Perils of Transitive Trust in the Domain Name System

Emin Gün Sirer

joint work with Venugopalan Ramasubramanian

Cornell University

How to Own the Internet via DNS

Emin Gün Sirer

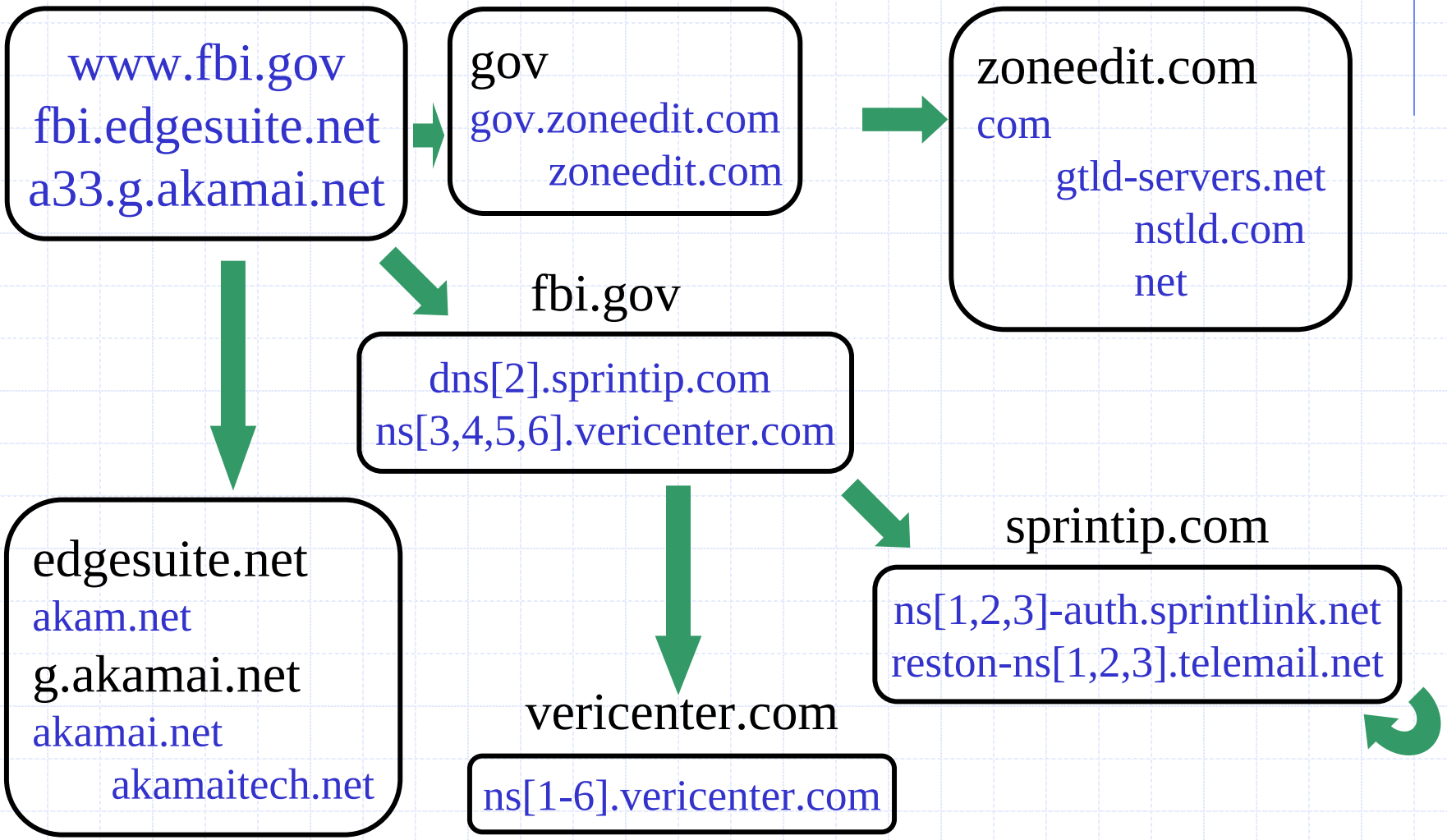
joint work with Venugopalan Ramasubramanian

Cornell University

Introduction

- DNS is critical to the Internet
- DNS architecture is based on delegations
  - Control for names is delegated to name servers designated by the name owner
- Delegations decentralize administration and improve fault tolerance
  - But create a dependence

