xfinity™

ICANN Meeting #38
PIR – DNSSEC Chain of Trust

Overview of Comcast's DNSSEC Work

http://www.dnssec.comcast.net

Wednesday, June 23, 2010

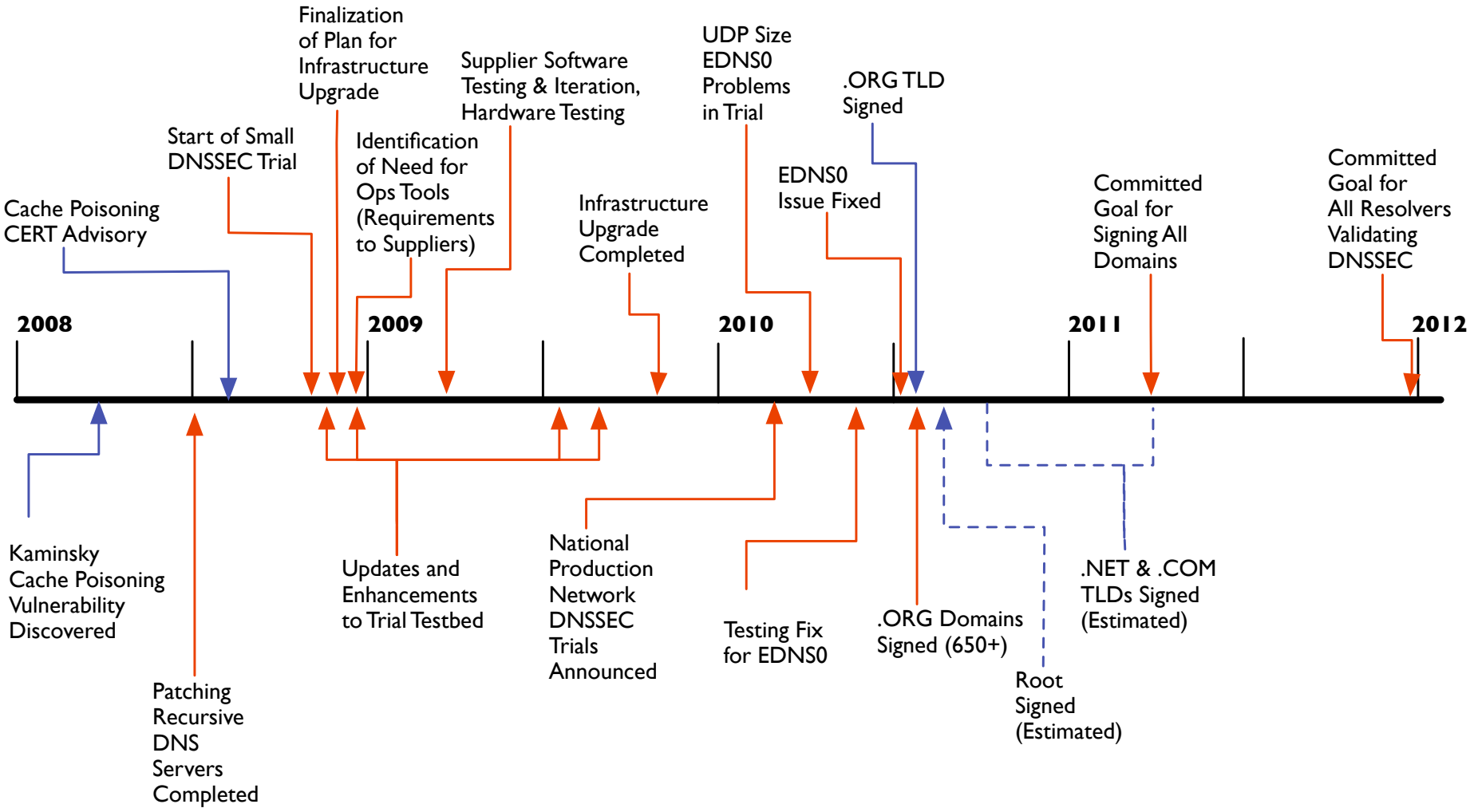
Comcast

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
- ISPs rely on a chain of trust:
  - a signed root (or ITAR)
  - a signed TLD
  - a signed domain
- Approach is:
  - ISP recursive resolver sets DNSSEC OK (DO) bit = 1
  - If validation fails for some reason, the end user's stub resolver receives a SERVFAIL response
- Comcast publicly announced our plans for DNSSEC in February 2010
  - Other ISPs need a similar plan

Timeline of Comcast's DNSSEC Work



xfinity™

Thank You!

More info at:

http://www.dnssec.comcast.net

Comcast

NATIONAL ENGINEERING & TECHNICAL OPERATIONS