
Using DNS to protect clients from malicious domains

Melissa Muth
University of Pennsylvania

Security Camp 2015
Boston University

The Problem

- ❖ Polymorphic Malware
- ❖ 50% Effective AV Software
- ❖ 0-Day Threats
- ❖ Legitimate websites serving malicious 3rd party ads
- ❖ Fast-flux DNS

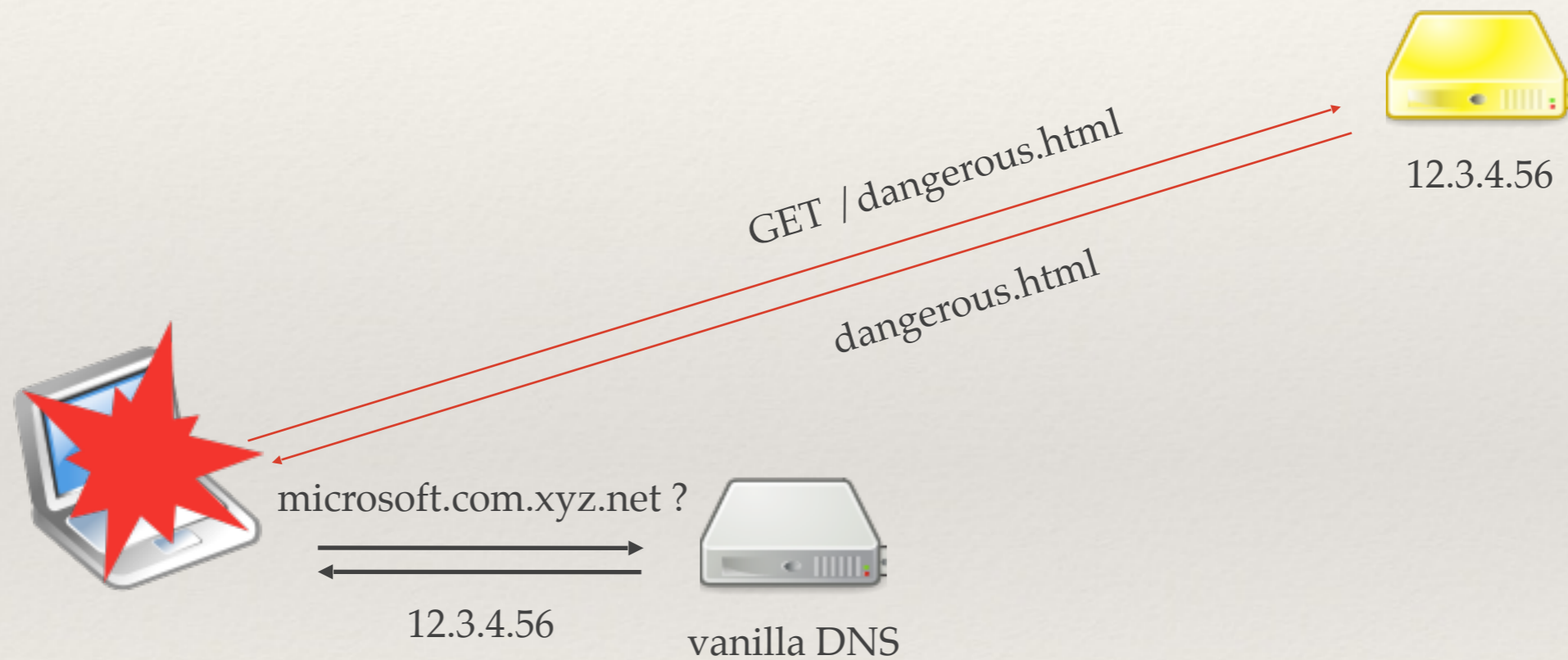
Leverage: Reputation

Malware Domain List
Zeus Tracker
REN-ISAC
...

