DNS Based Censorship

ISMA 2013 AIMS-5

John-Paul Verkamp
Indiana University
Motivation

● 73 out of 202 countries are rated highly in censorship; roughly 1/3-1/2 of those use DNS based censorship

● In several cases, there is fallout in neighboring countries

● Results vary widely:
  ○ resolve to a warning page server
  ○ resolve to localhost
  ○ resolve to a (random) currently unused IP
Technical details

- Direct control of DNS resolvers
- Cache poisoning
- In-flight modification / packet injection
How do we find it?

- **Open resolvers:**
  - Maintain a list of all of the open DNS resolvers we can find
  - Query by country, validating locally (using either SSL certificates or matching DNS results)
  - Future work: use PlanetLab to control for geographic bias

- **Passive DNS data:**
  - ISC/SIE passive DNS data
  - Raw data is about 1GB/10 minutes, so processing needs some work
  - Few (if any) data taps are in countries of interest
What are we looking for?

- Many domains resolving to a single IP (potential warning site or malware)
- One domain resolving to many diverse IPs (potential randomized results)
- Any domains resolving to localhost / local addresses
Preliminary results - China

- ~90% of the address space acts as a resolver for Facebook and Twitter,
  - Most do not respond to anything else
  - The Great Firewall itself is acting as a resolver

- Returned a static set of ~10 IPs
  - Two (different) DNS responses are sent back

- Seemingly randomly generated, none of them respond to HTTP traffic

<table>
<thead>
<tr>
<th>8.7.198.45</th>
<th>78.16.49.15</th>
</tr>
</thead>
<tbody>
<tr>
<td>37.61.54.158</td>
<td>93.46.8.89</td>
</tr>
<tr>
<td>46.82.174.68</td>
<td>159.106.121.75</td>
</tr>
<tr>
<td>59.24.3.173</td>
<td>203.98.7.65</td>
</tr>
<tr>
<td>243.185.187.39</td>
<td>127.0.0.1</td>
</tr>
</tbody>
</table>
Preliminary results - South Korea

● In one /24:
  ○ Over 1000 open resolvers
  ○ korea-dpr.com redirects to 121.189.57.82 (a warning page) at ~20% of open resolvers

● In another /24:
  ○ Only 18 open resolvers
  ○ Three went through the Great Firewall, resulting in the same IPs for Facebook and Twitter as before
Data Sharing

- Make the list of open resolvers available to other researchers
  - It takes a not-insignificant amount of time to generate

- Publish lists of countries where DNS based censorship is occurring to help in anti-censorship research
What do I hope to get out of AIMS-5?

- Contact with other people doing similar research
- Insight into tools and datasets that I would never otherwise have thought to look for
Questions?