Evading censorship using browser-based proxies

Dan Boneh, Roger Dingledine, Jonathan Ellithope,
David Fifield, Nate Hardison, Phil Porras, Emily Stark

November 30, 2011

https://crypto.stanford.edu/flashproxy/
git clone git://git.torproject.org/flashproxy.git

Summary

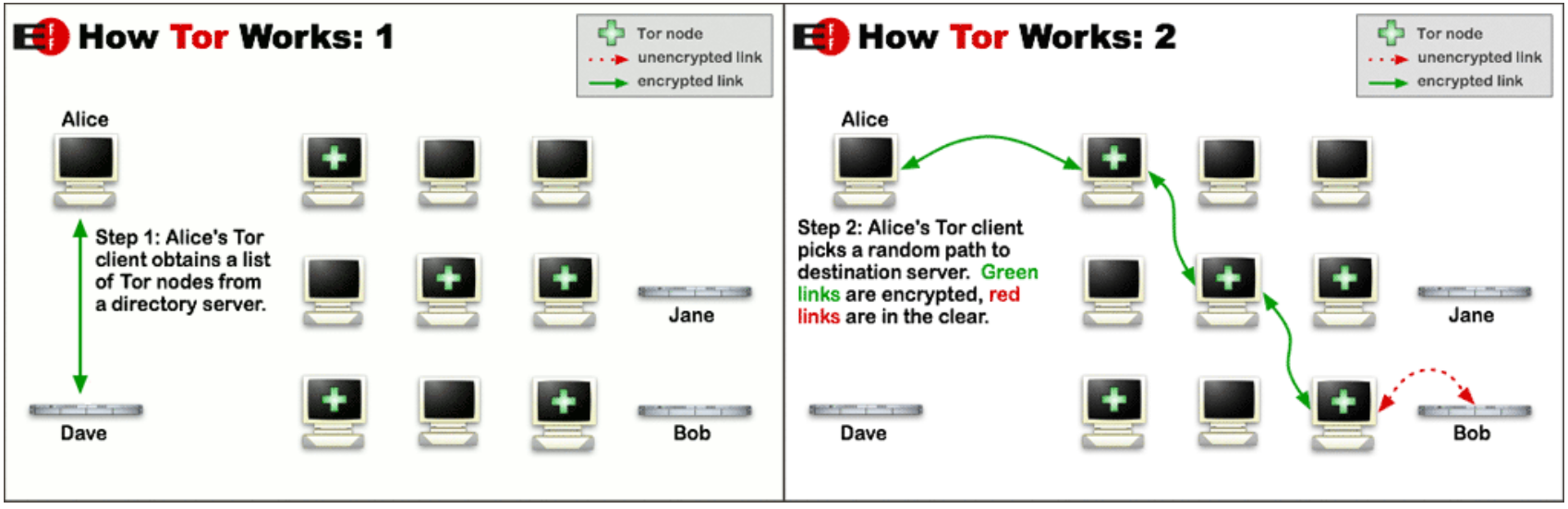
Use proxies running in web browsers as temporary, hard-to-block access points to a censorship circumvention system.

Why circumvention?

"hi.tnx for new release.i am from Iran and yahoo mail seems blocked and gmail work suspectly!(i don't know that it is blocked and banned by yahoo company (like messenger) or blocked inside of iran) i download this new release and test it.it work only by bridges under this suspect conditions!"

