Censorship Overview

Stephen Farrell
stephen.farrell@cs.tcd.ie
March 2025
https://down.dsg.cs.tcd.ie/farrell-censorship.pdf

From the TCD module
"What is the Internet doing to me?" (witidtm)
https://github.com/sftcd/witidtm
https://down.dsg.cs.tcd.ie/witidtm

Censorship

- Ireland then and now...
- Censorship techniques
- Circumvention techniques
- Measurement
- A recent case in point: ECH
- Conclusion

Ireland then and now...

A bit of Irish history

- Ireland has a long history of censorship: the wikipedia page for that seems relatively accurate
    - https://en.wikipedia.org/wiki/Censorship_in_the_Republic_of_Ireland
- Monty Python's Life of Brian was banned in 1979
    - https://www.irishtimes.com/culture/film/an-awful-dump-the-ireland-that-banned-monty-python-s-life-of-brian-1.3807270
    - 'The film censor at the time, (Frank) Hall, himself a skilled satirist, quipped that the film was "offensive to Christians and to Jews as well, because it made them appear a terrible load of gobshites"'
    - It was "unbanned" in 1987

Current Irish Internet Censorship

- Russia Today/rt.com – not blocked in TCD, but since ~2022, is blocked via IP address from my current home ISP (Eir) and likely others

- After a court case in 2013, thepiratebay.org was blocked from 6 ISPs in Ireland (not currently block from Eir)
    - https://www.bbc.com/news/technology-22888851

- The .ie ccTLD registry (IEDR/weare.ie) maintain a blocklist of names they will not allow be registered, e.g. porn.ie (you'll get an error from whois)
    - There are likely other names/sites blocked, but the list is not public
    - Should (some/more/all) of those lists be public?
    - For almost all people: There will be some names you'd prefer to never see and sites you'd rather not highlight

Coimisiún na Meán

- Media Service Code and Media Service Rules Audiovisual On-demand Media Service Providers
    - https://www.cnam.ie/app/uploads/2025/01/Media-Service-Code-Rules-Audiovisual-On-demand-Media-Service-Providers-November-2024.pdf
    - The above is a crappy URL – the '2025/01' part changes monthly even though the document doesn't!
- That includes
    - 13.3 Media service providers of on-demand services shall not provide audiovisual commercial communications that are harmful to the general public, namely: -
        - …
        - iv. audiovisual commercial communications which encourage behaviour grossly prejudicial to the protection of the environment.
- Question: does that seem ambiguous?

Coimisiún na Meán

- Online Safety Code
  - https://www.cnam.ie/app/uploads/2025/01/Coimisiun-na-Mean_Online-Safety-Code.pdf
  - Same complaint about a bad URL
- Mostly reasonable, but includes:
  - 12.10: A video-sharing platform service provider whose terms and conditions do not preclude the uploading or sharing of adult only video content as defined in this Code shall implement effective age assurance measures as defined in this Code to ensure that adult-only video content cannot normally be seen by children. An age assurance measure based solely on self-declaration of age by users of the service shall not be an effective measure for the purposes of this section.

Censorship techniques

RFC9505: A Survey of Worldwide Censorship Techniques

- Published in 2023 based on text accumulated since 2014, so inevitably outdated

- Nonetheless, a good reference

```
4.  Technical Identification
    4.1.  Points of Control
    4.2.  Application Layer
        4.2.1.  HTTP Request Header Identification
        4.2.2.  HTTP Response Header Identification
        4.2.3.  Transport Layer Security (TLS)
        4.2.4.  Instrumenting Content Distributors
        4.2.5.  DPI Identification
    4.3.  Transport Layer
        4.3.1.  Shallow Packet Inspection and Transport Header
                Identification
        4.3.2.  Protocol Identification
    4.4.  Residual Censorship
5.  Technical Interference
    5.1.  Application Layer
        5.1.1.  DNS Interference
    5.2.  Transport Layer
        5.2.1.  Performance Degradation
        5.2.2.  Packet Dropping
        5.2.3.  RST Packet Injection
    5.3.  Routing Layer
        5.3.1.  Network Disconnection
        5.3.2.  Adversarial Route Announcement
    5.4.  Multi-layer and Non-layer
        5.4.1.  Distributed Denial of Service (DDoS)
        5.4.2.  Censorship in Depth
6.  Non-technical Interference
    6.1.  Manual Filtering
    6.2.  Self-Censorship
    6.3.  Server Takedown
    6.4.  Notice and Takedown
    6.5.  Domain Name Seizures
7.  Future Work
```

Physical Layer

Sometimes to allow gov to maintain control or to block corporation control

- Regulatory: prohibit use of frequencies or operating a business
  - https://www.semafor.com/article/07/18/2024/elon-musks-starlink-battles-africa-regulators
- Radio jamming, e.g. against voice of America in China
  - https://www.sigidwiki.com/wiki/Chinese_Firedrake_Jammer
- Many (other) jammers are illegal!

