Quantifying the Impact of DNSSEC Misconfiguration

Casey Deccio

Sandia National Laboratories

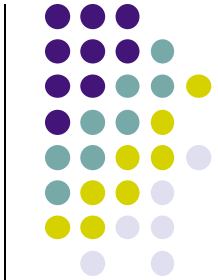
2010 DNS-OARC Workshop (2)

Denver, CO

Oct 14, 2010

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.

Availability and security

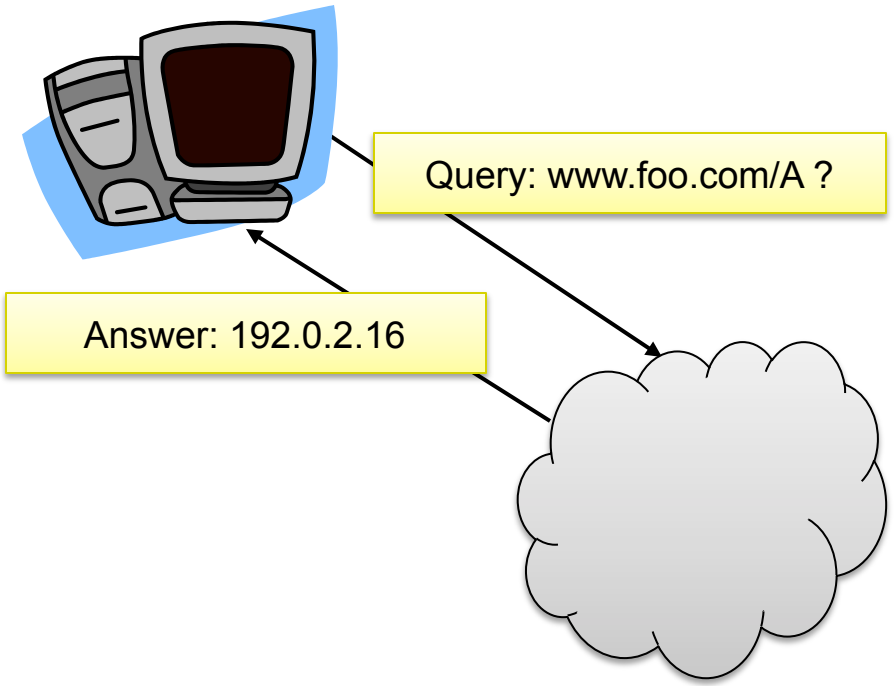


- DNS must be both ***available*** and ***accurate***
- DNSSEC is a security retrofit
  - DNSSEC increases maintenance complexity
  - Troubleshooting is difficult
- Misconfigurations abound, rendering name resolution unavailable

Sandia National Laboratories

Objectives

- Establish model and metrics for assessing availability of DNSSEC deployments
- Quantify complexity that may increase potential for DNSSEC misconfiguration
- Introduce techniques to mitigate effects of misconfiguration



Sandia National Laboratories

Outline

- DNSSEC availability model
- DNS complexity analysis
- Misconfiguration mitigation
- Summary

Outline

- DNSSEC availability model
- DNS complexity analysis
- Misconfiguration mitigation
- Summary

Classes of DNSSEC misconfiguration

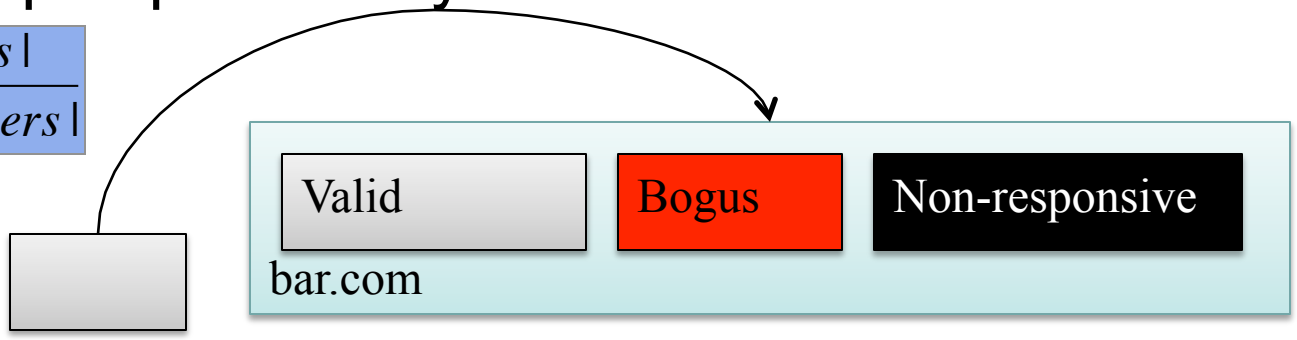
- Zone misconfigurations
  - Missing, expired, or bogus RRSIG
  - Missing DNSKEYs
- Delegation misconfigurations
  - No DNSKEY in child matching any DS in parent
  - Missing NSEC RRs for insecure delegation
- Trust anchor misconfiguration
  - Stale trust anchor at resolver

