SAND2011-2210C

A Case for Comprehensive DNSSEC Monitoring and Analysis Tools

Casey Deccio

Sandia National Laboratories

SATIN 2011

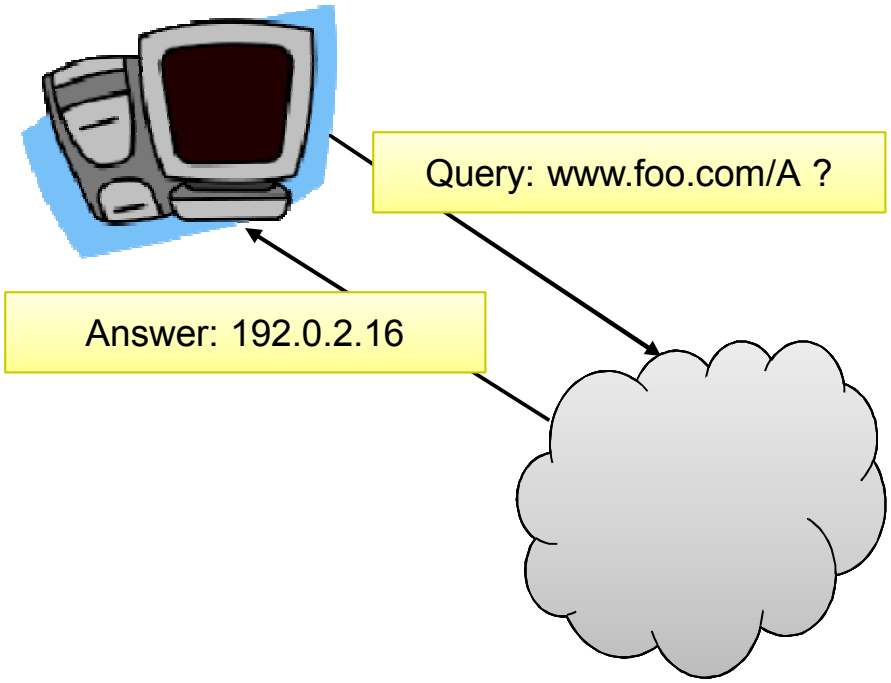
National Physical Laboratory, Teddington, UK

Apr 4, 2011

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.

DNS objectives and challenges

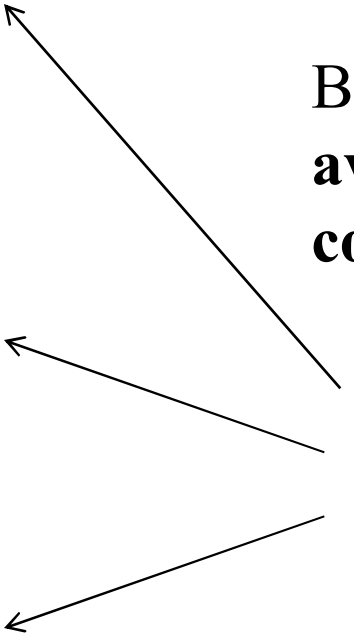
- **Availability**
  - Responsiveness of authoritative servers upon which name resolution is dependent
- **Consistency**
  - Consistent responses across authoritative servers
- **Integrity**
  - Correctness of data returned by resolvers



Sandia National Laboratories

DNSSEC implications

- **Availability**
  - Responsiveness of authoritative servers upon which name resolution is dependent
- **Consistency**
  - Consistent responses across authoritative servers
- **Integrity**
  - Correctness of data returned by resolvers



Brings challenges to **availability** and **consistency**

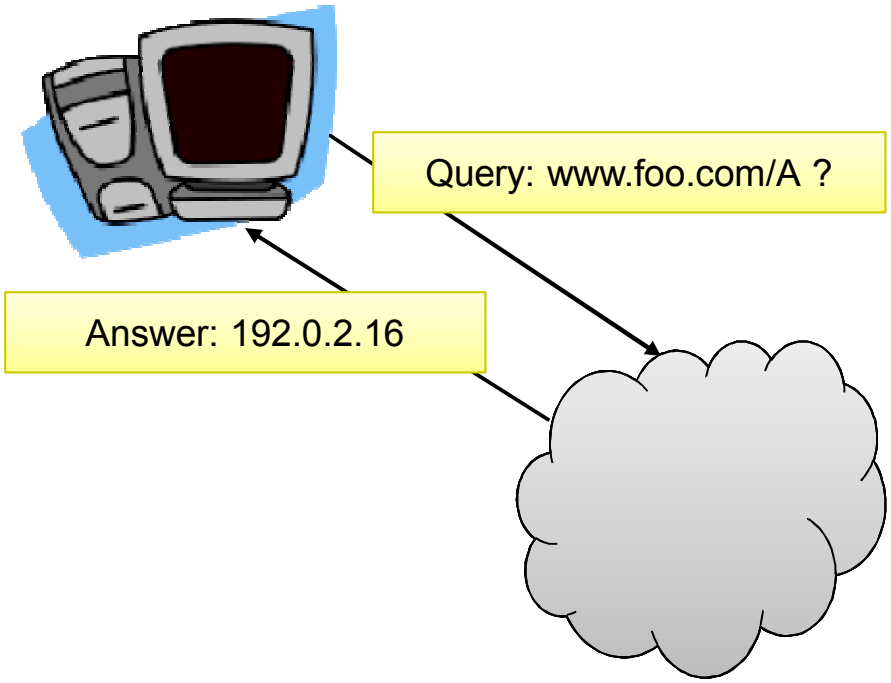
DNSSEC

Explicitly addresses **integrity**

Sandia National Laboratories

Objectives

- **Identify** DNSSEC operational pitfalls
- **Analyze** results of DNSSEC deployment survey to determine problem pervasiveness
- **Propose** solutions for improving DNS availability, consistency, and integrity

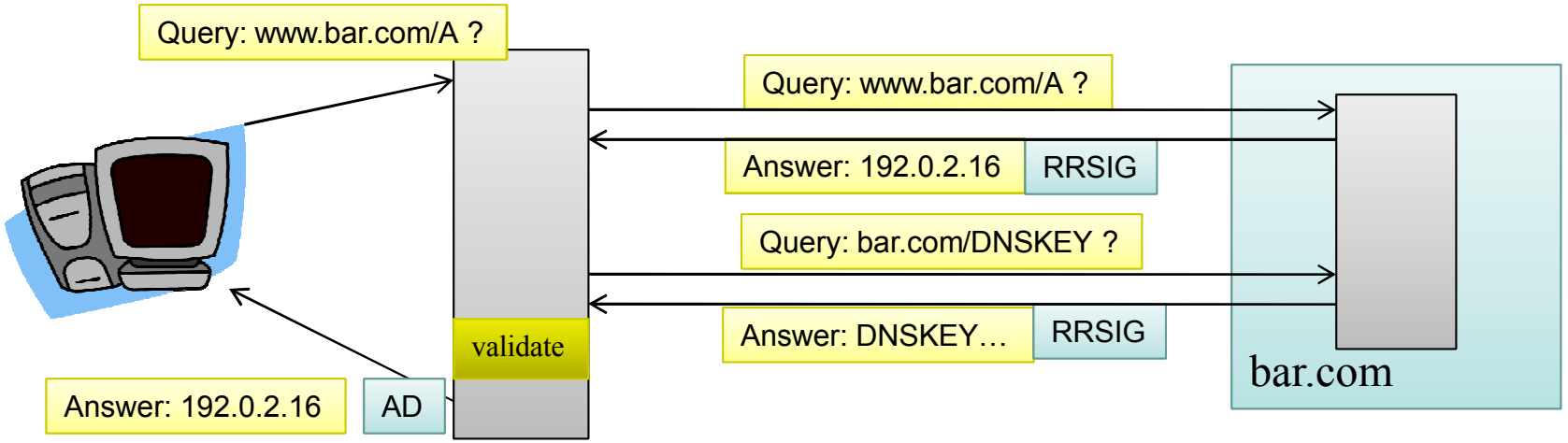


Outline

- DNSSEC workings
- DNSSEC challenges
- DNSSEC survey and results
- Solutions

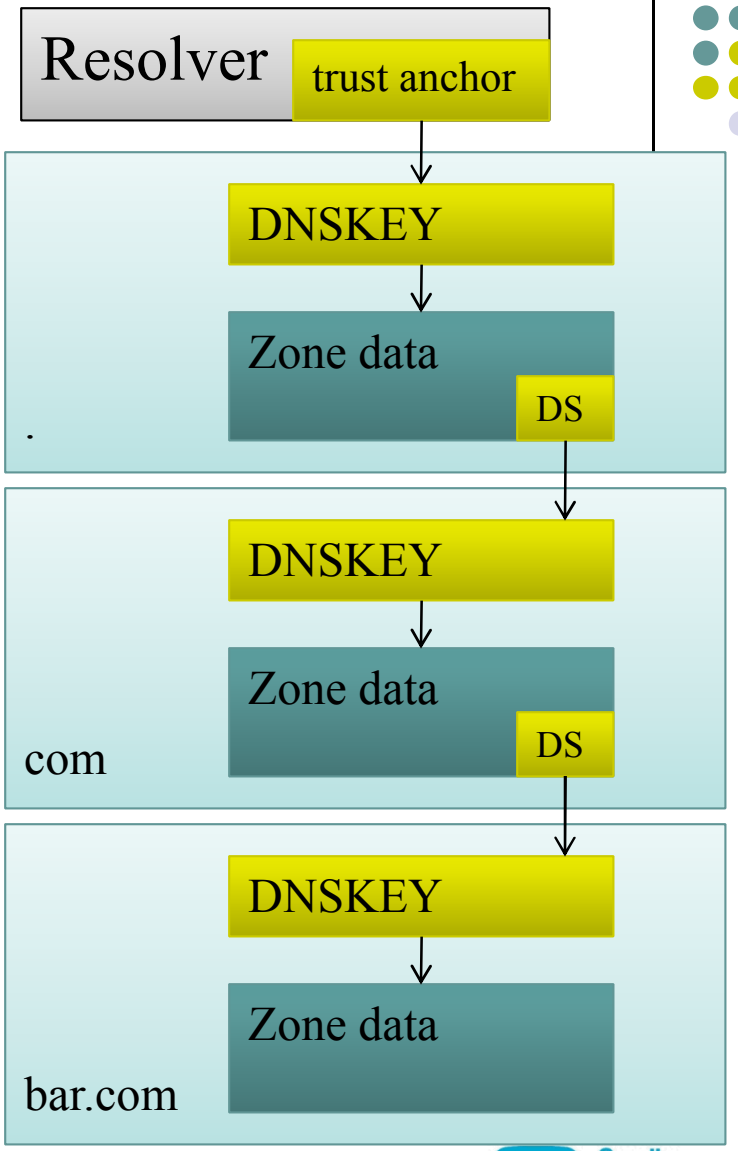
DNS Security Extensions (DNSSEC)