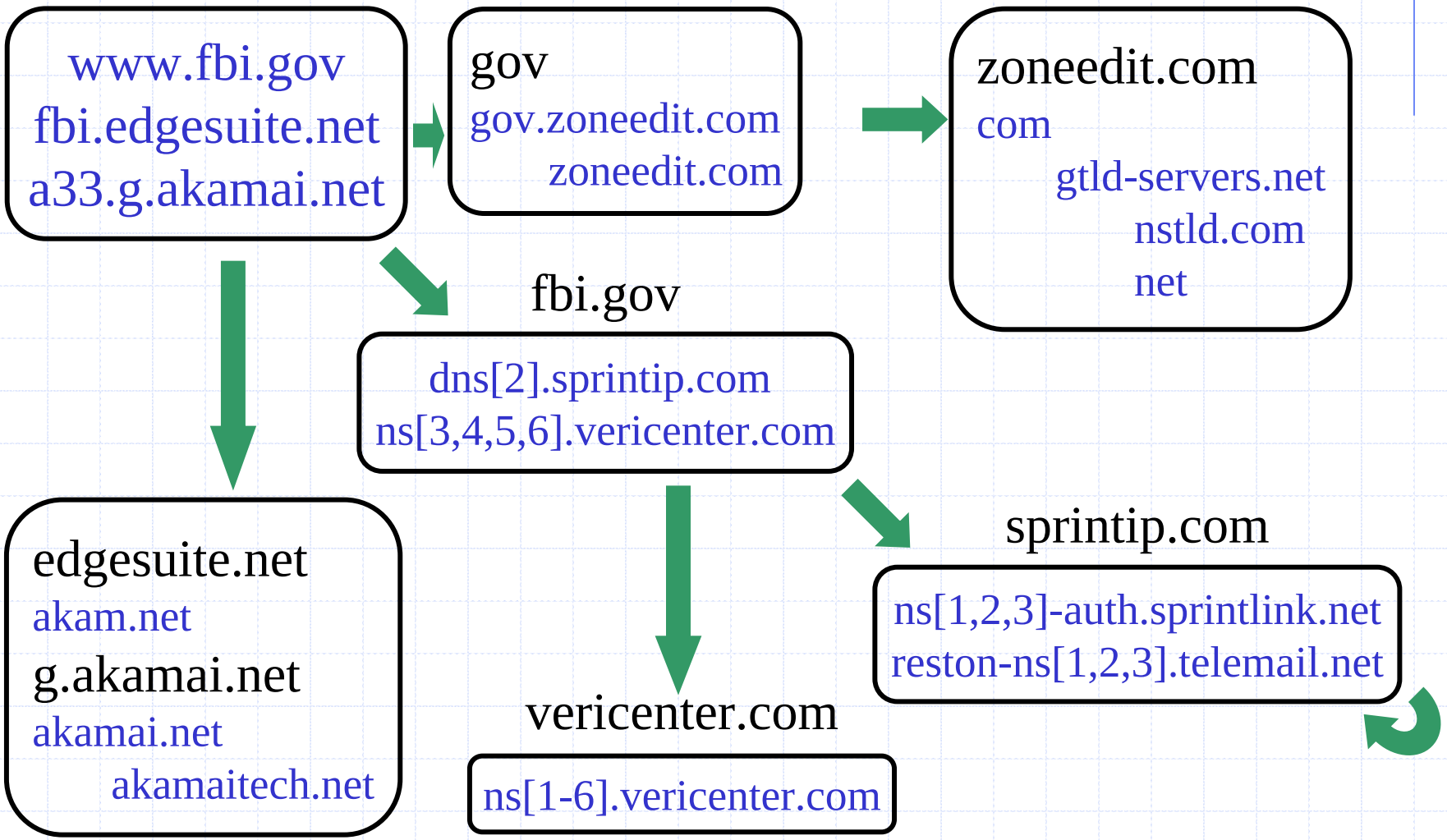
Dependencies for www.fbi.gov



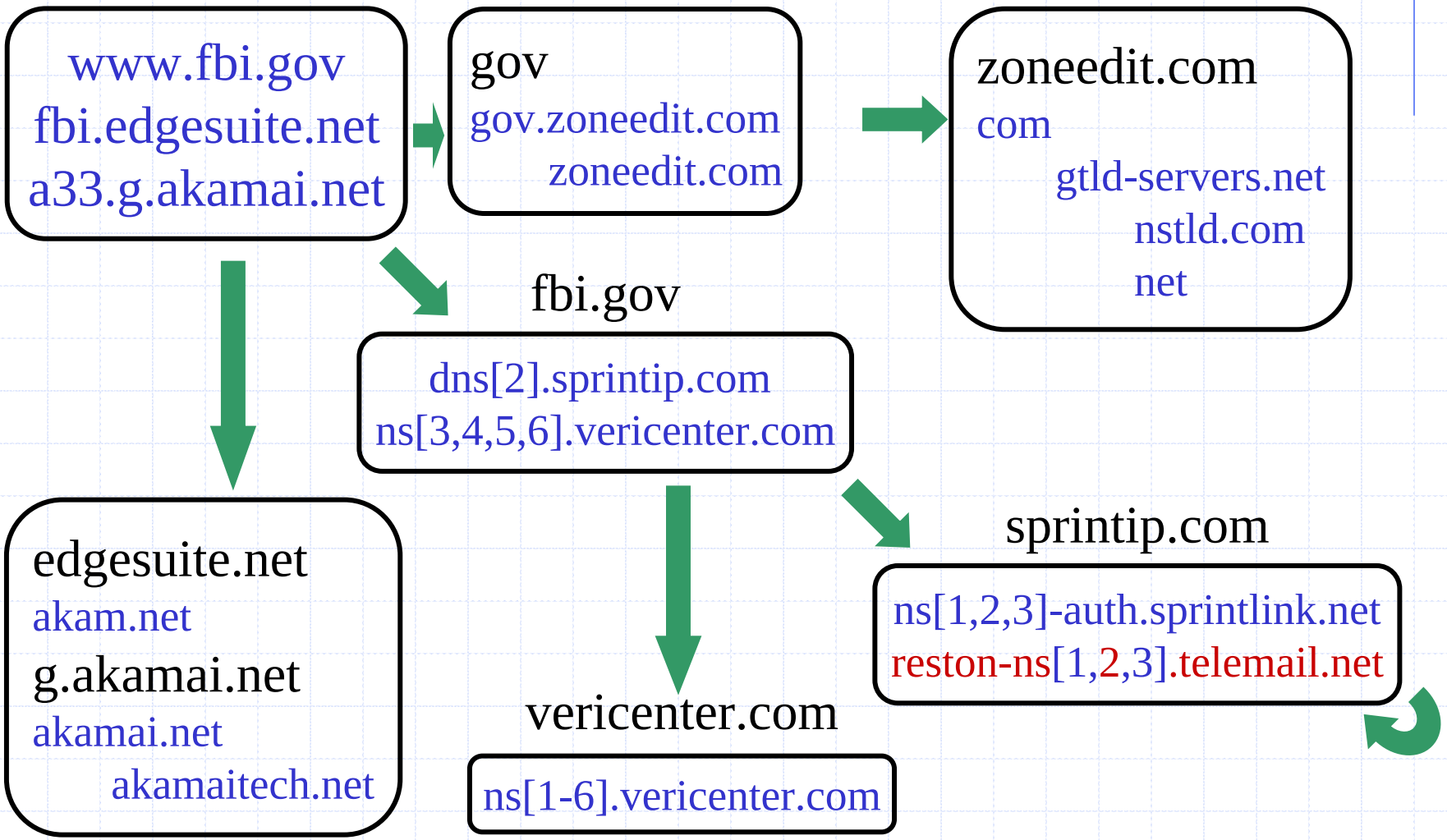
Subtle Dependencies in DNS

- DNS dependencies are subtle and complex
  - www.fbi.gov
    - ➔86 servers, 17 domains
  - www.cs.cornell.edu
    - ➔cs.rochester.edu ➔ cs.wisc.edu ➔ itd.umich.edu
    - ➔48 nameservers, 20 domains
- Conventional wisdom says "add redundant nameservers to mask failures, at no cost"
- Conventional wisdom is wrong
  - Increases risk of domain hijacks

