DNS-sly: Avoiding Censorship through Network Complexity



Qurat-Ul-Ann Akbar, Northwestern U.
Marcel Flores, Northwestern U.
Aleksandar Kuzmanovic, Northwestern U.

http://networks.cs.northwestern.edu

Internet Censorship is a prevalent problem



By DANIEL SIEBERG / CBS / January 31, 2011, 6:30 PM

How Egypt Pulled the Plug on the Internet

Comment / 1 Share / Tweet / Stumble / @ Email

NEW YORK - The uprising in Egypt is a quintessential 21st century event - born on Facebook and other social networking sites - which led the government to cut off Internet service.

BUSINESS INSIDER

9 incredibly popular websites that are still blocked in China



BIZ CARSON
JUL. 23, 2015, 2:54 PM



he Plug on

ail

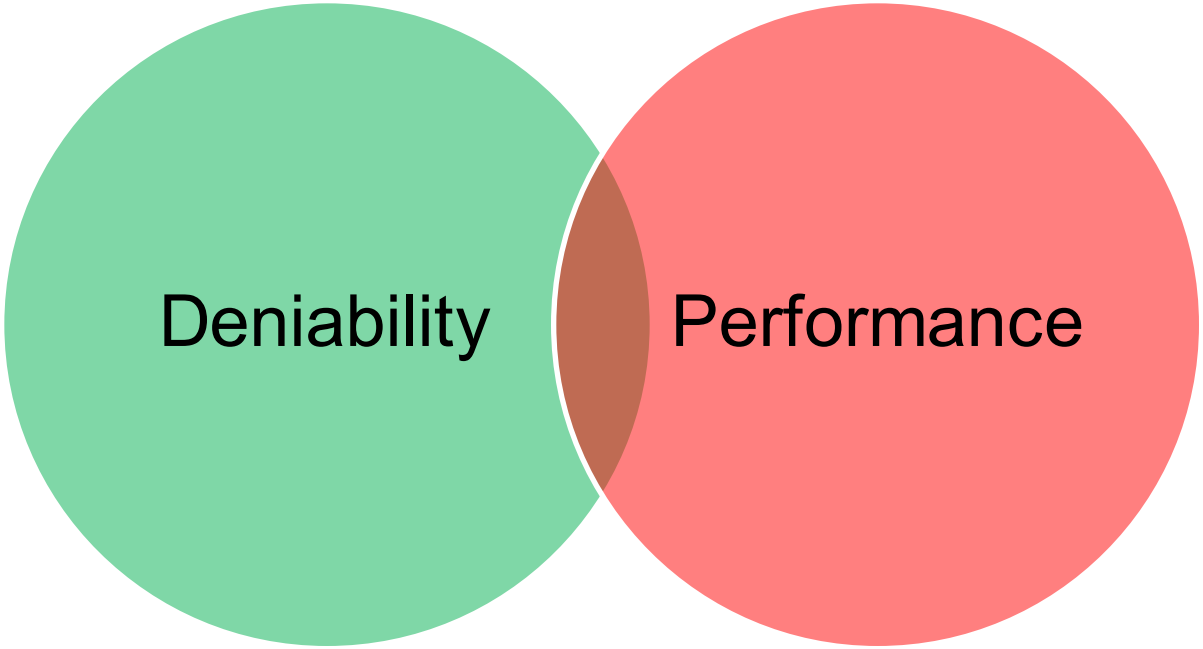
al 21st century event - born
h led the government to cut

Circumvention Techniques

Circumvention Technique	Covertness	Deniability	Performance
Proxies	Yes	No	High
Anonymous Networks	Yes	No	High
DNS Tunneling Techniques	Yes	No	High
HTTP Tunneling Techniques	Yes	Statistical Deniability	Low

Research Problem

Can we create a circumvention technique with high deniability with minimum impact on performance ?



