DNS-based censorship

Theory and measurements

Stéphane Bortzmeyer

AFNIC

bortzmeyer@nic.fr
Small reminder on the DNS

The DNS is a rendez-vous system.

Not on the path but necessary for almost all communications.

He who controls the DNS controls the Internet.
Small reminder on the DNS

The DNS is a **rendez-vous** system.
Small reminder on the DNS

1. The DNS is a *rendez-vous* system.
2. Not on the path but necessary for almost all communications.
Small reminder on the DNS

1. The DNS is a *rendez-vous* system.
2. Not on the path but necessary for almost all communications.
3. He who controls the DNS controls the Internet.
DNS in action

Two types of DNS servers

Authoritative servers know the data.

Resolvers learn the data and relay it faithfully to users.
DNS in action

1. Two types of DNS servers, and very different
DNS in action

1. Two types of DNS servers
2. Authoritative servers know the data. Examples: Verisign for .com, AFNIC for .fr, Example Inc. for example.com... May be outsourced to CloudFlare or similar.
DNS in action

1. Two types of DNS servers
2. Authoritative servers know the data.
3. Resolvers (recursive, caches...) learn the data and relay it faithfully to users. Examples: your access provider, your company, public resolvers like Google Public DNS or Cisco OpenDNS.
My goal in life: preventing users to go to http://www.p0rn.example/cats

Several technical solutions (and more non-technical such as sending violators in prison). See RFC 7754

We will limit ourselves to the DNS ones
My goal in life: preventing users to go to http://www.p0rn.example/cats
I want to censor

1. My goal in life: preventing users to go to http://www.p0rn.example/cats
2. Several technical solutions (and more non-technical such as sending violators in prison). See RFC 7754
I want to censor

1. My goal in life: preventing users to go to http://www.p0rn.example/cats
2. Several technical solutions (and more non-technical such as sending violators in prison). See RFC 7754
3. We will limit ourselves to the DNS ones
Where to attack the DNS

1. Take down the domain. Works only if you have power over the registry or registrar.

2. Make the resolver a liar. Allows you to censor domains located abroad.
Where to attack the DNS

Where to attack the DNS

1. Take down the domain. **Works only if you have power over the registry or registrar.**

2. Make the resolver a liar. Allows you to censor domains located abroad. Technical solutions: RPZ in BIND, Lua scripts in PowerDNS and many others... (Next choice: lying to redirect where?)
On the issues of filtering and blocking with DNS

Legal framework
Legal framework

- France, gambling sites (decree 2011-2122, 30 Dec. 2011): “procèdent à cet arrêt en utilisant le protocole de blocage par nom de domaine (DNS)”
Legal framework

- France, gambling sites
- France, terrorist sites (decree 2015-125 5 Feb. 2015): “Les adresses électroniques figurant sur la liste comportent soit un nom de domaine (DNS), soit un nom d’hôte caractérisé par un nom de domaine précédé d’un nom de serveur.” Note the users are redirected to a site with a warning message... and may be logging.
Legal framework

- France, gambling sites
- France, terrorist sites Note the users are redirected to a site with a warning message... and may be logging.
- France, music sharing (court order, no longer government decree): example of AlloStreaming, 28 Nov. 2013
Legal framework

- France, gambling sites
- France, terrorist sites Note the users are redirected to a site with a warning message... and may be logging.
- France, music sharing: example of AlloStreaming, 28 Nov. 2013
- Similar cases in many european countries E.g.: Ireland’s High Court, 12 Jun. 2013, ordering to block ThePirateBay
Legal framework

- France, gambling sites
- France, terrorist sites Note the users are redirected to a site with a warning message... and may be logging.
- France, music sharing: example of AlloStreaming, 28 Nov. 2013
- Similar cases in many european countries
- North America: “Projet de loi 74” in Québec, against gambling sites.
Measuring censorship

Cannot be done from any vantage point with dig
Requires access to a remote resolver
Good resolvers are no longer open (RFC 5358)
Measuring censorship

Cannot be done from any vantage point with dig
Measuring censorship

1. Cannot be done from any vantage point with dig
2. Requires access to a remote resolver
Measuring censorship

1. Cannot be done from any vantage point with dig
2. Requires access to a remote resolver
3. Good resolvers are no longer open (RFC 5358)
RIPE Atlas probes

https://atlas.ripe.net/
RIPE Atlas probes

https://atlas.ripe.net/

1 Small hardware probes installed by volunteers all around the world
RIPE Atlas probes

https://atlas.ripe.net/

1. Small hardware probes installed by volunteers all around the world
2. Connect to their master and perform measurements (a good botnet)
RIPE Atlas probes

https://atlas.ripe.net/

1. Small hardware probes installed by volunteers all around the world
2. Connect to their master and perform measurements
3. Can do ICMP echo, traceroutes, DNS...
RIPE Atlas probes

https://atlas.ripe.net/

1. Small hardware probes installed by volunteers all around the world
2. Connect to their master and perform measurements
3. Can do ICMP echo, traceroutes, DNS...
4. Can perform User-Defined Measurements
RIPE Atlas probes

https://atlas.ripe.net/

1. Small hardware probes installed by volunteers all around the world
2. Connect to their master and perform measurements
3. Can do ICMP echo, traceroutes, DNS...
4. Can perform User-Defined Measurements
5. The tool atlas-resolve asks N Atlas probes to do a DNS request
First measurement example