Sandia National Laboratories

Failure potential

- Probability of bogus validation
- Based on fraction of responsive authoritative servers serving bogus or incomplete data
  - Resolvers will retry if server non-responsive
  - Not all servers will retry if server responds with bogus data
- Assumption: resolver queries any authoritative server with equal probability

$$P_f(z) = \frac{|bogus\_servers|}{|responsive\_servers|}$$



recursive/validating resolver

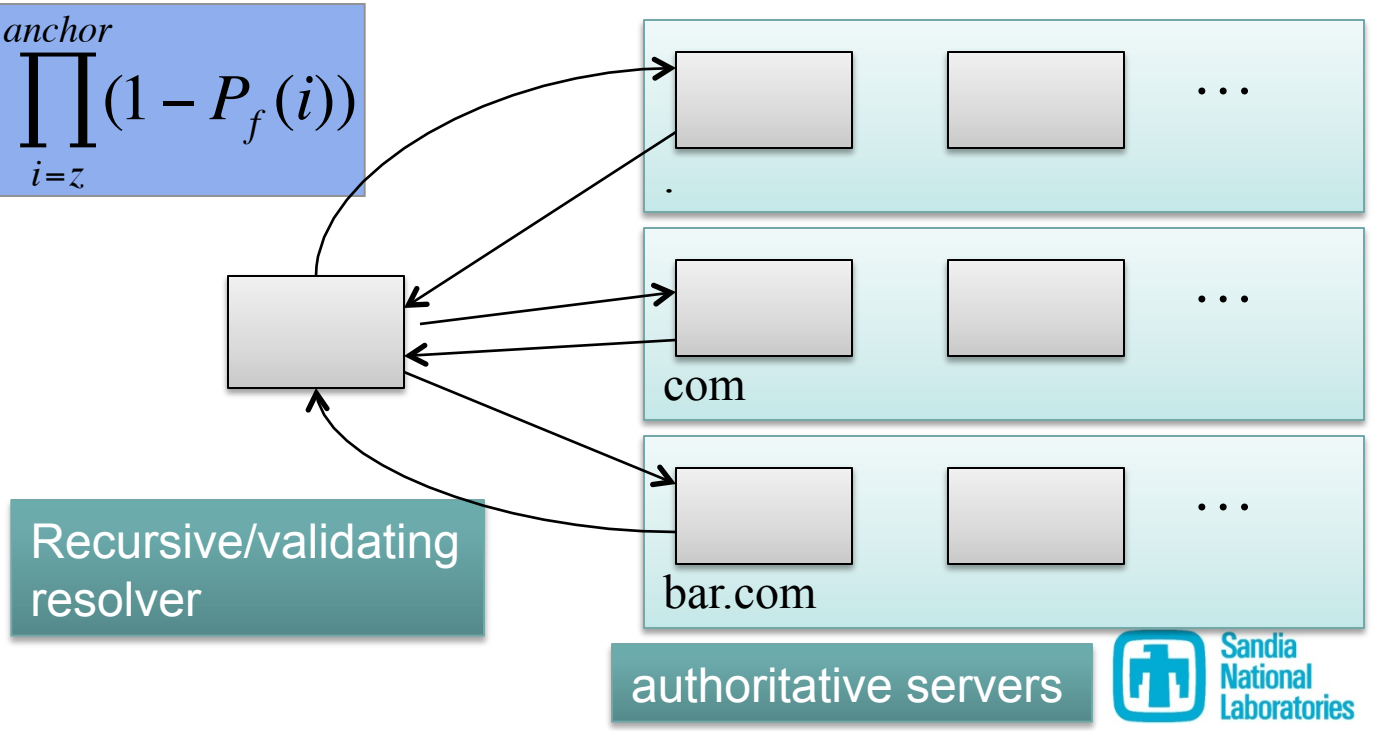
authoritative server

Sandia National Laboratories

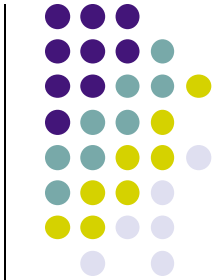
Failure potential

- Formula extends to chain of trust in ancestor zones
- Failure potential of each zone is combined independently of one another