Our Solution

- DNS is a core Internet service
- Significant network complexity in todays Internet
  - Trillions of DNS requests per day
  - Proliferation of public DNS servers
  - CDNs
- Leverage this complexity in DNS traffic to hide information

Outline

- Motivation
- DNS-sly Protocol
- Case for DNS-sly
- Evaluation

DNS-sly Overview

- Components : DNS-sly requester and responder
- DNS-sly responder **profiles** the clients DNS behavior
- **Exchanges** profile information with the requester
- In the downstream direction, responder **encodes** the content from the ‘censored website’ in DNS response packets

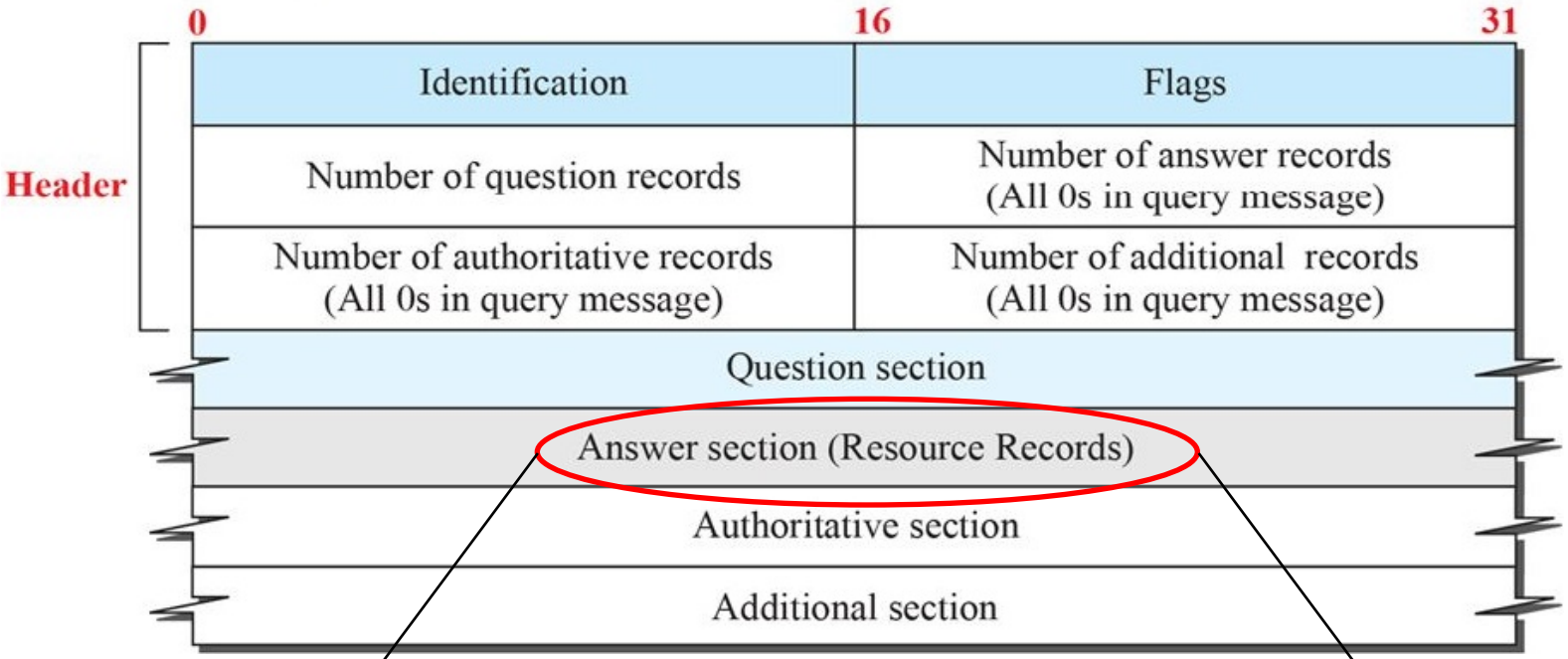
First Phase - Endpoint Profiling

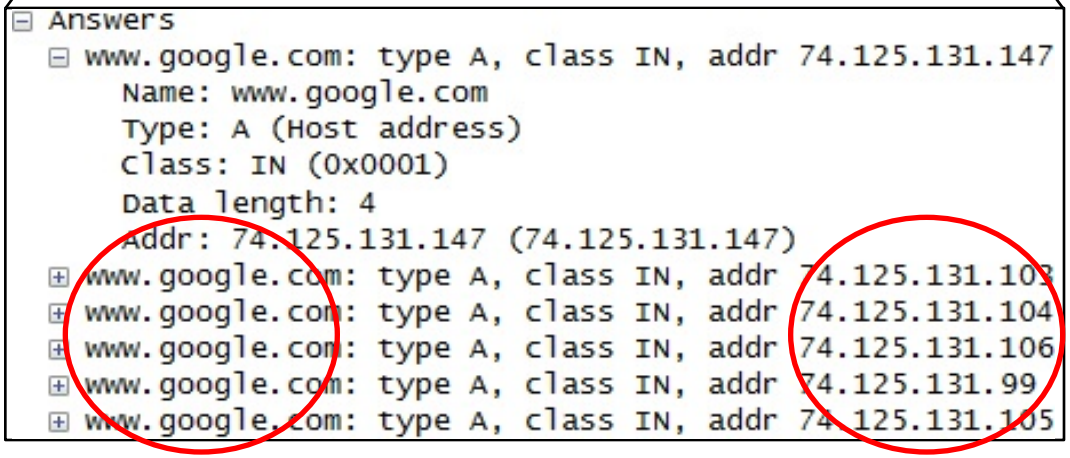
- DNS-sly responder profiles clients DNS behavior
  - Records domains
  - Forms IP set per domain
- Creates profile map – a mapping of domains to the server IPs they are hosted on
- Exchanges profile map with the requester via out-of-band communication

Second Phase - Communication

- In the upstream direction, the DNS-sly requester crafts DNS requests using the profile map
- Upon receiving the request, the responder retrieves the content from Web
- In the downstream direction, the DNS-sly responder encodes content using DNS responses

