Running Software in Albuquerque to Measure Censorship Anywhere

Jeffrey Knockel
Roya Ensafi
Jedidiah Crandall

Computer Science Department
University of New Mexico
When will Desert Storm invasion begin?
No access to Pentagon
Watch Dominos outside Pentagon
Pentagon deliveries normally
Night before an invasion
Moral of the story

We can measure what is happening in a thing without being in that thing
Question

Server

Can clients connect to the server?

Clients

Albuquerque
Measurement

• Run measurement software over there
• Problem: cannot get software in there
• Or:
  – Not in the right city
  – Not right now
• We don't need measurement software on client, on server, or in between
Client

- Find client with *globally incrementing IP ID*

### IP Header

<table>
<thead>
<tr>
<th>Version / IHL / TOS</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Flags / Fragment Offset</td>
</tr>
<tr>
<td>TTL / Protocol</td>
<td>Checksum</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IP</td>
</tr>
</tbody>
</table>

- Windows XP, FreeBSD, etc. globally increment this ID
Measure # of packets sent

- Ping every second
  - 1006, 1007, 1008, 1009…
    - 1, 1, 1… none sent
  - 3003, 3007, 3012, 3016…
    - 4, 5, 4… some sent
  - 4000, 5000, 6200, 7300…
    - 1000, 1200, 1100… lots sent
Experiment

Server

Client

Forged SYN

Albuquerque
No censorship (+1)

Server

Forged SYN

SYNACK

RST

Client

Albuquerque
Server $\rightarrow$ Client censored (+0)

Forged SYN

Albuquerque
Client → Server censored (+>1)

Server

SYNACK

RST

SYNACK

RST

...

Client

Forged SYN

Albuquerque
ARIMA time series
Iterative outlier removal

![Graph showing iterative outlier removal](image-url)
Intervention analysis

Server → Client 0
No censorship 5
Client → Server 15

Measured intervention: 15.1
Client → Server filtering!
Ethical concerns

Can clients sending RST's get them hurt?

Ethical Knob

← Decrease clarity        Decrease karma →
Future

• Gathering data
• Using other shared finite resources
  – Reassembly buffers
  – ...
• Other censorship
  – DNS
  – DPI
  – ...

SpookyScan

Spooky scanning at a distance
http://spookyscan.cs.unm.edu
Censorship Scan

Server: 85.25.208.201
Port: 443
Client: 124.42.54.88

Submit or choose a different type of scan.

Help

- For server and port, specify the service you want to test.
- For client, specify a machine in the region you would like to test with a globally incrementing IP id.
SpookyScan

SpookyScan - View - Mozilla Firefox

Viewing z-yUntNEAu4DSgMdhM9Q Ig

Type: Censorship Scan
Request time: 2013-07-26 12:50:52.205593+00:00
Server: 85.25.208.201
Client: 124.42.54.88
Port: 443
Scanning status: Queued
Queue position: 0

Bookmark this URL, or otherwise you will lose it!

Note: This scan will be automatically deleted one week after it is finished. Delete scan now.
Viewing z-yUntNEAu4DSgMdhM9Qlg

Type: Censorship Scan
Request time: 2013-07-26 12:50:52.205593+00:00
Server: 85.25.208.201
Client: 124.42.54.88
Port: 443
Scanning status: Finished
Result: SYNACK's are filtered from server 85.25.208.201 to client 124.42.54.88 on port 443

Debug output

Bookmark this URL, or otherwise you will lose it!

Note: This scan will be automatically deleted one week after it is finished. Delete scan now.
Acknowledgments

This material is based upon work supported by the U.S. National Science Foundation under Grant Nos. 0844880, 0905177, and 1017602.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. National Science Foundation.