$$P_f^r(z) = 1 - \prod_{i=z}^{anchor} (1 - P_f(i))$$



DNSSEC Deployment Survey

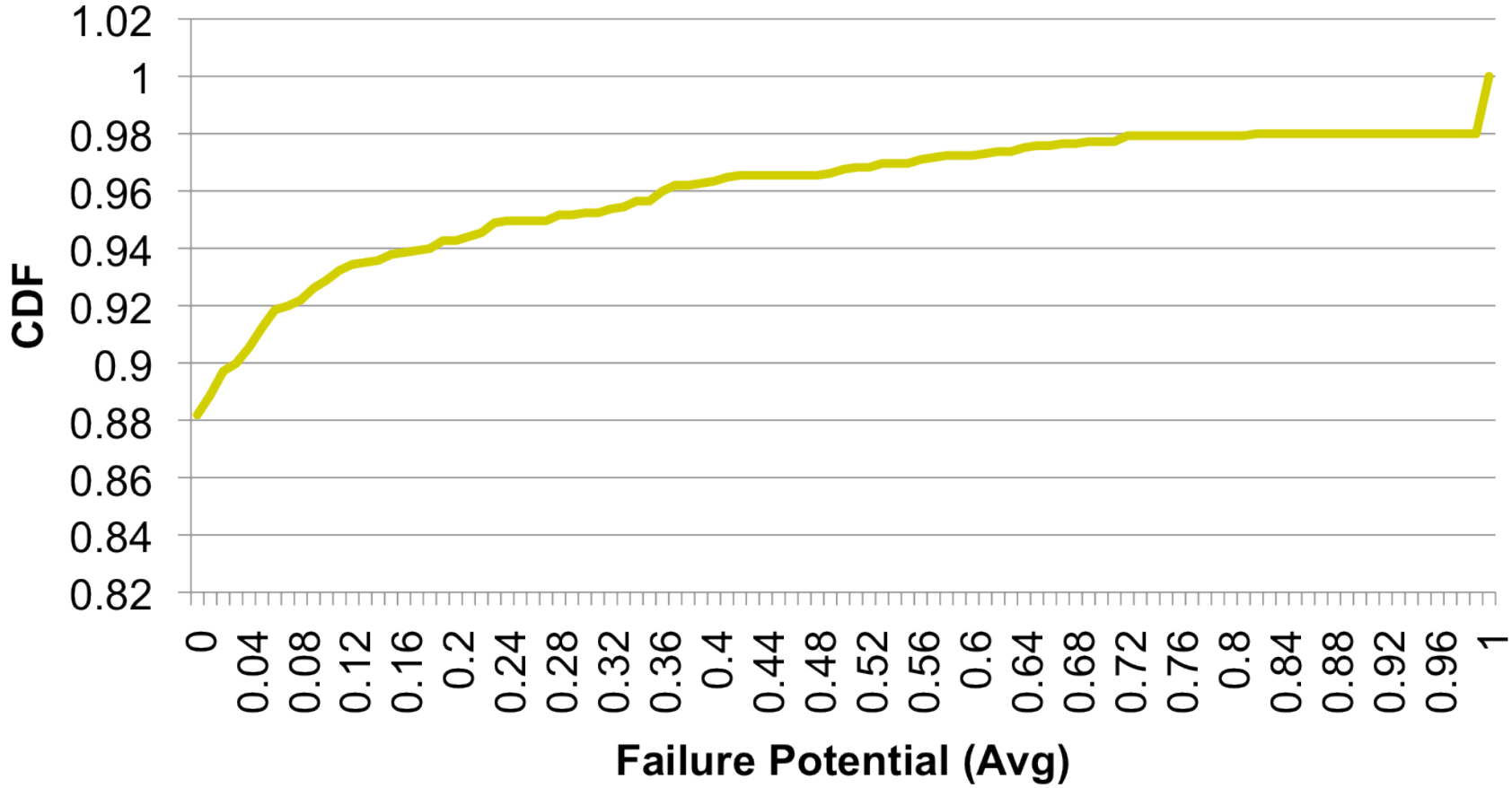


- Polled ~1500 production signed zones over a six-week period
- Recorded validation errors resulting from misconfiguration

Statistic	Value
Production signed zones polled	1,456
Total misconfigurations resulting in certain failure	194
Zone-class misconfigurations	134 (69%)
Delegation-class errors resulting in certain failure	60 (31%)
Errors (any class) caused by misconfigured ancestor zones	61 (31%)

