Assessing and Improving the Quality of DNSSEC Deployment

SAND2012-2068P

Casey Deccio, Ph.D.
Sandia National Laboratories

AIMS-4
CAIDA, SDSC, San Diego, CA
Feb 9, 2012

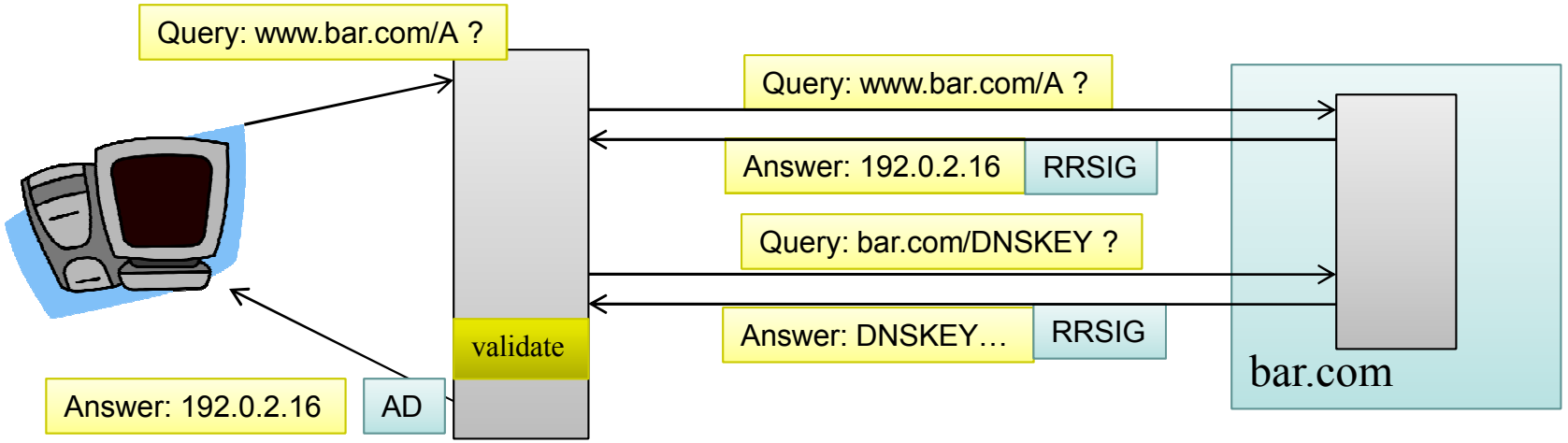
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Outline

- DNSSEC protocol review
- DNSSEC maintenance and misconfiguration
- DNSSEC survey and results
- Conclusions and solutions

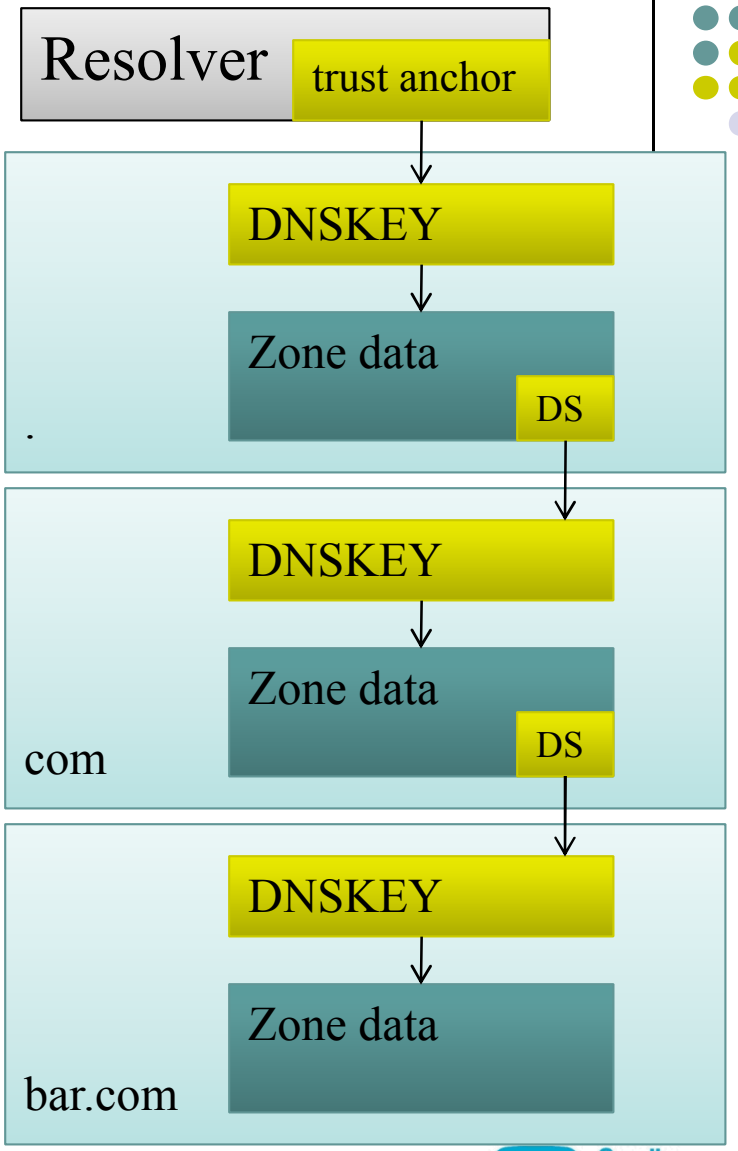
DNS Security Extensions (DNSSEC)

- RRsets signed with zone's private key(s)
- Signatures covering RRsets returned by server as RRSIGs
- Public keys published in zone data as DNSKEYs
- Resolver validates response
  - If authentic: Authenticated data (AD) bit is set
  - If bogus: SERVFAIL message is returned



Scalable authentication via a chain of trust

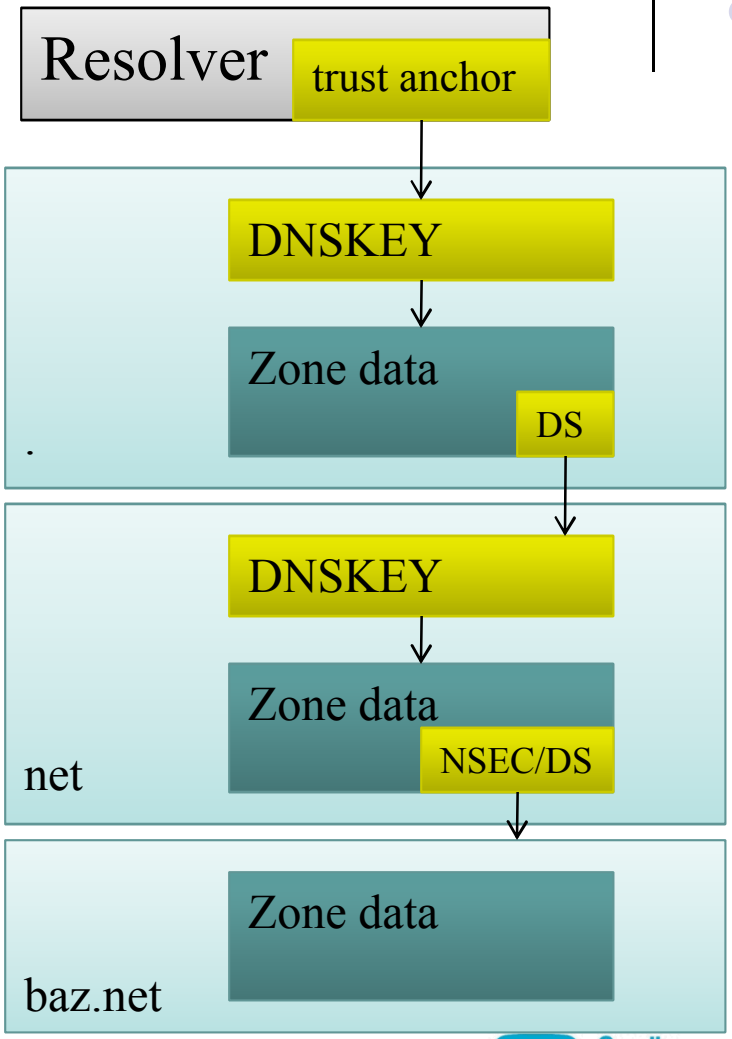
- DNSKEY must be authenticated
- Resolver must have some notion of trust
- Trust extends through ancestry to a trust anchor at resolver
- DS resource record – provides digest of DNSKEY in child zone



Sandia National Laboratories

Backwards compatibility… kind of

- If no secure link exists between parent and child, referring (parent) server must prove non-existence of DS RRs
- NSEC/NSEC3 resource records provide authenticated denial of existence
- Child zones of insecure delegations may be unsigned or signed (“islands of security”)

