Comments on DNS Robustness
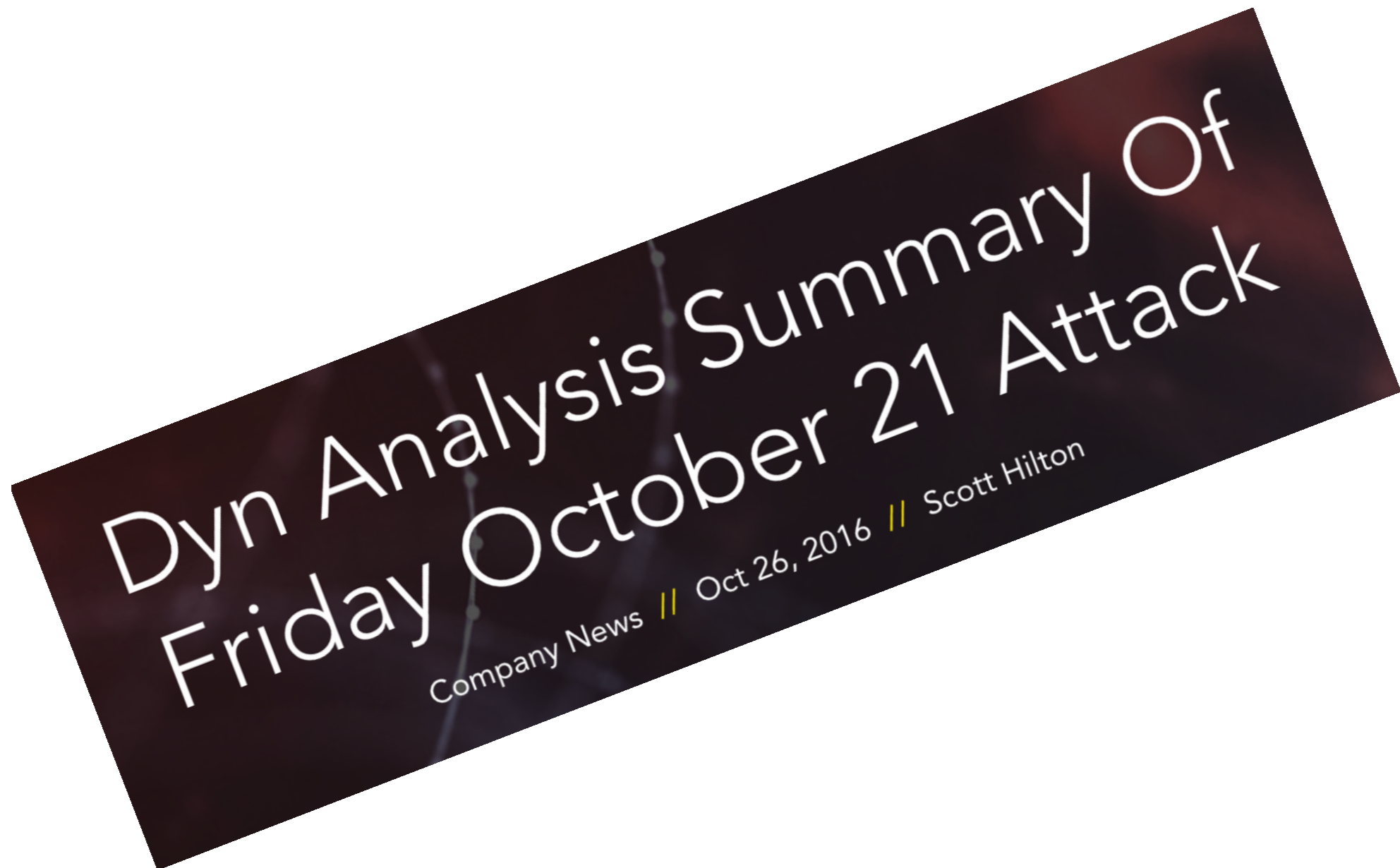
Mark Allman
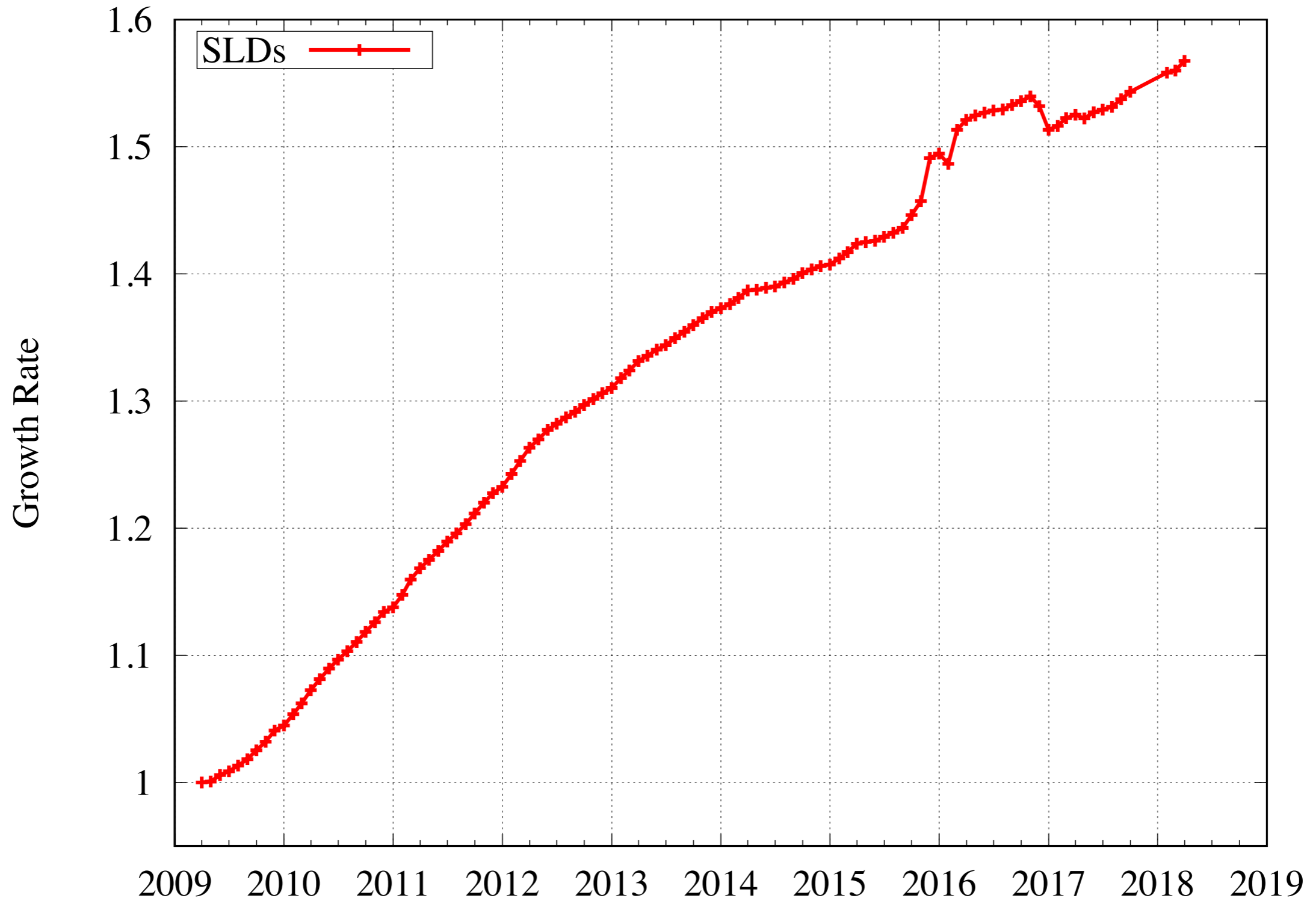*International Computer Science Institute*