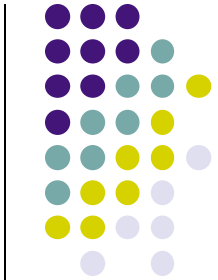
Sandia National Laboratories

Failure Potential of Zones



Sandia National Laboratories

Outline

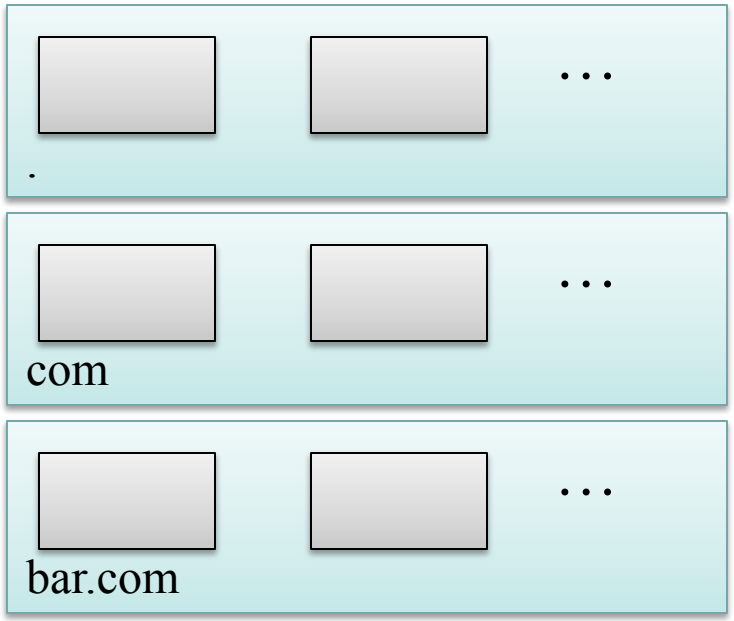


- DNSSEC availability model
- DNS complexity analysis
- Misconfiguration mitigation
- Summary

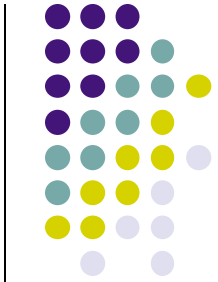
Sandia National Laboratories

Complexity analysis

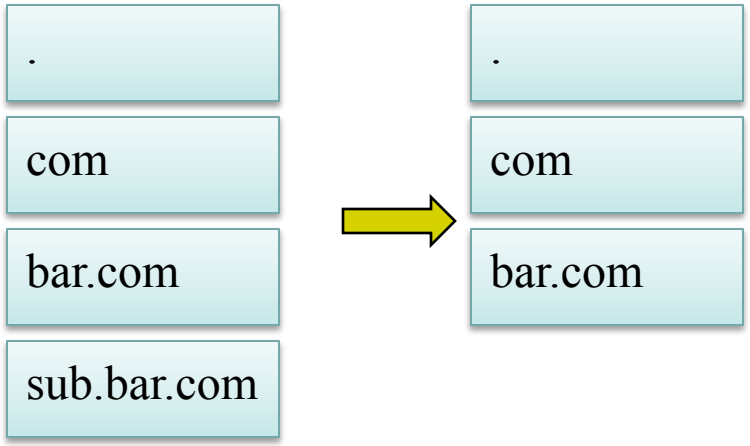
- Complexity creates potential for misconfiguration
- Hierarchical complexity:
  - Size of ancestry (zone depth)
- Administrative complexity:
  - Servers administered by distinct organizations



Hierarchical reduction potential



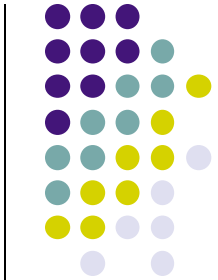
- If ancestry might reasonably be consolidated, what is the reduction?
- Ancestry reduced, but original namespace can be preserved



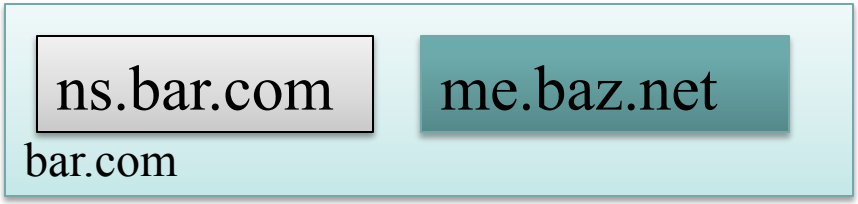
$$HRP = \frac{|orig\_zones| - |consolidated\_zones|}{|orig\_zones|}$$

