

From: Roger Dingledine
To: Chris Walker; Ken Berman; Kelly DeYoe
Cc: (b) (6)
Subject: (FWD) A Practical Congestion Attack on Tor Using Long Paths
Date: Thursday, December 11, 2008 2:09:16 PM
Attachments: torwriteup.pdf

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 <(b) (6)> -----

Date: Tue, 2 Dec 2008 15:10:56 -0500
From: Roger Dingledine <(b) (6)>
To: (b) (6)
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 amplification 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: Roger Dingledine
To: Chris Walker; Ken Berman; Kelly DeYoe
Cc: (b) (6)
Subject: (FWD) A Practical Congestion Attack on Tor Using Long Paths
Date: Thursday, December 11, 2008 2:09:16 PM
Attachments: torwriteup.pdf

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 <(b) (6)> -----

Date: Tue, 2 Dec 2008 15:10:56 -0500
From: Roger Dingledine <(b) (6)>
To: (b) (6)
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 amplification 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 Dingleline](#)
Cc: [Kelly DeYoe](#); [Shava Nerad](#)
Subject: [Fwd: Re: Fwd: Re: [Fwd: Fw: Vidalia looking for Farsi translator]]
Date: Monday, November 06, 2006 9:52:00 AM

Roger - Fred seems interested re Farsi, was supposed to hear from him by today.
Ken

----- Original Message -----

Subject: Re: Fwd: Re: [Fwd: Fw: Vidalia looking for Farsi translator]

Date: Thu, 02 Nov 2006 07:06:16 -0500

From: Ken Berman <(b) (6)>

To: farid pouya <(b) (6)>

CC: Shava Nerad <(b) (6)>

Kelly DeYoe

References:

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

thanks very much, Fred. This is something we are using and deploying worldwide for both Iranian and Chinese citizens to counteract their government's filtering. It is a very powerful tool with a thousand nodes worldwide and growing, and having it in Farsi will aid the overall effort.

Ken

farid pouya wrote:

Please let me check it and I will let you know about until Monday. Money does not matter. If I can do it it will be free of charge.

Best
Fred

On 11/1/06, **Ken Berman** <(b) (6)> wrote:

Great, Fred!. Not sure the level of effort involved, and the Vidalia engine requires a Unix platform, I believe. Pls look over the page below, see if you are comfortable with the directions and technical details, and then give us an idea for how many hours you think it would take plus your hourly rate. Then, if all is in order, our challenge would be how to actually pay you considering the multiple currencies and our Govmt funds being here in DC!

thanks for your support,
Ken

farid pouya wrote:

Dear Shava,
Dear Ken,

My real name is [REDACTED] (b) (6)
background). I will be glad to be able to do any help.

Best Regards

----- Forwarded message -----

From: **Shava Nerad** <[REDACTED] (b) (6)>
Date: Oct 31, 2006 8:59 PM
Subject: Fwd: Re: [Fwd: Fw: Vidalia looking for Farsi translator]
To: farid pouya <[REDACTED] (b) (6)>

Hi! Ken Berman from IBB is trying to reach you to help find Farsi translators -- his email is below. I had forgotten you write under a pseudonym, and gave him your pseudonym -- I hope I didn't make a mess?

Thanks!
Shava

>Delivered-To: [REDACTED] (b) (6)
>Date: Tue, 31 Oct 2006 08:26:46 -0500
>From: Ken Berman <[REDACTED] (b) (6)>
>
>
>Shava - I am trying to find out if this person is on payroll at
>Radio Farda or VOA. Can't seem to locate him yet. Ken

Shava Nerad
Executive Director
<http://tor.eff.org/>
<http://blogs.law.harvard.edu/anonymous/>

[REDACTED] (b) (6)
[REDACTED] (b) (6) (cell)
skype: shava23

From: [REDACTED] (b) (6) on behalf of Roger Dingledine
To: [REDACTED] (b) (6)
Subject: [PET] PETS 2011 stipend page up (June 1 deadline)
Date: Sunday, May 22, 2011 3:05:42 PM

Hi folks,

We've finally sorted out our sponsor situation and put up the page for stipend details:

<http://petsymposium.org/2011/stipends.php>

Note the (quite soon) deadline of June 1 if you want your stipend application to be considered on an equal footing with the other applications submitted by then.

--Roger

PET mailing list

[REDACTED] (b) (6)
<http://lists.links.org/mailman/listinfo/pet>

From: (b) (6) on behalf of Andreas Pfitzmann
To: Rafail Ostrovsky; Duvinage Nicolas; Gar Yeung Seto; Giovanni Baruzzi; Matthias Kirchner; Anja Jerichow; Vaclav Matyas; Marit Hansen; Dagmar Schönfeld; Heinrich Langos; Oliver Berthold; Martin Kurze; Elke Franz; Michael Waidner; (b) (6) PET-board; Stefanos Gritzalis; Martina Gersonde; Christos Kalloniatis; Rainer Böhme; Thomas Gloe; (b) (6) Karen Siebert; Hartmut Pohl; Rigo Wenning; Perez Oren Dr.; Holger Ziemek; Mike Bergmann; (b) (6) Ingo Friese; Thomas Kriegelstein; Dipl.-Inf. Heiko Boettcher; Andreas Westfeld; Horst Lazarek; (b) (6) Jörg Heuer; Antje Winkler; Günther Pernul; (b) (6) Stefan Berthold; Hagen Wahrig; Rolf Wendolsky; Huysmans Xavier; Haddad Wassim; Yves Deswarte; Stefan Schiffner; Riccardo Genghini; Stefan Köpsell; Stefan Zeidler; Katja Liesebach; Katrin Borcea-Pfitzmann; Vyskor Jozef; nymip-res-group; Jan Zöllner; Uwe Danz; Birgit Baum-Waldner; Alf Zugenmaier; Shlomi Dolev; Stefanie Pöttsch; Herbert Klimant; GI FG PET; Riha Zdenek; Sandra Steinbrecher; Rüdiger Dierstein; Caspar Bowden; Giuseppe Palumbo; Gritta Wolf; Andreas Juschka; Martin Rost; Silyia Labuschke; Matthias Schunter; Claudia Federrath; Gerhard Weck; Peter Weik; Petra Humann; Roger Dingleline; Sebastian Clauss; Honigova Alena; Thomas Weber; Birgit Pfitzmann; PRIME PRIME; Alexander Böttcher; Markus Hansen; Mailinglist PET; Hannes Federrath; list FIDIS; Anja Vogel; (b) (6) Doğan Norwegen Kesdoğan; Immanuel Scholz; Diskussion SPP; Claudia Diaz
Subject: [PET] Anon Terminology v0.29 is on the web
Date: Tuesday, July 31, 2007 6:53:29 AM

Hi,

Marit and myself are happy to announce

Anonymity, Unlinkability, Undetectability, Unobservability,
Pseudonymity, and Identity Management –
A Consolidated Proposal for Terminology
(Version v0.29 July 31, 2007)

http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

This is the largest revision ever - so hopefully worth reading.

We are happy to receive your comments and suggestions for improvements or extensions.

We hope that the next version v0.30, which probably will contain less changes, will come out in August or September - preferably this year ;-)

Best

Andreas

--

Andreas Pfitzmann

Dresden University of Technology Phone (mobile) + (b) (6)
Department of Computer Science (mobile) + (b) (6)
Institute for System Architecture (office) + (b) (6)
Noethnitzer Str. 46, Room 3071 (secretary) + (b) (6)
01062 Dresden, Germany Fax + (b) (6)
<http://dud.inf.tu-dresden.de> e-mail (b) (6)

PET mailing list

(b) (6)
<https://mailman.aldigital.co.uk/mailman/listinfo/pet>

From: PET on behalf of Roger Dingleline
To: Sadia Afroz
Cc: [REDACTED]
Subject: [PET] Surveillance-and-Technology workshop attached to PETS, deadline March 1
Date: Saturday, February 21, 2015 3:53:16 AM

On Thu, Feb 12, 2015 at 08:12:44PM -0800, Sadia Afroz wrote:
> CALL FOR PAPERS - PETS 2015
>
> Only 3 days to go for the last deadline for PETS 2015.

Hi Sadia,

Great job at telling the world about PETS this year. If you have a spare moment to do some more advocacy, the submission deadline for SAT, the Surveillance-and-Technology workshop attached to PETS, is coming up on March 1:

<https://satsymposium.org/>

It has a great program committee, and I am looking forward to the keynote by Chris Soghoian. But I bet approximately nobody knows about the workshop.

I am taking the first step by cc'ing the pets mailing list. :)

Thanks!
--Roger

PET mailing list

[REDACTED]
<http://lists.links.org/mailman/listinfo/pet>

From: [Roger Dingleline](#)
To: [Kelly DeYoe](#)
Cc: [Ken Berman](#); [Bennett Haselton](#); (b) (6) [Betty Pruitt](#)
Subject: "Anonymity and Usability"
Date: Wednesday, August 02, 2006 2:56:40 PM

Hi folks,

Did I ever point you at the Anonymity and Usability paper that Nick and I presented at WEIS 2006 at the end of June?

<http://freehaven.net/doc/wupss04/usability.pdf>
<http://freehaven.net/~arma/slides-weis06.pdf>

--Roger

From: [Ken Berman](#)
To: [Roger Dingleline](#)
Cc: [Kelly_DeYoe](#); [Shava Nerad](#)
Subject: 1:30>>2:00??
Date: Tuesday, October 16, 2007 2:26:41 PM

Can we move our call to 2:00?

From: Shava Nerad
To: [Roger Dingledine](#); (b) (6) [Ken Berman](#); [Kelly DeYoe](#)
Subject: 10am Monday call
Date: Monday, June 04, 2007 12:22:16 AM

We're assuming that you are going to call us and conference us in. Roger sent you his number; please use my landline, below.

Thanks, looking forward to it!

--

Shava Nerad
Executive Director
The Tor Project
<http://tor.eff.org/>
<http://blogs.law.harvard.edu/anonymous/>
(b) (6)
(b) (6)
(b) (6) (cell)
skype: shava23

From: [Kelly DeYoe](#)
To: [Shava Nerad](#); [Roger Dingleline](#)
Subject: 2007 contract SOW draft
Date: Thursday, January 18, 2007 4:45:23 PM
Attachments: [SOW-Tor2.doc](#)

Based on our discussions and review of your development roadmap and blocking resistance design, here's the statement of work I've come up with for our contract with you for 2007. Please review and let me know if you see any problem areas as soon as possible.

Sorry for the delay in getting this to you.

-k

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#)
Subject: Andrew in town May 2-3
Date: Sunday, April 28, 2013 12:14:33 PM

Hello Kelly,

It's been a while since we met. Are you up for a quick check-in either May 2nd or 3rd? I'll be in town both days and happy to meet up.

Thanks.

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: [Bennett Haselton](#)
To: [Kelly DeYoe](#); (b) (6) [Roger Dingleline](#)
Subject: are we having the meeting without Ken?
Date: Monday, July 24, 2006 4:05:39 AM

I got his auto-response that he was going to be out of the office until July 31st. Does that mean we'll be having the conference call without him or should we wait until he gets back?

-Bennett

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

<http://www.peacefire.org>

From: [Andrew Lewman](#)
To: [Ken Berman](#); [Kelly DeYoe](#); [Roger Dingleline](#); Sho Ho; [Jill Moss](#)
Subject: August 2011 BBG/Tor Report
Date: Thursday, September 15, 2011 10:50:04 AM
Attachments: [2011-August-Monthly-Report.pdf](#)

Hello Kelly, Ken, Kyle, Sho, and Jill,

Attached is the late August 2011 report. The release of a new stable tor branch dominates this report.

As always, if you have questions, feel free to ask. Thanks!

--

Andrew
pgp 0x74ED336B

From: Andrew Lewman
To: [REDACTED]; Roger Dingleline; 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: Andrew Lewman
To: Kelly_DeYoe; Marcia Jones
Cc: (b) (6)
Subject: BBG TSC invoice
Date: Tuesday, October 02, 2012 3:18:03 PM
Attachments: 2012-09-28-TorSolutions-Invoice-3.pdf

Hello Kelly and Marcia,

Please find attached our invoice for work performed in August-September. Thanks.

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: Roger Dingleline
To: Kelly DeYoe; Ken Berman
Subject: Bridge relays have users!
Date: Wednesday, June 11, 2008 7:37:58 AM

Hi folks,

We added a geoup db into Tor 0.2.0.27-rc a week or so back, so bridge relays could aggregate and report stats about their users. And now we have early answers.

The bridge named "drooper" was our first upgraded bridge, and it has reported:

```
geoup-start-time 2008-06-06 07:54:14  
geoup-client-origins ae=8,au=8,bh=8,gr=8,it=8,mx=8,pl=8,ro=8,tw=8,us=8
```

Ok, so it doesn't have our three target countries, but it has some countries next door!

(The "8" values represent somewhere between 1 and 8 users each; we intentionally blur the numbers so we don't introduce so much of an anonymity risk.)

In fact, I just checked further, and it looks like this bridge upgraded to the geoup db before we even released 0.2.0.27-rc. So it has older stats too:

```
geoup-start-time 2008-06-01 08:14:05  
geoup-client-origins ae=8,cn=8,de=8,it=8,pl=8,ro=8,tw=8,us=8
```

```
geoup-start-time 2008-06-03 14:25:34  
geoup-client-origins us=16,ae=8,au=8,cn=8,de=8,it=8,mx=8,pl=8,ro=8,tw=8
```

(Check out that 16! It represents somewhere between 9 and 16 users. That makes me believe a lot of these 8s represent more than one user.)

And I found another bridge ("carlos") reporting a few days ago:

```
geoup-start-time 2008-06-06 06:48:10  
geoup-client-origins cn=8,de=8,kw=8,vn=8
```

And the final note? carlos is running Windows XP. It looks like our push to make Windows users able to run bridges is working too.

--Roger

From: [Kelly DeYoe](#)
To: [Roger Dingleline](#)
Cc: [Ken Berman](#)
Subject: Call on Friday at 1:30?
Date: Tuesday, March 24, 2009 7:00:26 PM

Roger, you indicated Friday would be a good day for us to have a conference call to discuss the renewal for the next year. Ken suggested 1:30pm EDT, does that work for you?

-k

From: [Roger Dingleline](#)
To: [Demetria Anderson](#)
Cc: [Kelly DeYoe](#)
Subject: First invoice for Moria Research Labs, BBGCON1806S6149
Date: Friday, August 04, 2006 2:27:39 AM
Attachments: [mri-ibb1.pdf](#)

Hi Demetria,

Attached is my first invoice for contract BBGCON1806S6149. Please let me know if it includes all the needed information, or if I should add anything more.

Thanks!
--Roger

From: [Roger Dingleline](#)
To: [Demetria Anderson](#)
Cc: [Kelly DeYoe](#)
Subject: Fourth invoice for Moria Research Labs, BBGCON1806S6149
Date: Thursday, November 30, 2006 11:28:37 AM
Attachments: [mrl-ibb4.pdf](#)

Hi Demetria,

Attached is my fourth invoice for contract BBGCON1806S6149.

Thanks!
--Roger

From: Roger Dingleline
To: Kelly DeYoe
Cc: Ken Berman; (b) (6); (b) (6)
Subject: IBB's web-based translation system?
Date: Monday, February 04, 2008 11:22:47 AM

Hi Kelly,

We talked earlier about how IBB has a proprietary web-based translation system that makes it easier for the non-technical translators. Can you send me a few screenshots (or at least a description) to give me an idea of how the interface works?

We've been looking at <https://translations.launchpad.net/> but all the web-based translation paradigms I've seen so far are designed for short phrases like in dialog boxes, where context doesn't matter much. Translating a tutorial or a webpage one sentence at a time without regard for context seems like a recipe for disaster. So does it break it up into sentences on a single page and give you a series of "sentence and translation box for that sentence"? Or is there a better way?

Thanks!
--Roger

From: [Shava Nerad](#)
To: [Ken Berman](#); [Roger Dingledine](#); [Shava Nerad](#); [Kelly DeYoe](#)
Subject: in DC surrounding 3/23-25
Date: Thursday, March 08, 2007 10:20:19 AM

Coming down for shmoocon. I'm planning on taking a day or so one or both sides of the weekend to visit folks. Should I drop by? And what are the odds I'll have a contract to sign at that point? ;)

Thanks!