% atlas-resolve -r 500 -c FR fifostream.tv  
[52.0.7.30] : 408 occurrences  
[ERROR: SERVFAIL] : 1 occurrences  
[ERROR: NXDOMAIN] : 10 occurrences  
[127.0.0.1] : 72 occurrences  
Test #3677498 done at 2016-04-13T10:02:34Z  

1 Domain banned by a french court order in 2013
First measurement example

% atlas-resolve -r 500 -c FR fifostream.tv
[52.0.7.30] : 408 occurrences
[ERROR: SERVFAIL] : 1 occurrences
[ERROR: NXDOMAIN] : 10 occurrences
[127.0.0.1] : 72 occurrences
Test #3677498 done at 2016-04-13T10:02:34Z

1 Domain banned by a french court order in 2013
2 Choice of lies: localhost or NXDOMAIN (no such domain)
First measurement example

% atlas-resolve -r 500 -c FR fifostream.tv
[52.0.7.30] : 408 occurrences
[ERROR: SERVFAIL] : 1 occurrences
[ERROR: NXDOMAIN] : 10 occurrences
[127.0.0.1] : 72 occurrences
Test #3677498 done at 2016-04-13T10:02:34Z

1. Domain banned by a french court order in 2013
2. Choice of lies: localhost or NXDOMAIN (no such domain)
3. Censorship decays: the court order was not repelled but it is no longer widely enforced
Second measurement example

Always compare with a base case, here another country

```bash
% atlas-resolve -r 500 -c CA fifostream.tv
[52.0.7.30] : 169 occurrences
[ERROR: SERVFAIL] : 5 occurrences
Test #3677499 done at 2016-04-13T10:06:14Z
```
Second measurement example

Always compare with a base case, here another country

% atlas-resolve -r 500 -c CA fifostream.tv
[52.0.7.30] : 169 occurrences
[ERROR: SERVFAIL] : 5 occurrences
Test #3677499 done at 2016-04-13T10:06:14Z

1 SERVFAIL can be a routing problem (all the NS in the same AS and the same /14)
Second measurement example
Always compare with a base case, here another country

% atlas-resolve -r 500 -c CA fifostream.tv
[52.0.7.30] : 169 occurrences
[ERROR: SERVFAIL] : 5 occurrences
Test #3677499 done at 2016-04-13T10:06:14Z

1. SERVFAIL can be a routing problem
2. But censorship is indeed country-specific
Recent case: WhatsApp in Brazil

% atlas-resolve -r 500 -c BR www.whatsapp.com

[ERROR: NXDOMAIN] : 10 occurrences
[169.44.82.102 169.44.84.178 184.173.147.38 184.173.147.39 \n 192.155.212.202 192.155.212.203] : 37 occurrences
Test #3748757 done at 2016-05-03T08:16:19Z

Did not last:

[169.44.82.102 169.44.84.178 184.173.147.38 184.173.147.39 \n 192.155.212.202 192.155.212.203] : 45 occurrences
Test #3754788 done at 2016-05-04T12:31:41Z
Note on RIPE Atlas probes

https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes
Note on RIPE Atlas probes

1. Installed by volunteers so probably on “geekier” networks (local resolver, DNSSEC, etc)

https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes
Note on RIPE Atlas probes

1. Installed by volunteers so probably on “geekier” networks
2. Only 4 probes in Taiwan, 8 in Mexico

https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes
Note on RIPE Atlas probes

1. Installed by volunteers so probably on “geekier” networks
2. Only 4 probes in Taiwan, 8 in Mexico
3. If 50 % of Atlas probes see something, it does **not** mean 50 % of users will see it!

https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes
Redirecting to another site

% atlas-resolve -r 500 -c TR www.etha.com.tr
Measurement #2905528 for www.etha.com.tr/A uses 32 probes
[213.14.227.50] : 5 occurrences   <--- Local ISP
[195.175.254.2] : 6 occurrences   <--- Local ISP
[176.9.34.7] : 20 occurrences      <--- The real address
Test done at 2015-11-03T08:47:09Z
Redirection in Malaysia

% atlas-resolve -r 500 -c MY themalaysianinsider.com
[203.223.159.194] : 19 occurrences
[175.139.142.25] : 4 occurrences
Test #3585216 done at 2016-02-28T10:40:24Z

203.223.159.194 is the real IP address. 175.139.142.25 belongs to Telekom Malaysia.
Ethics of measurements

Note that the measurements themselves raise ethical issues. What if I run measurements for www.p0rn.example from Iran or from www.gay.example from North Carolina?
Note that the measurements themselves raise ethical issues
Ethics of measurements

1. Note that the measurements themselves raise ethical issues.
2. What if I run measurements for www.p0rn.example from Iran or from www.gay.example from North Carolina?
But IPv4 is obsolete, no?