DNS Packet Format





Domain

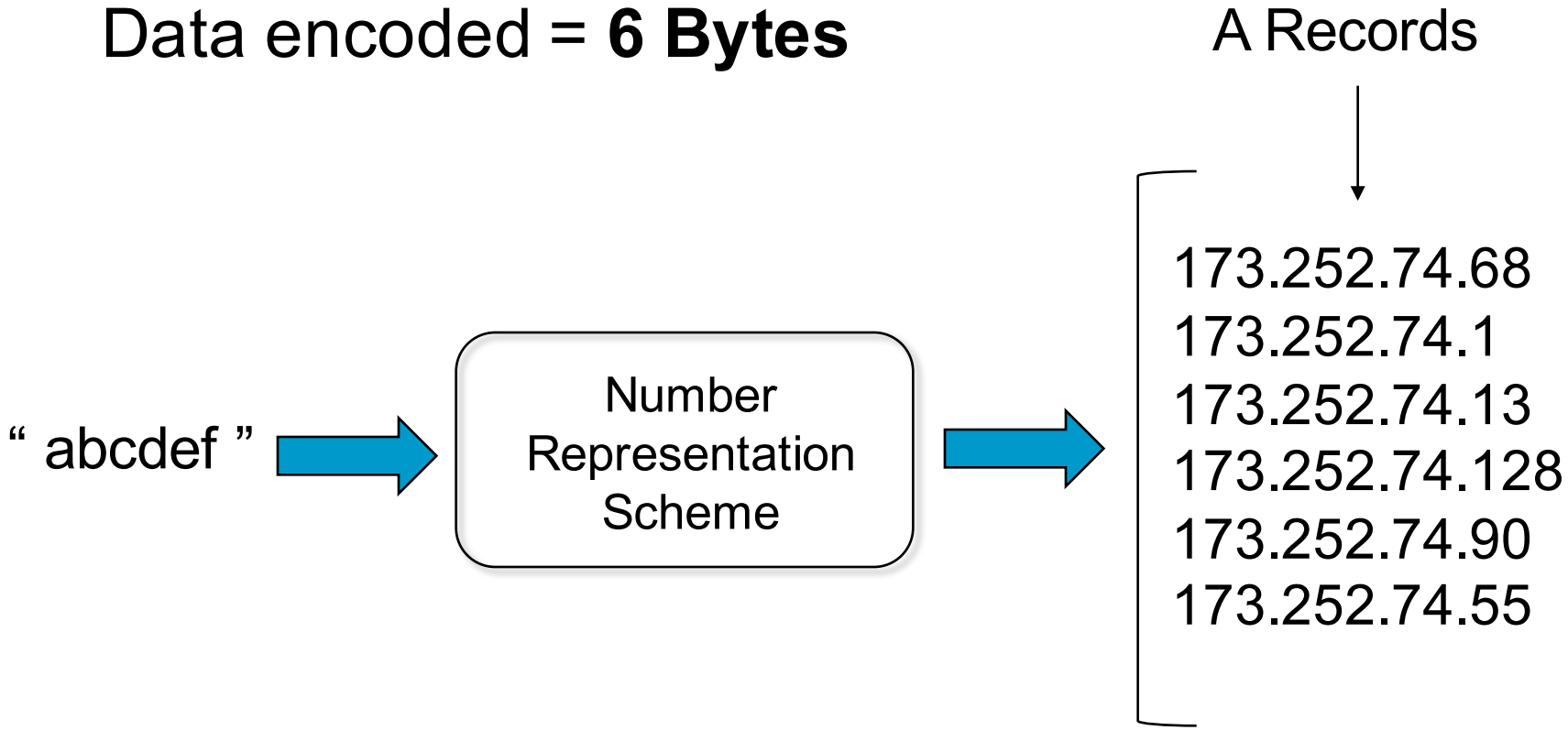
Associated IP addresses

Encoding Data

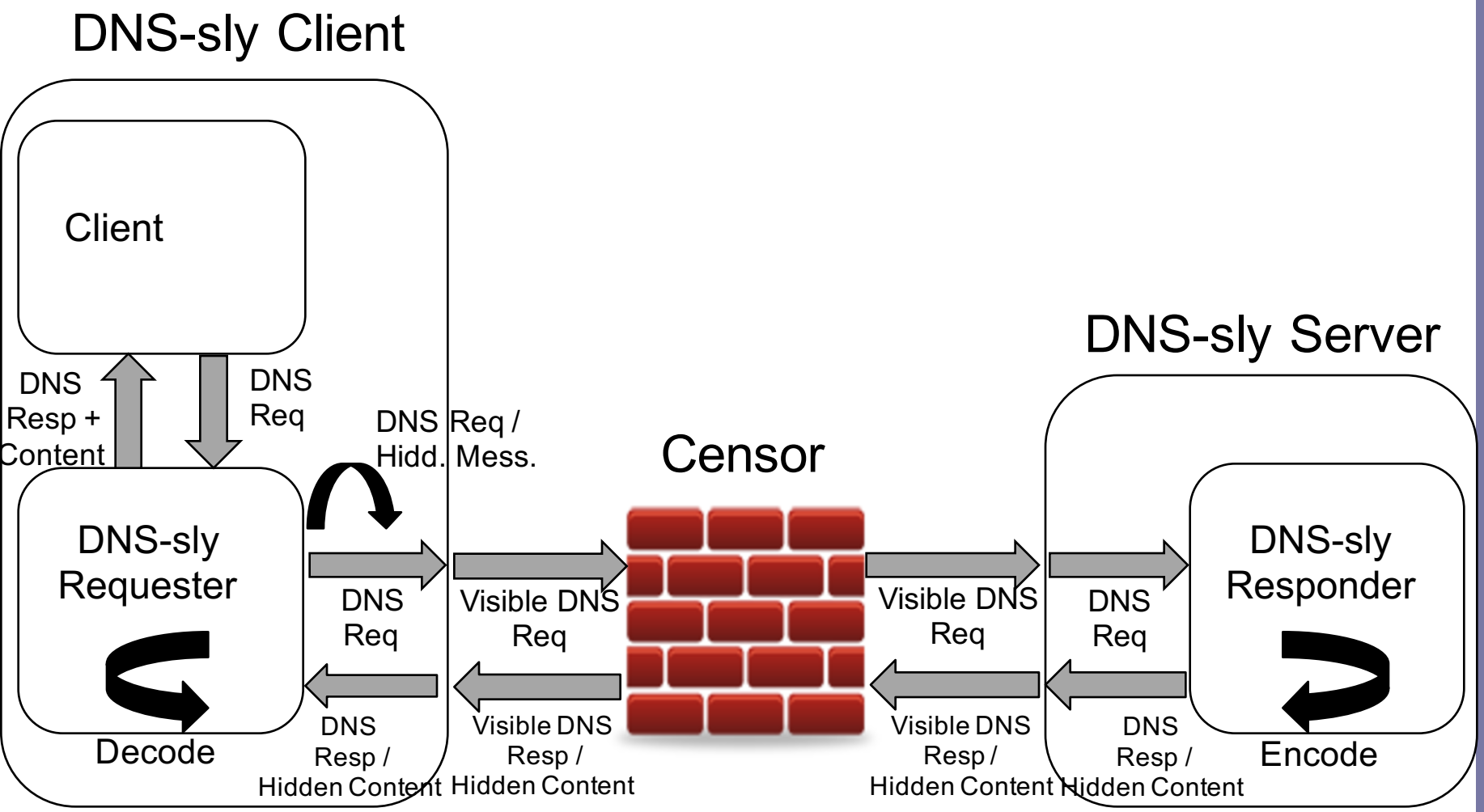
- Goal - Represent data as a choice of A records from a pool of IP addresses
- Responder computes the number of bytes of data to be encoded
- Uses a number representation scheme to map data to a set of IP addresses
- Forms a valid DNS response and sends it back to the DNS-sly requester

