This is part of a push to
> internationalize the board. We have a good fellow from Germany in mind.
> We'd like to add somebody from the Middle East, but we don't have very
> many great candidates in mind. Do you know some who would be great?
>
> b) See Isaac's mail below. Is this something we should try to get in on?
> Do you know any of the right people behind the scenes?
>
> (You can also read our Tor annual meeting minutes, quoted below, if you
> like. :)
>
> Thanks!
> --Roger
>
> ----- Forwarded message from Isaac Mao <[redacted (b)(6)]> -----
>
> From [redacted (b)(6)]
> To: [redacted (b)(6)]
> Subj[redacted] 11 2008
> Delivery-Date: Sat, 12 Jan 2008 03:54:10 -0500
>
> fyi. maybe you have seen this news too
>
> http://www.defensenews.com/story.php?F=3286113&C=asiapac
>
> * U.S. Launches Inter[redacted]t *
> By WILLIAM MATTHEWS<[redacted (b)(6)]
> subject=Question%20fr[redacted]der>
> Posted 01/07/08 14:51
> The U.S. Congress is funding a modest assault on the great firewall of
> China.
> The newly approved budget for the U.S. State Department includes $15 million
> for developing "anti-censorship tools and services" which could help
> Internet users breach electronic firewalls set up by China, Iran and other
> "closed societies."
> The money is part of the 2008 budget for the State Department's Bureau of
> Democracy, Human Rights and Labor. It is to be awarded competitively to
> software developers to produce "internet technology programs and protocols"
> that enable "widespread and secure internet use" in countries where the
> Internet is now heavily censored.
> The funding bill says the anti-censorship effort is intended "for

the
advancement of information freedom in closed societies, including the Middle
East and Asia."
In a report that accompanies the bill, the House Appropriations Committee
singles out China as a particular target. It cites recent efforts by Chinese
President Hu Jintao "to 'purify' the Internet via further monitoring and
censorship," and through punishing Internet users who engage in uncensored
communications.
The report also decries recent Internet crackdowns by the Cuban and Russian
governments.
The $15 million for anti-censorship technology is a small part of a $164
million "Democracy Fund" that the State Department receives to promote
democracy around the globe, but is a 30-fold increase over the half-million
dollars provided for that purpose in 2007.
A spokeswoman said the State Department "is engaged globally promoting
freedom of expression and the free flow of information on the Internet."
Lawmakers said programs they are funding"should be able to support large
numbers of users simultaneously in a hostile Internet environment."
The Internet in China fits the "hostile" description.
The free-press organization Reporters Without Borders labels China "the
world's most advanced country in Internet filtering."
Chinese authorities monitor Web sites, chat forums, blogs and video exchange
sites, and have imprisoned more than 50 Internet users for postings deemed
to be anti-government, subversive and otherwise objectionable, Reporters
Without Borders reports.
The Chinese government has required companies like Google, Yahoo! and
Microsoft to censor their search engines as a condition for operating in
China. As a result, Internet searches for terms such as "human rights" and
"Taiwan independence" have been blocked.
According to some reports, a Chinese Internet search on Google for
"Tiananmen Square" produces images of buildings and smiling tourists, while
the same search in the United States generates pictures of the Chinese tanks
used to crush pro-democracy protestors in 1989.
Internet censorship in North Korea is worse. Government control makes North
Korea "the world's worst Internet black hole," Reporters Without Borders
says. "Only a few officials are able to access the Web, using connections
rented from China."
Cuba is repressive as well. Virtually all Internet connections are
government-controlled, and "you can get five years just for connecting to
the Internet illegally," the organization says.
The Iranian government boasts that it blocks access to 10 million "immoral"
Web sites, including political and religious sites.
Saudi Arabia, Syria and Egypt also make the Reporters Without Borders list
of "Internet enemies."
The new funding for State Department efforts to defeat Internet censorship
"is a welcome arrow" in a modest arsenal of weapons for defending

Internet
freedom, said Leslie Harris, president of the Center for Democracy and
Technology.
Protecting the Internet from abusive governments is important to supporting
democracy, she said. But accomplishing that "will require the free world to
take much harder positions" against abuses such as censorship. Ultimately,
the odds may favor technology.
"No matter how many restrictions are written in China, the Internet is a
very hard technology to control," Harris said. "The number of users is
growing exponentially ? blogs, e-mail accounts, the magnitude is
extraordinary. At the end of the day, governments trying to control the
Internet
E-mail: [redacted] (b) (6) (b) (6)
subject=
.

On Jan 12, 2008 3:30 AM, Roger Dingledine <[redacted] (b) (6) wrote:

> Meeting minutes: Tor annual meeting, Jan 11, 2008.
>
> Ian calls meeting to order, 11:13am EST.
> Roger, Andrew, Fred, Ian, Nick, Wendy, Rebecca present.
> Frank Rieger also here as an invited observer, with John Gilmore
> and Isaac Mao joining later as invited observers.
>
> Item 0: approve last meeting's minutes.
> No objections to approving last meeting's minutes.
> Approved.
>
> a) Treasurer's report (Andrew).
>
> Andrew gives budget overview. 2007 was a great year for us.
>
> Ian reminds us the details of the MITACS arrangement. First research
> project is Ian's grad student who wants to work on DTLS / UDP transport.
> Conclusion: we'll wait until Ian learns more; he expects to learn more
> in February, and we can decide how much money to put in then.
>
> Andrew: the final question is whether we'll get an audit. Still up in
> the air. Most likely the IRS letter will arrive in March. Andrew will
> continue to look for good auditing firms in anticipation that such a
> letter will arrive.
>
> b) The year in review, and funding prospects (Roger).
>
> 2007 public-facing features:
> - great progress on supporting apps like vidalia and torbutton
> - we made it much easier for clients to be relays
> - we launched the blocking-resistance work
>
> Wendy asks if we should be doing press releases about our progress;
> this causes Roger to add a new agenda item (g) for that question.

Roger's intended 2008 focus:
- Make it even easier for clients to be relays
- Tolerate network scaling (see first section of roadmap-future.pdf)
- Alternate packaging: USB images, VM-based images, LiveCD images, ...
- More organizational depth: an exec dir, fundraising, handling press.

(Isaac Mao arrives: 11:34)

2008 prospective funders:
IBB and France continue as our main prospects.
We submitted a proposal to Google.
Roger is working on a funder that could fund us via ARL (the same
funding avenue as our SRI contract).

c) Broad goals over the next several years.

Roger enumerates some 3-year goals:
- 10000 servers.
- Make it easy (back end and interface) to run an exit relay
- More consistent funding (30-50% of our yearly funding stable)
- Understand anonymity enough to discard our when-Tor-starts warning.
- Outreach and education
  - With law enforcement
  - With media

Nick wants us to win the "global privacy war" (a la global crypto war).
Public opinion. Public awareness of the value of anonymity. Getting an
exec dir who understands this will help a lot.

Fred points out that we've got a good opportunity here for this war,
because right now nobody is taking up our side in the media. So if we
have the right person, we'll be the group that the media always calls.

Frank points out that the war on crypto was won by putting ssl into
the browser. Not just by politics and talking. Fred agrees but says we
need both.

d) Trademark update (Andrew and Wendy).

Andrew and Wendy talked to our mofo lawyers. We're working towards a
licensing document so we can license people who are using our brand.

Ian wants to make sure that the people who get it licensed will put a
little note saying 'Tor and the onion logo are trademarks of...'

Roger agrees, and wants to make a list of the approved projects on the
Tor trademark page, so everybody can know.

Fred says that the Torrify trademark app has now been abandoned. That's
good news.

Andrew says that our trademark is still on track. Now that the two
competing trademarks are withdrawn/abandoned, that goes in our favor.

Roger asks if we should pick up our European trademark filing discussion,
or just leave it alone? Andrew reminds us that the Madrid filing was
potentially very expensive.

Frank explains that there's a prohibition against registering every-day
terms in Europe, and speculates that Tor counts.

Roger asks Frank to look into doing it in Germany. Frank needs an example
application. Andrew has one of those, and will send it to Frank.

e) New directors.

Frank wants to see more focus on long-term: developing the parts of Tor
that are not dependent on exit nodes: hidden services, making exit nodes
more dynamic so they can survive better.

John wants to see bylaws and other docs. What form of protections do we
have for directors? Andrew is still looking into this -- board insurance
is tricky because we're in a category that most insurance companies
don't have a category for.

Isaac is excited to spread the word about Tor in many different countries.
He's quite familiar with Web 2.0 approaches and getting word out that
way. Along with tutorial / outreach program, we should try to simplify
the user interface (installation, configuration) as well. Viral marketing
plan. Isaac is ready to start right away.

We delay actual elections until the end of the agenda, so Ian and Isaac
can stay on the call.

f) The exec dir hunt.

Ian had a good set of questions about an exec dir. Fred had some good
answers. Ian and Fred will assemble answers and send them back.

Fred graciously relents to be the executive director search committee
chair.

Ian moves that Fred will be chair of above.
Roger seconds.
Further discussion? "Thanks Fred!"
No objections. Passed.

John asks if we've considered a search firm. Fred and John will talk about
that more offline.

Fred will write a few wish-list bullet points and Roger will make a web
page out of it, so people know we're looking.

g) Should we be doing press releases?

Roger thinks this should be a major bullet point on the exec dir "desired
skills" list.

Rebecca says press releases are nice and all, but what we really need
is to develop relationships with journalists.
"Cultivating the media."

Roger suggests that that's a great thing to do once we have the bandwidth
for it. Let's keep this in mind, and also put it on our "3-year vision"
list.

e) Director elections

(Ian, Frank, John, and Isaac hang up.)

Andrew moves to reelect Ian to his director position.
Wendy seconds.
Nobody opposed.
Motion Passes. Ian is a director for three more years.

Roger moves to elect Isaac Mao to the director position that is currently
Rebecca's.
Fred seconds.
Nobody opposed.
Motion passes. Isaac is now a director for three years.

Wendy moves to thank Rebecca for her fine work as a director.
Roger seconds.
General agreement.
Motion passes.

Rebecca is excited to stay as an active contributor, particularly with
respect to educating journalists and users in Asia.

Any final topics?
No final topics.

Andrew moves to adjourn.
Adjourned at 12:38.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.6 (GNU/Linux)

iD8DBQFHh8Pz61qJaiiYi/URAp55AKDH4g8iloOXWJvZsyt/QrJM+Q1KIgCfXTVm

szx/E2WR4jzsGEdfx9EQLk4=
=3hbd
-----END PGP SIGNATURE-----

From: Ken Berman
To: Roger Dingledine; Kelly DeYoe
Subject: RE: (FWD) Notes from ITSG meeting, Oct 22-23
Date: Monday, November 24, 2008 3:46:35 PM

Great stuff, thanks for this and the goggle email...Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Saturday, November 22, 2008 1:19 AM
To: Kelly DeYoe
Cc: Ken Berman
Subject: (FWD) Notes from ITSG meeting, Oct 22-23

And here are the more details about the FBI conference I told you about. Keeping FBI informed of (and using!) Tor contributes to project and network sustainability.

--Roger

----- Forwarded message from Roger Dingledine <[redacted] -----

Date: Mon, 3 Nov 2008 00:12:18 -0500
From: Roger Dingledine <[redacted]
To: [redacted]
Subject: Notes from ITSG meeting, Oct 22-23

[Please don't spread this document around. The conference was one of those "not for attribution, now we can talk freely" sort of gigs. I figure that means I can summarize it internally.]

On Oct 22-23, I met with about 50 DoJ/FBI agents in San Diego. The context was an "industry and government" conference series they run, which was born out of the CALEA / lawful intercept / key escrow debacles. Now they gather people from industry together twice a year to talk to them early in the process about how law enforcement is going and what capabilities they would benefit from, so industry can put in the backdoors early in the design process when they're still cheap.

I was there on a panel about anonymity with John Bashinski (of Cisco, but before that from Zero-Knowledge Systems) and Christian Grothoff (author of Gnunet, now a CS professor at Denver University). I only got about 20 minutes for my talk, so I focused on "who uses Tor and why -- all the various good uses of an anonymity system". I also put in a slide or two about bad people on the Internet, to counter the traditional "sure, I admit there are good uses, but aren't you destroying the world too?" questions.

