

# Facilitating Global DNSSEC Deployment

Casey Deccio  
Sandia National Laboratories

NANOG 54  
DNS Track  
Feb 7, 2012



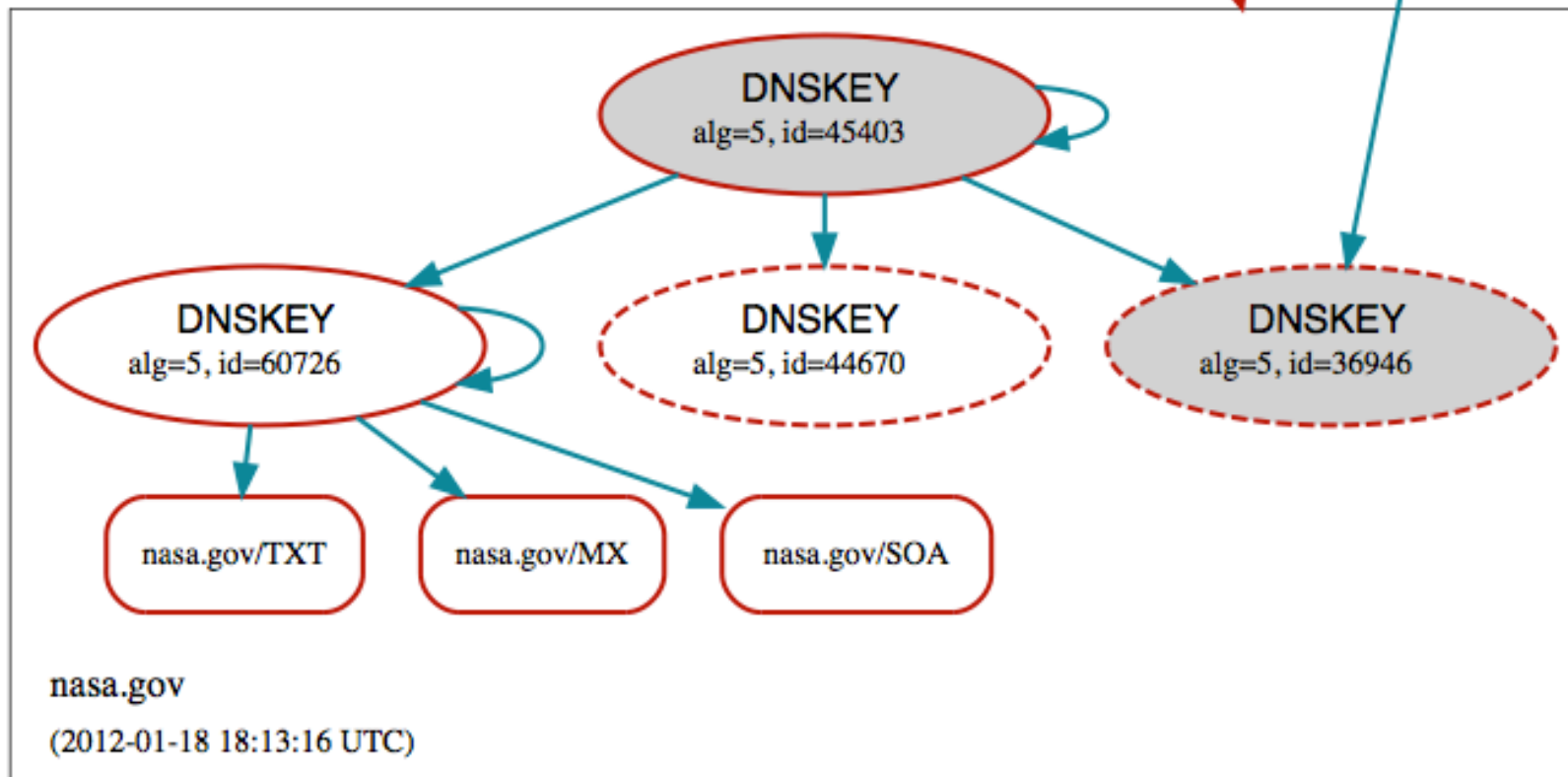
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