- 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

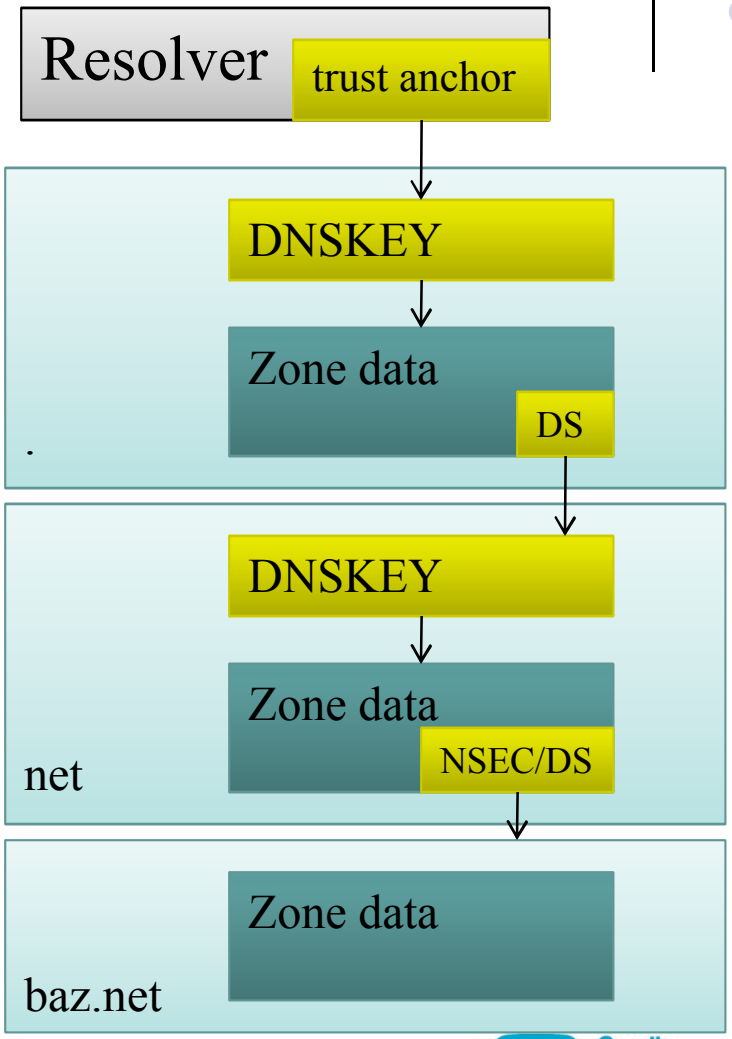
- DNSKEY must be authenticated
- Resolver must have some notion of trust
- Trust extends through ancestry to a trust anchor at resolver
- DS resource record – provides digest of DNSKEY in child zone



Sandia National Laboratories

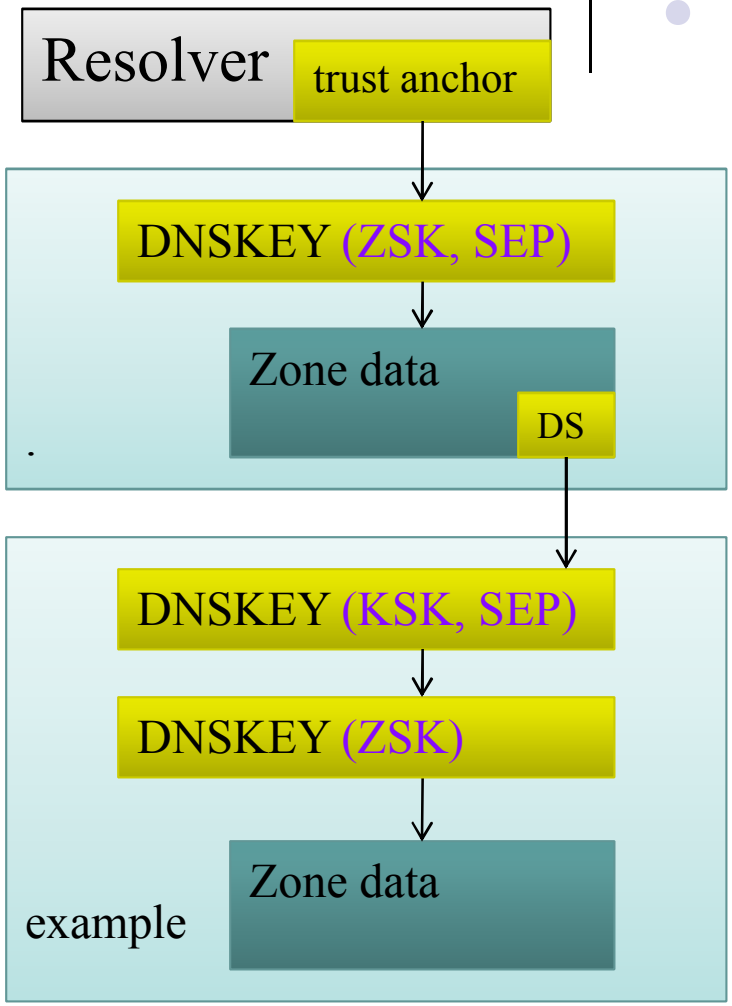
Backwards compatibility… kind of

- 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”)



DNSKEY roles

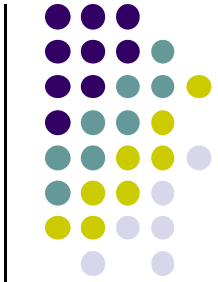
- Secure entry point (SEP)
  - Provides trusted entry into zone (via DS or trust anchor)
  - Every secure zone must have SEP
- Key-signing key (KSK)
  - Signs (only) DNSKEY RRset
  - Typically functions as SEP
  - Authenticates other DNSKEYs
- Zone-signing key (ZSK)
  - Signs zone data
  - If one DNSKEY setup: ZSK also signs DNSKEY RRset and is SEP
- Published key
  - No signing role



Outline

- DNSSEC workings
- DNSSEC challenges
- DNSSEC survey and results
- Solutions

DNSSEC challenges – maintenance



- More maintenance required than for unsigned zones
  - RRSIG refreshing
  - DNSKEY rollovers
    - ZSK (only) rollovers (self-contained)
    - SEP rollovers (interaction with parent or trust anchor)
  - Algorithm changes

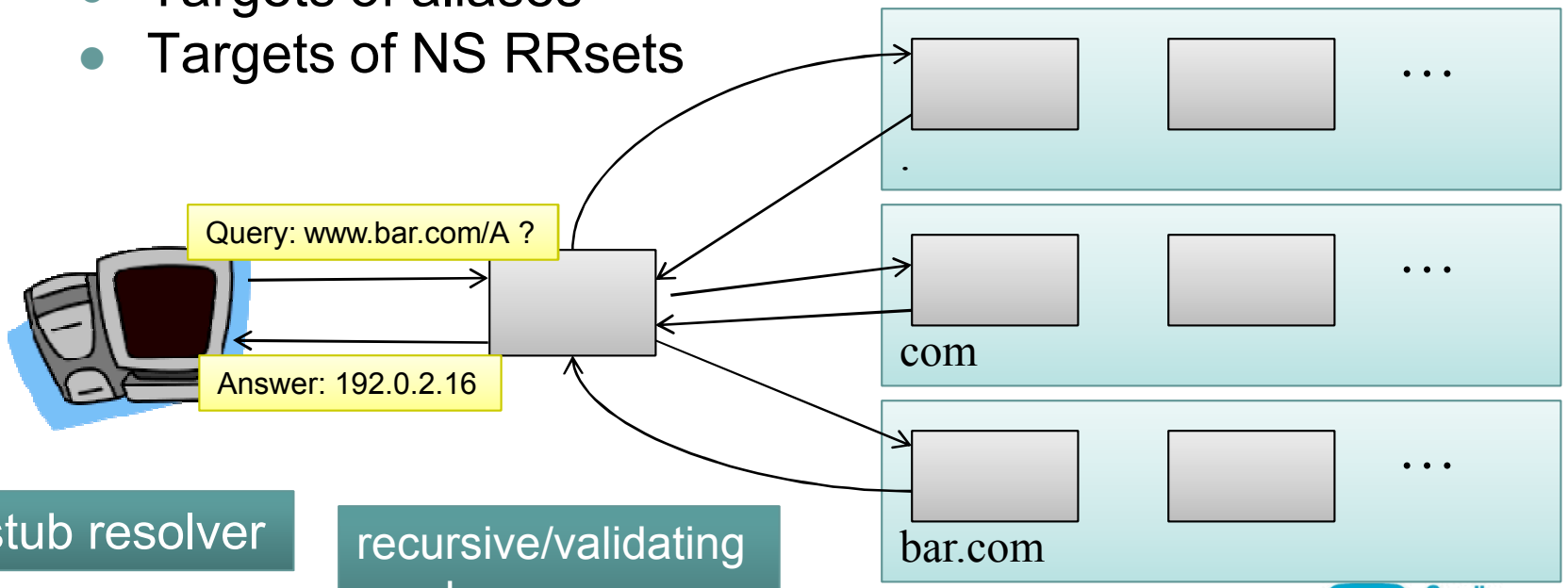
DNSSEC challenges – product support

- DNSSEC implementations are “new”
- There are varying levels of DNSSEC support on authoritative servers
  - Support for DNSSEC RR types
    - Accept DNSSEC RR types (DNSKEY, NSEC, etc.)
  - DNSSEC protocol support
    - Return RRSIGs, NSEC, DS, appropriately
  - NSEC3 support
    - Return NSEC3s appropriately