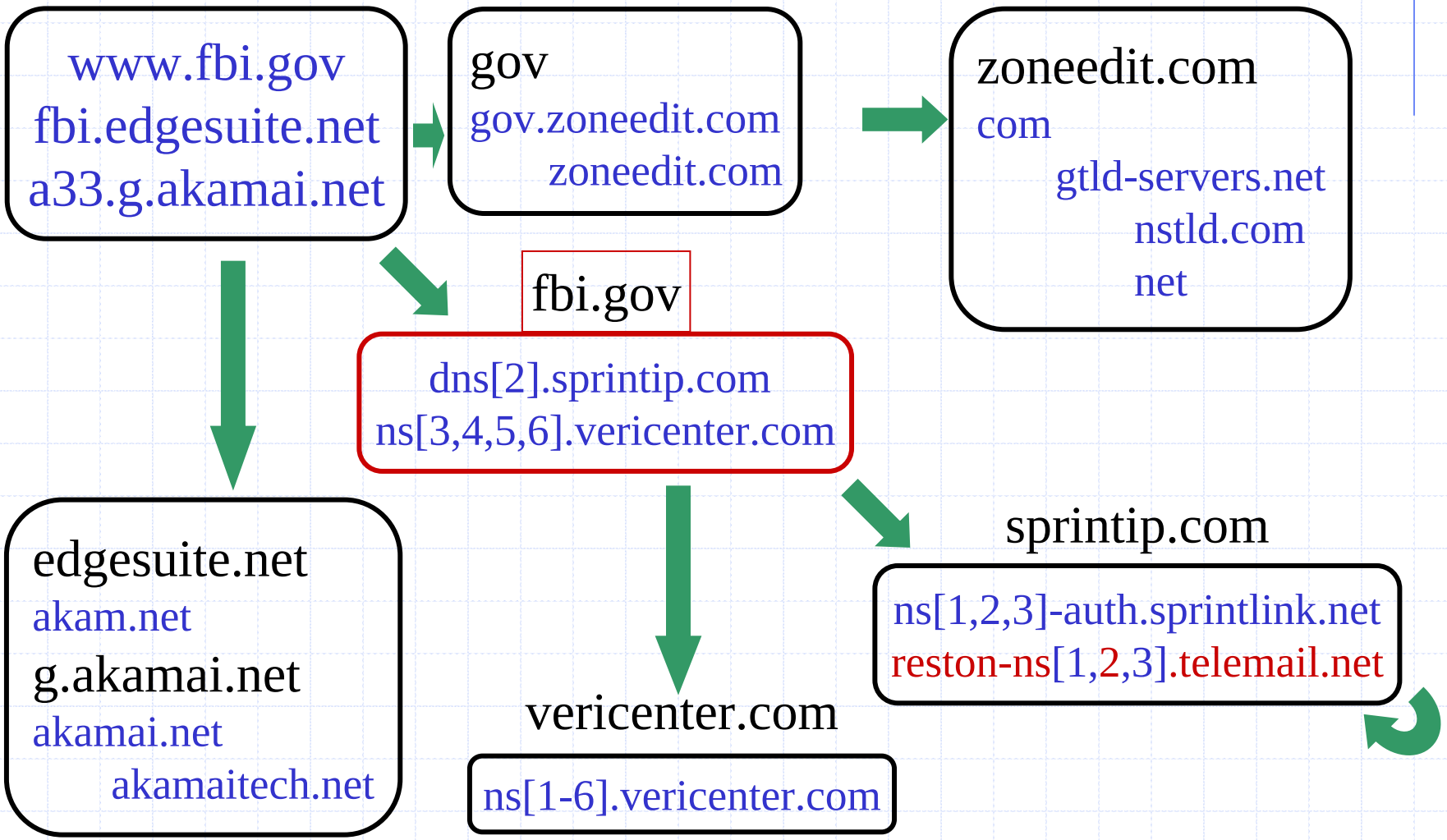
Dependencies for www.fbi.gov



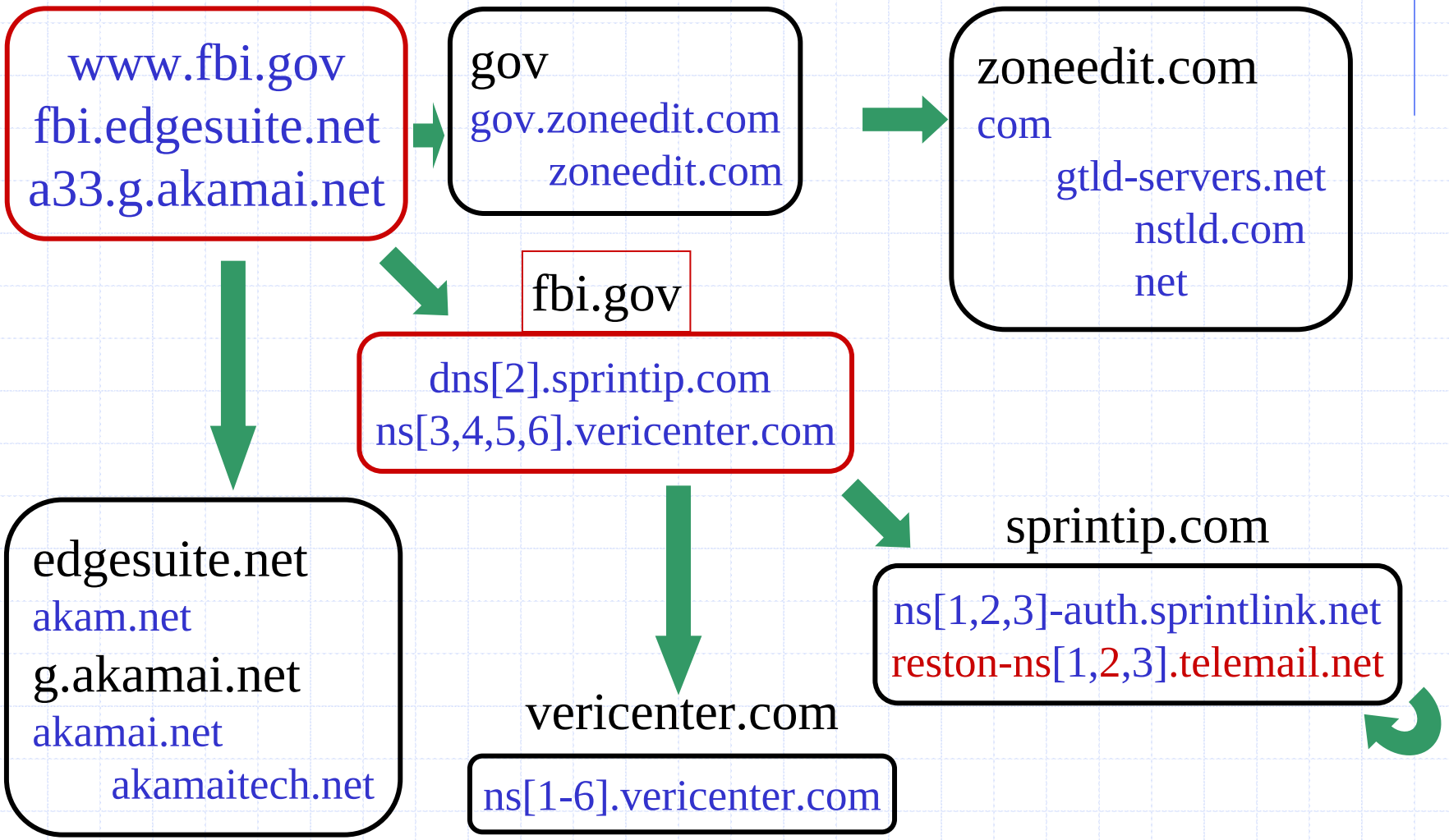
Dependencies for www.fbi.gov



Dependencies for www.fbi.gov

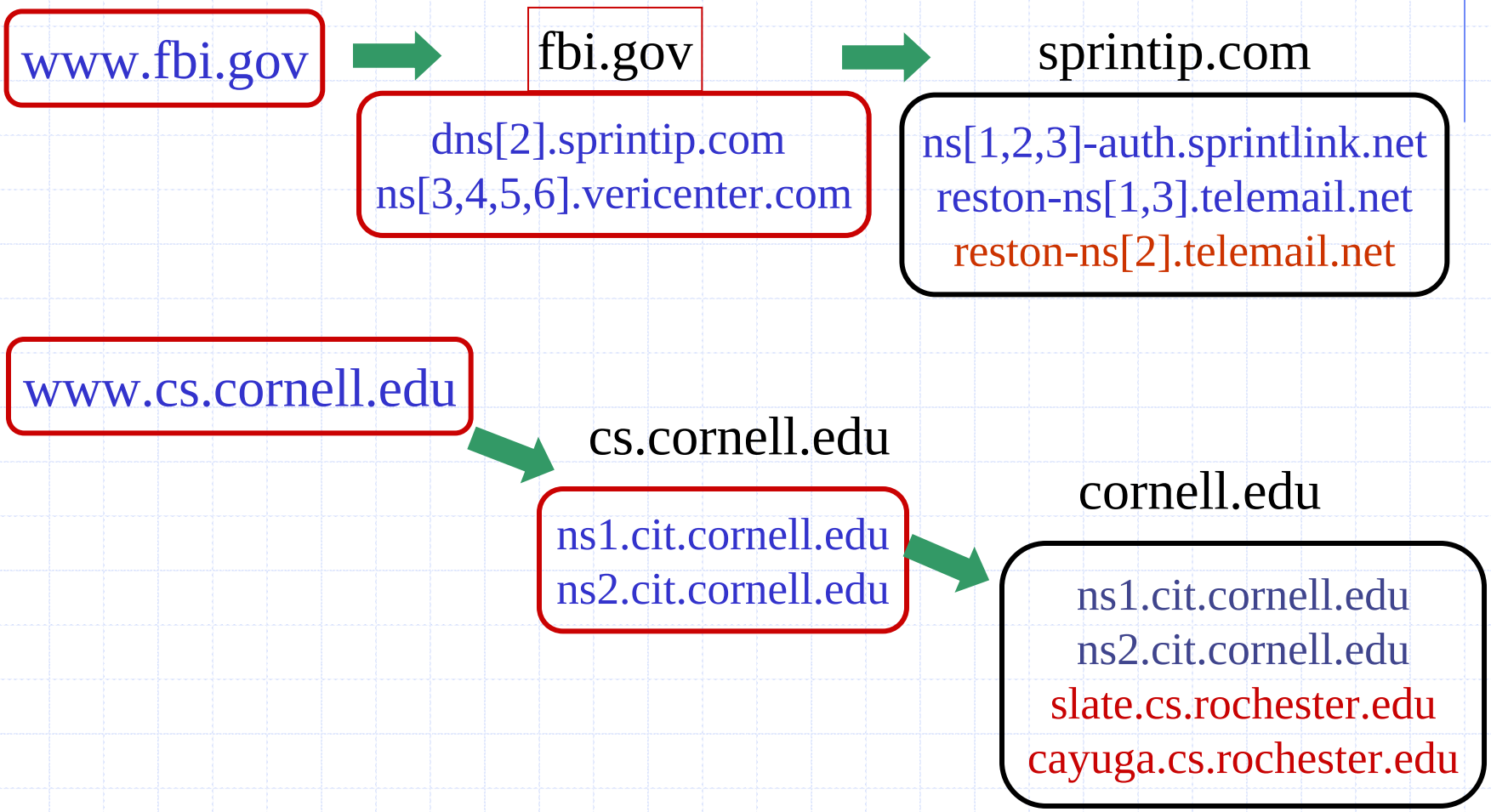


Dependencies for www.fbi.gov

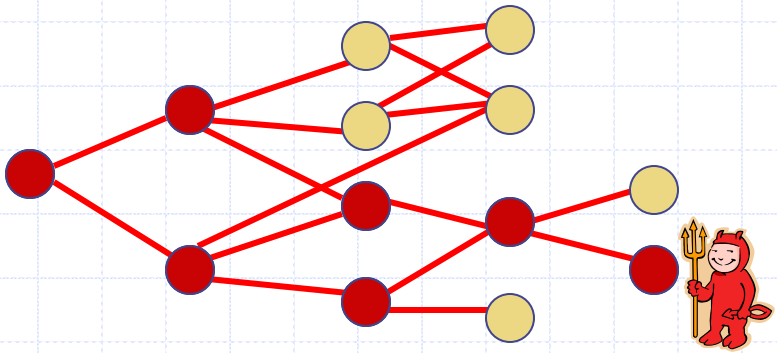


Servers with Security Loopholes

Servers with Security Loopholes



Lessons



- DNS delegations create a directed acyclic graph of dependencies