ACM Internet Measurement Conference
November 2018
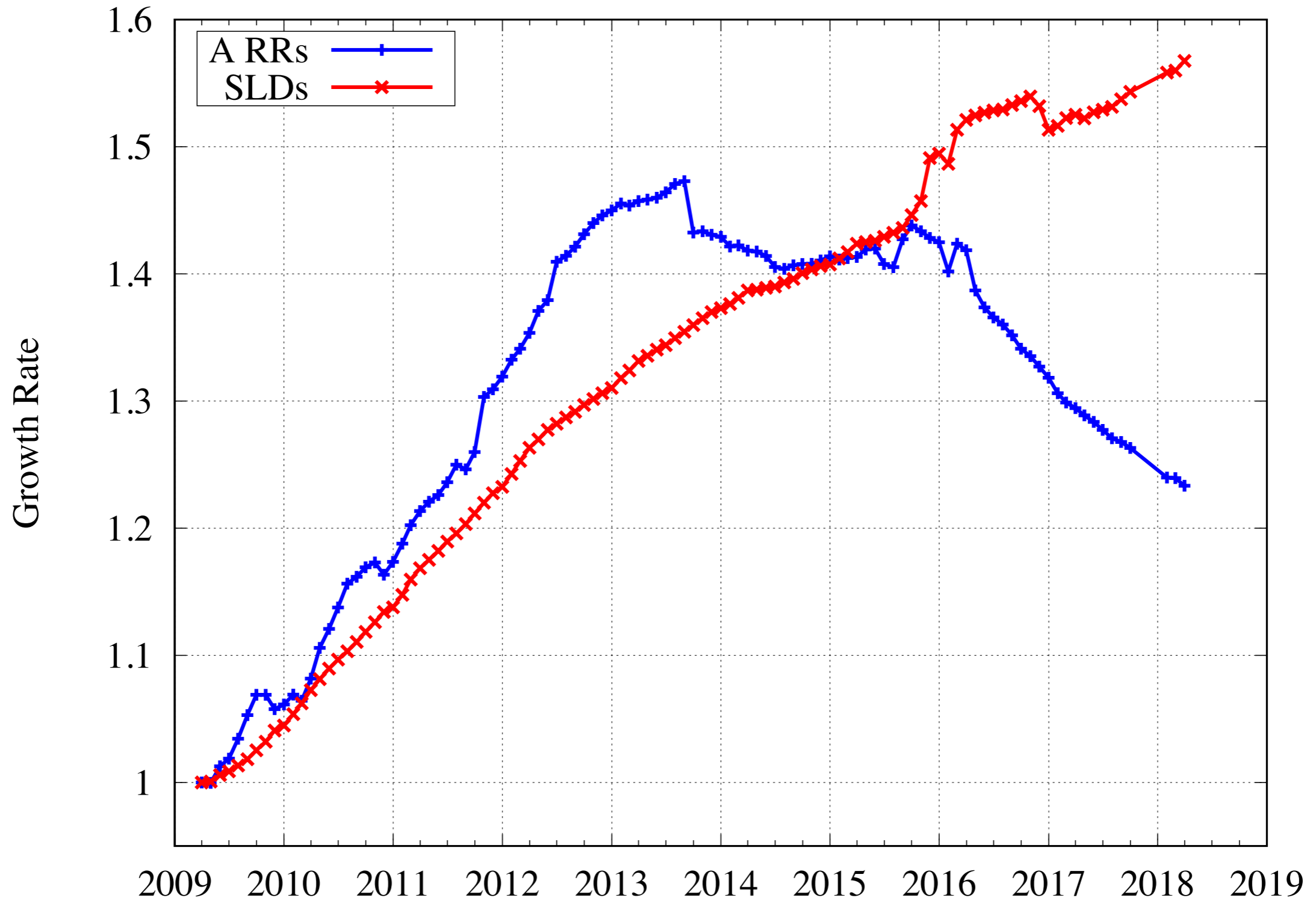
Observation #1