Sandia National Laboratories

DNSSEC challenges – dependencies

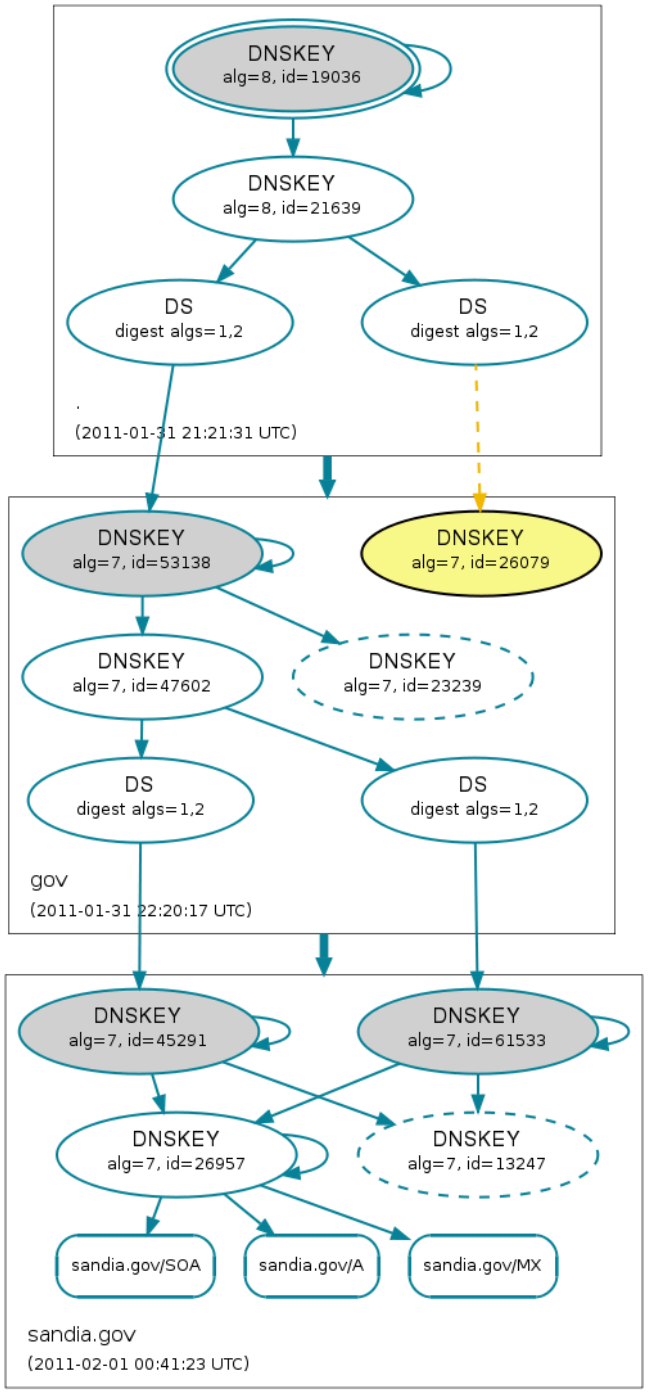
- Dependence on other zones and servers increased for authentication
  - Proper DNSSEC support by authoritative servers
  - Ancestor zones
  - Targets of aliases
  - Targets of NS RRsets



DNSSEC validation status

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

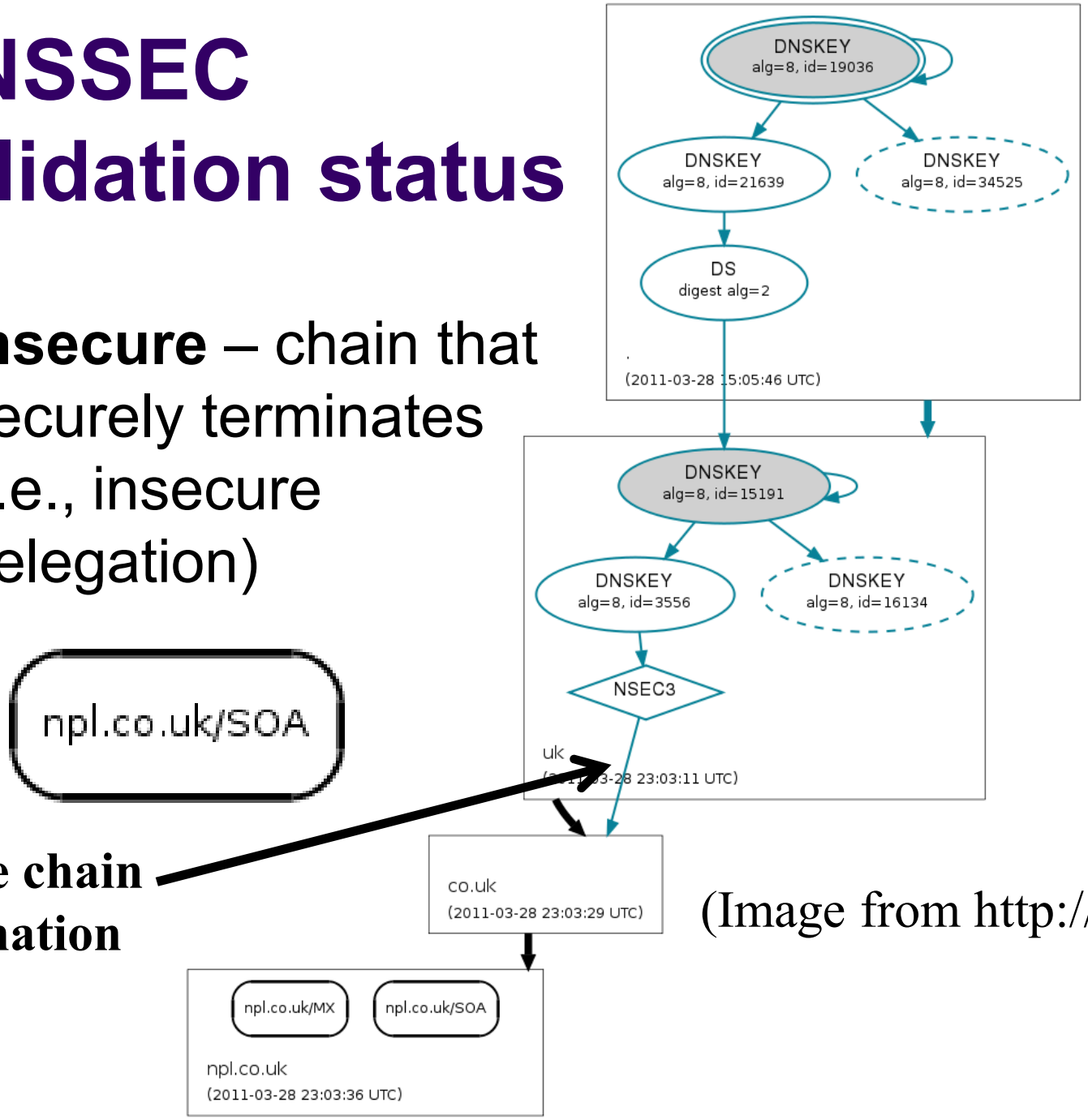
sandia.gov/SOA



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

DNSSEC validation status

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

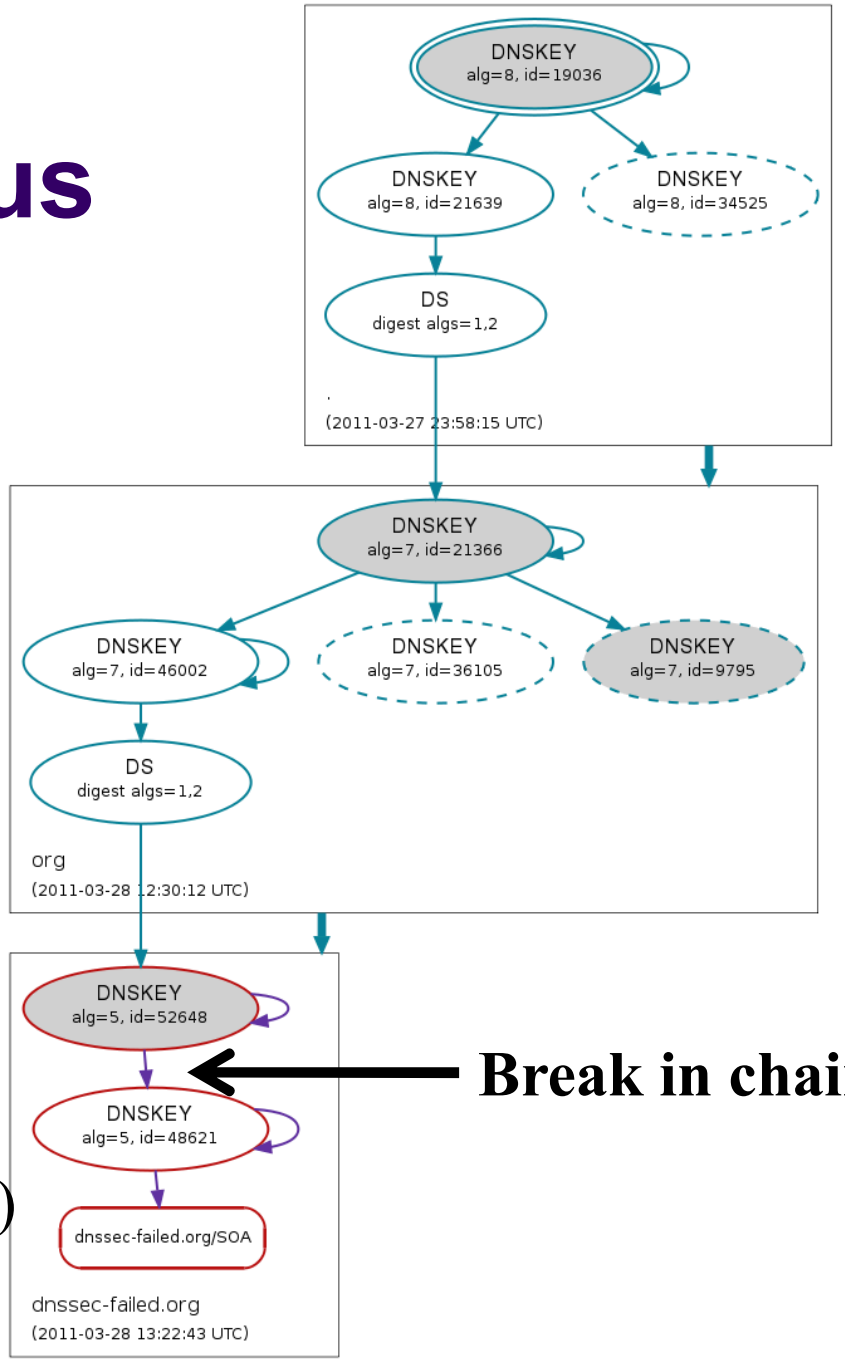


(Image from http://dnsviz.net/)