$$= 0.25$$

Administrative Complexity



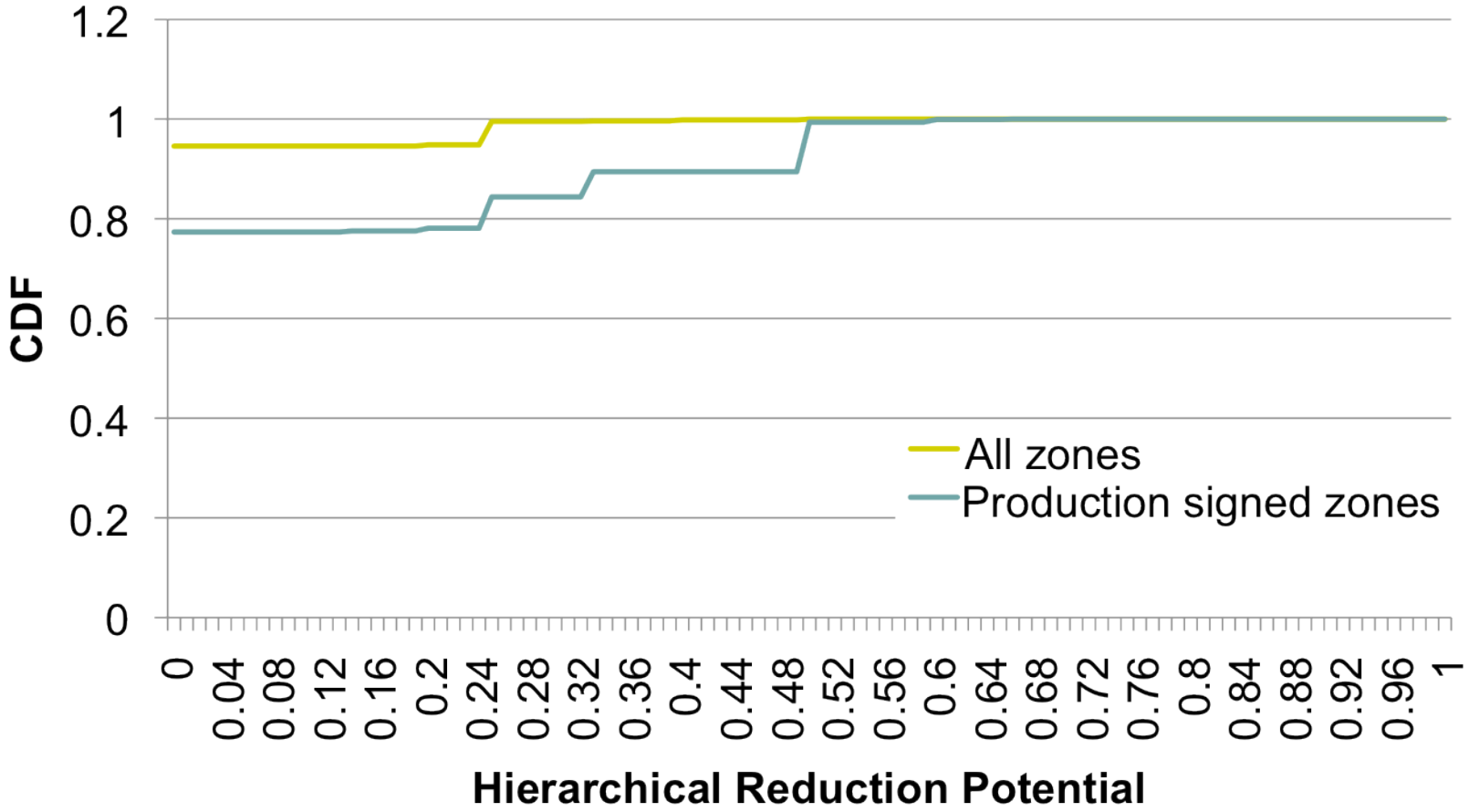
- How diverse is the set of organizations administering a zone?
- Complexity measured by random sampling (with replacement) of authoritative servers to determine the probability that two organizations are selected



$$AC = 1 - \sum_{o \in orgs} \left(\frac{|\, servers(o) \,|}{|\, all\_servers \,|} \right)^2$$