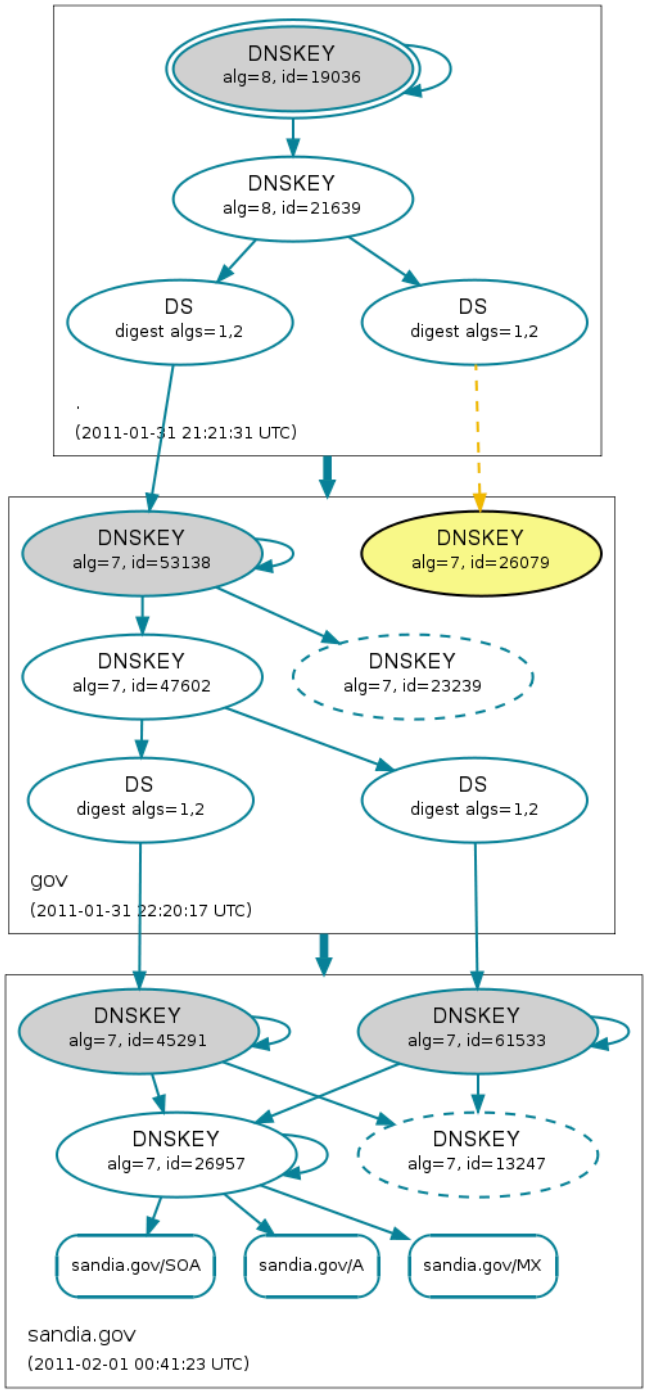


Sandia National Laboratories

DNSSEC validation status

- **Secure** – unbroken chain from anchor to RRset

sandia.gov/SOA



(Image from http://dnsviz.net/)

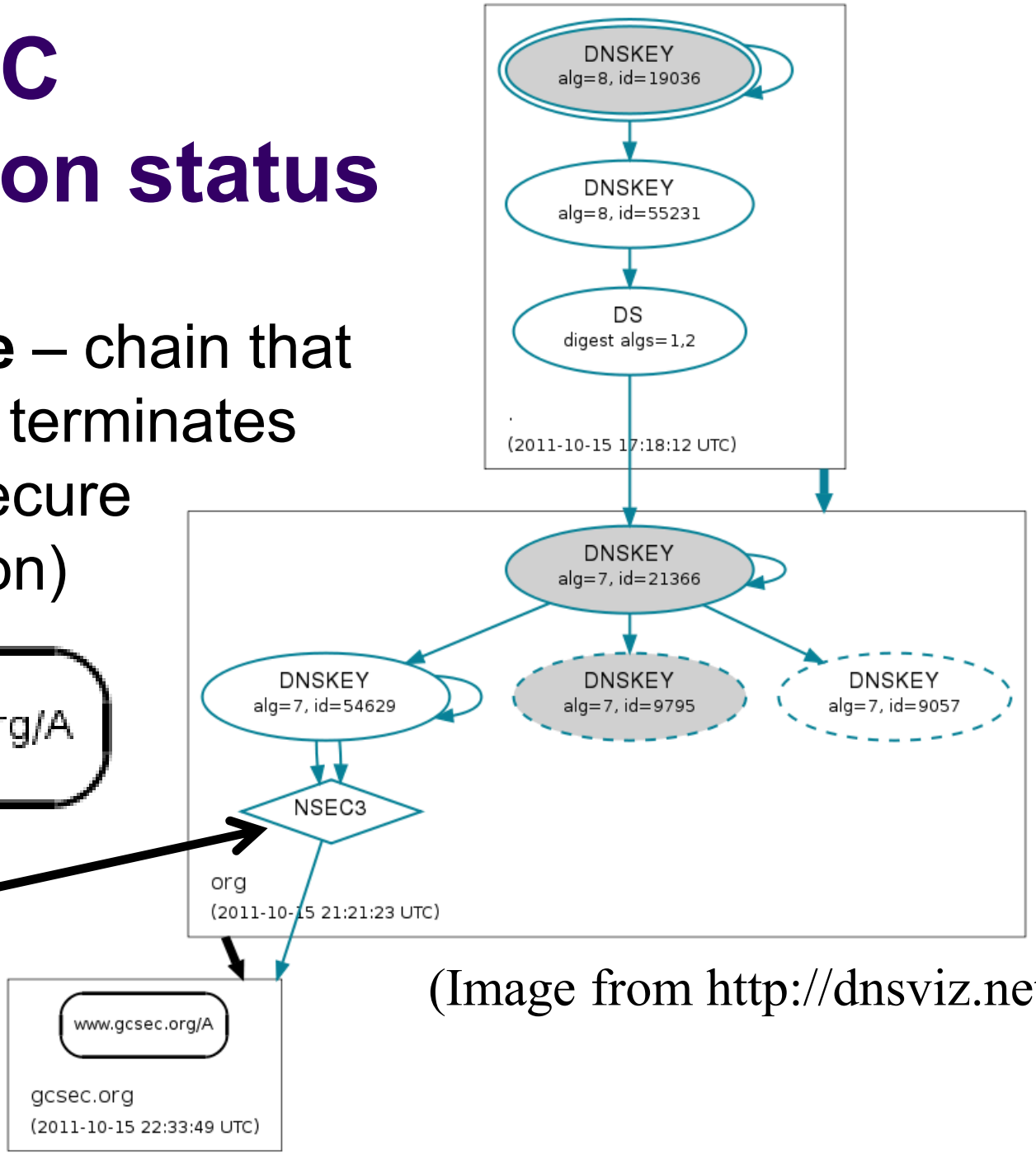
Sandia National Laboratories

DNSSEC validation status

- **Insecure** – chain that securely terminates (i.e., insecure delegation)

www.gcsec.org/A

Secure chain termination

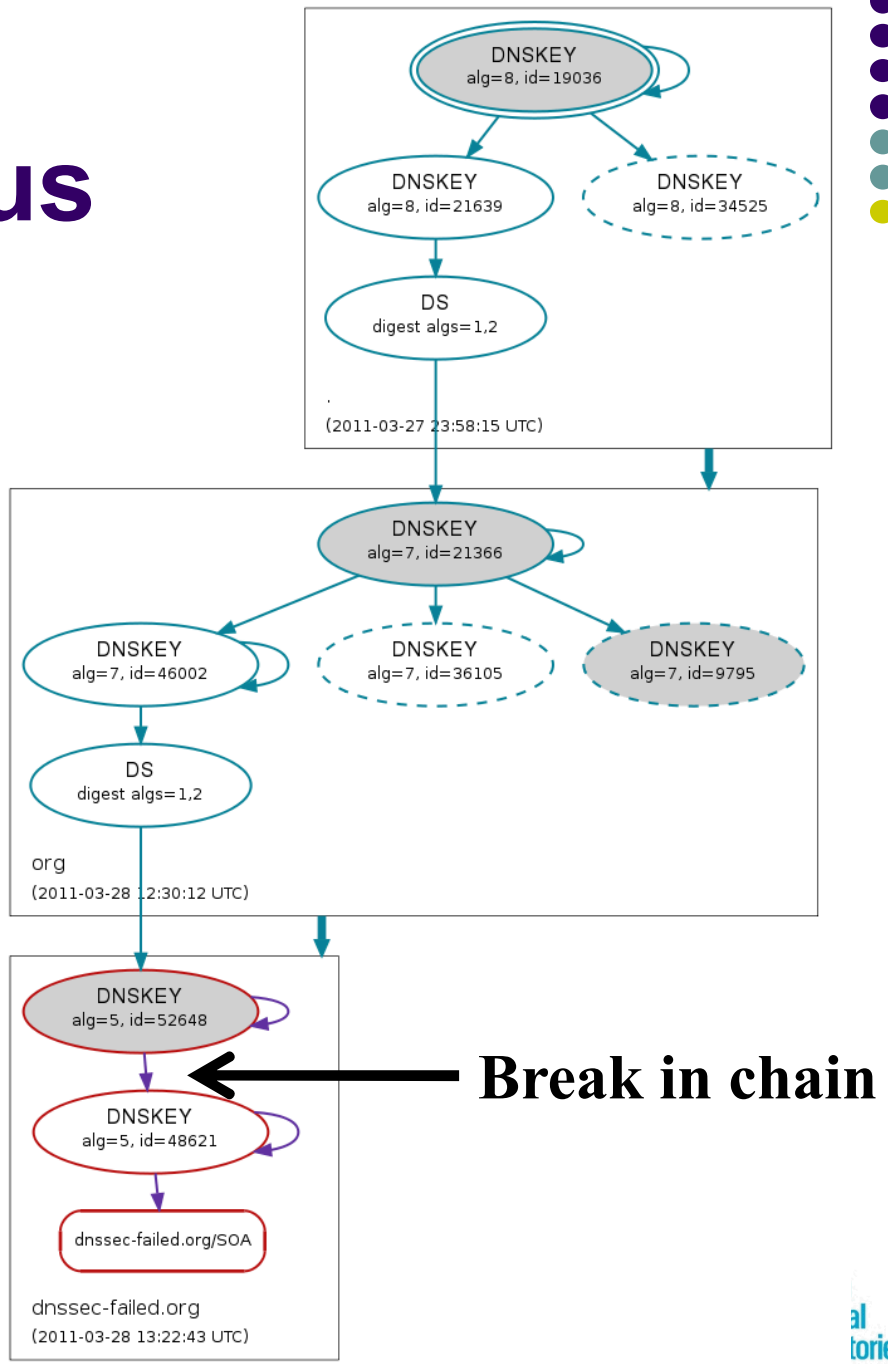


(Image from http://dnsviz.net/)

