NIST DNSSEC Project

DNSSEC Deployment in the .gov TLD

Scott Rose, NIST

scott.rose@nist.gov

LISA 2012, San Diego CA

Dec. 14, 2012

What This Talk Will Cover

- DNSSEC deployment drivers in the US Federal government
- How did deployment progress?
  - SPOILER ALERT: It wasn't speedy
- Addressing poor deployment progress
- Errors in deployment
- What lessons were learned?
  - i.e. If we could start over, what would I do different?

- This talk will not be about how DNSSEC works

Drivers of DNSSEC Deployment

- Black Hat 2008 – Kaminsky Bug presented.
- Same month: OMB-08-23 issued
  - .gov to be signed Jan 2009
  - Rest of Federal (Executive Branch) zones by Dec 2009
- DNSSEC added to Federal Information Security Measurement Act (FISMA) controls
  - All Federal information systems fall under this regulation.

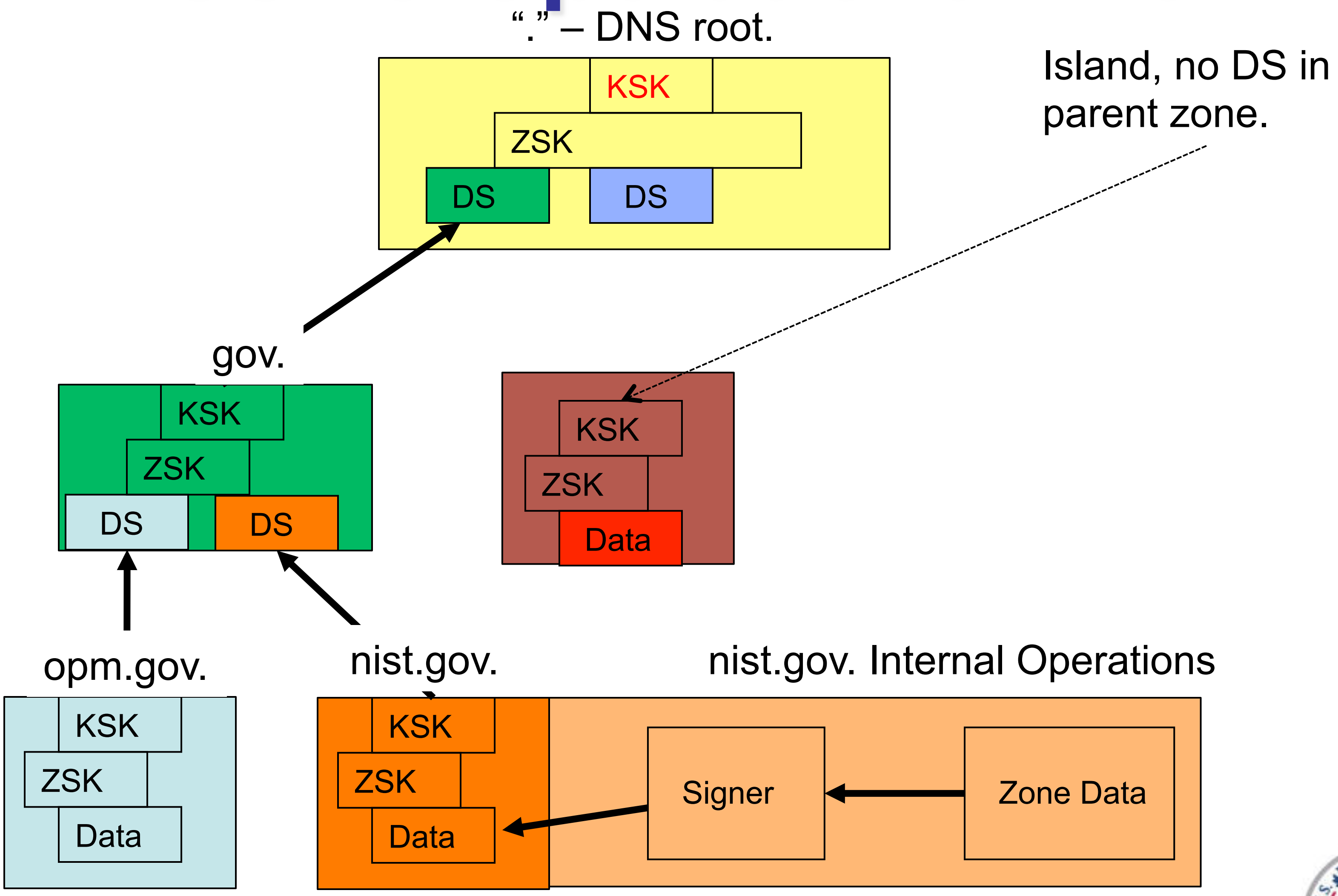
So How Did We Do?