- This graph forms the trusted computing base for that name
- This graph is often large and includes many vulnerable hosts, making domain hijacks possible

Goals

- Identify vulnerable assets
  - Which domain names have large dependencies and entail high risk?
  - Which domains are affected by servers with known security holes and can be easily taken over?
- Identify valuable assets
  - Which servers control the largest portion of the namespace and are thus likely to be attacked?

Survey Methodology

- Collected 593160 domain names
  - Visible names people care about from Yahoo & DMOZ
  - Separately examined the Alexa Top-500
- Traversed 166771 name servers
  - Large set of important nameservers
- Examined the dependence graphs for 535036 domains, 196 top-level-domains

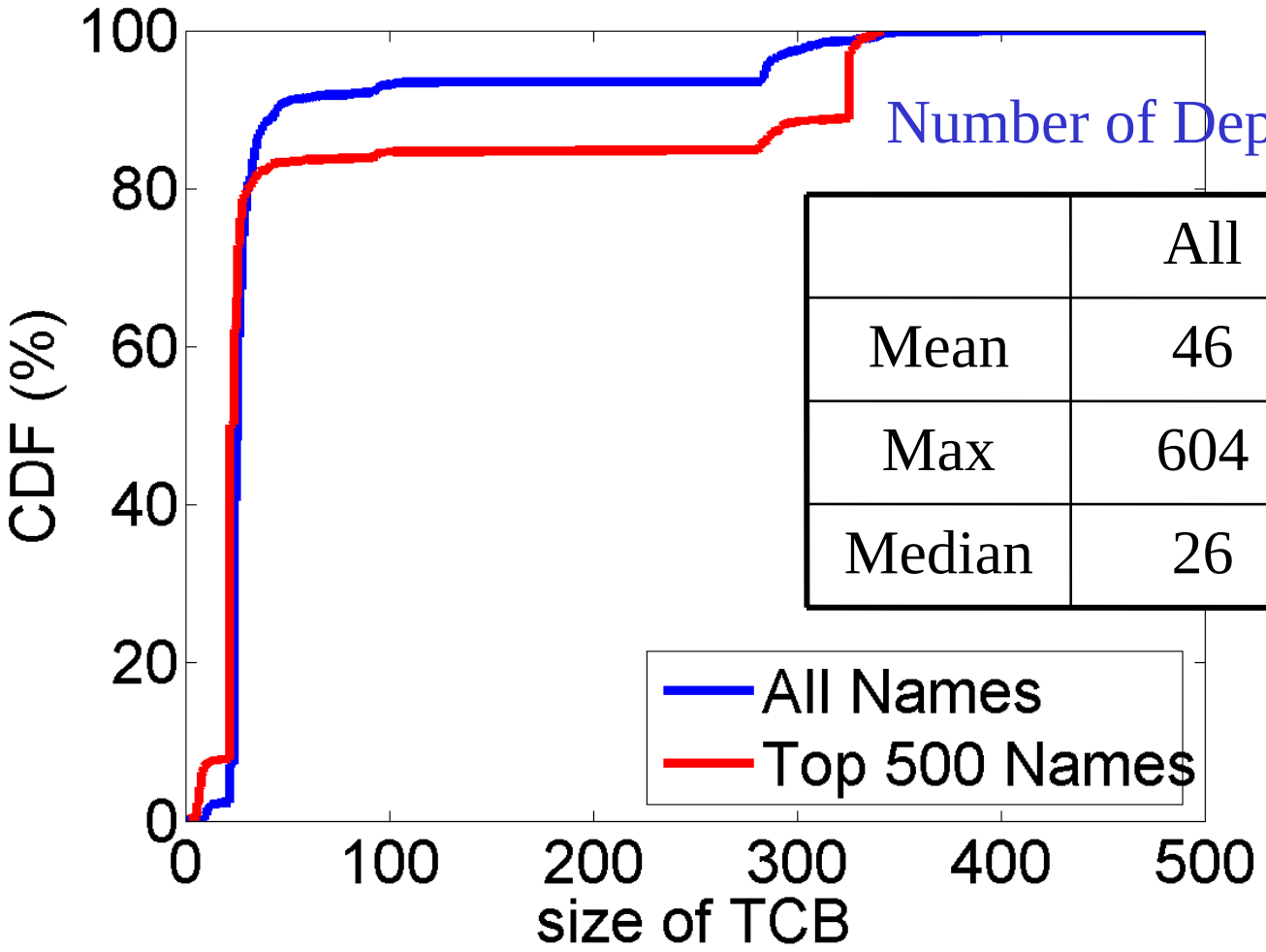
How vulnerable is a typical name?