DNSSEC validation status

- **Bogus** – broken chain

dnssec-failed.org/SOA



(Image from http://dnsviz.net/)

Outline

- DNSSEC protocol review
- DNSSEC maintenance and misconfiguration
- DNSSEC survey and results
- Conclusions and solutions

DNSSEC Maintenance

- RRSIG refresh
- DNSKEY rollovers
  - ZSK rollovers – non-SEP (secure entry point), self-contained
  - KSK rollovers – SEP requires interaction with parent or trust anchor
- Algorithm changes

Sandia National Laboratories

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

DNSSEC is hard.

Sandia National Laboratories

Jan 10, 2012 – Comcast turned on DNSSEC validation for all its residential customers.

http://blog.comcast.com/2012/01/comcast-completes-dnssec-deployment.html

Sandia National Laboratories

Jan 18, 2012 – Comcast customers could not access nasa.gov.

NASA.gov blocked
01-18-2012 04:01 PM

Comcast has blocked access to NASA.gov. I am outraged! Is this China or something worse?

Comcast Blocks Customer Access to NASA.gov

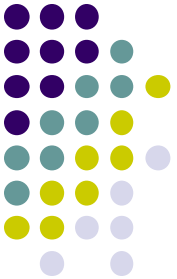
By Keith Cowing on January 18, 2012 1:17 PM 16 Comments

Keith's note: Comcast has decided to block customer access to *.NASA.gov due, I am told, to an issue involving how NASA maintains its DNS records. Why these geniuses at Comcast chose the SOPA/PIPA protest day to do this is curious to say the least. Right now, if you are a Comcast customer, you are being purposefully denied access to one part of your government's services.

http://forums.comcast.com/t5/Connectivity-and-Modem-Help/NASA-gov-blocked/td-p/1169657
http://nasawatch.com/archives/2012/01/comcast-blocks.html

Jan 22, 2012 – Comcast customers could not access bitcoinica.com.

http://www.reddit.com/r/Bitcoin/comments/orzpq/attention_comcast_users_we_have_been_censored/



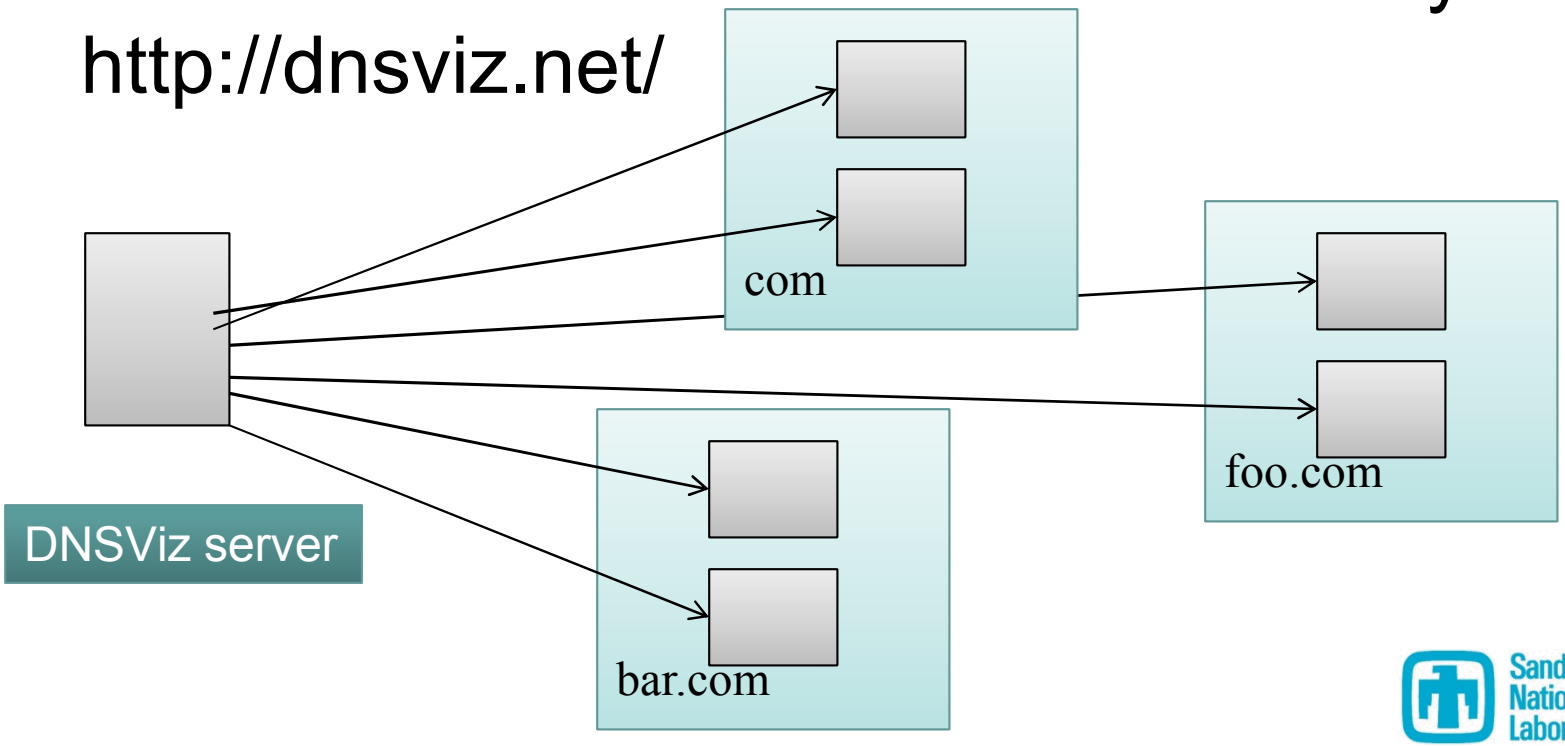
Comcast is *clearly* "censoring" these sites. But why?

