DNSSEC: Lessons From A Generic TLD

James Galvin

ICANN 36 Seoul
DNSSEC Workshop
28 October 2009

www.afilias.info

Know The Material

- **Security is being added**
  - Changes everything
- **Need a good understanding**
  - There are a lot of documents
- **There are more working parts**
  - Some outside your control
- **Keep current**
  - Ask for help

Algorithms and Parameters

- Choices
  - DSA vs RSA, SHA1 vs SHA2, more
  - Key Lengths
  - NSEC vs NSEC3
- TLDs will make a choice
- Registries permit them all
- Registrars may make choices
- Registrants may want choices

New Processes

- ## KSKs and ZSKs
  - Should have more than one of each available at all times: active vs inactive

- ## Key Rollovers
  - Planned
  - Unplanned – early usage of "next"
  - Emergency – replace all

Operations - then

ORG 2006-06-20 TCP Reply pct of total queries
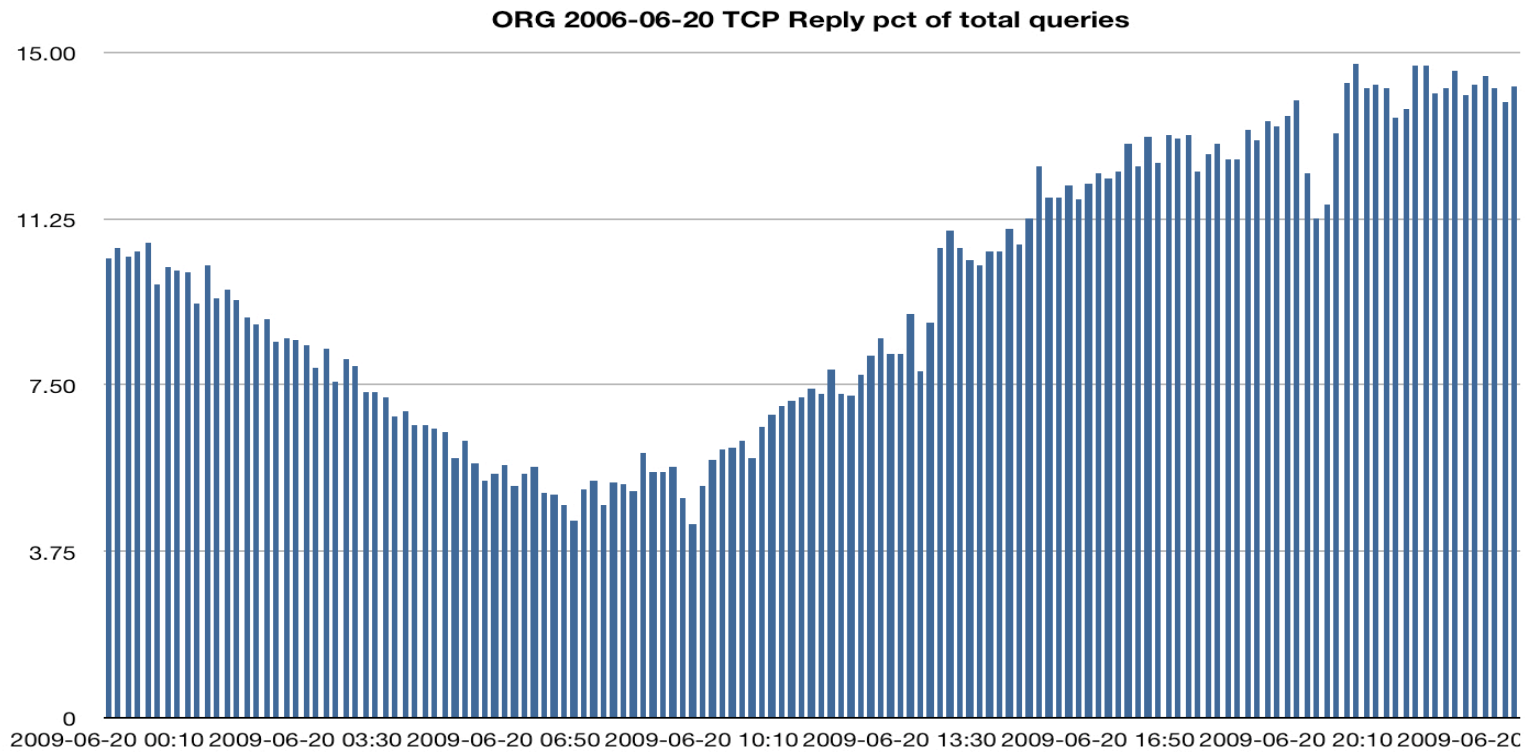
Operations - now

.ORG - TCP as Percentage of DNS Queries, 2009-08-27