Assessing and Improving the Quality of DNSSEC Deployment

Casey Deccio, Ph.D.

Sandia National Laboratories

AIMS-4

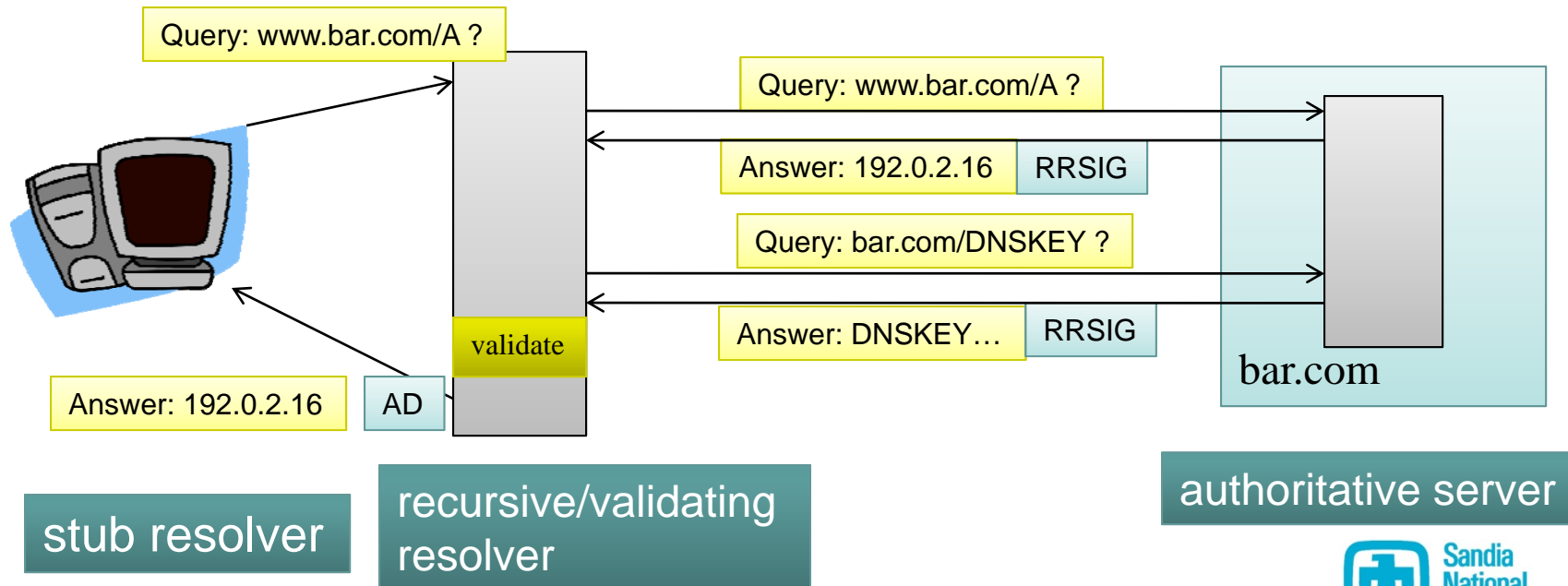CAIDA, SDSC, San Diego, CA

Feb 9, 2012

Outline

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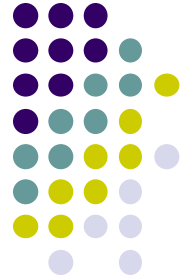- DNSSEC survey and results
- Conclusions and solutions

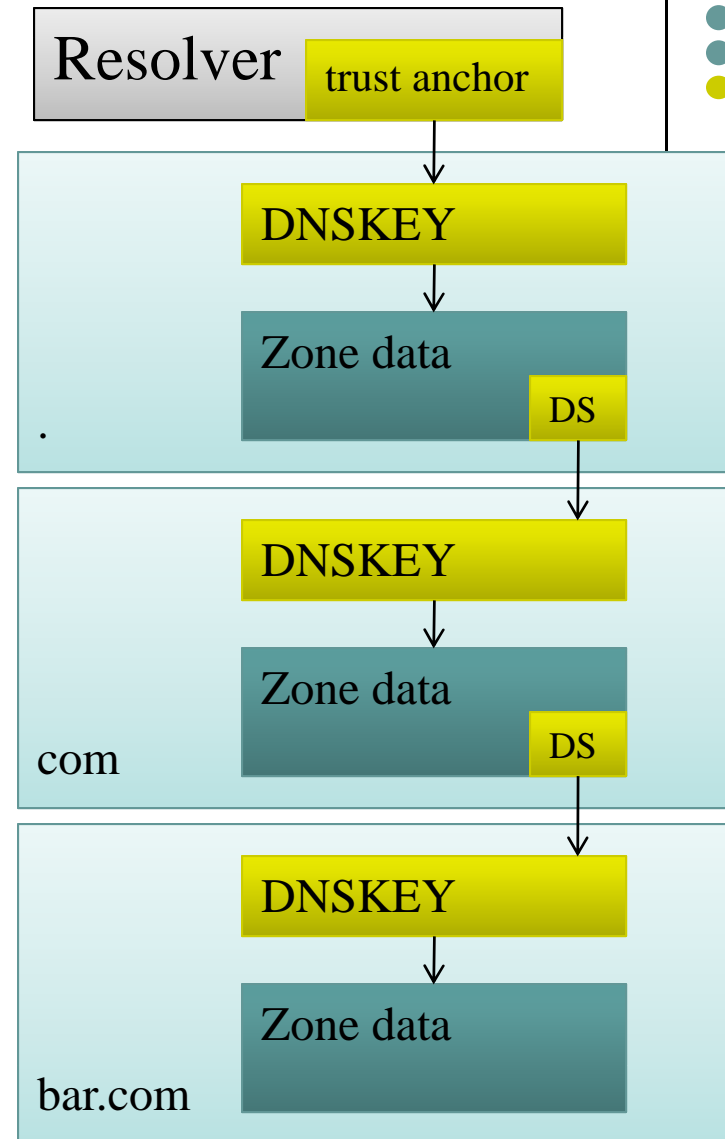# DNS Security Extensions (DNSSEC)

- 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

Query: www.bar.com/A ?

Query: www.bar.com/A ?

Answer: 192.0.2.16 | RRSIG

Query: bar.com/DNSKEY ?

Answer: DNSKEY… | RRSIG

bar.com

validate

Answer: 192.0.2.16

AD

stub resolver

recursive/validating resolver
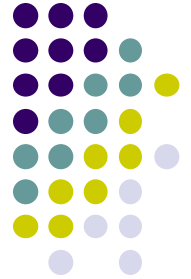
authoritative server
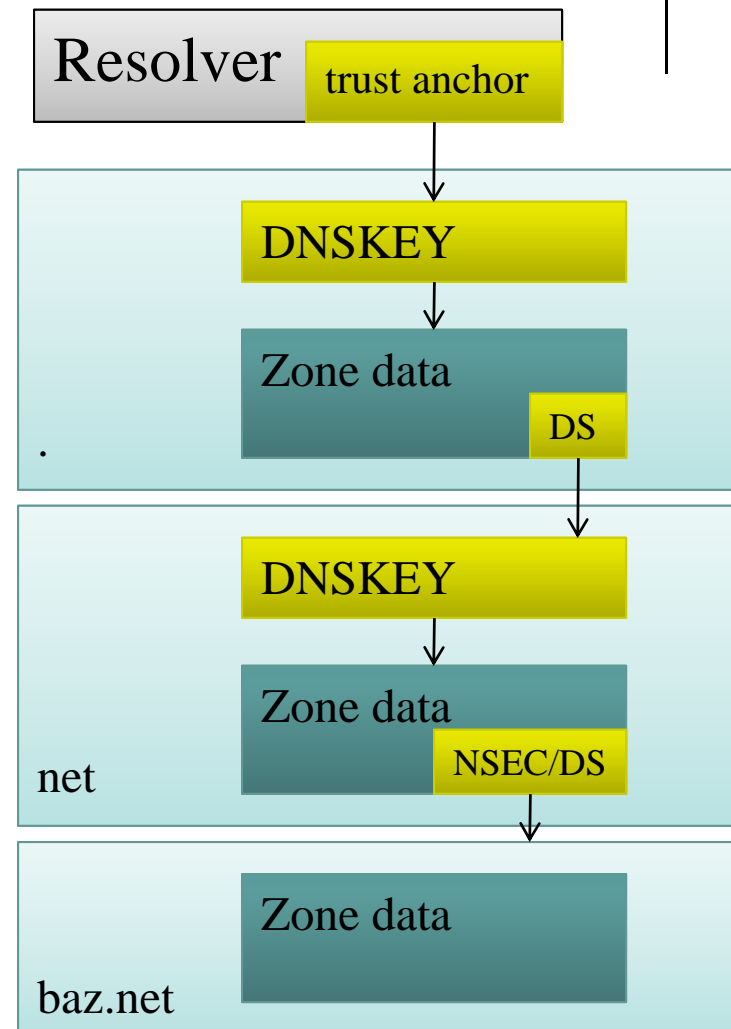
3

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

Resolver | trust anchor

DNSKEY

Zone data

DS

.