Link Layer

- Link layer (e.g. WiFi/mobile-data) connection could be dropped if censor detects misbehaviour at this or other layer(s)
    - I heard anecdotal reports of that behaviour some years ago
- Requires binding between higher-layer data visible to censor and link layer (which may be a random MAC address) so we need to worry about creating such bindings within networks
    - Such bindings could also be used for access-control if long-lived identifiers are used (or forced to be used) at the link layer
    - Proposals for exactly that have been promoted by some in industry: "Source Address Validation Improvements" (savi)
- Not much else for censors here directly

IP layer

- Lots of IP address based blocking, typically configured via address-ranges, e.g. "134.226/16" (for IPv4) or "2001:770:10::/48" (IPv6) would block all of TCD
  - Overblocking is therefore common
- Just throw away packets destined for an IP on the block-list
  - Can be done in a normal router easily enough or using special kit
  - Simple and scalable for the censor, if the to-be-censored site/content has stable IP addresses
- Or, rate-limit packets to that destination so the destination isn't "blocked" but becomes too slow to be usable
- Or, use Deep Packet Inspection (DPI) to only drop/limit some packets for that destination

IP layer/Routing

- A way to censor an entire network is to publish bad routing information about that network, using BGP
  - BGP announcements include AS number and specifiy the set of related IP addresses
  - If you're a BGP speaker then you can lie
  - If other BGP speakers (are coerced to) believe you, or don't notice, then they'll mis-route packets for destinations you've chosen

- Pakistan attempting to block youtube locally, but in fact causing a brief global outage is the classic example
  - https://adminhacks.com/bgp-internet-censorship.html

- Perhaps not the censor's favourite technique as it's pretty public and people do carefully monitor BGP announcements for accidental misconfigurations as those happen all the time, so the censor's attempts will likely be spotted
  - Doesn't stop nation states trying though, though perhaps more to inspect mis-routed traffic rather then to censor
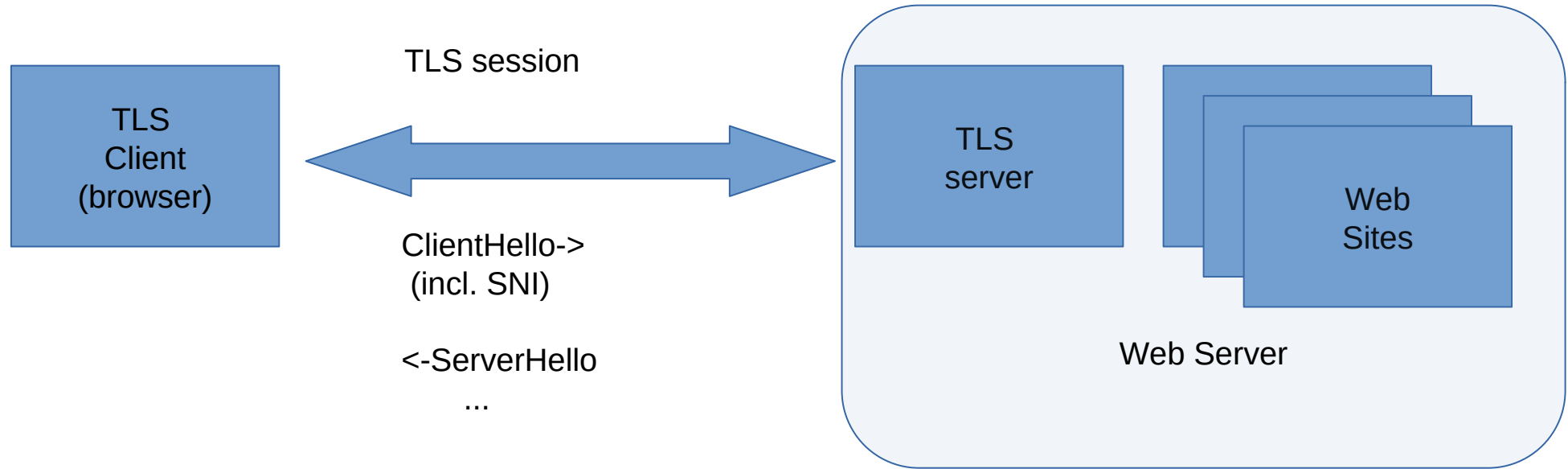
Transport Layer Reset

- Censors might not just drop packets – they may instead send RST (reset) packets to try convince both sides of a transport connection to drop the connection - pretending to both sides that an error has occurred

- This can be "easier" for the censor as they can just copy some possibly-matching packets off the "fast-path" and, when desired, send the few(ish) RST packets needed from off-path devices

  - The "fast-path" of routers is expensive kit so better for the censor to interfere with that as little as possible

Transport Layer

- Port-blocking – as well as IP addresses transport protocol have source and destination ports, e.g. destination port 25 is for SMTP (email), port 53 is for DNS etc. A censor can block by port number.

- Many (enterprise) networks (including TCD) block outbound connections by destination port in order to try prevent use of some protocols or try force hosts/users into using "local" services such as DNS

  - TCD block outbound port 53 in order to force those of us using the TCD network to use TCD's DNS services

  - You can circumvent that by using a system resolver running DoT on port 443 though (as I do:-)

TLS for multiple web sites

TLS
Client
(browser)

TLS session

ClientHello->
(incl. SNI)

<-ServerHello
...