# DNSSEC Misconfiguration



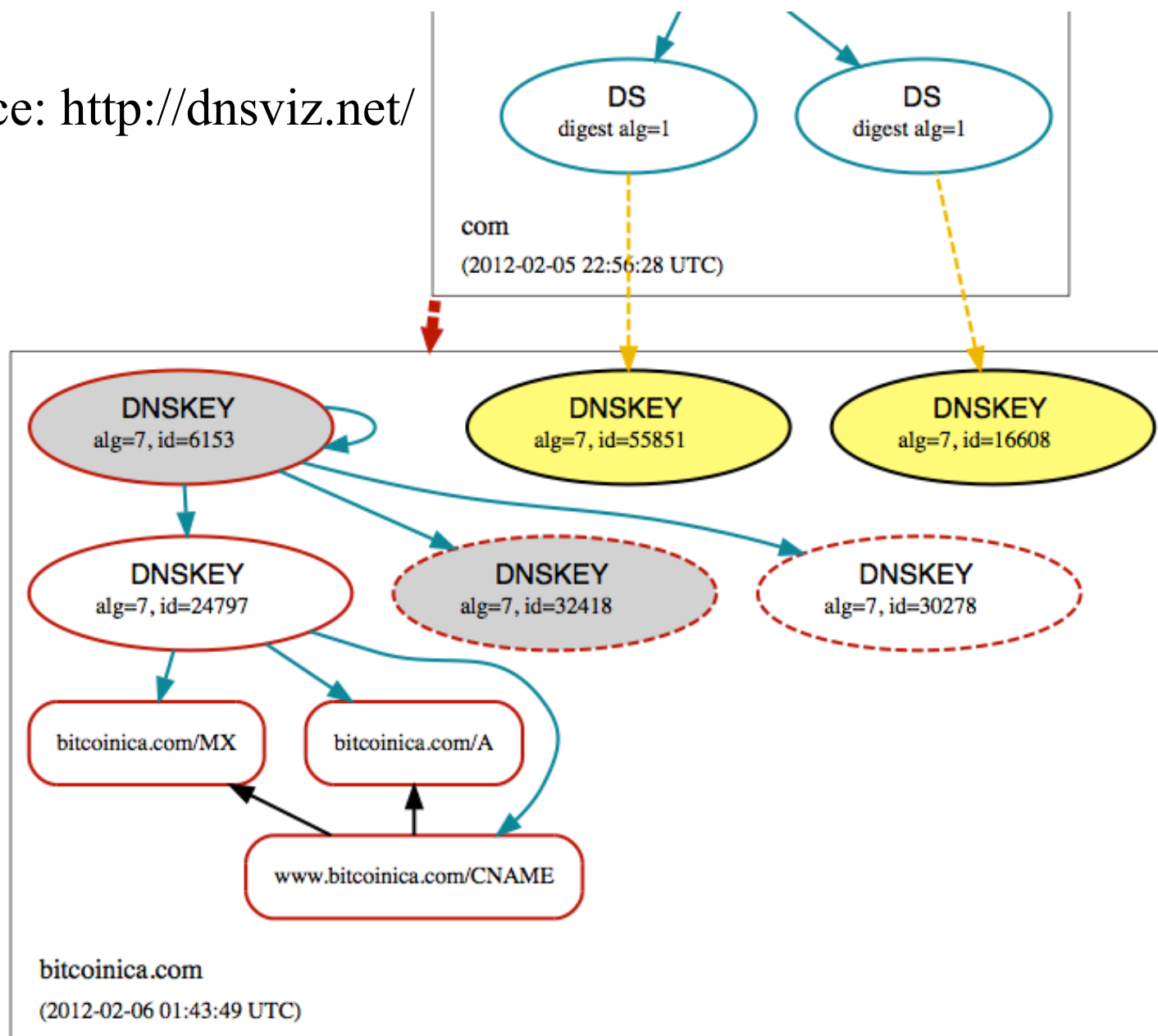
- **DS Mismatch** – No DNSKEY matching DS in parent zone
- **DNSKEY Missing** – DNSKEY not available to validate RRSIG
- **NSEC Missing** – NSEC RRs not returned by authoritative server
- **RRSIG Missing** – RRSIGs not returned by some servers
- **RRSIG Bogus** – Signature in RRSIG does not validate
- **RRSIG Dates** – Expired or premature RRSIG dates

