Update: A Survey of Worldwide Censorship Techniques

Joseph Lorenzo Hall, Michael Aaron, Nick Feamster, Ben Jones

July 21, 2017

History and Motivation

Link to current -04 draft: draft-hall-censorship-tech-04

- Presented rough draft at IETF 91 in Hawaii at SAAG
- Motivation: reference for protocol spec authors and implementers on technical censorship methods
- Great feedback, changes since then:
  - Worked through a series of issues (link) that have improved the substance and structure
  - Many thanks to Stephane Bortzmeyer and Martin Nilsson
- IAB pushed out RFC7754 on technical considerations in filtering and blocking

Important Changes

- General terminology clearer:
  - Old: "Aggregation, Identification, Prevention"
  - New: "Prescription, Identification, Interference"
- Added Services, CAs, CDNs as points of control
- Removed a statement that implied Swiss TLD `.ch` censors
- Many changes to DNS interference:
  - Clarified cache poisoning (censor replies to a query from a cache before real authoritative)
  - Added "mangling" (network-level misresponse to stub)
  - Added "lying" (recursive resolver returns mandated response; doesn't check authoritative)

What Next?

- A number of TODOs left in the doc
  - Identification section is new organized in a layered manner, Interference section should be too
- This is a very dynamic space. How to keep it current?
- Want to get more areas' eyes on this (Routing, Apps)
- Would benefit from the IETF process. Security AD sponsorship as Informational?
- Are there other informational reference documents that might be useful to the IETF security community? (traffic analysis?)