TLS
server

Web
Sites

Web Server

Transport Layer/SNI

- The Transport Layer Security (TLS) protocol is used to encrypt at the tranport layer for the web, email transport security and many other protocols

- The first packet in a TLS session is a ClientHello packet, inside of which is the server-name-indication (SNI) that tells the server with which service (e.g. web site) the client wishes to establish an encrypted transport connection

  - SNI is needed as many services can be run on the same port, e.g. a single web server install can be used for many different web sites, and the server has to disambiguate in order to pick the right keys for the TLS session

- Censors commonly examine the SNI in ClientHello messages and block if that matches a block-list

  - More on this later (spoiler: Encrypted ClientHello or ECH:-)

- South Korea has used this method to block things, including pornography

  - https://www.technadu.com/south-korea-extend-site-blocking-snooping-sni/58125/

(Transport) Protocol Fingerprinting

- A censor can examing the set of protocol options used to "fingerprint" specific clients or implementations and then block those
  - This is easier than you might think, developers make seemingly inconsequential choices all the time and those can end up reflected in protocol options, e.g. the order of fields in a packet or the set of cryptographic algorithms supported
  - Similar to the panopticon: https://coveryourtracks.eff.org/
- This is a bit like DPI but typically applied against ClientHello-like messages that initiate an encrypted transport connection
- This has been used against Tor:
  - https://blog.torproject.org/browser-fingerprinting-introduction-and-challenges-ahead/

The "Great Cannon"

- The GFW also actively probes, partly to inform itself on what to block, but also sometimes as an attack

- In 2015 citizenlab documented DDoS attacks against greatfire.org and github originating from hosts co-located with the GFW and coined the "great cannon" phrase

    – Not clear how often this is used

    – https://citizenlab.ca/2015/04/chinas-great-cannon/

DNS Censorship

- Many protocols start with a DNS request
- If you want to censor clients in your location, then having DNS servers tell lies is a good option for you as a censor
  - Rather than the real IP address, the censor might return the IP address for a web server only hosting a "forbidden" web page
- One technique that could be used for this is DNS RPZ (response policy zone) - https://dnsrpz.info/
  - That involves DNS servers getting a "feed" of names and the related lies to tell, so can scale well
- DNS RPZ can be (and is) also used for good – if you get a feed for "domains less than 1 day old" then you may want to not help your email users to click on links to those domains from emails
  - Huge probability super-fresh domains are being used for phishing

Application Layer

- Human and/or machine-learning systems that (auto)delete posts
  - Some level of that is seemingly required in all large-scale systems with user-generated content (UGC)
- This extends to memes and images, e.g. of Winnie-the-pooh
    - https://www.theguardian.com/world/2018/aug/07/china-bans-winnie-the-pooh-film-to-stop-comparisons-to-president-xi
- Meta/facebook censoring Palestinian content
  - This is the 1ˢᵗ place we mention a private sector entity being in control of censorship (as opposed to for-profit co-operation with nation states which is common)
    - https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and

Application Layer

- Child Sexual Abuse Material (CSAM) is a horrible, and criminal, problem for which better solutions are pressingly needed

- CSAM is also regularly used to argue for the kind of controls that censors would really like to have

- Client-side scanning proposals:

  - Apple (abandoned) https://educatedguesswork.org/posts/apple-csam-intro/

  - EU Chatcontrol (keeps coming back) https://www.patrick-breyer.de/en/posts/chat-control/

- Issue: with even a 0.001% false positive rate, these schemes would utterly overwhelm law enforcement with bogus alerts

  - There are more issues;-)

Application Layer

- Many censorship schemes depend on surveillance as an enabler
- Commercial surveillance (advertising) builds profiles of people/interests based on knowing who is involved in a particular e.g. web interaction
- If you know who is attempting access then you could control what they have access to and on the basis of advertising profiles, e.g. religious affiliation

Application Layer

- In places where censorship is "strict," posting critical comments can get you in trouble:
  - Nov 2024: Co Tyrone man detained in Dubai over online review
    - https://www.rte.ie/news/ireland/2024/1113/1480697-craig-ballentine/
  - Oct 2020: US man avoids jail in Thailand over bad resort review left on Tripadvisor and Google
    - https://www.abc.net.au/news/2020-10-09/us-man-wesley-barnes-avoid-jail-thailand-over-bad-resort-review/12748666
- Be careful what you say when (and before/after!) you travel to places with very different expectations/rules
- The "before/after" aspect here is why this relates to censorship

App Stores

- Censors and app store curators may block or remove applications considered undesirable

- Curators can be coerced or may co-operate (even if gruddingly)

- Same issues could arise with any s/w distribution scheme

App Store Monitor (ASM): Global Unavailability Map

App Availability Index

Very High Availability (0-10%)

High Availability (10.01-13%)

Moderate Availability (13.01-16%)

Low Availability (16.01-20%)

Very Low Availability (Over 20%)

No App Store

*Percentage ranges represent the proportion of unavailable apps in relation to the total number of apps tested in each App Store.

https://applecensorship.com/

Internet Kill Switches

- Rather than censor at various layers some governments (also) like to have an Internet kill switch, at national or regional level