DNSKEY

Zone data

DS

com

DNSKEY

Zone data

bar.com

Sandia National Laboratories

4

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

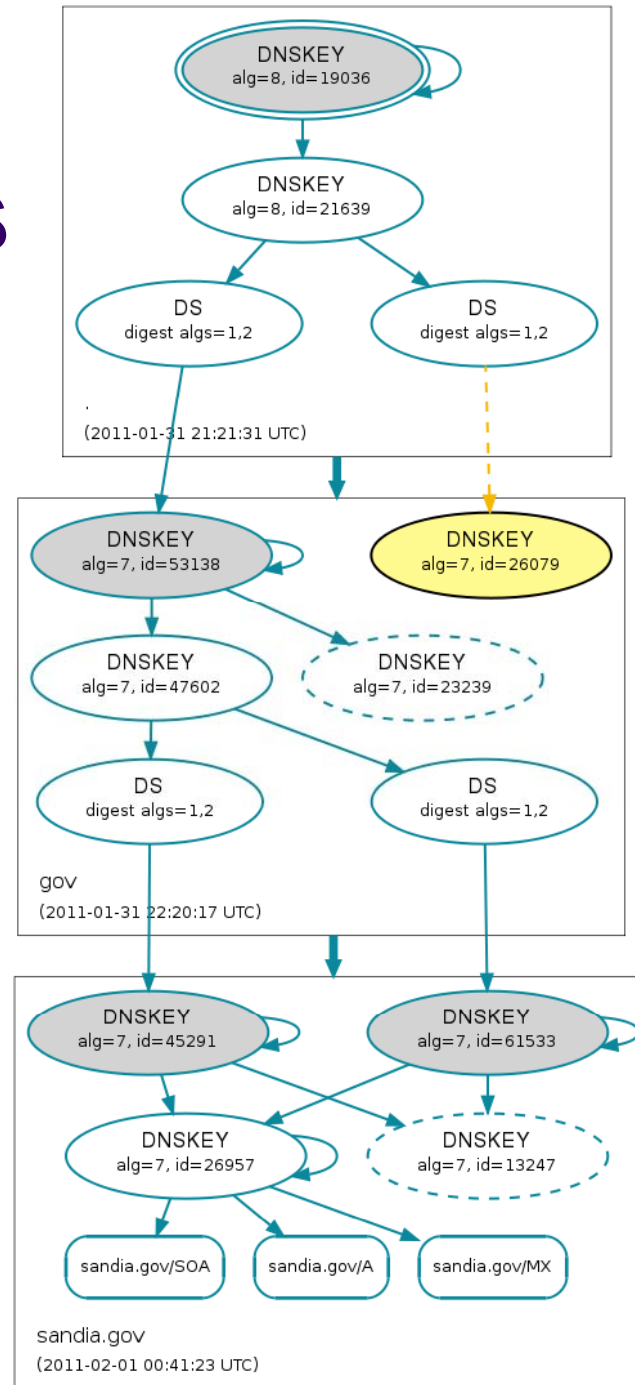- Child zones of insecure delegations may be unsigned or signed ("islands of security")

Resolver | trust anchor

.
DNSKEY → Zone data | DS

net
DNSKEY → Zone data | NSEC/DS

baz.net
Zone data

Sandia National Laboratories

5

DNSSEC validation status

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

(Image from http://dnsviz.net/)
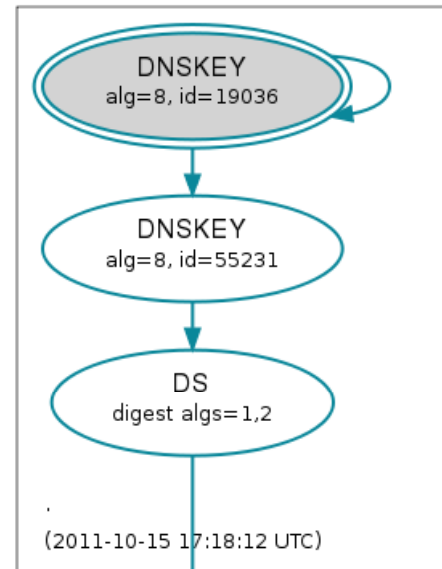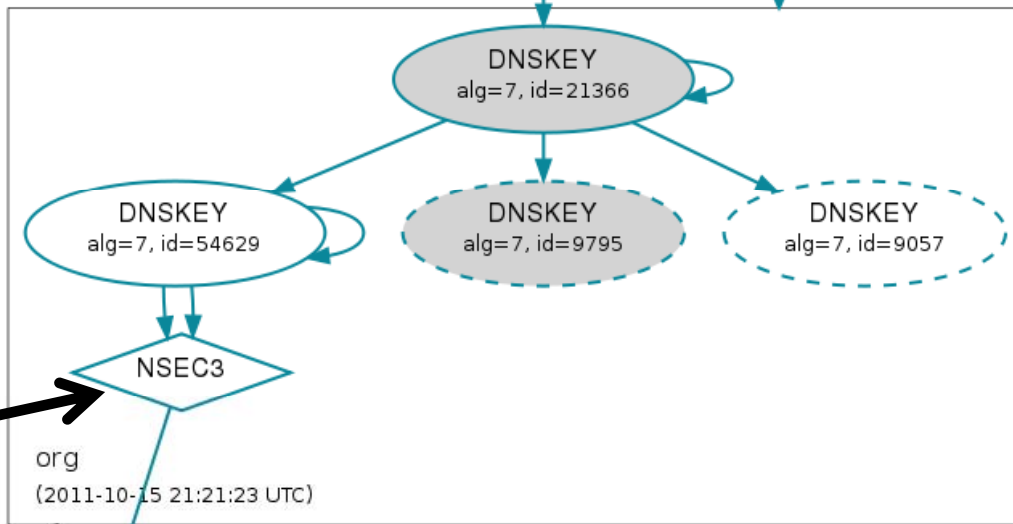
DNSSEC validation status

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

Secure chain termination

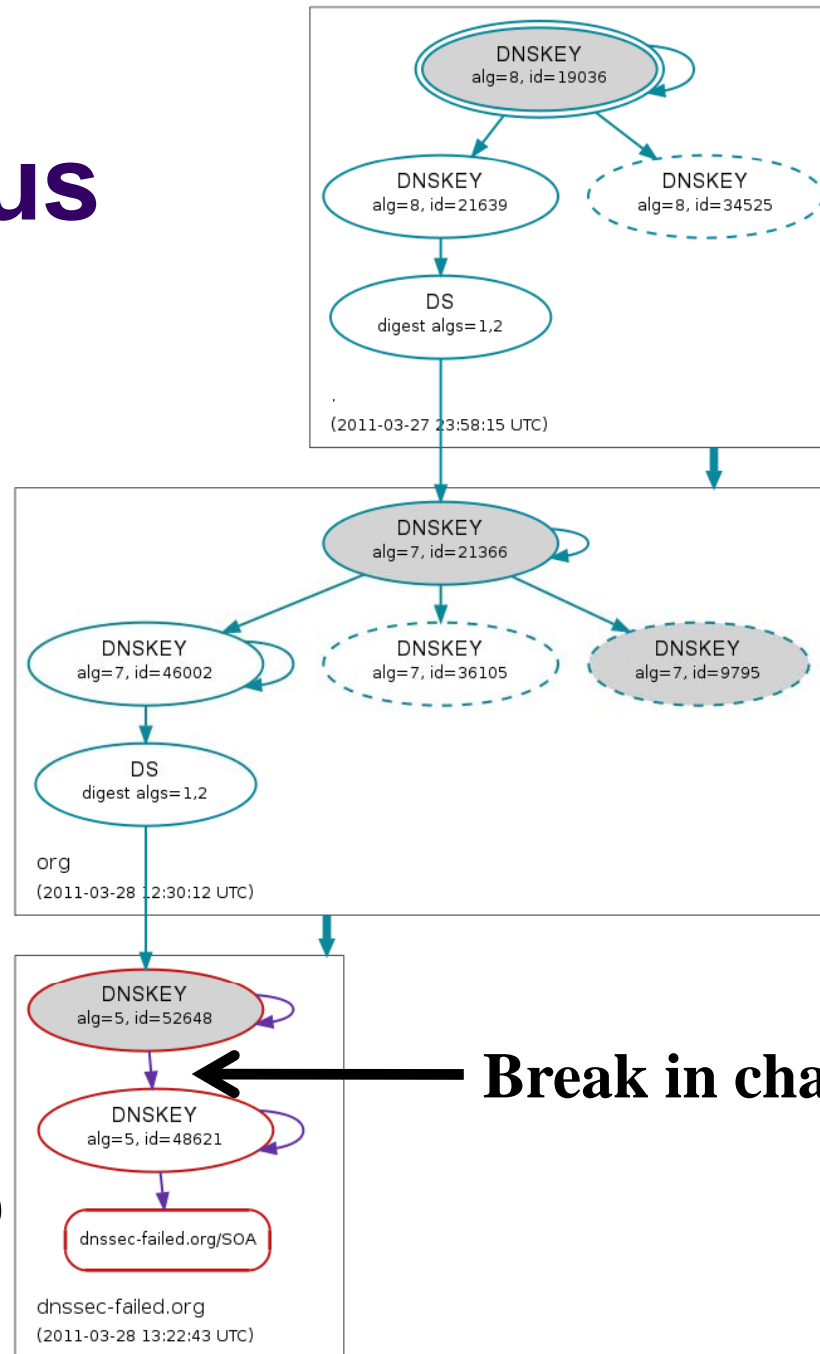(Image from http://dnsviz.net/)