Encoding Data - Example

Domain = “ facebook.com ”
IP set size = **256**
Number of A records = **6**
Choices ~ P(256,6)
Data encoded = **6 Bytes**



System Overview



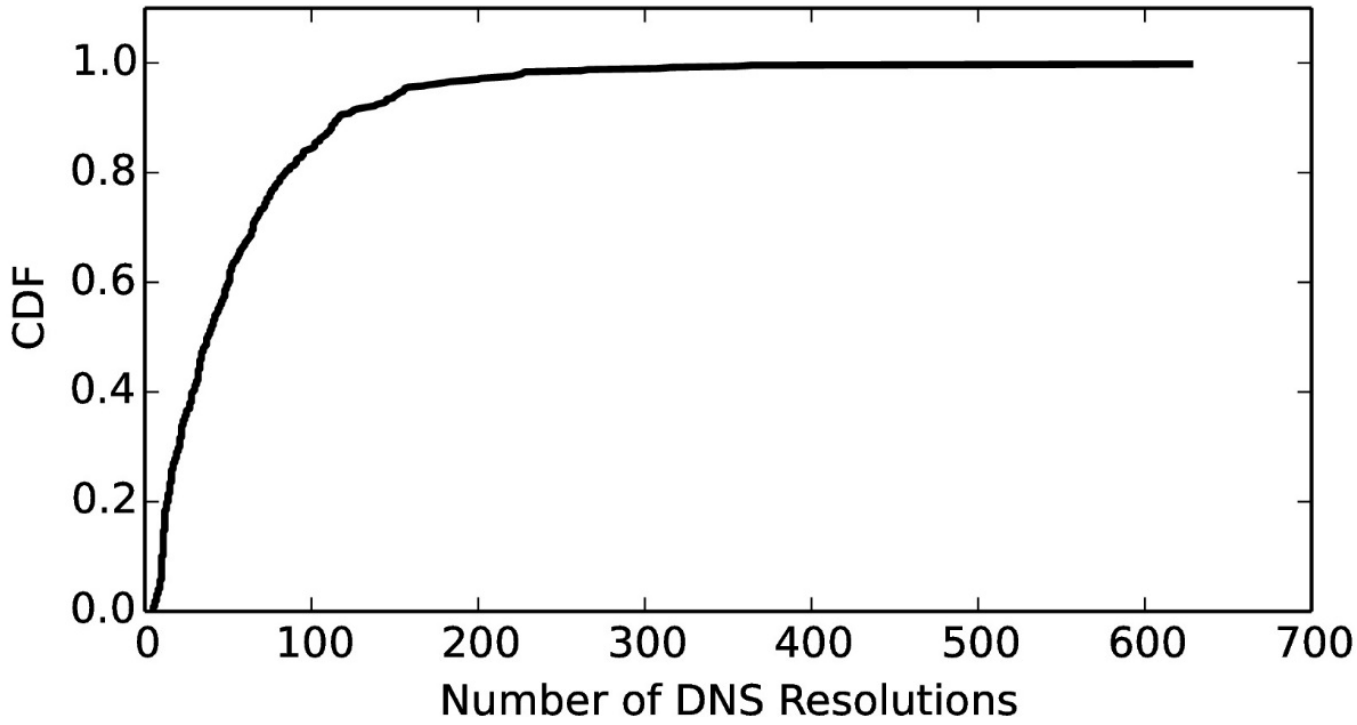
Outline

- Motivation
- DNS-sly Protocol
- Case for DNS-sly
- Evaluation

DNS Request Variability

- Fragmented Web pages
- Larger number of DNS requests better for deniability:
  - DNS-sly requests hard to detect
  - Leads to increased probability of DNS responses suitable for data encoding