DNSSEC validation status

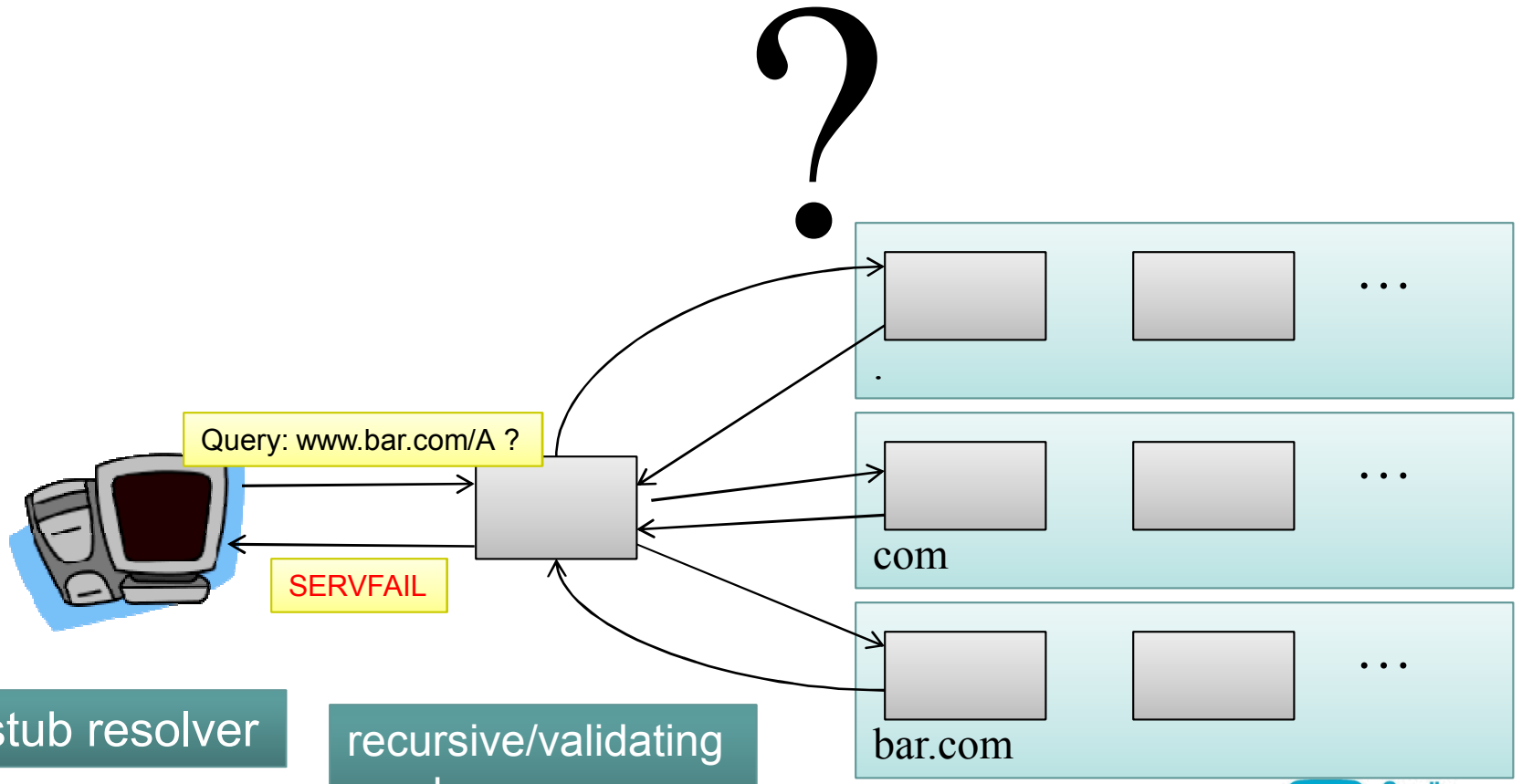
- **Bogus** – broken chain

dnssec-failed.org/SOA



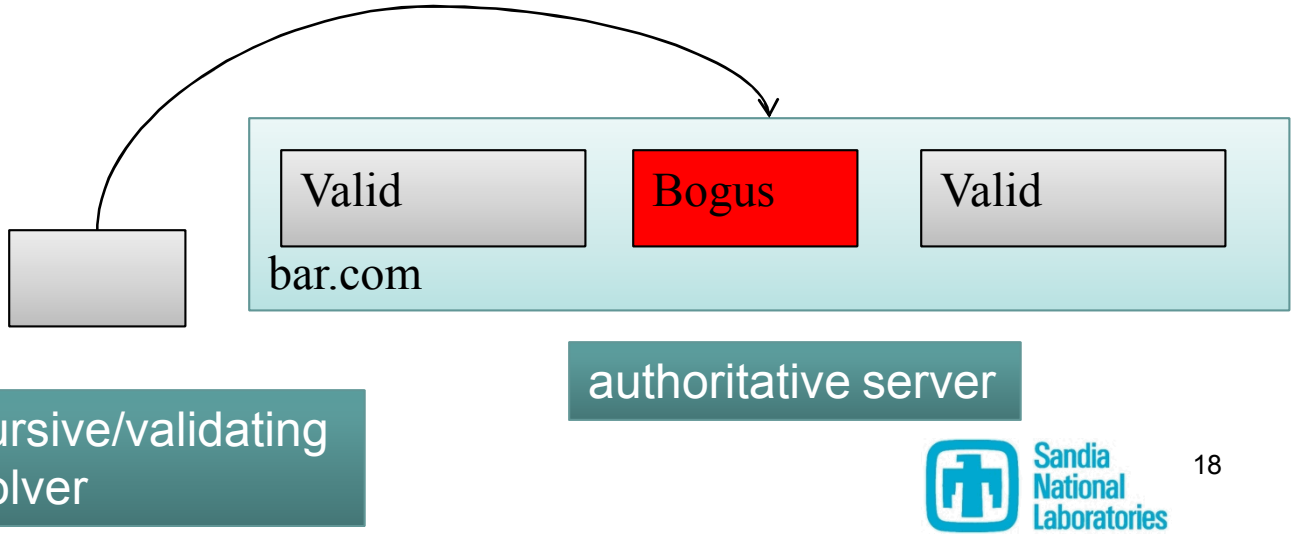
(Image from http://dnsviz.net/)

Data tampering or misconfiguration?



Inconsistent responses

- Inconsistent responses due to stale zone data or insufficient DNSSEC support
- **Possible** failure vs. **certain** failure
- “Smart” resolver implementations exist, but cannot be depended upon
  - Load balancing
  - Failover