DNSSEC validation status

- **Bogus** – broken chain

dnssec-failed.org/SOA

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

Break in chain

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

Sandia National Laboratories

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

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

Sandia National Laboratories

14

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

BITCOIN comments related

Attention Comcast Users - We have been Censored! (self.Bitcoin)
submitted 17 days ago by LsDmT

Hello all I just recently found something that has really made things dawn on me. It seems like Comcast has gone ahead with their own version of the oppressive behavior SOPA looked to implement. Comcast has recently made some changes and has introduced "DNSSEC-validating resolvers" and has deemed bitconica as a risk.

THREAD: https://bitcointalk.org/index.php?topic=60741.0

10 comments   share

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

Sandia National Laboratories

15

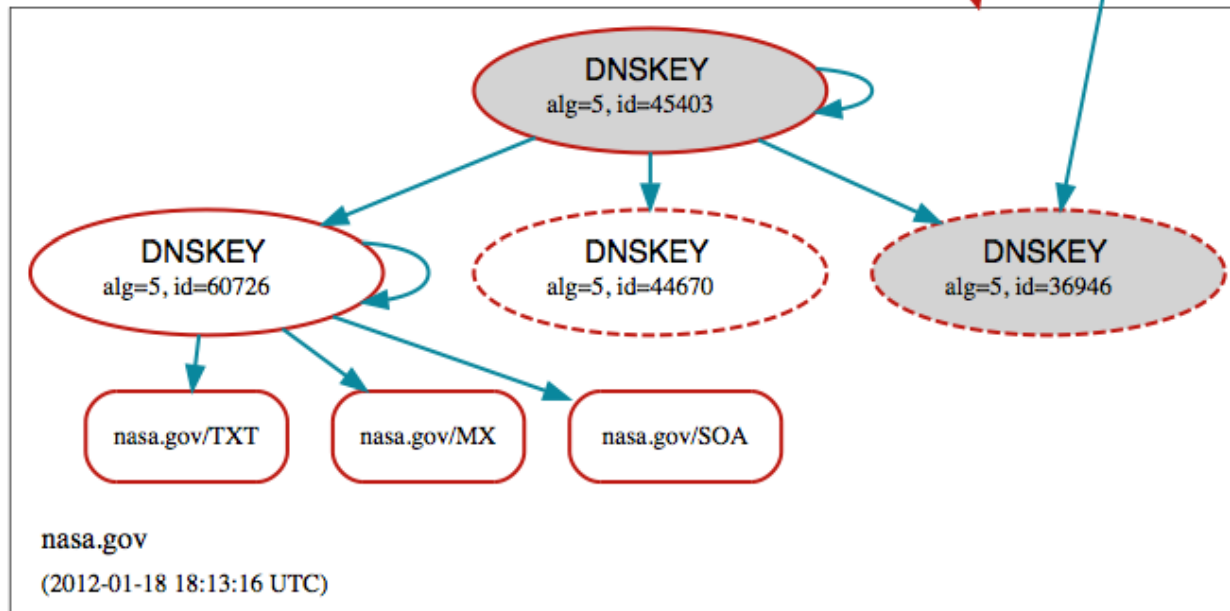# Comcast is *clearly* "censoring" these sites. But why?
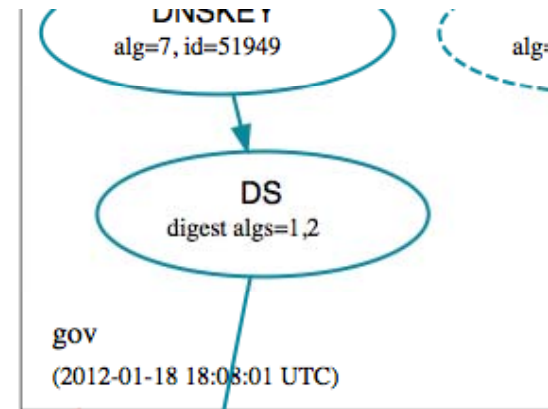
Enter DNSViz…

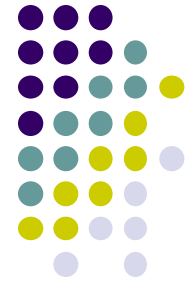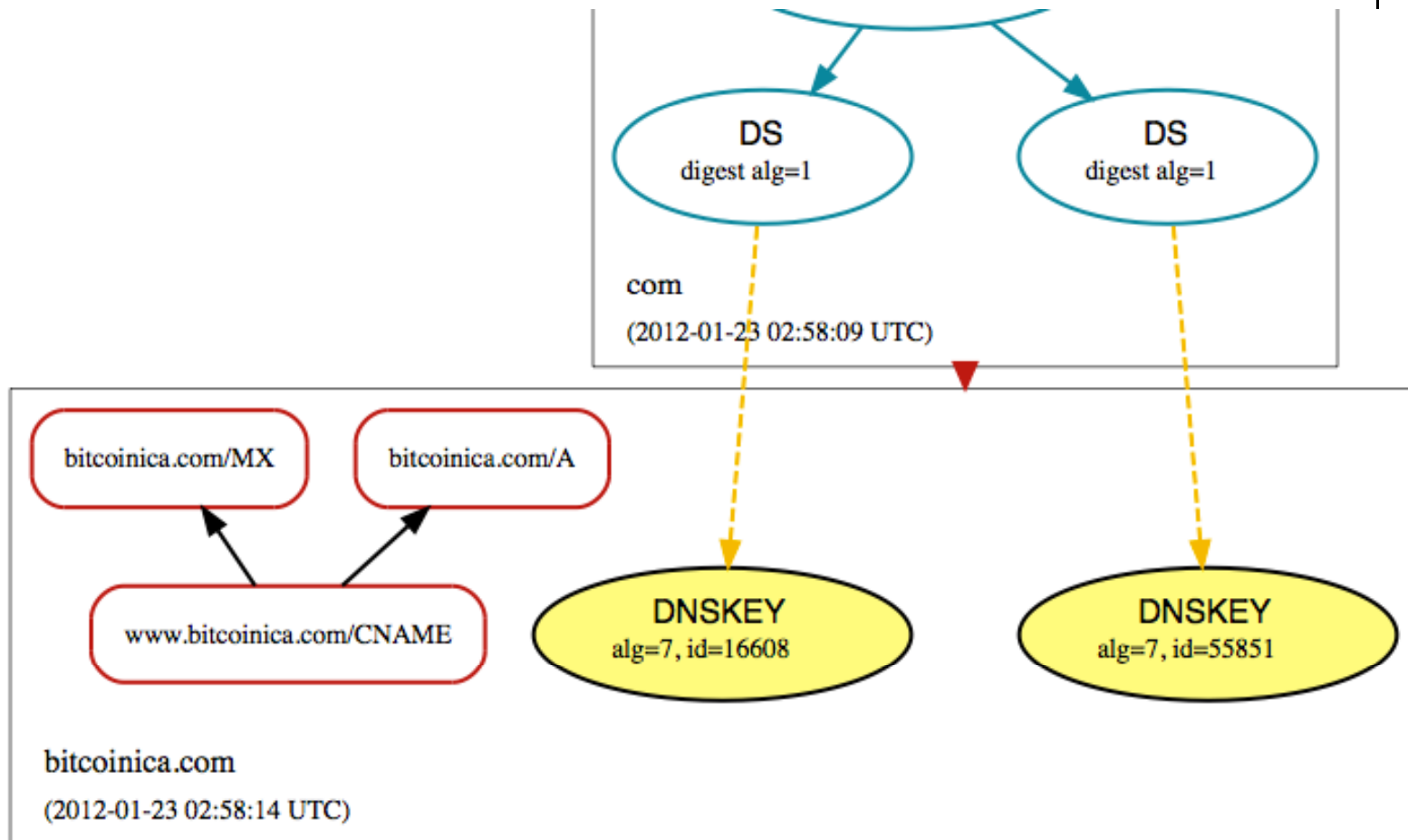# DNSViz