How big is the average TCB?

Which domains have the largest TCBs?

What are the chances of a successful domain hijack?

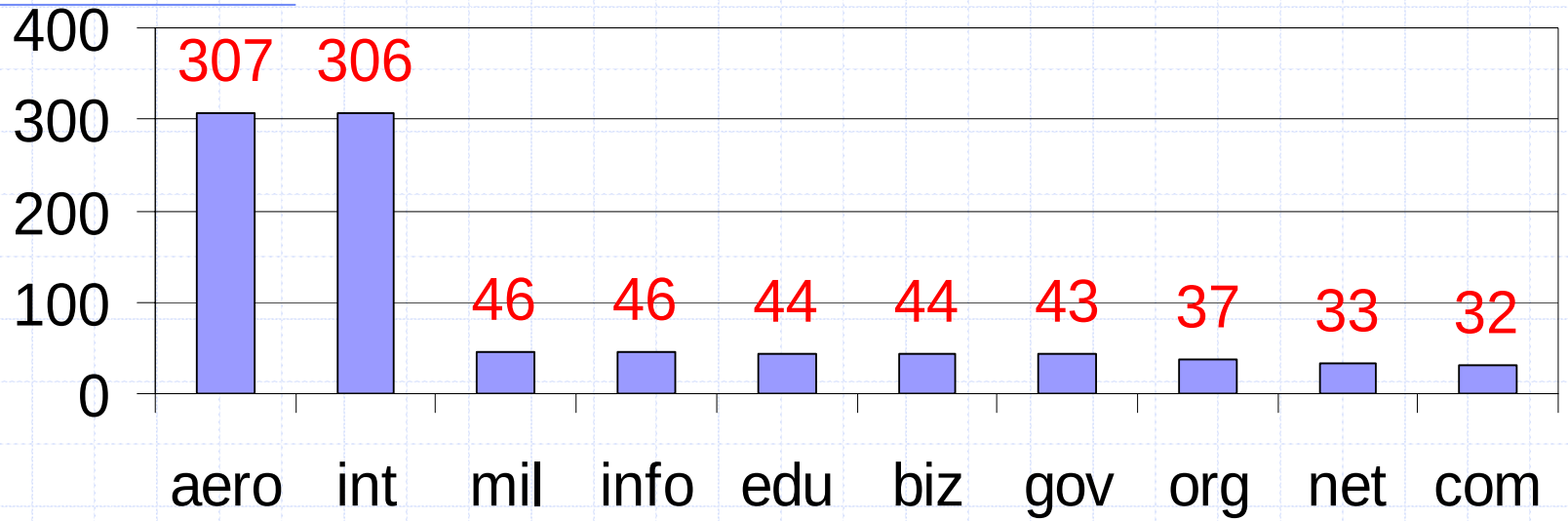
TCB Size

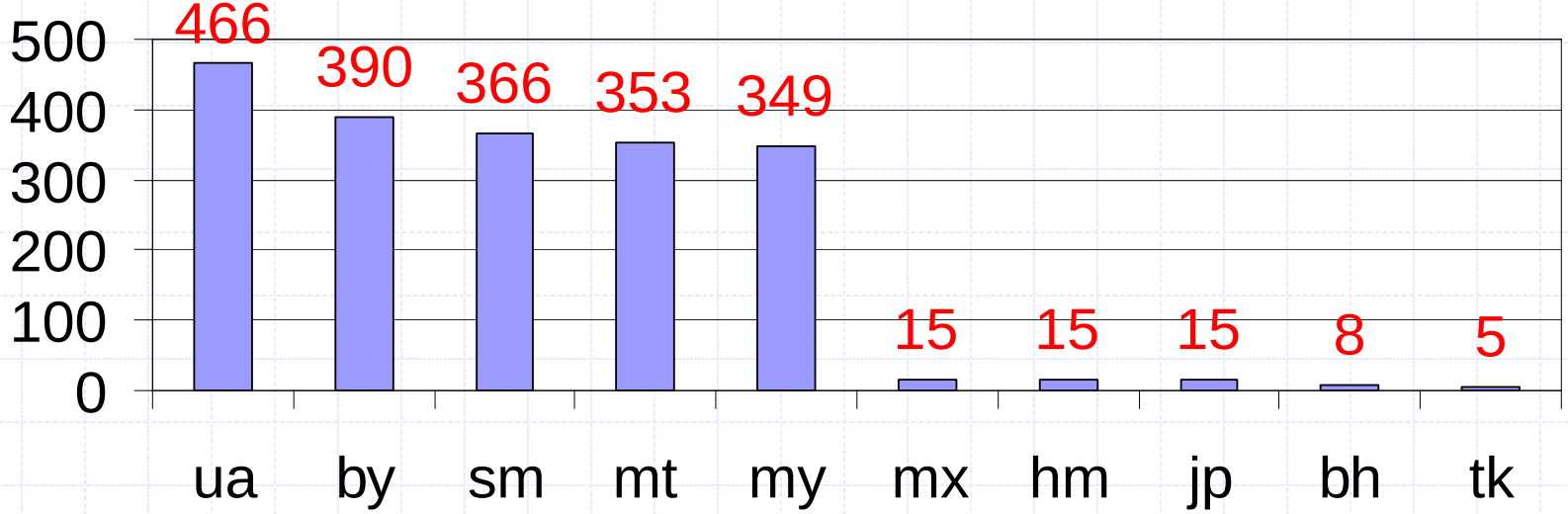


Number of Dependencies

	All	Top 500
Mean	46	68
Max	604	342
Median	26	22

Dependencies by TLD





Most Vulnerable Name

- Roman Catholic Church website in the Ukraine depends on nameservers in
  - Berkeley, NYU, UCLA, Russia, Poland, Sweden, Norway, Germany, Austria, France, England, Canada, Israel, Australia
- An attacker in Monash, Australia could redirect the IP binding for a website in Ukraine
- It's a small world after all...

