xfinity™

ICANN Meeting #38
DNSSEC Workshop

Overview of Comcast's DNSSEC Work

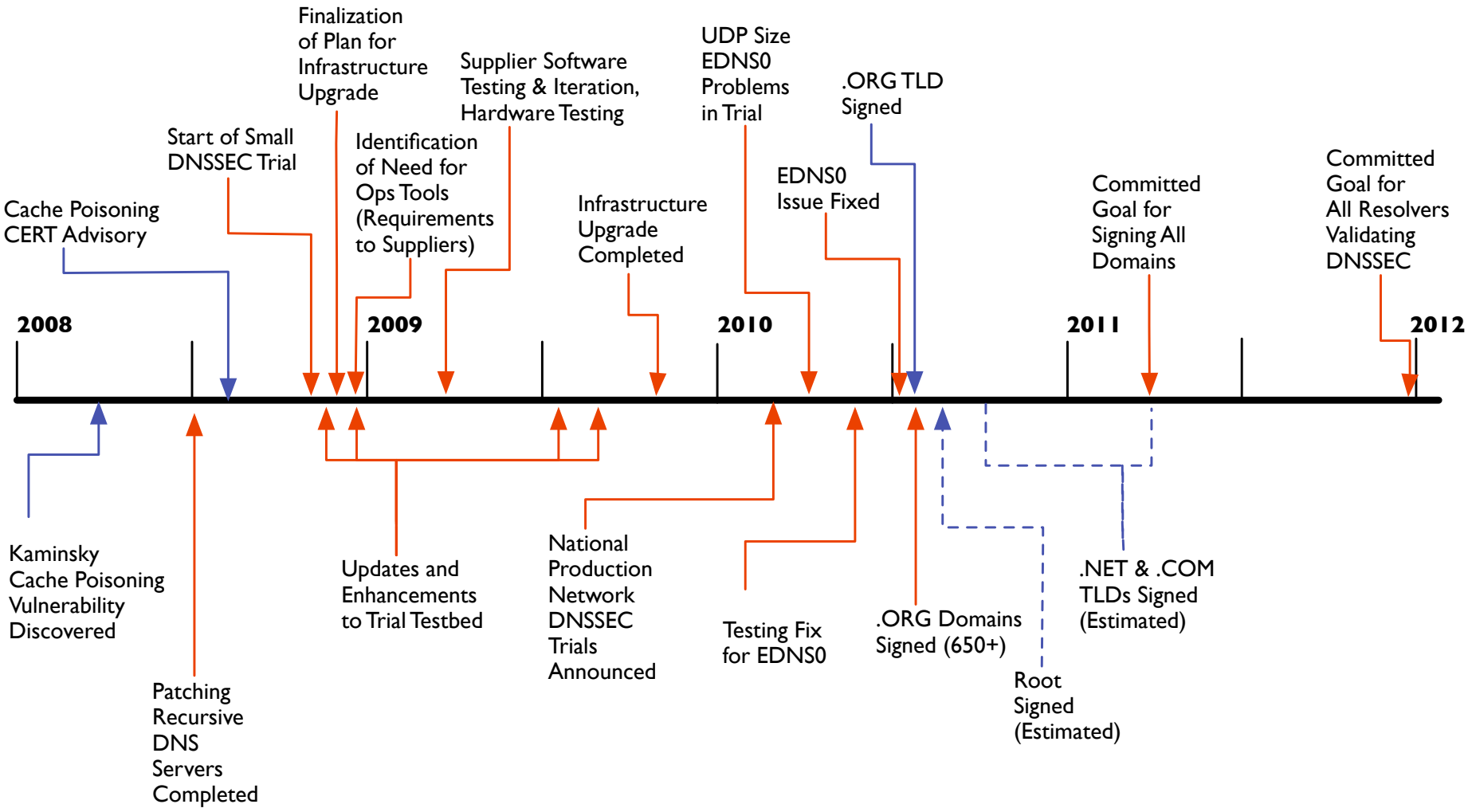
http://www.dnssec.comcast.net

Wednesday, June 23, 2010

Comcast

NATIONAL ENGINEERING & TECHNICAL OPERATIONS

Timeline of Comcast's DNSSEC Work



Interesting Issues Encountered & Other Data

- Initially, operational tools for signing zones and rolling over keys was lacking
  - This is now much improved over the past 12 months
  - We expect to learn more as we start signing in production, so we're ready to quickly iterate operational tool enhancements
- Unexpected UDP payload size issue encountered on load balancers, now resolved
  - UDP responses usually up to 512 bytes
  - But responses with DNSSEC can be up to 4,000 bytes (EDNS0)
  - Interim fix was to limit the UDP response size to 512 bytes, since fragmentation was not working as expected, forcing responses over this level to fall back to TCP instead
- During time when EDNS0 was disabled, forcing large responses to TCP, we observed less than 1% of queries used TCP (based on a sampling of recent data).
  - We enabled EDNS0 again recently, so this should now drop.
- The workload of our DNSSEC servers is very low compared to our normal peak queries per second
  - This is due primarily to the trial being opt-in
  - We are considering expanding use by having our IPv6 trial customers also use the DNSSEC-validating resolvers
  - Typical peak queries per second, in total nationally, are 250 queries per second, with a high mark of roughly 800 queries per second (a fraction of typical volume on our standard resolvers)

xfinity™

Thank You!

More info at:

http://www.dnssec.comcast.net

Comcast

NATIONAL ENGINEERING & TECHNICAL OPERATIONS