- At first: Not good.
  - The .gov TLD signed Feb 2009
  - Less than 30% of child zones met their deadline
- Error rates high
  - 10% plus of (signed) zones had errors on a given day
    - Very few caught by operators or noticed by clients (validation rarely seen)
  - Some lingered in error state for weeks

Deployment Challenges

- Time is now a factor
  - Regular care and feeding required (i.e. resigning) even if DNS zone data has not changed.
- Increased Parent-Child Interaction
  - Child zones upload key material to Parent zone
- New operations require time, training to learn
  - Or (sometimes) new equipment or service change

DNSSEC Operational Flow



DNSSEC Tiger Team

- Formed in April 2011 to address lagging deployment in .gov and failed security audits
  - Chartered by the Federal CIO Council and composed of volunteers from various agencies.
  - Held monthly meetings to discuss progress, issues and roadblocks to deployment.
- Helped produce training material, monitoring tools and discussion forums for USG admins.

Impact of Tiger Team Activity

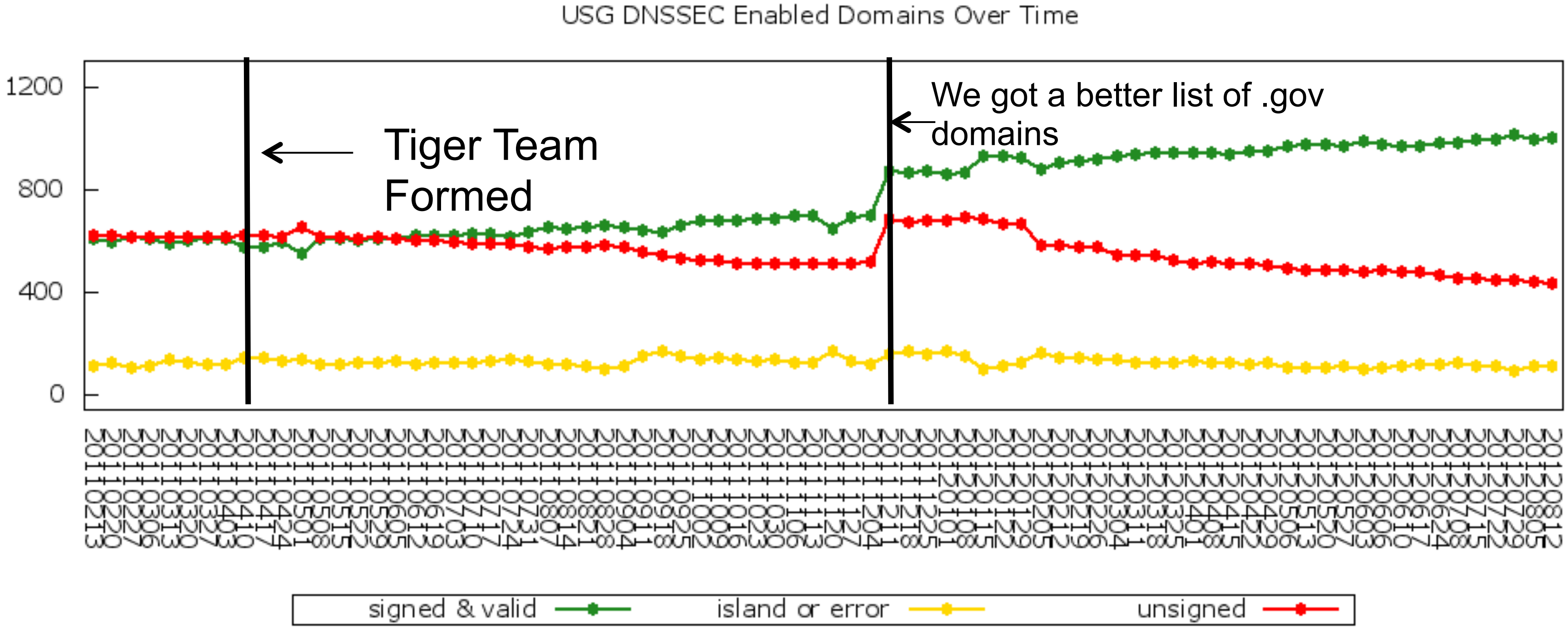


Table taken from the NIST IPv6 and IPv6 monitor showing total number of zones instead of number of agencies.