% atlas-resolve -r 500 -t AAAA -c FR islamc-news.info
Measurement #1895755 for islamc-news.info/AAAA uses 498 probes
[] : 586 occurrences
[::1] : 191 occurrences
Test done at 2015-03-15T20:25:57Z
But IPv4 is obsolete, no?

% atlas-resolve -r 500 -t AAAA -c FR islamic-news.info
Measurement #1895755 for islamic-news.info/AAAA uses 498 probes
[] : 586 occurrences
[::1] : 191 occurrences
Test done at 2015-03-15T20:25:57Z

At least one provider managed to censor IPv6 as well
Other measurements

The Pirate Bay, Ireland

% atlas-resolve -r 500 -c IE www.thepiratebay.se
[ERROR: SERVFAIL] : 1 occurrences
[85.91.6.46] : 4 occurrences
[141.101.118.194 141.101.118.195] : 85 occurrences
[67.212.88.146] : 6 occurrences
[ERROR: NXDOMAIN] : 1 occurrences
Test #3677553 done at 2016-04-13T14:58:34Z
Port 53 hijacking (Indonesia)

```bash
% atlas-resolve -r 500 -c ID www.reddit.com
[118.97.116.27] : 3 occurrences
[103.53.76.25] : 1 occurrences
[202.43.190.98] : 1 occurrences
[103.10.56.5] : 1 occurrences
[198.41.208.137 198.41.208.138 ... ] : 22 occurrences
Test #3754481 done at 2016-05-04T09:06:39Z
```

Is it lying resolvers? Can I switch to another one (not Google, too often hijacked by routing):

```bash
% atlas-resolve -r 500 -c ID -e 80.67.169.12 www.reddit.com
Nameserver 80.67.169.12
[118.97.116.27] : 7 occurrences
[TIMEOUT(S)] : 5 occurrences
[198.41.208.137 198.41.208.138 ... ] : 28 occurrences
Test #3754678 done at 2016-05-04T09:37:02Z
```

Apparently a combination of port blocking, port hijacking and lying resolvers.
Not every glitch is censorship


It was actually a DNSSEC problem at NASA
Solutions

Many workarounds to DNS-based censorship:
Many workarounds to DNS-based censorship:

1. Editor may switch to another name (The Pirate Bay does it all the time)
Solutions

Many workarounds to DNS-based censorship:

1. Editor may switch to another name
2. User can switch to a local resolver (aptitude install unbound) or a public resolver (high risk of hijacking, see Turkey or Indonesia, may be DNScrypt or DNS-over-TLS, RFC 7858?)
Solutions

Many workarounds to DNS-based censorship:

1. Editor may switch to another name
2. User can switch to a local resolver
Solutions

Many workarounds to DNS-based censorship:

1. Editor may switch to another name
2. User can switch to a local resolver
3. User can use Tor, a VPN...
Solutions

Many workarounds to DNS-based censorship:

1. Editor may switch to another name
2. User can switch to a local resolver
3. User can use Tor, a VPN...
4. DNSSEC can detect censorship (I’m still waiting for a censored domain using DNSSEC)
Solutions

Many workarounds to DNS-based censorship:

1. Editor may switch to another name
2. User can switch to a local resolver
3. User can use Tor, a VPN...
4. DNSSEC can detect censorship
5. More high-tech: Namecoin, BlockStack, Ethereum Name Service
Solutions

Many workarounds to DNS-based censorship:

1. Editor may switch to another name
2. User can switch to a local resolver
3. User can use Tor, a VPN...
4. DNSSEC can detect censorship
5. More high-tech: Namecoin, BlockStack, Ethereum Name Service
6. And certainly others. **Apps must behave like botnets if they want to continue to work.**
Important points about these workarounds
Important points about these workarounds

1. They are brittle (public DNS resolvers are very easy to spoof)
Important points about these workarounds

1. They are brittle (public DNS resolvers are very easy to spoof)
2. They separate the ordinary user from the guy with a Guy Fawkes mask
Censorship is often not complete, but the authorities don't care: they don't need 100% success to see some web sites, you'll need to be an engineer. What does it say about democracy?
Summary

- Censorship is often not complete
Summary

- Censorship is often not complete
- But the authorities don’t care: they don’t need 100 % success
Censorship is often not complete
But the authorities don’t care: they don’t need 100 % success
To see some Web sites, you’ll need to be an engineer. What does it say about democracy?
The future

The tussle will probably last forever

Censorship will improve, but the Internet will adapt. As a result, name resolution will be more and more messy and complicated.
Merci !