--

Shava Nerad
Executive Director
The Tor Project
<http://tor.eff.org/>
<http://blogs.law.harvard.edu/anonymous/>

(b) (6)

(b) (6)

(b) (6)

(cell)

skype: shava23

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


Website: <https://www.torproject.org/>

Blog: <https://blog.torproject.org/>

Identi.ca: torproject

Skype: lewmanator

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#)
Cc: [Ken Berman](#); [Jill Moss](#); [Sho Ho](#)
Subject: July Progress Report from Tor
Date: Wednesday, August 10, 2011 4:11:11 PM
Attachments: [2011-July-Monthly-Report.pdf](#)

Hello Kelly, Ken, Sho, and Jill,

Attached is our July progress report. As always, please ask questions if you have them.

Thanks!

--

Andrew
pgp 0x74ED336B

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#); [Marcia Jones](#)
Cc: [REDACTED]
Subject: Invoice 5 for Tor Solutions
Date: Wednesday, November 28, 2012 2:49:58 PM
Attachments: [2012-11-28-TorSolutions-Invoice-5.pdf](#)

Hello Kelly and Marcia,

Please find attached invoice #5 for our current contract.

Thanks.

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: [Andrew Lewman](#)
To: [Marcia Jones](#); [Kelly DeYoe](#)
Cc: (b) (6)
Subject: Invoice 11 for Tor Solutions
Date: Tuesday, June 04, 2013 1:39:23 PM
Attachments: [2013-06-04-TorSolutions-Invoice-11.pdf](#)

Hello Marcia and Kelly,

Please find attached our 11th invoice for the current contract.

Thanks.

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#); [Marcia Jones](#)
Cc: (b) (6)
Subject: Invoice for Tor Solutions Sep - Oct 2012
Date: Monday, October 29, 2012 3:12:39 PM
Attachments: [2012-10-28-TorSolutions-Invoice-4.pdf](#)

Hello Kelly and Marcia,

Please find attached our invoice for Sep - Oct 2012 work. Thanks.

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: [Andrew Lewman](#)
To: [Malita Dyson](#)
Cc: [Kelly DeYoe](#);
Subject: Invoice from Tor Project
Date: Tuesday, June 14, 2011 12:43:38 PM
Attachments: [2011-May-invoice-no37.pdf](#)

Hello Malita and Kelly,

Please find attached our invoice for work performed between April 17 and May 17. Thank you.

--

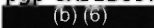
Andrew
pgp 0x74ED336B

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#); [Ken Berman](#); [Sho Ho](#)
Cc: [Roger Dingledine](#)
Subject: January 2010 Tor Project Report
Date: Tuesday, February 09, 2010 7:49:00 PM
Attachments: [2010-02-01-IBB-January-report.pdf](#)

Hello,

Please find attached the January Report. Sorry for the delay, I was in Belgium talking to EU Parliament and FOSDEM through today.

--

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

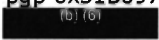
Website: <https://torproject.org/>
Blog: <https://blog.torproject.org/>
Identi.ca: torproject

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#); [Ken Berman](#); [Sho Ho](#)
Cc: [Roger Dingledine](#)
Subject: January 2010 Tor Project Report
Date: Tuesday, February 09, 2010 7:49:00 PM
Attachments: [2010-02-01-IBB-January-report.pdf](#)

Hello,

Please find attached the January Report. Sorry for the delay, I was in Belgium talking to EU Parliament and FOSDEM through today.

--

Andrew Lewman
The Tor Project
pgp 0x31B0974B


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

From: [Shava Nerad](#)
To: [Ken Berman](#); [Roger Dingledine](#)
Cc: [Kelly DeYoe](#); [Andrew Lewman](#)
Subject: July 10 report for Tor
Date: Tuesday, July 10, 2007 2:35:21 PM
Attachments: [Tor June 07 report.doc](#)

Please find attached! :)

Thanks!

--

Shava Nerad
Development Director
The Tor Project
<http://tor.eff.org/>
<http://blogs.law.harvard.edu/anonymous/>

(b) (6)

(b) (6)

(cell)

skype: shava23

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#); [Sho Ho](#)
Subject: July 17 - August 18 Progress Report from Tor
Date: Thursday, August 30, 2012 1:04:15 PM
Attachments: [2012-July-TorSolutions-BBG-Monthly-Report.pdf](#)

Hello Kelly and Sho,

Please find attached our progress report for last month. As always, feel free to ask questions.

Thanks!

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#); [Sho Ho](#)
Subject: July 17 - August 18 Progress Report from Tor
Date: Thursday, August 30, 2012 1:04:41 PM
Attachments: [2012-July-TorSolutions-BBG-Monthly-Report.pdf](#)

Hello Kelly and Sho,

Please find attached our progress report for last month. As always, feel free to ask questions.

Thanks!

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: Tov, Debbie
To: Ken Berman; Danny Bilson; David Cannon; Kelly DeYoe; Flint Dille; Roger Dingleline; Cristin Goodwin (FLYNN); Lance James; Todd Richmond; Paul Syverson; Rob Thomas; [REDACTED] Bill Marlow
Cc: Shultis, John; Kangaroo, Sunny
Subject: CENTRA conference Sept. 20-21, 2006
Date: Tuesday, September 12, 2006 12:42:40 PM

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.stratagroup.org>

I or my colleague Sunny Kangaroo 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: [REDACTED] (b) (6)
Fax: [REDACTED] (b) (6)
Email: [REDACTED] (b) (6)

From: [Roger Dingleline](#)
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

From: [Andrew Lewman](#)
To: [REDACTED], [Sho Ho](#)
Cc: [Roger Dingledine](#)
Subject: June 2009 Tor Progress Report
Date: Saturday, July 11, 2009 12:21:33 AM
Attachments: [2009-07-06-IBB-June-report.pdf](#)

Hello all,

Sorry for the delay in getting this to you. Due to a death in the family my schedule has been turned upside down.

Please find attached our June 2009 Progress Report.

--

Andrew Lewman
The Tor Project
pgp 0x31B0974B
[REDACTED]

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

From: Andrew Lewman
To: Kelly Mays; Ken Vermaas; [REDACTED]
Subject: June 2011 Progress Report from Tor
Date: Wednesday, July 13, 2011 3:49:41 PM
Attachments: 2011-June-Monthly-Report.pdf

Hello Kelly, Sho, and Ken,

Sorry for the delayed progress report. Please find it attached.

Thanks!

--

Andrew
pgp 0x74ED336B

From: [Roger Dingledine](#)
To: [Ken Berman](#); [Kelly DeYoe](#); [Isaac Mao](#)
Subject: Ken and Kelly should meet Isaac
Date: Wednesday, October 25, 2006 8:47:42 PM

Hi Ken, Kelly, Isaac,

I should introduce you to each other.

Ken and Kelly work at IBB, which helps support Voice of America, Radio Free Europe and Radio Liberty, 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).

Isaac is a nice guy, presumably in PRC, who has gathered together a group of experts in the Chinese firewall, and to a lesser extent various similar firewalls around the world. I haven't met Isaac yet, but I've met people who say they have. :)

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

Thanks,
--Roger

From: [Bennett Haselton](#)
To: [Roger Dingleline](#); [Ken Berman](#); (b) (6) [Kelly DeYoe](#)
Date: Monday, July 24, 2006 3:14:12 AM
Attachments: [tor-modifications-for-china.html](#)
[ATT00001.txt](#)

This is short but actually took several revisions to get right, to find the most efficient routes and to eliminate weaknesses that could be attacked. Hopefully we can use this as the jumping-off point for the conference call.

As usual the best times for me are around noon or 1 PM Pacific Coast time.

-Bennett

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#)
Cc: [REDACTED]
Subject: Missing payment to Tor somewhere
Date: Monday, December 12, 2011 3:27:48 PM

Hello Kelly,

Melissa and I were closing out our last contract today. We notice we're missing \$15,000 somewhere. Who can we work with on your end to figure out if we missed an invoice, or a payment got crossed up somewhere?

Thanks!

--

Andrew
pgp 0x74ED336B

From: [Kelly DeYoe](#)
To: [Andrew Lewman](#)
Cc: [Roger Dingleline](#); [Diane Sturgis](#); [Rachel Johnson](#)
Subject: Modification to BBG50-J-12-0508 for Tor Solutions Group to exercise options
Date: Wednesday, September 26, 2012 5:44:36 PM
Attachments: [BBG50-J-12-0508 MOD 001.pdf](#)

Andrew & Roger, attached is a modification to our existing task order BBG50-J-12-0508 for Tor Solutions Group to exercise options for some of the software development items that are in the SOW. I would like to schedule a conference call soon to discuss these newly awarded options, please let me know about your availability over the next couple weeks. Thanks,

-k

From: Roger Dingledine
To: Ken Berman; Kelly DeYong; Sho Ho
Cc: [REDACTED]
Subject: More Tor URLs to read
Date: Thursday, February 19, 2009 8:52:25 PM

Hi folks,

Here are some other URLs you might find interesting, from what we've been up to over the past month:

<https://blog.torproject.org/blog/two-incentive-designs-tor>
fleshes out the two incentive designs we've been thinking about, and discusses how to move forward.

<https://blog.torproject.org/blog/overhead-directory-info%3A-past%2C-present%2C-future>
explains our next steps in making Tor more suitable for modern users (along with trying to document our previous steps).

<https://blog.torproject.org/blog/one-cell-enough>
walks through an attack on Tor presented this week.

<http://freehaven.net/~karsten/lenhard2009performance-submitted.pdf>
is Karsten's paper with Jörg Lenhard on hidden service performance measurements in low-bandwidth access networks. It's not published yet, so please don't share it too widely, but hopefully it will be another component in letting us understand our current slowdowns.

<https://www.torproject.org/projects/metrics>
are some other graphs that Karsten has been making lately. When we met a few weeks ago I mentioned that the number of Tor relays slowly decreased in 2008; Karsten figured out that actually only the number of relays in Germany decreased; the rest are doing fine. Looks like we're going to need to pay even more attention to the "data retention in Germany" question.

<https://www.torproject.org/torbrowser/>
The new TBB we put out this week moves us to Firefox 3, but more importantly it gets rid of the "PortableFirefox" build requirement we used to have, which was preventing our users from running TBB alongside another copy of Firefox. Now this is possible.

More soon,
--Roger

From: Roger Dingledine
To: Ken Berman; Kelly DeYoe; Sho Ho
Cc: [REDACTED]
Subject: More Tor URLs to read
Date: Thursday, February 19, 2009 8:52:25 PM

Hi folks,

Here are some other URLs you might find interesting, from what we've been up to over the past month:

<https://blog.torproject.org/blog/two-incentive-designs-tor>
fleshes out the two incentive designs we've been thinking about, and discusses how to move forward.

<https://blog.torproject.org/blog/overhead-directory-info%3A-past%2C-present%2C-future>
explains our next steps in making Tor more suitable for modem users (along with trying to document our previous steps).

<https://blog.torproject.org/blog/one-cell-enough>
walks through an attack on Tor presented this week.

<http://freehaven.net/~karsten/lenhard2009performance-submitted.pdf>
is Karsten's paper with Jörg Lenhard on hidden service performance measurements in low-bandwidth access networks. It's not published yet, so please don't share it too widely, but hopefully it will be another component in letting us understand our current slowdowns.

<https://www.torproject.org/projects/metrics>
are some other graphs that Karsten has been making lately. When we met a few weeks ago I mentioned that the number of Tor relays slowly decreased in 2008; Karsten figured out that actually only the number of relays in Germany decreased; the rest are doing fine. Looks like we're going to need to pay even more attention to the "data retention in Germany" question.

<https://www.torproject.org/torbrowser/>
The new TBB we put out this week moves us to Firefox 3, but more importantly it gets rid of the "PortableFirefox" build requirement we used to have, which was preventing our users from running TBB alongside another copy of Firefox. Now this is possible.

More soon,
--Roger

From: Roger Dingledine
To: Ken Berman; Kelly DeYoe; Sho Ho
Cc: [REDACTED]
Subject: More Tor URLs to read
Date: Thursday, February 19, 2009 8:52:25 PM

Hi folks,

Here are some other URLs you might find interesting, from what we've been up to over the past month:

<https://blog.torproject.org/blog/two-incentive-designs-tor> fleshes out the two incentive designs we've been thinking about, and discusses how to move forward.

<https://blog.torproject.org/blog/overhead-directory-info%3A-past%2C-present%2C-future> explains our next steps in making Tor more suitable for modem users (along with trying to document our previous steps).

<https://blog.torproject.org/blog/one-cell-enough> walks through an attack on Tor presented this week.

<http://freehaven.net/~karsten/lenhard2009performance-submitted.pdf> is Karsten's paper with Jörg Lenhard on hidden service performance measurements in low-bandwidth access networks. It's not published yet, so please don't share it too widely, but hopefully it will be another component in letting us understand our current slowdowns.

<https://www.torproject.org/projects/metrics> are some other graphs that Karsten has been making lately. When we met a few weeks ago I mentioned that the number of Tor relays slowly decreased in 2008; Karsten figured out that actually only the number of relays in Germany decreased; the rest are doing fine. Looks like we're going to need to pay even more attention to the "data retention in Germany" question.

<https://www.torproject.org/torbrowser/>
The new TBB we put out this week moves us to Firefox 3, but more importantly it gets rid of the "PortableFirefox" build requirement we used to have, which was preventing our users from running TBB alongside another copy of Firefox. Now this is possible.

More soon,
--Roger

From: Roger Dingledine
To: (b) (6) Ken Berman; Kelly DeYoe
Subject: Notes on Apr and May
Date: Monday, June 04, 2007 12:04:54 AM

Hi folks,

I've sorted the items from the previous mail by category based on the SOW-Tor2-1.doc dated March 19 from Kelly. Some of the items fit into several categories, so I put each item in the best one I could think of and made a note about the other related ones.

This obviously isn't the pretty version (Shava will be working on that for the 10th), but I figured I should send it before the phone call tomorrow.

I hope this makes things clearer. When we're on the phone I'll explain why all of this translates to "good news, we're on track!" :)
--Roger

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

APR New Tor stable release comes with a much newer version of Vidalia (0.0.11 vs 0.0.7):
<http://trac.vidalia-project.net/browser/releases/vidalia-0.0.11/CHANGELOG>
which includes a Farsi translation now as well as the traditional Chinese translation.
[Also C.2.10]

APR The Windows Tor bundle now ships with Torbutton and installs it automatically during the bundle install process.
[Also C.2.10]

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

MAY We're on target with the current design document. For a more detailed description of the immediate next steps, see
<http://archives.seul.org/or/dev/May-2007/msg00008.html>

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

APR It's a lot easier to run Tor as a server now: it does rate limiting in a more intuitive way, it automatically detects your IP address so you don't have to configure that, and it does a brief bandwidth test when it starts up so it's useful to the network more quickly.
[Also C.2.7]

APR The new Vidalia includes a new more intuitive interface that makes it easier to opt to become a Tor server.
[Also C.2.7]

APR Google gave us four interns for the summer as part of their Google Summer of Code project, and one of them is working directly on the Tor-server-on-Windows-XP stability bug.

MAY Rate limiting that only applies to relayed connections -- now servers can set a bandwidth rate on traffic they carry for other people, without that limit applying to their own Tor traffic.
This is a critical step for making it easy to run a bridge.

[Also C.2.7]

MAY The 0.2.0 Tor branch uses way less memory to run a Tor server. Hopefully this will let things scale to a larger Tor network, and it may also mean people can run bridges on lighter hardware.

[Also C.2.7, C.2.11]

C.2.5. Hide Tor's network signature.

APR Servers no longer demand the particular Tor TLS handshake we currently use -- so now we can change it down the road and they will still accept the connections.

MAY Encrypted directory connections: If you add two lines to your Tor configuration file, all your directory connections happen over TLS-encrypted links. There's no need for plaintext http connections anymore. Not enabled by default yet, because we need to think about strategy in the arms race: how many cards do we play vs how many do we hold in reserve?