Dyn Analysis Summary Of Friday October 21 Attack

Company News || Oct 26, 2016 || Scott Hilton
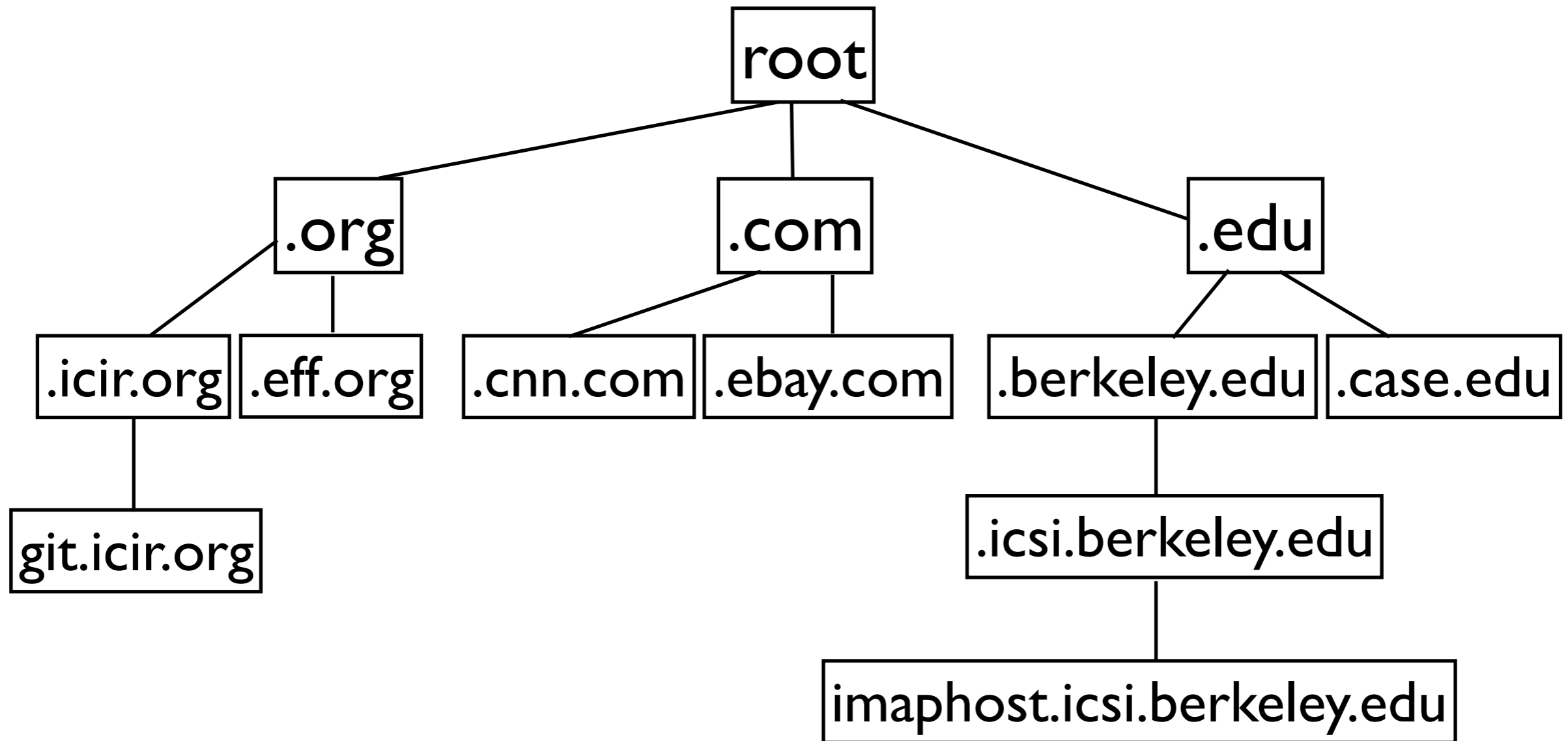
Observation #2
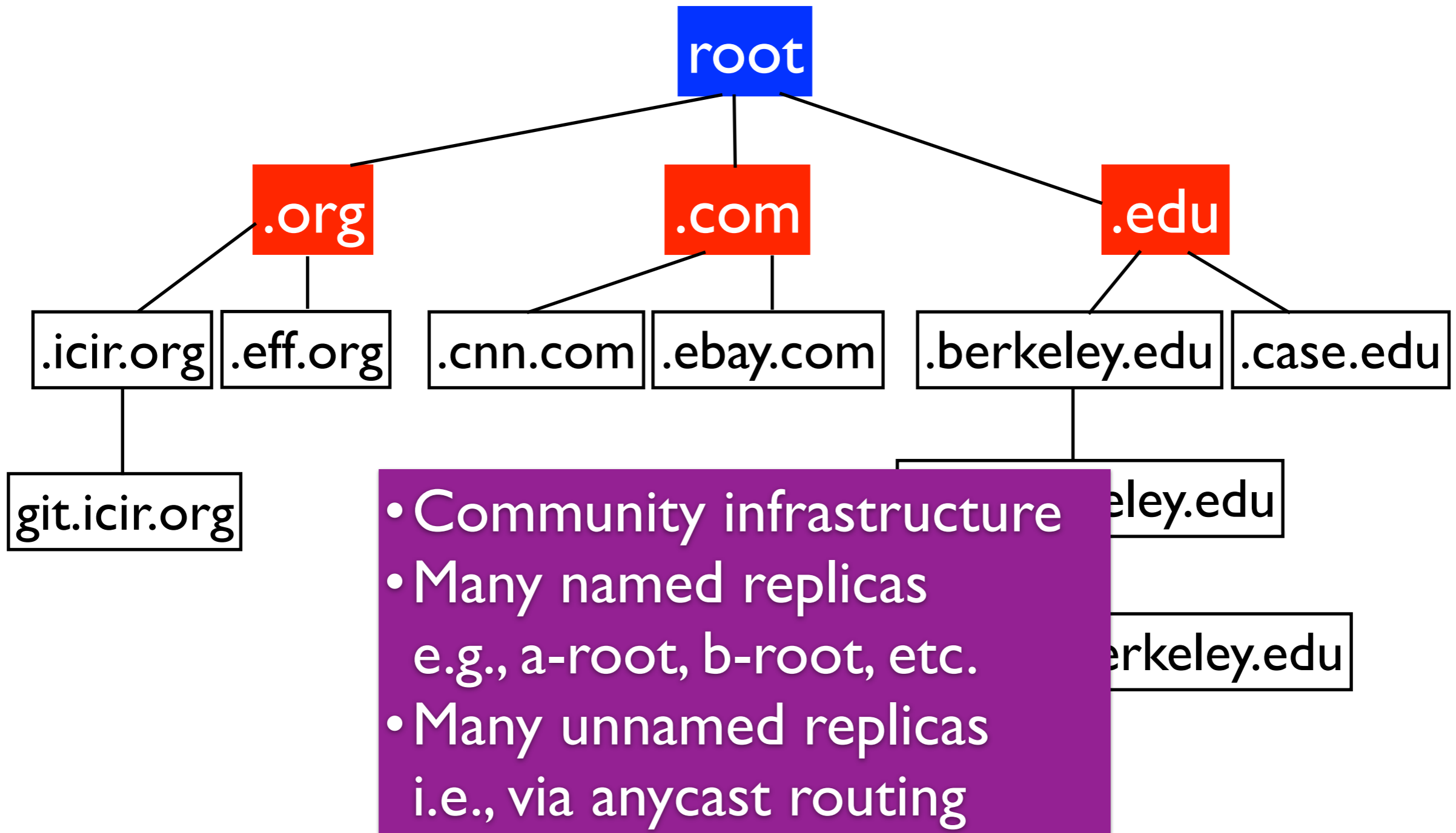
Observation #2

How Robust Is DNS?