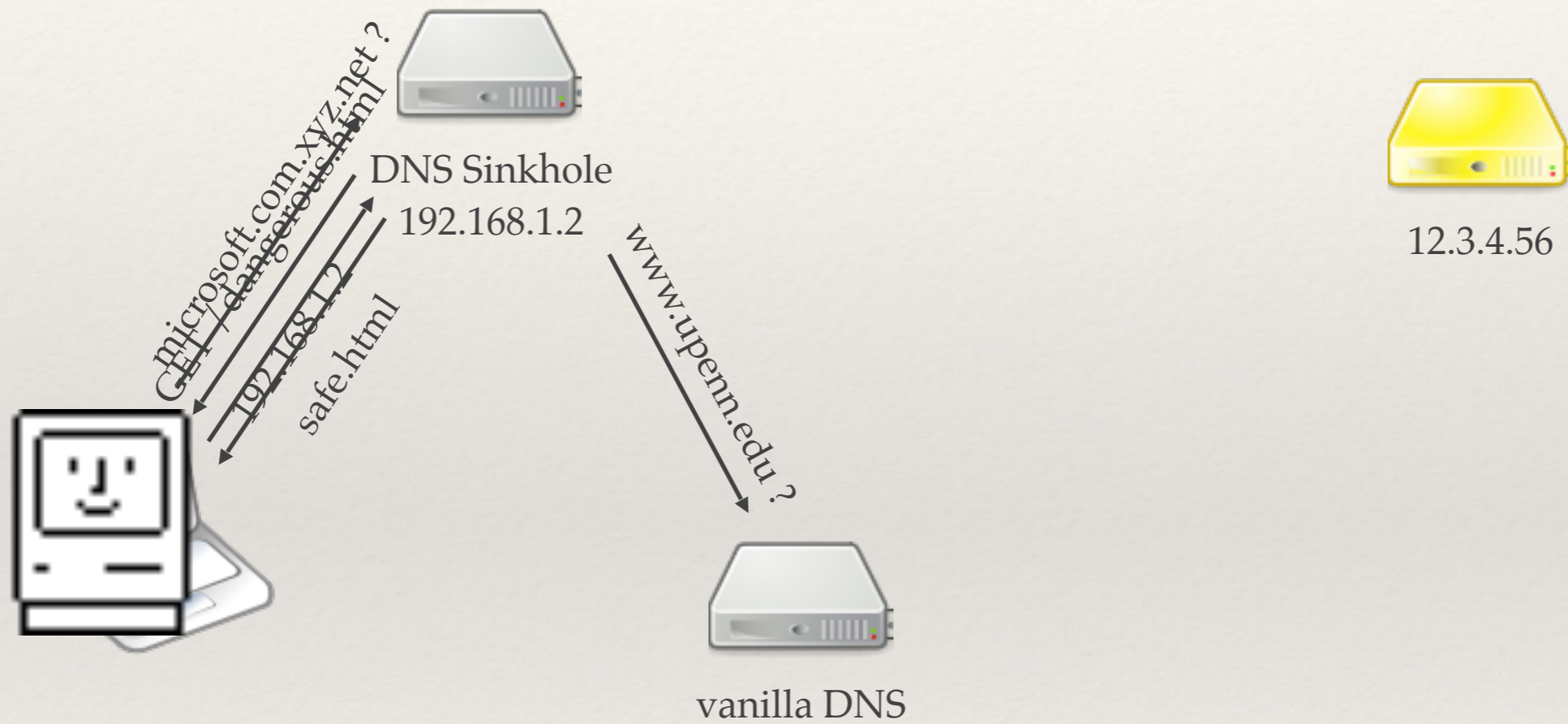


DNS

Without DNS Sinkhole



With DNS Sinkhole



Benefits

- ❖ Opt-in
- ❖ Can supplement existing campus DNS
- ❖ Can be anywhere on the network
- ❖ Easy to deploy (if using DHCP)
- ❖ Lightweight (compare: proxy)