Source: <http://dnsviz.net/>



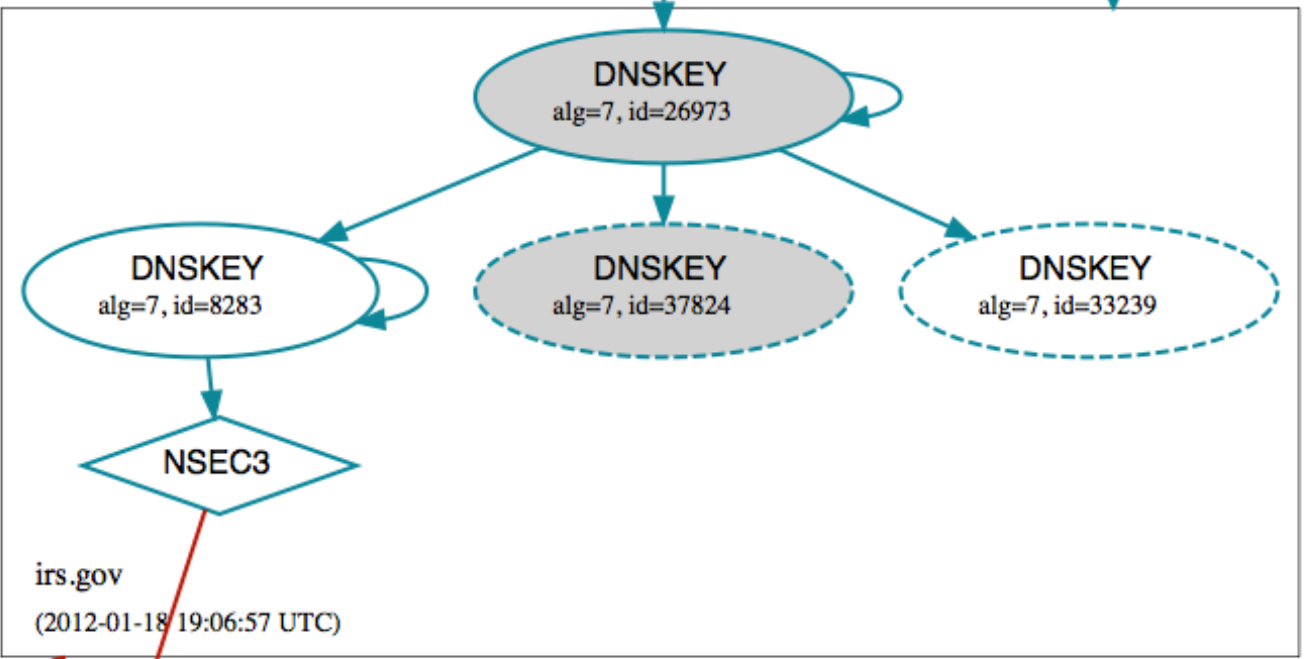


Source: <http://dnsviz.net/>





(2012-01-18 18:26:44 UTC)



irs.gov  
(2012-01-18 19:06:57 UTC)