The talk was quite well received overall. Most people recognized that Tor has good uses -- in fact, some of the agents in the audience told me they use Tor for their work already. One agent who works in the "innocent images unit" (how's that for a unit title) told me that he uses Tor every day for his work. Recall that I got the same statement from the FBI agent I met with in Indiannapolis. I wonder how we can make better use of these non-attributable quotes.

Another interesting response was "Wow, that was great. There are so many landmines in that topic here, and you managed to avoid them all." I

suppose that's a good thing. :)

One of the key points here is the narrow audience they had. I heard many of them say "I'm so glad we get this opportunity to interact with the rest of industry". But the industry representatives were basically Microsoft, Google, Yahoo, AOL, Cisco, and a few others. Not really a good cross-section of the whole community doing innovation. I asked whether they had other outreach conferences (human rights, civil liberties, hacker con audiences, etc), and the answer was that FBI as a whole probably does, but this particular piece of FBI is focused on this small segment of industry, so that's what outreach means for them.

I also noticed that pretty much all the industry talks contained the phrase "We cooperate fully with the FBI". Boy, that's a phrase we are steering clear of.

I now expect to have invitations from many FBI groups around the east coast to come talk to them in more detail. One of the downsides I'm beginning to realize is the high rate of churn of good technical people at FBI. Once they learn enough useful technical stuff, they can get higher-paying jobs elsewhere. So is my goal of training all the FBI people about Tor and anonymity a losing proposition? Some people say that FBI is really good at maintaining its institutional memory, despite the turnover rate. Need to learn more.

One of the most interesting presentations was on their "Going Dark" initiative. They realize that the amount of darkness (stuff they can't observe with their current mechanisms and plans, e.g. due to encryption or jurisdiction or uncooperative ISPs) is increasing exponentially with time. They proposed some ways to address the darkness, but the industry side of the audience rightly pointed out that each of their points would only be a linear fix -- that is, not really address the problem at all.

Some of them are coming to accept that they need radically different solutions, since trying to claw back the progress of security technology really isn't going to work long-term. Worse, they suffer from the "plus one" effect -- just because a new technology comes out doesn't mean the old one goes away, so the set of technologies they need to know how to observe just keeps going up. The "old style" pre-wiretap approaches are hideously expensive and cumbersome though -- I heard the stat that the whole Bureau can only do something like 350 physical breakin jobs a year. So our concern that a physical attack is just as reasonable as an eavesdropping attack may be off-base, at least with respect to this threat class.

They also confirmed our assumption that law enforcement below the federal level has gone pretty much entirely dark already.

The other informative talk was from the #2 guy in the Bureau. He did the usual "zip in zip out" style of keynote. His talk was full of bold demands like "we must leave no hideouts left on the Internet for bad people". Another statement that stuck in my mind was how our colleagues in the EU have recently rolled out data retention, and he expects to see that in this country "very soon".

Another point I didn't realize was significant until afterwards was his demand that they need to move forward with new monitoring initiatives, and they can't afford to keep waiting until industry standardizes them. Apparently some people in their organization are very upset that the telcom industry has been so slow at coming to standards on how to put in

backdoors. One of the Microsoft people there had a fantastic response, which was "hey, we *can't* build something unless it's a standard. The DoJ guys smack us down whenever we try to do that."

Overall, the industry folks I met were pretty realistic about how hard tapping the Internet would be in practice, as well as the likelihood that taps would catch bad people vs good people. They weren't excited at all to deploy any solutions. I got the feeling that a lot of them were the same people who went through (and won) the crypto wars.

Since I'm not "industry" I'm unlikely to be invited back for another of these conferences, unless they end up with another topic for which I'd be a good speaker. (Alas, I'm pretty much a one-trick pony when it comes to this particular area.) But I do expect to hear back from some of the agents and go talk to their groups in more detail. So if there are any questions or topics you want me to bring up next time I talk to them, please let me know.

--Roger

----- End forwarded message -----

ARM RACE
/RUSSIA
((RUSSIAN DEPLOYMENT PLAN

From: Roger Dingledine
To: Ken Berman; Kelly DeYoe
Subject: Re: (FWD) Re: Meeting notes, Jan 11 2008
Date: Tuesday, January 15, 2008 5:03:23 PM

On Tue, Jan 15, 2008 at 08:07:05AM -0500, Ken Berman wrote:
> The main Persian blogger Hoder? Kelly, what do you think?
> Yes, try for a piece of the DoS $15M! Good luck, but don't hold your
> breath.....

Hi folks,

I just chatted with Paul Syverson about the Russian deployment plan.

A couple of questions:

1) We have a list of 100k addresses. Would it make sense to send to say 5k of them, and put out any fires, and continue from there? If we actually add most of those (or some of those plus their friends), that will be a pretty big increase in overall load on the Tor network; so they might have a better experience if they aren't all dumped in on the same day.

2) Should we get them all using bridges, or just vanilla Tor? Right now the Tor network works fine in Russia. Do you have an intuition about how quickly that might change if they wanted it to? I don't know how Russia's Internet filtering mechanisms work.

We could just get them using vanilla Tor. This would be useful for them, up until when the arms race starts. And it's certainly the most convenient way to use Tor. (That's why there are so many Tor users in China already.)

But that doesn't prepare them for being able to adapt once blocking starts; and it doesn't give us our full test case to learn from.

Perhaps we could explain it as "Tor is trying out their 'next generation' version, that includes this new feature called bridges. You can use it either the old way or the new way."?

More as I think of more,
--Roger

From: Roger Dingledine
To: Ken Berman; Kelly DeYoe
Subject: Re: (FWD) Re: Meeting notes, Jan 11 2008
Date: Tuesday, January 15, 2008 10:59:35 AM

On Tue, Jan 15, 2008 at 08:07:05AM -0500, Ken Berman wrote:
> The main Persian blogger Hoder? Kelly, what do you think?
> Yes, try for a piece of the DoS $15M! Good luck, but don't hold your
> breath.....

Great; I'll ask you for more details today during the call.

Also, take a brief look at
https://www.torproject.org/svn/trunk/doc/design-paper/roadmap-future.pdf

Some of the section titles will be self-explanatory, and I'll aim to get explanations of the rest into the doc over the next few weeks. I bet you'll recognize a lot of the topics in any case. A lot of these are topics I'd like to tackle more thoroughly in 2008.

In other news, the NGO we've been working with in France has given us a bit more funding, and they're applying (to *their* funders) for several more years of funding with us in mind. So that's good news all-around.

We've also tracked down our Farsi translator, and we're encouraging him to update the Vidalia translations.

Thanks,
--Roger

BBG giving instructions on Russia plan

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe
Subject: Re: (FWD) Re: Meeting notes, Jan 11 2008
Date: Wednesday, January 16, 2008 3:42:06 PM

Roger Dingledine wrote:

> On Tue, Jan 15, 2008 at 08:07:05AM -0500, Ken Berman wrote:
>
> > The main Persian blogger Hoder? Kelly, what do you
> > think?
> > Yes, try for a piece of the DoS $15M! Good luck,
> > but don't hold your
> > breath.....
>
> Hi folks,
>
> I just chatted with Paul Syverson about the Russian deployment
> plan.
>
> A couple of questions:
>
> 1) We have a list of 100k addresses. Would it make sense to send
> to
> say 5k of them, and put out any fires, and continue from there? If
> we actually add most of those (or some of those plus their
> friends),
> that will be a pretty big increase in overall load on the Tor
> network;
> so they might have a better experience if they aren't all dumped
> in on
> the same day.

Yes it would....

> 2) Should we get them all using bridges, or just vanilla Tor?
> Right now
> the Tor network works fine in Russia. Do you have an intuition
> about how
> quickly that might change if they wanted it to? I don't know how
> Russia's Internet filtering mechanisms work.

Vanilla, no filtering yet.....

> We could just get them using vanilla Tor. This would be useful for
> them,
> up until when the arms race starts. And it's certainly the most
> convenient way to use Tor. (That's why there are so many Tor users
> in
> China already.)
>
> But that doesn't prepare them for being able to adapt once
> blocking
> starts; and it doesn't give us our full test case to learn from.

Yep, none of us are really ready for prime-time.....

> Perhaps we could explain it as "Tor is trying out their 'next
> generation'

version, that includes this new feature called bridges. You can use it
either the old way or the new way."?

More as I think of more,
--Roger

From: Andrew Lewman
To: Ken Berman
Cc: Kelly DeYoe
Subject: Re: Egypt, Satellite, BGAN, thoughts
Date: Tuesday, February 01, 2011 8:13:43 AM

On Tue, 1 Feb 2011 08:04:12 -0500
Ken Berman <[redacted] wrote:

> We have 14 BGAN terminals, but they are all deployed!

That's good! Anyone tried tor over them?

--
Andrew
pgp 0x74ED336B

From: Ken Berman
To: Andrew Lewman; Kelly DeYoe
Subject: RE: Egypt, Satellite, BGAN, thoughts
Date: Tuesday, February 01, 2011 7:11:05 AM

Andrew - no one has ever used BGAN w/Tor, here. What do you mean by "spare" equipment? Ken

-----Original Message-----
From: Andrew Lewman [mailto:[redacted (b) (6)]
Sent: Monday, January 31, 2011 5:28 PM
To: Ken Berman; Kelly DeYoe
Subject: Egypt, Satellite, BGAN, thoughts

Hello Kelly and Ken,

I'm sure you are aware of the situation in Egypt all too well. I'll keep this short. The last ISP in Egypt, Noor, has just gone offline. Activists are telling us that landlines are going down too.

Do you have any experience, or spare equipment, with Tor over BGAN/Satellite?

Thanks!

--
Andrew
pgp 0x74ED336B
[redacted (b) (6)]

From: Andrew Lewman
To: Ken Berman
Cc: Kelly DeYoe
Subject: Re: Egypt, Satellite, BGAN, thoughts
Date: Tuesday, February 01, 2011 7:38:10 AM

On Tue, 1 Feb 2011 07:11:05 -0500
Ken Berman <(b) (6) wrote:

> Andrew - no one has ever used BGAN w/Tor, here. What do you mean by
> "spare" equipment? Ken

Ok. We had some testing with Tor and BGAN in Iraq, but it wasn't
detail enough, other than "it works".

I didn't know if you had equipment hanging around. Apparently not.

Thanks!

>
> -----Original Message-----
> From: Andrew Lewman [mailto:(b) (6)
> Sent: Monday, January 31, 2011 5:28 PM
> To: Ken Berman; Kelly DeYoe
> Subject: Egypt, Satellite, BGAN, thoughts
>
> Hello Kelly and Ken,
>
> I'm sure you are aware of the situation in Egypt all too well. I'll
> keep this short. The last ISP in Egypt, Noor, has just gone offline.
> Activists are telling us that landlines are going down too.
>
> Do you have any experience, or spare equipment, with Tor over
> BGAN/Satellite?
>
> Thanks!
>

--
Andrew
pgp 0x74ED336B

From: Ken Berman
To: Andrew Lewman
Cc: Kelly DeYoe
Subject: RE: Egypt, Satellite, BGAN, thoughts
Date: Tuesday, February 01, 2011 8:04:12 AM

We have 14 BGAN terminals, but they are all deployed!

-----Original Message-----
From: Andrew Lewman [mailto:[redacted (b) (6)]
Sent: Tuesday, February 01, 2011 7:38 AM
To: Ken Berman
Cc: Kelly DeYoe
Subject: Re: Egypt, Satellite, BGAN, thoughts

On Tue, 1 Feb 2011 07:11:05 -0500
Ken Berman <[redacted (b) (6)]> wrote:

> Andrew - no one has ever used BGAN w/Tor, here. What do you mean by
> "spare" equipment? Ken

Ok. We had some testing with Tor and BGAN in Iraq, but it wasn't
detail enough, other than "it works".

I didn't know if you had equipment hanging around. Apparently not.

Thanks!

