Exceptional service in the national interest

Sandia National Laboratories

Qualitative DNS Measurement Perspectives

Casey Deccio

Sandia National Laboratories

ISC/CAIDA Data Collaboration Workshop

Oct 22, 2012

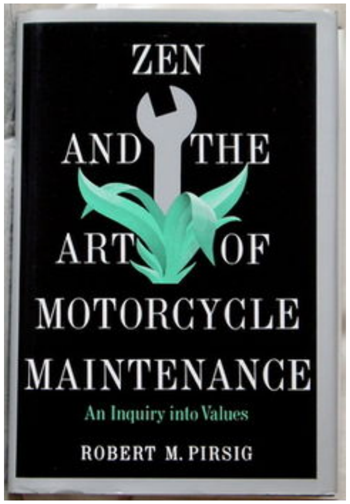
U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Qualitative Measurement?

- Baseline quantitative measurements
  - Responsiveness – is the service up?
  - Timeliness – what is its response time?
- Qualitative analysis
  - Behavioral analysis
    - Response completeness
    - Response correctness
    - Response consistency
  - Comprehensive analysis
    - Consideration of all dependent names
    - Consideration of all dependent servers
  - Temporal analysis
    - Consideration of caching behavior
    - Consideration of historical behavior
    - Timely identification and notification of problems



http://en.wikipedia.org/wiki/Zen_and_the_Art_of_Motorcycle_Maintenance

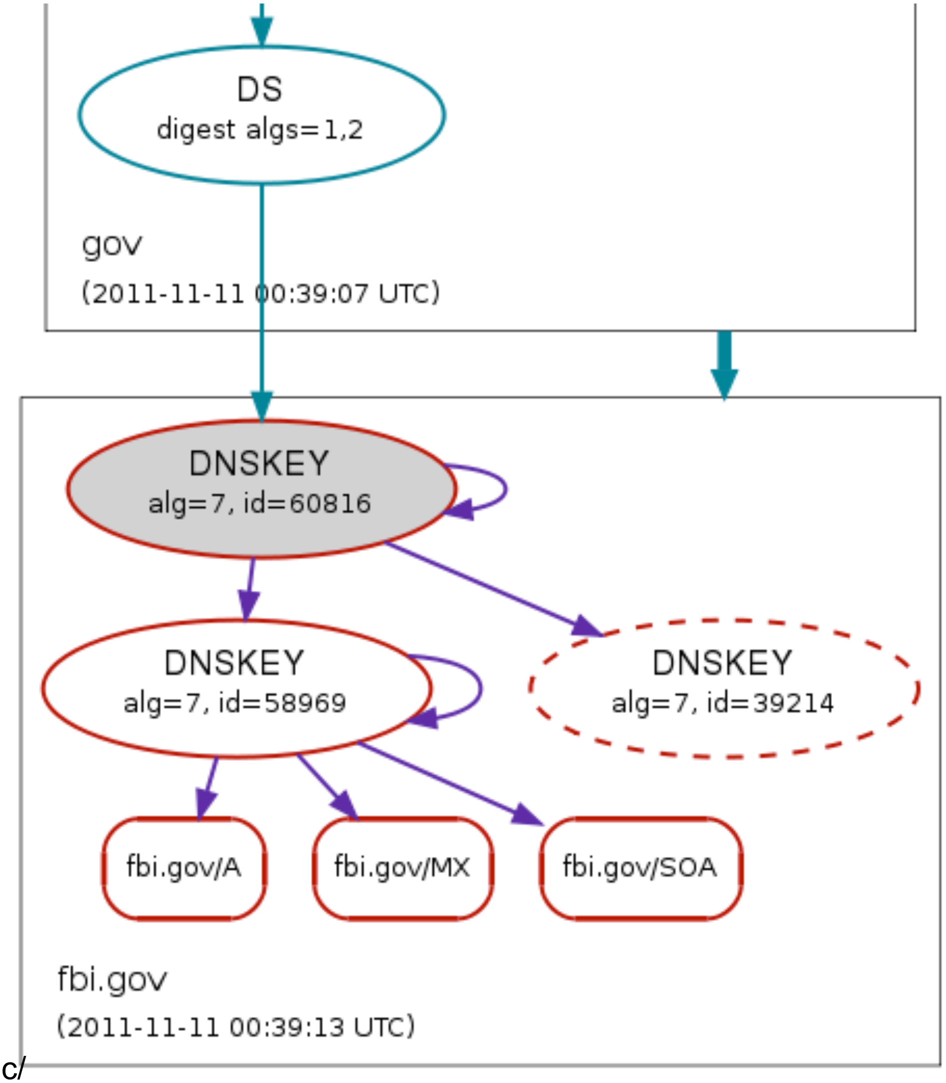
Why Qualitative Analysis?