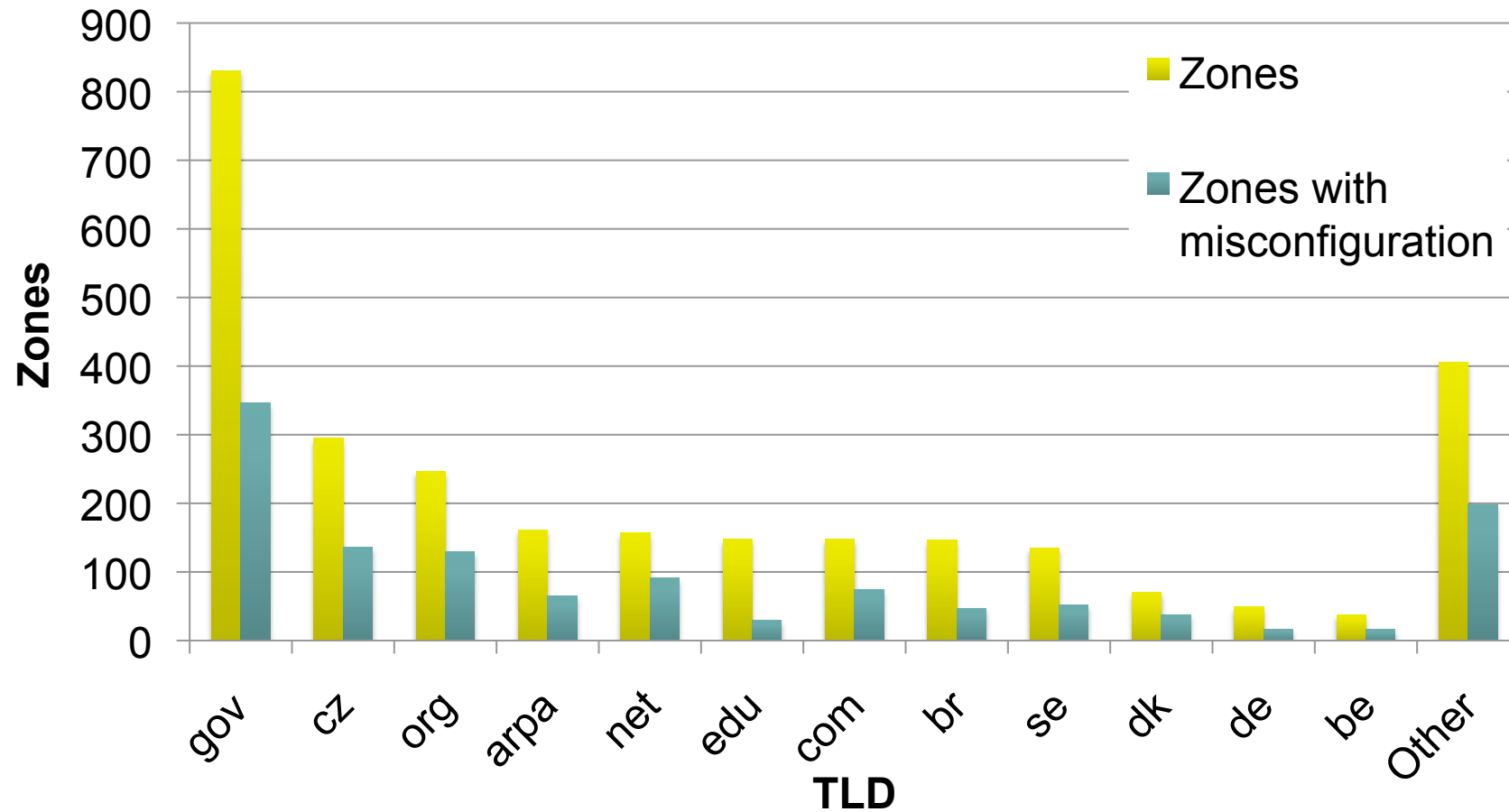
Source: <http://dnsviz.net/>

# DNSSEC deployment survey

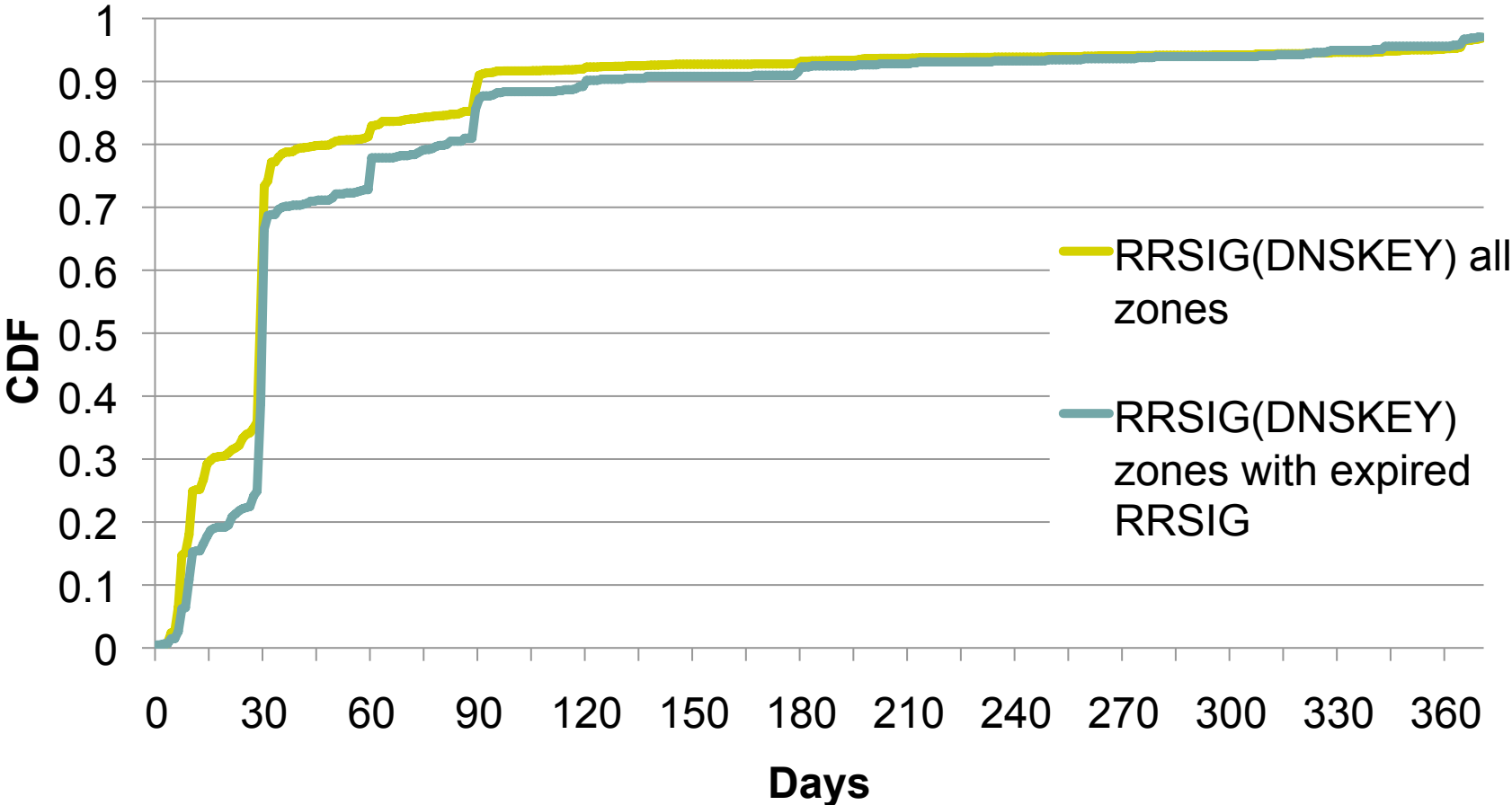


- Polled ~2,700 production signed zones over a year time frame (May 2010 – July 2011)
- Validation of SOA RR analyzed several times daily, anchored at ISC DLV or root zone (after July 2010 root signing)
- Identified maintenance and misconfigurations