Lessons for TLD Operators

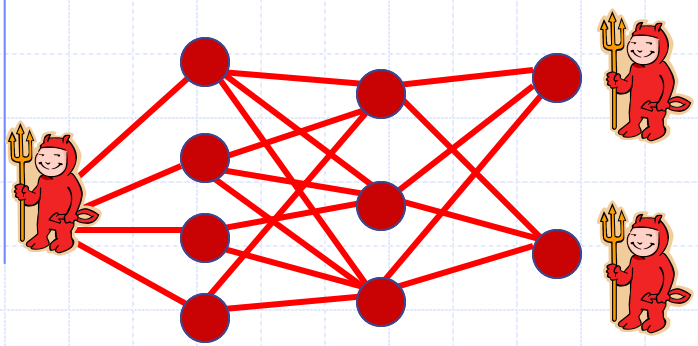
- Some TLDs are set up such that all names in them are dependent on many nameservers
  - AERO, Ukraine, Malaysia, Poland, Italy...
- Some TLDs have few dependencies
  - Japan
- Possible to achieve high failure resilience without depending on lots of hosts

Vulnerable Names

- Surveyed BIND version numbers
  - Queried public version numbers
  - 40% response rate
- Compared against database of known vulnerabilities from ISC
  - Many have well-known exploit scripts available
- Examined the dependency graphs to determine how vulnerable names are

Chances of domain hijacks

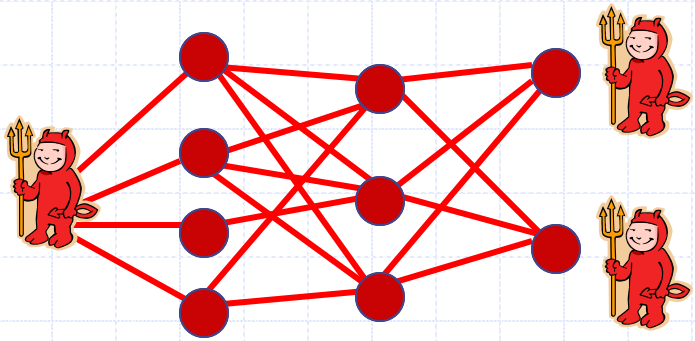
- Not all vulnerabilities are equal



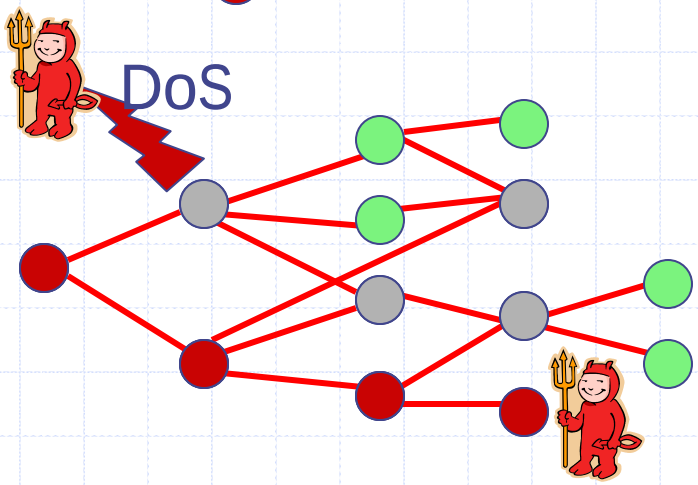
- An attacker can compromise a name completely (0wn it) if it can acquire a graph cut