- What do we mean by "robust"?

  - many dimensions

- Our focus: can we *always* communicate with an auth server holding the DNS record we seek

DNS Robustness

Allman

DNS Robustness

root

.org .com .edu

.icir.org .eff.org .cnn.com .ebay.com .berkeley.edu .case.edu

git.icir.org

...eley.edu

...erkeley.edu

- Community infrastructure
- Many named replicas
  e.g., a-root, b-root, etc.
- Many unnamed replicas
  i.e., via anycast routing

7

DNS Robustness

```
                         ┌──────┐
                         │ root │
                         └──────┘
            ┌───────────────┼───────────────┐
        ┌──────┐        ┌──────┐        ┌──────┐
        │ .org │        │ .com │        │ .edu │
        └──────┘        └──────┘        └──────┘
        ┌───┴───┐       ┌───┴───┐       ┌───┴───────┐
```

| .icir.org | .eff.org | | .cnn.com | .ebay.com | | .berkeley.edu | .case.edu |

```
    │
┌─────────────┐
│ git.icir.org│
└─────────────┘
```

.icsi.berkeley.edu
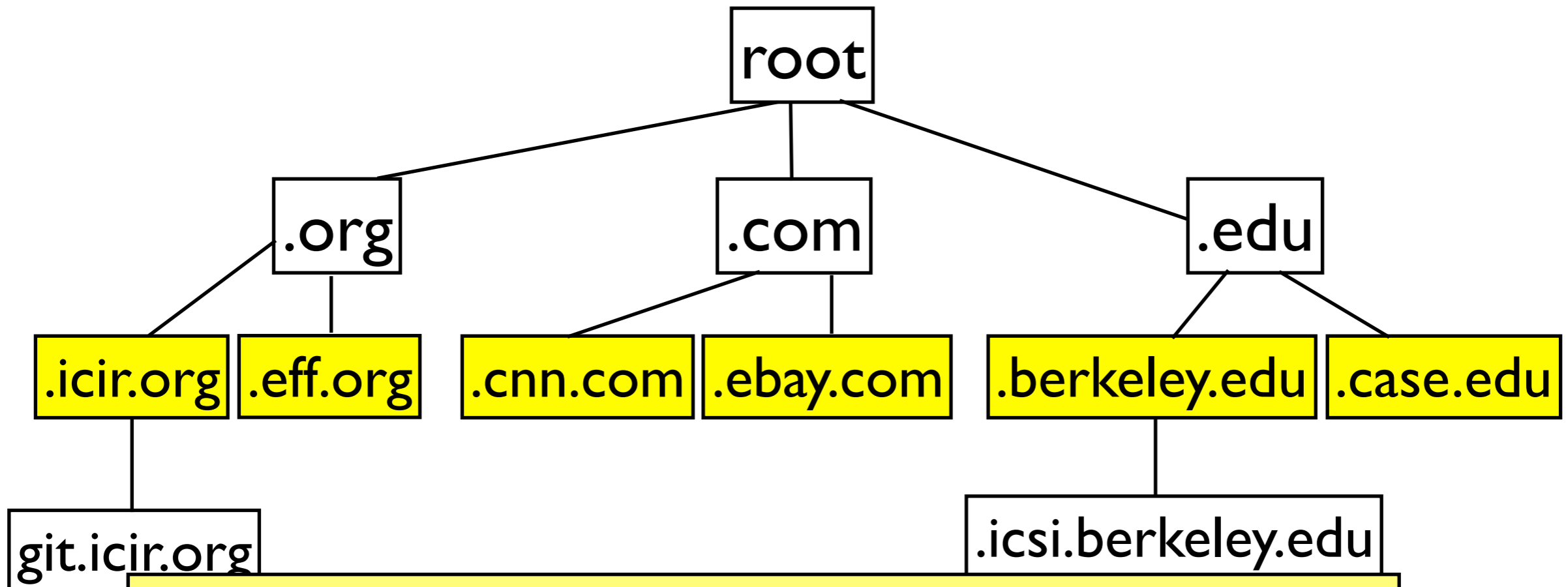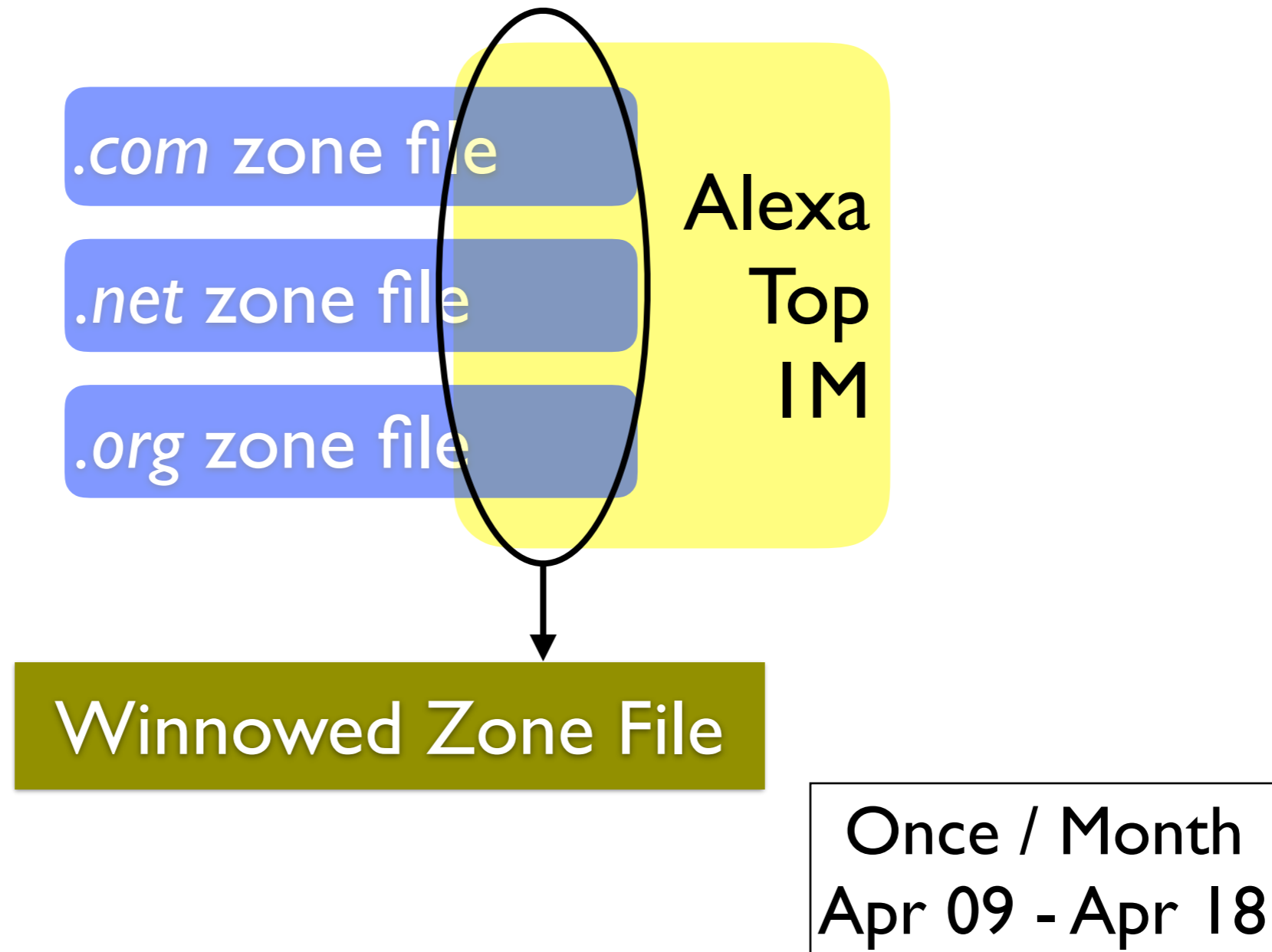
- Few named replicas
  ~80% of SLDs have <= 2 named auth servers
- Unknown / variable use of anycast replicas
- Myriad operators / policies

