Censored Planet Observatory

Measuring Internet censorship globally, continuously, and remotely

Internet Measurement Village 2020

Ram Sundara Raman

June 26, 2020
Measuring Censorship is a Complex Problem!

Internet censorship practices are diverse in their methods, targets, timing, differing by regions (even within countries or networks), as well as across time.
Direct Censorship Measurement

- Ask people on the ground, or deploy software or hardware in censored region (e.g. OONI probe, FreedomHouse)
- Use VPNs, or research networks (e.g. PlanetLab, ICLab)
<table>
<thead>
<tr>
<th>Challenges with Direct Measurements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scale</strong></td>
</tr>
<tr>
<td>Takes tremendous effort to recruit a large number of volunteers or access points</td>
</tr>
<tr>
<td><strong>Coverage</strong></td>
</tr>
<tr>
<td>Hard to obtain access points that cover a majority of networks in the country</td>
</tr>
<tr>
<td><strong>Continuity</strong></td>
</tr>
<tr>
<td>Hard to continuously and repetitively run measurements using volunteers</td>
</tr>
<tr>
<td><strong>Synchronization</strong></td>
</tr>
<tr>
<td>New updates and censorship measurement techniques must be pushed, and detection may be delayed</td>
</tr>
<tr>
<td><strong>Ethics</strong></td>
</tr>
<tr>
<td>Risky to run censorship measurements unless the proper precautions are taken</td>
</tr>
</tbody>
</table>
IPv4 hosts - Internet infrastructure is everywhere
Remote Censorship Measurements

Can we detect whether pairs of hosts around the world can talk to each other without controlling either endpoint?
Censorship can occur at multiple protocol layers

**Challenge:** Design methods to detect interference remotely at all network layers, without end-user participation.
Censorship can occur at multiple protocol layers

Satellite and Iris
(https://www.censoredplanet.org/projects/satellite)
Censorship can occur at multiple protocol layers

DNS query censoredplanet.org

DNS resolver

HTTP requests

(opt) TLS handshake

TCP handshake

IP routing

ISP

Server

Spooky Scan and Augur
(https://www.censoredplanet.org/projects/augur)
Censorship can occur at multiple protocol layers

DNS query censoredplanet.org

DNS resolver

HTTP requests

TCP handshake

(opt) TLS handshake

IP routing

Quack and Hyperquack
(https://www.censoredplanet.org/projects/quack)
(https://www.censoredplanet.org/projects/hyperquack)
Remote Measurement Techniques

1. **Satellite and Iris**
   Measure DNS manipulation using Open DNS resolvers

2. **Quack and Hyperquack**
   Measure application-layer keyword censorship using Echo and HTTP(S) servers

3. **Spooky Scan and Augur**
   Measure global TCP/IP blocking using IP ID side channels
Remote Measurement Techniques

1. **Satellite and Iris**
   Measure DNS manipulation using Open DNS resolvers

2. **Quack and Hyperquack**
   Measure application-layer keyword censorship using Echo and HTTP(S) servers

3. **Spooky Scan and Augur**
   Measure global TCP/IP blocking using IP ID side channels
DNS Manipulation

Client

DNS query for https://censoredplanet.org

200.31.1.49

216.239.34.21

DNS Resolver
Satellite & Iris
Satellite & Iris

Measurement Machine

1. DNS query for censoredplanet.org
2. Test IP

OpenDNS Resolver

3. DNS query for censoredplanet.org
4. Control IP

Control Resolvers
Satellite & Iris

Compare:
- Test IP vs Control IP
- HTTP content hashes
- TLS certificates
- ASN and AS Name etc.

1. DNS query for censoredplanet.org
2. Test IP
3. DNS query for censoredplanet.org
4. Control IP
5. Measurement Machine

OpenDNS Resolver
Control Resolvers
Satellite Scale, Coverage and Ethics

- More than 8.2 million OpenDNS resolvers in 232 countries
- To reduce risk, we want to choose infrastructural resolvers
- We use resolvers with a valid PTR record beginning with the subdomain `ns[0-9]*` or `nameserver[0-9]*` → Likely to be part of big organizations
- 30k resolvers in ~4,500 ASes in 175 countries
- Stable DNS resolvers allow us to repetitively run measurements over time
Remote Measurement Techniques

1. **Satellite and Iris**
   Measure DNS manipulation using Open DNS resolvers

2. **Quack and Hyperquack**
   Measure application-layer keyword censorship using Echo and HTTP(S) servers

3. **Spooky Scan and Augur**
   Measure global TCP/IP blocking using IP ID side channels
Application-layer keyword blocking

TCP Handshake
GET https://censoredplanet.org

User → RST → Server
User → RST → Server
An Echo service simply sends back to the originating source any data it receives.
Quack

33,000 usable Echo Servers in ~2,800 ASes in 166 countries
Hyperquack
Hyperquack
Hyperquack
Hyperquack

TCP Handshake

Measurement Machine

104.198.14.52

Web Server

GET https://censoredplanet.org

Found

The document has moved here.
Hyperquack

TCP Handshake

104.198.14.52

Web Server

Measurement Machine

GET https://torproject.org

Found

The document has moved here.
Hyperquack

Measurement Machine

TCP Handshake

Web Server

GET http://example{1,2,3}.com

HTTP reply
(e.g., Status Code: 302 Found)