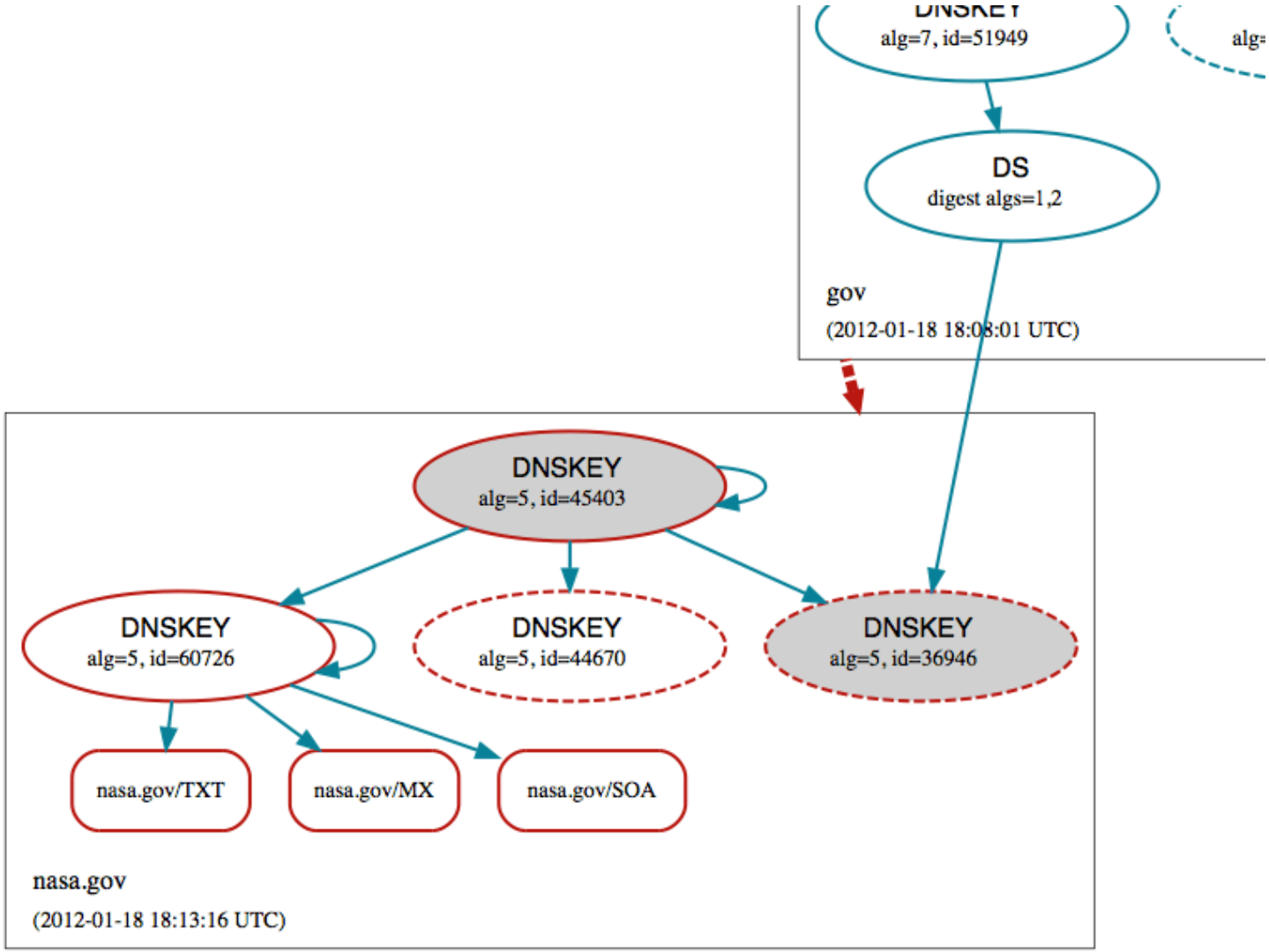
Enter DNSViz…

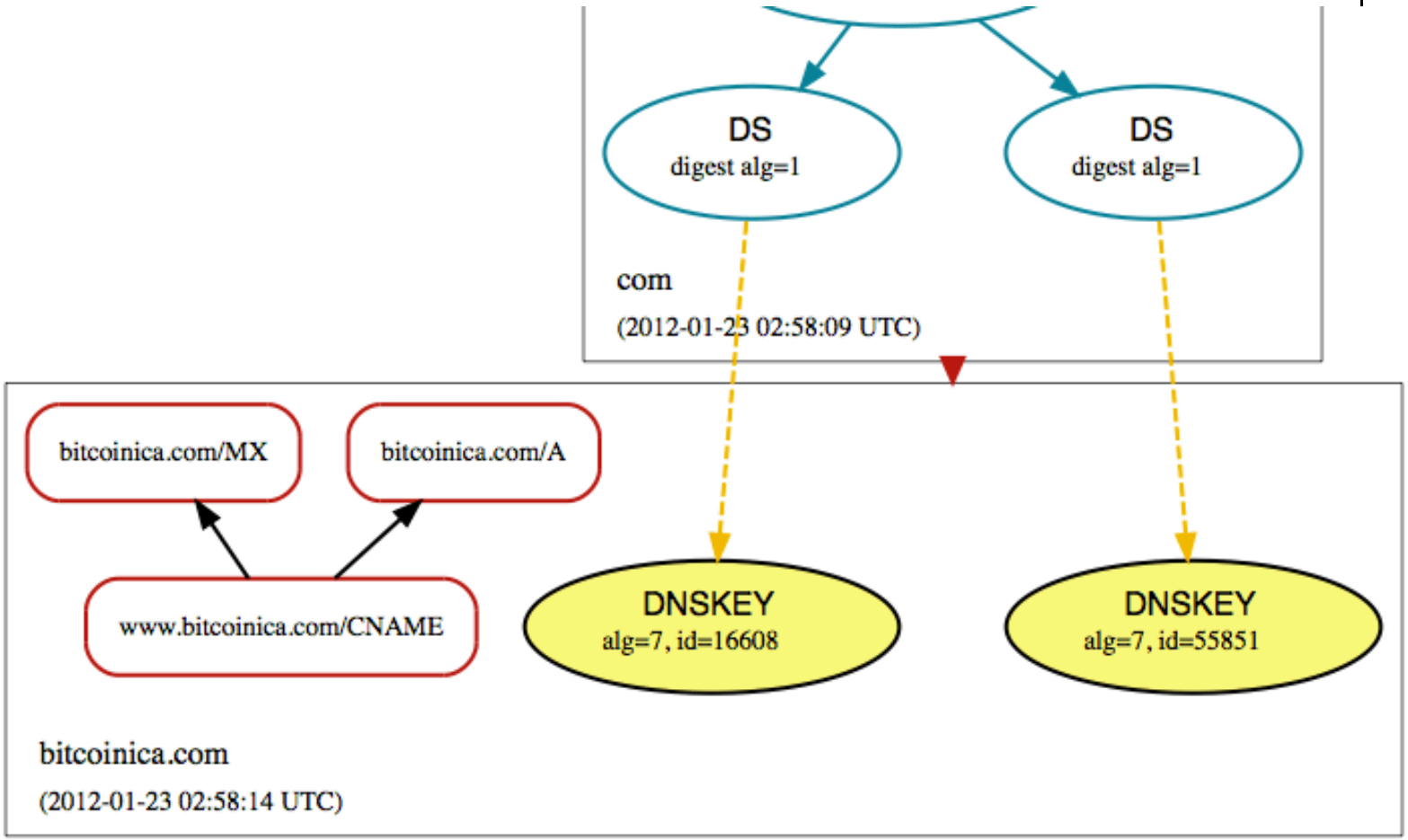
Sandia National Laboratories

DNSViz

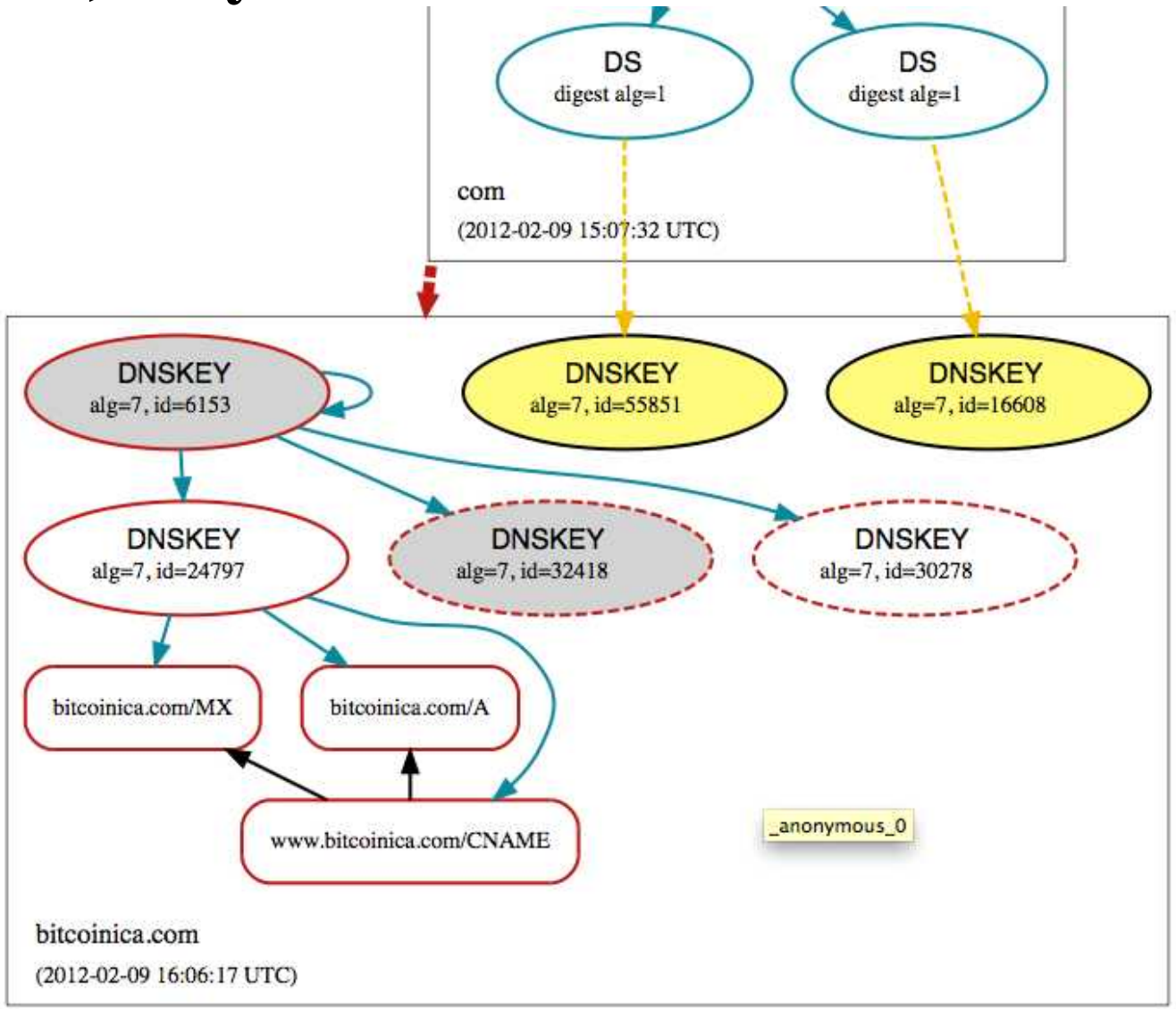
- Actively monitors domains from single vantage point
- Makes results available for visual analysis at http://dnsviz.net/




DNSKEY
alg=7, id=51949
DS
digest algs=1,2
gov
(2012-01-18 18:08:01 UTC)
DNSKEY
alg=5, id=45403
DNSKEY
alg=5, id=60726
DNSKEY
alg=5, id=44670
DNSKEY
alg=5, id=36946
nasa.gov/TXT
nasa.gov/MX
nasa.gov/SOA
nasa.gov
(2012-01-18 18:13:16 UTC)