- Usually requires forcing ASes to each implement this (with a turn-it-on-again switch!), which is somewhat non-trivial

- India/Kashmir
    - https://internetshutdowns.in/

- Gabon on election day:
    - https://netblocks.org/reports/internet-cut-in-gabon-on-election-day-Q8oxM3An

Coverage

- Each nation seems to have a different way of distributing censorship instructions, with varying consequences

  – This also changes over time

- China: highly efficient (in terms of coverage) and scaleable (seemingly both bottom-up and top-down)

  – "The total number of people employed to monitor opinion and censor content on the internet – a role euphemistically known as "internet public opinion analyst" – was estimated at 2 million in 2013. " https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

- Russia: instructions from centre sent to AS/ISPs who choose HOWTO implement, leading to spotty coverage

  – Some indications this may change via hardware distributed from the centre and to be installed in each ISP

- India: coverage has been both regional and per-AS/ISP, perhaps being part of the motiviation for liking kill switches

Circumvention techniques

Caution!

- In some places, having circumvention technology on your device, or attempting to use such technologies, can itself get you in trouble
    - https://www.businessinsider.com/chinese-police-search-banned-foreign-apps-phones-2022-11
- Presumably part of this is to encourage more self-censorship
- SO – be careful and consider what you're doing before adopting the the things discussed in this part
- OTOH, it'd be bad if we all self-censor just in case

DNS

2014 incident: https://www.bortzmeyer.org/dns-routing-hijack-turkey.html

Choose your DNS preferences

- DoT – for your (home?) upstream
- DoH – for your browser**(s)**
- There's no point in round-robin'ing your queries, as each server will basically learn everything eventually, so choose well!
- The above would basically take your ISP out of the loop for DNS but replace that with your chosen public recursive servers

Public Recursive Filtering

- Many public recursives offer service at a few different IPs, some with various kinds of filtering, e.g for malware sites, net-nanny stuff etc. You can choose which to configure.

- Is that censorship? Depends who controls which services are allowed/forced to do what.
    - https://www.quad9.net/service/service-addresses-and-features/

Virtual Private Networks (VPN)

- A VPN will "move" the source location of your traffic to a VPN egress node

- That can get you "outside" a censorship regime

- Or, make it a bit harder for a censor to track the actual origin of traffic (you!)

- VPNs vary hugely in levels of trustworthiness

- Often used for access to geo-blocked content

- If you **really** depend on the VPN for hiding your origin, then you need to be much more sure that no traffic (e.g. DNS, NTP) is leaking so as to be visible to a censor

Tor

https://2019.www.torproject.org/about/overview.html.en
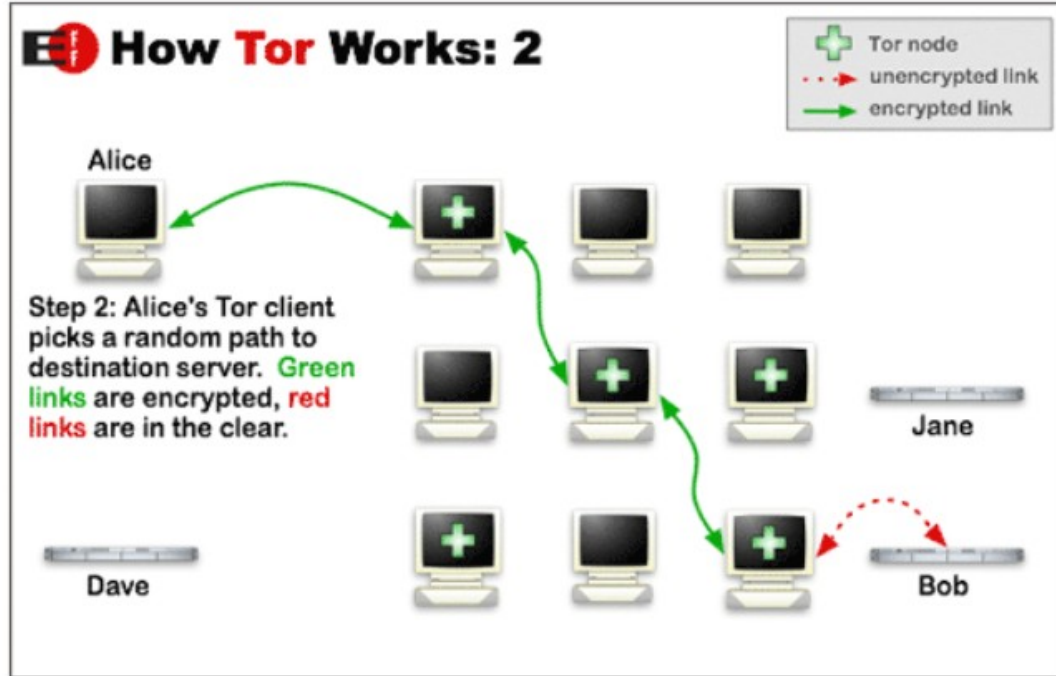
Tor Browser