Number of DNS Resolutions per Domain



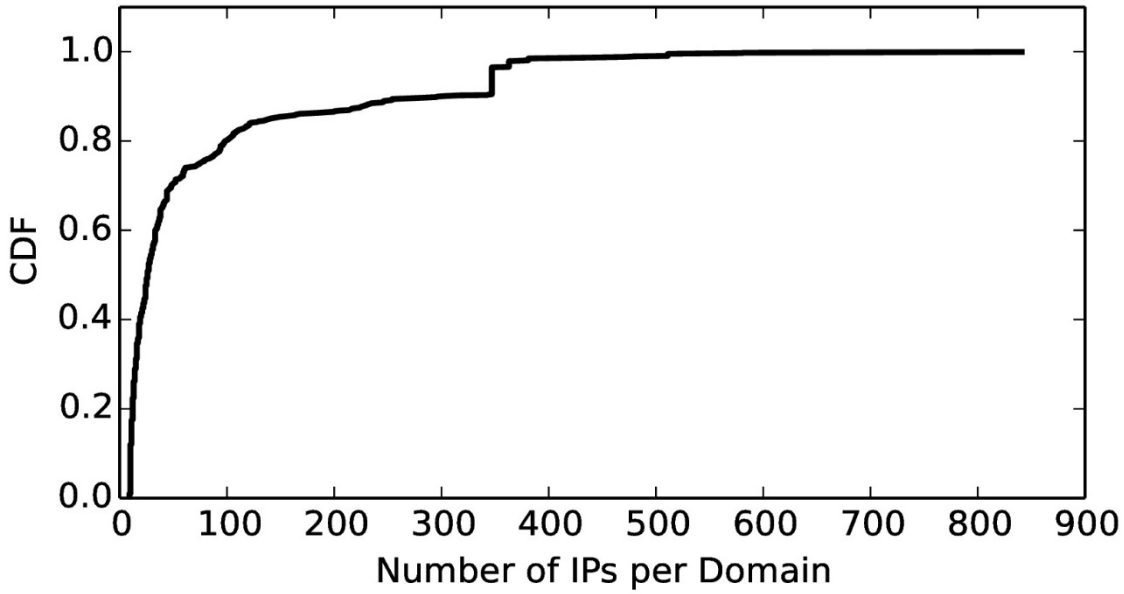
Median is **~50** DNS resolutions per domain

20% of domains have **>90** DNS resolutions

DNS Response Variability

- Number of IP addresses a domain maps to determines the potential for encoding downstream data
  - Global and local
- Number of A records determines data that can be embedded in a single DNS response
- Rate of change in A records determines the timescales at which to operate to retain statistical deniability