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 have a few plans but we still need to refine them. Stay tuned. (Or read <https://tor.eff.org/svn/trunk/doc/spec/proposals/105-handshake-revision.txt> if you can't wait. :)

C.2.7. Let the Tor network scale better.

MAY Separate out a few of the biggest entries in Tor server descriptors and put them in a different "extrainfo" descriptor that most clients will never need to fetch. This should save about 60% for directory descriptor fetching overhead.

[Also C.2.1, C.2.3]

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

To be filled in by Shava:

Through community outreach in the press

[examples [[look in google for those two months]]]

and through events

[examples SXSW and Shmocon in March and Oxford in May], The Tor Project has brought substantial additional attention to the project to the public and among our communities of interest.

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

APR A new "AvoidDiskWrites" config option for Tor that you can set when you're running on media that's slow or shouldn't get rewritten often -- like a USB key or a linksys router. Still has a lot of room for improvement.

MAY Tor can now resolve DNS requests itself: just enable your DNSPort in the Tor configuration file. This feature makes it a lot easier to ship a self-contained Tor on a LiveCD, USB bundle, etc.

[Also C.2.1]

MAY Three volunteer LiveCD Tor distributions have appeared. None have good (or at least documented) security yet, but I hope June's report will talk about how we're starting to coordinate them to produce a

"best practices" document for how to securely configure the common applications, so they don't have to independently discover it each time.

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#); [Ken Berman](#); [Sho Ho](#)
Cc: [Roger Dingedine](#)
Subject: November 2010 Progress Report from Tor
Date: Friday, December 10, 2010 1:22:27 PM
Attachments: [2010-November-Monthly-Report-BBG.pdf](#)

Hello Kelly, Ken, and Sho,

Please find attached our monthly progress report for November 2010. As always, we're open to discussion about the contents.

Thanks!

--

Andrew
pgp 0x74ED336B

From: Shava Nerad
To: Kelly DeYoe; Roger Dingledine
Subject: penultimate draft
Date: Friday, March 16, 2007 8:11:15 PM
Attachments: [Statement of work Mar 16 2007.pdf](#)

Still needs signature inserted, but changes incorporated.

Thanks!

--

Shava Nerad
Executive Director
The Tor Project
<http://tor.eff.org/>
<http://blogs.law.harvard.edu/anonymous/>

(b) (6)

(b) (6)

(b) (6)

(cell)

skype: shava23

From: Bennett Haselton
To: Ken Berman; Simson Garfinkel; Roger Dingledine; (b) (6); Kelly DeYoe; (b) (6)
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

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

From: Andrew Lewman
To: [REDACTED]; Dingledine, Roger
Subject: Popular Chinese Filtering Circumvention Tools Sell User Data
Date: Monday, January 12, 2009 1:09:59 PM

In case you haven't seen this:

<http://blogs.law.harvard.edu/hroberts/2009/01/09/popular-chinese-filtering-circumvention-tools-dynaweb-freegate-gpass-and-firephoenix-sell-user-data/>

I did a blog post with a general response,

<https://blog.torproject.org/blog/circumvention-and-anonymity>

--

Andrew Lewman
The Tor Project

[REDACTED]
pgp 0x31B0974B
[REDACTED]

Website: <https://torproject.org/>
Blog: <https://blog.torproject.org/>
Twitter: <http://twitter.com/torproject>

From: Roger Dingledine
To: Kelly DeYoe
Cc: Sho Ho; Ken Berman; [REDACTED] [REDACTED]
Subject: Preliminary performance changes in Tor
Date: Wednesday, September 23, 2009 8:16:51 AM

Hi Kelly,

[Executive summary: median download time is down to 2.5 seconds from 7.8 seconds, but several caveats, and still much to do.]

We've got two early graphs to indicate we're heading in the right direction.

First, recall the slide from my HAR talk where we remarked that the median latency for fetching a 50KB file through Tor was 7.8 seconds.

Now check out graphs 4-6 of <https://git.torproject.org/checkout/metrics/master/report/performance/torperf-2009-09-22.pdf>
We've rolled out Mike's new "bwaauthority" scripts, where four of the directory authorities are now doing active bandwidth measuring of relays, and voting on the bandwidth values for the consensus. Clients then do their load balancing based on the numbers in the consensus rather than the numbers self-claimed by each relay. Technical details here:
<https://svn.torproject.org/svn/torflow/trunk/NetworkScanners/BwAuthority/README.BwAuthorities>
<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/161-computing-bandwidth-adjustments.txt>

Check out the two dips in latency on the right-hand side of each graph. The first dip was our first experimental rollout; it had some bugs, so we stopped doing it for a couple days. The second dip is when we turned it on again, a week or two ago. So it's a bit early to say for sure, but for now at least we've cut the median download time for a 50KB file from 7.8 seconds to around 3.7 seconds.

Now for the second graph. Check out Figure 3 in <https://git.torproject.org/checkout/metrics/master/report/buildtimes/buildtimes-2009-09-22.pdf>
This is using Mike's new algorithm for throwing away the worst 20% of the circuits we make. Technical details here:
<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/151-path-selection-improvements.txt>
The goal is for each user to adapt their own timeout, based on how long it's taken them to build circuits in the past. So people on fast connections will end up discarding any circuit that's taken more than 5 or 6 seconds to build, whereas people on slow connections could have a timeout closer to 30 or 60 seconds. We clearly need more testing for slower connections; but the code only came together this week, so we're focusing on debugging it for normal users first.

So with the bwaauthority results, we moved from 7.8 to 3.7 for the median download time. With both improvements in action together, we moved down to more like 2.5 seconds for users on a fast connection. Woo.

Now, the job isn't done. One of the main next pieces is to give reduced priority to circuits that have sent a lot of cells lately. We're working with Ian Goldberg and his students at Waterloo to figure out the right design to use there. If we don't do this step, people are going to catch on that "lower latency in Tor" actually corresponds really well to "higher throughput in Tor", and the file-sharers will march in and take

back the ground we've gained. But on the plus side, Tor is faster for youtube this week. :)

Another component that will slow down the file-sharers is reducing our circuit window:

<http://archives.seul.org/or/dev/Aug-2009/msg00006.html>

<http://archives.seul.org/or/dev/Sep-2009/msg00000.html>

There's some ongoing spirited debate about whether this "should" make things better or worse for the ordinary users. We've even got some preliminary measurements that aren't convincing in either direction.

Check out Figure 3 of

<https://git.torproject.org/checkout/metrics/master/report/circwindow/circwindow-2009-09-20.pdf>

They clearly ruin the download speed for 1MB files, but it's unclear whether the emergent properties when more relays run the code would cause less congestion overall. So our conclusion is that we're now broadcasting the circuit window that relays should use as a parameter in the directory consensus:

<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/167-params-in-consensus.txt>

and once a lot of relays have upgraded (so they read the number out of the consensus rather than using their own hard-coded value), we can deploy various numbers and see if the Tor network gets faster, slower, or what. That test is probably several months away though, since we need enough relays to upgrade first.

--Roger

From: Roger Dingledine
To: Kelly DeYoe
Cc: Sho Ho; Ken Berman; (b) (6); (b) (6)
Subject: Preliminary performance changes in Tor
Date: Wednesday, September 23, 2009 8:16:51 AM

Hi Kelly,

[Executive summary: median download time is down to 2.5 seconds from 7.8 seconds, but several caveats, and still much to do.]

We've got two early graphs to indicate we're heading in the right direction.

First, recall the slide from my HAR talk where we remarked that the median latency for fetching a 50KB file through Tor was 7.8 seconds.

Now check out graphs 4-6 of <https://git.torproject.org/checkout/metrics/master/report/performance/torperf-2009-09-22.pdf>
We've rolled out Mike's new "bwauthority" scripts, where four of the directory authorities are now doing active bandwidth measuring of relays, and voting on the bandwidth values for the consensus. Clients then do their load balancing based on the numbers in the consensus rather than the numbers self-claimed by each relay. Technical details here:
<https://svn.torproject.org/svn/torflow/trunk/NetworkScanners/BwAuthority/README.BwAuthorities>
<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/161-computing-bandwidth-adjustments.txt>

Check out the two dips in latency on the right-hand side of each graph. The first dip was our first experimental rollout; it had some bugs, so we stopped doing it for a couple days. The second dip is when we turned it on again, a week or two ago. So it's a bit early to say for sure, but for now at least we've cut the median download time for a 50KB file from 7.8 seconds to around 3.7 seconds.

Now for the second graph. Check out Figure 3 in <https://git.torproject.org/checkout/metrics/master/report/buildtimes/buildtimes-2009-09-22.pdf>
This is using Mike's new algorithm for throwing away the worst 20% of the circuits we make. Technical details here:
<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/151-path-selection-improvements.txt>
The goal is for each user to adapt their own timeout, based on how long it's taken them to build circuits in the past. So people on fast connections will end up discarding any circuit that's taken more than 5 or 6 seconds to build, whereas people on slow connections could have a timeout closer to 30 or 60 seconds. We clearly need more testing for slower connections; but the code only came together this week, so we're focusing on debugging it for normal users first.

So with the bwauthority results, we moved from 7.8 to 3.7 for the median download time. With both improvements in action together, we moved down to more like 2.5 seconds for users on a fast connection. Woo.

Now, the job isn't done. One of the main next pieces is to give reduced priority to circuits that have sent a lot of cells lately. We're working with Ian Goldberg and his students at Waterloo to figure out the right design to use there. If we don't do this step, people are going to catch on that "lower latency in Tor" actually corresponds really well to "higher throughput in Tor", and the file-sharers will march in and take

back the ground we've gained. But on the plus side, Tor is faster for youtube this week. :)

Another component that will slow down the file-sharers is reducing our circuit window:

<http://archives.seul.org/or/dev/Aug-2009/msg00006.html>

<http://archives.seul.org/or/dev/Sep-2009/msg00000.html>

There's some ongoing spirited debate about whether this "should" make things better or worse for the ordinary users. We've even got some preliminary measurements that aren't convincing in either direction.

Check out Figure 3 of

<https://git.torproject.org/checkout/metrics/master/report/circwindow/circwindow-2009-09-20.pdf>

They clearly ruin the download speed for 1MB files, but it's unclear whether the emergent properties when more relays run the code would cause less congestion overall. So our conclusion is that we're now broadcasting the circuit window that relays should use as a parameter in the directory consensus:

<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/167-params-in-consensus.txt>

and once a lot of relays have upgraded (so they read the number out of the consensus rather than using their own hard-coded value), we can deploy various numbers and see if the Tor network gets faster, slower, or what. That test is probably several months away though, since we need enough relays to upgrade first.

--Roger

From: Roger Dingledine
To: Kelly DeYoe
Cc: Sho Ho; Ken Berman; [REDACTED] [REDACTED]
Subject: Preliminary performance changes in Tor
Date: Wednesday, September 23, 2009 8:16:51 AM

Hi Kelly,

[Executive summary: median download time is down to 2.5 seconds from 7.8 seconds, but several caveats, and still much to do.]

We've got two early graphs to indicate we're heading in the right direction.

First, recall the slide from my HAR talk where we remarked that the median latency for fetching a 50KB file through Tor was 7.8 seconds.

Now check out graphs 4-6 of

<https://git.torproject.org/checkout/metrics/master/report/performance/torperf-2009-09-22.pdf>

We've rolled out Mike's new "bwauthority" scripts, where four of the directory authorities are now doing active bandwidth measuring of relays, and voting on the bandwidth values for the consensus. Clients then do their load balancing based on the numbers in the consensus rather than the numbers self-claimed by each relay. Technical details here:

<https://svn.torproject.org/svn/torflow/trunk/NetworkScanners/BwAuthority/README.BwAuthorities>

<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/161-computing-bandwidth-adjustments.txt>

Check out the two dips in latency on the right-hand side of each graph. The first dip was our first experimental rollout; it had some bugs, so we stopped doing it for a couple days. The second dip is when we turned it on again, a week or two ago. So it's a bit early to say for sure, but for now at least we've cut the median download time for a 50KB file from 7.8 seconds to around 3.7 seconds.

Now for the second graph. Check out Figure 3 in

<https://git.torproject.org/checkout/metrics/master/report/buildtimes/buildtimes-2009-09-22.pdf>

This is using Mike's new algorithm for throwing away the worst 20% of the circuits we make. Technical details here:

<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/151-path-selection-improvements.txt>

The goal is for each user to adapt their own timeout, based on how long it's taken them to build circuits in the past. So people on fast connections will end up discarding any circuit that's taken more than 5 or 6 seconds to build, whereas people on slow connections could have a timeout closer to 30 or 60 seconds. We clearly need more testing for slower connections; but the code only came together this week, so we're focusing on debugging it for normal users first.

So with the bwauthority results, we moved from 7.8 to 3.7 for the median download time. With both improvements in action together, we moved down to more like 2.5 seconds for users on a fast connection. Woo.

Now, the job isn't done. One of the main next pieces is to give reduced priority to circuits that have sent a lot of cells lately. We're working with Ian Goldberg and his students at Waterloo to figure out the right design to use there. If we don't do this step, people are going to catch on that "lower latency in Tor" actually corresponds really well to "higher throughput in Tor", and the file-sharers will march in and take

back the ground we've gained. But on the plus side, Tor is faster for youtube this week. :)

Another component that will slow down the file-sharers is reducing our circuit window:

<http://archives.seul.org/or/dev/Aug-2009/msg00006.html>

<http://archives.seul.org/or/dev/Sep-2009/msg00000.html>

There's some ongoing spirited debate about whether this "should" make things better or worse for the ordinary users. We've even got some preliminary measurements that aren't convincing in either direction.

Check out Figure 3 of

<https://git.torproject.org/checkout/metrics/master/report/circwindow/circwindow-2009-09-20.pdf>

They clearly ruin the download speed for 1MB files, but it's unclear whether the emergent properties when more relays run the code would cause less congestion overall. So our conclusion is that we're now broadcasting the circuit window that relays should use as a parameter in the directory consensus:

<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/167-params-in-consensus.txt>

and once a lot of relays have upgraded (so they read the number out of the consensus rather than using their own hard-coded value), we can deploy various numbers and see if the Tor network gets faster, slower, or what. That test is probably several months away though, since we need enough relays to upgrade first.

--Roger

From: Roger Dingledine
To: Kelly DeYoe
Cc: Sho Ho; Ken Berman; (b) (6) (b) (6)
Subject: Preliminary performance changes In Tor
Date: Wednesday, September 23, 2009 8:16:51 AM

Hi Kelly,

[Executive summary: median download time is down to 2.5 seconds from 7.8 seconds, but several caveats, and still much to do.]

We've got two early graphs to indicate we're heading in the right direction.

First, recall the slide from my HAR talk where we remarked that the median latency for fetching a 50KB file through Tor was 7.8 seconds.

Now check out graphs 4-6 of

<https://git.torproject.org/checkout/metrics/master/report/performance/torperf-2009-09-22.pdf>

We've rolled out Mike's new "bwauthority" scripts, where four of the directory authorities are now doing active bandwidth measuring of relays, and voting on the bandwidth values for the consensus. Clients then do their load balancing based on the numbers in the consensus rather than the numbers self-claimed by each relay. Technical details here:

<https://svn.torproject.org/svn/torflow/trunk/NetworkScanners/BwAuthority/README.BwAuthorities>

<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/161-computing-bandwidth-adjustments.txt>

Check out the two dips in latency on the right-hand side of each graph. The first dip was our first experimental rollout; it had some bugs, so we stopped doing it for a couple days. The second dip is when we turned it on again, a week or two ago. So it's a bit early to say for sure, but for now at least we've cut the median download time for a 50KB file from 7.8 seconds to around 3.7 seconds.

Now for the second graph. Check out Figure 3 in

<https://git.torproject.org/checkout/metrics/master/report/buildtimes/buildtimes-2009-09-22.pdf>

This is using Mike's new algorithm for throwing away the worst 20% of the circuits we make. Technical details here:

<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/151-path-selection-improvements.txt>

The goal is for each user to adapt their own timeout, based on how long it's taken them to build circuits in the past. So people on fast connections will end up discarding any circuit that's taken more than 5 or 6 seconds to build, whereas people on slow connections could have a timeout closer to 30 or 60 seconds. We clearly need more testing for slower connections; but the code only came together this week, so we're focusing on debugging it for normal users first.