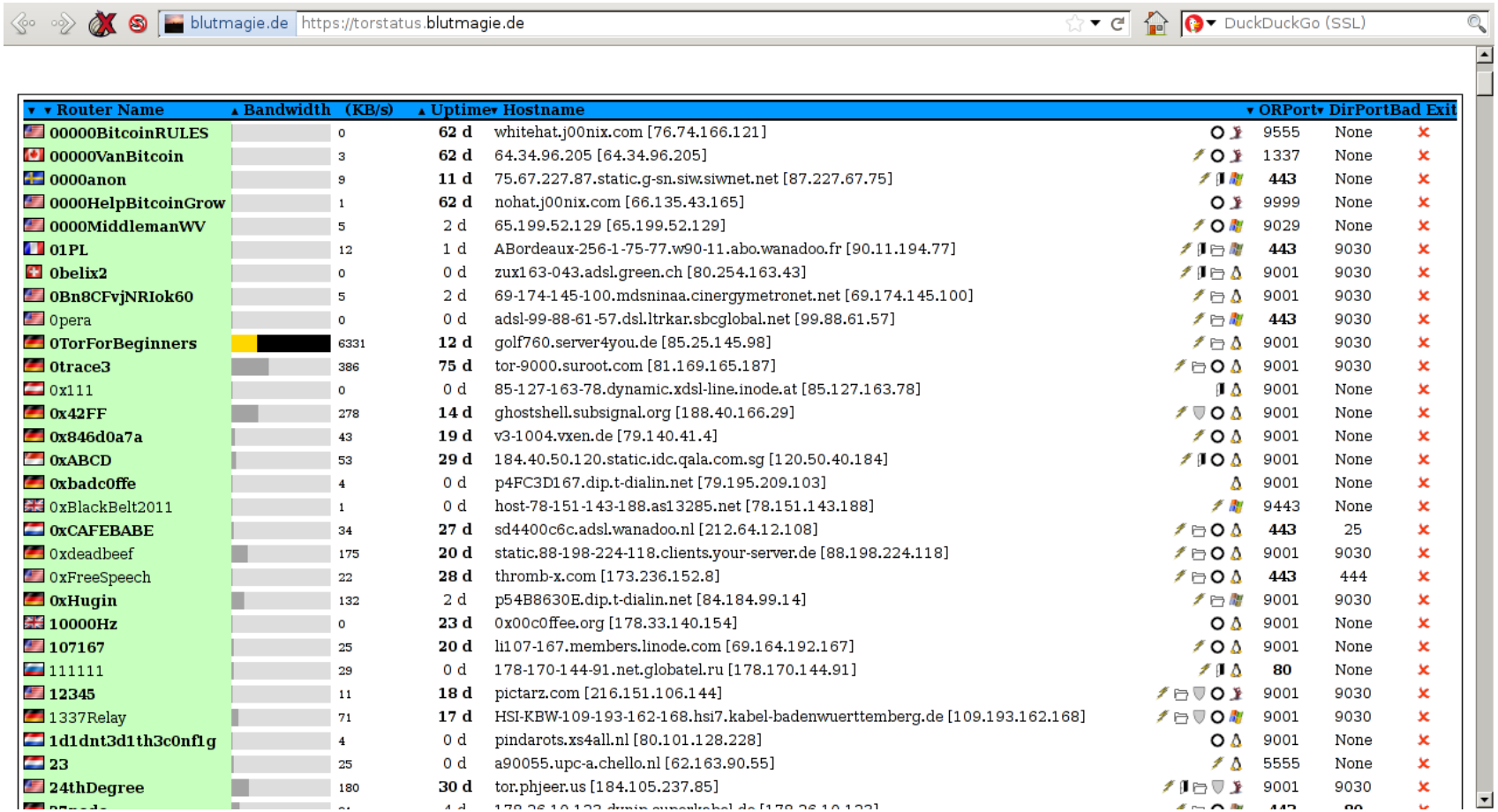
`https://blog.torproject.org/blog/new-tor-browser-bundles-7#comment-11955`