8

How Robust Is DNS?

- Let's measure some facets of the system at the SLD level that bear on robustness

Datasets

.*com* zone file

.*net* zone file

.*org* zone file

Alexa
Top
1M

Winnowed Zone File

Once / Month
Apr 09 - Apr 18

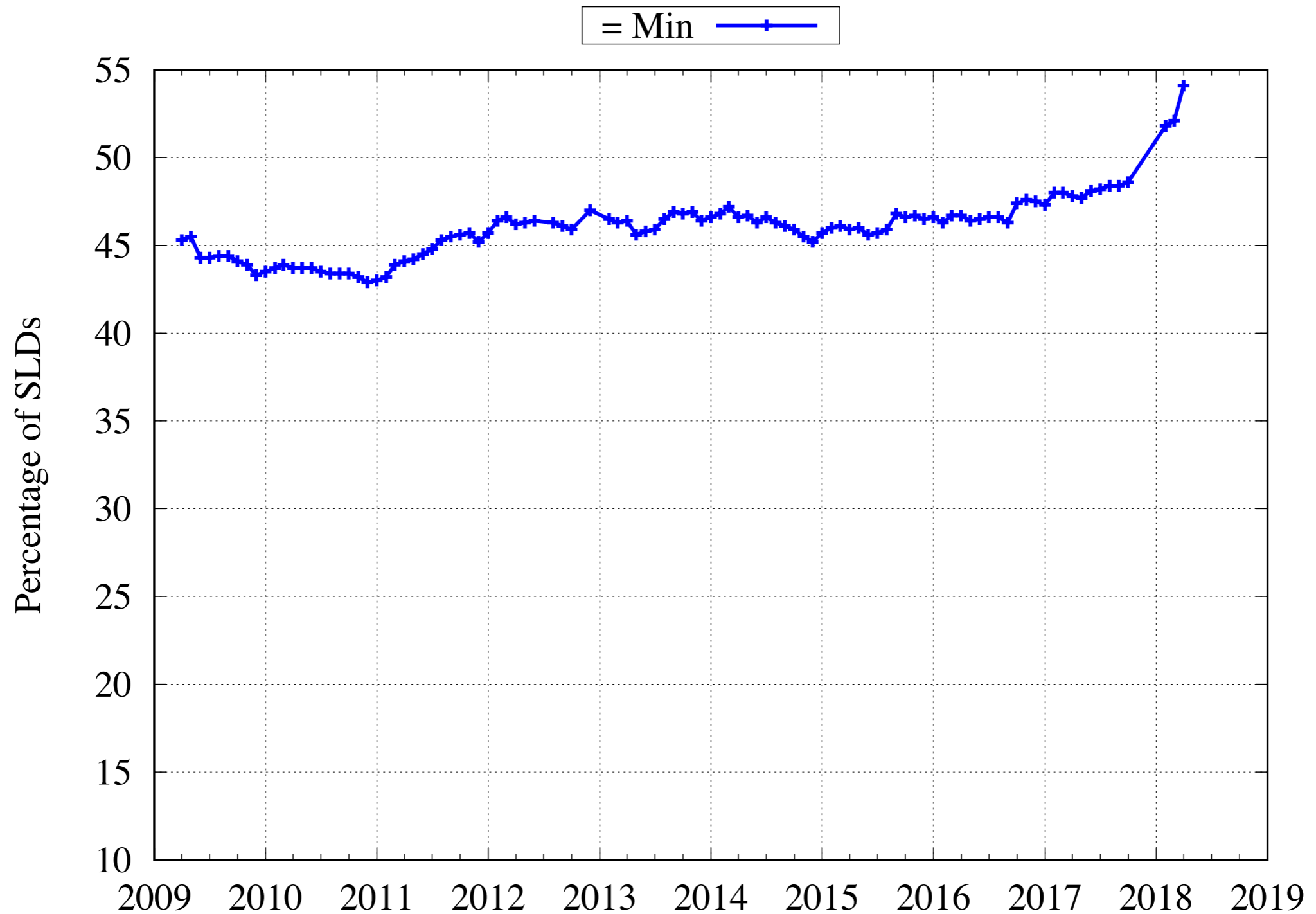Data courtesy of Verisign, Alexa, Emile Aben (RIPE) and Quirin Scheitle (TUM)