- Actively monitors domains from single vantage point

- Makes results available for visual analysis at http://dnsviz.net/

DNSViz server

com

bar.com

foo.com

DNSKEY
alg=7, id=51949

alg=

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

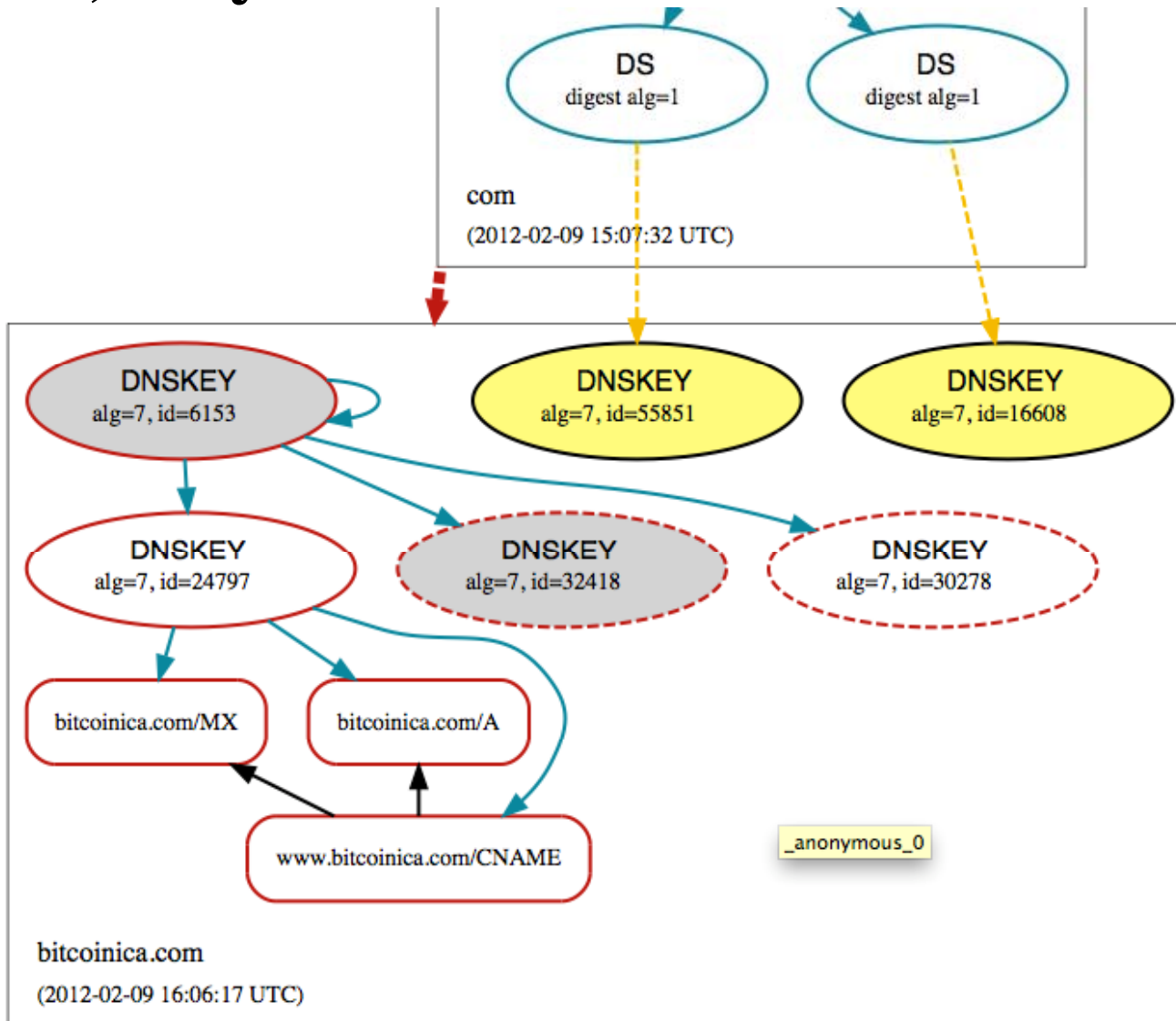nasa.gov/MX

nasa.gov/SOA

nasa.gov
(2012-01-18 18:13:16 UTC)
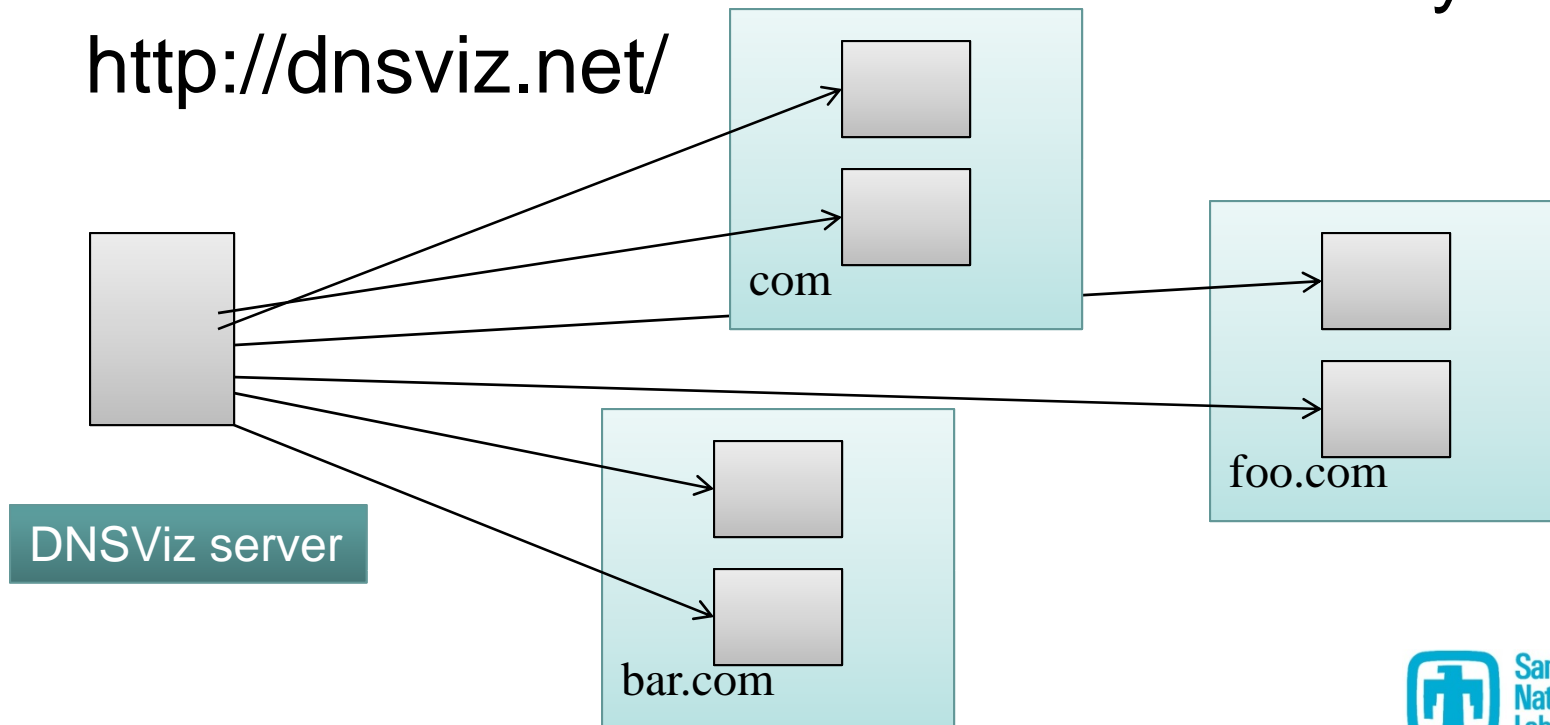
But, they "fixed" it…