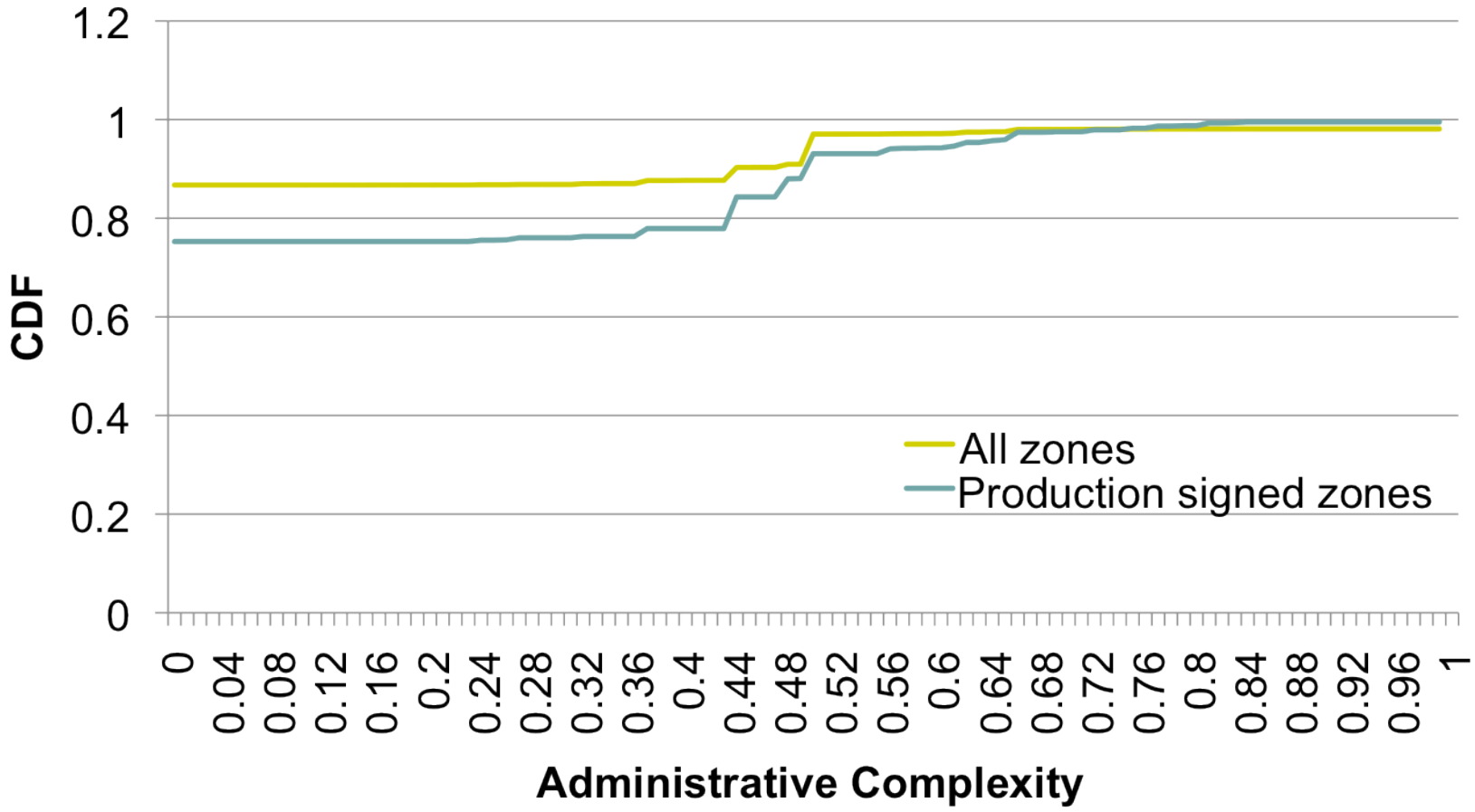
$$= 0.5$$

Hierarchical Reduction Potential



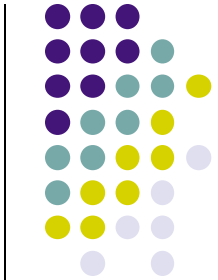
Sandia National Laboratories

Administrative complexity



Sandia National Laboratories

Outline



- DNSSEC availability model
- DNS complexity analysis
- Misconfiguration mitigation
- Summary

Sandia National Laboratories

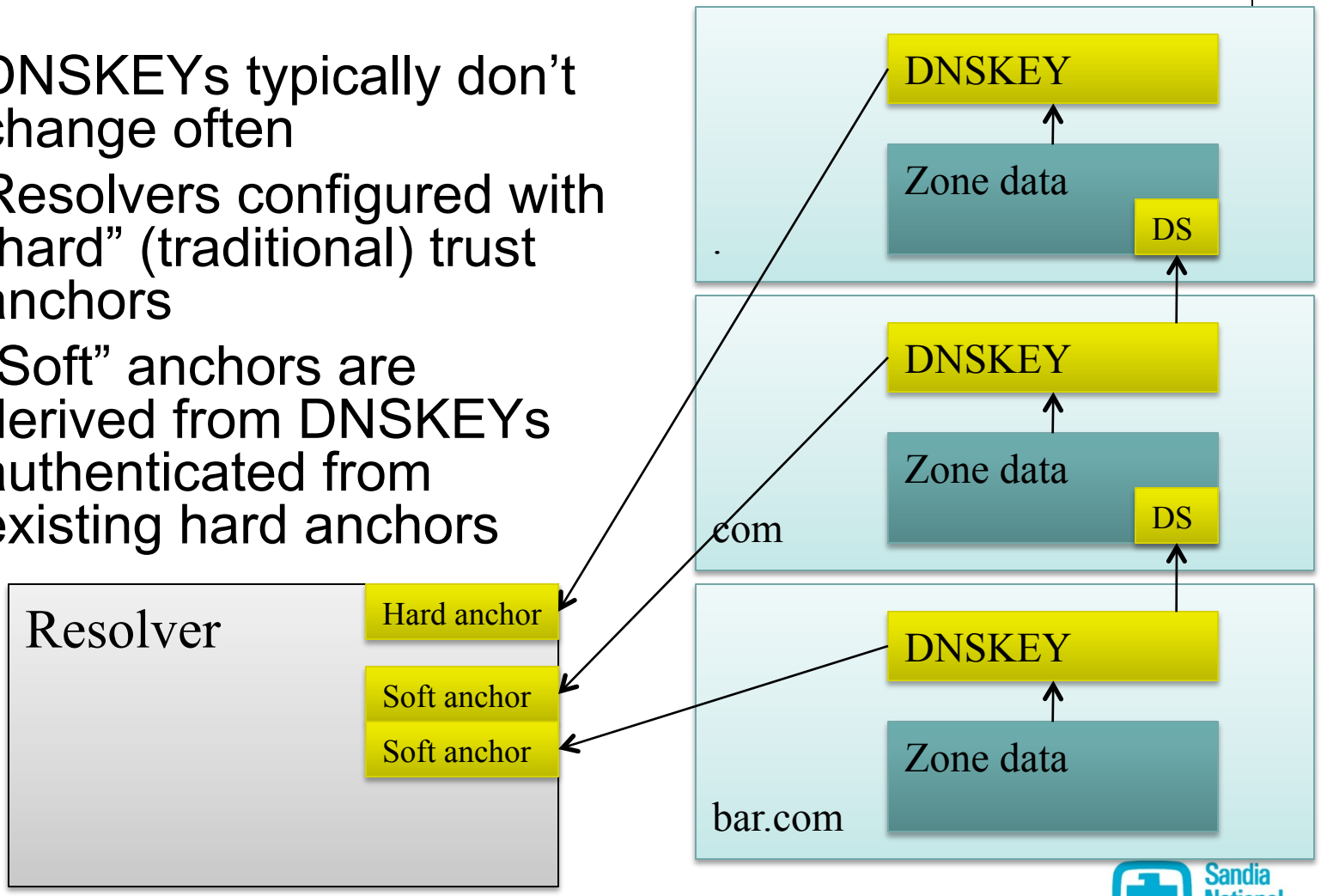
Avoiding and mitigating effects of misconfiguration

