

A horizontal banner with a dark blue background. On the left, there is a glowing blue globe with a grid overlay. The text "DNSSEC: Lessons From A Generic TLD" is written in large, white, bold, sans-serif font across the center. Below the text, there are faint, glowing lines of binary code (0s and 1s) and a grid pattern.

DNSSEC: Lessons From A Generic TLD

Three faint, light-colored globe icons with grid lines, arranged horizontally across the bottom left of the slide.

James Galvin

ICANN 36 Seoul
DNSSEC Workshop
28 October 2009



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

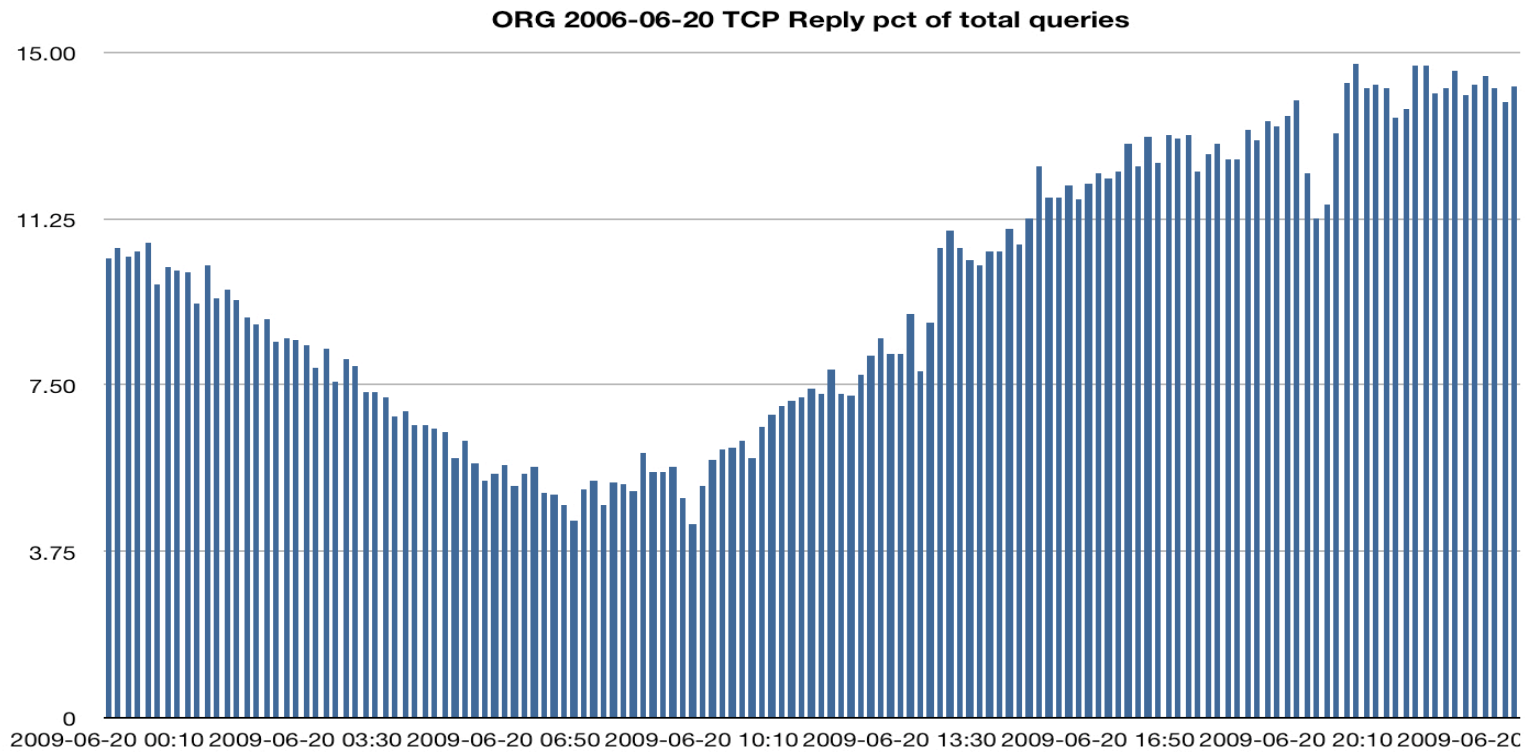
- Choices
 - DSA vs RSA, SHA1 vs SHA2, more
 - Key Lengths
 - NSEC vs NSEC3
- TLDs will make a choice
- Registries permit them all
- Registrars may make choices
- Registrants may want choices



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



Operations - now

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