Outline

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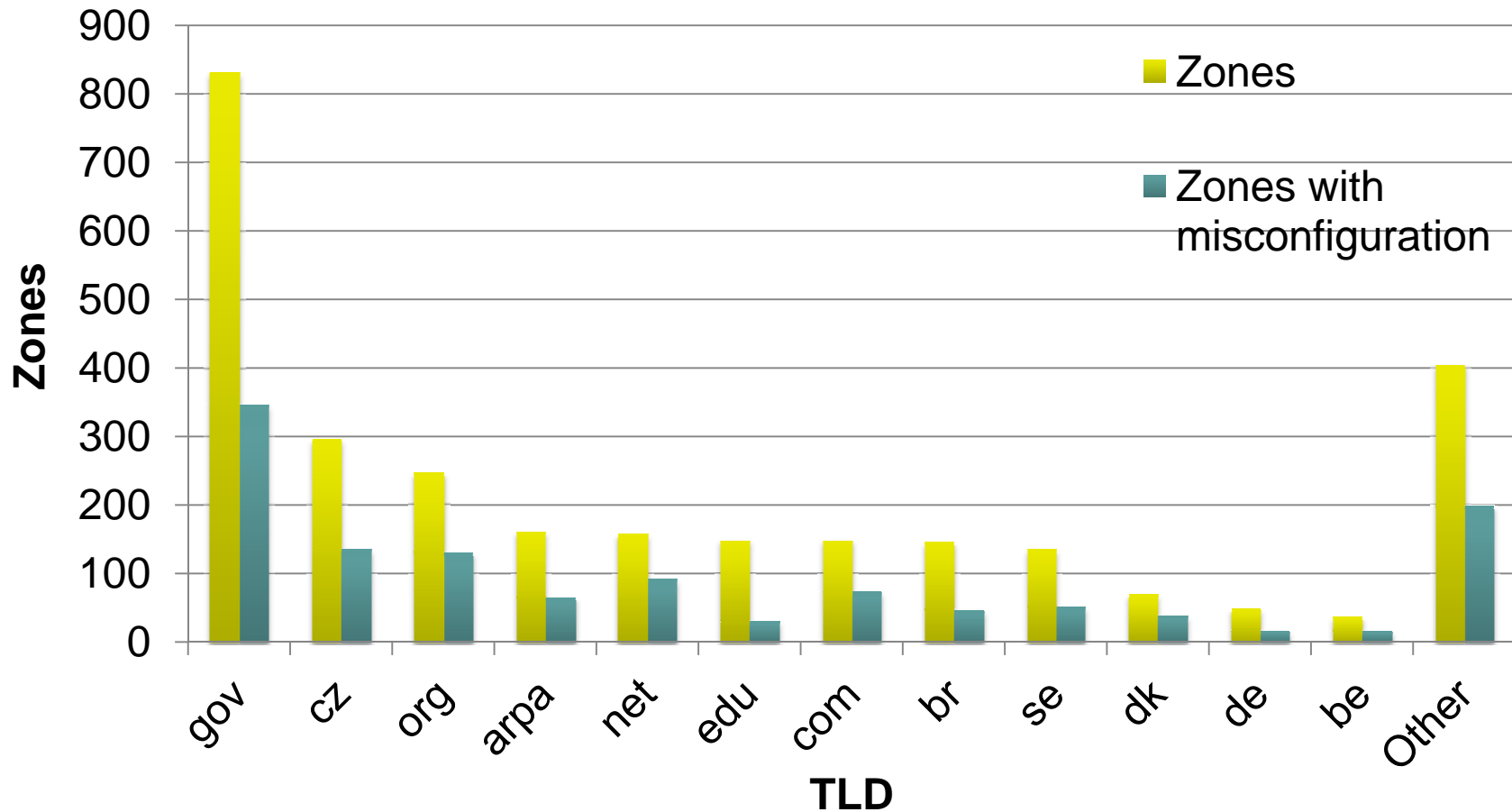- **DNSSEC survey and results**
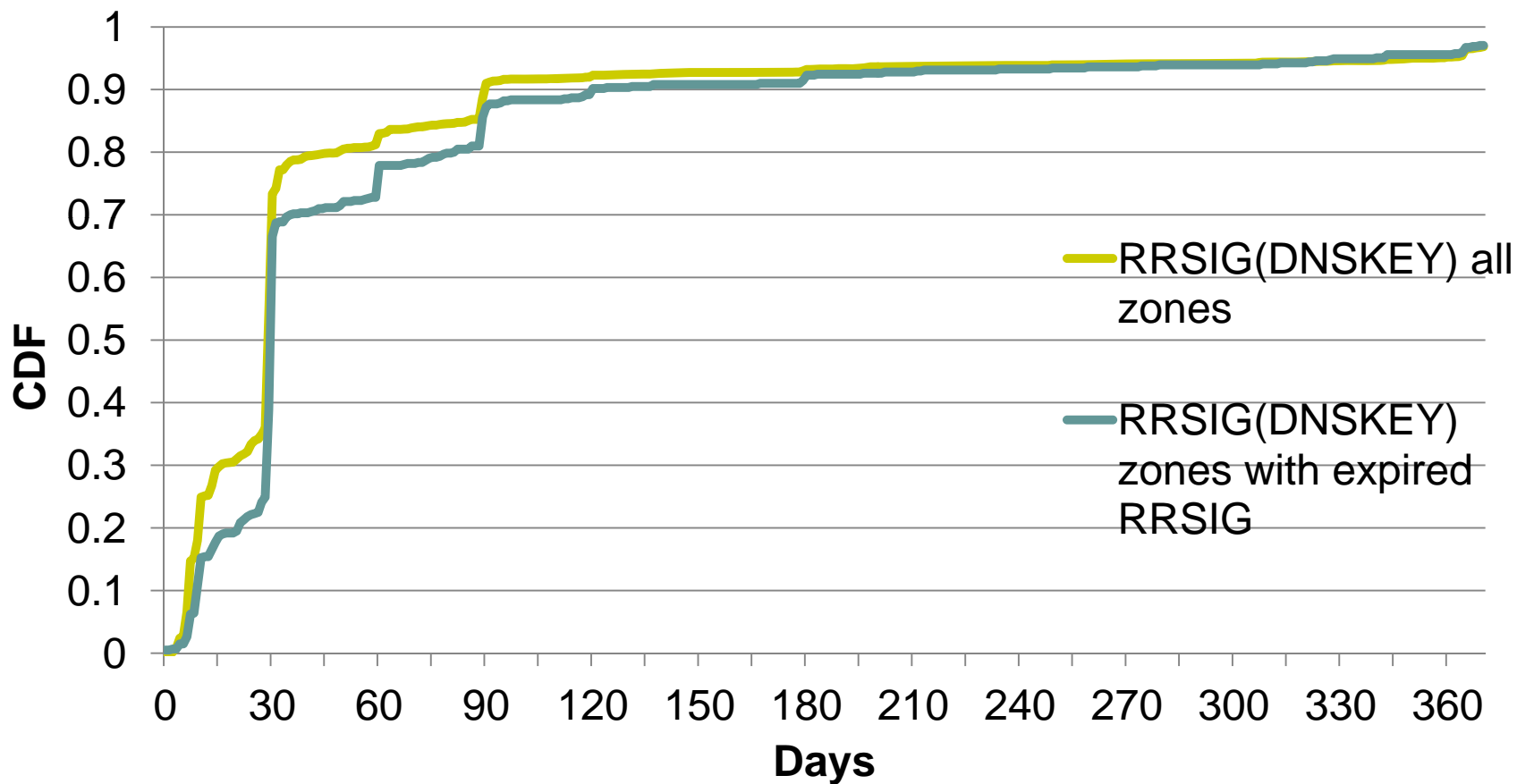- Conclusions and solutions