- Follow best practice operational standards (RFCs)
  - Key rollover procedures
  - Trust anchor rollover procedures
- Validation diligence
  - Resolver keeps trying alternative authoritative servers to find valid response
  - Optimality can be difficult – where is the break in the chain?
  - Implemented in BIND 9

Sandia National Laboratories

Soft anchoring

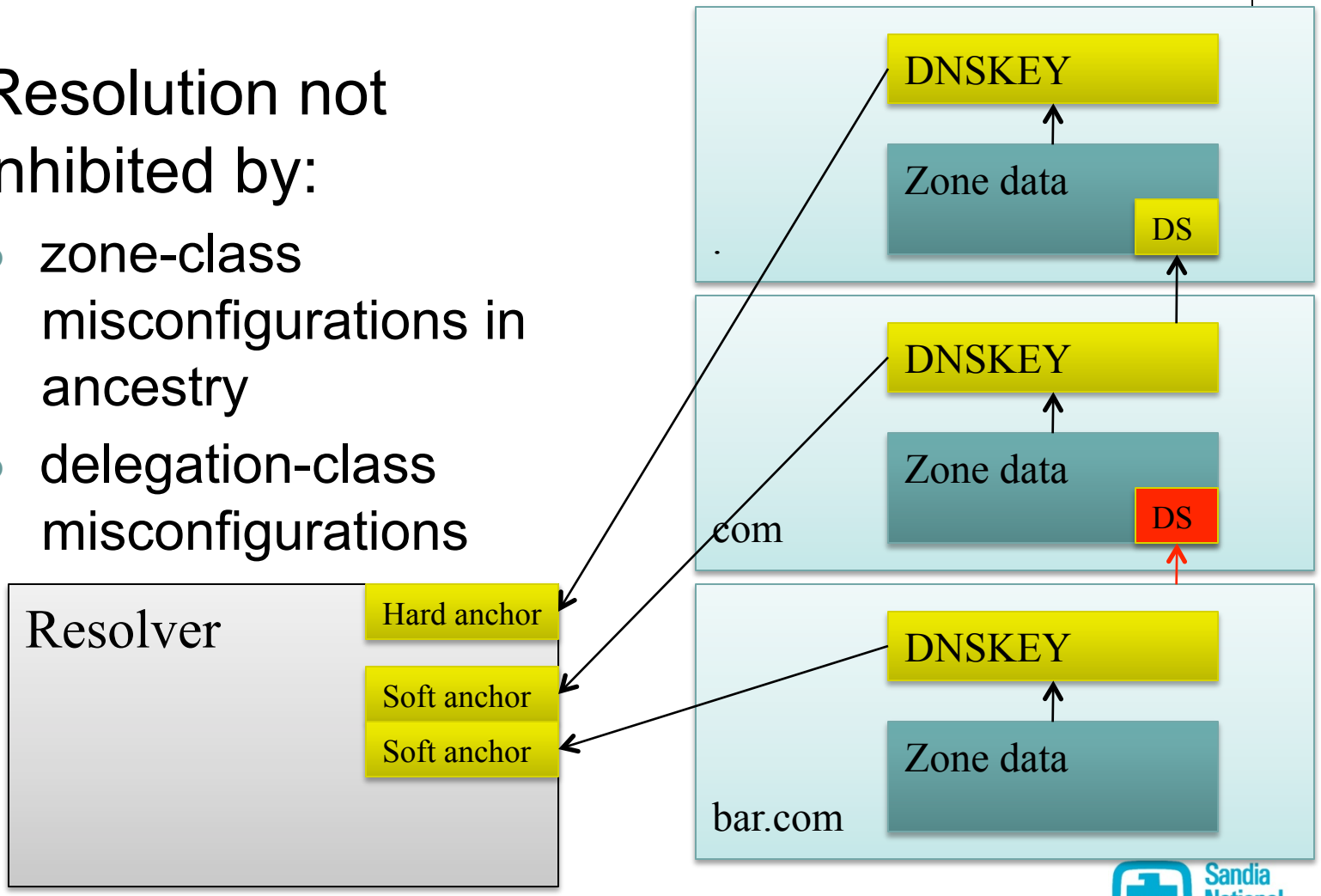
- DNSKEYs typically don't change often
- Resolvers configured with "hard" (traditional) trust anchors
- "Soft" anchors are derived from DNSKEYs authenticated from existing hard anchors