Experimental Results



Maximum number of IPs a domain maps to is **850**

~ 1/3rd of DNS responses have **8 A records** with maximum up to **15**,

Every **30 minutes** the responses change completely

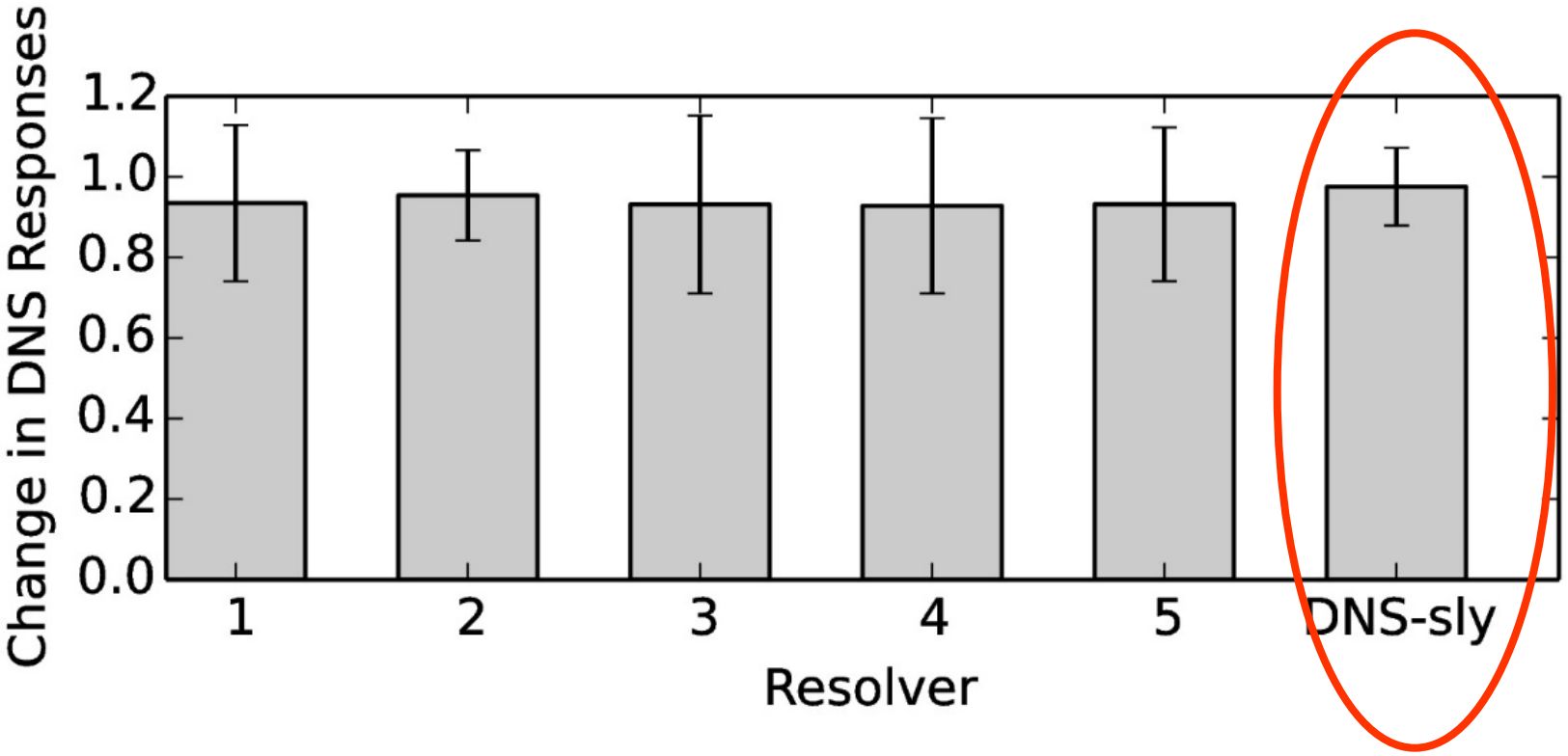
Outline

- Motivation
- DNS-sly Protocol
- Case for DNS-sly
- Evaluation

Security Evaluation: Methodology

- Emulated a censors probing attack
- For every response from a DNS-sly responder, queried five other DNS resolvers for the same domain
- Evaluated by computing the mean and variance of the change between the DNS responses