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
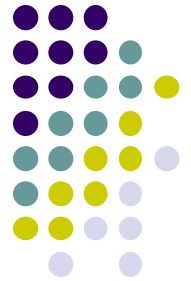
Survey breakdown by TLD
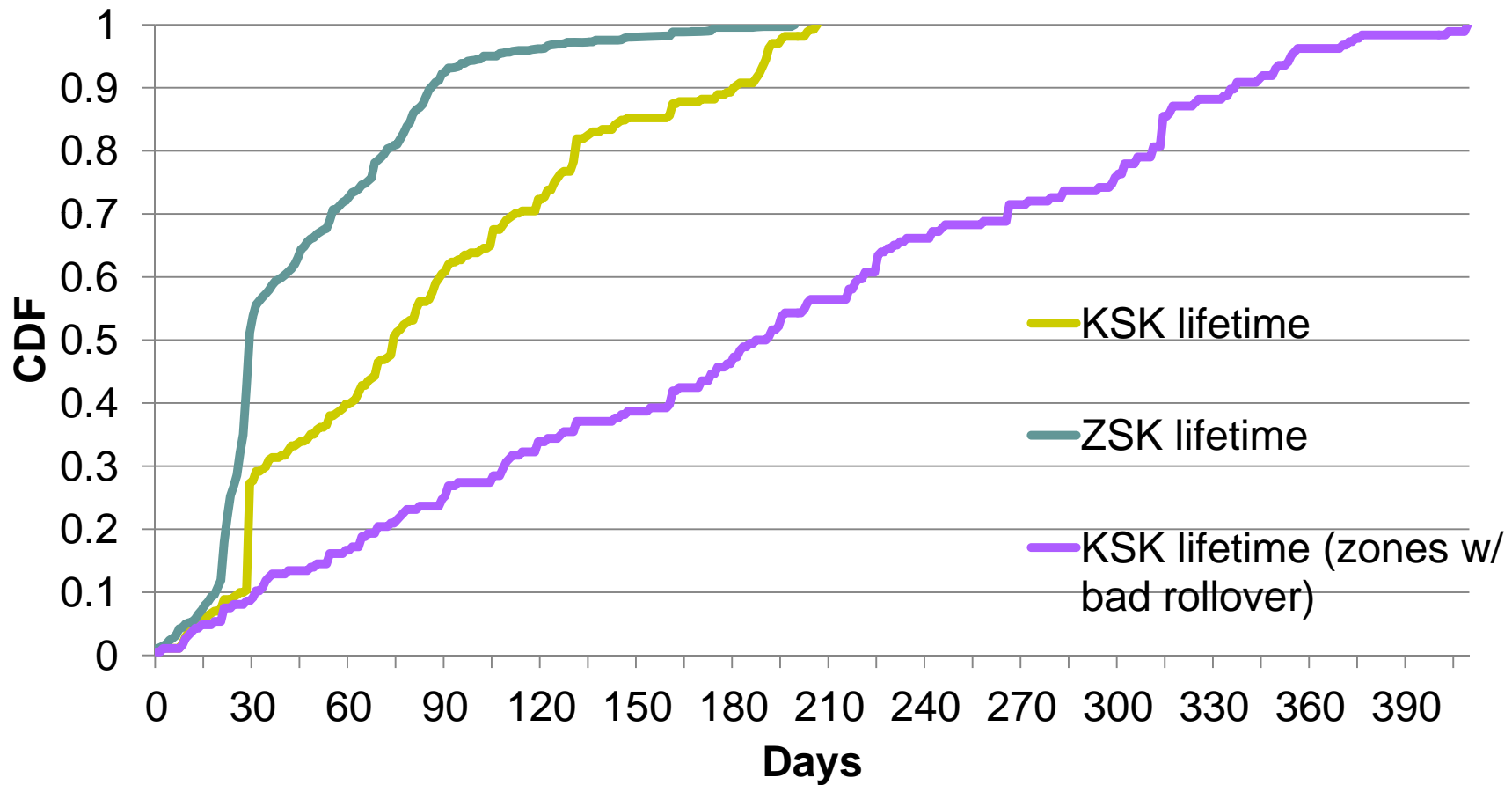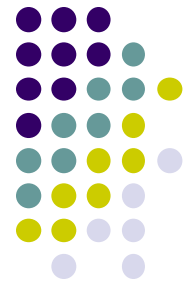

23

RRSIG lifetimes

DNSKEY rollovers

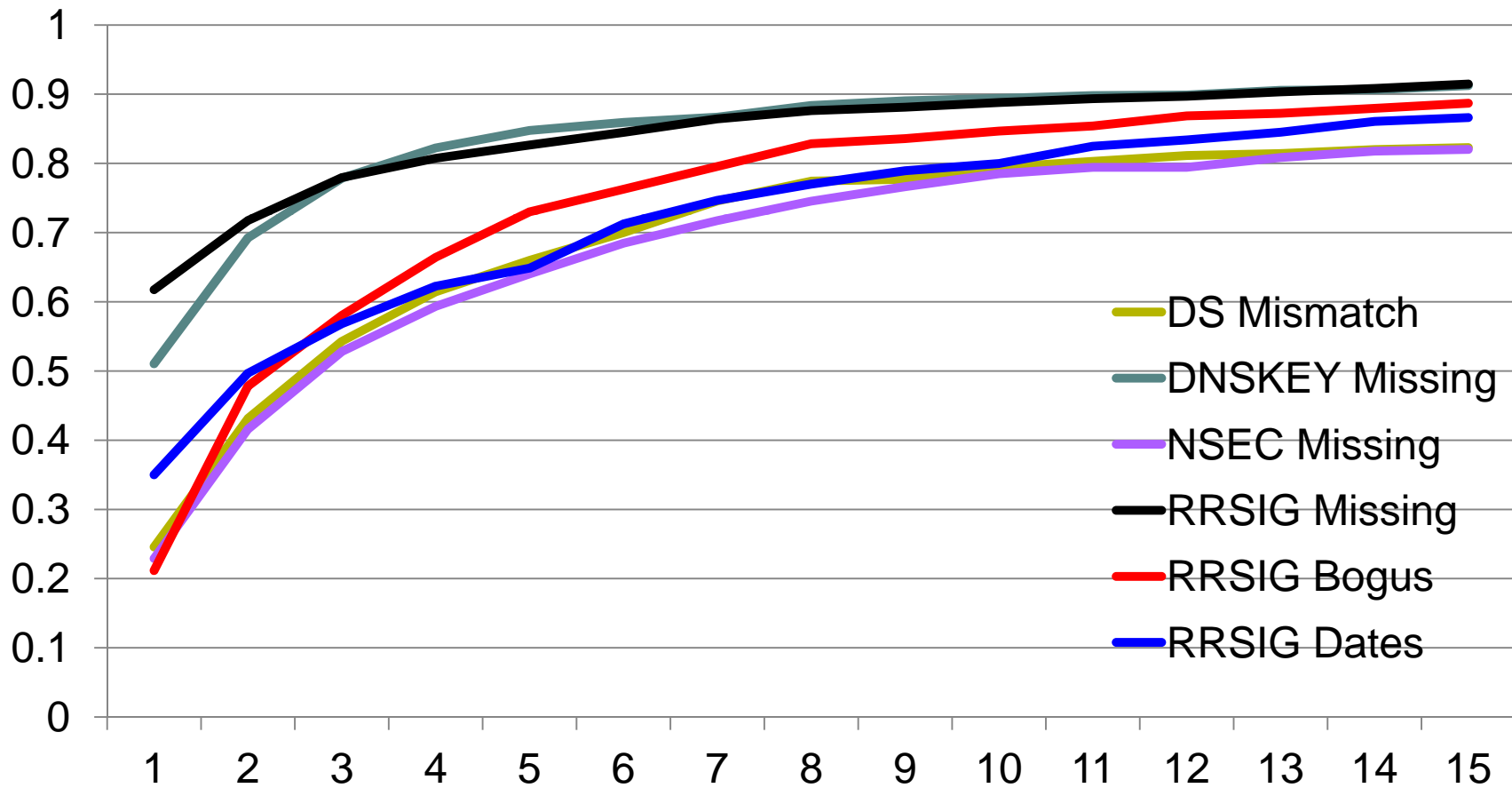| Key role	Zones that did not roll key (0)	Zones that rolled key once (1)	Zones that rolled key more than once (>1)
ZSK	37%	11%	52%
KSK	72%	17%	10%