How Tor works



https://www.torproject.org/about/overview

Tor entry relays are public



Router Name	Bandwidth (KB/s)	Uptime	Hostname	ORPort	DirPort	Bad Exit
00000BitcoinRULES	0	62 d	whitehat.j00nix.com [76.74.166.121]	9555	None	
00000VanBitcoin	3	62 d	64.34.96.205 [64.34.96.205]	1337	None	
0000anon	9	11 d	75.67.227.87.static.g-sn.siw.siwnet.net [87.227.67.75]	443	None	
0000HelpBitcoinGrow	1	62 d	nohat.j00nix.com [66.135.43.165]	9999	None	
0000MiddlemanWV	5	2 d	65.199.52.129 [65.199.52.129]	9029	None	
01PL	12	1 d	ABordeaux-256-1-75-77.w90-11.abo.wanadoo.fr [90.11.194.77]	443	9030	
0belix2	0	0 d	zux163-043.adsl.green.ch [80.254.163.43]	9001	9030	
0Bn8CFvjNRIok60	5	2 d	69-174-145-100.mdsninaa.cinergymetronet.net [69.174.145.100]	9001	9030	
0pera	0	0 d	adsl-99-88-61-57.dsl.ltrkar.sbcglobal.net [99.88.61.57]	443	9030	
0TorForBeginners	6331	12 d	golf760.server4you.de [85.25.145.98]	9001	9030	
0trace3	386	75 d	tor-9000.suroot.com [81.169.165.187]	9001	9030	
0x111	0	0 d	85-127-163-78.dynamic.xdsl-line.inode.at [85.127.163.78]	9001	None	
0x42FF	278	14 d	ghostshell.subsignal.org [188.40.166.29]	9001	None	
0x846d0a7a	43	19 d	v3-1004.vxen.de [79.140.41.4]	9001	None	
0xABCD	53	29 d	184.40.50.120.static.idc.qala.com.sg [120.50.40.184]	9001	None	
0xbadc0ffe	4	0 d	p4FC3D167.dip.t-dialin.net [79.195.209.103]	9001	None	
0xBlackBelt2011	1	0 d	host-78-151-143-188.as13285.net [78.151.143.188]	9443	None	
0xCAFEBABE	34	27 d	sd4400c6c.adsl.wanadoo.nl [212.64.12.108]	443	25	
0xdeadbeef	175	20 d	static.88-198-224-118.clients.your-server.de [88.198.224.118]	9001	9030	
0xFreeSpeech	22	28 d	thromb-x.com [173.236.152.8]	443	444	
0xHugin	132	2 d	p54B8630E.dip.t-dialin.net [84.184.99.14]	9001	9030	
10000Hz	0	23 d	0x00c0ffee.org [178.33.140.154]	9001	None	
107167	25	20 d	li107-167.members.linode.com [69.164.192.167]	9001	None	
111111	29	0 d	178-170-144-91.net.globatel.ru [178.170.144.91]	80	None	
12345	11	18 d	pictarz.com [216.151.106.144]	9001	9030	
1337Relay	71	17 d	HSI-KBW-109-193-162-168.hsi7.kabel-badenwuerttemberg.de [109.193.162.168]	9001	9030	
1d1dnt3d1th3c0nf1g	4	0 d	pindarots.xs4all.nl [80.101.128.228]	9001	None	
23	25	0 d	a90055.upc-a.chello.nl [62.163.90.55]	5555	None	
24thDegree	180	30 d	tor.phjeer.us [184.105.237.85]	9001	9030	

Public relays are trivial to block by IP address.

Assumptions

- The censor tries to minimize collateral damage.
- The censor operates at line rate.
- The user is in control of their computer.