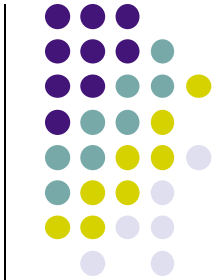
Sandia National Laboratories

Impact of soft anchoring

- Resolution not inhibited by:
  - zone-class misconfigurations in ancestry
  - delegation-class misconfigurations



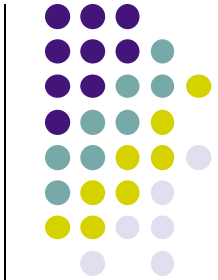
Maintaining soft anchors



- Resolvers follow procedure similar to that used for rolling hard trust anchors (RFC 5011)
- Resolver periodically polls soft anchor zone
- Soft anchor addition:
  - Newly authenticated DNSKEYs persist for “hold down” period
  - New DNSKEY seen with corresponding DS
- Soft anchor removal:
  - Delegation to soft anchor made insecure
  - DNSKEY is revoked
  - DNSKEY and its DS RR are removed

Sandia National Laboratories

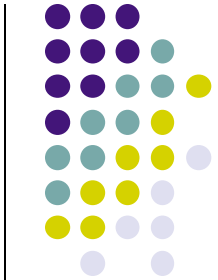
Soft anchoring limitations



- Doesn’t help when misconfigurations are at or below the bottom “link” in the chain of trust
- Resolver must have authenticated soft anchors through valid chain of trust before misconfiguration
- Scalability
  - Maintenance overhead of all trust anchors may be intense
  - Least-recently used policy may help

Sandia National Laboratories

Outline

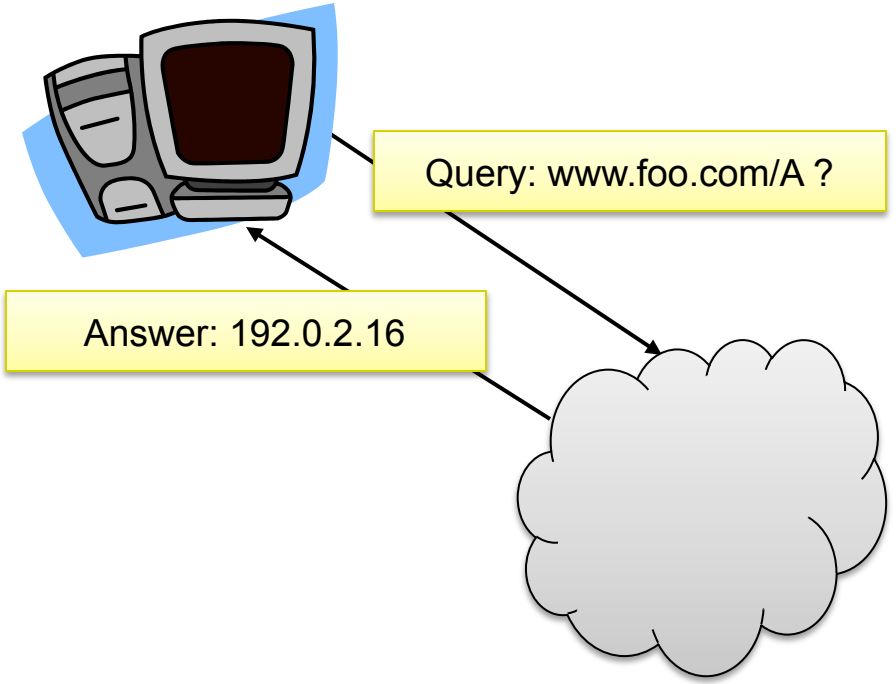


- DNSSEC availability model
- DNS complexity analysis
- Misconfiguration mitigation
- Summary

Sandia National Laboratories

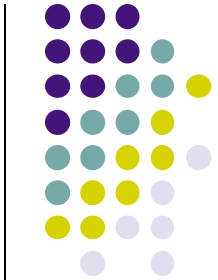
Summary

- DNS responses must be both accurate and available
- DNSSEC deployment requires careful deployment and maintenance
- Soft anchoring can mitigate effects of misconfiguration



Sandia National Laboratories

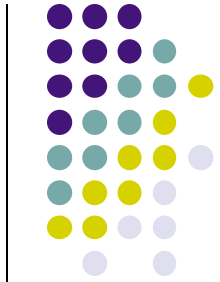
Acknowledgements



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

Sandia National Laboratories

Questions?



- ctdecci@sandia.gov

Sandia National Laboratories