So with the bwauthority results, we moved from 7.8 to 3.7 for the median download time. With both improvements in action together, we moved down to more like 2.5 seconds for users on a fast connection. Woo.

Now, the job isn't done. One of the main next pieces is to give reduced priority to circuits that have sent a lot of cells lately. We're working with Ian Goldberg and his students at Waterloo to figure out the right design to use there. If we don't do this step, people are going to catch on that "lower latency in Tor" actually corresponds really well to "higher throughput in Tor", and the file-sharers will march in and take

back the ground we've gained. But on the plus side, Tor is faster for youtube this week. :)

Another component that will slow down the file-sharers is reducing our circuit window:

<http://archives.seul.org/or/dev/Aug-2009/msg00006.html>

<http://archives.seul.org/or/dev/Sep-2009/msg00000.html>

There's some ongoing spirited debate about whether this "should" make things better or worse for the ordinary users. We've even got some preliminary measurements that aren't convincing in either direction.

Check out Figure 3 of

<https://git.torproject.org/checkout/metrics/master/report/circwindow/circwindow-2009-09-20.pdf>

They clearly ruin the download speed for 1MB files, but it's unclear whether the emergent properties when more relays run the code would cause less congestion overall. So our conclusion is that we're now broadcasting the circuit window that relays should use as a parameter in the directory consensus:

<https://git.torproject.org/checkout/tor/master/doc/spec/proposals/167-params-in-consensus.txt>

and once a lot of relays have upgraded (so they read the number out of the consensus rather than using their own hard-coded value), we can deploy various numbers and see if the Tor network gets faster, slower, or what. That test is probably several months away though, since we need enough relays to upgrade first.

--Roger

Shava, would you like to be in on the discussion? If so, do you have additional constraints to the ones I list at the top of this mail? :)

--Roger

From: [Shava Nerad](#)
To: [Shirley Hao](#); [Sharon Hom](#); [Ken Berman](#); [Roger Dingledine](#)
Cc: [Kelly DeYoe](#); [Hiu Ho](#)
Subject: RE: Conference call next Monday?
Date: Friday, November 17, 2006 10:01:46 PM

At 03:58 PM 11/17/2006, Shirley Hao wrote:

>I hope we'll be able to talk more (e-mail/phone/in person) on this. I'll
>be out of the office through the end of the November, but would be happy
>to send a follow-up email and more information after I return...

Actually, I've been meaning to get up with you since at least August, when I visited your near neighbors at Amnesty and then in DC met with Ken and also Human Rights Watch, and everyone was saying "Why aren't you talking to HRIC?"

I'd love to get together, phone or in person, to talk about how many ways our work can fit together! It's a short run between Boston and NYC. Email/phone/skype are also fine. But yes, let's set up something for December, perhaps?

I just got back from France myself (Ken et al -- a productive trip, I'll catch up later...) but I did want to send you email as soon as I landed.

Xi jian!

Shava Nerad
Executive Director
<http://tor.eff.org/>
<http://blogs.law.harvard.edu/anonymous/>

(b) (6)
(b) (6)
(b) (6) (cell)
skype: shava23

From: [Roger Dingleline](#)
To: [Kelly DeYoe](#)
Subject: Re: Contract status update
Date: Wednesday, March 22, 2006 7:31:47 PM

On Wed, Mar 22, 2006 at 06:18:14PM -0500, Kelly DeYoe wrote:
> Ok, so the latest update on the contract is that it is just awaiting the
> CFO's approval before it can go to the Contracts office for award...
> which sounds not much further along than it was 3 weeks ago I'm afraid.
> Unfortunately, the administrative person who is in charge of this from
> our office is out this week, so I was receiving the info secondhand from
> another admin. officer, so I will check with the primary contact again
> on Monday.

Exciting. Thanks for sticking with this.

Just so we're on the same page, the money for the current contract is intended to be spent in FY06 on work in FY06? So that means that once the contract finally does come through, we're still planning for me to bill all the hours in the current round by the end of FY06?

Thanks,
--Roger

From: (b) (6)
To: Roger Dingleline
Cc: Shava Nerad
Subject: Re: Conference call next Monday?
Date: Friday, November 03, 2006 7:42:46 AM

Roger, haven't heard anything back from you about your availability for a conference call this coming Monday 11/6. I've been in class all day the past 2 days, and will be again today, so haven't been able to follow up with a telephone call.

If you could confirm a time by email, or let me know that you're not available on Monday, as soon as possible, it would be appreciated.

Thanks,

-k

----- Original Message -----

From: Kelly DeYoe <(b) (6)>
Date: Tuesday, October 31, 2006 3:52 pm
Subject: Conference call next Monday?

- > We haven't talked for awhile, could we set up a conference call
- > next
- > Monday to discuss what's new with Tor and discuss a bit of long-
- > term
- > planning?
- >
- > Ken, Hiu and I will be participating on this end, you can feel
- > free to
- > invite anyone else from your side that you'd like to be involved.
- >
- > We're flexible on times, any time except between 2-3pm should be
- > good,
- > so just let me know.
- >
- > -k
- >
- >

From: [Ken Berman](#)
To: [Roger Dingedine](#); [Sharon Hom](#)
Cc: [Terry Davies](#); [Shava Hered](#); [Hui Ho](#)
Subject: Re: Conference call next Monday?
Date: Thursday, November 09, 2006 7:41:07 AM

Roger - Sharon is the Executive Director of Human Rights in China, and a real supporter of tools needed to help the PRC citizens get unbiased news on all issues, but especially Human Rights. She has engaged some of the leading technology leaders in this area to help their program overcome extreme censorship. Tor would fit right in with her groups goals, especially since you are working with Nart and others who have also helped her.

Sharon - Hello! I wanted to introduce you to the founders of Tor, a network to allow anonymous web browsing, a program we are fully behind. Would you pass along this info to your IT person over there, and see if he/she feels it is worth pursuing?

thanks,
Ken

Roger Dingedine wrote:

>Here's a followup from the call: can you provide details about "Sharon
>Hom" in NYC? It's always good to meet new people, especially folks who'd
>be excited about our current directions.

>

>Thanks,

>--Roger

>

>

>

From: [Roger Dingleline](#)
To: [Kelly DeYoe](#)
Subject: Re: Contract status update
Date: Friday, March 31, 2006 2:53:19 AM

On Wed, Mar 22, 2006 at 06:18:14PM -0500, Kelly DeYoe wrote:
> Ok, so the latest update on the contract is that it is just awaiting the
> CFO's approval before it can go to the Contracts office for award..
> which sounds not much further along than it was 3 weeks ago I'm afraid.
> Unfortunately, the administrative person who is in charge of this from
> our office is out this week, so I was receiving the info secondhand from
> another admin. officer, so I will check with the primary contact again
> on Monday.

Any progress here?

I'm going to want a check at some point in the not-too-distant future. :)

Thanks,
--Roger

From: [Kelly DeYoe](#)
To: [Roger Dingledine](#)
Subject: Re: Contract status update
Date: Wednesday, March 22, 2006 7:18:14 PM

Ok, so the latest update on the contract is that it is just awaiting the CFO's approval before it can go to the Contracts office for award... which sounds not much further along than it was 3 weeks ago I'm afraid.

Unfortunately, the administrative person who is in charge of this from our office is out this week, so I was receiving the info secondhand from another admin. officer, so I will check with the primary contact again on Monday.

-k

Roger Dingledine wrote:

> On Tue, Mar 21, 2006 at 10:35:09AM -0500, Kelly DeYoe wrote:

>

>>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.

>

>

> Sounds good.

>

>

>>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.

>

>

> Ok.

>

> --Roger

>

From: [Roger Dingleline](#)
To: [Kelly DeYoe](#)
Subject: Re: Contract status update
Date: Tuesday, March 21, 2006 10:45:30 PM

On Tue, Mar 21, 2006 at 10:35:09AM -0500, Kelly DeYoe wrote:
> 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.

Sounds good.

> 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.

Ok.

--Roger

From: [Bennett Haselton](#)
To: [Simson's Treo 650](#); [Ken Berman](#); [REDACTED]; [Kelly DeVoe](#); [REDACTED]; [roger.dinaledine](#)
Subject: Re: are there any character sequences that identify TOR traffic?
Date: Thursday, December 15, 2005 8:06:09 PM

Actually the Circumventor was only designed to be the optimal solution under some very pessimistic assumptions (namely, that your adversary will be able to reverse-engineer the algorithm completely and look for a way to beat it). I thought this was reasonable, since if the Chinese have spent tens of millions of dollars on their censorship system, wouldn't they pay a consultant \$100,000 to find a way to block a circumvention scheme? The mistake I made was in not knowing that most Chinese simply don't care about circumvention; the government is just trying to stop casual users from reaching these sites. So the optimal system might be the one that works the best when the Chinese aren't trying to block it.

It's a cliché that there is no "best" solution, but I believe it is possible to break up the different sets of assumptions that characterize the different problems we're trying to solve, and find the "best" solution under each of those sets of assumptions. For example:

- You could assume the Chinese won't try to fight the system at all. Under that assumption, TOR is best, since you don't have to make contact with someone outside China to install a TOR node for you that you can connect to -- all you need to do is connect to the directory server.
- You could assume the Chinese might try to fight it by adding IPs to their firewall or adding new strings to their banned-string list -- since they already have the architecture in place to do this -- but they're not going to develop any new kinds of countermeasures. In this case, TOR might still be best, since after the directory servers are blocked, the TOR client can fail over to the other nodes it already knows about. Assuming that TOR traffic doesn't contain headers that would identify it uniquely.
- You could assume the Chinese WILL try to fight it and they WILL go to the trouble of paying someone to come up with new kinds of countermeasures. Here, the current implementation of TOR has a weakness in that, as Roger described it, many TOR nodes mirror the directory. That means a determined Chinese censor could install a node, mirror the directory, and block all the IPs in that directory, severing all connections between Chinese nodes and "free world" nodes.

Or you could make subtle changes to these conditions that have big implications for the "best" solution -- for example, assume that AT FIRST the Chinese won't care about blocking it, but at some point they will wake up and they will care, and then they'll spend a lot of effort cracking down. The solution in this case might be to use a TOR directory server to link up Chinese nodes with free-world nodes, but prevent any one node from having a mirror of the entire directory. Then as long as the Chinese censors aren't paying attention, people can bootstrap easily by using the directory server to link up. But when the Chinese crack down, they can block the TOR directory server, but there's no way for them to get a directory of all the nodes already out there that are talking to each other, so those connections will stay live.

My theory is that because most Chinese people don't care enough about getting around the firewall, if you want to make real inroads into Chinese culture and change how people think, you have to come up with a "killer

app" that lots of Chinese people will want to use for other reasons, and make circumvention a built-in feature. That brings in another set of problem assumptions that also changes the nature of what would be the "best" solution.

-Bennett

At 06:03 PM 12/15/2005 -0500, Simson's Treo 650 wrote:

>Sounds like there are a lot of good Circumventer ideas to be adopted in a
>possibly merged system. Do you have a paper that describes the issues and
>your design decisions?

>___

>Sent with SnapperMail from my Treo 650.

>Please excuse any typos.

>www.snappermail.com

>

>..... Original Message

>On Thu, 15 Dec 2005 13:25:39 -0800 "Bennett Haselton"

><(b) (6)> wrote:

>>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

>>

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

>>(b) (6)

>>

From: Simson's Treo 650
To: Bennett Haselton; Ken Berman; (b) (6); Kelly DeYoe; (b) (6); roger.dingledine
Subject: Re: are there any character sequences that identify TOR traffic?
Date: Thursday, December 15, 2005 6:03:07 PM

Sounds like there are a lot of good Circumventer ideas to be adopted in a possibly merged system. Do you have a paper that describes the issues and your design decisions?

Sent with SnapperMail from my Treo 650.
Please excuse any typos.
www.snappermail.com

..... Original Message

On Thu, 15 Dec 2005 13:25:39 -0800 "Bennett Haselton"

<(b) (6)> wrote:

>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 Circumventer 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
>Circumventer traffic from any other type of HTTPS traffic.
>
> -Bennett
>
>
>(b) (6) <http://www.peacefire.org>
>(b) (6)
>

From: [Bennett Haselton](#)
To: [Simson L. Garfinkel](#); [Ken Berman](#); (b) (6); [Kelly DeYoe](#); (b) (6); [roger dingedline](#)
Subject: Re: are there any character sequences that identify TOR traffic?
Date: Friday, December 16, 2005 5:33:24 PM

At 10:15 PM 12/15/2005 -0500, Simson L. Garfinkel wrote:

>Two comments on what you wrote, Bennett:

>

>1. I think that the Chinese attack on Tor that you describe won't actually
>work, because I believe that the directory needs to be digitally signed.
>Roger?

Digitally signing just prevents the contents from being *altered*, but doesn't prevent the contents from being read. If you're a (secretly hostile) mirror node and you get a mirror of all the nodes in the directory server, then once you know all those node IP addresses, you can block them all on the Chinese firewall.

>2. If what you really need is a "killer app," then it sounds like you want
>to give the Chinese a new web browser that has built-in anti-censorship
>technology. This sounds like a Firefox plug-in that's a default for the
>"all china release."

I'm concerned that if any major browser tries to make this an option included by default, they'll just find their site blocked by the Chinese censors until they take it out. The killer app would have to be something offered separately.

While the Net is certainly saturated with would-be "killer apps", not all of them have a slick interface written specifically in Chinese, so it may be easier to write a killer app for China than to write a killer app for the English-speaking world.

It wouldn't have to be limited to Web browsers, plug-ins, or similar applications. There are two approaches you could take here:

- The 'killer app' works like a network-on-top-of-the-network (for whatever reason that is relevant to the program's alleged purpose), and people only gradually discover that as a side effect, it can be used to circumvent the firewall. This limits the types of applications that could be used.
- The 'killer app' is something completely unrelated, used frankly as a way to sneak the circumvention client onto many Chinese machines, and only later we reveal that it can be used to circumvent the firewall.

But Roger's right that this would be a major undertaking and we should probably look for simpler solutions first!

>----- Original Message ----- From: "Bennett Haselton"

><(b) (6)>

>To: "Simson's Treo 650" <(b) (6)> "ken berman"

><(b) (6)> <(b) (6)> <(b) (6)> <(b) (6)>

>"roger dingedline" <(b) (6)>

>Sent: Thursday, December 15, 2005 8:06 PM

>Subject: Re: are there any character sequences that identify TOR traffic?

>

>

>>Actually the Circumventor was only designed to be the optimal solution
>>under some very pessimistic assumptions (namely, that your adversary will
>>be able to reverse-engineer the algorithm completely and look for a way

>>to beat it). I thought this was reasonable, since if the Chinese have
>>spent tens of millions of dollars on their censorship system, wouldn't
>>they pay a consultant \$100,000 to find a way to block a circumvention
>>scheme? The mistake I made was in not knowing that most Chinese simply
>>don't care about circumvention; the government is just trying to stop
>>casual users from reaching these sites. So the optimal system might be
>>the one that works the best when the Chinese aren't trying to block it.

>>

>>It's a cliché that there is no "best" solution, but I believe it is
>>possible to break up the different sets of assumptions that characterize
>>the different problems we're trying to solve, and find the "best"
>>solution under each of those sets of assumptions. For example:

>>

>>- You could assume the Chinese won't try to fight the system at all.
>>Under that assumption, TOR is best, since you don't have to make contact
>>with someone outside China to install a TOR node for you that you can
>>connect to -- all you need to do is connect to the directory server.

>>

>>- You could assume the Chinese might try to fight it by adding IPs to
>>their firewall or adding new strings to their banned-string list -- since
>>they already have the architecture in place to do this -- but they're not
>>going to develop any new kinds of countermeasures. In this case, TOR
>>might still be best, since after the directory servers are blocked, the
>>TOR client can fail over to the other nodes it already knows about.
>>Assuming that TOR traffic doesn't contain headers that would identify it
>>uniquely.

>>

>>- You could assume the Chinese WILL try to fight it and they WILL go to
>>the trouble of paying someone to come up with new kinds of
>>countermeasures. Here, the current implementation of TOR has a weakness
>>in that, as Roger described it, many TOR nodes mirror the
>>directory. That means a determined Chinese censor could install a node,
>>mirror the directory, and block all the IPs in that directory, severing
>>all connections between Chinese nodes and "free world" nodes.