Robustness Specifications

- RFC 1034: must have multiple authoritative nameservers for robustness

- RFC 2182: authoritative nameservers must be geographically and topologically diverse
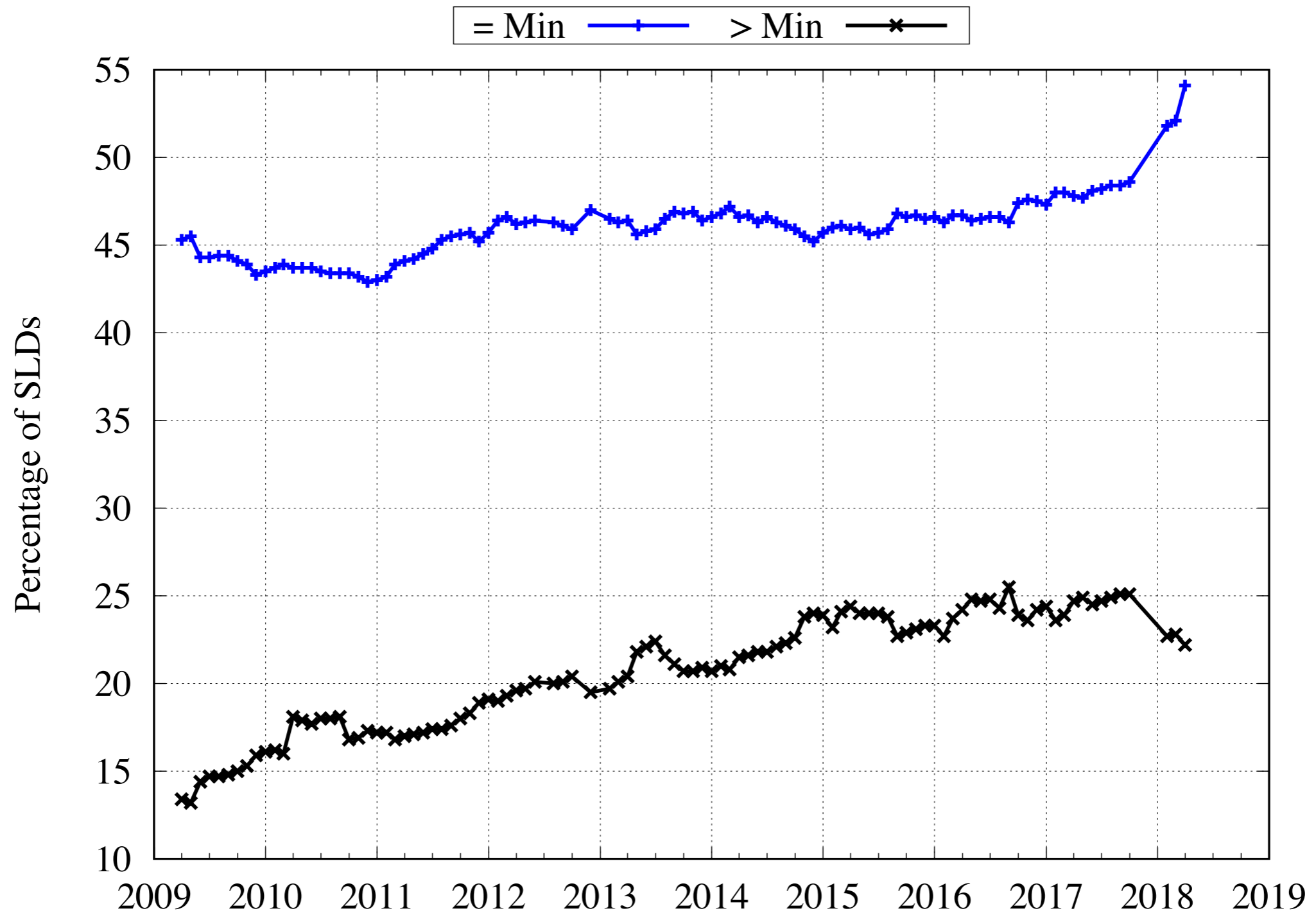
What Is Network Diversity?

- We start cheap & conservative:

  - use /24 address blocks to define diversity

  - two addresses in one /24: no diversity

  - two addresses in two /24s: diversity
    (but, really, who knows?!)