- Easiest way to use Tor is via the Tor browser
  - A special build of firefox using Tor for it's HTTP traffic
- Brave browser supports "new private window with Tor"
  - A bit more deniable!
- You won't be able to connect to the Tor network from everywhere – "bridges" exist to try help here by obfuscating the connection from you to the ingress node and using a (hopefully not well known) bridge for ingress
  - This is to help people get connection to "outside" the censor
- Remember: if you are the only one using Tor in your local network, then that fact is detectable
  - Corollary: if we use Tor when we don't really need to, we're maybe helping others a teeny bit

Psiphon

- Windows + phones VPN-like tool
- Obfuscates traffic to ingress, otherwise similar ideas as Tor
- Supports "pluggable transports" to enable flexibility if censor blocks some methods of connecting to ingress
  - https://www.psiphon.ca

Browser/Stack Tricks

- Both sides can ignore (some) RST messages
- The TLS ClientHello message can be split into two, with the SNI value spanning the split
  - Many censors no longer find the value
- Similar tricks are discovered from time to time, used in circumvention tools, eventually become public and likely result in censors changing their setup

IP Layer Mitigation

- A recent paper reverse-engineered GFW blocking rules
  - https://gfw.report/publications/usenixsecurity23/en/

- Adding non-random data (cleverly) mitigated these checks

Censor's Traffic Analysis Algorithm
Block the connection *unless any of the following hold*

Fraction of zeroes ≤ 42.5% or ≥ 57.5%

The first six bytes are printable ASCII

>50% of bytes are printable ASCII

20 contiguous bytes are printable ASCII

Matches the fingerprint for HTTP or TLS

Sneakernet

- Passing around censored content and/or tools on a physical storage medium (e.g. USB stick) has often been a good fallback
- The Cuban El Paquette was(?) perhaps the best known example
  - https://laredcubana.blogspot.com/search/label/paquete
- This was a weekly distribution of content, including web sites, TV shows etc
- Source unclear
- May have fallen victim to pandemic:
- https://web.archive.org/web/20200123173814/http://paquetedecuba.com/

Weaponizing Censorship Infrastructure

- Since a censor (like the GFW) may send RST packets towards endpoints, that can be used to mount attacks on those if the attacker spoofs source addresses

  - Attack effective due to "residual censorship" – censor may ovcerblock for an extended period if it sees something it wants to block

  - Attack is conceptually simple but making it effective is tricky and details differ by country (China, Iran, Kazakhstan in the paper)

- "Your Censor is My Censor: Weaponizing Censorship Infrastructure for Availability Attacks"

  - https://geneva.cs.umd.edu/papers/woot21-weaponizing-availability.pdf

- Take away: censors can damage themselves, but it likely won't convince them to stop

Measurement

Open Observatory of Network Interference (OONI)

- ooniprobe is an (open-source) installable app that tries to access a curated list of Internet resources (DNS names, web sites) and reports back

- Data:

    – https://explorer.ooni.org/
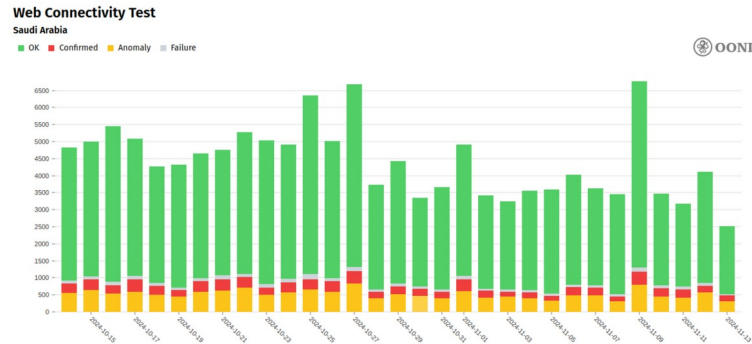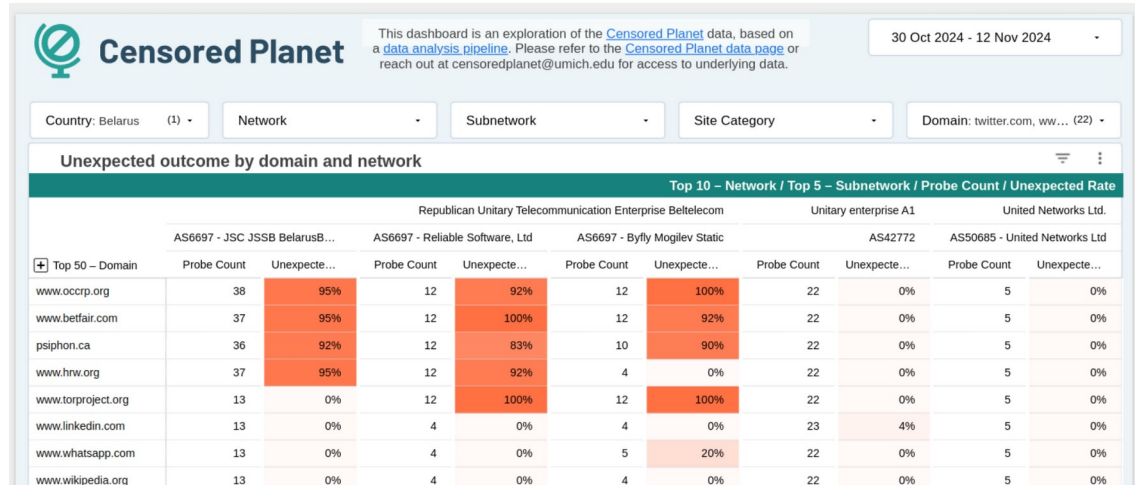
Netblocks