DS
digest alg=1
DS
digest alg=1
com
(2012-01-23 02:58:09 UTC)
bitcoinica.com/MX
bitcoinica.com/A
www.bitcoinica.com/CNAME
DNSKEY
alg=7, id=16608
DNSKEY
alg=7, id=55851
bitcoinica.com
(2012-01-23 02:58:14 UTC)

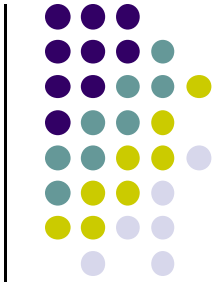
But, they “fixed” it…



Outline

- DNSSEC protocol review
- DNSSEC maintenance and misconfiguration
- DNSSEC survey and results
- Conclusions and solutions

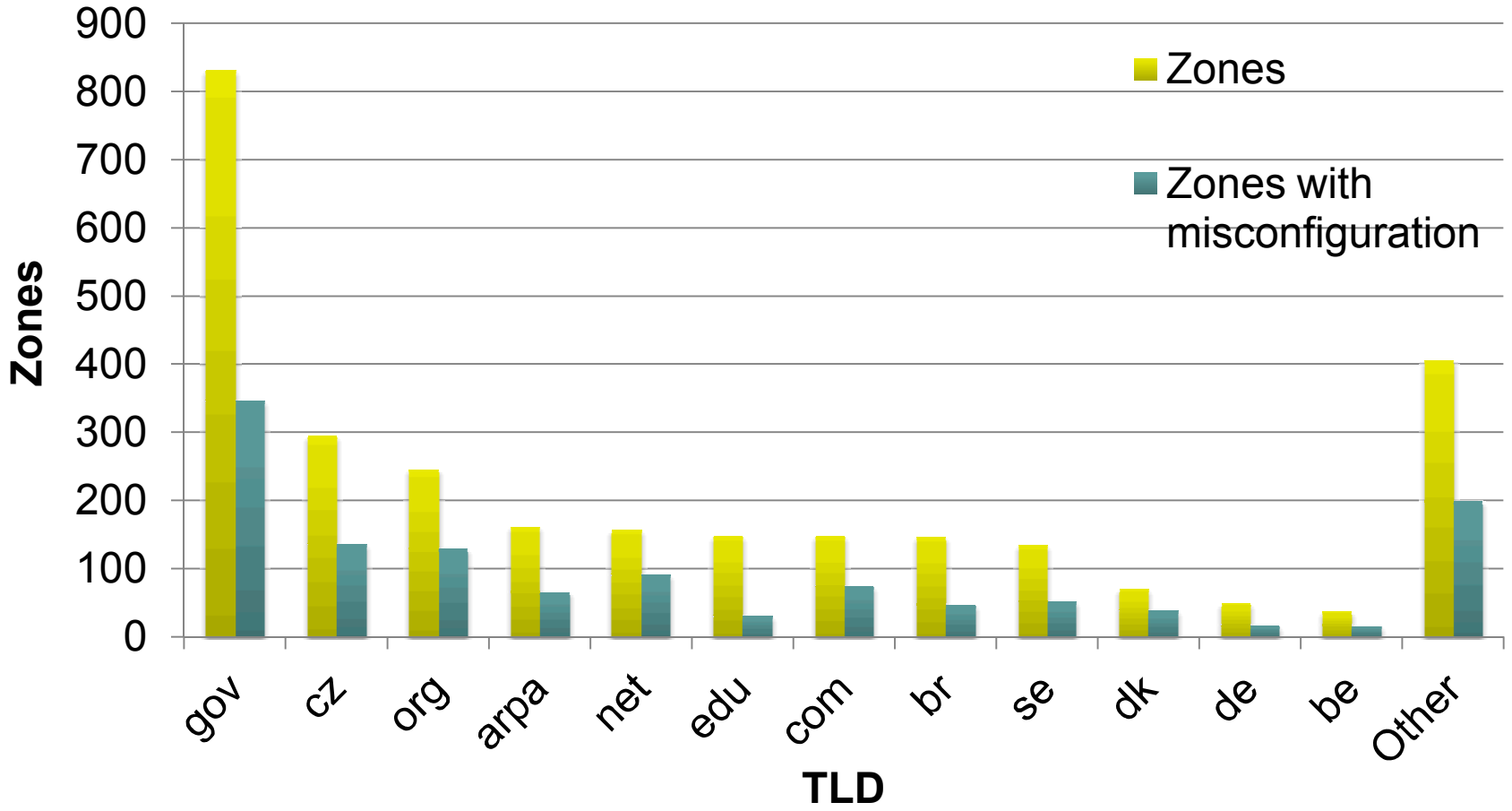
DNSSEC deployment survey



- 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

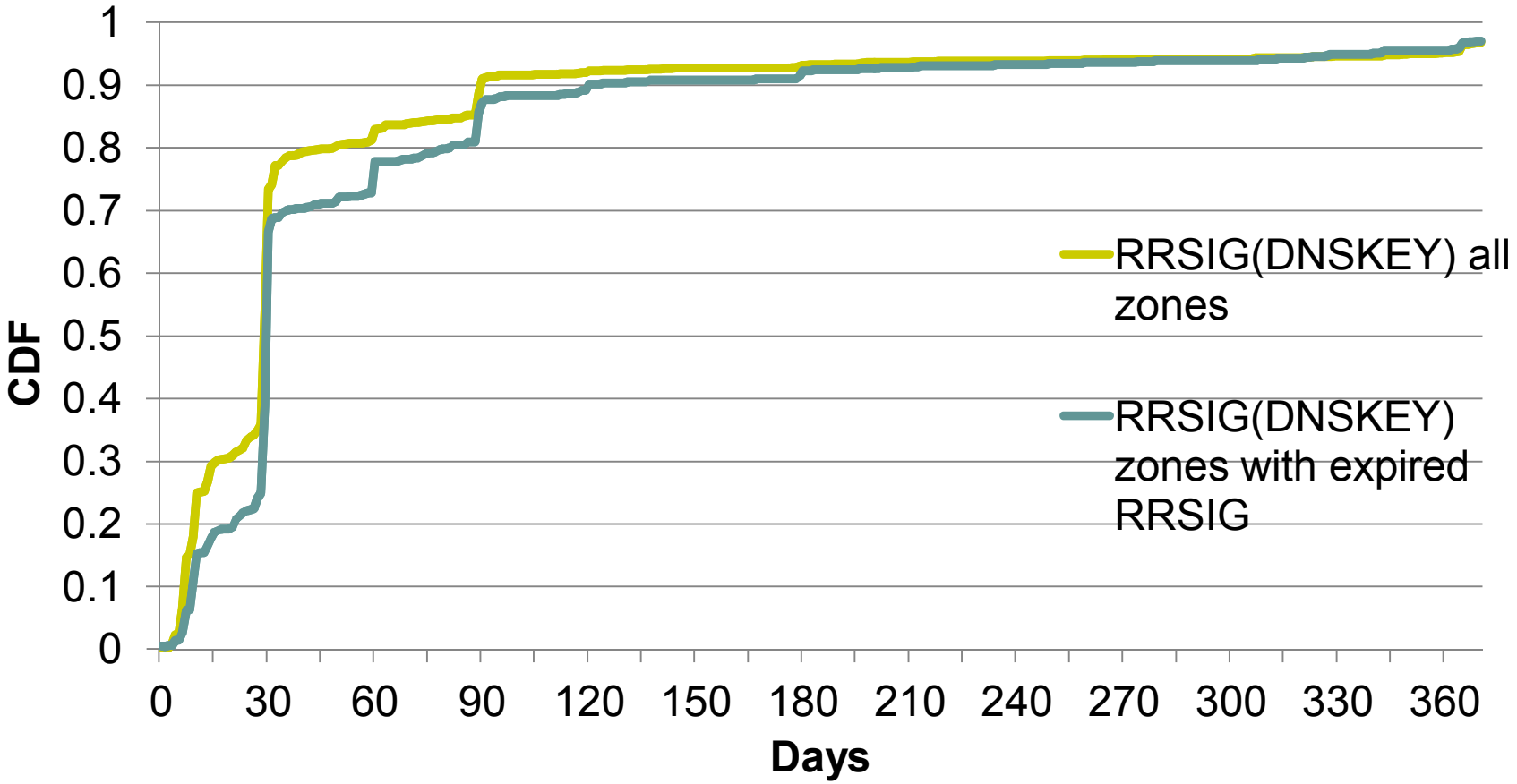
Sandia National Laboratories

Survey breakdown by TLD



Sandia National Laboratories

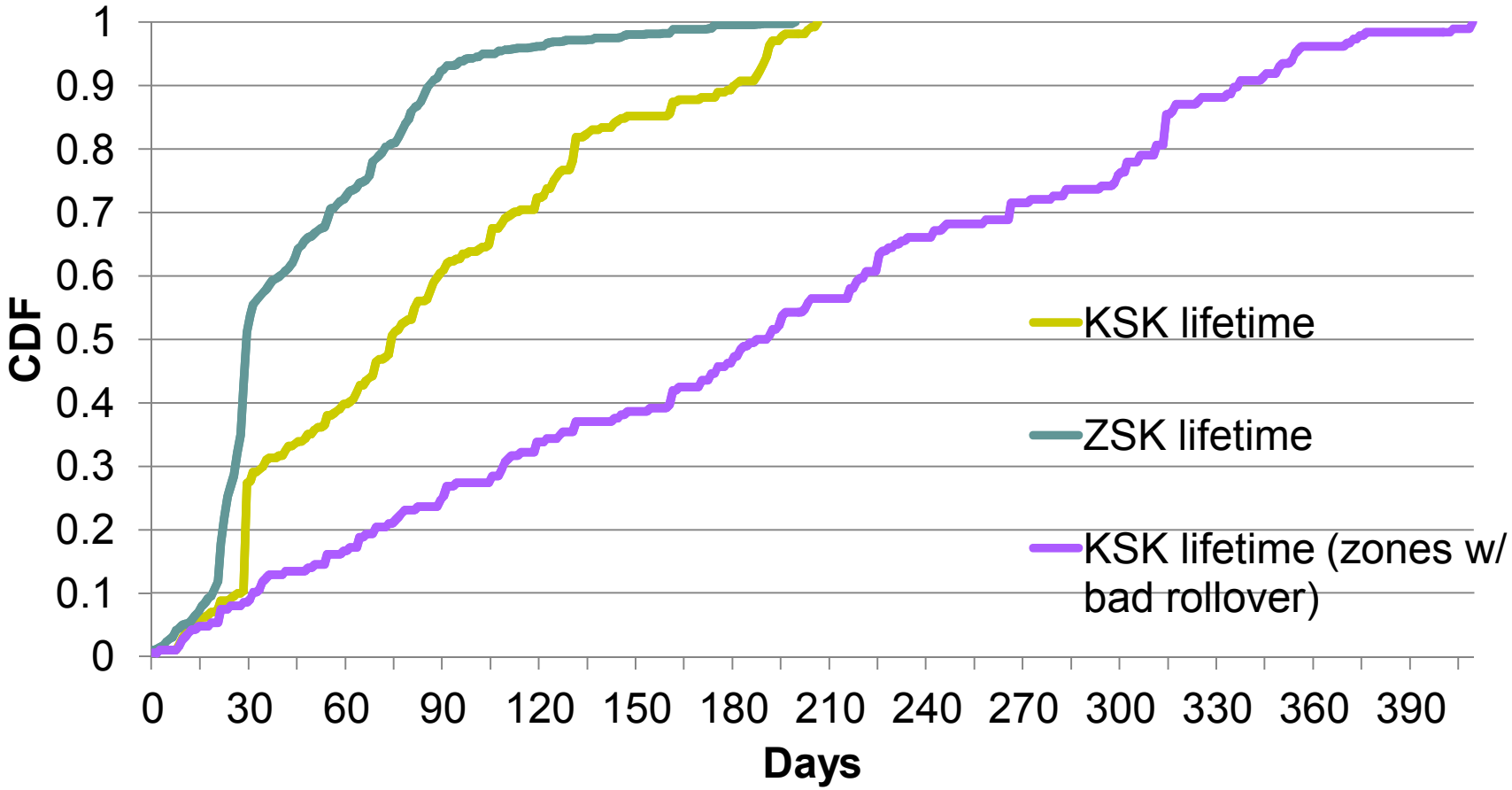
RRSIG lifetimes



