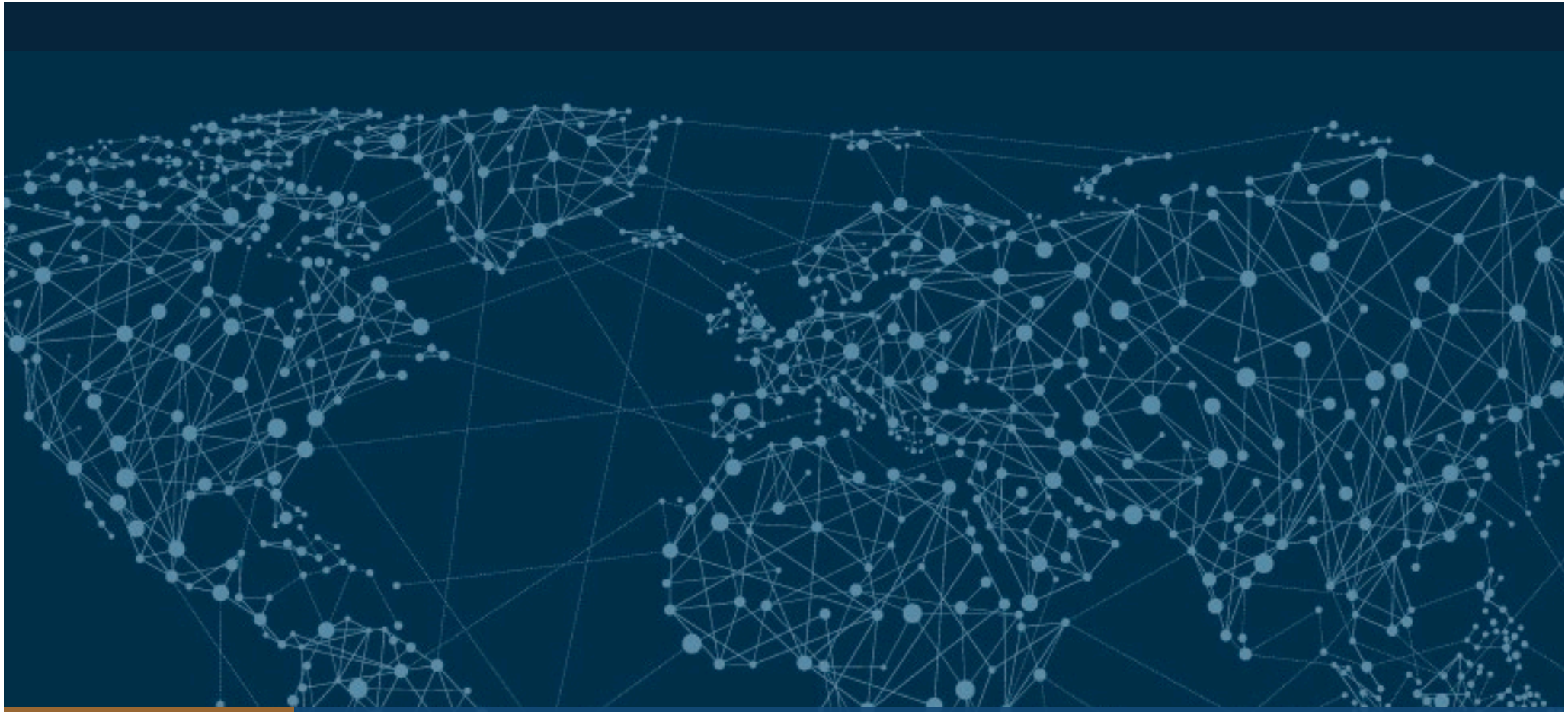

Introduction to the OCTO Research Middlebox Lab

Paul Hoffman | ICANN DNS Symposium | May 13, 2017

What's in the lab

- A few dozen middleboxes
  - SOHO routers
  - Enterprise-grade firewalls
  - Enterprise-grade routers
- VMware Workstation
  - VMs with open source firewalls and routers
  - VMs with commercial firewalls and routers
- Systems for running tests (also on VMware Workstation)
- Networking stuff
  - Lots and lots of cables

Goals of the middlebox lab for DNS

- Catalog how devices affect the DNS
  - Middleboxes that block some types of resolution
  - Middleboxes that silently act as proxies, maybe not in a good way
  - Middleboxes that block future development of the DNS

- Find similarities and differences between products
  - Common OEMs
  - Different development teams within a single vendor

Goals of the middlebox lab for others

- Collect data for other technical organizations about middlebox behavior
- Find transport protocols that are blocked or broken by middleboxes
- Determine which middleboxes intercept TLS, and how

Non-goals of the middlebox lab

- Name-and-shame of misbehaving models or vendor
- Conformance testing
- Ability to say “X% of middleboxes show this bad behavior”
- Collect every possible model of middlebox

Some easy-to-spot problems with middleboxes

- Harmful default values in firewalls
  - Block TCP on port 53 unless you change the configuration
  - Block port 853
  - Nothing in the documentation about how to fix these
- SOHO routers that do DNS forwarding instead of passing through
  - ...and then do it poorly
- Firmware update procedures that are cumbersome
  - ...or that brick the system

Possible research topics for middleboxes

- Do middleboxes do DNSSEC validation by default?
  - Is it easy to turn on from the configuration?
- EDNS behavior
- IPv6 behavior, particularly fragmentation
- Forwarding to fixed addresses (such as 8.8.8.8) instead of to what came in from DHCP
- Ability to support various transports such as SCTP and QUIC
- We want to hear from the various technical communities what kind of research would be useful from the lab

Not just middleboxes: lots of VMs

- Many distros, Windows versions, resolvers, authoritative servers
- For the upcoming KSK rollover, tested what Linux and BSD distros do when starting up
  - Started each one up, captured its output to see if it was acting like a stub or a recursive resolver
  - Only two were acting as recursive resolvers, and neither were doing DNSSEC by default
- Can perform similar tests up to the KSK rollover, particularly if we hear of any distros or resolvers that have potentially problematic defaults

Future projects for lots of VMs

- Update “how resolvers pick which authoritative server to talk to” timings from five years ago
- How validators handle new DNSSEC algorithms
- Resolvers that only do TCP
- Determine best way to get anonymized dumps from various resolvers
- Model IPv6 behaviors for ISPs who do not control the devices that connect to them

Engage with ICANN

Thank You and Questions

Reach us at:
Email: engagement@icann.org
Website: icann.org/technology

twitter.com/icann

soundcloud.com/icann

facebook.com/icannorg

weibo.com/ICANNorg

youtube.com/user/icannnews

flickr.com/photos/icann

linkedin.com/company/icann

slideshare.net/icannpresentations