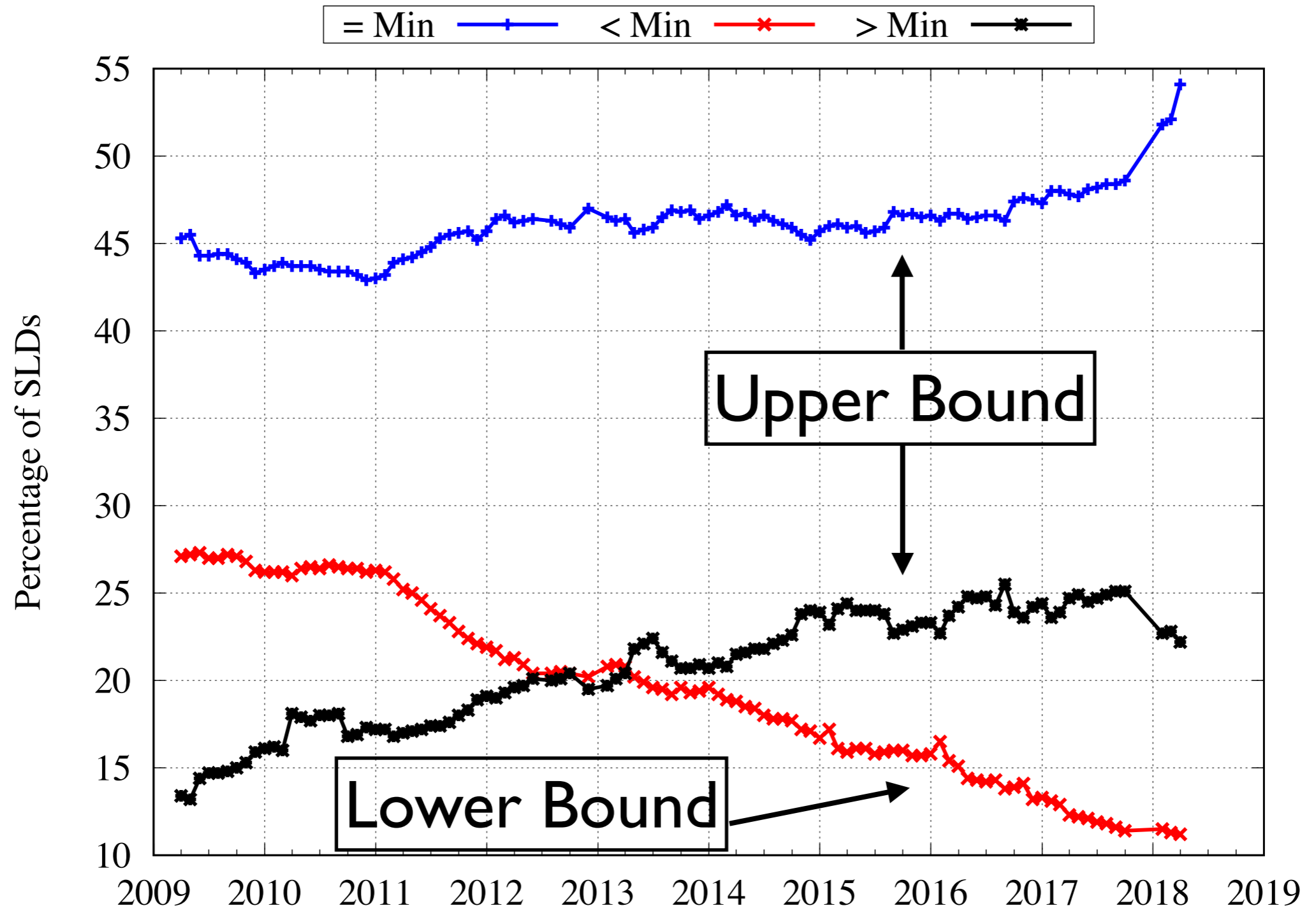- Future work includes using historical routing data

