xfinity™

NANOG DNS BoF

DNS – DNSSEC – IPv6

Tuesday, February 1, 2011

Comcast

NATIONAL ENGINEERING & TECHNICAL OPERATIONS

The Role Of An ISP In DNSSEC Validation

- ISPs act in two different DNSSEC roles, both signing and validating
  - *Signing*: authoritative infrastructure domains & customer domains
  - *Validating*: recursive resolvers operating across the ISP network
- ISPs operate the majority of resolvers that end users query
  - It is relatively rare for most residential end users to operate their own DNS, or to change their DNS settings to use a third-party DNS
  - In most cases, ISPs can automatically update DNS server IP addresses, such as via DHCP lease updates
- As such, good DNSSEC adoption by end users hinges on ISP adoption of DNSSEC
- Comcast publicly announced our plans for DNSSEC in February 2010
  - Other ISPs need a similar plan
- Begin with documenting and validating your DNS operational processes
  - Put together a small trial, one server or several in a lab and/or production
  - Talk to your vendors and make sure they can meet your requirements

Lessons Learned

- ISPs have many operational processes that may need to be adjusted to support DNSSEC validation
  - Authoritative infrastructure may need to be augmented to support signing your zones
    - Zone signing can be resource intensive
    - Chaining your zones to parents at the TLD as well as subzones can be tricky and require planning and coordination with your registry.
  - Recursive resolvers may need to be updated to software that supports validation
    - Deploying a configuration that scales to meet your customers needs

Lessons Learned Continued

- Upstream routers and firewalls may need to be addressed to support larger DNSSEC traffic for both Authoritative and Caching DNS servers
- Customer edge devices like routers and home gateways may also impact the ability to deploy DNSSEC in the long term as DNS services move closer to the customer
    - There is currently standards work happening to help define how home gateways and routers should work with DNSSEC and IPv6
- Choose your Registrar wisely
    - Make sure they support DNSSEC on the TLDs you have domains, and that they can handle DS record insertion for you
    - Validate that they can support 24/7/365 support for key rollovers

Some Additional Thoughts

- Global Services Load Balancing and Content Delivery Networks
  - How to balance responses in different regions and how to deal with services that are slaved to remote systems?
  - How to respond with different signed records in different regions?
- Dealing with delegation zones
  - How do you get DS records up and down the tree with automation?
- End user validation
  - How do we get validation closer to the customer?

Resources

- There are many resources on the Internet to learn about DNSSEC and help prepare for a deployment
  - https://www.dnssec-deployment.org/
  - http://www.dnssec.net/projects
  - https://www.dns-oarc.net/
  - https://data.iana.org/root-anchors/draft-icann-dnssec-trust-anchor.html
  - http://www.nlnetlabs.nl/publications/dnssec_howto/
- Testing
  - https://addons.mozilla.org/en-US/firefox/addon/64247/
  - http://dnsviz.net/
  - https://www.dns-oarc.net/oarc/services/replysizetest
  - https://www.dns-oarc.net/oarc/services/odvr
  - http://www.bortzmeyer.org/tests-dns.html
- Tools
  - https://www.dnssec-tools.org/
  - http://www.kirei.se/xfiles/dnssec/ta-tool.pl
  - http://www.opendnssec.org
  - http://www.isc.org/software/bind/dnssec

IPv6 and DNS

- Transition to end user dual-stack IPv6 environments will drive the need for deployment of dual-stack on DNS servers
  - Begin turning up IPv6 on caching and authoritative DNS servers
- Deployment strategies
  - Audit end to end IPv6 connectivity to and from DNS platforms
  - Verify operations tools will function with IPv6
  - Use of Anycast for IPv6 address
  - Test and deploy AAAA records for Authoritative data
  - No more pre-populating PTR records! Its just simply not possible
    - DDNS and wildcards can be used instead
    - We have found the need to still deploy empty PTR zones delegated from ARIN
      - Some tools like ssh performs DNS lookups which will cause long delays if no message is returned like an NXDOMAIN
- ISOC World IPv6 day is a great opportunity to test connectivity so start planning now

Thank You!

For more information on the Comcast DNSSEC and IPv6 deployments:

http://www.dnssec.comcast.net
http://www.comcast6.net
Chris Griffiths
chris_griffiths@cable.comcast.com

NATIONAL ENGINEERING & TECHNICAL OPERATIONS