>
> -----Original Message-----
> From: Andrew Lewman [mailto:[redacted (b) (6)]
> Sent: Monday, January 31, 2011 5:28 PM
> To: Ken Berman; Kelly DeYoe
> Subject: Egypt, Satellite, BGAN, thoughts
>
> Hello Kelly and Ken,
>
> I'm sure you are aware of the situation in Egypt all too well. I'll
> keep this short. The last ISP in Egypt, Noor, has just gone offline.
> Activists are telling us that landlines are going down too.
>
> Do you have any experience, or spare equipment, with Tor over
> BGAN/Satellite?
>
> Thanks!
>

--
Andrew
pgp 0x74ED336B

From: Ken Berman
To: Roger Dingledine
Cc: Andrew Lewman; Kelly DeYoe; Sho Ho
Subject: RE: DARPA contact
Date: Tuesday, July 06, 2010 3:13:59 PM

Nope, never met....

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Tuesday, July 06, 2010 11:30 AM
To: Ken Berman
Cc: Andrew Lewman; [redacted] [redacted]
Subject: DARPA contact

Hi Ken,

Have you met Drew Dean from DARPA yet? If not, I should do an introduction.

--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe; Shava Nerad; Hiu Ho
Subject: Re: First draft of blocking-resistance design
Date: Tuesday, January 30, 2007 8:43:21 AM

Is it time for a status phone call? Th Feb 1st at 3:00??

Ken

Roger Dingledine wrote:

> On Mon, Nov 20, 2006 at 08:17:03AM -0500, Roger Dingledine wrote:
>
> > Take a look at
> > http://tor.eff.org/svn/trunk/doc/design-paper/blocking.pdf
> > for our first draft on how to adapt Tor to have a
> > blocking-resistance
> > component.
>
> Hi folks,
>
> I presented this design a few weeks ago at the CCC congress in
> Berlin,
> and there's a snazzy video here:
>
> http://freehaven.net/~arma/23C3-1444-en-tor_and_china.m4v
> http://freehaven.net/~arma/slides-23c3.pdf
>
> Ken will be happy to learn that I have started using VoA as one of
> the example websites in my talks. :)
>
> Thanks,
> --Roger

From: Roger Dingledine
To: Ken Berman
Cc: Kelly DeYoe; Jill Moss; [redacted]
Subject: Re: Fwd: MEDIA Query - TOR - other uses
Date: Thursday, February 23, 2012 6:57:55 PM

On Thu, Feb 23, 2012 at 11:22:34PM +0000, Ken Berman wrote:
> Roger,
> Suggestions for a response?
> Ken

The response below sounds plausible. Sounds like the journalist is trying to stir up some controversy, and "Internet used for crime" isn't working well enough anymore so she's trying something different.

I'm cc'ing Andrew in case he has more to add.

--Roger

> A Boston Globe reporter is inviting our comment on a story she is doing related to TOR. She understands we work with them in our web anti-censorship program. Her piece focuses on the fact that there are reports that the TOR anonymizing technology is used for other purposes (including the silk road drug trade and child pornography).
>
> She asked if we were aware of those reports and if we had a comment. She?d like to hear from us by NOON tomorrow, Friday, Feb. 24.
>
> How about this as a possible statement:
>
> Our work with TOR focuses on international audiences that face Internet censorship and lack press freedom to a degree that protecting one?s identity can be a matter of life-or-death. We are providing news seekers online access to reliable news and information that they might not otherwise get.
>
> Optional ? do we want to say anything?
> Clearly, it is unfortunate that some individuals might use such tools for nefarious purposes.
>
> Welcome your thoughts and guidance on the subject:
>
>
> - Tish
>
>
> Letitia King
> Director, Office of Public Affairs
> Broadcasting Board of Governors
> 330 Indepedence Ave, SW
> Washington, DC 20237
> Office [redacted]
> Mobile: [redacted]
> [redacted] mailto:[redacted]
> www.bbg.gov<http://www.bbg.gov>
> Twitter: @[redacted]
>

From: Ken Berman
To: [redacted] Roger Dingledine
Cc: Kelly DeYoe; Jill Moss
Subject: RE: Fwd: MEDIA Query - TOR - other uses
Date: Friday, February 24, 2012 7:19:13 AM

Would have included Andrew, sent from my phone, and I didn't have his contact info. Thx, all.
Ken

After March 2nd, you can reach me at [redacted]

-----Original Message-----
From: [redacted] [mailto:[redacted]
Sent: Thursday, February 23, 2012 8:04 PM
To: Roger Dingledine
Cc: Ken Berman; Kelly DeYoe; Jill Moss
Subject: Re: Fwd: MEDIA Query - TOR - other uses

On Thu, Feb 23, 2012 at 06:57:42PM -0500, [redacted] wrote 1.7K bytes in 41 lines about:
: The response below sounds plausible. Sounds like the journalist is trying
: to stir up some controversy, and "Internet used for crime" isn't working
: well enough anymore so she's trying something different.
:
: I'm cc'ing Andrew in case he has more to add.

If I guess right, I spent 2h with this reporter a few weeks ago. She is an investigative reporter looking into silk road and child porn. Her initial story was just that tor was a botnet run by unknowns. She was surprised to learn the reality. Your PR response sounds good.

--
Andrew
http://tpo.is/contact
pgp 0x74ED336B

From: [redacted]
To: Roger Dingledine
Cc: Ken Berman; Kelly DeYoe; Jill Moss
Subject: Re: Fwd: MEDIA Query - TOR - other uses
Date: Thursday, February 23, 2012 8:03:49 PM

On Thu, Feb 23, 2012 at 06:57:42PM -0500, [redacted] wrote 1.7K bytes in 41 lines about:
: The response below sounds plausible. Sounds like the journalist is trying
: to stir up some controversy, and "Internet used for crime" isn't working
: well enough anymore so she's trying something different.
:
: I'm cc'ing Andrew in case he has more to add.

If I guess right, I spent 2h with this reporter a few weeks ago. She is an investigative reporter looking into silk road and child porn. Her initial story was just that tor was a botnet run by unknowns. She was surprised to learn the reality. Your PR response sounds good.

--
Andrew
http://tpo.is/contact
pgp 0x74ED336B

From: Andrew Lewman
To: Ken Berman
Cc: Kelly DeYoe; Roger Dingledine
Subject: Re: Free on the afternoon of the 20th?
Date: Friday, January 15, 2010 7:59:12 AM

On 01/15/2010 07:47 AM, Ken Berman wrote:
> Leaving at 3:00 for a Drs appt, but, sure, 1:30 or so? Ken

1:30 it is. Thanks!

>
> -----Original Message-----
> From: Andrew Lewman [mailto:[redacted]
> Sent: Thursday, January 14, 2010 10:27 PM
> To: Ken Berman; Kelly DeYoe
> Cc: Roger Dingledine
> Subject: Free on the afternoon of the 20th?
>
> Hello Ken and Kelly,
>
> I'm going to be in town on the afternoon of the 20th. If you're free, I'd like to catch up to see how things are going, tell you about what we're up to, and here some feedback from your customers about Tor and what's working and what's not around the world.
>
> We've heard from some people that RFA is using Tor to upload videos safely. This is great, but wondering how their performance is, and if there are some tricks we can help them do to make it faster.
>
> Thanks!

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

Website: https://torproject.org/
Blog: https://blog.torproject.org/
Identi.ca: torproject

From: Ken Berman
To: Andrew Lewman; Kelly DeYoe
Cc: Roger Dingledine
Subject: RE: Free on the afternoon of the 20th?
Date: Friday, January 15, 2010 7:47:42 AM

Leaving at 3:00 for a Drs appt, but, sure, 1:30 or so? Ken

-----Original Message-----
From: Andrew Lewman [mailto:[redacted (b) (6)]
Sent: Thursday, January 14, 2010 10:27 PM
To: Ken Berman; Kelly DeYoe
Cc: Roger Dingledine
Subject: Free on the afternoon of the 20th?

Hello Ken and Kelly,

I'm going to be in town on the afternoon of the 20th. If you're free, I'd like to catch up to see how things are going, tell you about what we're up to, and here some feedback from your customers about Tor and what's working and what's not around the world.

We've heard from some people that RFA is using Tor to upload videos safely. This is great, but wondering how their performance is, and if there are some tricks we can help them do to make it faster.

Thanks!

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

Website: https://torproject.org/
Blog: https://blog.torproject.org/
Identi.ca: torproject

From: Ken Berman
To: Roger Dingledine; Kelly DeYoe
Cc: [redacted] [redacted]
Subject: RE: Followup from last week"s meeting
Date: Tuesday, October 07, 2008 8:39:38 AM

Roger - here is James contact info, and he probably already knows all about Tor.....

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Tuesday, September 23, 2008 8:41 PM
To: Kelly DeYoe; Ken Berman
Cc: [redacted]
Subject: Followup from last week's meeting

Hi folks,

Hope everything is going well with you. Great to see you last week.

Let me know if you have any questions or comments about the roadmap, when you get around to looking at it.

Also, give me a holler when you want me to show up again in person. I'm not so far away, it turns out.

I mailed Ali, and will hopefully connect with Jeremiah.

iFree is in fact focusing on Saudi Arabia as one of its first six countries.

I have a note here that Ken wanted me to meet "James Mulvenon", from CIRA.

Thanks,
--Roger

From: Andrew Lewman
To: Ken Berman
Cc: Kelly DeYoe; Kyle Noori
Subject: Re: FW: Tor + Iran - HELPDESK
Date: Thursday, September 08, 2011 8:50:34 AM

On Wednesday, September 07, 2011 13:54:40 Ken Berman wrote:
> Andrew - any idea whose these people are, soliciting funding for Tor!? I
> remember the message below, but what's the connection with you?

I assume this means you never met Sina or Kim after the introduction ages ago.

Actually, they're asking for help for themselves. We've been working with PNN for the past month on a campaign to spread Tor inside Iran. This has resulted in increased usage, https://metrics.torproject.org/users.html?graph=direct-users&start=2011-06-10&end=2011-09-08&country=ir&dpi=72#direct-users

It's also resulted in thousands of farsi emails to our tor-assistants address asking for help. It seems a few things are happening here:

1) Our get-tor email robot defaults to english when it doesn't understand the commands from the human. Many of these Iranians do not understand english, so they blindly email the address, [redacted] (b) (6) listed in the robot's response. This is the same system used by the entire world, so we default to english, but can also respond in mandarin, russian, french, german, arabic, etc.

2) The whole diginotar fiasco has scared lots of people in country, https://blog.torproject.org/category/tags/ohdiginotaryoudidnt. This has actually helped drive more people to Tor once they understand what's going on and how useless the current CA model for ssl certificates really is at protecting anything (other than the CA profit margin).

3) Sina and crew are already very active in Iran, native farsi speakers, in some cases exiled Iranians themselves, and are trying to help PNN and Tor. The idea is to setup a landing page website, in all farsi, along with a fully farsi-only get-tor email robot. This should solve most of the "I don't understand english" problems we're seeing today.

4) The farsi translation of tor's website is wrong and needs to be reworked. This isn't helping people in Iran get accurate information. It's wrong from a translated text (someone not technical did the translation) and the css/left-to-right alignment is wrong. We have an open ticket on this, https://trac.torproject.org/projects/tor/ticket/3806

The idea, as discussed with PNN and Sina, is rather than give Tor funding for: farsi translations, farsi landing page, farsi get-tor, and a farsi help desk; Sina's team are the experts, so they should get a person or two to do all of this. This is why Sina is asking for help. I'm sure PNN put him up to it.

An alternate model is to simply hire a technical farsi speaker at Tor and do it all ourselves. This would then have to scale to mandarin, arabic, russian, and soon tor has a massive translation/support team. I'd rather push it off to partners who know the content, can adapt the sites and needs to the locale the best, and who have shown commitment to tor already. An example site is https://iranitor.com/

--

Andrew
pgp 0x74ED336B

From: Ken Berman
To: Andrew Lewman
Cc: Kelly DeYoe; Kyle Noori
Subject: RE: FW: Tor + Iran - HELPDESK
Date: Friday, September 09, 2011 5:01:20 PM

You know, I don't' think I ever met Sina or Kim - if I did, shame on me.

Did Tor ever sign off on the IDIQ contract, btw??

Ken

-----Original Message-----
From: Andrew Lewman [mailto:[redacted]
Sent: Thursday, September 08, 2011 7:51 AM
To: Ken Berman
Cc: Kelly DeYoe; Kyle Noori
Subject: Re: FW: Tor + Iran - HELPDESK

On Wednesday, September 07, 2011 13:54:40 Ken Berman wrote:
> Andrew - any idea whose these people are, soliciting funding for Tor!? I
> remember the message below, but what's the connection with you?