# Survey breakdown by TLD

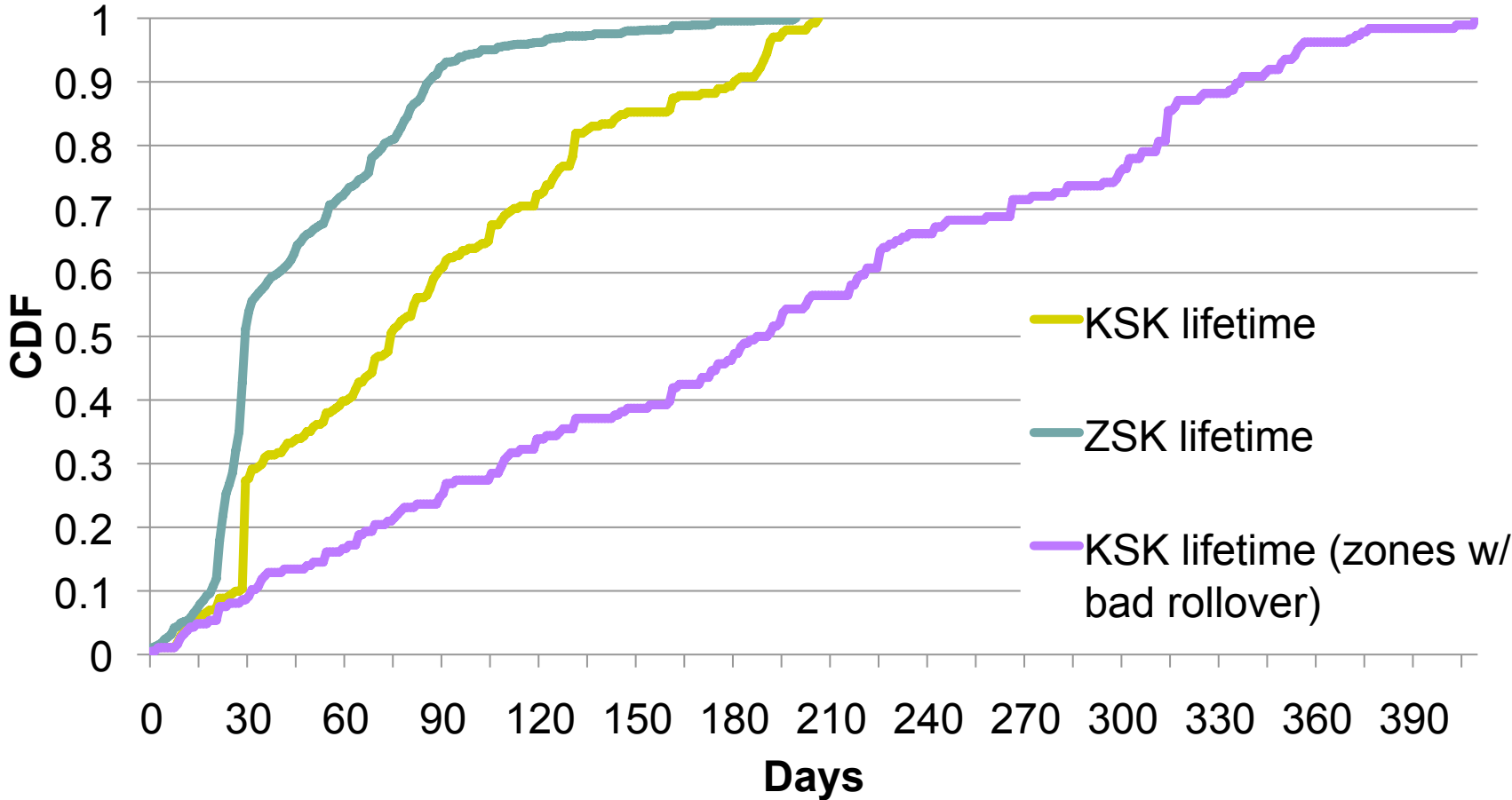


# RRSIG lifetimes





# DNSKEY lifetime



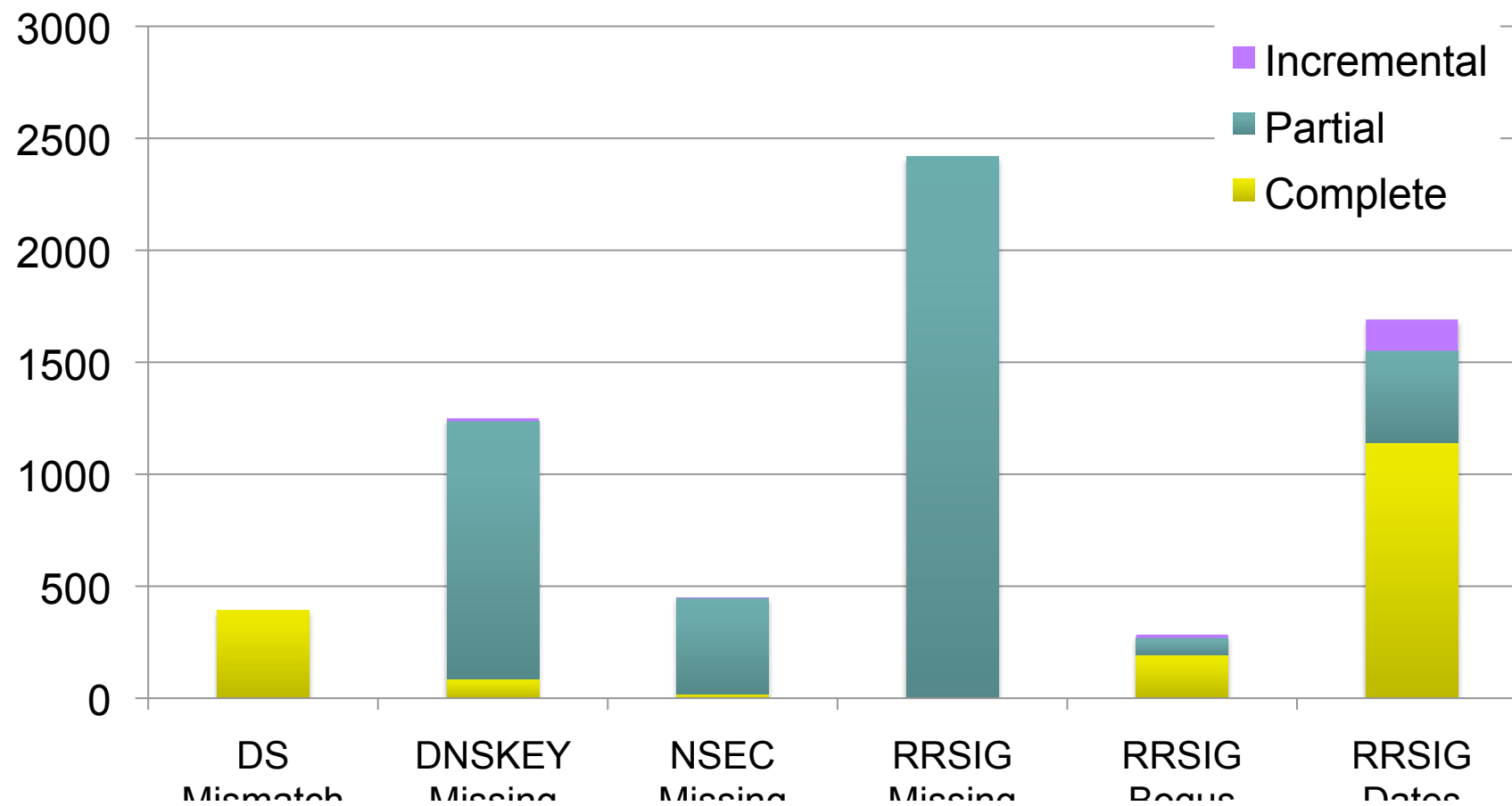
# DNSKEY rollovers