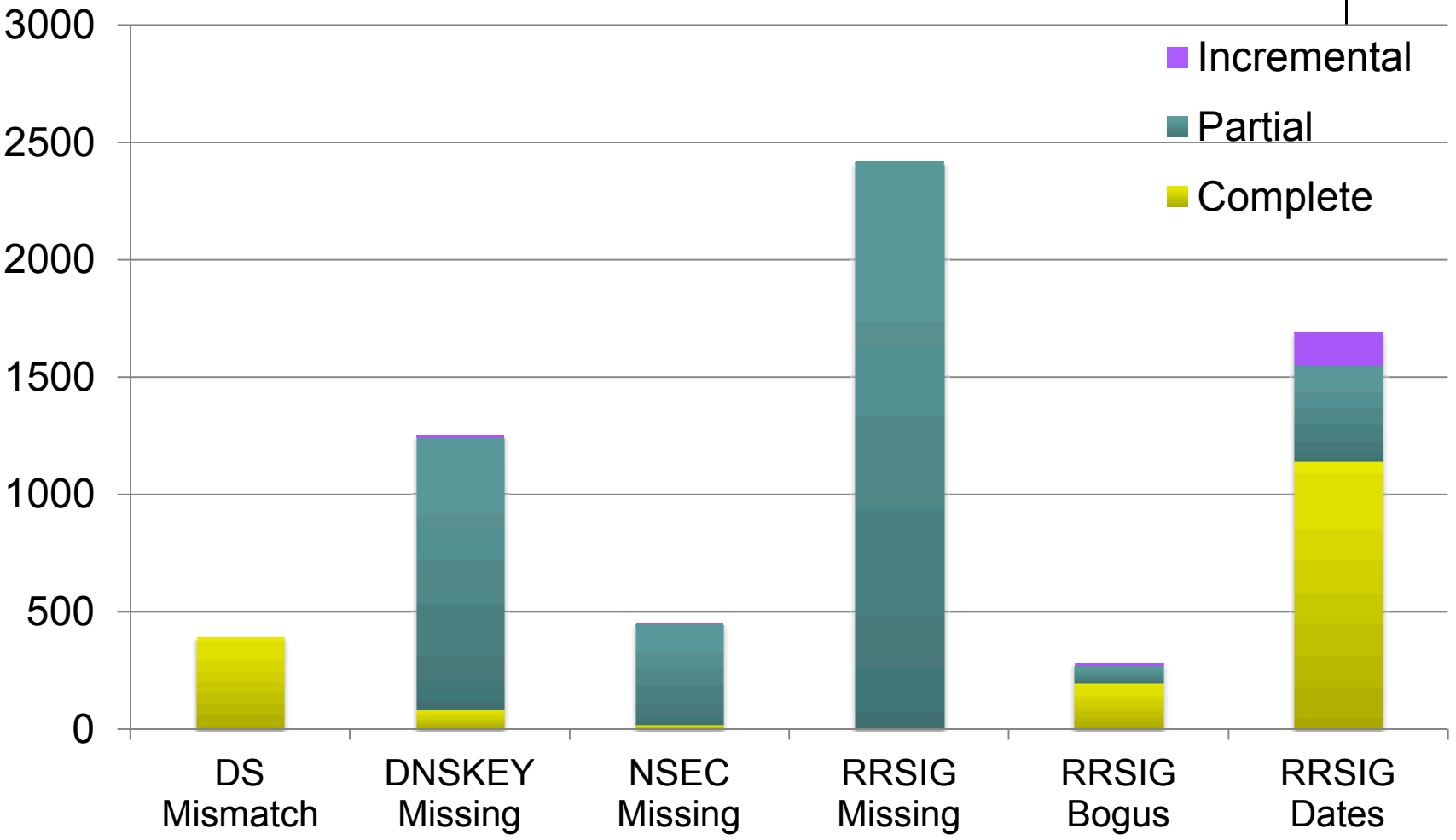
DNSKEY rollovers

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%

DNSKEY lifetime

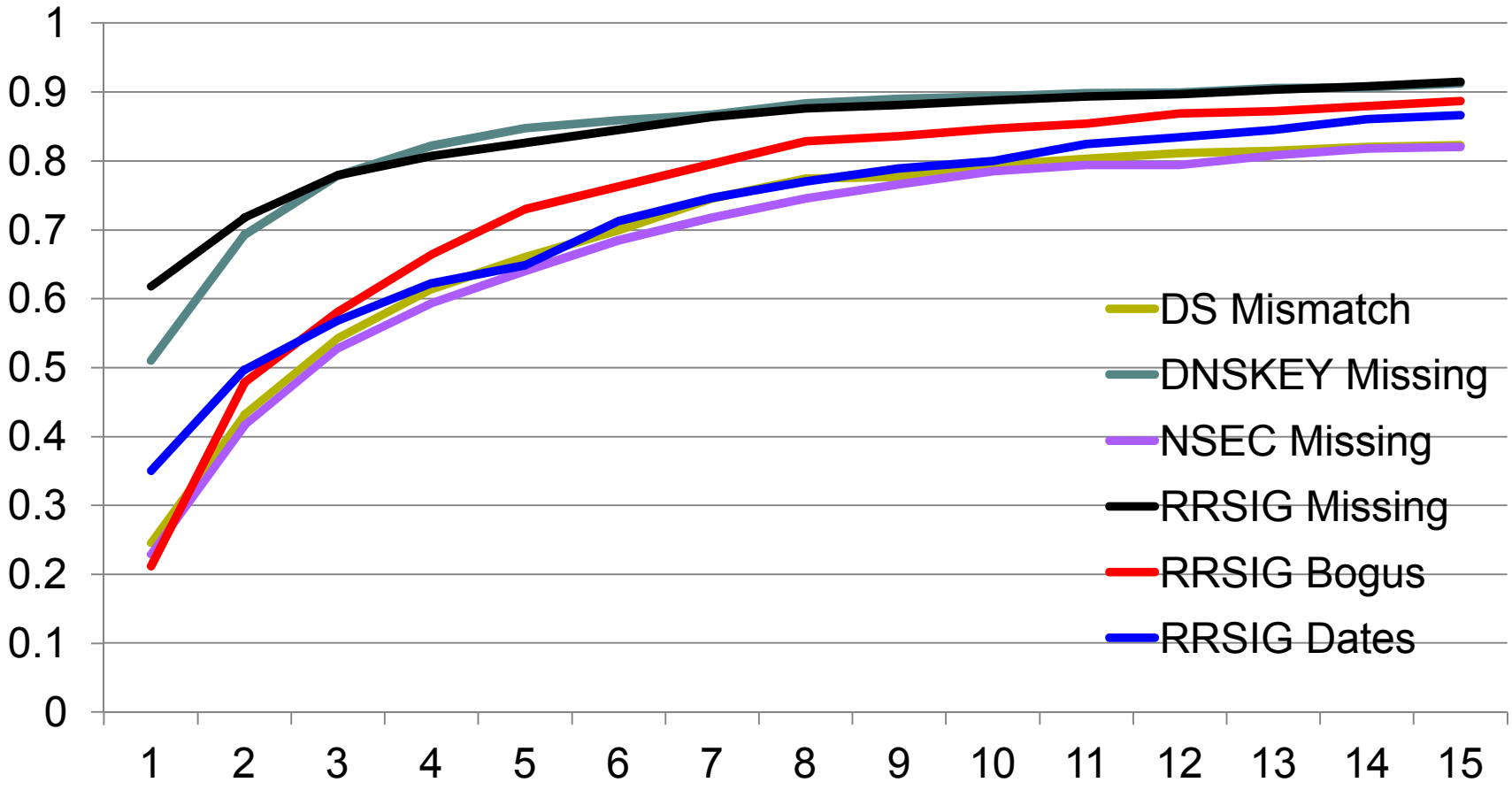


Misconfigurations by type

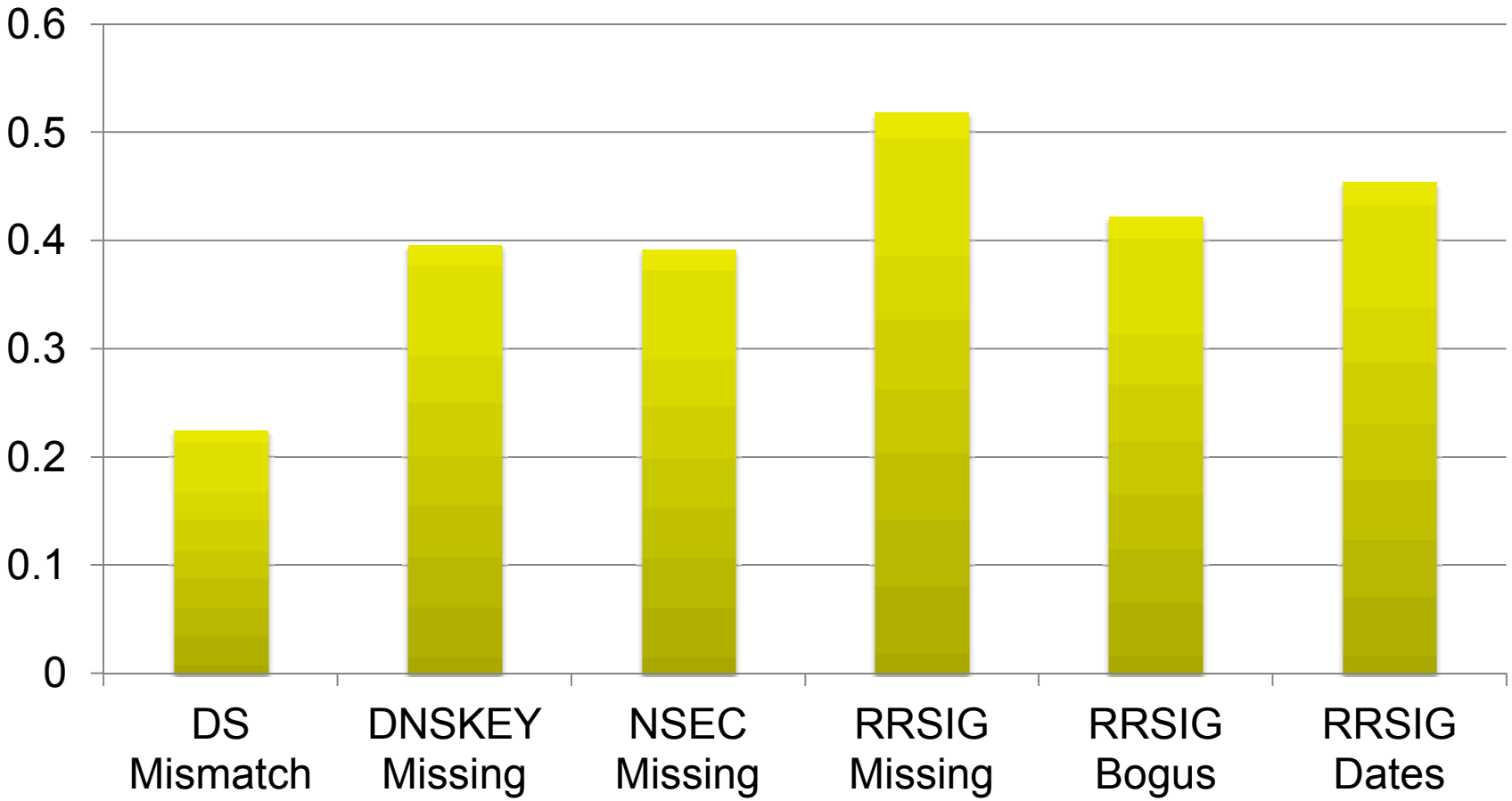


Sandia National Laboratories

Event duration

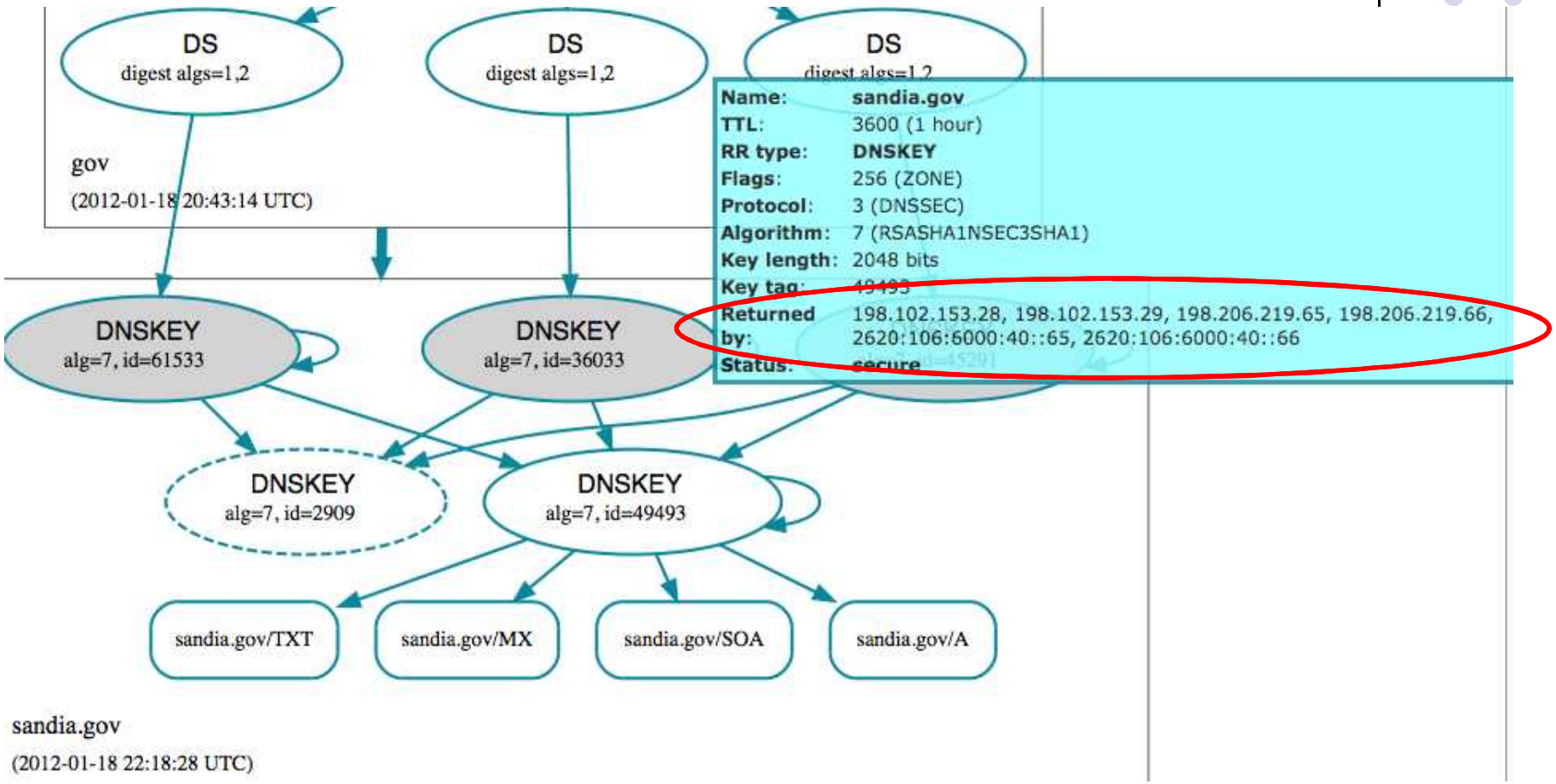


Repeat offense rate

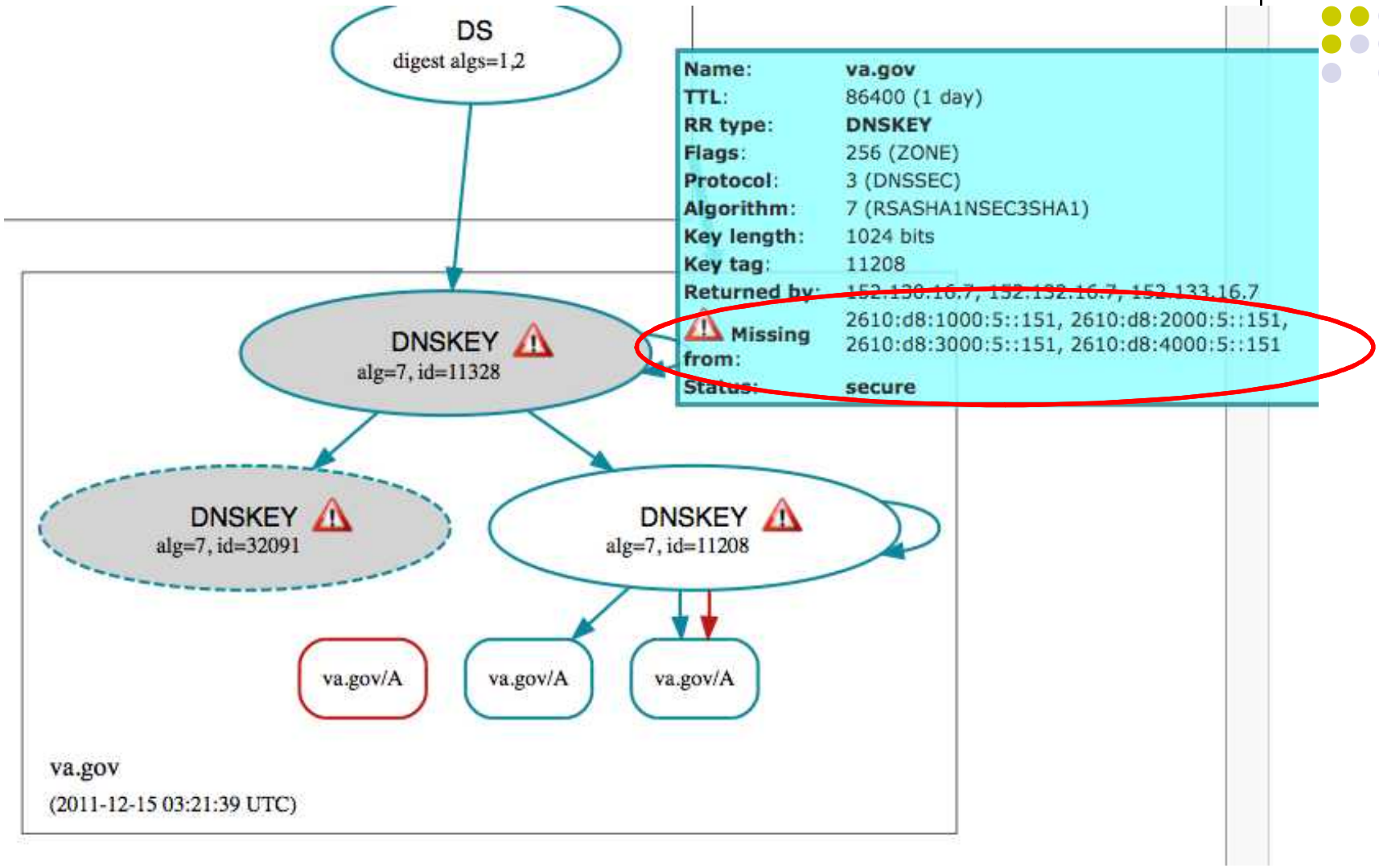


Sandia National Laboratories

IPv6 analysis



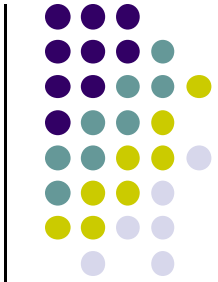
IPv6 inconsistencies



Outline

- DNSSEC protocol review
- DNSSEC maintenance and misconfiguration
- DNSSEC survey and results
- Conclusions and solutions

Summary of Observations



- Resolver operators are learning about third-party DNSSEC misconfigurations from their customers.