I assume this means you never met Sina or Kim after the introduction ages ago.

Actually, they're asking for help for themselves. We've been working with PNN for the past month on a campaign to spread Tor inside Iran. This has resulted in increased usage, https://metrics.torproject.org/users.html?graph=direct-users&start=2011-06-10&end=2011-09-08&country=ir&dpi=72#direct-users

It's also resulted in thousands of farsi emails to our tor-assistants address asking for help. It seems a few things are happening here:

1) Our get-tor email robot defaults to english when it doesn't understand the commands from the human. Many of these Iranians do not understand english, so they blindly email the address, [redacted] listed in the robot's response. This is the same system used by the entire world, so we default to english, but can also respond in mandarin, russian, french, german, arabic, etc.

2) The whole diginotar fiasco has scared lots of people in country, https://blog.torproject.org/category/tags/ohdiginotaryoudidnt. This has actually helped drive more people to Tor once they understand what's going on and how useless the current CA model for ssl certificates really is at protecting anything (other than the CA profit margin).

3) Sina and crew are already very active in Iran, native farsi speakers, in some cases exiled Iranians themselves, and are trying to help PNN and Tor. The idea is to setup a landing page website, in all farsi, along with a fully farsi-only get-tor email robot. This should solve most of the "I don't understand english" problems we're seeing today.

4) The farsi translation of tor's website is wrong and needs to be reworked. This isn't helping people in Iran get accurate information. It's wrong from a translated text (someone not technical did the translation) and the css/left-to-right alignment is wrong. We have an open ticket on this, https://trac.torproject.org/projects/tor/ticket/3806

The idea, as discussed with PNN and Sina, is rather than give Tor funding for: farsi translations, farsi landing page, farsi get-tor, and a farsi help desk; Sina's team are the experts, so they should get a person or two to do all of this. This is why Sina is asking for help. I'm sure PNN put him up to it.

An alternate model is to simply hire a technical farsi speaker at Tor and do it all ourselves. This would then have to scale to mandarin, arabic, russian, and soon tor has a massive translation/support team. I'd rather push it off to partners who know the content, can adapt the sites and needs to the locale the best, and who have shown commitment to tor already. An example site is https://iranitor.com/

--
Andrew
pgp 0x74ED336B

From: Andrew Lewman
To: Ken Berman
Cc: Kelly_DeYoe; Kyle Noori
Subject: Re: FW: Tor + Iran - HELPDESK
Date: Saturday, September 10, 2011 12:17:16 AM

On Fri, Sep 09, 2011 at 04:01:20PM -0400, [redacted] wrote 3.3K bytes in 93 lines about:
: You know, I don't' think I ever met Sina or Kim - if I did, shame on me.

They were at the Google censorship meeting in 2009 as part of Access. They broke off from Access in November 2011. Kim lives in DC. I can introduce you two if you'd like.

: Did Tor ever sign off on the IDIQ contract, btw??

We haven't received the corrected contract yet. I talked to Diane and there were a few technical errors in the proposed contract she was fixing before sending another copy over to me. This was supposed to happen Thursday. I owe her a call on Monday.

--
Andrew
pgp key: 0x74ED336B

From: Ken Berman
To: Andrew Lewman
Cc: Kelly DeYoe; Kyle Noori
Subject: RE: FW: Tor + Iran - HELPDESK
Date: Monday, September 12, 2011 10:01:20 AM

Yes, pls hook us up with Kim.....

-----Original Message-----
From: Andrew Lewman [mailto:[redacted (b) (6)]
Sent: Friday, September 09, 2011 11:17 PM
To: Ken Berman
Cc: Kelly DeYoe; Kyle Noori
Subject: Re: FW: Tor + Iran - HELPDESK

On Fri, Sep 09, 2011 at 04:01:20PM -0400, [redacted (b) (6)] wrote 3.3K bytes in 93 lines about:
: You know, I don't' think I ever met Sina or Kim - if I did, shame on me.

They were at the Google censorship meeting in 2009 as part of Access. They broke off from Access in November 2011. Kim lives in DC. I can introduce you two if you'd like.

: Did Tor ever sign off on the IDIQ contract, btw??

We haven't received the corrected contract yet. I talked to Diane and there were a few technical errors in the proposed contract she was fixing before sending another copy over to me. This was supposed to happen Thursday. I owe her a call on Monday.

--
Andrew
pgp key: 0x74ED336B

From: Ken Berman
To: Roger Dingledine
Cc: Jacob Appelbaum; Andrew Lewman; Kelly DeYoe
Subject: RE: Security concerns with Ultrasurf
Date: Wednesday, December 07, 2011 8:23:15 AM

Thx, Roger. Will only share with Kelly.
Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Wednesday, December 07, 2011 8:19 AM
To: Ken Berman
Cc: Jacob Appelbaum; Andrew Lewman
Subject: Re: Security concerns with Ultrasurf

Hi Ken,

We now have an initial draft set of notes from investigating Ultrasurf. I don't think it would be useful or wise to publish this as-is, but I figure that shouldn't stop us from sharing an internal review copy with you so you can keep in the loop. I've attached it here; please don't publish it further.

My early thoughts about the right direction for a revision is to look at the concrete set of things that went wrong in the Ultrasurf design and deployment as a set of *symptoms* for more fundamental underlying problems. Then we should try to make it clearer why the underlying problems are bad, how one might resolve them, and how one might recognize the same problems in other contexts without needing to break out the ida pro debugger and waste a few months.

Thanks,
--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Jacob Appelbaum; Andrew Lewman; Kelly DeYoe
Subject: RE: Security concerns with Ultrasurf
Date: Wednesday, December 07, 2011 8:23:15 AM

Thx, Roger. Will only share with Kelly.
Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted] (b) (6)
Sent: Wednesday, December 07, 2011 8:19 AM
To: Ken Berman
Cc: Jacob Appelbaum; Andrew Lewman
Subject: Re: Security concerns with Ultrasurf

Hi Ken,

We now have an initial draft set of notes from investigating Ultrasurf. I don't think it would be useful or wise to publish this as-is, but I figure that shouldn't stop us from sharing an internal review copy with you so you can keep in the loop. I've attached it here; please don't publish it further.

My early thoughts about the right direction for a revision is to look at the concrete set of things that went wrong in the Ultrasurf design and deployment as a set of *symptoms* for more fundamental underlying problems. Then we should try to make it clearer why the underlying problems are bad, how one might resolve them, and how one might recognize the same problems in other contexts without needing to break out the ida pro debugger and waste a few months.

Thanks,
--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Jacob Appelbaum; [redacted] Kelly DeYoe; Jill Moss
Subject: RE: Roger and Jake in DC next week?
Date: Thursday, October 13, 2011 3:32:15 PM

OK, see you tomorrow. Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Thursday, October 13, 2011 9:06 AM
To: Ken Berman
Cc: Jacob Appelbaum; [redacted]
Subject: Re: Roger and Jake in DC next week?

On Wed, Oct 12, 2011 at 07:38:53AM -0400, Ken Berman wrote:
> How about 9:30 on Friday?

Sounds great. Nathan and Wendy are in town but busy then; but I think
Karen might still join us.

--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe; Sho Ho; [redacted] (b) (6)
Subject: RE: Getting together Oct 7?
Date: Thursday, October 08, 2009 4:25:45 PM

Thanks, just thinking out loud....

-----Original Message-----
From: Roger Dingledine [mailto:[redacted] (b) (6)
Sent: Thursday, October 08, 2009 10:41 AM
To: Ken Berman
Cc: Kelly DeYoe; Sho Ho; [redacted] (b) (6)
Subject: Re: Getting together Oct 7?

On Wed, Sep 23, 2009 at 04:06:00PM -0400, Ken Berman wrote:
> Oct 7 works for me. Lunch??

Hi Ken,

You mentioned yesterday that you get some push-back from people wondering "what about bad people" with respect to Tor.

A first answer is here:
https://www.torproject.org/faq-abuse.html.en#WhatAboutCriminals

A second answer is: if you have specific people in mind, I'd be happy to come chat with them and walk them through who uses Tor, why bad people are already doing fine, etc. For example, here are the slides I'm using for my FBI talk today:
http://freehaven.net/~arma/slides-fbi-oct09.pdf

--Roger

From: Roger Dingledine
To: Ken Berman
Cc: Kelly DeYoe; Sho Ho; [redacted]
Subject: Re: Getting together Oct 7?
Date: Thursday, October 08, 2009 11:41:09 AM

On Wed, Sep 23, 2009 at 04:06:00PM -0400, Ken Berman wrote:
> Oct 7 works for me. Lunch??

Hi Ken,

You mentioned yesterday that you get some push-back from people wondering "what about bad people" with respect to Tor.

A first answer is here:
https://www.torproject.org/faq-abuse.html.en#WhatAboutCriminals

A second answer is: if you have specific people in mind, I'd be happy to come chat with them and walk them through who uses Tor, why bad people are already doing fine, etc. For example, here are the slides I'm using for my FBI talk today:
http://freehaven.net/~arma/slides-fbi-oct09.pdf

--Roger

From: Kelly DeYoe
To: Roger Dingledine
Subject: Proposed statement of work for contract renewal
Date: Friday, March 14, 2008 7:02:28 PM
Attachments: SOW-Tor3-Mod.doc

Ok, so I got dumped on with 2 other big projects and never got this done until now, sorry. Attached is the proposed modification to our contract for the next 12 month period, these new terms are in addition to the existing ones. Ken has also proposed increasing the funding to $360,000 from the $300,000 this year.

Please let me know right away if you see any problems with any of these new terms. They should mostly look familiar, but it is possible I over-estimated some of your proposals.

I'll be out of the office on Monday, but if there is anything that doesn't look right on this, let's try to talk by Tuesday since we'll need to get everything resolved quickly to make sure the renewal happens on schedule.

-k

From: Kelly DeYoe
To: Roger Dingledine
Subject: Proposed Tor statement of work for IBB
Date: Sunday, March 29, 2009 10:39:23 PM
Attachments: SOW-Tor4-Mod.doc

Roger, here's the proposed statement of work modification for your work for IBB for the next year -- 4 points, all pulled from the proposed performance improvements document you sent.

Let me know what you think, and if any changes need to be made.

-k

From: Ken Berman
To: Roger Dingledine; Kelly DeYoe
Cc: [redacted]
Subject: RE: (FWD) A Practical Congestion Attack on Tor Using Long Paths
Date: Tuesday, December 16, 2008 9:52:38 AM

Oh well....

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Thursday, December 11, 2008 2:09 PM
To: Chris Walker; Ken Berman; Kelly DeYoe
Cc: [redacted]
Subject: (FWD) A Practical Congestion Attack on Tor Using Long Paths

Hi Chris, Ken, Kelly,

Here's a paper draft that I wrote with some Denver University researchers on a more effective version of the "congestion attack" that Steven Murdoch and George Danezis came up with in 2005. This vulnerability is one of the big reasons we're worried about encouraging Tor users to be relays too. (See also section 4.2.1 of the roadmap-full document.)

The good news is that we showed that the attack from Steven and George is no longer practical on the Tor network, since the network has gotten much bigger and has much more traffic.

The bad news is that we came up with a way to make it practical again.

I had thought I had a solution to the new attack:
https://svn.torproject.org/svn/tor/trunk/doc/spec/proposals/110-avoid-infinite-circuits.txt
But then it turned out I didn't:
http://archives.seul.org/or/dev/Dec-2008/msg00001.html

Discussion continues. :)

--Roger

----- Forwarded message from Roger Dingledine <[redacted] -----

Date: Tue, 2 Dec 2008 15:10:56 -0500
From: Roger Dingledine <[redacted]
To: [redacted]
Subject: Re: Roger's periodic status report, Oct 1-Oct 31

On Sat, Nov 29, 2008 at 08:11:24AM -0500, Roger Dingledine wrote:
> Agreed to help Christian Grothoff and his grad student to flesh out
> their "infinite length circuit attack" paper and defenses. My goal is
> to help get the attack details and numbers written down clearly, so we
> will have a headstart on understanding how bad it is and how much we
> need to fix. More on that in November.