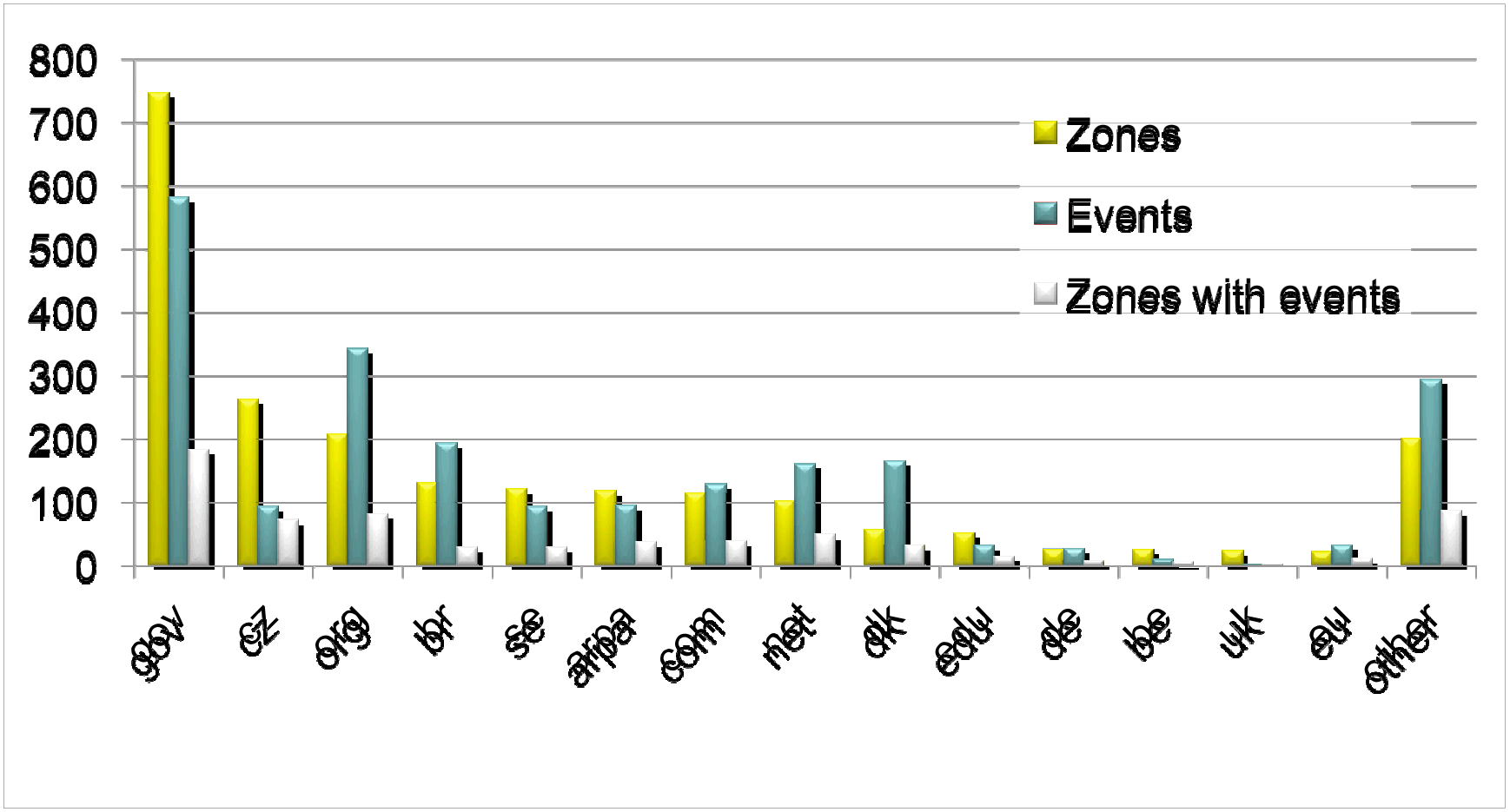
Outline

- DNSSEC workings
- DNSSEC challenges
- DNSSEC survey and results
- Solutions

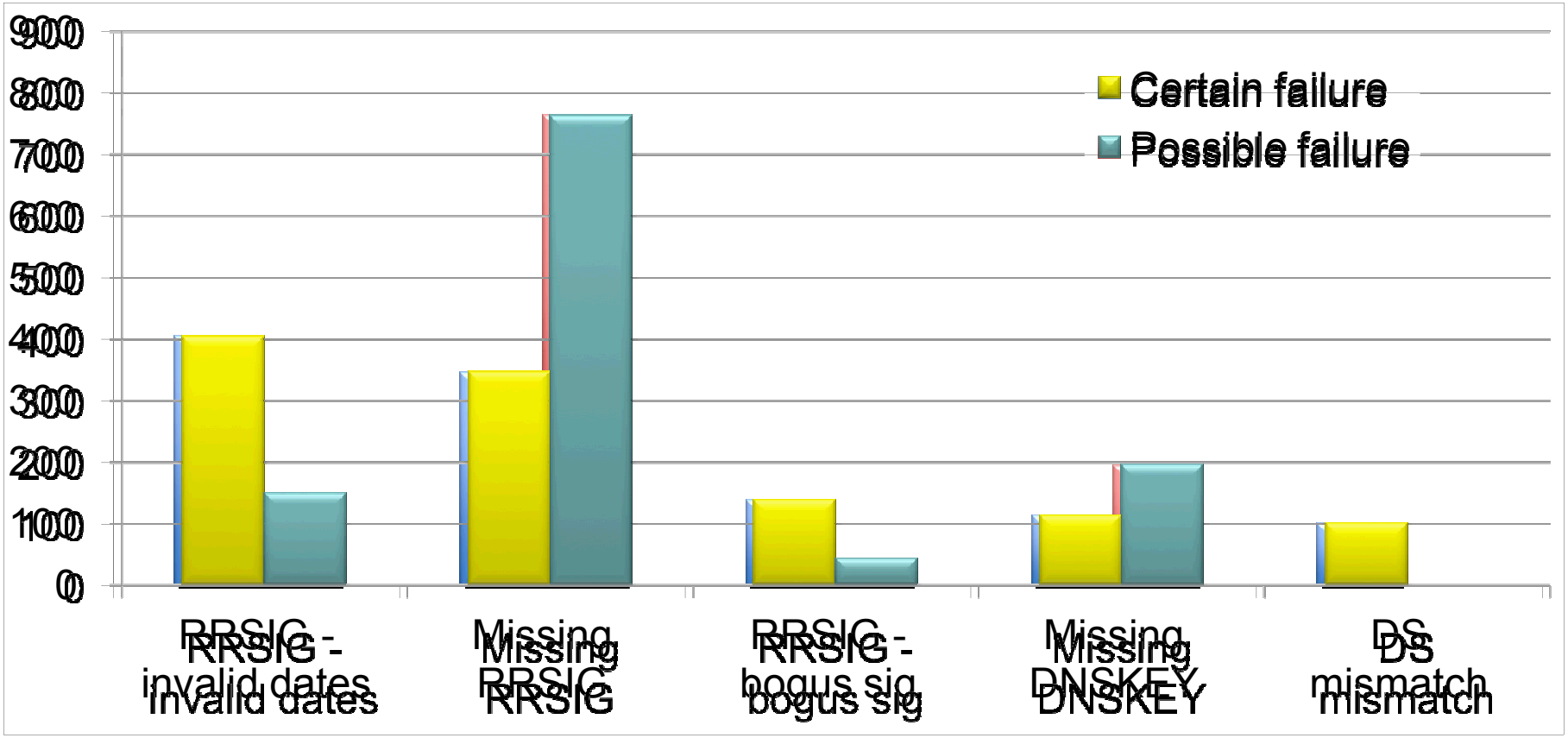
DNSSEC deployment survey

- Polled ~2,200 production signed zones over a five month time frame (June – Nov 2010)
- Validation of SOA RR analyzed every four hours, anchored at ISC DLV or root zone (after July 2010)
- Identified misconfigurations observed in two or more consecutive polls (4+ hours)