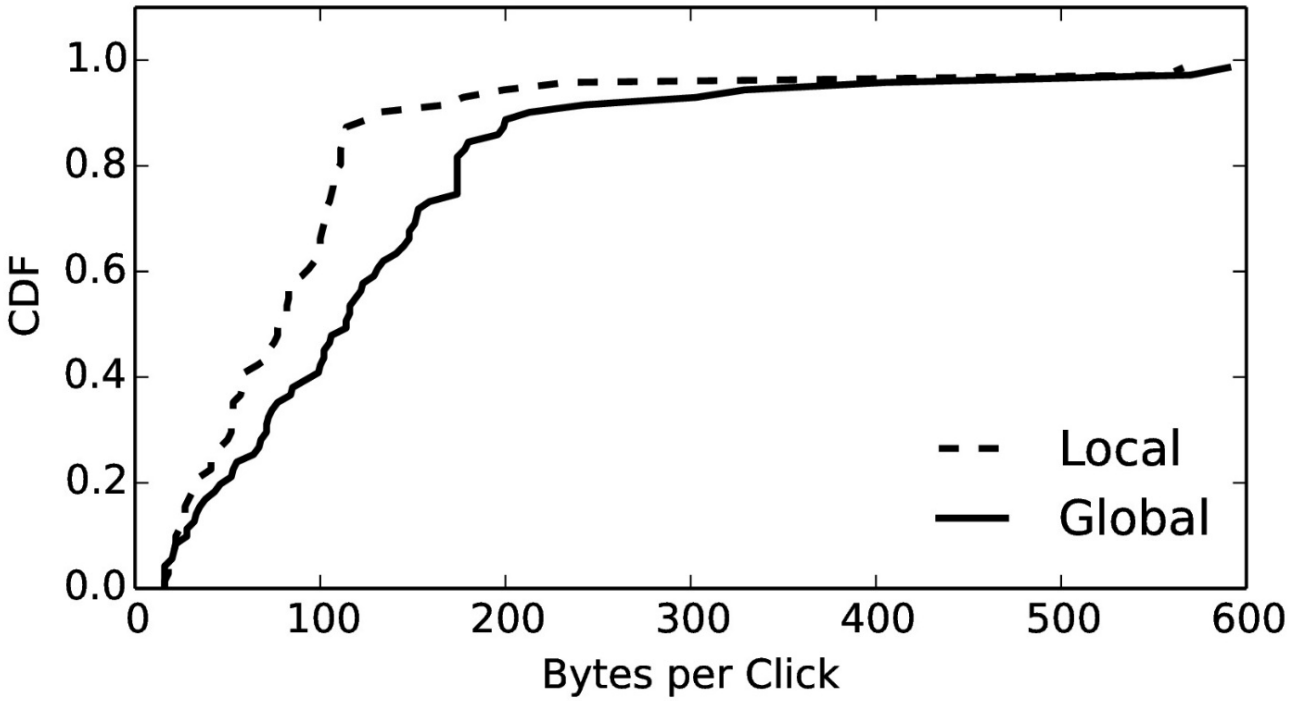
Security Evaluation: Results



Performance Evaluation: Methodology

- Evaluated downstream performance using the metric, *bytes per click*
  - Single *click* defined as loading of a page, including DNS resolutions for all domains included on the page
- Deployed DNS-sly in a known-censored environment to exchange data from a known-censored website

Performance Evaluation: Results



Median Page Click (global) > **100 Bytes**

Median Page Click (local) ~ **75 Bytes**

Maximum Bytes encoded ~ **600 Bytes**

Conclusion

- DNS-sly: a system that enables a DNS covert channel which provides high deniability while maintaining good performance
- DNS-sly adjusts its behavior to the clients
- Utilizes frequently changing A records to embed data in DNS responses
- Achieves downstream throughput of upto 600 Bytes of hidden data per Web page click

Thank You



http://networks.cs.northwestern.edu