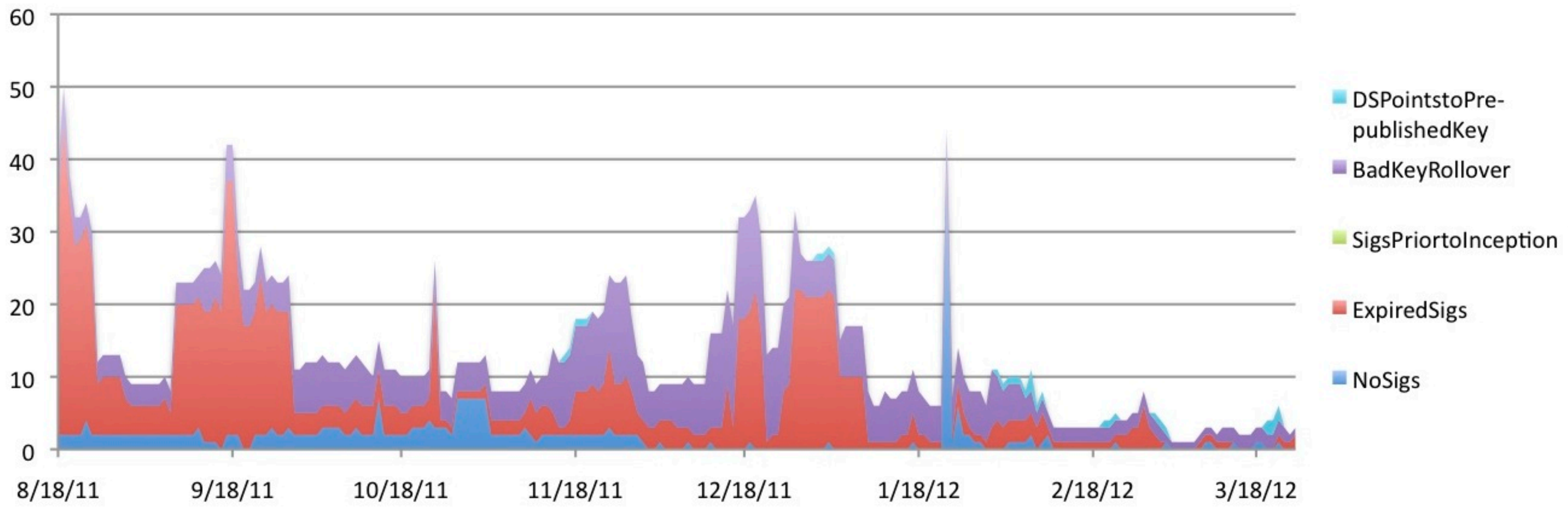
However, the trend is the same.

What the Numbers Mean

- Signed and Valid: We see DNSSEC signatures and a secure link from the .gov TLD
- Unsigned: No DNSSEC
- Error or Island: DNSSEC signatures are found over data, but we couldn't validate it.
  - Error in deployment
  - No link from .gov (very common part of deployment progress: sign zone first, link from .gov second).

Errors Seen in .gov

Number of Daily Errors Obtained via Scanning Zone List at data.gov



Definition of Errors Seen

- No Sig: Zone was signed and DS in .gov, but signatures or keys missing.
- Expired Sigs: RRSIG RR’s expiration time has passed (no longer valid)
- Sigs prior to inception: RRSIG inception time in the future.
- Bad KSK rollover: Key mismatch between .gov and zone
- DS points to pre-published key: DS in .gov points to KSK not in use in zone
- Other: Some non-DNSSEC error e.g. server down, etc.

Response to Errors

Errors Seen	April 2011		April 2012	
	Number Errs.	Avg. Days to Resolution	Number Errs	Avg Days to Resolution
NoSigs	41	2	6	1
ExpiredSigs	21	6	4	2
SigsPriorto-Inception	1	9	0	0
BadKeyRollover	3	14	2	12
DSPointsToPre-PublishedKeys	6	9	3	3

Lessons Learned

- Set up a monitoring regime to report errors.
- Insure each organization provides up to date POC for zone and/or security operations.
  - Who to contact when things go wrong.
- Encourage automation for applicable DNSSEC operations (e.g. resigning).
- Foster an internal community for admins to discuss issues, ask questions, etc.
  - Closed membership, if necessary