Attached is the submission version of the paper. Please don't share it with the outside world yet, until it either gets published or they tech report it. But I think it is quite good work.

Abstract:
In 2005, Murdoch and Danezis demonstrated the first practical congestion attack against a deployed anonymity network. They could identify which relays were on a target Tor user's path by building paths one at a time through every Tor relay and introducing congestion. However, the original attack was performed on only 13 Tor relays on the nascent and lightly loaded Tor network.

We show that the attack from their paper is no longer practical on today's 1500-relay heavily loaded Tor network. The attack doesn't scale because
a) the attacker needs a tremendous amount of bandwidth to measure enough relays in the attack window, and b) there are too many false positives now that many other users are adding congestion at the same time as the attacks.

We then strengthen the original congestion attack by combining it with a novel bandwidth amplication attack based on a flaw in the Tor protocol that lets us build long circuits that loop back on themselves. We show that this new combination attack is practical by demonstrating a working attack on today's deployed Tor network. By coming up with a model to better understand Tor's routing behavior under congestion, we further provide a statistical analysis characterizing exactly how effective our attack is in each case. Finally, we designed a defense against our new attack and are working with the Tor developers to deploy the defense.

--Roger

----- End forwarded message -----

From: Ken Berman
To: Roger Dingledine
Cc: Andrew Lewman; Kelly DeYoe; Sho Ho; Richard J. Bertaut; Gregory Gray
Subject: RE: (FWD) FISMA -- I think we"re clear
Date: Monday, August 09, 2010 3:48:04 PM

Great, thanks very much Wendy/Roger. Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Friday, August 06, 2010 12:05 PM
To: Ken Berman
Cc: Andrew Lewman; [redacted] [redacted]
Subject: (FWD) FISMA -- I think we're clear

I asked Wendy to take a look at the FISMA situation. Here's her answer.

--Roger

----- Forwarded message from Wendy Seltzer <[redacted]> -----

From: Wendy Seltzer <[redacted]>
To: [redacted]
Subject: FISMA -- I think we're clear
Delivery-Date: Fri, 06 Aug 2010 07:07:14 -0400

I did a very brief review of the Federal Information Security Management Act (44 U.S.C. s 3541-49), as Roger said Ken was wondering whether it applied to Tor. From my read of the statute, some White House and OMB guidance memos, and the FIPS 199 standard, I'd say that FISMA does not apply to Tor because Tor doesn't process "Federal Information."

FISMA is designed to assure the security, integrity, and availability of federal information, whether that information is processed by federal agencies or by third-party contractors. It makes agency heads responsible for information risk management. It doesn't put any direct obligations on federal contractors, but it might induce agencies to do so when the contractors process government information.

Tor doesn't process any federal information; we can't breach anyone's privacy, lose any federal secrets, or interfere with federal business even if the network goes down. I think that should mean that Tor is out-of-scope from Ken's FISMA obligations. That conclusion comes both from the design of the Tor network (we can't learn anything about individuals whom the government might want using the network), and the nature of the services we're providing.

Happy to send pointers or do more analysis if you think it's useful.

--Wendy

§ 3544. Federal agency responsibilities
(a) In General.? The head of each agency shall?
(1) be responsible for?
(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of?
(i) information collected or maintained by or on behalf of the agency; and
(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency; ... <http://www.law.cornell.edu/uscode/44/3544.html>
--
Wendy Seltzer -- [redacted]
phone: [redacted]

Fellow, Silicon Flatirons Center at University of Colorado Law School Fellow, Berkman Center for Internet & Society at Harvard University http://cyber.law.harvard.edu/seltzer.html
http://www.chillingeffects.org/
https://www.torproject.org/

----- End forwarded message -----

From: Roger Dingledine
To: Kelly DeYoe
Cc: Ken Berman; [redacted]
Subject: Re: (FWD) Potential CFP panelist Thursday during lunch?
Date: Wednesday, June 03, 2009 11:26:21 PM

On Wed, Jun 03, 2009 at 05:36:56PM -0400, Kelly DeYoe wrote:
> I'm actually registered for the conference, but haven't attended after
> all, just got caught up in a few things here and didn't see any sessions
> that were so compelling to drag me across town.
>
> I may make it over for the Tor panel, but afraid I cannot commit to
> being on it.

Sounds good. The panel is happening, and we have Robert Guerra and a nice blogger from Tunisia to spice things up. Do feel free to drop by if you're in the area.

--Roger

From: Ken Berman
To: Roger Dingledine; Kelly DeYoe; Sho Ho
Cc: [redacted] [redacted]
Subject: RE: (FWD) Re: [liberationtech] belarus opposition site hijacking
Date: Monday, December 20, 2010 7:35:20 AM

Roger - true. BUT what if they DID know what Tor is. Then what? Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Monday, December 20, 2010 2:38 AM
To: Ken Berman; [redacted] [redacted]
Cc: [redacted] [redacted]
Subject: (FWD) Re: [liberationtech] belarus opposition site hijacking

Another success for Tor. It's a shame there are so many places these
days where Tor is useful, but it's good that the censors in most of
these places don't know what Tor is.

--Roger

----- Forwarded message from Evgeny Morozov <[redacted]> -----

From: Evgeny Morozov <[redacted]>
To: "[redacted]" <[redacted]>
Subject: Re: [liberationtech] belarus opposition site hijacking
Delivery-Date: Sun, 19 Dec 2010 11:02:25 -0500

I'm in Belarus right now and can confirm that the redirects were, indeed,
taking place for some time. It also seems that https is blocked. Tor's site
is not blocked and Tor is working fine.

On Sun, Dec 19, 2010 at 3:45 PM, Hal Roberts <[redacted]>
> wrote:

> Hi All,
>
> I've written up a report today about opposition sites in Belarus being
> hijacked with redirects to fake (presumably government controlled) versions
> by BELPAK, the national ISP:
>
>
> http://blogs.law.harvard.edu/hroberts/2010/12/19/independent-media-sites-in-belarus-reportedly-hijacked-during-election/
>
> I'm taking the redirects on faith according to a report by a digital
> activist that I trust, but you can see the faked sites with almost identical
> domain names yourself, as well as that the fake sites are all hosted within
> IP addresses owned by BELPAK. He is also reporting some DDoS attacks and
> that international ports 443 and 465 are currently being blocked.
>
> -hal
>
> --
> Hal Roberts
> Fellow
> Berkman Center for Internet & Society
> Harvard University

> [redacted]
> [redacted]

---

liberationtech mailing list
[redacted]

----- End forwarded message -----

From: Ken Berman
To: Andrew Lewman
Cc: Roger Dingledine; Kelly DeYoe; Sho Ho; [redacted]
Subject: RE: (FWD) Re: [liberationtech] belarus opposition site hijacking
Date: Monday, December 20, 2010 11:27:34 AM

Interesting, thanks....

-----Original Message-----
From: Andrew Lewman [mailto:[redacted]
Sent: Monday, December 20, 2010 10:53 AM
To: Ken Berman
Cc: Roger Dingledine; [redacted] [redacted] [redacted]
Subject: Re: (FWD) Re: [liberationtech] belarus opposition site hijacking

On Mon, 20 Dec 2010 07:35:20 -0500
Ken Berman <[redacted] wrote:

> Roger - true. BUT what if they DID know what Tor is. Then what? Ken

Then we're in the same situation as China, Iran, Burma, and most
American companies and governments. Step one is to block the public
list of relays. Only China has taken step two, which is to try to
block all of the bridges.

We're working on making Step two much harder to do. It's going to take
more research and time.

However, we've heard from a few people that the ex-Russian bloc is much
more about social pressure than technical. People in Belarus seem to
be scared to death of a stray packet going to somewhere banned. The
technical censorship infrastructure of Belarus seems to be in the late
1990s. It's been suggested to us that the govt of Belarus mostly
ignores the Internet, and has little capability to enforce censorship
on a technological level.

--
Andrew
pgp 0x74ED336B

Google items

From: Ken Berman
To: Roger Dingledine; Kelly DeYoe
Subject: RE: (FWD) Re: Vidalia and Torbutton localization
Date: Wednesday, June 11, 2008 3:16:53 PM

Great news, thanks. Let us know how the Farsi translation is going...Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Wednesday, June 11, 2008 7:18 AM
To: Kelly DeYoe; Ken Berman
Subject: (FWD) Re: Vidalia and Torbutton localization

Chris has found us a Farsi translator who is comfortable with text editors, so we're working on getting more Tor components translated into Farsi.

In other news, we've finally found a web-based translation project that doesn't suck. It's called Pootle. You can check out the editing interface at
http://translation.torproject.org/de/vidalia/translate.html?editing=1&blank=1

and you can compare the Farsi, Russian, and Chinese translation progress at a glance:
http://translation.torproject.org/projects/torbutton/
http://translation.torproject.org/projects/vidalia/
http://translation.torproject.org/projects/torcheck/
though there are still some kinks to iron out -- for example it looks like it can't find the zh-CN vidalia translation file, even though there is one:
https://svn.torproject.org/svn/translation/trunk/projects/vidalia/zh_cn/vidalia.po

Plus it can commit changes directly to our SVN repository, so we don't have to deal with manually importing and exporting "po" string files all the time.

(Pootle can handle the string formats for Vidalia, Torbutton, and Torcheck, but it can't yet handle the wml files that we use for our website. So we have directed one of our Google Summer of Code students to work for the summer on teaching Pootle how to handle wml files.)

We've only found it in the past week, so all of this set-up is very new. We hope to clean it up in the next few weeks and then have it go 'live', meaning we will actually encourage translators to show up and help out.

--Roger

----- Forwarded message from Jacob Appelbaum <[redacted]> -----

From: Jacob Appelbaum <[redacted]>
To: Shahab Gashti <[redacted]>
CC: Chris Walker <[redacted]>
'Roger Dingledine' <[redacted]>
Subject: Re: Vidalia and Torbutton localization
Delivery-Date: Tue, 10 Jun 2008 19:27:09 -0400

We do have a new process that will hopefully be "officially" launched in the next few days. We're planning on merging all of the translation

files for Vidalia, Torbutton and any other projects (currently just TorCheck) into a single website. Translators will be able to download .po files for editing as they prefer or by using a website directly.

Currently, I'm working on a few details to ensure this rolls out smoothly and I'll be documenting the process once we've agreed on a solid one.

The website is up and running, though users can really only translate into German at the moment (this limitation is to make testing more manageable and not a permanent issue). The website is also synced with subversion, so users no longer need to know anything about subversion or diffing files unless they directly want to do so. This is the subversion repository:
https://tor-svn.freehaven.net/svn/translation/trunk/

If you'd like to see how the translation website works, this is the current version of the website, possibly as we will deploy it in the next few days:
http://translation.torproject.org/

You'll need to sign up for an account and register it before you'll be able to make translations. As I said above, only German is available for translation at the moment but it should work well for demonstration purposes.

This is the German section of the website, listing all projects:
http://translation.torproject.org/de_DE/index.html

This is the German section of the website, listing only files for Torbutton:
http://translation.torproject.org/de_DE/torbutton/

If there is a specific language, we can easily enable it for testing purposes and hopefully we'll be able to test a full translation from start to re-integration with upstream.

I hope this is helpful. I'm excited to see this new website and these new processes in place!

Please do send me any feedback and do not hesitate to ask questions, I'm all ears!