>>

>>Or you could make subtle changes to these conditions that have big
>>implications for the "best" solution -- for example, assume that AT FIRST
>>the Chinese won't care about blocking it, but at some point they will
>>wake up and they will care, and then they'll spend a lot of effort
>>cracking down. The solution in this case might be to use a TOR directory
>>server to link up Chinese nodes with free-world nodes, but prevent any
>>one node from having a mirror of the entire directory. Then as long as
>>the Chinese censors aren't paying attention, people can bootstrap easily
>>by using the directory server to link up. But when the Chinese crack
>>down, they can block the TOR directory server, but there's no way for
>>them to get a directory of all the nodes already out there that are
>>talking to each other, so those connections will stay live.

>>

>>My theory is that because most Chinese people don't care enough about
>>getting around the firewall, if you want to make real inroads into
>>Chinese culture and change how people think, you have to come up with a
>>"killer app" that lots of Chinese people will want to use for other
>>reasons, and make circumvention a built-in feature. That brings in
>>another set of problem assumptions that also changes the nature of what
>>would be the "best" solution.

>>

>> -Bennett

>>

>>At 06:03 PM 12/15/2005 -0500, Simson's Treo 650 wrote:

>>>Sounds like there are a lot of good Circumventer ideas to be adopted in

>>>a
>>>possibly merged system. Do you have a paper that describes the issues
>>>and
>>>your design decisions?
>>>____
>>>Sent with SnapperMail from my Treo 650.
>>>Please excuse any typos.
>>>www.snappermail.com
>>>
>>>..... Original Message

>>>On Thu, 15 Dec 2005 13:25:39 -0800 "Bennett Haselton"
>>><[REDACTED]> wrote:
>>> >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>
>>> > (b) (6)
>>> >
>>
>

From: [Andrew Lewman](#)
To: [Ken Berman](#)
Cc: [Roger Dingleline](#); [Kelly DeYoe](#); [Sho Ho](#)
Subject: Re: Attached: Mod to Extend PoP thru Oct 17, 2011
Date: Wednesday, April 20, 2011 11:57:53 AM

On Wed, 20 Apr 2011 06:58:46 -0400
Ken Berman <[\(b\) \(3\)](#)> wrote:

> Hello Tor: sign your new contract!!

It's signed.

Thanks!

--

Andrew
pgp 0x74ED336B

From: [Jill Moss](#)
To: "[Andrew Lewman](#)"; [Ken Berman](#); [Kelly DeYoe](#); "[Roger Dingleline](#)"; [Sho Ho](#)
Subject: RE: August 2011 BBG/Tor Report
Date: Thursday, September 15, 2011 11:19:36 AM

Thanks for sending Andrew. JILL

-----Original Message-----

From: Andrew Lewman [<mailto:> (b) (6)]
Sent: Thursday, September 15, 2011 9:50 AM
To: Ken Berman; Kelly DeYoe; Roger Dingleline; Sho Ho; Jill Moss
Subject: August 2011 BBG/Tor Report

Hello Kelly, Ken, Kyle, Sho, and Jill,

Attached is the late August 2011 report. The release of a new stable tor branch dominates this report.

As always, if you have questions, feel free to ask. Thanks!

--

Andrew
pgp 0x74ED336B

From: [Ken Berman](#)
To: [Roger Dingledine](#)
Cc: [Kelly DeYoe](#)
Subject: Re: Basic bridgedb server is up
Date: Monday, December 17, 2007 10:48:00 AM

It works. I had to use my gmail account. IBB domain has changed to BBG domain - note our email addresses; we can still receive ibb.gov emails. Ken

Roger Dingledine wrote:

>Hi Kelly,
>
>Our prototype bridge address server is up.
>
>You can check it out at <https://bridges.torproject.org/>
>(and go there over Tor to see the answer possibly change -- there are
>four partitions of answers right now)
>
>Then send mail to [REDACTED] from an email address in
>the gmail.com, yahoo.com, or ibb.gov domain, with the line
>"get bridges" by itself in the message body,
>and you'll get an answer there too.
>
>There are many next steps, such as a) writing some text to go with the
>bridge lines it gives out, so ordinary people know what to do with them,
>b) writing text for Vidalia so people know to visit this url / send this
>email, and c) getting more or-talk people to operate bridges so we have
>more than 21 bridge addresses to work with.
>
>There are many later steps too, like a) doing more thorough reachability
>testing on the bridge addresses we give out so we give out fewer duds, b)
>having Vidalia make an automated attempt at the above, and c) making it
>harder for attackers to make slight modifications in their email address
>to get a new set of answers.
>
>We should probably get a "real" cert for bridges.torproject.org at some
>point too.
>
>Anyway, try it out. :) We'll be cleaning up the rough edges over the
>next days/weeks.
>
>--Roger
>
>
>

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#)
Cc: [Roger Dingleline](#); [Sho Ho](#)
Subject: Re: BBG / Tor Solutions Call
Date: Wednesday, October 03, 2012 3:06:05 PM

On Mon, 1 Oct 2012 21:20:04 +0000
Kelly DeYoe <[\(b\) \(6\)](#)> wrote:

> Please call in to:
>
> + [\(b\) \(6\)](#)
> conference code: [\(b\) \(6\)](#)

It fails for me. I enter the conf code and it tells me the keycode has been cancelled and hangs up.

[\(b\) \(6\)](#) is me.

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

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#)
Cc: [Roger Dingleline](#); [Sho Ho](#)
Subject: Re: BBG / Tor Solutions Call
Date: Wednesday, October 03, 2012 3:06:05 PM

On Mon, 1 Oct 2012 21:20:04 +0000
Kelly DeYoe <[\(b\) \(6\)](#)> wrote:

> Please call in to:
>
> + [\(b\) \(6\)](#)
> conference code: [\(b\) \(6\)](#)

It fails for me. I enter the conf code and it tells me the keycode has been cancelled and hangs up.

[\(b\) \(6\)](#) is me.

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

From: [Ken Berman](#)
To: [Andrew Lewman](#)
Cc: [Kelly DeYoe](#); [Roger Dingleline](#); [Karen Reilly](#)
Subject: RE: BBG and Tor
Date: Thursday, March 11, 2010 8:41:49 AM

In the AM is perfect. Ken

-----Original Message-----

From: Andrew Lewman [mailto:[\(b\) \(6\)](#)]
Sent: Wednesday, March 10, 2010 10:30 AM
To: Ken Berman
Cc: Kelly DeYoe; Roger Dingleline; Karen Reilly
Subject: Re: BBG and Tor

On Tue, 9 Mar 2010 13:19:28 -0500, Ken Berman <[\(b\) \(6\)](#)> wrote:

:Sure, let us know when you will be in town. Ken

How about April 7th?

--

Andrew Lewman
The Tor Project
pgp 0x31B0974B
[\(b\) \(6\)](#)

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

From: [Andrew Lewman](#)
To: [Ken Berman](#)
Cc: [Kelly DeYoe](#); [Roger Dingledine](#); [Karen Reilly](#)
Subject: Re: BBG and Tor
Date: Wednesday, March 10, 2010 10:29:32 AM

On Tue, 9 Mar 2010 13:19:28 -0500, Ken Berman <[\(b\) \(6\)](#)> wrote:

:Sure, let us know when you will be in town. Ken

How about April 7th?

--

Andrew Lewman
The Tor Project
pgp 0x31B0974B
[\(b\) \(6\)](#)

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

From: Ken Berman
To: Andrew Lewman
Cc: Kelly DeYoe; Roger Dingledine; Karen Reilly
Subject: RE: BBG and Tor
Date: Thursday, March 11, 2010 8:41:49 AM

In the AM is perfect. Ken

-----Original Message-----

From: Andrew Lewman [mailto:(b) (6)]
Sent: Wednesday, March 10, 2010 10:30 AM
To: Ken Berman
Cc: Kelly DeYoe; Roger Dingledine; Karen Reilly
Subject: Re: BBG and Tor

On Tue, 9 Mar 2010 13:19:28 -0500, Ken Berman <(b) (6)> wrote:

:Sure, let us know when you will be in town. Ken

How about April 7th?

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

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

From: [Andrew Lewman](#)
To: [Ken Berman](#)
Cc: [Kelly DeYoe](#); [Roger Dingledine](#); [Karen Reilly](#)
Subject: Re: BBG and Tor
Date: Wednesday, March 10, 2010 10:29:32 AM

On Tue, 9 Mar 2010 13:19:28 -0500, Ken Berman <[\(b\) \(6\)](#)> wrote:

:Sure, let us know when you will be in town. Ken

How about April 7th?

--

Andrew Lewman
The Tor Project
pgp 0x31B0974B
[\(b\) \(6\)](#)

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

From: [Ken Berman](#)
To: [Andrew Lewman](#); [Kelly DeYoe](#); [Roger Dingledine](#); [Karen Reilly](#)
Subject: RE: BBG and Tor
Date: Tuesday, March 09, 2010 1:19:28 PM

Sure, let us know when you will be in town. Ken

-----Original Message-----

From: Andrew Lewman [<mailto:> (b) (6)]
Sent: Tuesday, March 09, 2010 11:29 AM
To: Ken Berman; Kelly DeYoe; Roger Dingledine; Karen Reilly
Subject: BBG and Tor

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
(b) (6)

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

From: Ken Berman
To: Andrew Lewman; Kelly DeYoe; Roger Dingleline; Karen Reilly
Subject: RE: BBG and Tor
Date: Tuesday, March 09, 2010 1:19:28 PM

Sure, let us know when you will be in town. Ken

-----Original Message-----

From: Andrew Lewman [mailto: (b) (6)]
Sent: Tuesday, March 09, 2010 11:29 AM
To: Ken Berman; Kelly DeYoe; Roger Dingleline; Karen Reilly
Subject: BBG and Tor

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
(b) (6)

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

From: [Andrew Lewman](#)
To: [Ken Berman](#)
Cc: [Kelly DeYoe](#); [Roger Dingleline](#); [Karen Reilly](#)
Subject: Re: BBG and Tor
Date: Friday, March 12, 2010 3:04:23 PM

On Thu, 11 Mar 2010 08:41:49 -0500, Ken Berman <[\(b\) \(6\)](#)> wrote:

:In the AM is perfect. Ken

Great. What time do you prefer?

--

Andrew Lewman
The Tor Project
pgp 0x31B0974B
[\(b\) \(6\)](#)

Website: <https://www.torproject.org/>

Blog: <https://blog.torproject.org/>

Identi.ca: torproject

From: Ken Berman
To: Andrew Lewman
Cc: Kelly DeYoe; Roger Dingledine; Karen Reilly; Sho Ho
Subject: RE: BBG and Tor
Date: Monday, March 15, 2010 9:48:35 AM

10:00.....

-----Original Message-----

From: Andrew Lewman [mailto:(b) (6)]
Sent: Friday, March 12, 2010 3:04 PM
To: Ken Berman
Cc: Kelly DeYoe; Roger Dingledine; Karen Reilly
Subject: Re: BBG and Tor

On Thu, 11 Mar 2010 08:41:49 -0500, Ken Berman <(b) (6)> wrote:

:In the AM is perfect. Ken

Great. What time do you prefer?

--

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

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

From: Kelly DeYoe
To: Andrew Lewman; Marcia Jones
Cc: [REDACTED] (b) (6)
Subject: RE: BBG TSC invoice
Date: Wednesday, October 03, 2012 5:24:41 PM

Thanks Andrew, I have approved the invoice for payment, and also have Marcia checking into the status of the previous 2 payments as well.

-k

From: Andrew Lewman [REDACTED] (b) (6)
Sent: Tuesday, October 02, 2012 3:17 PM
To: Kelly DeYoe; Marcia Jones
Cc: [REDACTED] (b) (6)
Subject: BBG TSC invoice

Hello Kelly and Marcia,

Please find attached our invoice for work performed in August-September. Thanks.

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: Roger Dingleline
To: Kelly DeYoe
Cc: Ken Bernick; [REDACTED]
Subject: Re: Call on Friday at 1:30?
Date: Wednesday, March 25, 2009 9:33:31 AM

On Tue, Mar 24, 2009 at 06:00:26PM -0400, Kelly DeYoe wrote:
> Roger, you indicated Friday would be a good day for us to have a
> conference call to discuss the renewal for the next year. Ken suggested
> 1:30pm EDT, does that work for you?

Perfect.

(It also works for Andrew.)

Thanks,
--Roger

From: Kelly DeYoe
To: Roger Dingledine
Cc: Ken Burman; [REDACTED]
Subject: Re: Call on Friday at 1:30?
Date: Wednesday, March 25, 2009 10:44:52 AM

Great, 1:30pm EDT this Friday 3/27 it is then.

-k

Roger Dingledine wrote:

> On Tue, Mar 24, 2009 at 06:00:26PM -0400, Kelly DeYoe wrote:
>> Roger, you indicated Friday would be a good day for us to have a
>> conference call to discuss the renewal for the next year. Ken suggested
>> 1:30pm EDT, does that work for you?
>
> Perfect.
>
> (It also works for Andrew.)
>
> Thanks,
> --Roger
>

From: [Roger Dingleline](#)
To: [Toy, Debbie](#)
Cc: [Ken Berman](#); [Kelly DeYoe](#)
Subject: Re: CENTRA conference - Esoteric Use of the Internet
Date: Tuesday, August 22, 2006 6:02:21 PM

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: [Toy, Debbie](#)
To: [Ken Berman](#); [Roger Dingledine](#)
Cc: [Kelly DeYoe](#)
Subject: RE: CENTRA conference - Esoteric Use of the Internet
Date: Wednesday, August 23, 2006 10:17:40 AM

Hello Ken,

I have passed your name over to the sponsoring office, and once I hear back from them on space and other restrictions I will let you know. Coincidentally, I have been following stories on censorship and Circumventor in China – I would love to hear what unclass stuff you and Kelly may have been working on in this area if any. It's always curious to watch the "race" that goes on between blocking and finding holes around it.

Debbie

From: Ken Berman [mailto:[\(b\) \(6\)](#)]
Sent: Wednesday, August 23, 2006 7:37 AM
To: Roger Dingledine
Cc: Toy, Debbie; Kelly DeYoe
Subject: Re: CENTRA conference - Esoteric Use of the Internet

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: [Hiu Ho](#)
To: [Roger Dingledine](#)
Cc: [Kelly DeYoe](#); [Ken Berman](#); [Bennett Haselton](#); [Betty Pruitt](#)
Subject: Re: Choosing your Tor exit node
Date: Wednesday, August 02, 2006 5:37:41 PM

Thanks!

-Hiu

Roger Dingledine wrote:

>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
>
>
>

From: [Shirley Hao](#)
To: [Sharon Hom](#); [Ken Berman](#); [Roger Dingledine](#)
Cc: [Kelly DeYoe](#); [Shava Nerad](#); [Hiu Ho](#)
Subject: RE: Conference call next Monday?
Date: Friday, November 17, 2006 3:58:21 PM

Hello Ken,

Many apologies for the late reply! We have too many projects going on at once...

Roger, Shava,

It's a pleasure to get in touch with you both! We've been familiar with Tor for quite a while, but have not yet had the opportunity yet to explore it in more detail.

I'm not sure how much Ken has spoken to you about HRIC. Perhaps the aspect of our work that is most relevant here is our E-Activism Project, an on-the-ground, three-year-old project focused on providing Internet users in China with open access to information. Content and technology both feature equally as prominent in the project.

One of our recent pushes in the project has been to build a resource center of accessible toolkits, multimedia resources, etc.--including methods of Internet censorship circumvention. It would be great to hear more about Tor and how we might be able to integrate/help develop information on it to reach a wider audience within China.

I hope we'll be able to talk more (e-mail/phone/in person) on this. I'll be out of the office through the end of the November, but would be happy to send a follow-up email and more information after I return...

Best,

shirley

-----Original Message-----

From: Sharon Hom
Sent: Thursday, November 09, 2006 10:32 PM
To: Ken Berman; Roger Dingledine; Shirley Hao
Cc: Kelly DeYoe; Shava Nerad; Hiu Ho
Subject: RE: Conference call next Monday?