Chances of domain hijacks

- Not all vulnerabilities are equal

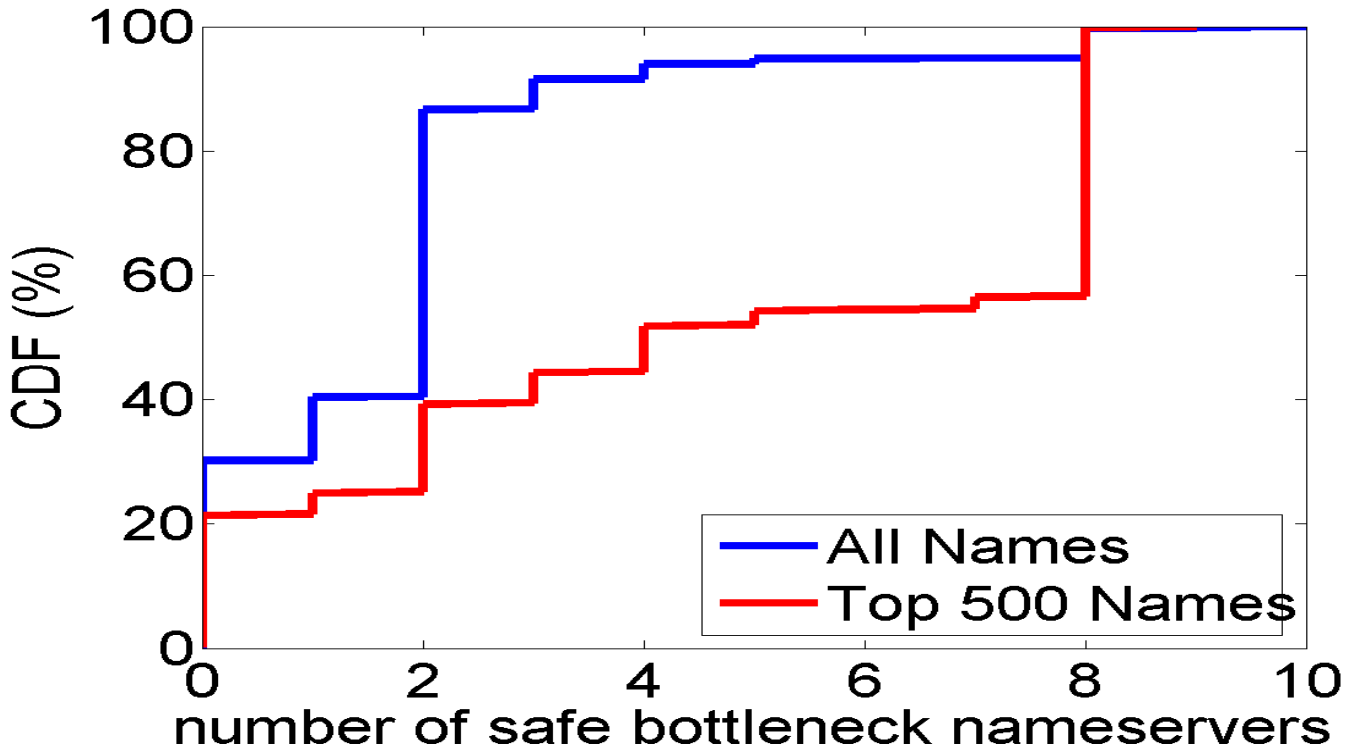


- An attacker can compromise a name completely (0wn it) if it can acquire a graph cut



- If a full cut is not vulnerable, attacker must combine compromise with DoS

Vulnerability to Security Flaws



- Due to large TCBs for names, an attacker can use vulnerable servers and small DoS attacks to 0wn many names

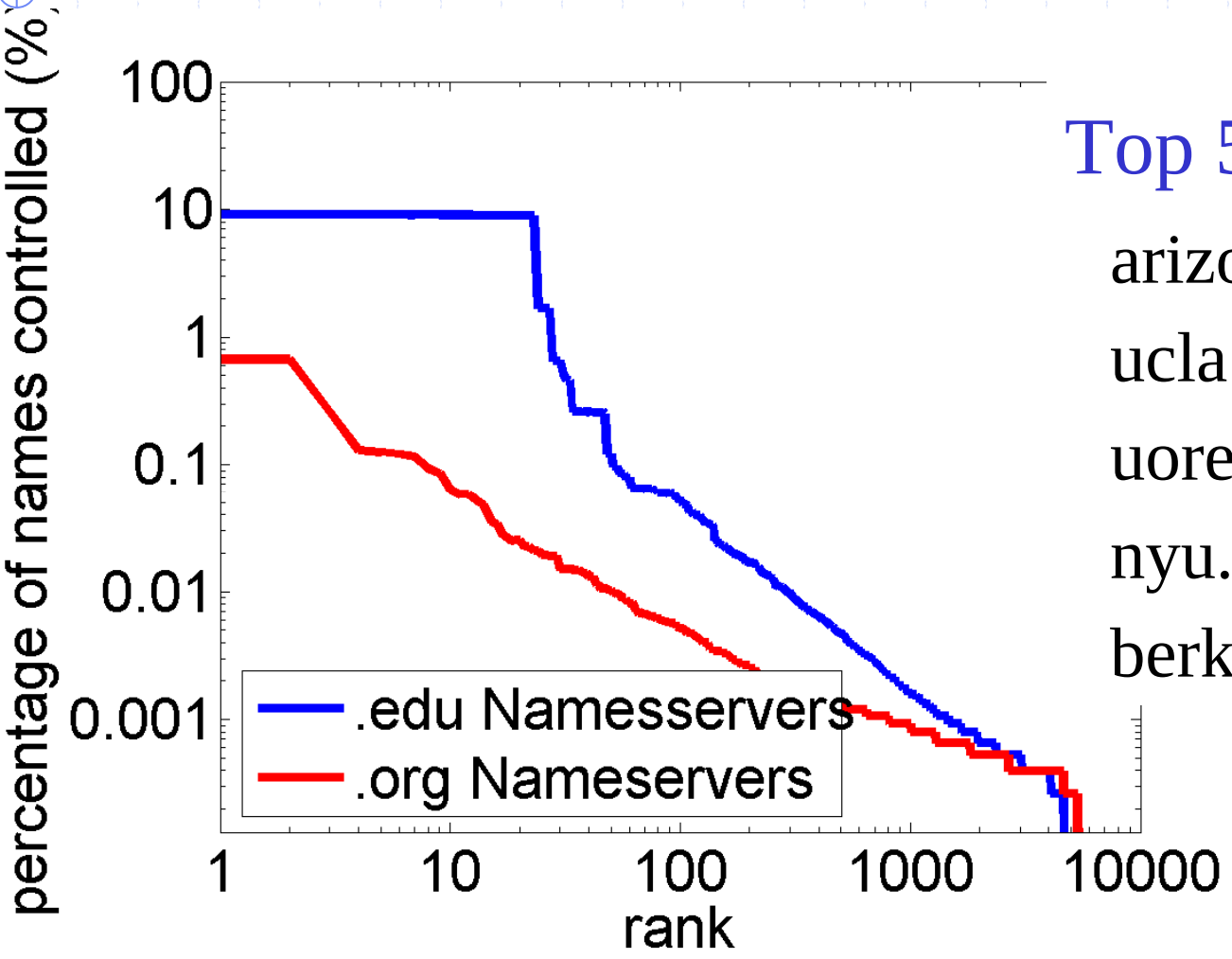
Vulnerable Names

- 17% of servers have known loopholes
- 30% of names are directly vulnerable
- 84% are vulnerable with 2-host DoS
- An attacker that can DoS 8 hosts can 0wn almost any name
- DNS dependencies expand the impact of vulnerabilities

Where are the valuable nameservers?

“Ok, I want to take over the Internet. Where do I start?”

Most Valuable Nameservers



Top 5 Domains

arizona.edu

ucla.edu

uoregon.edu

nyu.edu

berkeley.edu

Valuable Nameservers

- Many nameservers in the .EDU domain appear in dependency graphs
- Operators have no fiduciary responsibility to name owners
- Name owners as well as operators most likely do not realize the dependencies
  - Potential security risks and legal liabilities!

Conclusions

- Domain names have subtle dependencies
  - Due to name-based delegations inherent to DNS
- High risk of domain hijacks
  - Conventional wisdom is wrong, name owners should delegate carefully
- DNS is overdue for a redesign, for security
  - More data available at: http://www.cs.cornell.edu/people/egs/beehive/