- Monitors BGP and other visible traffic to detect network outages and generally correlates those with ongoing events
  - https://netblocks.org/
- Image from Nov 6 2024 shows outages in Mozambique, seemingly related to election results

Internet Traffic Data - Mozambique: 2024-11-02 to 2024-11-06 UTC
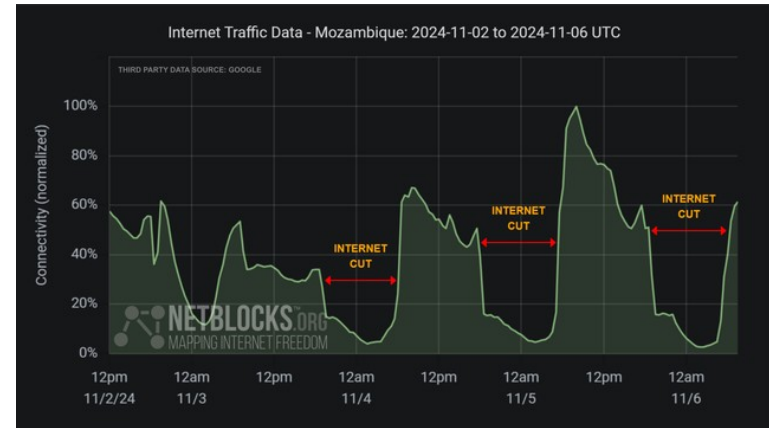
CensoredPlanet

- More academic observatory, multiple sources and projects ongoing, plenty of publications
  - https://data.censoredplanet.org/
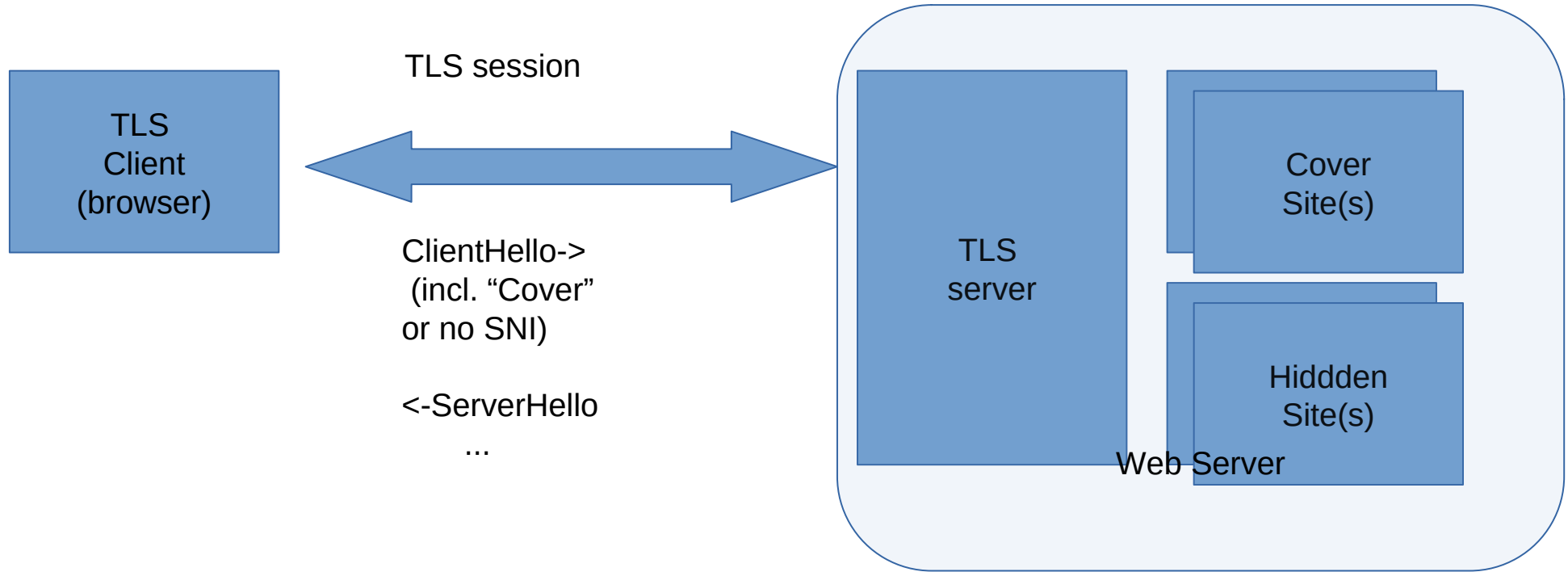
Encrypted ClientHello (ECH)

Overview

- As well as knowing about today's Internet it might be useful to know a bit about what's coming and how some things evolve
- So I'll describe some work I've been helping with for the last couple of years, how that might go and how it might ultimately affect you
- That's a thing called "Encrypted ClientHello" (ECH)
- The goal is to improve privacy and to partly mitigate the kind of SNI censorship mentioned earlier

TLS for multiple web sites

TLS
Client
(browser)

TLS session

ClientHello->
(incl. SNI)

<-ServerHello
...

