One Namespace, Many Circles

Dr. Paul Vixie, CEO
Farsight Security, Inc.

DNS Works Only Because of Voluntary Cooperation

- Every Internet host chooses Recursive DNS servers
  - Can either believe ISP settings, choose OpenDNS or Google DNS, run Recursive locally, or *innovate further*
- Every Recursive DNS chooses its Root DNS servers
  - Can either use IANA, use enterprise level, use ISP level, run Root locally, or *innovate further*
- Unilateralism in DNS is unreliable
  - Hotels and ISP’s can force use of their DNS – but, VPNs?
- DNSSEC deepens the cooperative aspect of DNS
  - Recursive DNS servers also subscribe to Root signing key

Who is IANA?

- IANA = Internet Assigned Numbers Authority
  - Operational DNS stewardship for IETF, ICANN, ISOC
  - Policies are transparent; by Internet operators, users
- Has diverse servers globally, with anycast
  - Server operators are volunteers from many nations
- Uses DNSSEC, with a published signing key
  - Has its own DNSSEC signing and validation keys
- Coordinators: ICANN, US-DoC-NTIA, Verisign (US)
- System is intended for Internet-scale *production*

Who is Yeti?

- Yeti is an experimental root name service project
  - Precisely mirrors the IANA DNS namespace
- Like IANA, has diverse servers globally
  - Server operators are volunteers from many nations
- Like IANA, has DNSSEC, with a published signing key
  - Has its own DNSSEC signing and validation keys
- Coordinators: BII (China), WIDE (Japan), TISF (US)
- System is intended for Internet-scale *science*

Why Not Use IANA or Yeti?

- Because you won’t have all of the IANA or Yeti servers represented inside your network perimeter
- So, it’s an **external dependency** – you might be unable to reach local servers due to remote outage
- And, it’s a **surveillance** opportunity for outsiders – who can learn what your network is interested in
- Due to **external dependency** and **surveillance** risks, many autonomous networks run their own root name server systems that are not Internet-visible

What’s an Autonomous Network?

- Any cooperating set of Internet hosts, Recursive DNS servers, and Root servers
- This could be a single host, on *loopback* network
- Or a LAN, campus, ISP, country, or region
- IANA’s content is openly available – anyone anywhere can mirror the IANA namespace
    - For example, this is what ORSN does
    - Many secure or private networks also do this
- Note! *One World, One Internet,* ***One Namespace***

DNS Autonomy: Part 1: Design

- Decide on four invariants:
  - a set of name server operators, names and addresses
  - a root zone signing key, and a key management regime
  - a set of distribution master operators, names, addresses
  - a publication point for hints, trust anchor, and zone data
- This determines the shape of the *circle of cooperation* for your local root hints file, root zone signing and verification keys, and root zone

DNS Autonomy, Part 2: Processing

- Craft an import process to be run one or more times daily:
  - Fetch the IANA zone
  - Verify, and then strip off, IANA’s DNSSEC signatures
  - Replace apex NS RR set with locally designated servers
  - Re-sign the zone using the locally created signing key
  - Publish the new zone, using NOTIFY and IXFR
- This is the work of the *distribution master servers* of which you ought to have more than one, for reasons of *high availability*

DNS Autonomy, Part 3: Action!

- Begin root zone processing as described in *Part 2*
- Begin operations at local root servers designated in *Part 1*
- Reconfigure cooperating Recursive DNS servers to use the “hints file” and root zone verification key chosen in *part 1*
- That’s it – you’re done – set up daily monitoring
  - External dependency is now *daily* not *real-time*
  - Surveillance is now limited to knowledge of your network’s autonomy in providing its own root service

Background: the Yeti DNS Testbed

- Internet Governance policy must be informed
  - How many root name servers is enough, or too many?
  - How easily can root name server operators be replaced?
  - How often can DNSSEC keys be replaced?
  - Would an all-IPv6 root server system work?
- The Yeti DNS testbed will search for these answers
  - Objective science; transparent policy; open governance
  - Lasting until 31-DEC-2018 unless extended
- The IANA name space will be copied exactly!
  - Only the root name servers and DNSSEC keys will differ

End Notes

- This proposal is controversial, since many people feel that a *root zone* is the same as a *namespace*
  - Not so! Many root zones can represent given namespace
- This proposal has a downside: less measurement
  - However, Google DNS and OpenDNS already do this
  - As do many ISP’s, researchers, and test labs world wide
  - Also, outside measurement can feel like surveillance

- Comments and questions welcome!