Regards,
Jacob Appelbaum

----- End forwarded message -----

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe
Subject: Re: [Fwd: Master"s Thesis Referral from Simson Garfinkel]
Date: Wednesday, October 17, 2007 11:19:18 AM

OK, let's talk today. I have a meeting at 1:30 that I PRAY will be over at 2:00. May Kelly and I call you when I'm done? (might be 2:15). Ken

Roger Dingledine wrote:

> On Tue, Oct 16, 2007 at 07:49:18AM -0400, Ken Berman wrote:
>
> > Roger - your thoughts??
>
> Depends what he's looking for.
>
> If he's asking for you to say "yes, good idea, work on that" then by all means, sure. :)
>
> If he's asking for sponsorship or funding? It would be a pretty risky
> bet I think.
>
> This particular problem he wants to tackle has a dozen wrong ways to do
> it, as we've been finding out over the past few years trying to find a
> way that won't screw up scalability or anonymity too much. I don't think
> I've heard of this student before, which means he likely isn't involved
> in the anonymity research community, which means he likely has a lot of
> work ahead of him before he can have good intuition about all the ways
> these designs can be attacked. And I don't think Simson has worked in
> this particular area either.
>
> We can talk about this more tomorrow.
>
> (If you *are* looking for some grad students to fund for anonymity work,
> let me know and I'd be happy to recommend some good profs in the area. :)
>
> --Roger
>
> > -------- Original Message --------
> > <pre>Mr. Berman,
> >
> > I'm a second year masters student at Naval Postgraduate School and I was
> > talking with Simson the other day about a list of research topics you
> > sent him. I'm particularly interested in looking into a method of
> > decentralizing Tor's directory servers.
> > I have a diverse background in networks, exploitation, and programming
> > so something like this feels right up my alley. Would you be interested
> > in having someone such as myself work on this?
> >
> > If so, could you expand a little bit about what it is

that you want and
what your organization has tried already? If this is
easier via
number is [redacted] (b) (6)

To be fair, I am considering another topic (which I'm a
little less
interested in) but it seems to be hung up in the
bureaucracy.

Thanks,
Steve

From: Berel Dorfman
To: Andrew Lewman
Cc: Berel Dorfman; Herman Shaw; Kelly DeYoe
Subject: Re: [Fwd: Re: [redacted] Re: The TOR Project]]
Date: Wednesday, April 30, 2008 7:05:44 PM
Attachments: 6700-TORcontractsigned.pdf

Andrew,

Attached please find the final counter-signed contract document for your records. I would like to get the original top contract page that you signed in ink back for my files. Please send it to :

Berel Dorfman
Broadcasting Board of Governors
Office Of Contracts (CON)
Swtizter Building
330 C Street, SW Room 4007
Washington, DC 20237

Please do not hesitate to contact me if you have any questions.

Thanks and regards,

Berel

Berel Dorfman wrote:

> Dear Andrew,
>
> I am pleased to attach our contract package to this e-mail for TOR Project Services. In order to complete this contract document I require the following from you:
>
> 1- Signature, Title, and Date in boxes 30a, 30b, and 30c - page 1
>
> 2- Pricing schedule to be filled in by hand - page 9
>
> 3- Representations and Certifications to be filled out where applicable - pages 25- 35
>
> Also, please verify the DUNS number we are using. It is different than the one we used on the last contract.
>
> Andrew, I am leaving today for an 11 day period. I will out of the office through 4/28/08. If for any reason you need assistance with this request or have any questions, please direct them to Herman Shaw, e-mail = [redacted]
>
> Thanks for all of your help!
>
> Berel

Andrew Lewman wrote:

> Hello Berel,
>
> I believe this is what you are looking for as a response. Roger and I worked on this last night. Sorry for the delayed response.
>
> -Andrew
>
> -------- Origi[redacted] ---
> Subject: Re: [redacted] Re: The TOR Project]
> Date: Wed, 16 [redacted]
> From: Roger Dingled[redacted]
> To: Andrew Lewman <[redacted]
> R[redacted]
> <[redacted]
>
> On Wed, Apr 16, 2008 at 09:38:37PM -0400, Andrew Lewman wrote:
>
> > OK, I am trying to put together a contract document and need some more help from you. Kelley DeYoe has expleined that all the requirements I sent you earlier to price for me are only the "new" ones, but that he wants ALL the old requirements included in the contract as well. Below you will find a complete list of requirements. I need you to advise me how to price them in the contract. If there is no charge becuase it is included in another requirement you can say that. Please feel free to contact me if you have any questions.
>
> Ok. I've revised our estimates as below. A lot of the items overlap, so it isn't so much of a shifting of what work we'll do as it is a shifting of what categories the planned work will fall into.
>
> --Roger
>
> C.2 TECHNICAL REQUIREMENTS
>
> C.2.1 The Contractor shall continue design and development of enhancements to the existing Tor software to increase its suitability as a tool for Internet users in countries with government-sponsored Internet censorship to circumvent censorship controls, based on the existing research and documentation performed during the previous contract period (e.g. as described in the paper "Design of a blocking-resistant anonymity system").
> C.2.2 The Contractor shall submit system architecture and technical design documentation for Tor enhancements specifically related to anti-censorship improvements in C.2.1 to the Authorized Representative of the Contracting Officer (AR/CO) for review

and approval before
implementation. Significant changes to the
design that are discovered
during implementation must be documented and
reviewed by the AR/CO as
soon as the Contractor becomes aware of the
need for these revisions.

C.2.1 and C.2.2 together will get another $70k of continued effort.

C.2.3 The Contractor shall develop and implement the bridge relay mechanism as designed during the previous contract period to allow individual Tor users to easily reconfigure their Tor client to automatically relay traffic from users in countries with government-imposed Internet censorship so as to circumvent that censorship.

C.2.4 The Contractor shall develop and implement the bridge directory authority mechanism as designed during the previous contract period to allow Tor clients configured as bridge relays (as described in C.2.3) to communicate their existence to the bridge directory authority, and to allow users in countries with government-imposed Internet censorship to discover addresses of available bridge relays so that they may access the Tor network.

C.2.3 and C.2.4 are included in C.2.12.

C.2.5 The Contractor shall design and develop revisions to the Tor network protocols to hide the network signature of Tor traffic so it is difficult for government-sponsored Internet censors to identify Tor traffic and trivially block it.

Continued work, $20k.

C.2.6 The Contractor shall develop and implement enhancements to Tor's cell-based protocol to improve performance on substandard network connections including those with low bandwidth and/or high latency and/or high packet loss.

C.2.7 The Contractor shall continue development of Tor network scalability, with the goal of supporting 2 million or more concurrent end users. This requirement is only a goal for system scalability and is not a requirement on number of actual concurrent users of the Tor network.

C.2.6 and C.2.7 are included in C.2.13.

C.2.8 The Contractor shall work with IBB staff and other IBB contractors to identify tasks in support of this program that might be developed collaboratively with Contractor. Tasks involving areas such as documentation, bug fixes, software testing, and any area where specific knowledge of foreign government-sponsored Internet censorship may be especially appropriate for this purpose.

C.2.9 The Contractor shall communicate tasks identified for delegation to IBB in C.2.8 to the AR/CO and negotiate time frames for their completion. The Contractor shall monitor and coordinate work performed by IBB staff on delegated tasks and integrate it into Tor software releases as appropriate.

$0

C.2.10 The Contractor shall promote active growth of the Tor server network and advocacy of Tor products to increase the performance, stability, and usability of Tor, with a focus on the end user experience for users in countries with government-sponsored Internet censorship.

Continued work, $20k

C.2.11 The Contractor shall improve the ease of use of Tor for end users by continuing research and development of one or both of the following products: (1) all-in-one software bundle containing Tor and supporting applications, as well as an easy-to-use installer for Microsoft Windows operating systems, as well as option to install and run from a Universal Serial Bus (USB) flash device; (2) bootable CD-ROM image ("LiveCD") which contains a minimal operating system, Tor, and supporting applications. Both would have all appropriate applications pre-configured to use Tor out of the box with only minimal additional configuration required by the end user. If Contractor determines it is not feasible to develop both products, Contractor will provide detailed written technical analysis and explanation to the AR/CO. The Contractor shall make an initial public release of at least one of these products during the term of this contract.

Continued work, $20k

C.2.12 The Contractor shall continue to develop and implement improvements to the bridge relay and bridge directory authority mechanisms to improve the usability, performance and reliability of the Tor network by users in countries with government-imposed Internet censorship.

Research and development, $80k

C.2.13 The Contractor shall research and document additional options for the scalability of the Tor network beyond 2 million concurrent users, including analysis of splitting the network into multiple segments, switching to datagram-based protocols, and improving the load balancing within the network.

Research $50k
Design and prototyping $30k

C.2.14 The Contractor shall continue research into the option of providing incentives for Tor users to run Tor relay servers. If further research indicates that this should be pursued, the Contractor shall develop a project plan and timeline for this work. If further research indicates this option should be abandoned, the Contractor shall document and explain in writing the reasoning behind this decision.

Research $30k

C.2.15 The Contractor shall develop a more reliable download mechanism for the Tor browser bundle for users on slow and/or unreliable network connections, by means of a split download of multiple smaller files, implementation of a lightweight download manager, reduction in the software bundle file size, or other method as chosen by the Contractor.

Research and deployment $10k

C.2.16 The Contractor shall test the Tor browser bundle on multiple computer systems and analyze these systems afterwards for any changes to the system that may have been made inadvertently by use of the Tor browser bundle. The Contractor shall document any such changes found

and develop a plan to reduce the footprint of Tor browser bundle use.

Research and deployment $10k

C.2.17 The Contractor shall develop or adapt existing open source software to implement a web-based portal to manage the translations of text into multiple languages for the user interface text of software of Torbutton and Vidalia and other software that may in the future be included in the Tor browser bundle. The web site must allow non-technical users the ability to contribute translations by providing text to be translated in English, as well as any needed context on the use of the text, and allowing users to enter the translation into their language from their web browser.

Research and deployment $10k
Maintenance and improvements $10k

From: Andrew Lewman
To: Bart Childs
Cc: Ken Berman; Kelly DeYoe
Subject: Re: BGAN test
Date: Tuesday, February 01, 2011 9:04:42 AM

On Tue, 1 Feb 2011 08:06:20 -0500
Ken Berman <[redacted]> wrote:
> We work with a group called Tor and they wanted to run some tests
> w/Tor over BGAN. Next time you fire it up, pls consider downloading
> the Tor s/w and giving this circumvention app a try.

Thank you Ken.

Hello Bart,

With the protests in Tunisia and now Egypt, people are trying to route Tor over BGAN connections. It will work, but like everything BGAN, it will be slow. We have been working on making Tor more friendly for mobile phone data connections. The same sort of constraints exist for satellite, but with greater latencies.

If you can test Tor for us, please let me know. I'm happy to coordinate some testing and get some feedback as to how Tor is behaving over the connection.

It would be great to see if there are easy things to fix to make Tor work better on satellite Internet connections.

Thanks!

--
Andrew
pgp 0x74ED336B

CENTRA
Military/intl contractr

From: Ken Berman
To: Roger Dingledine
Cc: Toy, Debbie; Kelly DeYoe
Subject: Re: CENTRA conference - Esoteric Use of the Internet
Date: Wednesday, August 23, 2006 8:36:53 AM

Thanks, Roger.
Debbie - yes, we would like to attend, and can fill you in on more details of our unclass Internet anti-censorship program. We have some fairly esoteric apps that we have developed and would like to hear from you.

thanks,

Ken Berman
(b) (6)

Roger Dingledine wrote:

> On Fri, Aug 11, 2006 at 11:21:11AM -0400, Toy, Debbie wrote:
>
> > I am taking over for Lacey Chong at CENTRA in organizing
> > the conference
> > "Esoteric Use of the Internet Conference" to be held in
> > the DC area on
> > September 20-21.
>
> Hi Debbie,
>
> I'd like to introduce you to my friends Ken Berman and Kelly DeYoe
> of
> IBB.gov (the International Broadcasting Bureau, affiliated with
> Voice
> of America and Radio Free Europe/etc). We've been working with
> them
> to adapt Tor for use in countries where the government censors
> some
> communications. They are interested to hear more about the
> conference,
> and also more about your organization. I'll let them take it from
> here.
>
> Thanks,
> --Roger

From: Shultis, John
To: Ken Berman; Danny Bilson; David Dagon; Kelly DeYoe; Flint Dille; Roger Dingledine; Cristin Goodwin (FLYNN); Lance James; Todd Richmond; Paul Syverson; Rob Thomas; [redacted] Bill Marlow
Cc: Kangarloo, Sunny; Toy, Debbie
Subject: RE: CENTRA conference Sept. 20-21, 2006
Date: Tuesday, September 12, 2006 6:06:07 PM
Importance: High

Hello! I am John Shultis, one of the program managers for CENTRA Technology, Inc. You've been working with our Project Manager for this conference--Debbie Toy. I want to thank you for your participation, and emphasize a couple of points. First, if you haven't provided Debbie with your paperwork for the consultant's agreement and the non-disclosure agreement, I urge you to do so right away. We won't be able to reimburse you for your expenses or pay your honorariums without those. Likewise, it will be important for you to provide Debbie with your travel vouchers as soon as possible for the same reason; in our experience, some consultants have put this off for months, which is hard to understand, since we were trying to pay them, not bill them! Also, if you have not provided Debbie with a good contact telephone number yet, please do so immediately, as she must use the phone to provide you with your conference website login information instead of the Internet.