Limitations

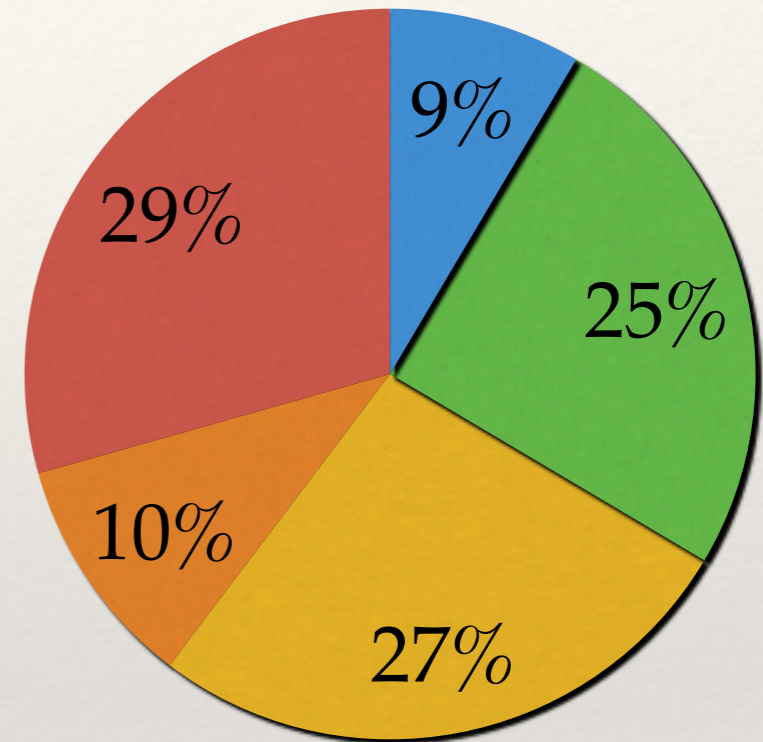
- ❖ Granularity
 - ❖ Hostname / domain
 - ❖ IP / CIDR
 - ❖ Not by URL
- ❖ DNSSEC broken (for malicious domains)

Poll

- ❖ Are you using a DNS Sinkhole?
- ❖ Are you thinking about it?
- ❖ What are your concerns?

Environment at Penn

- ❖ Tier 1 Research University
- ❖ 40,000 users, incl. 4000 international
- ❖ 50,000+ nodes
- ❖ Decentralized



- P/T students
- Undergraduates
- Graduate/Professional
- Faculty
- Staff

Implementation options



(tied to older software version)