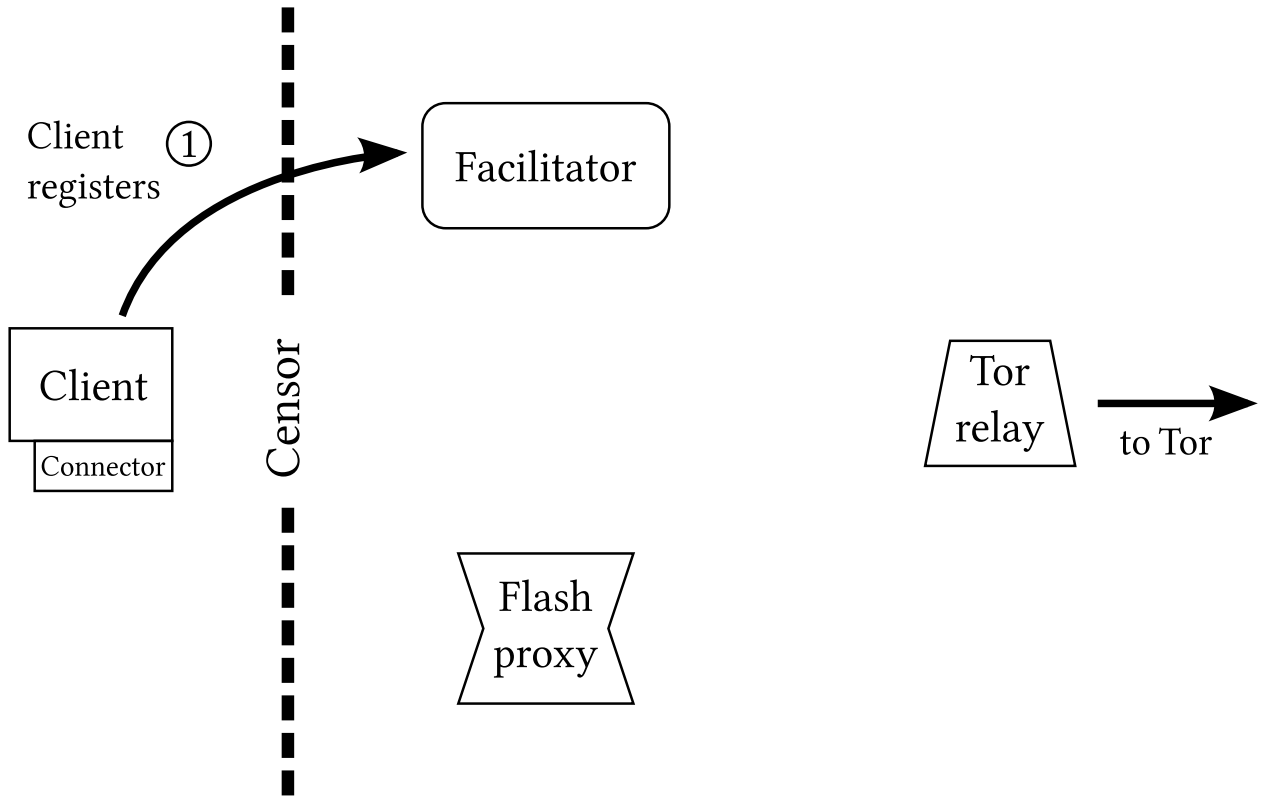
Flash proxies

A flash proxy is an applet on a web page that turns that your browser into a proxy for as long as you keep the page open.

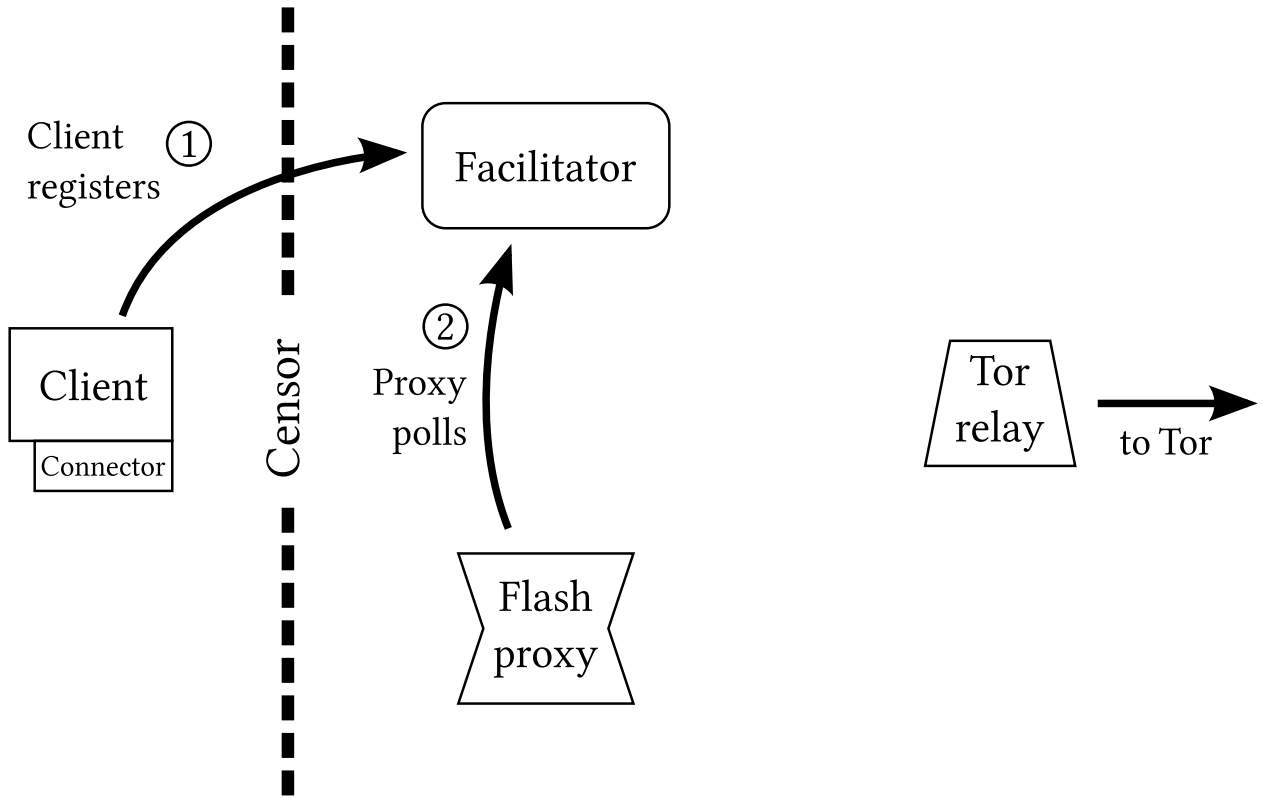
Flash proxies appear and disappear quickly enough that they can't all be blocked.

