Comcast DNSSEC Trial Test Bed

Chris Griffiths

Principal Engineer – DNS and Network Management

Product Engineering

Overview

- What is DNSSEC
- DNSSEC at Comcast
- Test Platforms
- Deployment Learnings
- Performance
- Related Initiatives at Comcast
- Looking Forward
- Resources

What is DNSSEC

- DNSSEC (Domain Name System Security Extensions) provides validation of data requested in DNS lookups. It verifies that the data received by a recursive server matches the data on the authoritative server and that the zone wasn't modified in transit.

- DNSSEC doesn't encrypt data. It only adds an authentication record that can be verified by a recursive server.

- DNSSEC is backwards compatible. A recursive server can ignore the signing information and return a normal response.

DNSSEC at Comcast

- 14.7 million broadband subscribers
- Protecting our subscriber facing recursive clusters is our highest DNS priority
- Current recursive infrastructure is not vulnerable but we cannot sit back and wait for the next big bug/exploit
- DNSSEC has been on our internal DNS roadmap
- Kaminsky Vulnerability increased our priority to test and deploy DNSSEC

Test Platforms deployed

- DNSSEC-capable resolvers have been deployed into our production Comcast High-Speed Internet network.
  - Nominum Vantio
  - ISC BIND
  - Unbound
- These resolvers are available for any IPv4 address to query.
- Trial info is available at http://www.dnssec.comcast.net.
- This is available for the DNS community at large to test against.
- Contact us if you'd like to obtain error logs or need other support.
- Contact us if you'd like us to add a key for testing a domain

Available for DNS Community Testing

- We have loaded the following ccTLD public keys in use worldwide:
  - .br
  - .bg
  - .pr
  - .se
  - .cz
- A Comcast sub-domain has been signed: dnssec.comcast.net
- Also loaded public keys for:

e164.arpa
ripe.net
ripencc.com
ripencc.net
ripencc.org
ripe-ncc.com
ripe-ncc.net
ripe-ncc.org
ripe.int
89.in-addr.arpa
90.in-addr.arpa
213.in-addr.arpa
193.in-addr.arpa
195.in-addr.arpa

212.in-addr.arpa
194.in-addr.arpa
145.in-addr.arpa
217.in-addr.arpa
62.in-addr.arpa
77.in-addr.arpa
78.in-addr.arpa
79.in-addr.arpa
87.in-addr.arpa
83.in-addr.arpa
84.in-addr.arpa
86.in-addr.arpa
88.in-addr.arpa
80.in-addr.arpa

81.in-addr.arpa
141.in-addr.arpa
91.in-addr.arpa
92.in-addr.arpa
93.in-addr.arpa
94.in-addr.arpa
95.in-addr.arpa
188.in-addr.arpa
151.in-addr.arpa
82.in-addr.arpa
85.in-addr.arpa
0.4.1.0.0.2.ip6.arpa
1.4.1.0.0.2.ip6.arpa
4.1.1.0.0.2.ip6.arpa

5.1.1.0.0.2.ip6.arpa
6.0.1.0.0.2.ip6.arpa
6.1.1.0.0.2.ip6.arpa
7.0.1.0.0.2.ip6.arpa
7.1.1.0.0.2.ip6.arpa
7.4.1.0.0.2.ip6.arpa
8.0.1.0.0.2.ip6.arpa
9.0.1.0.0.2.ip6.arpa
a.0.1.0.0.2.ip6.arpa
a.1.1.0.0.2.ip6.arpa
a.4.1.0.0.2.ip6.arpa
b.0.1.0.0.2.ip6.arpa
b.1.1.0.0.2.ip6.arpa
b.4.1.0.0.2.ip6.arpa

c.4.1.0.0.2.ip6.arpa
d.4.1.0.0.2.ip6.arpa
0.a.2.ip6.arpa
4.2.0.0.1.6.0.1.0.0.2.ip6.arpa
5.2.0.0.1.6.0.1.0.0.2.ip6.arpa
6.2.0.0.1.6.0.1.0.0.2.ip6.arpa
7.2.0.0.1.6.0.1.0.0.2.ip6.arpa
uk-dnssec.nic.uk
dlv.isc.org
dnsops.gov
dnsops.biz

Deployment Learnings

- Signing of internal zone
  - Currently a manual process
  - Seems complex generating ZSK’s and KSK’s
  - Additional complexity by having to rollover keys
    - RFC states 30 days for ZSK and 1 year for KSK
    - Keyset expiry issues
    - Use of over lapping keys for ZSK and KSK to avoid expiration
  - Not many DNSSEC tools available to manage signing of zones and maintenance of keys
  - Process of signing zones every time a change is made has to be automated for an enterprise deployment
    - Some form of zone management engine/platform with a scheduler would be optimal to avoid human error for zone and key signing processes
- What processes are available to publish signed zones to the world?
- Understanding processes of updating registries when well know TLDs are signed.

Deployment Learnings cont’d

- Loading known public keys of signed zones
  - Spent a lot of time finding keys for different signed domains
  - No one repository was available for providing a list of all trust anchors
    - Looking forward to IANA’s global trust anchor repository
    - ISC DLV repository available
      - Look aside validation is specific to BIND and now supported by Unbound
    - Haven’t published test domain KSK with ISC DLV yet

Performance

- Platforms tested with DNSSEC
    - Nominum Vantio
    - ISC BIND
    - Unbound

- Impact on authoritative infrastructure
    - Increased memory footprint
        - ~5-9 times
        - If you have large zones and/or a lot of zones need to seriously think about breaking up the zones
            - Ex: Comcast roughly manages 30 million A and PTRs for subscribers
    - Disk store, startup times

- Impact on recursive infrastructure
    - Being prepared to deploy additional DNS recursive clusters
    - Impact to cache-hit ratios (mem-cache configuration)
    - Size of configuration file if root zone is not signed
        - Management of trust anchors
            - Automating the update of trust anchors for all loaded public keys

Related Initiatives at Comcast

- Working with organizations such as CableLabs and National Cable and Telecommunications Association (NCTA) to create awareness amongst the MSO community

- Adding DNSSEC related test cases to device certification processes.
  - Test report – DNSSEC impact on broadband routers and firewalls
    - http://download.nominet.org.uk/**dnssec**-cpe/**DNSSEC**-CPE-Report.pdf

Looking forward

- Sign Comcast.net top level domain
- Look to enable DNSSEC validation on recursive clusters
- Hopeful that root will be signed in the next 6-9 months
  - Reduces the complexity of searching for public keys
  - Reduces the number of third party trust anchor repositories
  - Will help with the deployment of DNSSEC
- Verisign must Sign ".COM" and ".NET" as early as possible (9-12 months)
- Large ISPs must start testing DNSSEC capable resolvers
- Large companies must look at signing their zones to put pressure on registrars and registries to support DNSSEC

Resources

- RFC 4033
- RFC 4034
- RFC 4035
- RFC 4641
- RFC 5011
- RFC 5155
- http://www.dnssec-tools.org/
- http://www.dnssec-deployment.org/
- http://www.dnssec.net/
- IETF: DNS Extensions Working Group
- IETF: DNS Operations Working Group