That brings me to the second point: A large part of what we hope to accomplish with this conference will be influenced by your paticipation on the website prior to arriving. We have posted some articles to provoke thought and discussion, and we also have posted in a separate page the discussion questions that we would like you to consider. Your participation will be anonymous, and we hope to delve into some obscure/esoteric concepts, ideas, and techniques, so please feel free to kick around the ideas, develop your thoughts, and follow rabbit trails. I cannot overemphasize how important your participation will be on this website both before and after the conference event. We plan to post additional questions based on the conference outcomes, and we'll ask you to continue to participate in these discussion threads over the coming weeks. Moreover, if you think we're not asking the right questions, tell us that, as well. Those ideas may prove to be the most fruitful discussion threads.

Again, I thank you for your decision to participate in this event, and I look forward to following your discussions and meeting you all in person next week. If you have any problems using the website, please contact me, Debbie, or Sunny Kangarloo, and we'll help you to resolve it.

Very respectfully,

John Shultis

From: Toy, Debbie
Sent: Tue 9/12/2006 11:42 AM
To: Ken Berman; Danny Bilson; David Dagon; Kelly DeYoe; Flint Dille; Roger Dingledine; Cristin Goodwin (FLYNN); Lance James; Todd Richmond; Paul Syverson; 'Rob Thomas'; [redacted] Bill Marlow
Cc: Shultis, John; Kangarloo, Sunny
Subject: CENTRA conference Sept. 20-21, 2006

September 12, 2006

To all conference consultants:

The website for the upcoming conference "Esoteric Uses of the Internet" (Sept. 20-21, 2006) is now up and running. On this site, you will find the key questions for the conference, organized in a discussion board, which we would like you to participate in prior to the event. You will also find bios of non-government attendees, an agenda, many background articles, and hotel information.

The website is at http://www.stratgroup.org <http://www.stratgroup.org/>

I or my colleague Sunny Kangarloo will be calling you today to give you a user ID and password.

In addition to participating in the discussion board for both the conference questions and the articles section, please feel free to call or email me with any details you feel have been omitted, or if you have articles you feel would be helpful to the group. I will see that they are added to the site.

Again, I look forward to seeing everyone on the 20th,

Debbie

CENTRA Technology, Inc.

4121 Wilson Blvd. Suite 800

Arlington, VA 22203

Ph: (b) (6)

Fax: (b) (6)

Email: (b) (6)

Discussi[redacted]
attac[redacted]

From: Roger Dingledine
To: Kelly DeYoe
Cc: Shava Nerad; Ken Berman
Subject: Re: Conference call next Monday?
Date: Monday, November 06, 2006 2:14:48 AM

Hi Kelly,

Shava says she can do Monday at 4pm, or any other afternoon except Tuesday. So now we've narrowed things down a bit more. :)

While I'm at it, here's a slightly expanded status report, for some of the items since I last updated you on Sept 19:

On Sat, Nov 04, 2006 at 01:17:52AM -0500, Roger Dingledine wrote:
> The most interesting news from our end is that we've got partial drafts
> of two new documents:
>
> The first is
> http://tor.eff.org/svn/trunk/doc/design-paper/blocking.tex
> aka
> http://freehaven.net/~arma/blocking.pdf
> which is the design document for our blocking-resistant adaption of Tor.
> I had a good conversation with Nart Villeneuve and Ron Diebert in the
> past few days (I'm in Toronto) and I think I can help them solve the fact
> that they have no real documentation or design documents for Psiphon --
> a lot of this document is reusable by them. This way Tor and Citizen
> Lab can take advantage of each other's strengths.
>
> The other is
> http://tor.eff.org/svn/trunk/doc/design-paper/roadmap-2007.tex
> aka
> http://tor.eff.org/svn/trunk/doc/design-paper/roadmap-2007.pdf
> which maps out the development tasks we need to tackle in the next few
> years. It's missing non-development activities, but those will get folded
> in as we start listing them.
>
> I'm hoping to have a complete draft of blocking.tex by the end of this
> coming week, and the roadmap will continue to grow as we need it to.
>
> Another pair of write-ups you might find interesting are:
> http://www.ethanzuckerman.com/blog/?p=1015
> http://www.ethanzuckerman.com/blog/?p=1019

We put out a new development release, Tor 0.1.2.2-alpha:
http://archives.seul.org/or/talk/Oct-2006/msg00147.html
and today I just released Tor 0.1.2.3-alpha, which prepares the Tor directory authorities to integrate with Mike Perry's new Tor controller, so we can detect broken exit relays.

(Broken exit relays have become an increasing problem lately, since we're attracting more "ordinary" Tor servers, and in many places in the world ISPs try to hijack their users' Internet connections to sell more encyclopedias. Who would have thought.)

We also put out a new stable bugfix release (0.1.1.24), and I'm expecting to put 0.1.1.25 out in the next few days.

I gave a Tor demo a few days ago in Toronto with Mike Chiussi to a bunch of Canadian privacy people. Mike is making progress at solving the Windows XP stability bug. We've heard several reports that Vista doesn't have these problems, so in the worst case it's just a matter of time.

Shishir (the Cambridge UK student) is moving forward with the Tor Windows USB package (internal codename Torpedo). More news on that soon I hope.

Matt and Justin have finished Vidalia 0.0.8, and today we finally released Vidalia 0.0.9. This latest release improves the interface for setting up and configuring a Tor server using Vidalia. The Windows Vidalia and bundle installers now also support multiple languages, and the Windows bundle installs Torbutton now so users don't have to go fetch it separately.

Near-term plans are to start notifying Vidalia of certain key Tor events ("our reachability tests failed", "our clock is really skewed, please fix it", etc), so Vidalia can help the user resolve the issues. We've got most of the features in place, but we're still working on how to actually present the issues to the user.

We're looking forward to the Farsi translation for Vidalia and the installer. Is there anything we should do to keep that moving forward? We've also just found another potential volunteer, so if this translation thing is a big hassle on your side, we could try him.

Next week Shava and I are flying to France to meet with RSF and several other European non-profits, to coordinate and talk more about the blocking-resistance design.

We're working with several academic groups (in particular, U Waterloo, U Indiana, U Colorado, and UMass Amherst) who have been developing attacks on Tor -- and in most cases, but not all, defenses to go with them. :) I am optimistic that we'll be able to fund a grad student at U Waterloo (via our contacts at Bell) to focus his research on Tor.

Hope that helps to keep you up to date. :)
--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe; Shava Nerad; Hiu Ho
Subject: Re: First draft of blocking-resistance design
Date: Tuesday, November 21, 2006 1:09:28 PM

When's our next call? Ken

Roger Dingledine wrote:

> On Mon, Nov 20, 2006 at 09:16:35AM -0500, Ken Berman wrote:
>
> > Roger - our team went thru this last Friday and were
> > quite impressed.
>
> Great. This new version has an ending, and other fixes and ideas
> sprinkled
> throughout, compared to the one you read last Friday.
>
> > We have some thoughts as to how this fits into your
> > overall road map and
> > our funding desires. Next time we talk we can explore
> > this.
>
> Great. There's lots to be done. I figure my job is to lay out what
> needs to be done and figure out how quickly we can do it, and then
> everything else will follow. :)
>
> > btw - this guy "fred", aka "farid pouya" reports on the
> > translation to
> > Farsi:
> > In a week. We have been preparing launch of new site
> > then everything
> > was and still quite crazy. Sorry for delay. In a wee k
> > it will be done.
> >
> > We'll see.....
>
> When he starts the translation, he should check out the latest
> Vidalia
> from the repository -- somebody gave us a partial Farsi
> translation last
> week, so it is at least a starting point.
>
> > Should we bring Bennett back in at this point?
>
> Any thoughts on this one? I don't want to cut him totally out of
> the
> loop; I just realized that I needed to write the "how Tor offers
> now"
> section before he could be more useful. But I figure I should
> check with
> you first, since I haven't heard from him in a few months and you
> might
> be using him for other things at this point.
>
> Thanks!
> --Roger

From: Ken Berman
To: Roger Dingledine; Eric Johnson; Christopher Walker; Persephone Miel; Kelly DeYoe
Cc: [redacted]
Subject: RE: (FWD) Notes from Shiyu Zhou meeting
Date: Monday, December 15, 2008 10:57:23 AM

" Nothing has come of that yet; I just sent him a followup mail." And my bet is that nothing will....

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Friday, December 12, 2008 1:56 PM
To: Eric Johnson; Christopher Walker; Persephone Miel; Ken Berman; Kelly DeYoe
Cc: [redacted]
Subject: (FWD) Notes from Shiyu Zhou meeting

[I'm sending this to both Sesawe people and BBG people. Feel free to strip off whichever cc's you're nervous about when replying.]

Here's a summary of my November meeting with Shiyu.

The more interesting summary (not written below) is that he spent a short while ranting about the State Dept money and how the State Dept people are too scared to actually put the money where it would make a difference, and apparently they prefer to give it to some group that is going to maintain the status quo.

He seemed to genuinely not know that Tor was receiving some of the DRL money. My sense was that he isn't a good enough actor to be secretly aware of the details of the grant but be talking about it like that anyway.

He started the meeting thinking Tor was just some tiny volunteer project.

I followed Eric's request and didn't talk about our role in the DRL grant at all. I talked a lot about our other funders (IBB, NRL, Google, etc) and why each of them cares about Tor. Hopefully he won't later learn the details about DRL and decide to hate me for not being clear with him.

Yay politics,
--Roger

----- Forwarded message from Roger Dingledine <[redacted] -----

Date: Fri, 12 Dec 2008 13:41:52 -0500
From: Roger Dingledine <[redacted]
To: [redacted]
Subject: Notes from Shiyu Zhou meeting

On Nov 4 I met with Shiyu Zhou in NYC. He's a nice fellow who lives in NYC, after being a CS professor in Philly for a while. He moved to the States in '91 after experiencing the Tiananman massacre. Around that time his father, a high-ranking government official, also got really sick, and found a fine new government-approved health practice that seemed to be working for him. Until suddenly Falun Gong was outlawed and his father ended up in house arrest, with now a very limited life.

Now Shiyu lives in NYC, doing human rights work for various groups including a television station there. He works with a variety of the member groups of GIFC (Global Internet Freedom Consortium), which work on various circumvention tools to let Falun Gong members in China communicate with each other and with the outside world. They send out mass mailings into China (in fact, our friends at IBB fund them for that), and they've accumulated a lot of wisdom about how the arms race proceeds once you really catch the attention of a a well-funded adversary.

I gave him the quick version of the same talk I gave Jeremiah from CDHR a few weeks before. I tried to emphasize the many different uses that people find for Tor, and the improved sustainability that the project gets from the diversity of users and funders. I also tried to emphasize that Tor's security and sustainability comes from transparency -- we want to explain exactly how it works to everybody, yet still remain secure.

He didn't seem to care much about the non-circumvention uses or users for Tor. Regarding our circumvention arms race plans, he said they seemed reasonable, but he really wanted us to learn from what the other members of GIFC have learned. I told him I'd already met Bill Xia in Oxford (Bill runs Dynaweb in North Carolina), but I'd love to meet with more of the technical people in their consortium, and to hear more details about how their tools work. Nothing has come of that yet; I just sent him a followup mail.

He thought the cutoff for getting really noticed by the Chinese government is around 100K users.

We concluded with a "yay more circumvention tools, the more the better" agreement.

--Roger

----- End forwarded message -----

ARMS RACE / CHINA

From: Kelly DeYoe
To: Roger Dingledine
Cc: Ken Berman; Sho Ho; [redacted]
Subject: Re: (FWD) Re: Debugging Tor in China
Date: Friday, September 25, 2009 5:58:53 PM

Roger, a few comments back from our perspective inline below...