Howto

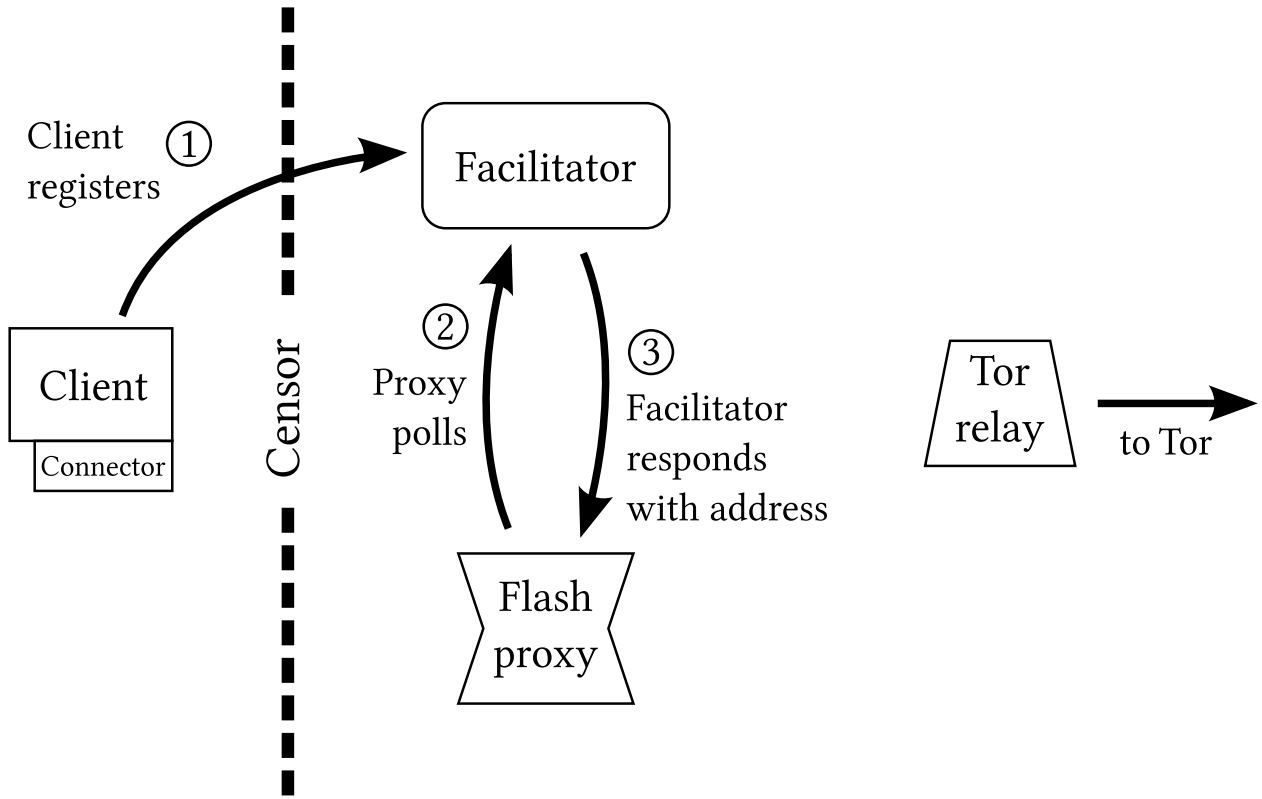
1. Download the flash proxy software.
   git clone git://git.torproject.org/flashproxy.git
2. Run the connector and Tor according to the instructions.
3. Hope that someone is viewing the proxy badge.