Build Canonical template of server response
Hyperquack
Hyperquack Scale, Coverage and Ethics

- More than 50 million web servers (all around the world)
- To reduce risk, we want to choose infrastructural vantage points
- Use web servers that produce a valid EV certificate, as they are more likely to be organizational
- After filtering for capacity, we regularly use 30k web servers in ~3,800 ASes in 191 countries
Remote Measurement Techniques

1. **Satellite and Iris**
   Measure DNS manipulation using Open DNS resolvers

2. **Quack and Hyperquack**
   Measure application-layer keyword censorship using Echo and HTTP(S) servers

3. **Spooky Scan and Augur**
   Measure global TCP/IP blocking using IP ID side channels
The Censored Planet Observatory uses remote measurement tools to scalably, ethically and continuously measure different kinds of global Internet censorship.
Censored Planet Observatory

- Launched in August 2018 and running continuously since
- Continuous baseline of reachability data for **2000 sensitive domains and IP addresses** (From Alexa and Citizen Lab) each week
- More than **95,000 vantage points** in **221 countries and territories** (updated every week)
- Rapid focus capabilities to analyze censorship events in detail
25 billion
Measurements over 22 Months

221 countries
42%-360% increase compared to OONI, ICLab

8 ASes (median)/country
Median increase of 4-7 ASes per country
Vantage Points in March 2020 (Scale 1 - 29,617)
Vantage Points over time
Identifying Network Censorship Devices

Censored Planet data identified the deployments of many network censorship devices

Publication - Measuring the Deployment of Network Censorship Filters at Global Scale; R. Sundara Raman, A. Stoll, J. Dalek, R. Ramesh, W. Scott, and R. Ensafi; Network and Distributed System Security Symposium (NDSS), 2020

Real-time monitor tracks the growing use of network filters for censorship

February 21, 2020

The team says their framework can scalably and semi-automatically monitor the use of filtering technologies for censorship at global scale.
Investigating Russia’s Censorship Model

Censored Planet helped investigate large-scale ISP specific blocking of online resources in Russia’s authoritative blocklist.

Complementing Direct Measurements

Censored Planet can complement in-depth direct measurements by providing higher scale. Censored Planet data confirmed OONI’s observation about the blocking of abortion rights websites.

Censored Planet’s Rapid Focus

Kazakhstan’s HTTPS interception
https://censoredplanet.org/kazakhstan
Kazakhstan’s National TLS Interception

- **July 17, 2019**: Government started intercepting large fraction of HTTPS traffic within its borders.
- Local ISPs told to instruct users to install a government-issued certificate on all devices and in every browser.
How the interception works

- **Client Hello**: (,...Cipher supported, sessionid, random data,SNI,...)
- **Server Hello**: (,...selected Cipher, ..., Certificate,...)
- **Client certificate**
- **Key exchange**
- **HTTP GET request**
- **HTTP reply**

**MITM**

- **Client Hello**: (,...Cipher supported, sessionid, random data,SNI,...)
- **Server Hello**: (,...selected Cipher, ..., Certificate,...)
- **Client certificate**
- **Key exchange**
- **HTTP GET request**
- **HTTP reply**

**HTTPS server**

- **HTTP GET request**
- **HTTP reply** (e.g., Facebook materials)

**Encrypted using MiTM injected certificate**

**Encrypted using trusted certificate**
What does this mean for users?

- Complete visibility
- Traffic modification
- Selective blocking

Haven’t installed the fake cert?

- Security warnings for all website access
- Access essentially blocked if HSTS is enabled
Hyperquack detects the use of rogue certificates
Measurements to some VPs in Kazakhstan saw the ‘Qaznet Trust Network’ cert
Running customized measurements
Observations

- Only 7.0 - 24% of TLS hosts tested had certificates injected → interception only happened in a fraction of the country.

- Using TTL-limited measurements, observed only certain portions of the connections, passing through AS9198 (KazakhTelecom) were affected

```
1  185.120.76.1
2  88.204.195.89
3  212.154.195.97
4  92.47.151.210
5  95.56.243.92
6  178.89.110.198
7  178.89.110.206
8  *
Certificate injection occurred between hops 4 and 5.
```
Observations

37 domains were affected - Mostly social media domains
- 20 Google domains
- 7 Facebook domains
- 4 vk domains
Longitudinal Tracking
Browsers Take a Stand Against Interception

The use of ‘Qaznet Trust Network’ root CA certificate in Chrome, Firefox, and Safari is now prevented.
Censored Planet
Website

https://censoredplanet.org/observatory

Please contact us at: censoredplanet@umich.edu
Some Future Plans

- Expanding rapid focus capabilities - Ability to quickly run custom measurements working with the community
- Real-time data analysis pipeline and API for easy access into the data
- Collaborating with direct measurement platforms like OONI to combine the power of both worlds
Censored Planet

Thank you!

https://censoredplanet.org
Contact us at
censoredplanet@umich.edu