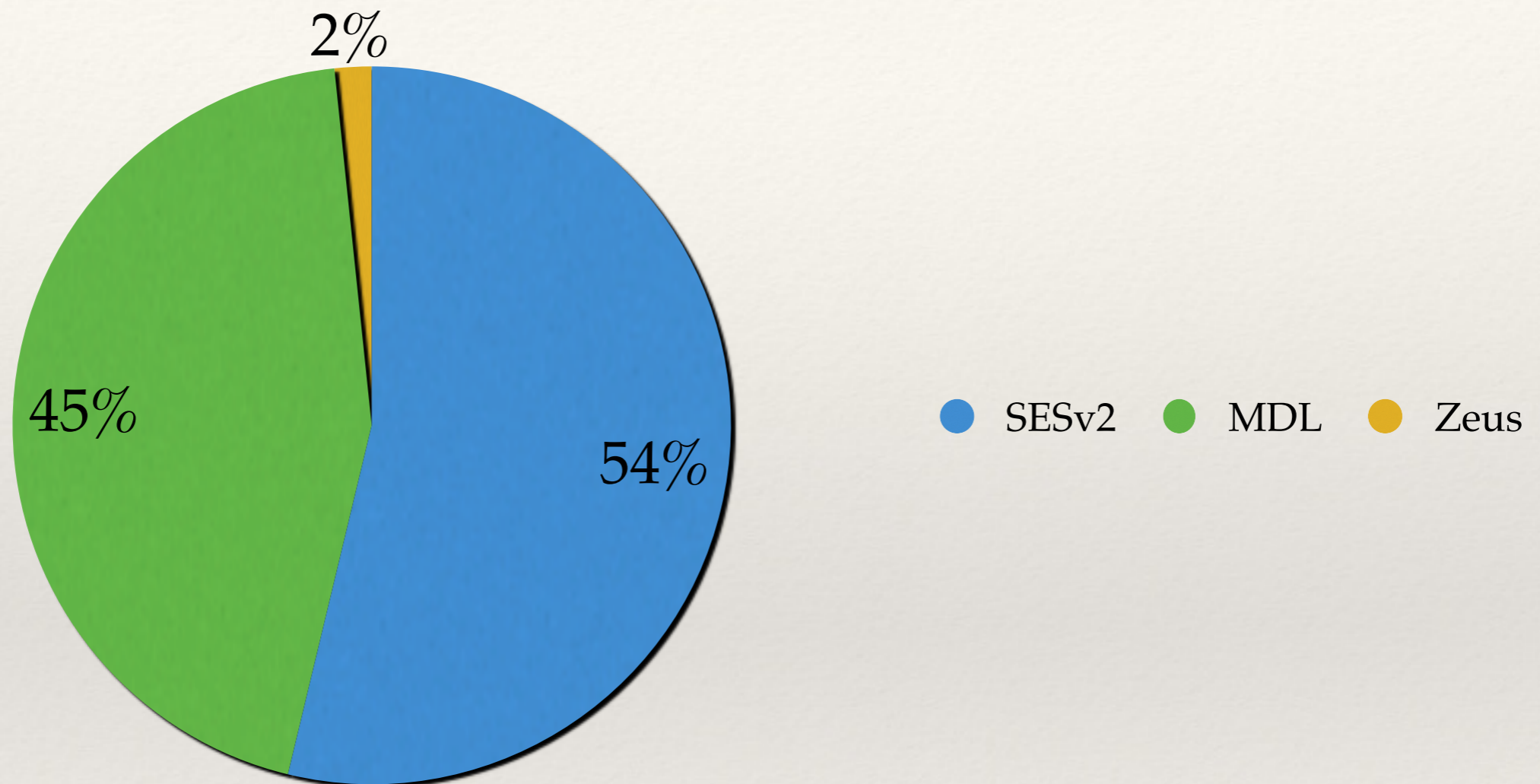
+



(\$)