- DNSSEC brings new challenges to name resolution – in addition to its security benefits
  - More interactive and critical relationship between parent and child
    - DS/DNSKEY consistency
  - Temporal challenges
    - Expiring signatures
    - Key rollovers
    - Caching behaviors considered for maintenance
- Standards and implementations are relatively new

Photo By Diego Torres Silvestre from Sao Paulo, Brazil ([2005] Rusty Padlock & Fence) [CC-BY-2.0 (http://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons

Example: fbi.gov

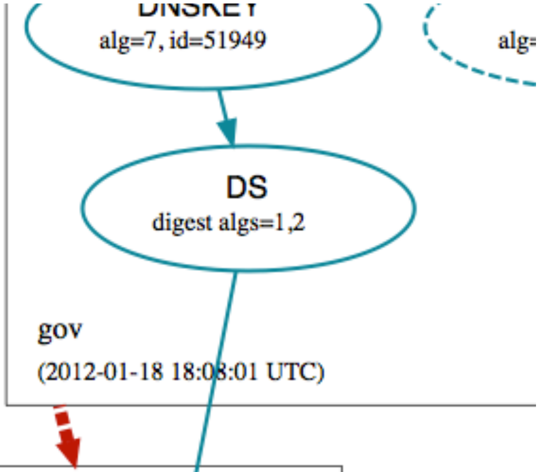
Expired RRSIG

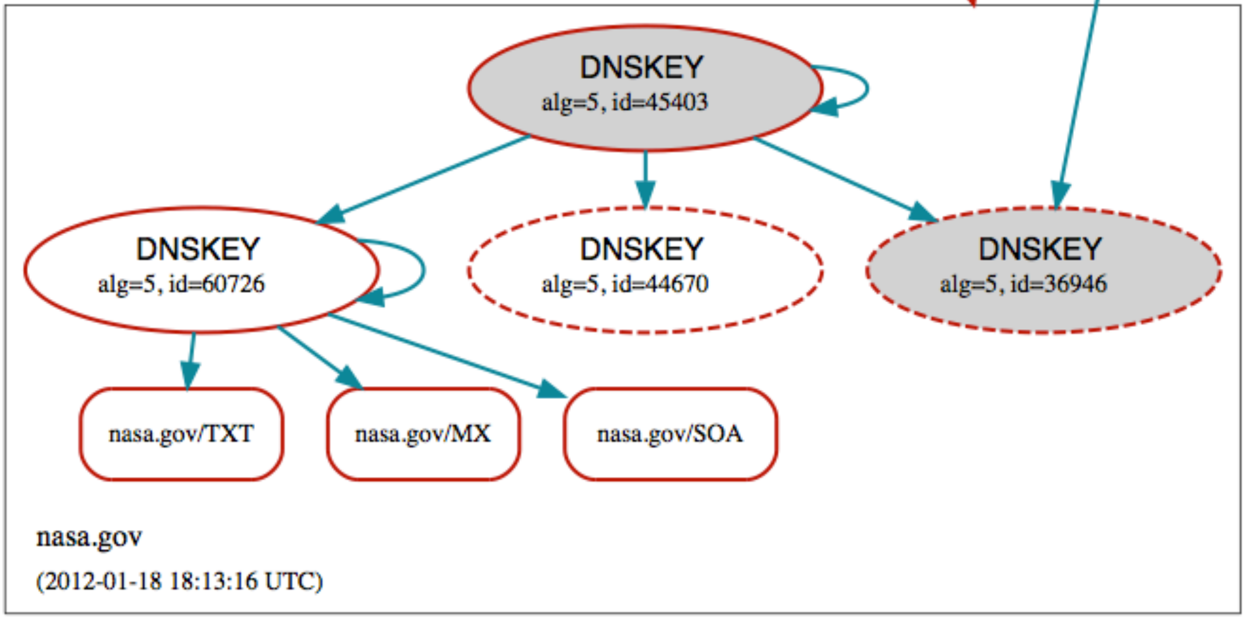


http://dnsviz.net/d/nasa.gov/TxcLvQ/dnssec/

Example: nasa.gov

DS mismatch caused by bad KSK rollover

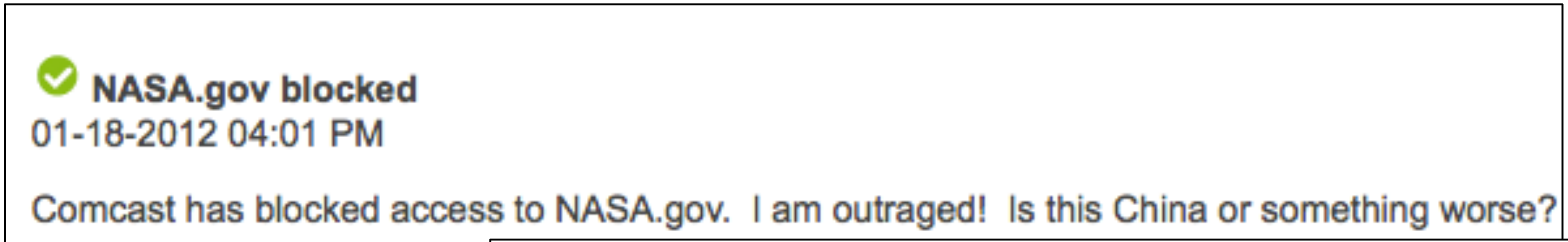




http://dnsviz.net/d/nasa.gov/TxcLvQ/dnssec/

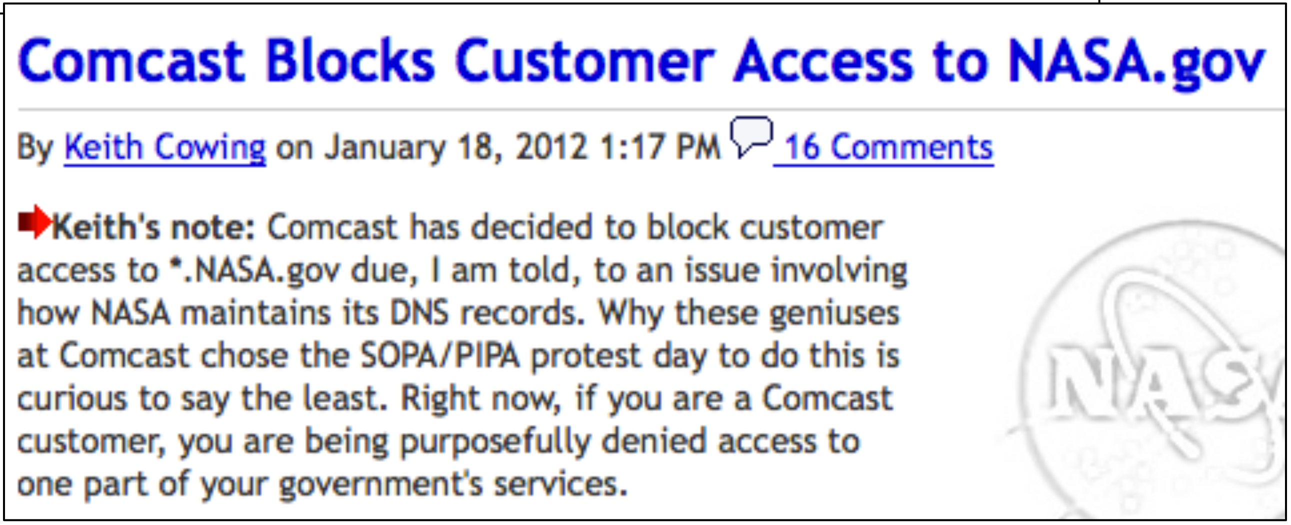
nasa.gov Aftermath

nasa.gov incident came just one week after Comcast enabled DNSSEC validation for residential users