- Administrators aren't detecting and correcting their DNSSEC problems in a timely fashion.
- Administrators aren't learning from past mistakes.

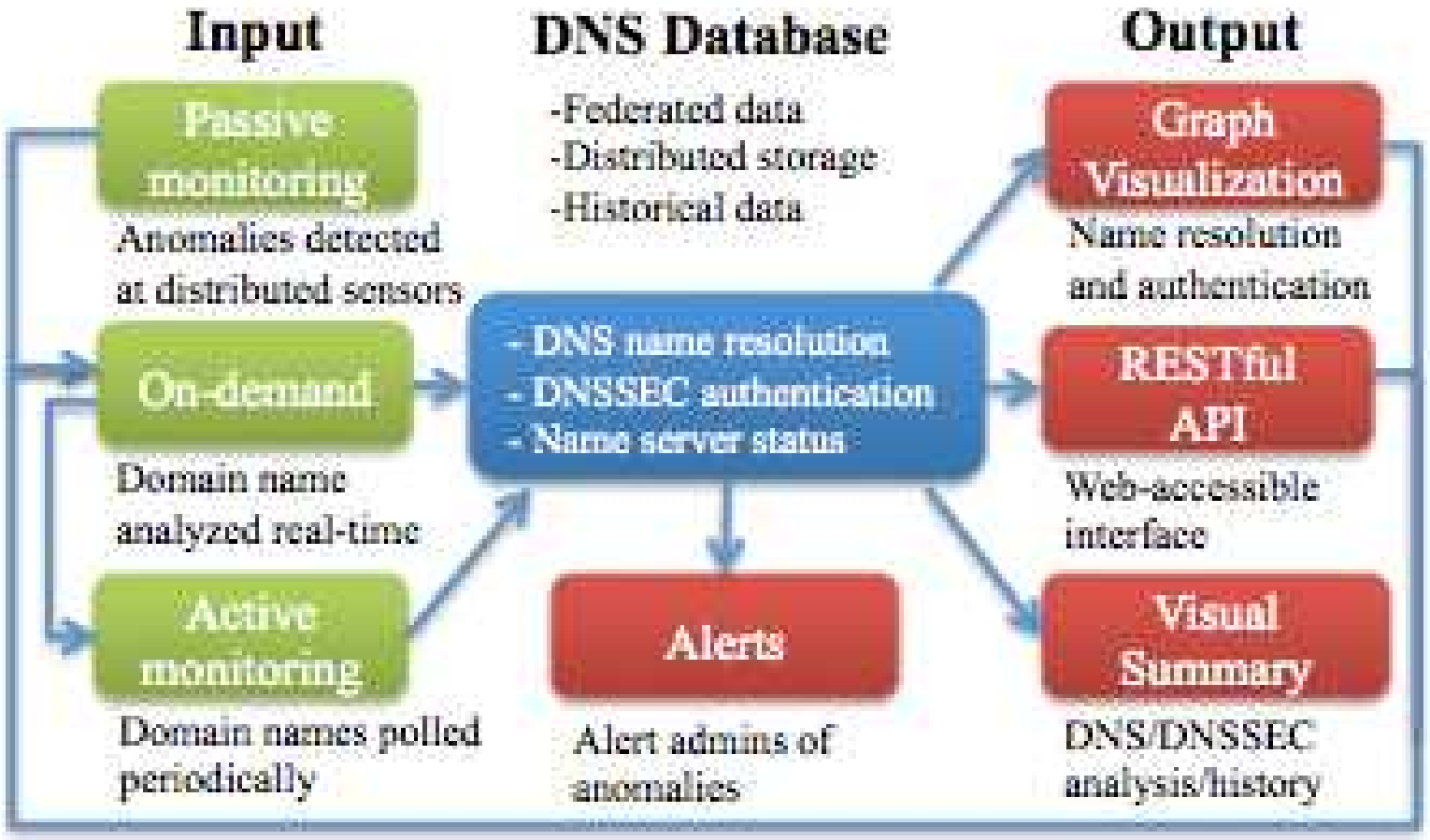
Solutions

- Tools for DNSSEC comprehensive analysis
  - Hierarchical analysis (chain of trust)
  - Dependency analysis (CNAME, MX, NS, etc)
  - Server consistency analysis
  - Pointers to specification
  - Resources for corrective action
- Tools/resources for detection/notification of misconfiguration
  - Individual monitoring and alerts
  - Global monitoring and alerts

DNSViz – future plans

- Expansion of detailed analysis
- Passive monitoring, in addition to active monitoring
  - Diverse backend support
    - e.g., ISC Security Information Exchange (SIE)
  - Prioritized active probing
  - Alerts of misconfiguration
- RESTful API for programmatic third-party monitoring
- Cache analysis/local perspective
- Availability of software for diverse uses

Sandia National Laboratories


Input
DNS Database
Output
Passive monitoring
Anomalies detected at distributed sensors
On-demand
Domain name analyzed real-time
Active monitoring
Domain names polled periodically
-Federated data
-Distributed storage
-Historical data
- DNS name resolution
- DNSSEC authentication
- Name server status
Alerts
Alert admins of anomalies
Graph Visualization
Name resolution and authentication
RESTful API
Web-accessible interface
Visual Summary
DNS/DNSSEC analysis/history

Questions?

- ctdecci@sandia.gov