-k

Roger Dingledine wrote:
> The third of three mails.
>
> It would be great to have your advice on these strategy questions.
>
> --Roger
>
> ----- Forwarded message from Roger Dingledine <[redacted]> -----
>
> From: Roger Dingledine <[redacted]>
> To: [redacted]
> Subject: Re: Debugging Tor in China
> Delivery-Date: Fri, 25 Sep 2009 04:47:52 -0400
>
> On Thu, Sep 24, 2009 at 11:28:04PM -0400, Roger Dingledine wrote:
>> So what does this mean? Use bridges, and get them via gmail, and your
>> Tor will work fine.
>
> We have a couple of strategy choices to make. Isaac, I'd love to have
> your input on these.
>
> A) How loudly do we tell people that getting bridges via gmail still
> works? It seems clear that we should tell people like Isaac and Nathan,
> and let them do with the information what they will. Do we blog about
> it? Tell people on IRC?
>
> B) More generally, should we scramble before Oct 1 to put out a new
> version of Tor that has some directory authorities at new addresses,
> ask the fast entry guards to get a different IP address, etc? We could
> show the world that we can't be stopped that easily. Or should we
> just let Tor be blocked for a week, and then fix things afterwards?
> Which approach would our users in China prefer? Which approach would
> get us more users in China later? If we lie low, are they more likely
> to remove the IP address filters later? We probably can go through the
> process of encouraging everybody to change IP addresses once or twice
> a year, but not every month.

If you escalate the arms race by updating IPs for the various Tor bits before 10/1, chances are they will be more likely to keep blocking the new addresses as quickly as possible, at least until 10/1. I think it is hard to say if they will keep it up after 10/1, and if they will make a greater effort after 10/1 if you guys make IP changes happen now. I think any plan you guys make for changing IPs has to be able to react daily until 10/1 at least to make much difference though.

> C) Right now https://bridges.torproject.org/ is offering mostly blocked
> bridges. So if you ask for bridges that way, you'll probably be

> sad. We could go through and remove the ones that are blocked, so the
> remaining ones work. But that makes it easier for the censors to just
> clean up the few that they missed. Eventually we will want to weed out
> the bad ones, but how urgently should we do that? Or said another way,
> are the censors all done for now or will they do another round of
> filtering before Oct 1?

I'm guessing they will do another round (and another and another as needed) until 10/1. Everything we've heard from everyone else trying to provide anti-censorship tools in China is that the censors are working really, really hard and being persistent right now.

> D) Mike Perry suggested that we should add some more IP:port combinations
> to the answers you get from https://bridges.torproject.org/ -- things
> like 64.4.241.45:443 (paypal) and other common ssl websites. There would
> be two goals: 1) raising the cost of blocking bridge addresses, since you
> have to check that it isn't a "real" site first. 2) Punish them if they
> slip up by having them block a site that they wouldn't have wanted to
> block. Are there such sites, or would they all just count as acceptable
> collateral damage? For example, I wouldn't want to put 66.249.80.83:443
> (gmail) on the list.

I'm not sure this is really helpful, since I get the feeling any collateral damage is acceptable at this point.

> E) Do we want to change Tonga's address? It's our bridge authority,
> and it got blocked -- and probably because it was a public relay, not
> because it was a bridge authority. Next time we should come up with
> an IP address that isn't the same address that Tonga publishes to the
> directory. Here we have the same question as B: eventually we should do
> this, but now or in two weeks?
>
> F) Nick wrote a great little Python tool called marco.py that takes in
> a cached-consensus file and tells you which relays are unreachable and
> why. We could give that out to people, and they could use it to find
> public relays that aren't blocked for them. Then they could configure
> those relays to be their bridges, and voila, their Tor works. Except,
> giving this script out means giving it to the bad guys too. Will it help
> them much, or are they already smart and technically skilled and just
> haven't messed with Tor yet for other reasons?
>
> Thanks,
> --Roger
>
> ----- End forwarded message -----
>

From: Andrew Lewman
To: Sho Ho
Cc: Roger Dingledine
Subject: Re: Current Tor Traffic from Iran
Date: Tuesday, March 12, 2013 11:42:02 AM

On Tue, 12 Mar 2013 15:30:22 +0000
Sho Ho <[redacted] wrote:

> Can I ask both of you a HUGE favor? can you please send me the
> current Tor traffic report today? Since Kelly is on sick leave today,
> my boss wants to find out Current Tor traffic from Iran after the
> IRIB implemented their VPN negating hardware.

What we have is here for direct connections:
https://metrics.torproject.org/users.html?graph=direct-users&start=2012-12-12&end=2013-03-12&country=ir&events=off#direct-users

And here for bridge connections:
https://metrics.torproject.org/users.html?graph=bridge-users&start=2012-12-12&end=2013-03-12&country=ir#bridge-users

What we don't have is obfsproxy stats from Iran. Obfsproxy is working fine, but integrating the stats from the obfsproxy bridges is an active project and work in progress.

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

From: Roger Dingledine
To: Kelly DeYoe
Cc: Hiu Ho; Ken Berman
Subject: Re: Rough agenda for your 7/24 visit
Date: Tuesday, July 24, 2007 4:04:37 AM

On Wed, Jul 18, 2007 at 06:42:38AM -0400, Roger Dingledine wrote:
> Sounds good. My flight gets into Dulles around 11:30am on the 24th. I am
> still trying to figure out my plan for the following day, so I don't yet
> know if I'm going to rent a car and drive to a metro stop and metro in,
> or take a bus to a metro stop and metro in, or what.
>
> In any case I will be there by 2 unless the planes don't work, and quite
> likely by 1 also.
>
> I'll keep you in the loop as I plan things better. :)

Ok. I should be all set, arriving to Dulles around 11:30, and will hopefully be in the lobby of your building by 12:30, or 13:00 if I'm late. That should give us enough time for lunch somewhere before the various meetings begin.

I'll call Ken's office at [redacted] once I get there. One day maybe I'll learn a number for some other office, so I don't have to hassle Ken every time I show up. :)

Thanks!
--Roger

From: Roger Dingledine
To: Kelly DeYoe
Subject: Re: Rough agenda for your 7/24 visit
Date: Wednesday, July 18, 2007 7:42:38 AM

On Mon, Jul 16, 2007 at 05:32:31PM -0400, Kelly DeYoe wrote:
> Roger, just wanted to give you a rough agenda for your visit here to IBB
> next Tuesday 7/24. When you first arrive, we'll just plan on a small
> chat with yourself, myself, Hiu and Ken, no fixed topics, just whatever
> seems interesting and wherever the discussion takes us.
>
> From 2:30-3, we will have a somewhat larger, but still smallish, group
> of folks from the VOA Persian News Network and VOA China Branch for you
> to give a general overview of Tor, why the original design is not a
> robust design for censorship circumvention, and explain the
> anti-censorship mechanism you're building for Tor. This group will be
> web news editors and journalists, so a somewhat less technical audience,
> but one that is quite familiar with the Internet censorship problems in
> their respective target countries. Obviously with only 30 minutes, it
> will have to be pretty brief too.
>
> From 3-4, Ken would like you to give a slightly more in-depth
> presentation on the same Tor topics to a more technical audience
> composed of some of the networking and computer security folks on the IT
> staff here. These are going to be folks who know a lot more about IP
> networking and probably quite a bit less about Internet censorship
> topics than the Persians and Chinese journalists actually.
>
> Depending on the timing, we could also get together for lunch, just let
> us know when you're on the ground here in DC and such.

Sounds good. My flight gets into Dulles around 11:30am on the 24th. I am still trying to figure out my plan for the following day, so I don't yet know if I'm going to rent a car and drive to a metro stop and metro in, or take a bus to a metro stop and metro in, or what.

In any case I will be there by 2 unless the planes don't work, and quite likely by 1 also.

I'll keep you in the loop as I plan things better. :)
--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Kelly DeYoe; Hiu Ho
Subject: Re: Rough agenda for your 7/24 visit
Date: Tuesday, July 24, 2007 8:05:15 AM

Kelly: (b) (6)
Hiu: (b) (6)

Roger Dingledine wrote:

> On Wed, Jul 18, 2007 at 06:42:38AM -0400, Roger Dingledine wrote:
>
> > Sounds good. My flight gets into Dulles around 11:30am
> > on the 24th. I am
> > still trying to figure out my plan for the following
> > day, so I don't yet
> > know if I'm going to rent a car and drive to a metro
> > stop and metro in,
> > or take a bus to a metro stop and metro in, or what.
> >
> > In any case I will be there by 2 unless the planes don't
> > work, and quite
> > likely by 1 also.
> >
> > I'll keep you in the loop as I plan things better. :)
>
> Ok. I should be all set, arriving to Dulles around 11:30, and will
> hopefully be in the lobby of your building by 12:30, or 13:00 if
> I'm
> late. That should give us enough time for lunch somewhere before
> the
> various meetings begin.
>
> I'll call Ken's office at (b) (6) once I get there. One day maybe
> I'll
> learn a number for some other office, so I don't have to hassle
> Ken
> every time I show up. :)
>
> Thanks!
> --Roger

From: Andrew Lewman
To: Ken Berman
Cc: Roger Dingledine; Kelly DeYoe; Sho Ho; [redacted]
Subject: Re: Saudi Arabian Tor use up?
Date: Tuesday, March 09, 2010 11:05:30 AM

On 03/08/2010 09:36 AM, Ken Berman wrote:
> I'll check with our Middle East boys to see if they have an idea why
> traffic is increasing. As for China, I'm still amazed you have been
> getting a nearly free ride all this time. Ken

Thanks Ken. As for a free ride, we've heard from a few people in China that Tor isn't politically sensitive. It's a fine privacy tool that also works for circumvention. With the growing mob rule of human flesh search and the like, protecting one's privacy online seems smarter and smarter.

However, we are getting more aggressively blocked as each political anniversary comes around.

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

Website: https://www.torproject.org/
Blog: https://blog.torproject.org/
Identi.ca: torproject

From: Ken Berman
To: Roger Dingledine; Kelly DeYoe
Cc: Sho Ho; [redacted]
Subject: RE: Saudi Arabian Tor use up?
Date: Monday, March 08, 2010 9:36:08 AM

I'll check with our Middle East boys to see if they have an idea why traffic is increasing. As for China, I'm still amazed you have been getting a nearly free ride all this time. Ken

-----Original Message-----
From: Roger Dingledine [mailto:[redacted]
Sent: Friday, March 05, 2010 11:56 PM
To: Kelly DeYoe
Cc: Ken Berman; Sho Ho; [redacted]
Subject: Saudi Arabian Tor use up?

http://metrics.torproject.org/graphs/bridge-users/saudi-bridges-90d.png

That's quite a growth recently. I wonder what's up, there.

Something similar going on in Syria:
http://metrics.torproject.org/graphs/bridge-users/syria-bridges-90d.png

In other news, China did another of their network-wide filtering attempts two days ago. Looks like soon we'll want to role out some of our smarter bridge distribution strategies...

--Roger

From: Andrew Lewman
To: Ken Berman
Cc: Roger Dingledine; Kelly DeYoe; Sho Ho; [redacted]
Subject: Re: Saudi Arabian Tor use up?
Date: Tuesday, March 09, 2010 11:05:30 AM

On 03/08/2010 09:36 AM, Ken Berman wrote:
> I'll check with our Middle East boys to see if they have an idea why
> traffic is increasing. As for China, I'm still amazed you have been
> getting a nearly free ride all this time. Ken

Thanks Ken. As for a free ride, we've heard from a few people in China that Tor isn't politically sensitive. It's a fine privacy tool that also works for circumvention. With the growing mob rule of human flesh search and the like, protecting one's privacy online seems smarter and smarter.

However, we are getting more aggressively blocked as each political anniversary comes around.

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

Website: https://www.torproject.org/
Blog: https://blog.torproject.org/
Identi.ca: torproject

From: Ken Berman
To: Roger Dingledine
Cc: [redacted]
Subject: Re: Roger visiting IBB Jan 27?
Date: Tuesday, January 24, 2006 11:17:59 AM

How interesting! Ken

Roger Dingledine wrote:

>In other interesting news, we just moved the "torpark" program (a
>combination of Tor and the latest Firefox called Deer Park) to my MIT
>computer for hosting, and in the past three days we've had more than
>100,000 downloads of the Chinese-language version. The next-most popular
>is the Taiwanese version at 1500 downloads, and the English version at
>1400 downloads.
>
>I guess we can see where our future users are.
>--Roger
>
>
>