

A horizontal banner with a dark blue background. On the left, there is a stylized globe showing the Americas in a lighter blue. Overlaid on the banner are several lines of white binary code (0s and 1s) that appear to be receding into the distance. The title "DNSSEC: Lessons From A Generic TLD" is written in large, white, sans-serif capital letters across the center of the banner.

DNSSEC: Lessons From A Generic TLD

A large, faint, light-gray world map is visible in the background of the lower half of the slide, spanning across the left and center areas.

James Galvin
internet dagarna '09
5 November 2009



Topics

- Know the Material
 - Algorithms and Parameters
 - Understanding Interactions
 - Making Choices
- New Processes
- Operations



Know The Material

- Need a good understanding
 - There are a lot of documents
- Security is being added
 - Changes everything
- Keep current
 - Ask for help



Algorithms and Parameters

- Algorithms
 - DSA vs RSA
 - SHA1 vs SHA2
 - next?
- Key lengths
- NSEC vs NSEC3
 - Zone walking vs performance



Understanding Interactions

- MaxSigLife: when a signature expires
- TTLs (DNSKEY, RRSIG)
- TTLs must be $<$ signature lifetime
- When to re-sign zone
 - Before signatures expire



Making Choices

- TLDs will make a choice
- Registries should 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

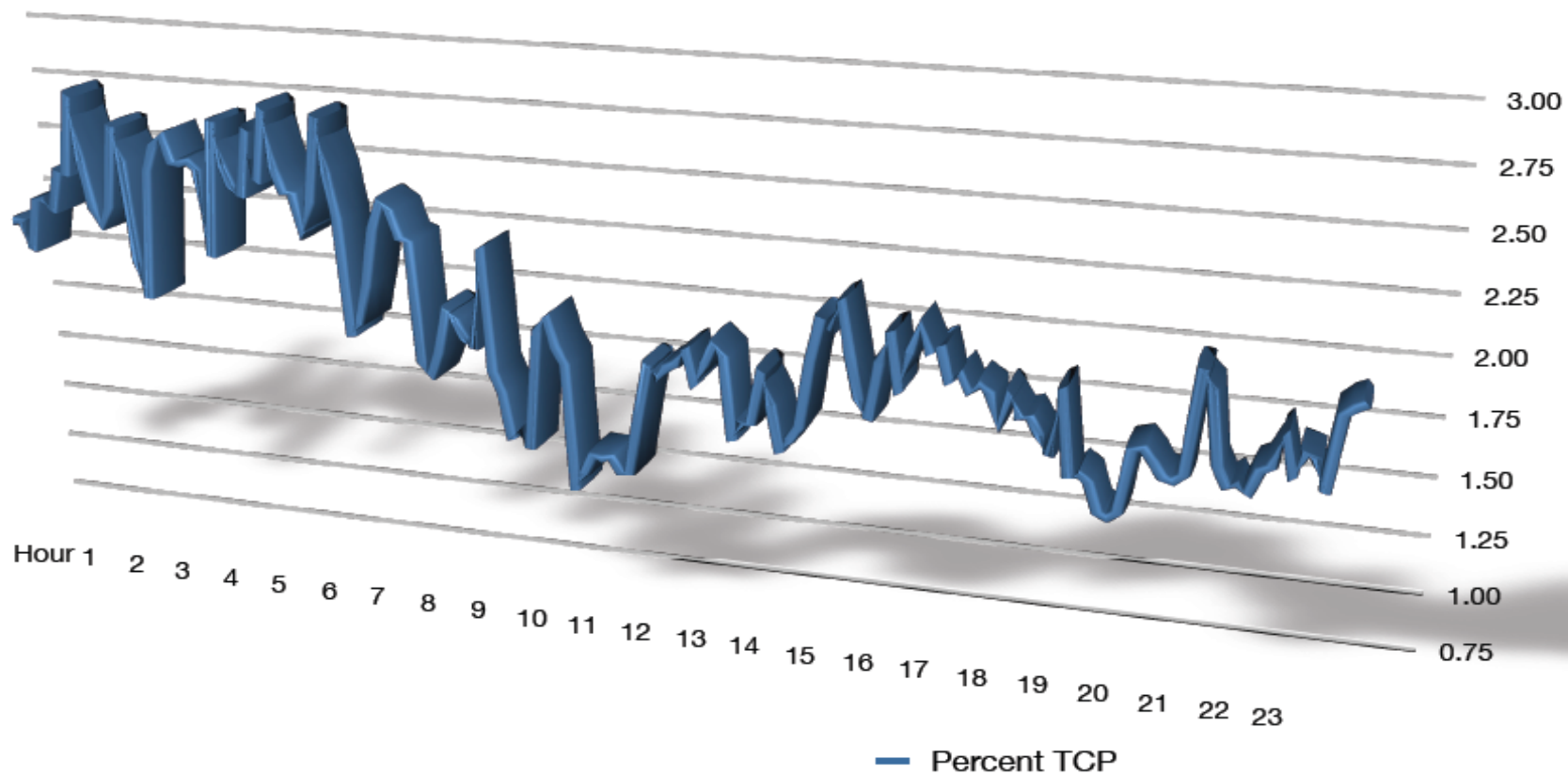


Operations - More Parts

- Last mile – validating resolvers
 - Not under your control
- Routers and firewalls
 - Sweden experience
 - Still at risk two years later
- Operational changes

Operations – TCP Replies

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





Thank You!

- Questions and Discussion