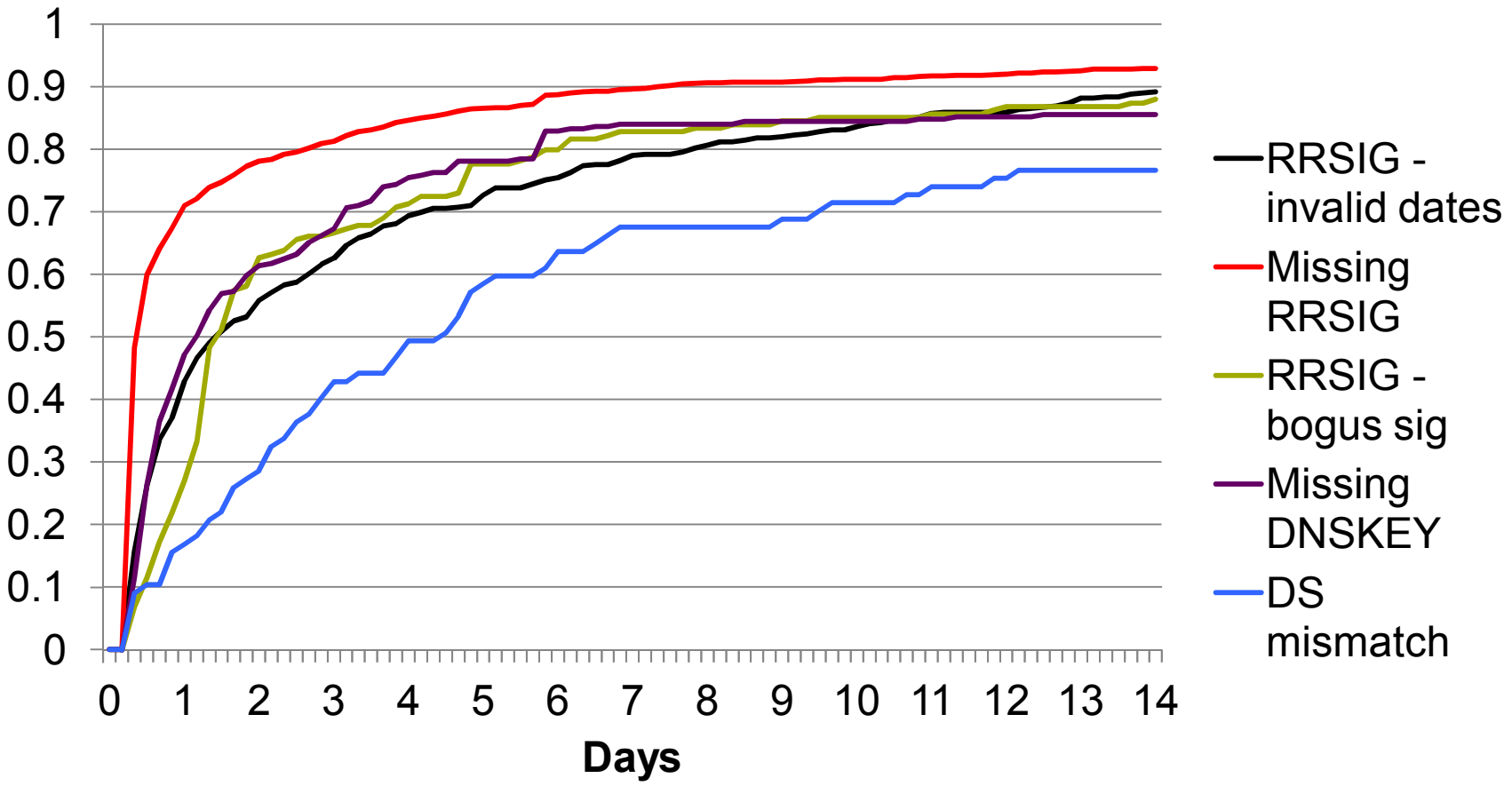
Survey breakdown by TLD



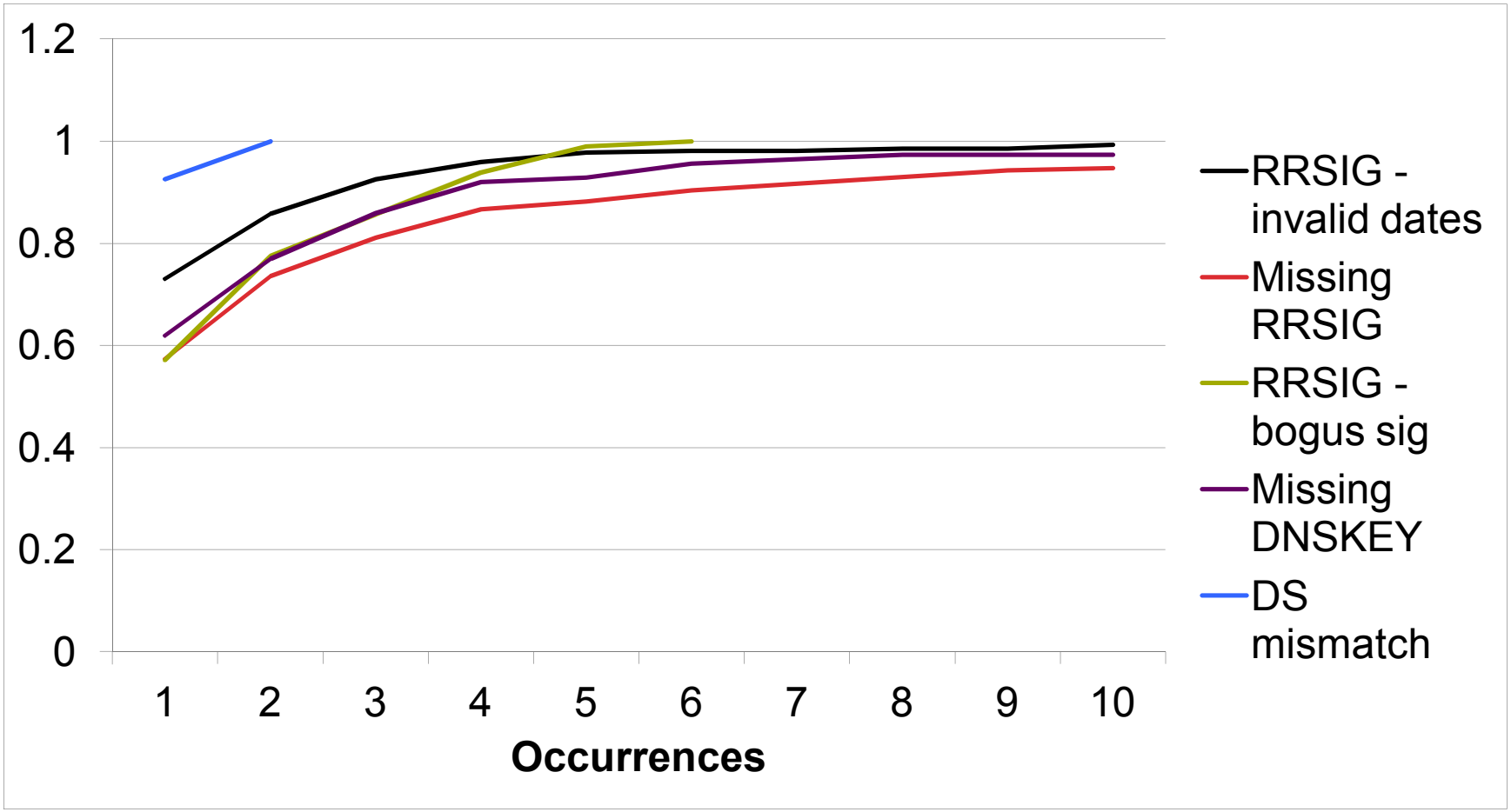
Misconfigurations by type



Event duration



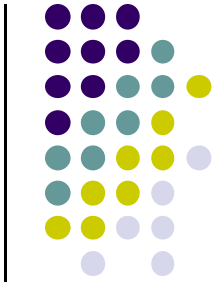
Event repetition



Outline

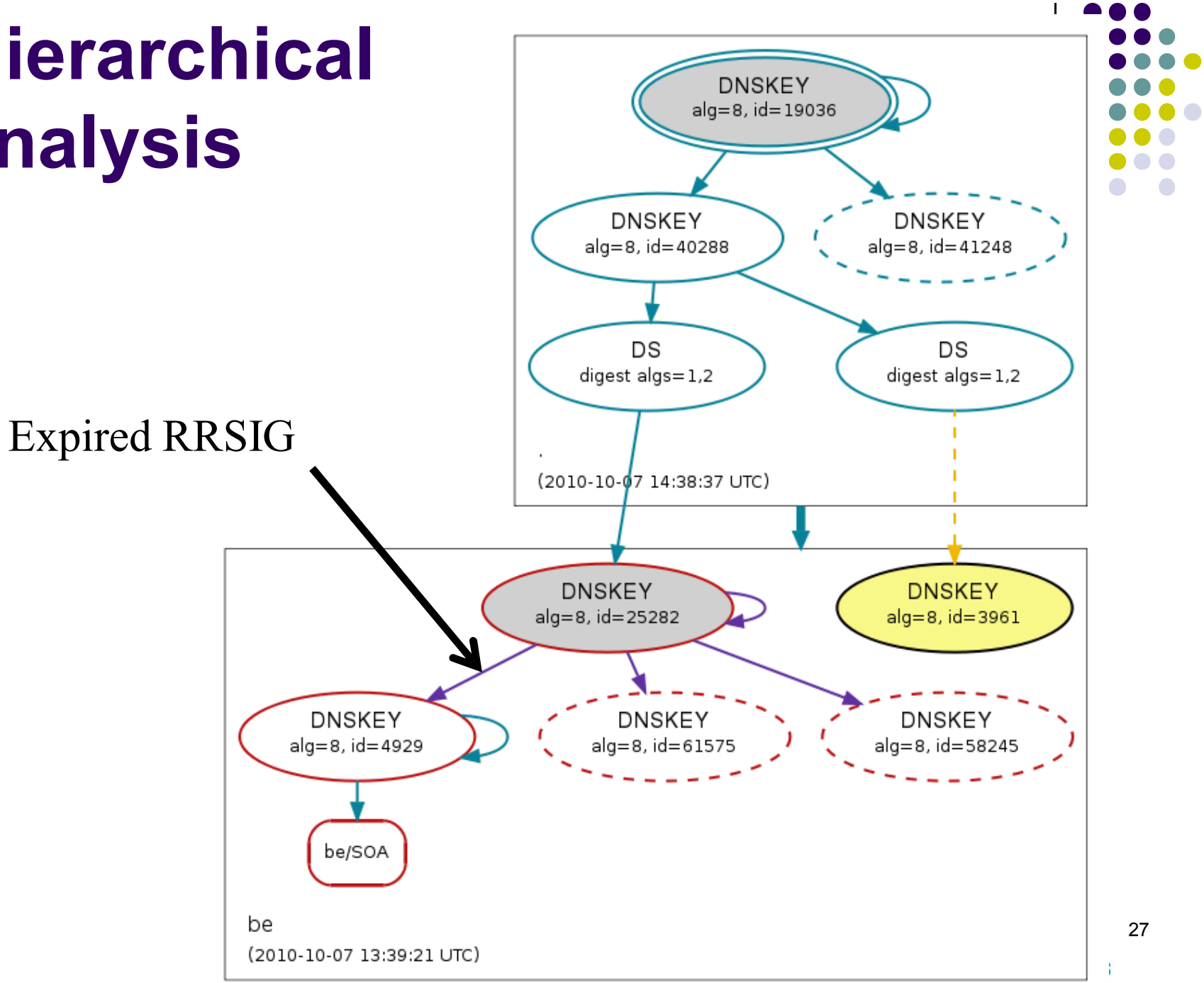
- DNSSEC workings
- DNSSEC challenges
- DNSSEC survey and results
- Solutions

Desired properties of analysis tools



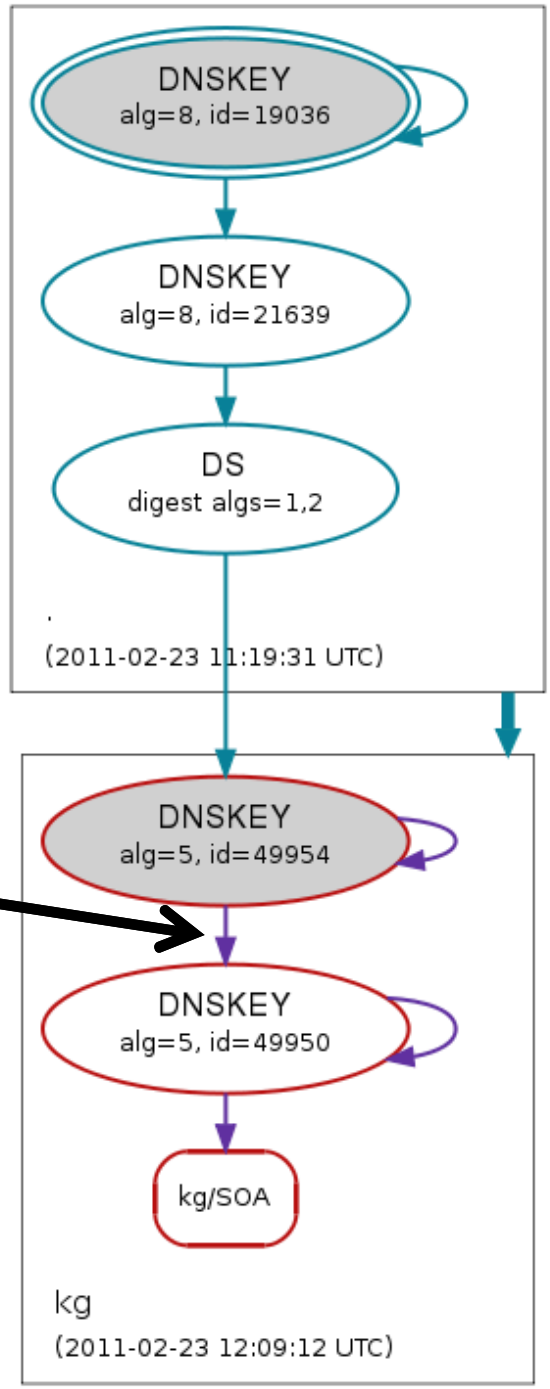
- Multi-dimensional
  - Hierarchical – along chain of trust
  - Lateral – across authoritative servers
  - Diverse – across anycast instances
- Dependency-aware
  - CNAME, MX, NS target dependencies
- Aggregation capable
  - Highlight anomalies
- Targeted
  - Cache analysis
  - Source consciousness

