DNSSEC Deployment Status

- We began working on this in 2008 (see timeline)
- We completed our DNSSEC deployment in January 2012
  - All customers use our validating resolvers (>18.1M homes)
  - All Comcast domain names signed (>6,000)
Lessons Learned in Testing & Early Deployment

• Is a software upgrade required?

• Can the servers handle incremental CPU load?

• Network equipment may need to be updated
  • Will they permit both UDP and TCP traffic on port 53?
  • Can they properly handle larger DNS responses? (with EDNS0, response may go from 512 bytes to 4,000 bytes)
  • Can they handle fragmentation?

• Authoritative infrastructure may need to be augmented to support signing your zones
  • Zone signing can be resource intensive
  • This can be complex if you have many sub-zones
Lessons Learned in Testing & Early Deployment

• Best way to figure this out is to test in the lab and validate with production traffic under close observation and measurement

• If you plan this at the same time as your IPv6 upgrade, they incremental cost and work is more modest than it otherwise would be.

• Look for operational processes that may need to be adjusted to support DNSSEC validation (i.e. troubleshooting, customer FAQs)

• Add new Key Performance Indicators (KPIs) or metrics, such as:
  • # of SERVFAILs (set an alarm threshold)
  • SERVFAILs as a % of all RCODEs (set an alarm threshold)
  • When top-10 domains sign, ad hoc temporary monitors?

• For signing your zones, be sure your registrar has an automated process for updating / inserting DS records
More Recent Lessons Learned at Scale

- Different software vendors interpret the RFCs differently, causing irregular validation results
  - CNAME at the zone apex, pointing to another zone
    - mail.comcast.net in CNAME mail.g.comcast.net (a GSLB)
    - Worked if you used BIND, but not Vantio (SERVFAIL = 😞)
  - So after signing a complex domain, we recommend you validate using different resolvers
- We’ve observed registries doing ‘interesting’ things. Such as:
  - One big registrar has a “Premium” service that automatically includes DNSSEC (DNSKEY, RRSIGs, DS inserted in the TLD)
  - If you downgrade from this service, your DNSKEY and RRSIGs are deleted – BUT the DS record is not removed from the TLD
  - This causes the domain to fail validation (SERVFAIL = 😞)
- On our authoritative servers, not many DNSSEC-related RR queries as of yet (expected based on the state of validation)
  - Of the top 2,000 domains:
    - 1.75% signed – which is oddly close to the % with AAAA RRs
More Recent Lessons Learned at Scale

- As with any new technology or deployment there will be problems
  - Prepare in advance (scripts, processes, testing, practice)
  - Most common issue is incorrectly signed zones, usually related to key rollovers (mostly in the .GOV TLD)
- One solution is a “Negative Trust Anchor” to temporarily skip validation for a given domain
  - Only when an engineer has personally verified the failure is due to DNSSEC misconfiguration and, preferably, communicated with the affected domain
  - Can temporarily restore end user access while the domain fixes their problem
  - Does NOT scale, but can be helpful for high traffic and other key domains
  - Probably useful for the next 1 – 2 years as domains mature and master their signing and key rollover processes
  - Ultimately, this is the responsibility of the domain owner or administrator to get right!
Validation Failure Example – NASA.GOV

- 18 January 2012: Domain performed a Key Signing Key (KSK) rollover
  - Created new key & signed domain with new key
  - Updated DS record in .GOV TLD
  - But did not double sign with old key, which would have ensured both the old and new keys worked simultaneously
  - So the new DS record pointed to the old KSK, which was no longer in the zone
  - Chain of trust broken = validation failure = SERVFAIL
Validation Failure Example – NASA.GOV

- Customers interpreted this as us “blocking” access to the site, some recommended switching to non-validating resolvers
- “Fixed” temporarily with a Negative Trust Anchor
- In parallel, the domain administrator repaired their zone

Customers interpreted this as us “blocking” access to the site, some recommended switching to non-validating resolvers. “Fixed” temporarily with a Negative Trust Anchor. In parallel, the domain administrator repaired their zone.
Some Measurement Data

Domains with DNS Records

General timeframe when we signed over 5,000 domains

Thank You!

For more information:
http://www.dnssec.comcast.net
http://dns.comcast.net
http://dns.comcast.net