Encore
Lightweight Measurement of Web Censorship

Alex Rao

October 21, 2020
What Is Censorship?

• Restriction of available information
• Examples?
  • United Arab Emirates: Human Rights links blocked (official govt page)
  • Replace resources with generic block page
  • Libya, Egypt, Turkey?, Belarus (slow), Georgia
  • Block bad news, banning adult/obscene material “not kosher”
  • Censorship from parental (child lock)
  • Company censorship on intranet
  • ID behind activists (drive fear against activism)
How does it Happen

• DNS Lookup
  • Not blocked
  • Respond with valid response – *wrong response* (blocking page...)

• TCP connection initialization
  • Reset vs drop

• Specific HTTP Request
Censorship and Security & Privacy

• Tech (i.e., VPNs) can be used with both censorship & privacy
  • VPN
  • DNS over HTTPS

• From user POV, breaking censorship => privacy will be targeted

• Privacy makes activism against censorship possible

• Example: Belarus Govt suppress, but could not ID police. Protestors used Facial Recognition to ID police, Dox them
  • Govt trying to protect privacy by censoring websites that would post

• Go hand in hand. Censorship vs Moderation – connotation is key

• Double Edged Sword, Eye of the beholder

• Tied to security! Network censors are doing traditional network attacks (DNS cache poison, etc.)
What Makes it Difficult to Measure?

- Vantage point – you can see only what you’re exposed to
- Censor blocks any way to measure, beyond what they block
- Don’t Know what you Don’t Know™
- Lots of variability (browsers, availability, tooling) -> COMPLEX
- Specificity of censorship (domains vs specific pages, etc.)
- Manifests as network problems – which is it?
- **False Negatives vs False Positives**
  - Censorship implies a motive (and not a good one...)
  - Censored material varies over time (location, time)
  - Viral content – not censorship but “legitimate DoS”
  - Censors will also adjust to new techniques – arms race
  - Big Platforms do go down every now and then
Existing Work

• Existing measurement tools
  • (OONI, Centinel, CensMon)
  • Limited Deployment

• Block Lists (Open Network Initiative)

• Bortz – Cross-origin requests!

• Most are based on volunteers running measurement software
Cross Origin Requests

• Specific to web browser – we’ve seen this before!
• Causes original page to request resource from other place
  • i.e., image, stylesheets, etc.
• XSS vulnerability mitigation limits kinds of resources we can ask for
How does it Work?

1. example.com (Origin server)
2. Coordination server
3. censored.com (Target)
4. Collection server

HTTP GET /foo.html

HTTP GET /task.js

HTTP GET /favicon.ico

HTTP GET /submit?result=failure
Highlights

• No user consent or involvement

• Completely Server-side
  • Data Self-Reported by webmasters

• For site-wide censorship
  • Images
  • Stylesheets

• For per-page
  • Inline Frames
  • Scripts
Pros

• Don’t need volunteers in countries to measure
• Exponentially increases sample space
• Avoid too much performance overhead (sheer size, or what its doing)
• Super easy to deploy as a webmaster
• Super small payload
• Why not VPN tho... (vantage points?)
What Possible *Non-Ethical* Issues?

- False Negative & False Positives
- If something goes wrong with Encore/Hacker, potentially load malicious payload (big stuff, among other things)
  - Thresholds are cool but... um, where did you pull that from?
  - MOBILE networks are big problem (esp in developing countries)
  - Not everyone is 30 feet from a backbone
- Censors can catch on, just block that too
- Only test certain pages (if you don’t have the right resources, Big Sad™)
Ethical Concerns?

• Greyscale of more/less ethical

• Endanger the user’s lives! If it looks like you’re accessing a lot of bad places
  • Flood the sources so it’s clear they’re not accessing
  • Govt will catch on to either a) users or b) Encore

• Could be extreme, but also maybe just a slap on the wrist?

• Value: People taking the risk don’t benefit... So, why do that?

• Guiding Principle: Belmont/Menlo Report => “Justice”: People who take risks should benefit
  • Respect for persons: Respect autonomy (INFORMED CONSENT LOL)
  • Beneficience: Do no harm (unless you have to but then minimize)
Was it Worth It?

• I mean........ Maybe. But risky
• Published because it was already done so... why not at least use the data
• Why was it not flagged – oops
  • IRB didn’t flag it – had two times to do so (didn’t review)
  • Not designed for this – ethical stuff is hard to reason about
  • Not really a user study, no interactions
  • Still issue in the field (esp CS), more for medical, sociology
• Value: People taking the risk don’t benefit... So, why do that?
Questions?