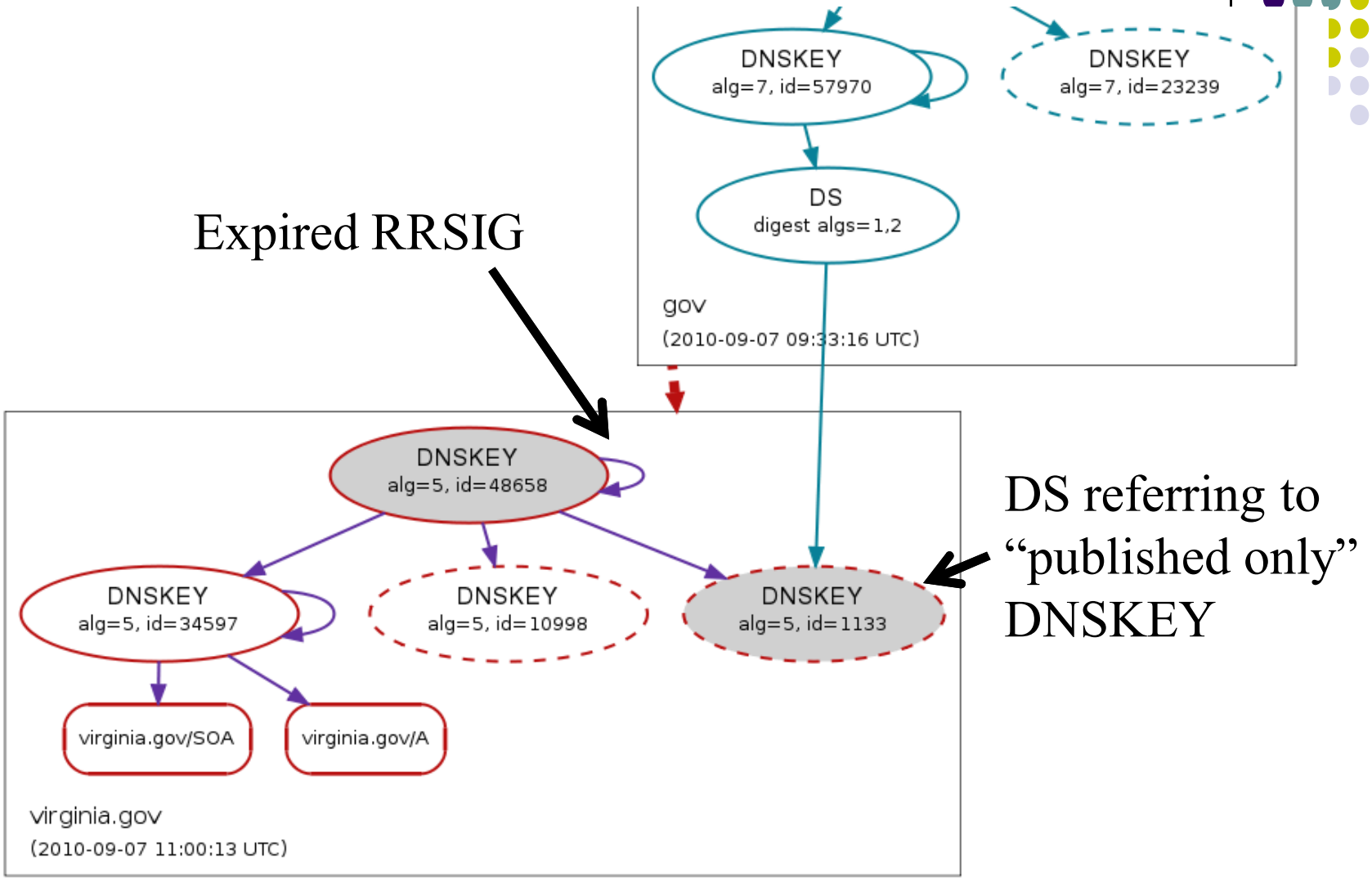
Hierarchical analysis



RRSIG not-yet-valid

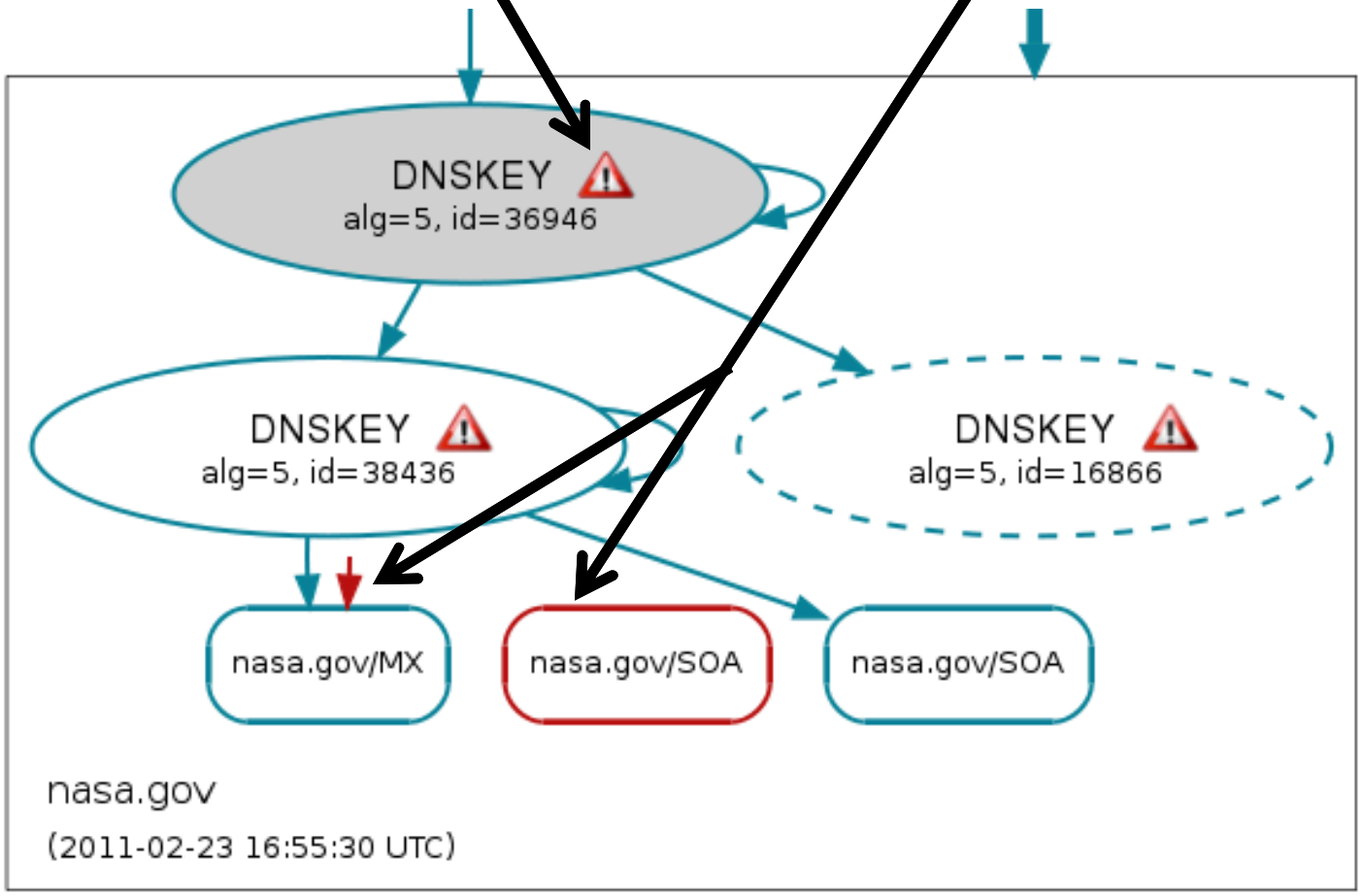
(Persisted for several days)



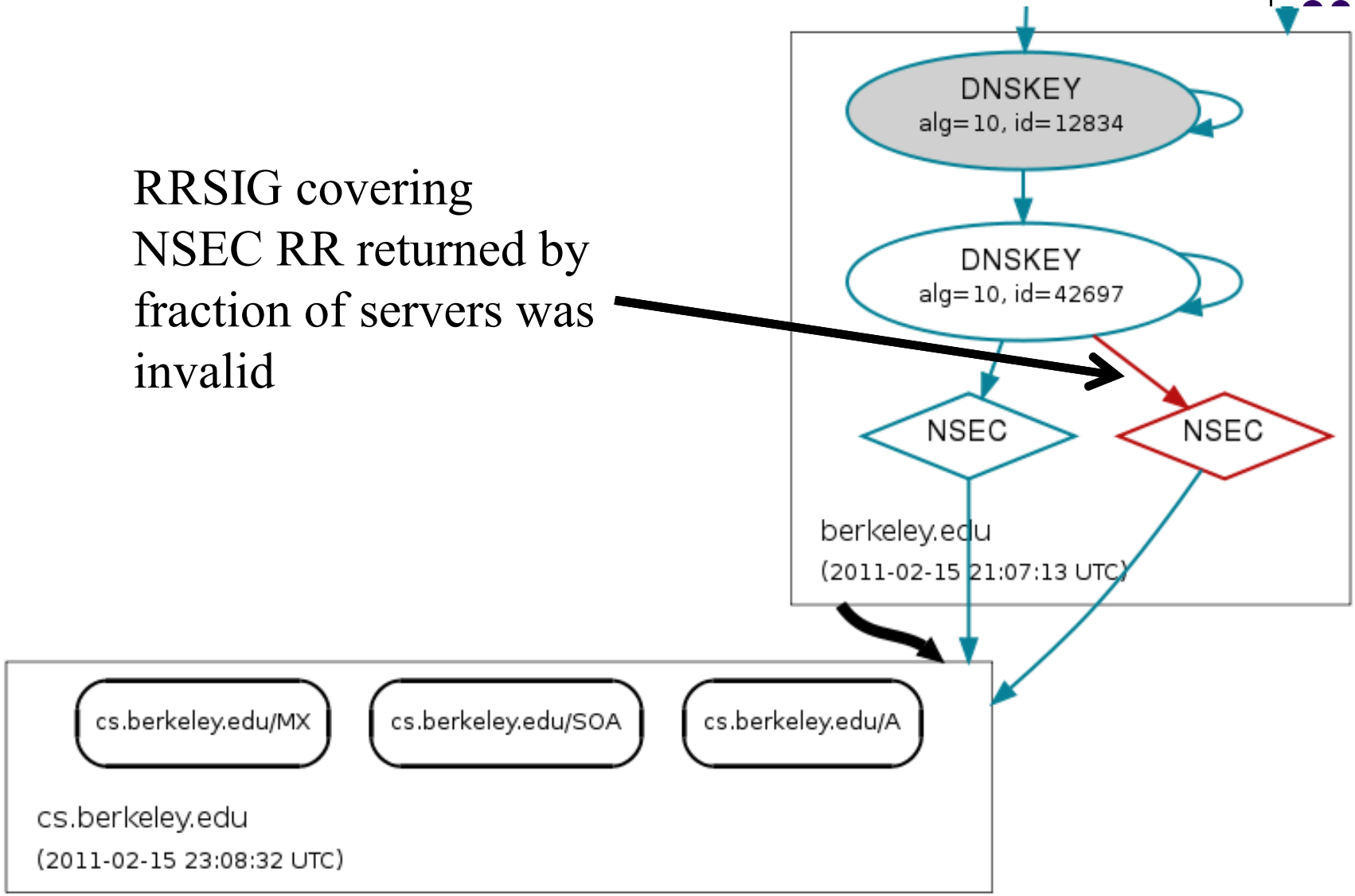

DNSKEY
alg=7, id=57970
DNSKEY
alg=7, id=23239
DS
digest algs=1,2
gov
(2010-09-07 09:33:16 UTC)
Expired RRSIG
DNSKEY
alg=5, id=48658
DNSKEY
alg=5, id=34597
DNSKEY
alg=5, id=10998
DNSKEY
alg=5, id=1133
DS referring to "published only" DNSKEY
virginia.gov/SOA
virginia.gov/A
virginia.gov
(2010-09-07 11:00:13 UTC)