DNSKEY lifetime

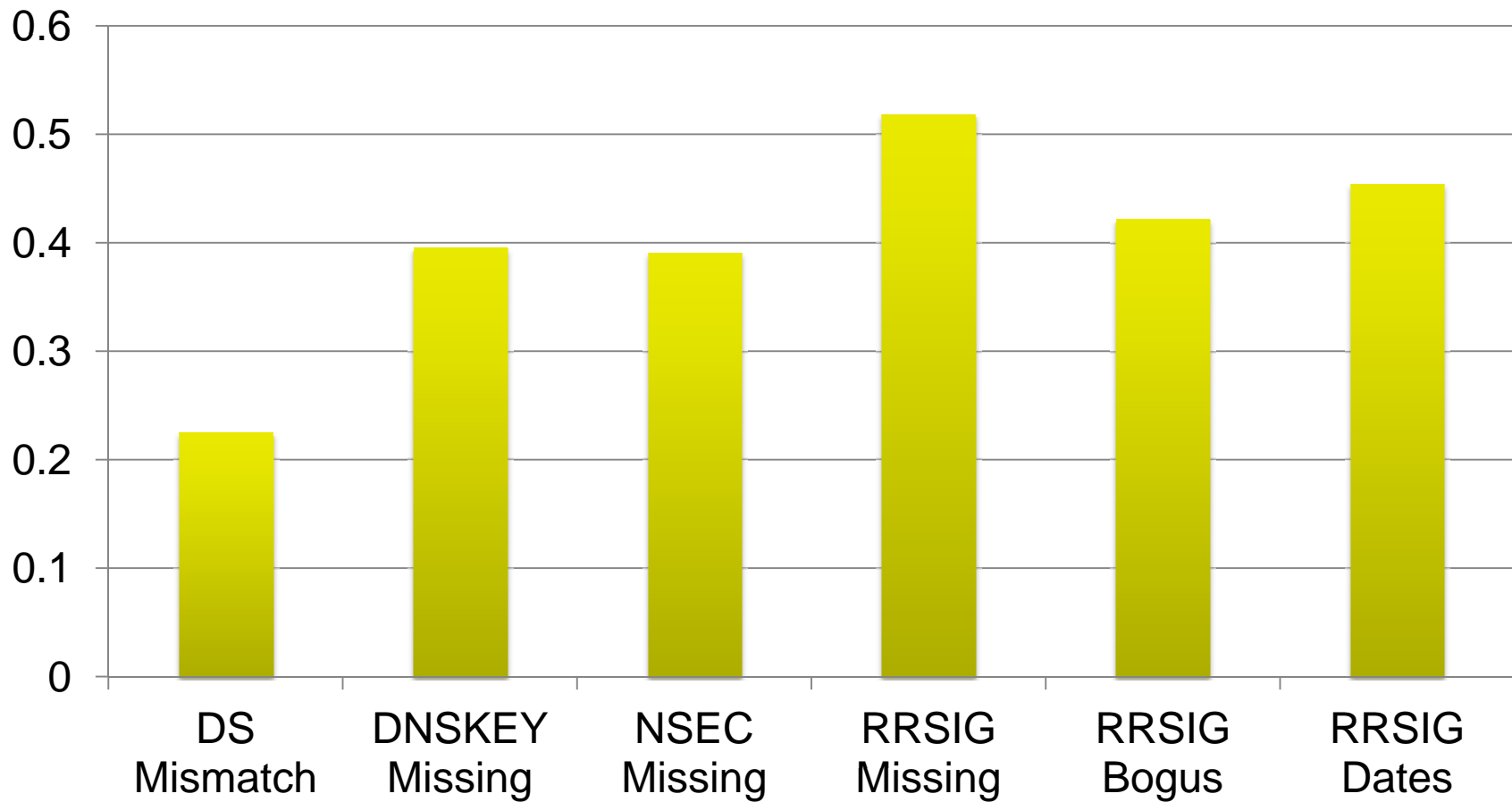# Misconfigurations by type
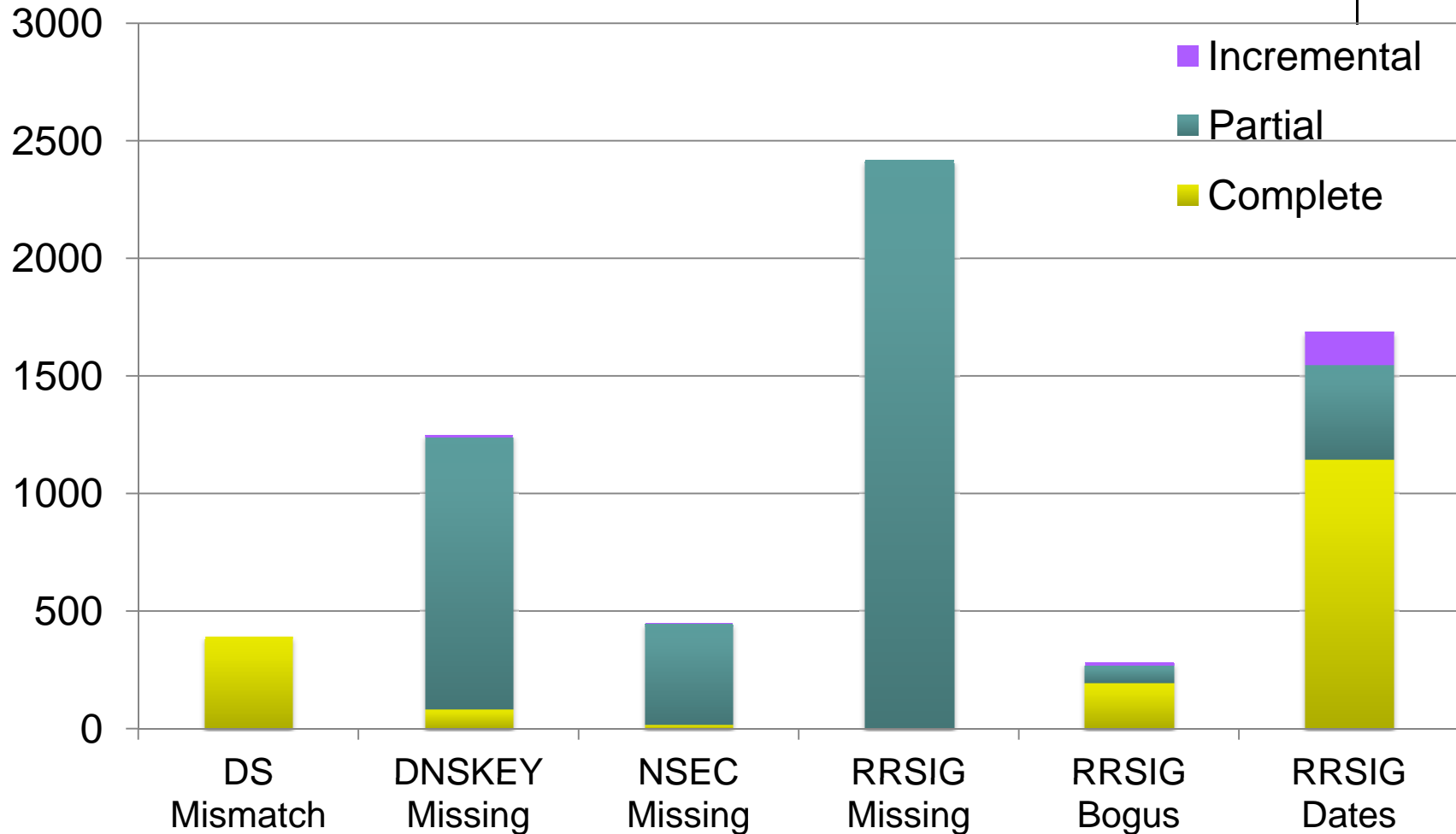
Event duration