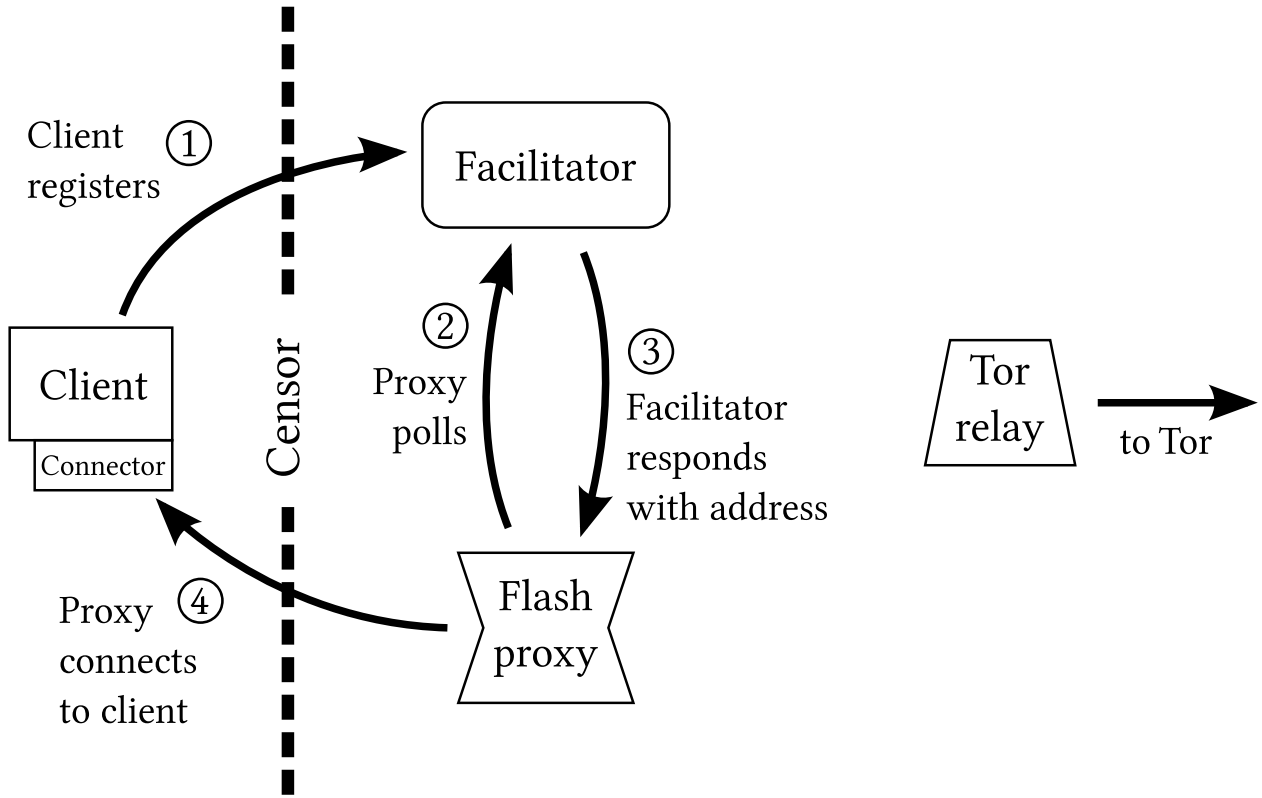
Step 1: A client indicates its need for a connection by registering with a *facilitator*.