In-house Proof of Concept

Implementation: Domain Sources



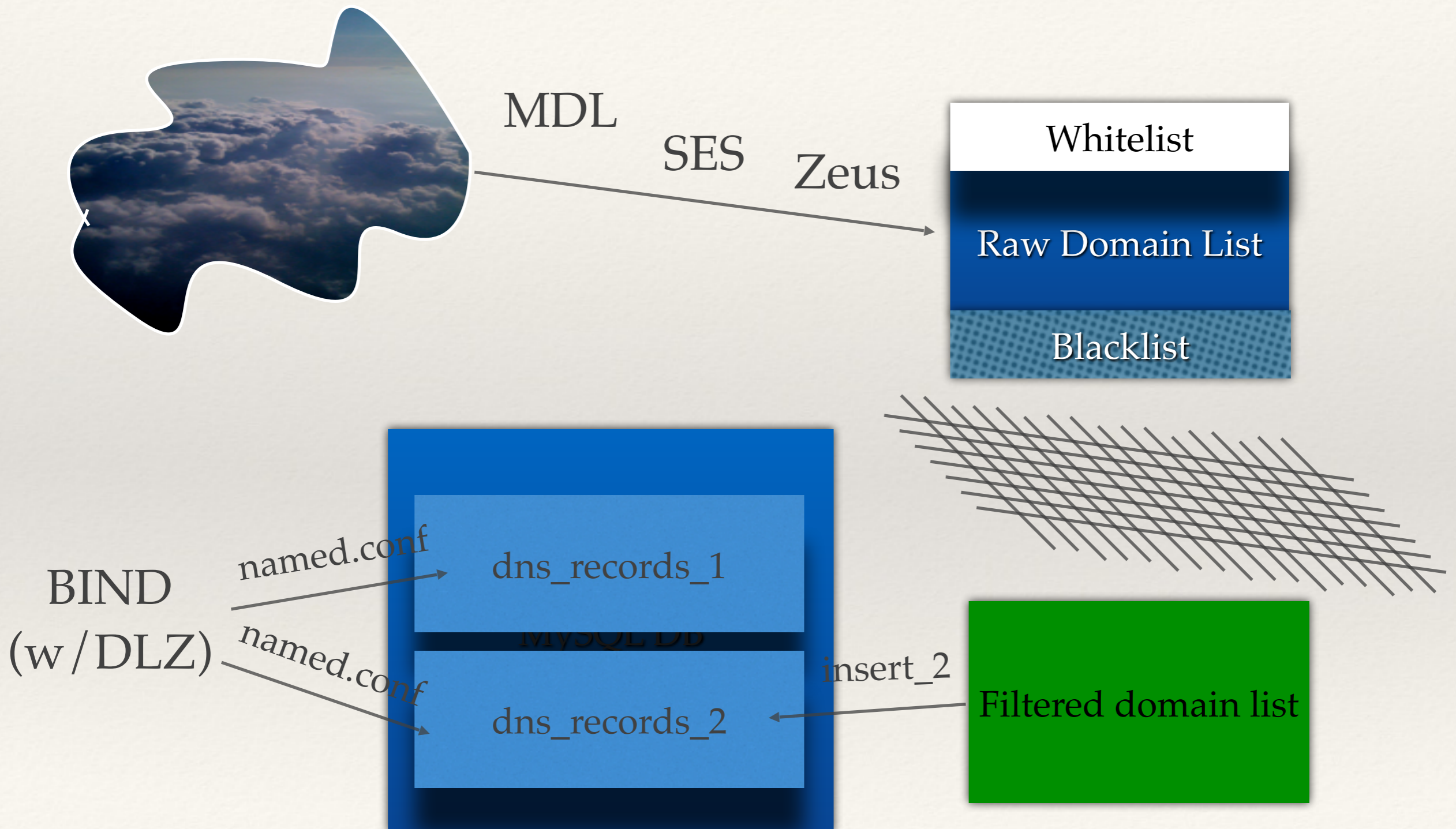
Implementation - platform



ubuntu[®]



Implementation - load



SafeDNS on Github

1. <https://github.com/mrmuth/SafeDNS/>
2. Install OS & Packages
3. Customize (School name, IPs)
4. Configure BIND
5. Set up loading of feeds, blacklist, whitelist
6. Set up Apache (landing page)

Recruiting Clients

❖ Increase subscribers gradually

❖ Communications

❖ Terms of Service

❖ Privacy Policy

❖ Documentation



The screenshot shows the Penn Computing Information Security website. The header includes the Penn Computing logo and navigation links. The main content area features a "SafeDNS Pilot" announcement. The announcement is structured as follows:

SafeDNS Pilot

The Problem

It has become increasingly difficult to protect client workstations from becoming compromised by malicious software. Even if workstations are patched and running up-to-date anti-virus software, some risks remain because of the:

- Increasing prevalence of 0-day threats (attacks that exploit vulnerabilities for which there is no patch);
- Incomplete effectiveness of anti-virus software in detecting polymorphic malware; and
- Prevalence of malicious third-party ads hosted on otherwise legitimate web sites.

The Pilot

You are invited to participate in this pilot service intended to protect client workstations at Penn from becoming infected by computers known to host malware. On a daily basis, this service updates a list of about 300,000 hosts that are known to be hosting malicious software.

How it Works

If a workstation is configured to use this as the DNS service, any attempt to reach a suspected malicious host gets redirected to the SafeDNS server itself. Web requests from the workstation will go here: [http://safedns\[12\].security.isc.upenn.edu/](http://safedns[12].security.isc.upenn.edu/) instead of to a malicious host.

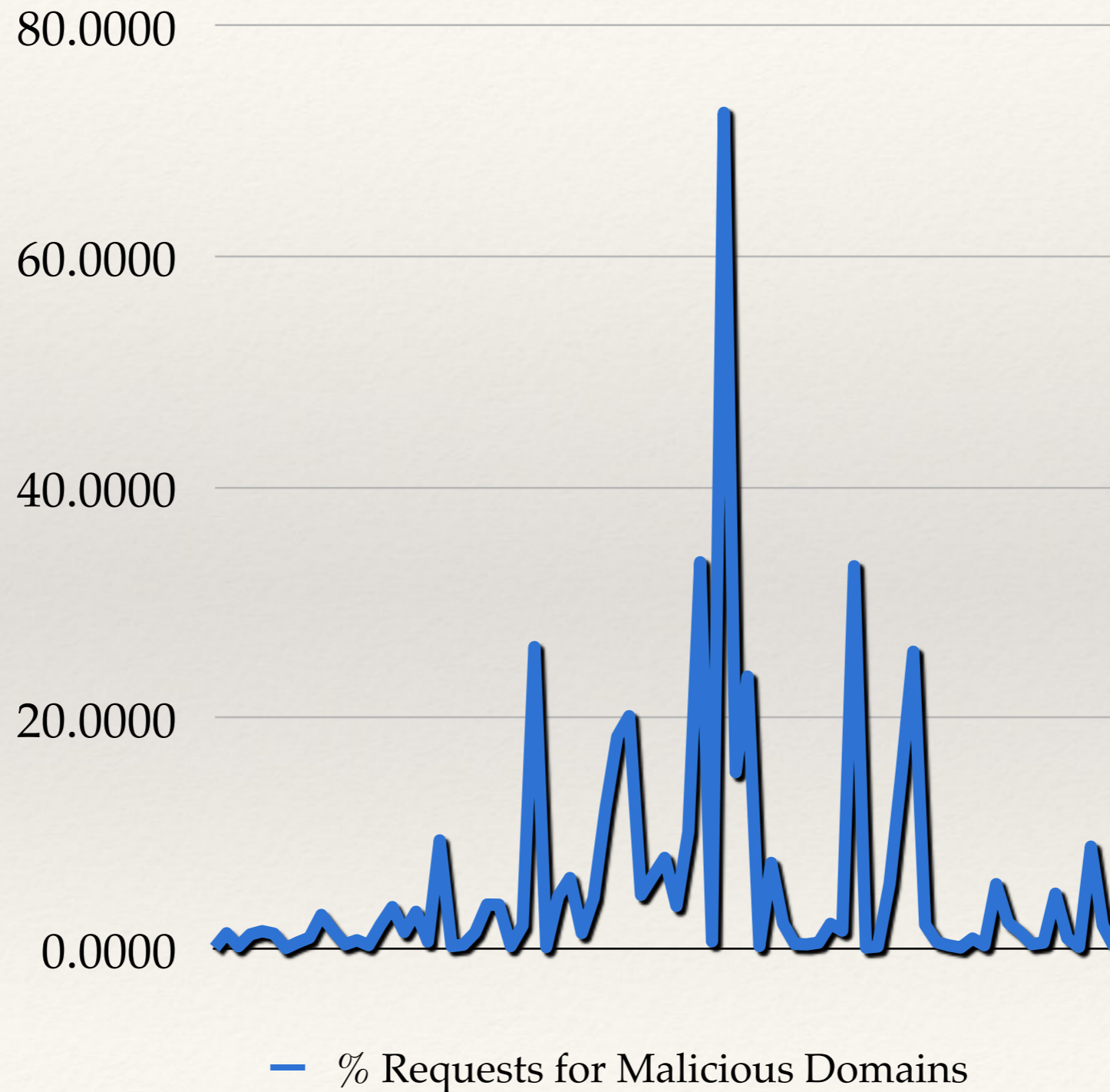
How do I join?