✓ **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

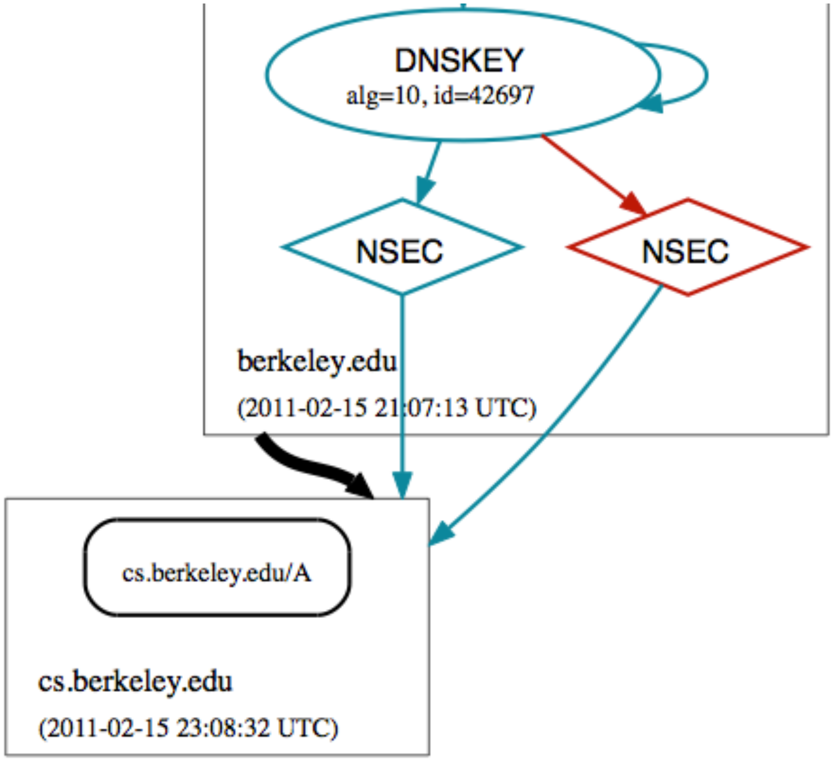
Why Comprehensive Analysis?

- Behavioral Consistency
  - Different implementations on servers
  - Different versions of implementations
  - Different versions of zone data
- Some resolver implementations retry when they experience validation failure – two-edged sword
  - Alleviates user pain when validation fails due to problems with proper subset of servers
  - Masks potential problems

By Mark and Allegra Jaroski-Biava from Lausanne, Switzerland (Apples, Pears, Oranges) [CC-BY-SA-2.0 (http://creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons

Example: berkeley.edu

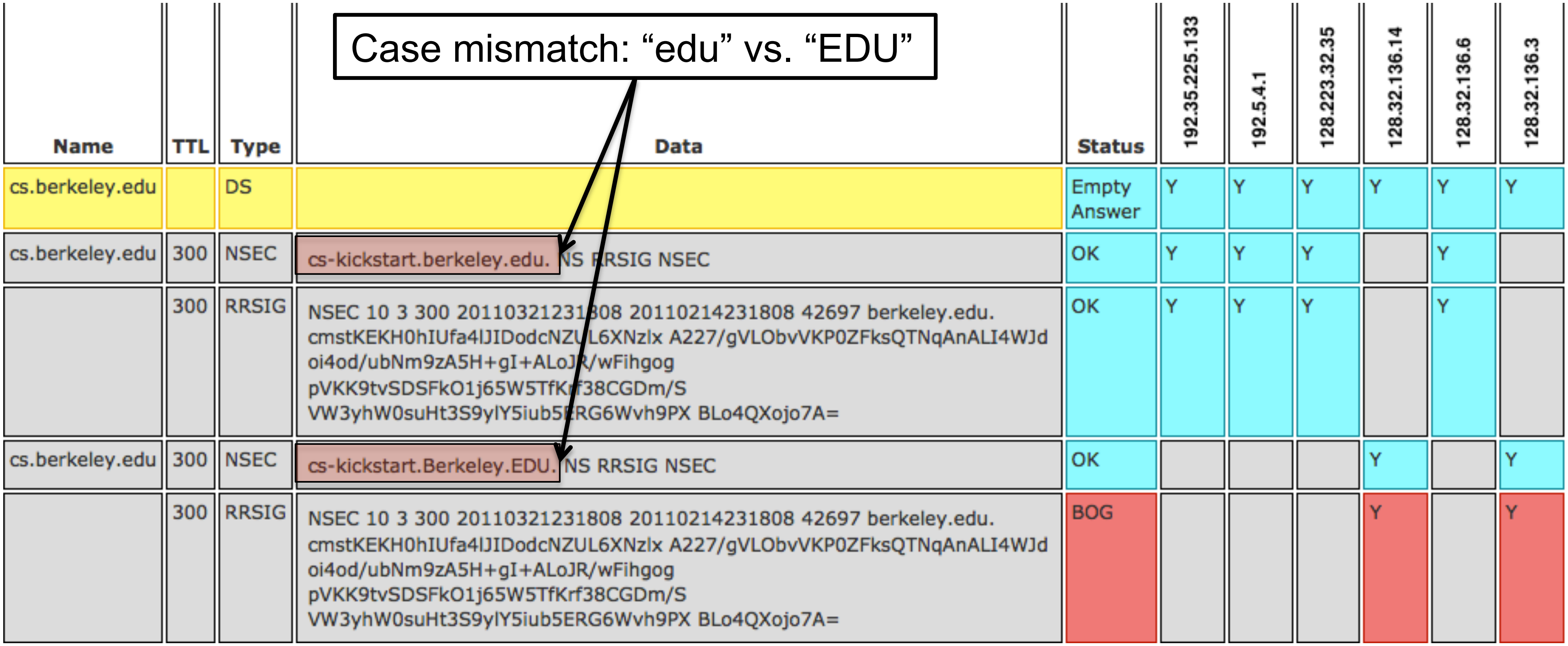
- Feb 2011 – Sandia experienced validation errors for unsigned zone cs.berkeley.edu
- DNSViz showed two NSEC RRs returned, one with bogus RRSIG