Hi Ken,

Thanks for the introduction! I am cc'ing Shirley to get her thoughts.

Best,
Sharon

-----Original Message-----

From: [Roger Dingleline](#)
To: [Kelly DeYoe](#)
Cc: [Shava Nerad](#); [Ken Berman](#); [Hiu Ho](#)
Subject: Re: Conference call next Monday?
Date: Monday, November 06, 2006 6:33:30 PM

Here's a followup from the call: can you provide details about "Sharon Hom" in NYC? It's always good to meet new people, especially folks who'd be excited about our current directions.

Thanks,
--Roger

From: Sharon Hom
To: Ken Berman; Roger Dingledine; Shirley Hao
Cc: Kelly DeYoe; Shava Nerad; Hiu Ho
Subject: RE: Conference call next Monday?
Date: Thursday, November 09, 2006 10:31:57 PM

Hi Ken,

Thanks for the introduction! I am cc'ing Shirley to get her thoughts.

Best,
Sharon

-----Original Message-----

From: Ken Berman [mailto:██████████ (b) (6)]
Sent: Thursday, November 09, 2006 7:41 AM
To: Roger Dingledine; Sharon Hom
Cc: Kelly DeYoe; Shava Nerad; Hiu Ho
Subject: Re: Conference call next Monday?

Roger - Sharon is the Executive Director of Human Rights in China, and a real supporter of tools needed to help the PRC citizens get unbiased news on all issues, but especially Human Rights. She has engaged some of the leading technology leaders in this area to help their program overcome extreme censorship. Tor would fit right in with her groups goals, especially since you are working with Nart and others who have also helped her.

Sharon - Hello! I wanted to introduce you to the founders of Tor, a network to allow anonymous web browsing, a program we are fully behind. Would you pass along this info to your IT person over there, and see if he/she feels it is worth pursuing?

thanks,
Ken

Roger Dingledine wrote:

>Here's a followup from the call: can you provide details about "Sharon
>Hom" in NYC? It's always good to meet new people, especially folks
who'd
>be excited about our current directions.
>
>Thanks,
>--Roger
>
>
>

From: [Roger Dingleline](#)
To: [Kelly DeYoe](#)
Cc: [Shava Nerad](#); [Ken Berman](#); [Hiu Ho](#)
Subject: Re: Conference call next Monday?
Date: Monday, November 06, 2006 11:46:03 AM

On Mon, Nov 06, 2006 at 10:54:32AM -0500, Kelly DeYoe wrote:
> Roger, glad to hear you're back and available. 4pm is good for Ken, Hiu
> and me.
>
> We'll be using a free voice conference bridge for the call, so please
> join the bridge at 4pm EST at:
>
> Phone Number: (b) (6)
> Access code: (b) (6)

Great. Talk to you in a few hours, then.

--Roger

From: Roger Dingledine
To: Kelly DeYoe
Cc: Shava Nerad
Subject: Re: Conference call next Monday?
Date: Saturday, November 04, 2006 2:17:52 AM

On Fri, Nov 03, 2006 at 06:42:46AM -0500, [REDACTED] wrote:
> Roger, haven't heard anything back from you about your availability
> for a conference call this coming Monday 11/6. I've been in class all
> day the past 2 days, and will be again today, so haven't been able to
> follow up with a telephone call.

Hi Kelly,

Sorry for the silence on this end -- I've been travelling, and for the past few days have been out of the country so telephone wouldn't have been very workable either. :)

> If you could confirm a time by email, or let me know that you're not
> available on Monday, as soon as possible, it would be appreciated.

I'd be happy to do Monday at 4pm. Or if that doesn't work, anytime after-noon Tuesday works for me too. Or after-noon Wed, or Thurs, or Fri, if it comes to that. :)

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>

> > Ken, Hiu and I will be participating on this end, you can feel
> > free to
> > invite anyone else from your side that you'd like to be involved.

From: (b) (6) on behalf of (b) (6)
To: [Discussion of privacy enhancing technologies](#)
Subject: Re: [PET] Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising
Date: Monday, November 14, 2011 11:35:54 PM

On Tue, Nov 08, 2011 at 08:06:00PM +0000, (b) (6) wrote 3.6K bytes in 48 lines about:
: Do you think OBA is a hindrance to technology or is it becomes a norm nowadays. If not, how website will make profits. IMHO, to should be better way of handling this from the user perspectives.

These are my thoughts. OBA isn't good enough to freak people out yet. A normal person doesn't see the aggregate data collection behind the scenes. Conversely, the ads aren't targeted enough to be useful and creepy at once. Facebook has made some progress in co-opting friends' images for ads, but even so, not generally creepy enough.

The general populace may not understand until ads/spam become targeted in near real time. Such as,

"Hello Mr. Jones,
Would you like to learn how Preparation H is better than the generic cream you bought at your local Duane Reade on 32nd street today? click here to learn more and save 10% off your next purchase."

Once an ad company figures out how to let you see all of the data they've collected about you, in order to better serve you ads, then people may realize what is going on. Amazon lets me see everything I've given them through my profile and purchases, but not what they've collected and collated about me overall. How this larger set of data feeds into the ad and recommendation networks is what I'm interested in learning. I sometimes see some very odd recommendations. This makes me wonder if it is Amazon experimenting or my data is crossed/corrupted in some way.

I'm making an assumption that the OBA from Amazon is based on what they know and what they infer about me.

--

Andrew
pgp key: 0x74ED336B

PET mailing list

(b) (6)
<http://lists.links.org/mailman/listinfo/pet>

From: Roger Dingledine
To: Simson Garfinkel
Cc: [REDACTED], Kelly DeYoe: [REDACTED] (b) [REDACTED] (b)
Subject: Re: "Help China"
Date: Friday, December 16, 2005 8:39:17 AM

On Thu, Dec 15, 2005 at 09:04:55AM -0500, Simson Garfinkel wrote:
> ** If TOR does have a "Help China" button, you are going to need some
> way of authenticating a proxy that is legitimately helping China and
> one that is run by a Hostile Organization (OH) that is trying to hurt
> china.

Right. There are a number of different forms this attack could take:

- 1) snoops on the dissident's traffic, or selectively modifies the web pages he gets back.
- 2) convinces him he's connected to the real Tor network when in fact he is sending him into a fake Tor network.
- 3) claims to relay traffic but doesn't actually.
- 4) relays traffic beautifully but writes down the dissident's IP.

Tor deals with attack 1 because the connection is encrypted and integrity-checked between the dissident and the exit node, so while the relay knows the dissident's location, he can't know what he's asking for and can't modify the traffic. Tor also deals with attack 2 assuming the dissident got a real copy of Tor (and therefore has the keys that sign the Tor directories). Attack 3 can be solved by measuring whether the relay works, though we will still be vulnerable to selective denial of service ("it works for all the tests but never for dissidents in a certain province"). As far as we know, there is no solution to attack 4.

> You could just say that IP addresses outside of China are
> good, and those inside are bad, but I don't think that this will
> eventually scale. Instead, you're going to have a way for a proxy
> that claims to be helping china to prove that it is a good proxy.

By "good proxy", do you mean with respect to attack 3 above?

> One
> way to prove this might be its ability to relay a challenge back to
> one of the TOR directory servers. The TOR directory servers could
> evolve into some kind of certification authority.

Roughly speaking, that's the plan. Except there's no reason it needs to be the current network's directory servers. It could be a separate set of directory servers that manage discovery for the China users. Think of it as two overlapping Tor networks, where any node will relay traffic wherever it can, but the two different types of directory servers give you different views of the network. The first type is the simple one, that just tells you all the servers -- this works great if your local network isn't censored. The second type is the more complex one, that only reveals a small subset at a time -- this is one of the pieces that we would be developing for IBB.

> ** Now, if you can do this kind of real-time certification, all you
> need authorized TOR servers that are happy to respond to these real-
> time queries, and a conventional P2P discovery mechanism. You'll also
> need something client-side so you can re-use these connections...

For reasons that Bennett described earlier, I do not think a conventional P2P discovery mechanism will cut it here. We need an additional security feature that other P2P networks don't have: curious attackers should not be able to enumerate all the available relays.

> ** If you are concerned about client-side footprint, couldn't that be
> resolved with a Java or JavaScript implementation? Or even a Firefox
> plug-in? Do we know which browser people in China are using?

Writing network-based crypto apps in javascript is harder than it sounds. We hope to start looking more at that eventually, but it's definitely not something I would want to promise at this point.

> ** You were concerned about random port assignment. My concern is a
> China that blocks everything except port 80. You may very well want
> to solve this problem by having TOR use HTTP as a transport layer.

Tor uses HTTP for directory fetches, and HTTPS for its encrypted connections. If China blocks everything but 80 and 443 -- even if it enforces that we actually use those protocols -- we should still be ok. And if it blocks HTTPS, I expect that'll have serious economic impact on the country's Internet use.

--Roger

From: [Andrew Lewman](#)
To: [Ken Berman](#); [Roger Dingledine](#)
Cc: [Kelly DeYoe](#); [Sho Ho](#)
Subject: Re: <No Subject>
Date: Sunday, February 20, 2011 10:57:05 AM

Ken Berman <[\[REDACTED\]](#)> wrote:

>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 came out of
>the back of the room to talk to me.

>

>

>

>Ken

>

>

>

><http://freenetproject.org/index.html>

>

>

>

>

Freenet is a distributed, anonymous storage system. It has been around for a decade, has few users, and is typically used for research theories. It doesn't allow exit from their darknet to the open internet.

The freenet that is referenced in papers appears to be different than the Java coded freenet. I tried freenet last year to see what it did and didn't do. It seemed the darknet approach took days to discover other nodes from the public list of nodes. The private methods didn't work because I don't know anyone else running freenet services.

As comparison, Tor's hidden services are a more used and proven design where the papers and research are working on the same system.

Freenet does seem to be very cheap. They do have lots of developer churn other than the main guy, Ian. As their homepage states, the \$10k they have will last for 118 days.

I wouldn't focus on version, as parts of tor that have been around for years are still version 0.2. Software developers and marketing demands for version numbers are different beasts entirely.

--

Andrew



From: [Roger Dingoledine](#)
To: [Ken Berman](#)
Cc: [Kelly DeYoe](#); [Shava Nerad](#)
Subject: Re: 1:30>>2:00??
Date: Tuesday, October 16, 2007 4:48:04 PM

On Tue, Oct 16, 2007 at 01:26:41PM -0400, Ken Berman wrote:

>
> Can we move our call to 2:00?

Yes.

--Roger

From: Shava Nerad
To:  Roger Dingleline
Cc:  Shava Nerad
Subject: Re: 1:30>>2:00??
Date: Wednesday, October 17, 2007 4:51:04 AM

At 01:26 PM 10/16/2007, Ken Berman wrote:

>Can we move our call to 2:00?

I may be on public transit at 2pm, do you need me, Ken?

Thanks!

--
Shava Nerad


From: Roger Dingedine
To: Kelly DeYoe
Cc: Shava Nerad
Subject: Re: 2007 contract SOW draft
Date: Tuesday, January 23, 2007 2:48:49 AM

On Thu, Jan 18, 2007 at 11:36:37PM -0500, Roger Dingedine wrote:
> Here are some first thoughts. I'll get some more thorough thoughts
> to you on Monday, but we can start with these.

Hi Kelly,

I've looked it over in more detail. It looks good to me. It's a lot of work, but well, you're the largest funder for 2007, so that makes sense. Thanks for getting this rolling. A few more details below:

> >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 cannot
> > be identified Tor traffic and trivially blocked by government-
> > sponsored Internet censors.
>
> We should change this to 'so it is harder to identify'. Absolutes are
> tough, and in this case we're sure not to achieve the absolute. :)
>
> >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.
>
> How much of me are we thinking of allocating to managing these other
> people? We're already listing quite a few topics here, and I worry about
> stretching Nick and me farther. In the past we've demonstrated ability
> to either code or manage, but doing both at once hasn't worked well.
>
> (Alternatively, we are hoping to get some volunteer coordinators or other
> people to help out there, but I'm not sure we're ready to put that hope
> into a contract. Hm.)

We should talk a bit more about this one. What sort of IBB-based resources are we intending to have? Are we thinking this will be a major part of the contract and work, or a minor part? If we want this piece to work better than it did in 2006, we should give some thought to how to be more active in making that happen.

And lastly:

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.

Just as a side-note, we don't have any plans to tackle the high packet loss scenario in 2007. We need a few years more research on replacements for TLS, and hopefully other people will do a lot of that research for us. But yes, working better with low bandwidth is part of the plan.

Thanks!

--Roger

From: [Roger Dingledine](#)
To: [Kelly DeYoe](#)
Cc: [Shaya Nerad](#)
Subject: Re: 2007 contract SOW draft
Date: Thursday, January 18, 2007 11:36:37 PM

On Thu, Jan 18, 2007 at 04:45:23PM -0500, Kelly DeYoe wrote:
> Based on our discussions and review of your development roadmap and
> blocking resistance design, here's the statement of work I've come up
> with for our contract with you for 2007. Please review and let me know
> if you see any problem areas as soon as possible.

Hi Kelly,

Here are some first thoughts. I'll get some more thorough thoughts to you on Monday, but we can start with these.

>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 cannot
> be identified Tor traffic and trivially blocked by government-
> sponsored Internet censors.

We should change this to 'so it is harder to identify'. Absolutes are tough, and in this case we're sure not to achieve the absolute. :)

>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.

How much of me are we thinking of allocating to managing these other people? We're already listing quite a few topics here, and I worry about stretching Nick and me farther. In the past we've demonstrated ability to either code or manage, but doing both at once hasn't worked well.

(Alternatively, we are hoping to get some volunteer coordinators or other people to help out there, but I'm not sure we're ready to put that hope into a contract. Hm.)

Thanks!
--Roger

From: [Shava Nerad](#)
To: [Kelly DeYoe](#); [Roger Dingledine](#)
Subject: Re: 2007 contract SOW draft
Date: Thursday, January 18, 2007 5:09:25 PM

At 04:45 PM 1/18/2007, Kelly DeYoe wrote:

>Based on our discussions and review of your development roadmap and
>blocking resistance design, here's the statement of work I've come
>up with for our contract with you for 2007. Please review and let
>me know if you see any problem areas as soon as possible.
>
>Sorry for the delay in getting this to you.

Thanks, Kelly! Is this in the critical path of getting the contract composed? Roger's out of town, so I'd like to suss out how urgent this is.

Yrs,

--

Shava Nerad
Executive Director
The Tor Project
<http://tor.eff.org/>
<http://blogs.law.harvard.edu/anonymous/>

(b) (6)

(b) (6)

(b) (6) (cell)

skype: shava23

From: [Roger Dingleline](#)
To: [Kelly DeYoe](#)
Cc: [Shaya Nerad](#)
Subject: Re: 2007 contract SOW draft
Date: Tuesday, January 23, 2007 8:40:34 PM

On Tue, Jan 23, 2007 at 06:12:51PM -0500, Kelly DeYoe wrote:
> Here's the latest draft with changes made based on your comments and a
> few internal comments here.

Hi Kelly,

This looks great from my end.

Thanks!
--Roger

From: Roger Dingledine
To: Bennett Haselton
Cc: Ken Bermer; Hiu Ho; Kelly DeYoe; [REDACTED] [REDACTED]
Subject: Re: algorithm for TOR to use non-discoverable redundant nodes
Date: Monday, December 19, 2005 5:21:49 AM

Hi Bennett,

A couple of design comments for your design proposal:

On Tue, Dec 13, 2005 at 02:09:36PM -0800, Bennett Haselton wrote:

- > 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.

I remember from the phone conversation that we disagree about this part: one of the lessons we've learned from working on Tor is that if your system is not usable, then you will have no users, so it doesn't have much impact on anything. Requiring relay discovery to be manual is a good way to make sure the system never gets much use. (And it's manual in both directions -- how many oppressed Chinese people has the typical Tor user in Indiana met?)

So I think it is particularly important that relay discovery in particular be made modular. We should certainly support manual relay discovery, and if our attacker is incredibly good, we'll end up falling back on that. But in the mean time, some automated mechanism would really help to bootstrap the system into seeing more use.

But as you say, the particular design you're talking about here doesn't care how relay discovery is done.

[snip]

- > 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'.