Repeat offense rate

IPv6 analysis
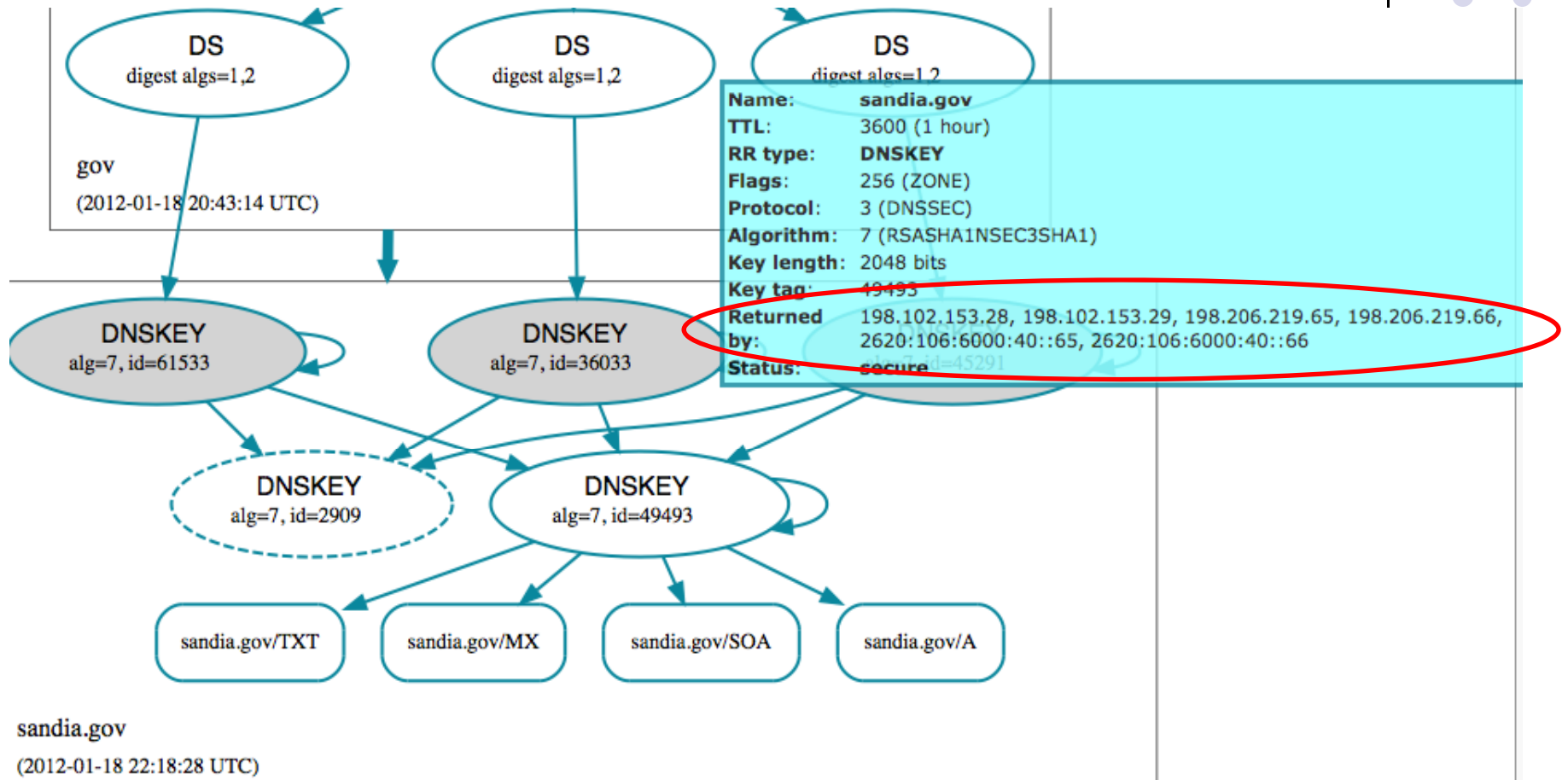
IPv6 inconsistencies
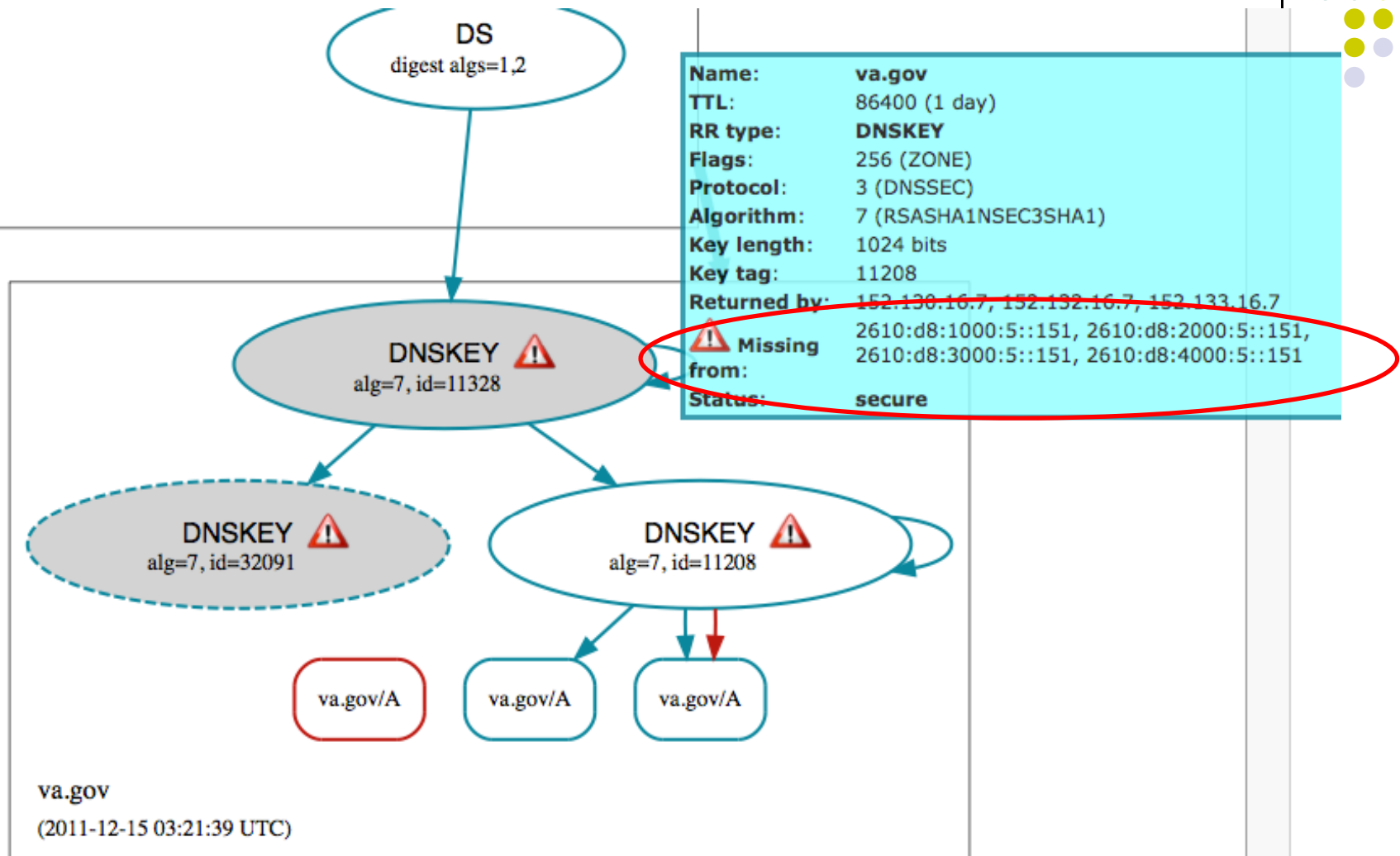
Outline

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

Sandia
National
Laboratories

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.

Sandia National Laboratories

Solutions

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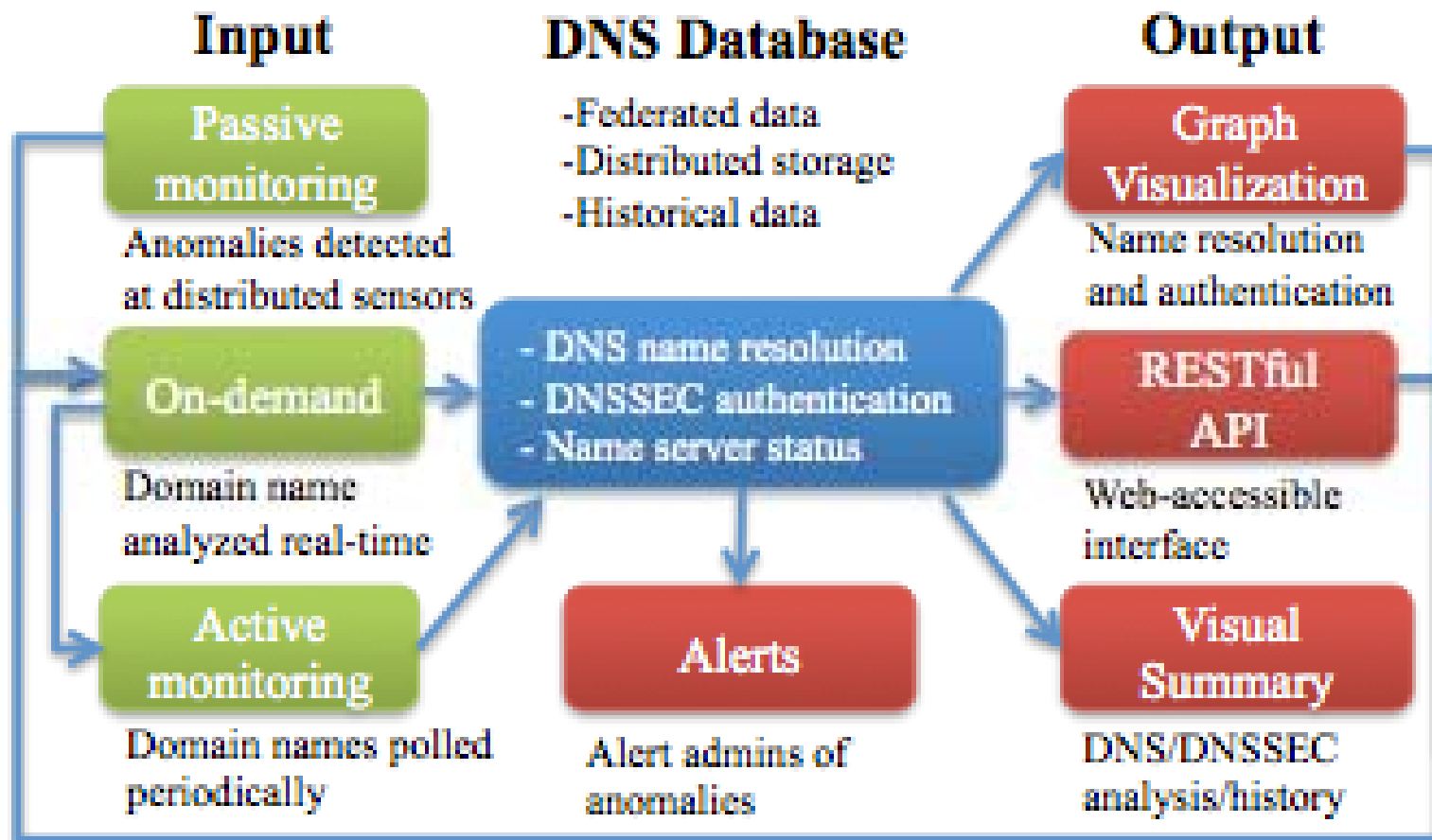 - Pointers to specification
  - Resources for corrective action
- Tools/resources for detection/notification of misconfiguration
  - Individual monitoring and alerts
  - Global monitoring and alerts

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

Input

Passive monitoring
Anomalies detected at distributed sensors

On-demand
Domain name analyzed real-time

Active monitoring
Domain names polled periodically

DNS Database
- Federated data
- Distributed storage
- Historical data

- DNS name resolution
- DNSSEC authentication
- Name server status

Alerts
Alert admins of anomalies

Output

Graph Visualization
Name resolution and authentication

RESTful API
Web-accessible interface

Visual Summary
DNS/DNSSEC analysis/history

Sandia National Laboratories

Questions?

- ctdecci@sandia.gov