TLS
server

Web
Sites

Web Server
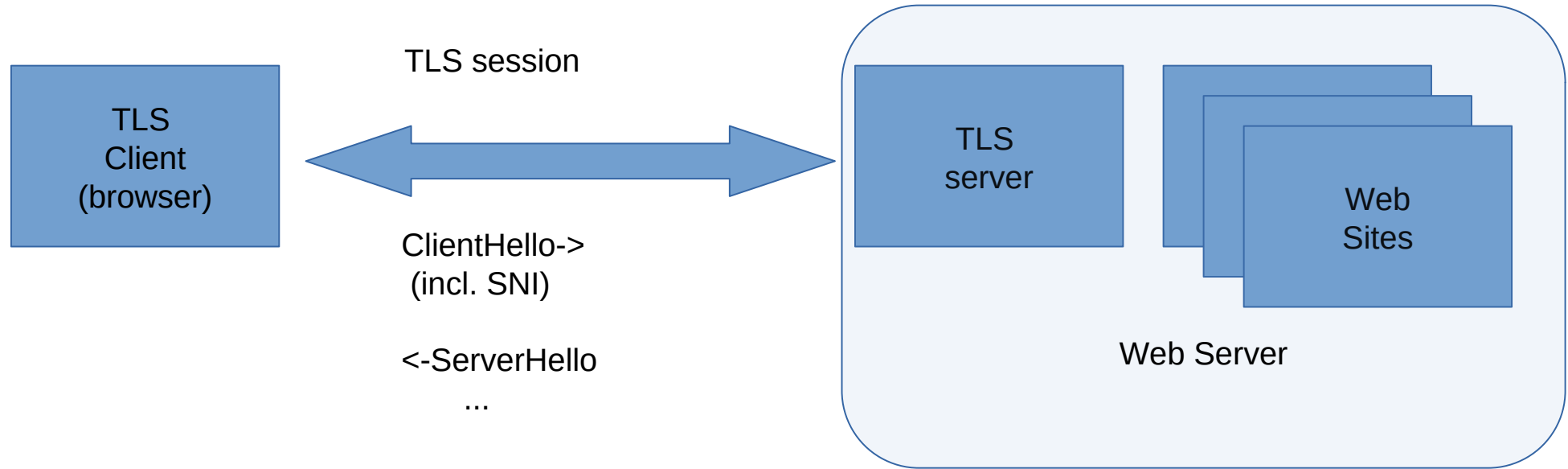
What we'd like, and can do now ("co-located" variant)

TLS session

TLS Client (browser)

ClientHello->
 (incl. "Cover"
or no SNI)

<-ServerHello
...

TLS server

Cover Site(s)

Hiddden Site(s)

Web Server

ECH Spec/Status

- Solution being developed in the IETF TLS WG: https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni
- Current draft is version -24, in development since mid-2018, with the spec "stable" since Aug 2021. should be done and an RFC "soon"
- Multiple implementations exist, including mine

  - https://defo-project/openssl/ is my "fork" of OpenSSL - a very widely used TLS/encryption library that can be used with apache, nginx, lighttpd (web server implementations) and haproxy versions I've modified to support ECH

- Deployed in most browsers now, and by Cloudflare for their web site customers

- Next big step will be to upstream code to OpenSSL, nginx, apache... hopefully during 2025

- (I have some funding from OTF to help get some of this done)

How ECH Works

Look up A/AAAA and HTTPS

DNS

TLS Client (browser)