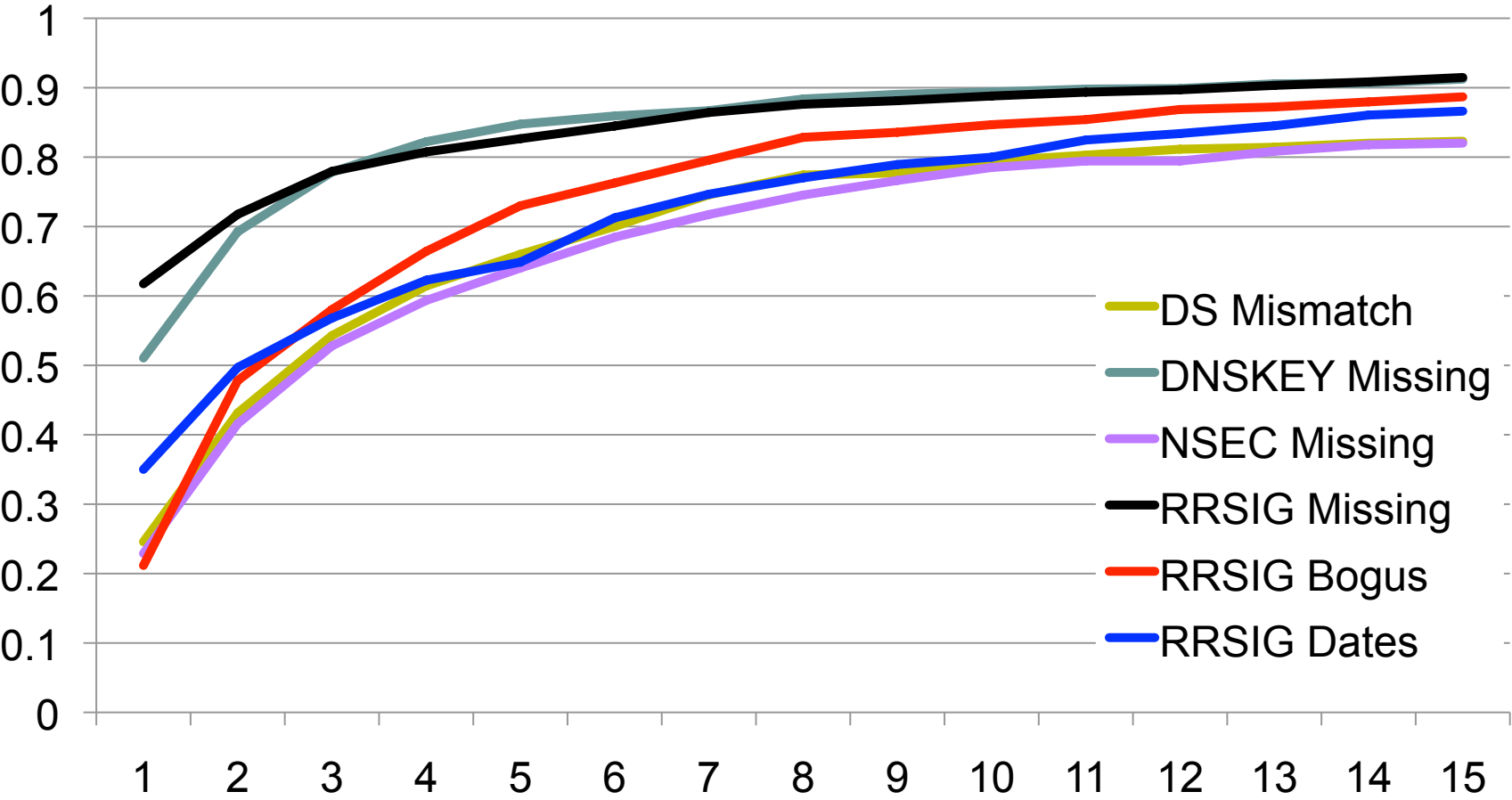
Key role	Zones that did not roll key (0)	Zones that rolled key once (1)	Zones that rolled key more than once (>1)
ZSK	37%	11%	52%
KSK	72%	17%	10%