1. If you're a Local Support Provider, feel free to try out the service yourself by setting your DNS server addresses as follows:
Primary: 165.123.39.180
Secondary: 165.123.39.171
2. Review the Terms of Service, below.
3. When you're ready to set up clients to use the service, contact ProDesk (prodesk@isc.upenn.edu), letting them know:
 - How many clients you'd like to add, so we can confirm that the service is ready to support that number; and
 - Whether you'd like to be added to a distribution list for outage notifications and notices about service changes or enhancements.
4. Once we confirm that the service is ready for you to join, distribute the Privacy Statement below to your users.
5. Reconfigure clients to use the DNS server addresses above.
6. Give us feedback about the rate of compromises before and after joining the pilot (as described in the Terms of Service, below). Contact ProDesk if you see any false positives.

Terms of Service

- While we have made reasonable efforts to provide a robust and reliable pilot service, it is provided on a best-effort basis, with no guarantees about uptime, protection from false positives, or true negatives.
- The pilot service should not be used by servers, only client computers. For example, a

Results - % malicious queries

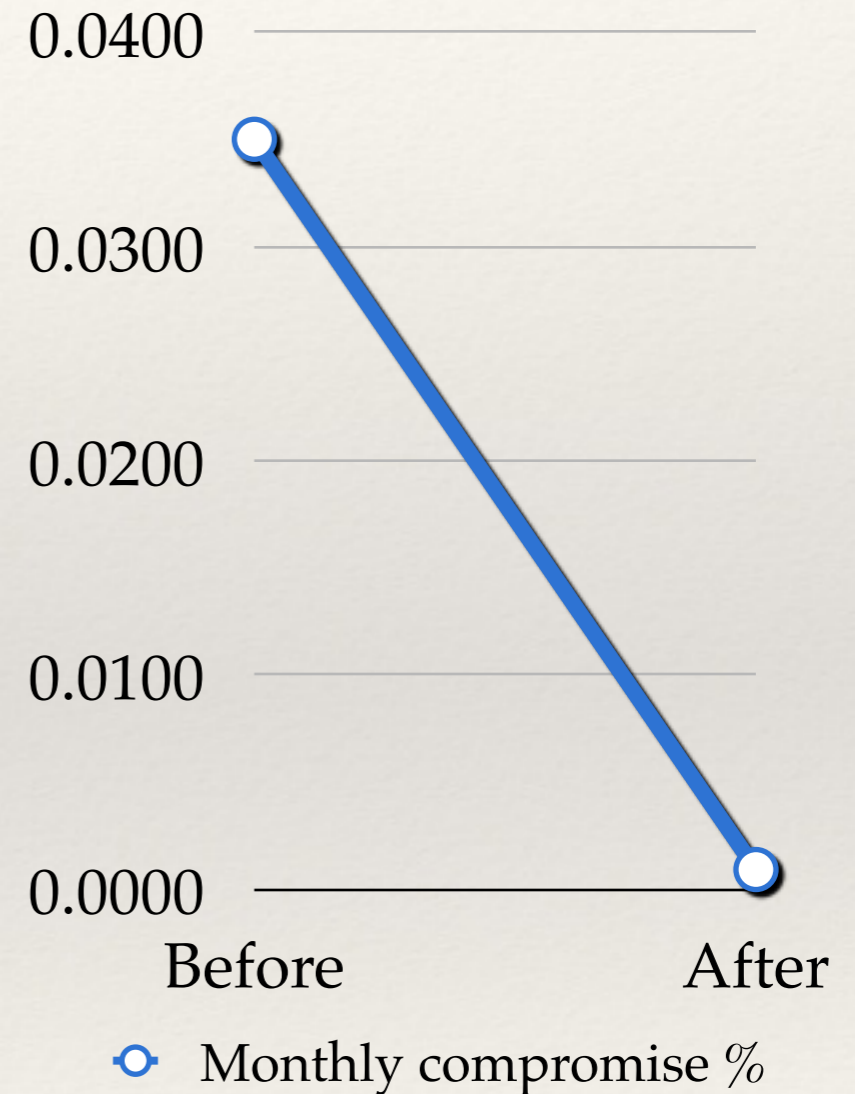


Results - user experience

- ❖ No downtime
 - ❖ Tertiary masked network outage
- ❖ False Positives
 - ❖ 3 from SRI (removed)
 - ❖ < 2 reported per year of operation

Success!

- ❖ 97% reduction in compromises
- ❖ Pilot: 7,700 clients
- ❖ Production: Feb 2015



Costs

Out-of-pocket	Hardware	\$0
	Software	\$0

Time	Build	2 person-weeks
	Maintenance	30 min/mo



Lessons Learned

Not a replacement
for campus DNS:

a value add



Lessons Learned

Branding
matters:




VS



Production!

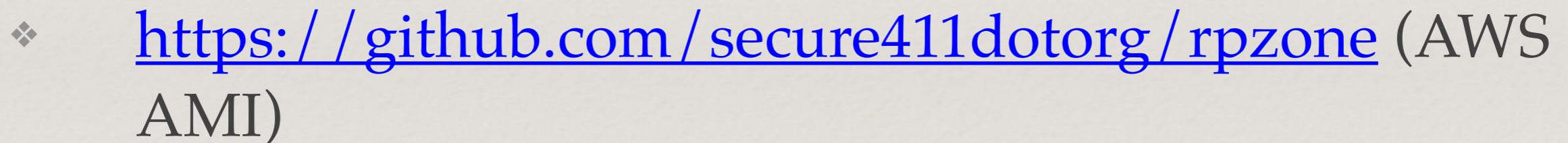
- ❖ 35,000 clients (including guest wireless)
- ❖ 440 DNS Queries / sec

Production: RPZs

- ❖ Response Policy Zones (BIND)
 - ❖ Overlay policy on native DNS responses
 - ❖ BIND 9.8 (supported), 9.10 (built-in feature)
- ❖ Block malicious name servers, IPs, CIDRs
- ❖ SpamHaus DROP list!  THE SPAMHAUS PROJECT
- ❖ Reputation feeds (SpamHaus, SURBL, ...)
- ❖ <https://dnsrcpz.info/>

DNS Sinkhole Options

- ❖ Roll Your Own:



- ❖ Commercial:

 OpenDNS

Infoblox 

Resources

- ❖ SANS dist: <https://isc.sans.edu/diary/DNS+Sinkhole+ISO+Available+for+Download/9037>
- ❖ SafeDNS:
 - ❖ <https://github.com/mrmuth/SafeDNS/>
 - ❖ <http://www.upenn.edu/computing/dns/safedns/>
- ❖ RPZs: <https://dnssrpz.info/>
 - ❖ <https://github.com/secure411dotorg/rpzone>

Melissa Muth

University of Pennsylvania

muthm@isc.upenn.edu

215-573-6798

<https://github.com/mrmuth/SafeDNS/>

<http://www.upenn.edu/computing/dns/safedns/>