Rather than putting more smarts into the relays, I think the right thing to do here is to put more smarts into the "network manager" -- the central location that keeps sorts and keeps track of the volunteers.

Then the dissident can just use the volunteer relays as relays, to get to

the end web site that keeps track of which relays he is supposed to know about, and gives him new server descriptors for those -- possibly with changes in IP address, keys, exit policy, and so on. (Don't be fooled by the fact that I call it a web site. All of the interactions will still be automated and done in the background. I think the Tim O'Reilly crowd calls this "web services".)

This way the Tor network can keep on being just for communication, and we can add features on the edges.

Other than these two notes, I think this is a fine first plan.
--Roger

From: Andrew Lewman
To: Walid Al-Saqaf
Cc: [REDACTED]; Kelly DeYoe; Sho Ho
Subject: Re: alkasir.com
Date: Thursday, September 30, 2010 4:41:03 PM

On Thu, 30 Sep 2010 15:58:42 +0200

Walid Al-Saqaf <[REDACTED]> wrote:

> Thanks for bringing this up and for an interesting and fruitful chat
> yesterday. Indeed, I'd really love to hear more from Roger and
> Andrew's experience in such legal matters. So as to be clear, I did
> not yet get any lawsuit, but it is always good to have all
> precautions.

Hello Walid,

Nice to virtually meet you. Thanks for introducing us Ken. I spent some time researching alkasir. Here are my assumptions:

- 1) It seems you run a big server in Los Angeles that proxies traffic from users through it and on to their destination;
- 2) You filter content to allow mainly text through your proxy, avoiding lots of images, videos, audio overhead;
- 3) You record destination traffic for use on your world censorship map;
- 4) and finally, your binary and code are secret, as is your design, and everything is packed into a Windows executable of varying size.

Feel free to correct any mistakes.

If my assumptions are somewhat accurate, I can see a number of legal issues relating to data retention, source and destination security, and being labeled a content provider in LA.

We appear to have fundamentally different threat models, so I'm not sure how much our experience is relevant. Tor hasn't had many legal issues because our design is such that we have no way to record or modify traffic; our relays are run by volunteers and spread over 79 countries; and our code and design are published and peer-reviewed.

You may want to start with our published article on "Ten Things to Look for in a Circumvention Tool" to understand our position,
<https://www.torproject.org/press/2010-09-16-ten-things-circumvention-tools.html.en>

If you're interested, Roger and I will be in Stockholm soon. Roger is doing a public presentation on Oct 26th we can invite you to attend if you want to talk more.

I look forward to your thoughts.

--

Andrew
pgp 0x31B0974B

From: [Roger Dingledine](#)
To: [Walid Al-Sagaf](#)
Cc: [Andrew Lewman](#); [Ken Berman](#); [Kelly DeYoe](#); [Sho Ho](#); [Linus Nordberg](#)
Subject: Re: alkasir.com
Date: Friday, October 08, 2010 4:19:08 PM

On Thu, Sep 30, 2010 at 03:41:03PM -0400, Andrew Lewman wrote:
> If you're interested, Roger and I will be in Stockholm soon. Roger is
> doing a public presentation on Oct 26th we can invite you to attend if
> you want to talk more.

Here are the details for my talk:
<http://www.internetdagarna.se/program/seminarium/6>

You're welcome to drop by and learn more about what Tor is up to.

--Roger

From: [Andrew Lewman](#)
To: [Kelly DeYoe](#)
Subject: Re: Andrew in town May 2-3
Date: Thursday, May 02, 2013 10:33:33 AM

On Wed, 1 May 2013 21:19:35 +0000
Kelly DeYoe <[\(b\) \(6\)](#)> wrote:

> Hey Andrew, sorry to not get back to you sooner, but how about
> sometime on Friday afternoon? I have a meeting from 3:30 - 4:30, but
> could do before or after that.

How about 1:30 on Friday?

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: [Kelly DeYoe](#)
To: [Andrew Lewman](#)
Subject: RE: Andrew in town May 2-3
Date: Wednesday, May 01, 2013 5:19:35 PM

Hey Andrew, sorry to not get back to you sooner, but how about sometime on Friday afternoon? I have a meeting from 3:30 - 4:30, but could do before or after that.

-k

From: Andrew Lewman [REDACTED] (b) (6)
Sent: Sunday, April 28, 2013 12:14 PM
To: Kelly DeYoe
Subject: Andrew in town May 2-3

Hello Kelly,

It's been a while since we met. Are you up for a quick check-in either May 2nd or 3rd? I'll be in town both days and happy to meet up.

Thanks.

--

Andrew
<http://tpo.is/contact>
pgp 0x6B4D6475

From: Bennett Haselton
To: [REDACTED]; simson garfinkel; (b) (6); Kelly DeYoe; (b) (6)
Subject: re: anon services
Date: Wednesday, December 28, 2005 8:08:45 PM

As far as the Jan. 13 meeting, I won't be in the area, but I'm a big believer in one thing with regards to meetings, and that is: getting the non-interactive part out of the way (like static presentations) before the meeting starts, so that the meeting time is spent on things that make the best use of the synergy of people in the same room.

In discussing the China problem, it seems like we switch back and forth a lot between different sets of assumptions (they will or won't reverse-engineer the program to find how it works; they will or won't use a network sniffer to see what IPs it connects to and block those). I think the way to find a best solution is to formally divide up the different sets of assumptions, and then for each set of assumptions, find the best solution under that scenario (for example, what is the best solution if you assume that they *will* use a network sniffer to see what IPs the program connects to, but they won't actually disassemble the software to find out how it works?). Then see if you can combine them all into one uber-solution that is flexible enough to switch to each one of the "best-case scenarios" depending on what countermeasures the Chinese take.

The goal is to see if we can find one such uber-solution that works the best under each different set of assumptions. Then the discussion can be focused on finding flaws in that uber-solution or ways that it can be improved. Whenever we're talking about the best solution under a certain set of assumptions, but then we start to wonder out loud "but what if they can also do this...", what we're doing is switching to a different set of assumptions in an ad hoc way. I want to see if this can give more structure to our problem-solving approach.

To kick things off I've listed some of the possible sets of assumptions about what the Chinese might do, and then attempted to give a best-case solution to only one of them, the case where the Chinese censors *do* install a network monitor to see what IPs the client connects to (and block those), but it is assumed that they *don't* disassemble the software: <http://www.peacefire.org/foreign-url-check/chinese-circumvention-designs.html>
The answer is quite complicated. And whenever you change any of the initial assumptions, you have to start all over again! Although you can re-use parts of a previous solution.

I will try to fill out all the cases in the next couple of days. The goal is to have something to refer to whenever discussing the problem, so that as soon as you clarify what assumptions you're making about what countermeasures the Chinese might take, you can say "Oh, we're using the assumptions in this paragraph" and then look at the solution that's already listed, and see if you can find problems or improvements.

-Bennett

(b) (6)
[REDACTED]
(b) (6)

<http://www.peacefire.org>

From: Roger Dingleline
To: Ken Berman
Cc: [Simon Garfinkel](#); (b) (6); Kelly DeYoe; (b) (6); (b) (6)
Subject: Re: anon services
Date: Friday, December 23, 2005 4:07:30 AM

On Thu, Dec 22, 2005 at 09:49:56AM -0500, Ken Berman wrote:
> Roger - The 13th it is; 1:30 to 3:30 OK? Or would 9-11 be better?
> Your call. btw - I'm inviting the some tech savvy members from our
> Persian and Chinese language services.

Sounds good -- let's plan on 13:30 to 15:30 then.

Can you send some directions to help us find IBB? Will we be happier flying into Dulles or BWI? (At this point going into DCA is quite expensive.)

--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Simson Garfinkel; (b) (6); Kelly DeYoe; (b) (6); (b) (6)
Subject: Re: anon services
Date: Thursday, December 22, 2005 9:49:56 AM

Roger - The 13th it is; 1:30 to 3:30 OK? Or would 9-11 be better? Your call. btw - I'm inviting the some tech savvy members from our Persian and Chinese language services.

Ken

Roger Dingledine wrote:

On Wed, Dec 21, 2005 at 11:08:23AM -0500, Ken Berman wrote:

ooooops, the 16th is a Federal Holiday, MLK Jr. no will be here except the overnight staff.....

Oops indeed. Ok. :) How about Friday the 13th then? (An auspicious time.)

Would an hour or two be useful, just after noon, or should we plan more time than that?

--Roger

From: Roger Dingleline
To: Ken Berman
Cc: Simson Garfinkel; (b) (6) Kelly DeYoe; (b) (6) (b) (6)
Subject: Re: anon services
Date: Wednesday, December 21, 2005 2:16:24 PM

On Wed, Dec 21, 2005 at 11:08:23AM -0500, Ken Berman wrote:

> oooooops, the 16th is a Federal Holiday, MLK Jr. nbsp;
> Sorry.....no will be here except the overnight
> staff.....

Oops indeed. Ok. :) How about Friday the 13th then? (An auspicious time.)

Would an hour or two be useful, just after noon, or should we plan more time than that?

--Roger

From: [Ken Berman](#)
To: [Roger Dingledine](#)
Cc: [Simson Garfinkel](#); [REDACTED] [Kelly DeYoe](#); [REDACTED]
Subject: Re: anon services
Date: Wednesday, December 21, 2005 11:08:23 AM

ooooops, the 16th is a Federal Holiday, MLK Jr. Sorry.....no will be here except the overnight staff.....

Roger Dingledine wrote:

On Mon, Dec 19, 2005 at 07:44:15AM -0500, Ken Berman wrote:

Yes, let's get together, either date is OK. Also, Hiu and Kelly may be at the conference. Ken

Great. I'm going to mark January 16 for you, then. I'm also going to bring Nick. We'll be around for the whole day if needed. Should I plan to do a brief (or more in-depth) talk about Tor, so you and the other folks there can get up to speed?

I'll also contact Paul Syverson at NRL, the other designer of Tor, and see if he wants to drop by for part of the discussion.

And we can also schedule something to coincide with Simson later on in January, but one step at a time.

Thanks,
--Roger

From: Roger Dingleline
To: Simson Garfinkel; Ken Berman; (b) (5); Nelly Delyou; (b) (5); (b) (6)
Subject: Re: anon services
Date: Monday, December 19, 2005 5:27:21 AM

On Tue, Dec 13, 2005 at 09:18:42PM -0500, Simson Garfinkel wrote:
> I must concur that Tor seems to be further along than the Peacefire
> Circumventor system. I think that Tor also has a better articulated
> threat model and many years of analysis by people throughout the
> world. It's probably a better base to continue building upon.

Ken, others,

Would it be useful for me to drop by in person in mid January? It looks like I'm going to be in the area already for Shmoocon, so I could add a few more days on either side.

For example, I could drop by Jan 13 or Jan 16.

But I should decide this soon so I can figure out flights. :)

Thanks,
--Roger

From: Ken Berman
To: Roger Dingledine
Cc: Bennett Haselton; Simpson Gartinzel; Kelly DeYoe;
Subject: Re: anon services
Date: Thursday, December 15, 2005 7:34:40 AM

128

Roger Dingledine wrote:

On Tue, Dec 13, 2005 at 11:58:45PM -0800, Bennett Haselton wrote:

Actually I think both systems have their advantages. For the plan that we discussed on the phone, we should probably go forward with TOR, but there are other areas where the Circumventor is useful.

The disadvantages, where I think the Circumventor has an edge, are:

- If China decides to take action against TOR and block the directory servers, then my understanding is that the system stops working for many users, and new users who join the network will have to make contact with someone outside China that they can connect to (which is the same hurdle faced by the Circumventor now). With the Circumventor, we've told people from the beginning that they have to connect to somebody they know. There is no single action that the Chinese could take that would harm the Circumventor network.

Well, the key here is that at its heart, Tor is a protocol for talking in a secure way to another server, and making a secure tunnel through a series of other servers. Now, to do this you need a way to learn what the servers are that you can route through. Tor is built such that you can use whatever "discovery mechanism" you want. Right now we built a simple one with a small set of directory servers, because that was easy to build. If we want people inside China to be able to get to the Tor network, we will want a second alternate discovery mechanism for them, that works in a far less centralized way.

But you're right, one disadvantage with Tor is the perception that "the Tor network" is all one big protocol that's built in an inflexible way. People might be confused about having two possible discovery mechanisms -- "what do you mean there are two Tors?"

- The Circumventor requires no client-side software, in fact it doesn't even require you to change browser proxy settings; all

you need is a URL. This allows it to be used in cybercafes and other settings where you can't install client-side software or change your browser's settings.

As far as aspects like encryption and usability, the Circumventor leverages the encryption of the browser and the OpenSA Web server (and for usability, it's just a URL you paste into your browser), so I don't think those are big differences.

You're right, the designs we've been talking about for using Tor in China require the user to have some local software installed -- and that's a big hurdle compared to just using an ordinary web browser. (Do our users in China have 128 bit crypto in their browsers, or are they stuck at 40 bit?)

The Tor approach has its own variant of the software-less scenario: the relays would run as socks proxies, users inside China would somehow learn an outside IP address and port, and they'd configure their browser (or other applications) to use the socks proxy. But then we lose the automated fail-over advantage, and we also lose encryption.

Unfortunately when I went with the Circumventor design, I over-estimated the number of Chinese who would want to beat the firewall, and hence over-estimated the efforts that the Chinese would put into stopping it. It seems that the Chinese users don't care as much as we hoped they would, and as a result, the Chinese censors don't either! From the Chinese users' point of view, TOR is "perfect" (the problems with TOR are mostly hidden from the user) -- and yet there still aren't enough Chinese who care about beating the firewall, to make it worthwhile for the Chinese censors to take notice and block the directory servers. That's unfortunate, but it may make our job easier if our opponents aren't trying :)

Well, I think a lot of it is a question of usability at this point. We haven't translated any of our site into Chinese, and you need to click a bunch of things and install a bunch of things before you can get it working. I would guess with some targetted documentation and some cleaner installers, the user base in China would jump dramatically.

And there *is* a point where the authorities start to notice things. After all, I'm told they block web pages with the string 'freenet' in them, and I'm also told that for quite a while they blocked web pages with the string 'privoxy' in them. So perhaps they were trying to block

Tor
after all -- and a design requirement we hadn't realized for Tor
was to
have a name for our program that is a common word in many
languages. ;)

But you're right, in a sense we succeed by having a program that
is
not-entirely-trivial-to-use and because of this fact it is not
blocked by
the firewall. But I'd like to take the arms race a bit farther
than that.

--Roger

From: Roger Dingledine
To: Simson Garfinkel
Cc: Ken Berman; (b) (6); Kelly DeYoe; (b) (6); (b) (6)
Subject: Re: anon services
Date: Thursday, December 15, 2005 12:53:24 AM

On Tue, Dec 13, 2005 at 09:18:42PM -0500, Simson Garfinkel wrote:
> I must concur that Tor seems to be further along than the Peacefire
> Circumventor system. I think that Tor also has a better articulated
> threat model and many years of analysis by people throughout the
> world. It's probably a better base to continue building upon.
>
> Does the current Tor system give you a way for communicating with
> your base of people?

Not directly. I think the right way to reach them is to give them a slick interface for Tor (in the works already -- see [1] and [2]) that they want anyway, and this would be a feature that they can turn on. Once it's in front of them, then word of mouth plus maybe a little flag on their interface (we'll have to tune that part of course) will hopefully be enough.

I think the key is to make them want to run the program anyway, and to make turning on the 'help China' part not screw up their experience. Once we get it working smoothly, we might even be able to make it on by default.

--Roger

[1] <http://tor.eff.org/qui/>
[2] <http://freehaven.net/~edmanm/torcp/>

From: Roger Dingleline
To: Simson Garfinkel
Cc: Ken Berman; [REDACTED] Kelly DeYoe; [REDACTED] [REDACTED]
Subject: Re: anon services
Date: Tuesday, December 13, 2005 7:11:05 PM

[I've added Hiu, Kelly, and Nick to the cc list]

On Tue, Dec 13, 2005 at 12:52:05AM -0500, Roger Dingleline wrote:
> At 3pm on this Tuesday (in about 14 hours).

Hi Simson,

I got your voicemail, after the phone call. Sorry that we didn't try to hook you into the call later on. I hope next time works better.