# Misconfigurations by type

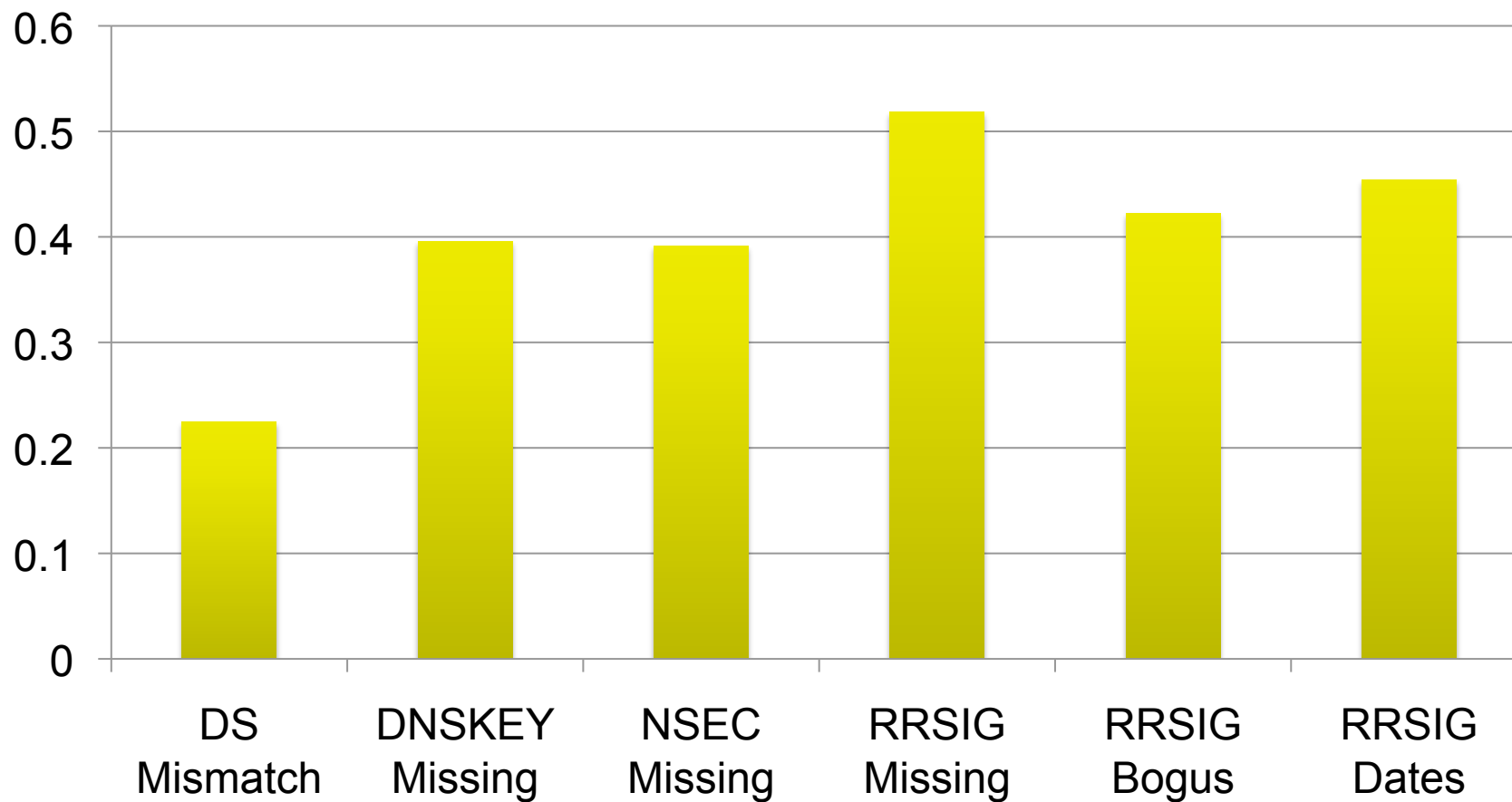


# Event duration





# Repeat offense rate



# Summary of Observations



- Administrators aren't detecting and correcting their DNSSEC problems in a timely fashion.
- Administrators aren't learning from past mistakes.
- There are varying levels of DNSSEC support in production DNS implementations.
- DNSSEC implementations are new and still being improved.

# How do we “sell” DNSSEC?



- Are we selling DNSSEC with too much maintenance complexity?
- What are the essential elements for successful DNSSEC deployment?
- How do we appropriately educate engineers and administrators of sophisticated DNSSEC maintenance?
- Does DNSSEC make sense for all domains?
- What are best current operational practices for DNSSEC?
  - Root zone
  - TLD
  - Major site
  - Other site

# Deployment Considerations



- RRSIG lifetime
- NSEC/NSEC3
- Regular KSK rollovers
- Signing of reverse zones
- Use of HSMs for offline key storage
- DNS hosting/registrar transfer