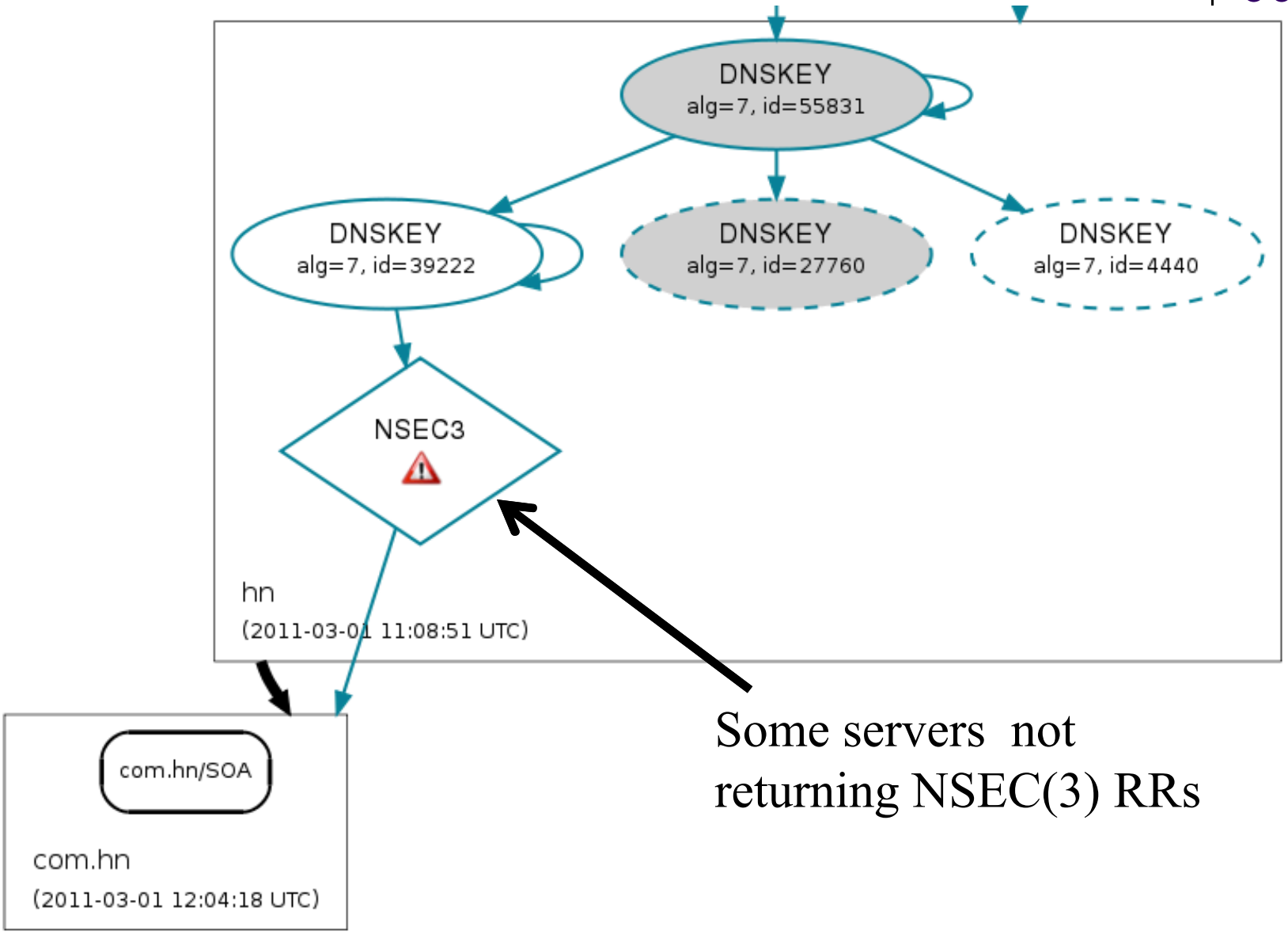
Missing DNSKEYs
from some servers

Missing RRSIGs
from some servers



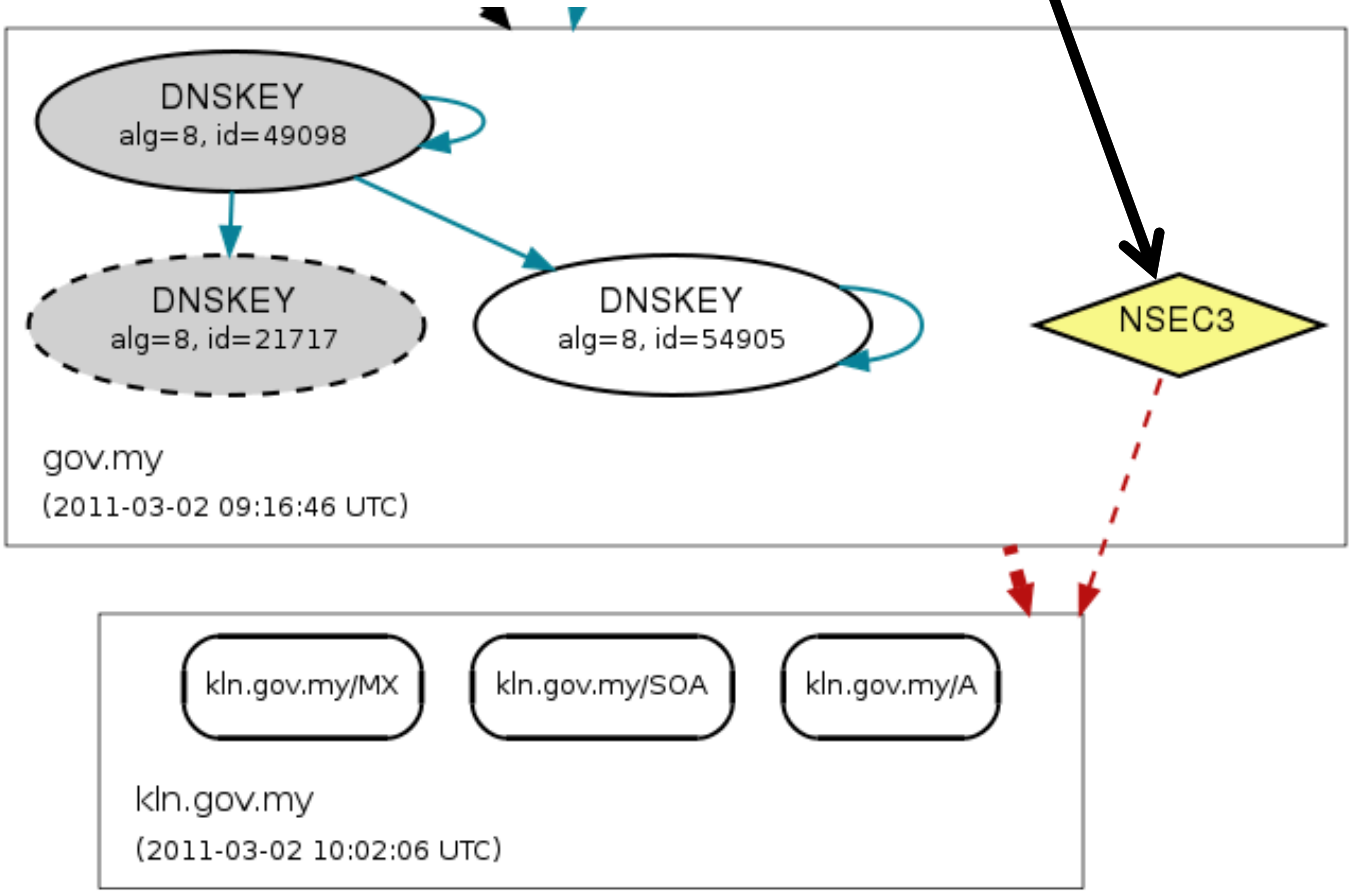
RRSIG covering NSEC RR returned by fraction of servers was invalid





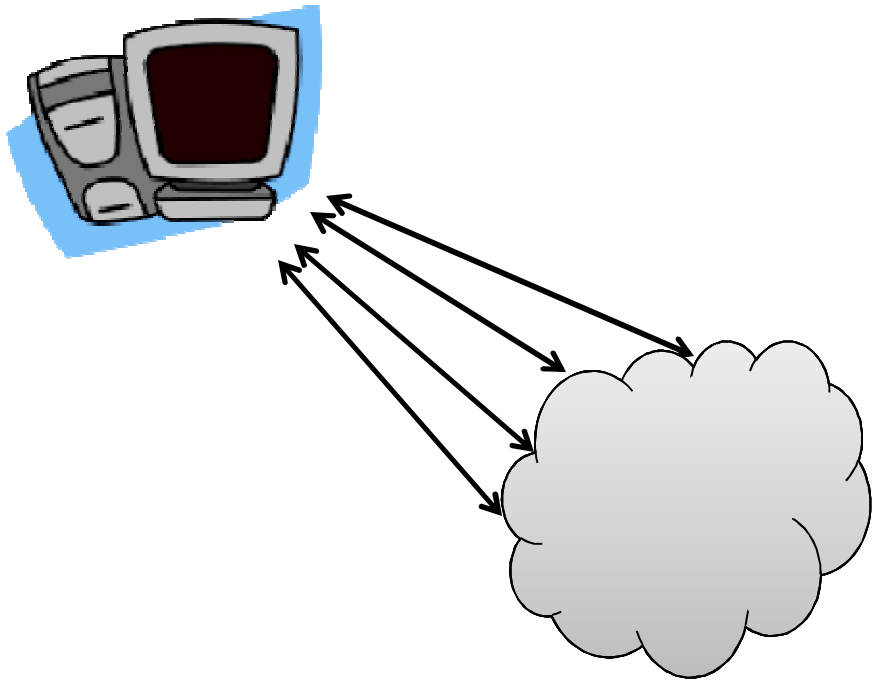
Some servers not returning NSEC(3) RRs

No servers returning NSEC RRs



Monitoring

- Active monitoring
  - Periodic, based on:
    - Usage
    - Level in hierarchy (e.g., TLD)
    - TTL, RRSIG expiration
    - Past experiencing
  - On-demand
- Passive monitoring
  - Validation failures
- Alerts
  - Subscription based
  - Targeted



Summary

- DNSSEC introduces challenges to availability and consistency
- Monitoring and analysis will help administrators learn, troubleshoot, and be alerted of issues in DNSSEC deployments

Acknowledgements

- Jeff Sedayao, Krishna Kant at Intel Corporation
- Prasant Mohapatra at UC Davis

Questions?

- ctdecci@sandia.gov