TLS session

Cover Site

ddden Site
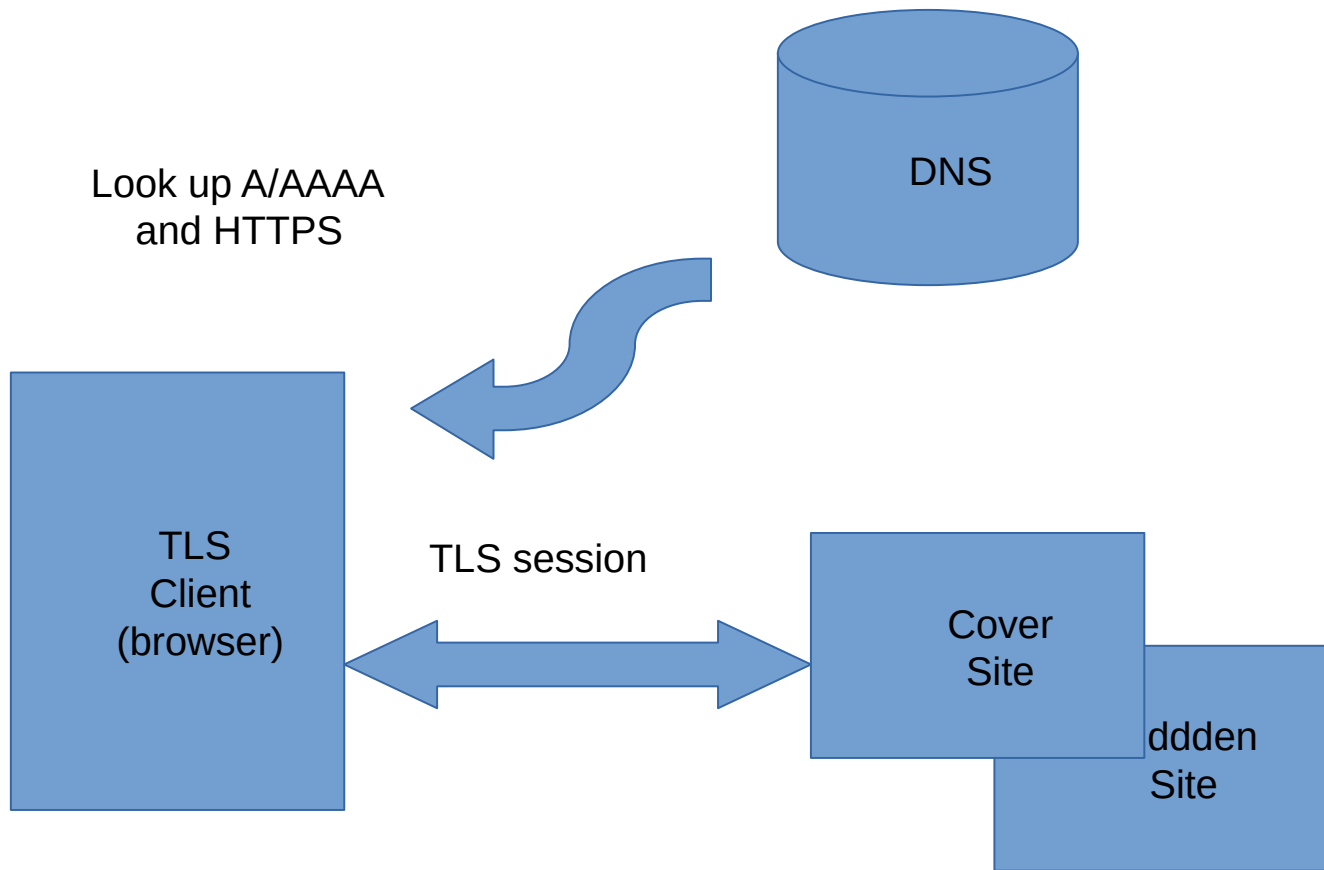
How does ECH work?

- Needs ability to create/consume new DNS resource records
- Needs TLS1.3 (earlier versions send server cert in clear)
- DNS privacy (DoT/DoH) not strictly needed but if you don't use that maybe there's less point in using ECH (Browsers may couple the two)
- Web site publishes a new public key/value in the DNS ("SVCB" or "HTTPS") with some additional keys (HPKE public values) for ECH
- ECH-aware client (e.g. browser) can check if DNS record exists and has ECH keys
- All going well, use those ECH keys with HPKE (RFC 9180) to derive a new shared-secret and send the "real" ClientHello message encrypted in side an "outer" ClientHello message
- The fact that ECH is being used is still visible

GREASEing ECH

- The fact that ECH is being used is still visible
- That may be countered via "GREASEing" - having browsers that are not using ECH sometimes send a ClientHello that looks like it does use ECH
- GREASEing is an anti-ossification TLS implementation trick – clients and servers include garbage values for optional things in order to decrease the probability that middleboxes fixate on currently deployed protocol options - RFC8701

November 2024

- Russia started blocking ECH when used with Cloudflare

- They actually issued a statement saying so!

- Be interesting to see how this evolves

Russian Statement

The Center for Monitoring and Control of Public Communications Networks (CMU SSOP) of Roskomnadzor recommends that owners of Internet resources stop using the CDN service of CloudFlare, since the extension used by default violates Russian legislation and is blocked in Russia. "The American company CloudFlare, a CDN service provider, enabled the use of the TLS ECH (Encrypted Client Hello) extension by default on its servers in October. This technology is a means of bypassing restrictions on access to information prohibited in Russia. Its use violates Russian legislation and is limited by technical means of countering threats (TSPU)," the center's website says. We recommend that owners of information resources disable the TLS ECH extension or, more correctly, use domestic CDN services that ensure reliable and secure operation of resources and protection from computer attacks," the center added.
Official confirmation: https://www.interfax.ru/russia/990568

Conclusion

Conclusion

- Remember that "ancient" Irish censorship?
- Brave new world:
  - https://www.theguardian.com/us-news/2024/nov/13/florida-book-bans-removals-education-department-list
  - That said, the article does not describe what kinds of school, nor ages, so it's maybe too easy to consider this ridiculuous
- Bottom line: we can go back, maybe as quickly as we advanced, and it's your future, so be informed, consider what you'd like to see, and work towards that! (as much as that's relevant to you)

Censorship Overview

Stephen Farrell
stephen.farrell@cs.tcd.ie
March 2025
https://down.dsg.cs.tcd.ie/farrell-censorship.pdf

From the TCD module
"What is the Internet doing to me?" (witidtm)
https://github.com/sftcd/witidtm
https://down.dsg.cs.tcd.ie/witidtm