In the call, we talked about some design goals and some options. We talked about Peacefire's "Circumventor" system, and how Tor improves over it:

- Tor has an established user base of 100k+ people we can leverage to run relays. I think we'll find it easier to find volunteers since they have their own incentive to run the software.
- Tor divides the role of "is willing to relay traffic from China" from the role of "is willing to connect to arbitrary websites".
- Tor is much farther along in terms of making good encrypted connections and tunnels, doing things in the background, usability, etc.

There are some hard problems which neither system has solved well, though. The biggest is the initial introduction problem. How does the user in China learn who to use at first? But we can separate that hard problem from a different hard problem, which is "given a few introduction points, how can we increase our robustness down the road?" Depending on the assumptions we want to make about social topologies inside China, there are some ok and some not-so-ok solutions.

So to take a step back, IBB does not have a solution in mind for step #3 of our "hard problems" list from <http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#China> so that would be a major part of what we would work on.

Two more observations:

- We don't need a perfect solution. This is going to be an arms race, and I bet there are going to be some steps that we expect to be easily censored that turn out to work better than we hoped.
- We have several resources in our favor. a) Lots of computers on the free side, and b) Lots of humans on the censored side. c) Others? Our solutions should try to take advantage of these.

We left it that Ken would sit down with the others and figure out where things should go next. Hopefully they will come back with further questions, and/or we'll have a discussion about what they want done, on what timeframe, for how much money, etc.

Fun stuff,
--Roger

From: Bennett Haselton
To: Ken Berman; Roger Dingledine; Simson Garfinkel; (b) (6); Kelly DeYoe; (b) (6)
Subject: re: anon services
Date: Wednesday, December 28, 2005 8:25:11 PM

At 05:08 PM 12/28/2005 -0800, ken berman , roger dingedine <(b) (6)>
simson garfinkel wrote:
>To kick things off I've listed some of the possible sets of assumptions
>about what the Chinese might do, and then attempted to give a best-case
>solution to only one of them, the case where the Chinese censors *do*
>install a network monitor to see what IPs the client connects to (and
>block those), but it is assumed that they *don't* disassemble the software:
><http://www.peacefire.org/foreign-url-check/chinese-circumvention-designs.html>

d'oh, I forgot to mention: to access that directory --
username: voa
password: 7947398453

The reason the ideas should not be widely distributed is that in some scenarios, we're assuming the Chinese won't reverse-engineer the software to figure out how it works. In order to gain an advantage from that assumption, obviously we'd have to keep certain workings of the software secret. (This is a departure from most security-oriented thinking, in which all details should be disclosed so that researchers can attack the algorithm, but in practice the Chinese don't seem to spend that much effort fighting circumvention systems.)

-Bennett

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

<http://www.peacefire.org>

From: [Simson Garfinkel](#)
To: [Roger Dingledine](#)
Cc: [Ken Berman](#); [REDACTED]; [Kelly DeYong](#); [REDACTED]; [REDACTED]
Subject: Re: anon services
Date: Friday, December 23, 2005 7:49:22 AM

DCA is your best choice. Failing DCA, go to BWI and take the train down. It's faster and easier than going to Dulles and taking in a shuttle or taxi. (I tried the Dulles thing recently and spent \$120 on taxis. I was shocked.) You can get a \$29 fare each way to BWI if you go on AirTran.

On Dec 23, 2005, at 4:07 AM, Roger Dingledine wrote:

> On Thu, Dec 22, 2005 at 09:49:56AM -0500, Ken Berman wrote:
>> Roger - The 13th it is; 1:30 to 3:30 OK? Or would 9-11
>> be better?
>> Your call. btw - I'm inviting the some tech savvy members
>> from our
>> Persian and Chinese language services.

>
> Sounds good -- let's plan on 13:30 to 15:30 then.
>
> Can you send some directions to help us find IBB? Will we be happier
> flying into Dulles or BWI? (At this point going into DCA is quite
> expensive.)
>
> --Roger
>

From: Roger Dingledine
To: Bennett Haselton
Cc: simson l. garfinkel; Ken Berman; (b) (6) Kelly DeYoe; (b) (6)
Subject: Re: are there any character sequences that identify TOR traffic?
Date: Friday, December 16, 2005 7:08:25 AM

On Thu, Dec 15, 2005 at 01:25:39PM -0800, Bennett Haselton wrote:
> Are there any headers that are sent back and forth at the beginning of a
> TOR connection, that would uniquely identify the traffic as TOR traffic?

Right now, we do an ordinary TLS connection for our handshake. This probably has some predictable strings in it. This should be pretty easy to fix, though, if we decide we want to.

> 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.

Right. And the step after this (if we need it) would be to re-use common HTTPS strings, because the response in the arms race for the censor is to look for certs with a lot of entropy in fields that don't normally have high entropy.

--Roger

From: Simson L. Garfinkel
To: Ken Berman; (b) (6); Kelly DeYoe; (b) (6); roger.dingledine; Bennett Haselton
Subject: Re: are there any character sequences that identify TOR traffic?
Date: Thursday, December 15, 2005 10:15:03 PM

Two comments on what you wrote, Bennett:

1. I think that the Chinese attack on Tor that you describe won't actually work, because I believe that the directory needs to be digitally signed. Roger?

2. If what you really need is a "killer app," then it sounds like you want to give the Chinese a new web browser that has built-in anti-censorship technology. This sounds like a Firefox plug-in that's a default for the "all china release."

----- Original Message -----

From: "Bennett Haselton" <(b) (6)>
To: "Simson's Treo 650" <(b) (6)>; "ken berman" <(b) (6)>; "roger dingedine" <(b) (6)>
Sent: Thursday, December 15, 2005 8:06 PM
Subject: Re: are there any character sequences that identify TOR traffic?

- > Actually the Circumventor was only designed to be the optimal solution
- > under some very pessimistic assumptions (namely, that your adversary will
- > be able to reverse-engineer the algorithm completely and look for a way to
- > beat it). I thought this was reasonable, since if the Chinese have spent
- > tens of millions of dollars on their censorship system, wouldn't they pay
- > a consultant \$100,000 to find a way to block a circumvention scheme? The
- > mistake I made was in not knowing that most Chinese simply don't care
- > about circumvention; the government is just trying to stop casual users
- > from reaching these sites. So the optimal system might be the one that
- > works the best when the Chinese aren't trying to block it.
- >
- > It's a cliché that there is no "best" solution, but I believe it is
- > possible to break up the different sets of assumptions that characterize
- > the different problems we're trying to solve, and find the "best" solution
- > under each of those sets of assumptions. For example:
- >
- > - You could assume the Chinese won't try to fight the system at all.
- > Under that assumption, TOR is best, since you don't have to make contact
- > with someone outside China to install a TOR node for you that you can
- > connect to -- all you need to do is connect to the directory server.
- >
- > - You could assume the Chinese might try to fight it by adding IPs to
- > their firewall or adding new strings to their banned-string list -- since
- > they already have the architecture in place to do this -- but they're not
- > going to develop any new kinds of countermeasures. In this case, TOR
- > might still be best, since after the directory servers are blocked, the
- > TOR client can fail over to the other nodes it already knows about.
- > Assuming that TOR traffic doesn't contain headers that would identify it
- > uniquely.
- >
- > - You could assume the Chinese WILL try to fight it and they WILL go to
- > the trouble of paying someone to come up with new kinds of

> countermeasures. Here, the current implementation of TOR has a weakness
> in that, as Roger described it, many TOR nodes mirror the directory. That
> means a determined Chinese censor could install a node, mirror the
> directory, and block all the IPs in that directory, severing all
> connections between Chinese nodes and "free world" nodes.

>
> Or you could make subtle changes to these conditions that have big
> implications for the "best" solution -- for example, assume that AT FIRST
> the Chinese won't care about blocking it, but at some point they will wake
> up and they will care, and then they'll spend a lot of effort cracking
> down. The solution in this case might be to use a TOR directory server to
> link up Chinese nodes with free-world nodes, but prevent any one node from
> having a mirror of the entire directory. Then as long as the Chinese
> censors aren't paying attention, people can bootstrap easily by using the
> directory server to link up. But when the Chinese crack down, they can
> block the TOR directory server, but there's no way for them to get a
> directory of all the nodes already out there that are talking to each
> other, so those connections will stay live.

>
> My theory is that because most Chinese people don't care enough about
> getting around the firewall, if you want to make real inroads into Chinese
> culture and change how people think, you have to come up with a "killer
> app" that lots of Chinese people will want to use for other reasons, and
> make circumvention a built-in feature. That brings in another set of
> problem assumptions that also changes the nature of what would be the
> "best" solution.

>
> -Bennett

>
> At 06:03 PM 12/15/2005 -0500, Simson's Treo 650 wrote:
>> Sounds like there are a lot of good Circumventer ideas to be adopted in a
>> possibly merged system. Do you have a paper that describes the issues and
>> your design decisions?

>> _____
>> Sent with SnapperMail from my Treo 650.
>> Please excuse any typos.
>> www.snappermail.com

>>
>> Original Message
>> On Thu, 15 Dec 2005 13:25:39 -0800 "Bennett Haselton"

>>< [REDACTED] wrote:
>> > 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

(b) (6)

<http://www.peacefire.org>

From: [Roger Dingedine](#)
To: [Ken Berman](#)
Cc: [Kelly DeYoe](#)
Subject: Re: [Fwd: Master's Thesis Referral from Simson Garfinkel]
Date: Wednesday, October 17, 2007 3:27:12 PM

<http://freehaven.net/anonbib/>

From: [Berel Dorfman](#)
To: [Andrew Lewman](#)
Cc: [Herman Shaw](#); [Berel Dorfman](#); [Kelly DeVos](#)
Subject: Re: [Fwd: Re: (b) (6) Re: The TOR Project]]
Date: Monday, April 28, 2008 4:09:03 PM

Andrew,

I am back from leave today. I have reviewed your fax and want to go over it with you by phone to make the contract complete. I anticipate it will be a very short phone conversation.

Thanks for your help!

Berel
Andrew Lewman wrote:

Herman Shaw wrote:

Andrew, Berel is on leave until Tuesday (4/29/08).
Please fax over a copy to Berel at (b) (6) Thanks. Herman

I'll fax it over today. Thanks.

From: [Andrew Lewman](#)
To: [Herman Shaw](#)
Cc: [Berel Dorfman](#); [Kelly DeYoe](#)
Subject: Re: [Fwd: Re: [REDACTED] Re: The TOR Project]]
Date: Monday, April 28, 2008 11:49:11 AM

Herman Shaw wrote:

> Andrew, Berel is on leave until Tuesday (4/29/08). Please fax over a
> copy to Berel at [REDACTED] Thanks. Herman

I sent the fax Saturday night. Feel free to call me with any corrections or concerns. Thanks!

--

Andrew Lewman
Director
The Tor Project
<https://www.torproject.org>
[REDACTED] (b) (6)
ppp 0x31B0974B
[REDACTED]

From: [Andrew Lewman](#)
To: [Herman Shaw](#)
Cc: [Berel Dorfman](#); [Kelly DeYoe](#)
Subject: Re: [Fwd: Re: [REDACTED] Re: The TOR Project]]
Date: Friday, April 25, 2008 11:47:41 AM

Herman Shaw wrote:

> Andrew, Berel is on leave until Tuesday (4/29/08). Please fax over a
> copy to Berel at [REDACTED] Thanks. Herman

I'll fax it over today. Thanks.

--

Andrew Lewman
Director
The Tor Project
<http://www.torproject.org>
[REDACTED] (b) (6)
pgp 0x31B0974B

From: [Herman Shaw](#)
To: [Andrew Lewman](#)
Cc: [Berel Dorfman](#); [Kelly DeYoe](#); [Herman Shaw](#)
Subject: Re: [Fwd: Re: (b) (6) Re: The TOR Project]]
Date: Friday, April 25, 2008 10:00:12 AM

Andrew, Berel is on leave until Tuesday (4/29/08). Please fax over a copy to Berel at (b) (6). Thanks. Herman

Andrew Lewman wrote:

> Hi,
>
> I attempted to email you the edited PDF but ran into your mail system
> limits. Do you have this document in the MS Word or Open Office Writer
> formats?
>
> Otherwise, I'll have to hope my edits are correct and fax it over. Thanks!
>

From: [Andrew Lewman](#)
To: [Berel Dorfman](#)
Cc: [Herman Shaw](#); [Kelly DeYoe](#)
Subject: Re: [Fwd: Re: (b) (6) Re: The TOR Project]]
Date: Thursday, April 24, 2008 5:01:55 PM

Hi,

I attempted to email you the edited PDF but ran into your mail system limits. Do you have this document in the MS Word or Open Office Writer formats?

Otherwise, I'll have to hope my edits are correct and fax it over. Thanks!

--

Andrew Lewman
Director
The Tor Project
<http://www.torproject.org>
(b) (6)
pgp 0x31B0974B

From: [Berel Dorfman](#)
To: [Andrew Lewman](#)
Cc: [Herman Shaw](#); [Kelly DeYoe](#)
Subject: Re: [Fwd: Re: (b) (6) Re: The TOR Project]]
Date: Friday, April 18, 2008 12:09:17 AM

Andrew,

Yes, filling in the prices is just a formality. They should match the numbers on your proposal. Thanks for verifying the new DUNS number.

Yes, I am already on vacation, but I usually keep up with important e-mail.

If anything else comes up, please do not hesitate to ask.

Thanks!

Berel

----- Original Message -----

From: Andrew Lewman <(b) (6)>
Date: Thursday, April 17, 2008 5:17 pm
Subject: Re: [Fwd: Re: (b) (6) Re: The TOR Project]]

> Berel Dorfman wrote:
> > 2- Pricing schedule to be filled in by hand - page 9
>
> Just to be clear, this should match the pricing proposals we've
> submitted to date, correct?
>
> >
> > 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.
>
> The DUNS number is correct. And yes it has changed since 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 = (b) (6)
>
> If your 11 days is for vacation, enjoy it. Otherwise, you should
> return to a completed contract.
>
> Thanks!
>
>
> --
> Andrew Lewman
> Director
> The Tor Project
> <http://www.torproject.org>

> [REDACTED] (b) (6)
> pgp 0x31B0974B
>

From: Andrew Lewman
To: Berel Dorfman
Cc: Herman Shaw; Kelly DeYoe
Subject: Re: [Fwd: Re: (b) (6) Re: The TOR Project]]
Date: Thursday, April 17, 2008 6:17:24 PM

Berel Dorfman wrote:

> 2- Pricing schedule to be filled in by hand - page 9

Just to be clear, this should match the pricing proposals we've submitted to date, correct?

>

> 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.

The DUNS number is correct. And yes it has changed since 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 = (b) (6)

If your 11 days is for vacation, enjoy it. Otherwise, you should return to a completed contract.

Thanks!

--

Andrew Lewman
Director
The Tor Project
<http://www.torproject.org>
(b) (6)

pgp 0x31B0974B

From: Berel Dorfman
To: Andrew Lewman
Cc: Herman Shaw; Kelly DeYoe
Subject: Re: [Fwd: Re: (b) (6) Re: The TOR Project]]
Date: Thursday, April 17, 2008 3:12:15 PM
Attachments: 6700-TORContract.pdf

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 = (b) (6)

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

----- Original Message -----
Subject: Re: (b) (6) Re: The TOR Project]
Date: Wed, 16
From: Roger Dingled (b) (6)
To: Andrew Le (b) (6)
References: (b) (6)

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 explained 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 because 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: [Berel Dorfman](#)
Cc: [Herman Shaw](#); [Kelly DeYoe](#)
Subject: Re: [Fwd: Re: [REDACTED] Re: The TOR Project]]
Date: Wednesday, April 30, 2008 10:36:36 PM

Berel Dorfman wrote:

> 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.

Awesome. I will send the original page 1 off in the mail tomorrow.

One minor question, I notice page 29 in the counter-signed contract is missing my circles around "50 or fewer" employees and "\$1 million or less" Annual gross revenues. Did you not receive my fax the other night?

Thank you!

--

Andrew Lewman
Director
The Tor Project
<https://www.torproject.org>

[REDACTED]
(b) (6)
pgp 0x31B0974B
[REDACTED]