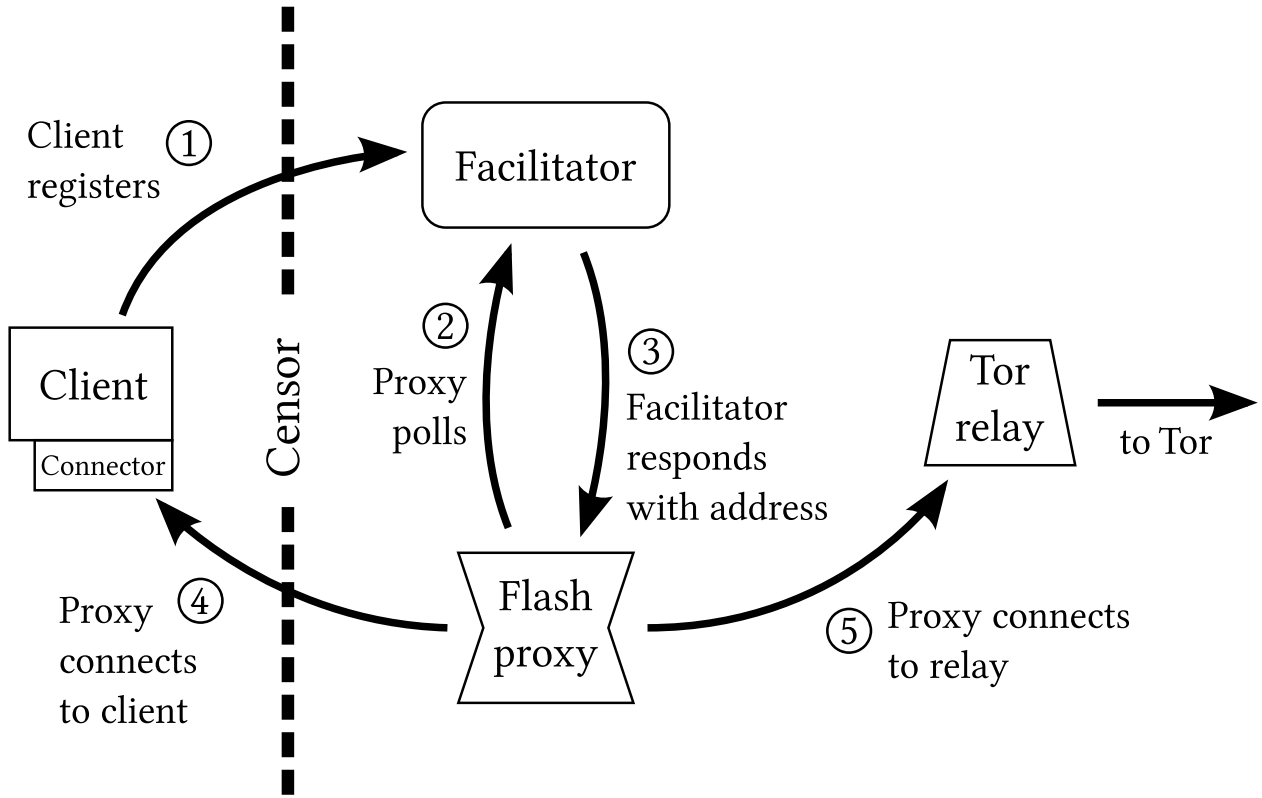
Step 2: A flash proxy in a web browser comes online and asks the facilitator for a client address.



Step 3: The facilitator sends the client's previously registered address.



Step 4: The flash proxy connects to the client. The connection is received by a small *connector* program running on the client.



Step 5: The flash proxy makes a second connection to a Tor relay, and begins proxying ciphertext between the client and the relay.

Proxy switching

When a proxy disappears, the connector switches to a different one.

Localhost download	Bandwidth
Uninterrupted flash proxy	5.95 MB/s
Alternating flash proxies	5.87 MB/s

Tor download	Bandwidth
Uninterrupted flash proxy	62.83 KB/s
Alternating flash proxies	27.93 KB/s

Challenges and limitations

Flash programs (and WebSockets, and XMLHttpRequest) can only open outgoing connections, and cannot listen for a connection like a normal proxy would.

TCP connections are broken whenever a proxy changes—which is fine for web browsing but can be annoying for long-lived connections like IMAP and SSH.

Attacks

Most attacks involve the facilitator.

- Enumeration of clients.
- Flooding facilitator with bogus registrations.
- Exhausting facilitator of registrations.

Greater deployment

Add this HTML to your web page:

```
<iframe src="//crypto.stanford.edu/flashproxy/embed.html"
 width="70px" height="23px" frameBorder="0" scrolling="no">
</iframe>
```

With badges on 100 lightly trafficked home pages, we can support an estimated number of 200 simultaneous censored users.

Our implementation uses Adobe Flash—is a plain JavaScript implementation possible?

Questions or ideas:
David Fifield <dcf@stanford.edu>

https://crypto.stanford.edu/flashproxy/
git clone git://git.torproject.org/flashproxy.git