Allman

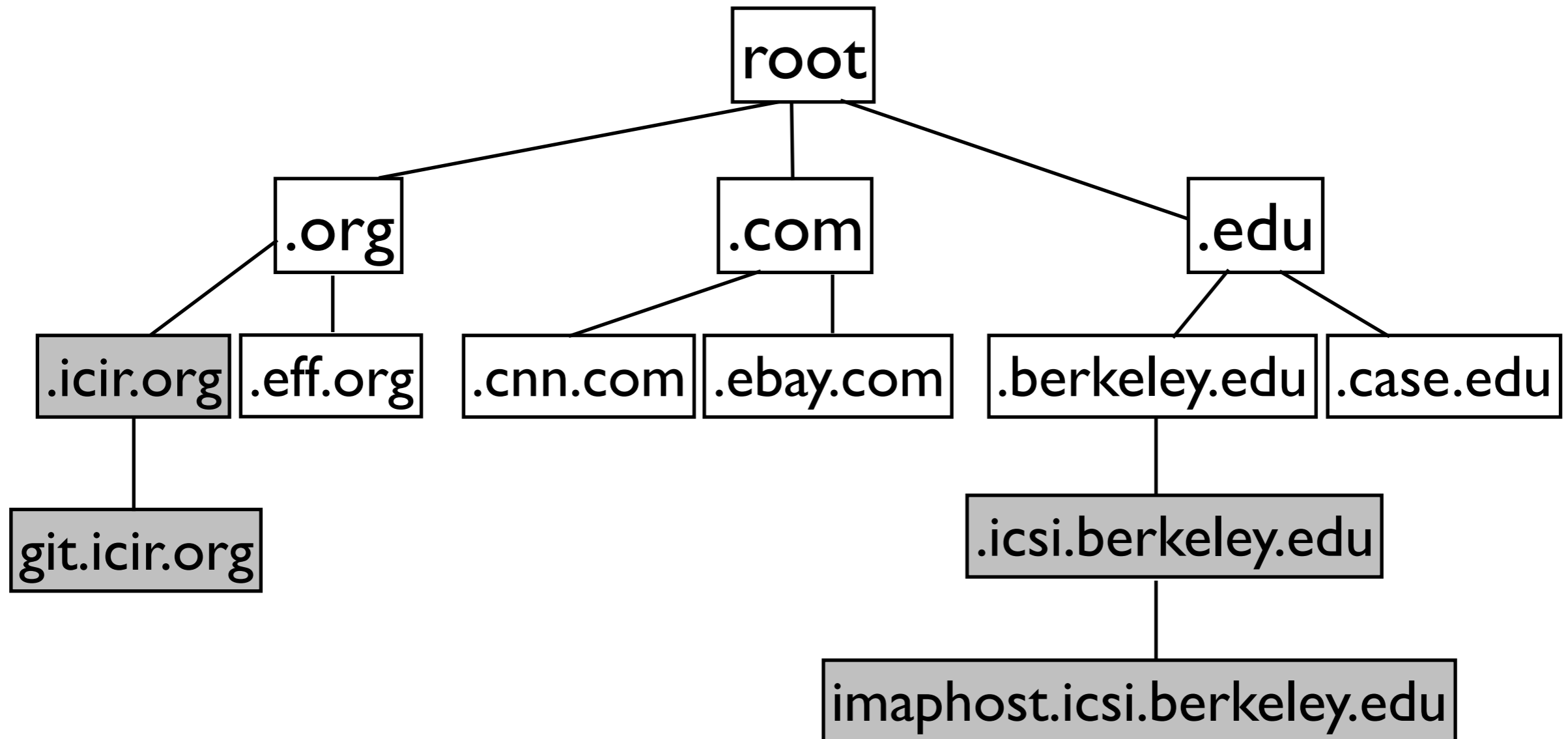# Spec. vs. Reality

Spec. vs. Reality

Spec. vs. Reality

Shared Infrastructure

root

.org   .com   .edu

.icir.org | .eff.org   .cnn.com | .ebay.com   .berkeley.edu | .case.edu

git.icir.org

.icsi.berkeley.edu

imaphost.icsi.berkeley.edu

- different parts of tree rely on same auth servers
- hierarchy belies (some) concentration
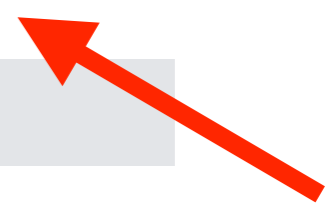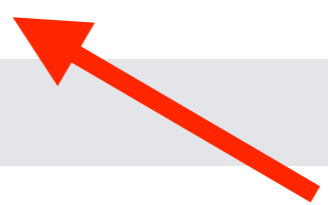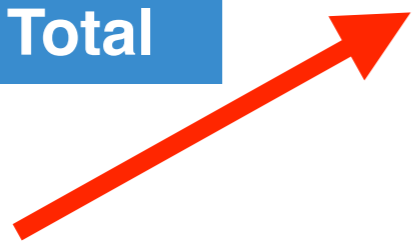
Network-Level Concentration

- For each SLD x determine:

    - determine N_x: set of /24s containing x's nameservers

    - determine number of other SLDs, M_x, relying on same N_x

- Build distribution of M_x across all SLDs

- Repeat for each month in dataset

Network-Level Concentration
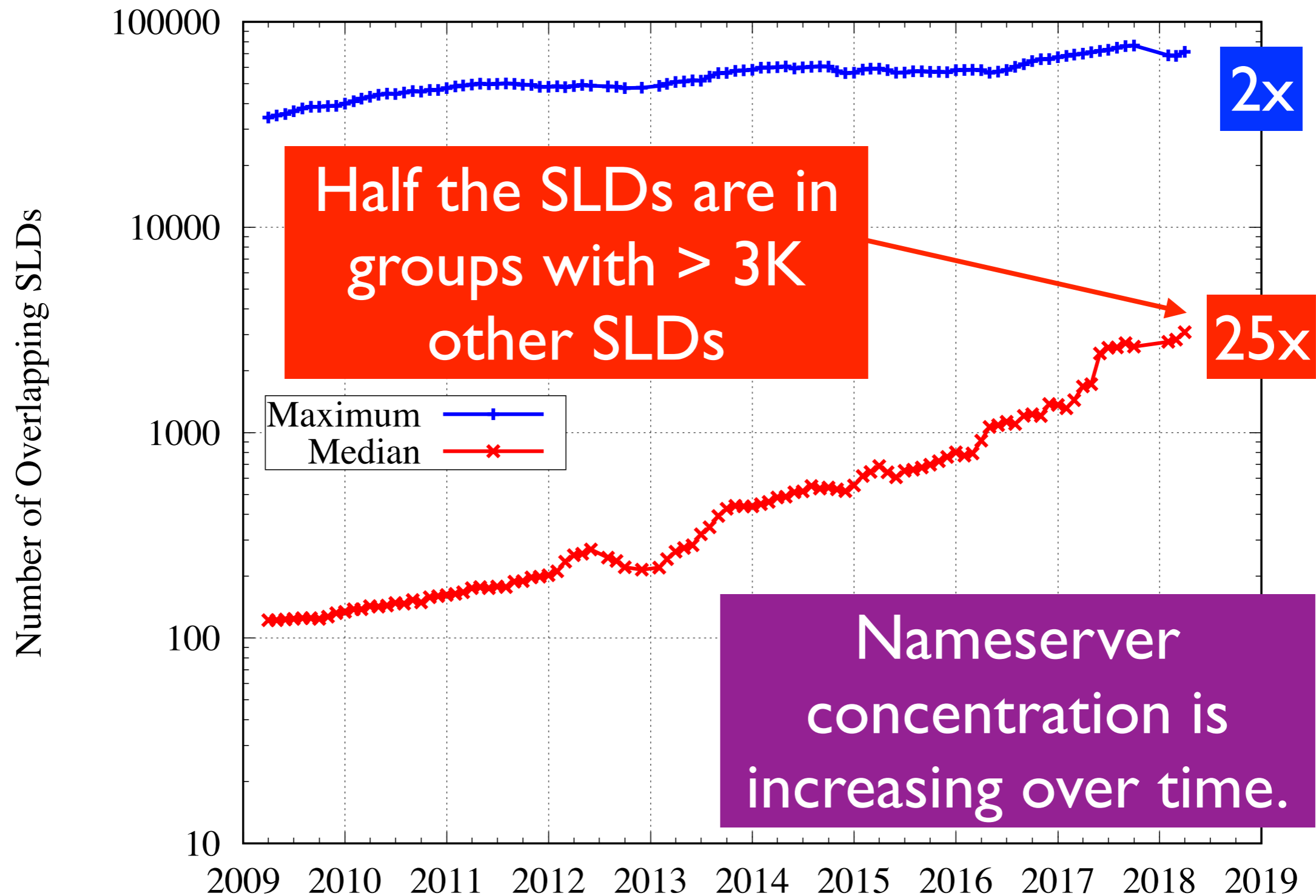
Network-Level Concentration

Rank	Num. SLDs	Num. /24s	Same Last Hop
1	71,472	2	✓
2	69,637	2	
3	15,421	2	✓
4	13,044	2	✓
5	8,347	2	
6	6,111	2	✓
7	5,568	3	✗
8	5,076	2	
9	4,788	2	
10	4,611	4	
Total	204,075		

> 20% of the popular SLDs fall within 23 /24 blocks!

> 20% of the popular SLDs rely on 19 edge networks!

Allman

Summary

- DNS sky is not falling

- But, we have some unhealthy habits …

  - too little auth server replication

  - too much auth server concentration

- More details, analysis, comments in the paper

Questions? Comments?

Mark Allman, *mallman@icir.org*
https://www.icir.org/mallman/
@mallman_icsi