http://dnsviz.net/d/cs.berkeley.edu/TVsHcQ/dnssec/

berkeley.edu – Further Analysis

- Some servers serving different NSEC with same RRSIG
- Case of NSEC was not preserved during transfer after upgrade
- Fortunately, servers upgraded incrementally
- Impact: Jan 2011 – .br servers suffered same bug on half of their authoritative servers

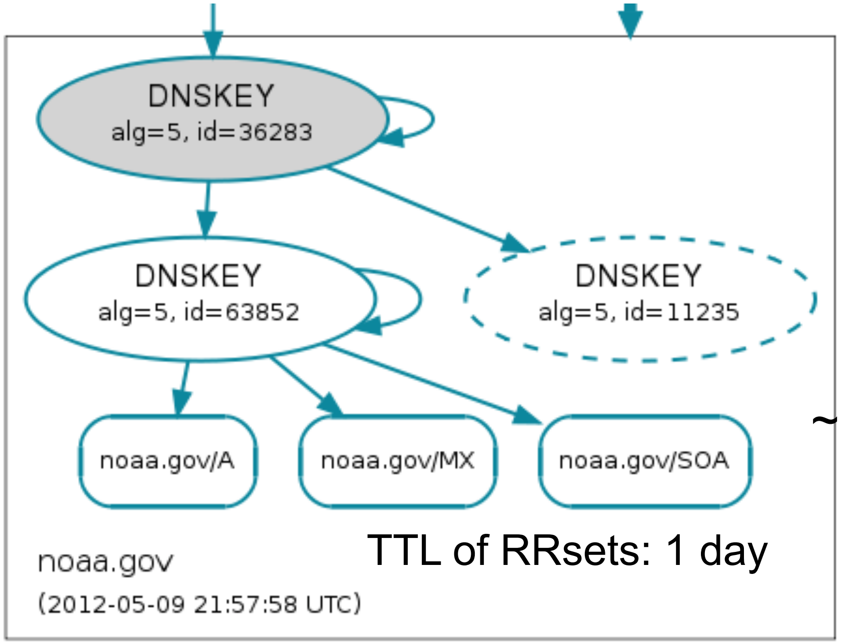


Case mismatch: "edu" vs. "EDU"

Name	TTL	Type	Data	Status	192.35.225.133	192.5.4.1	128.223.32.35	128.32.136.14	128.32.136.6	128.32.136.3
cs.berkeley.edu		DS		Empty Answer	Y	Y	Y	Y	Y	Y
cs.berkeley.edu	300	NSEC	cs-kickstart.berkeley.edu. NS RRSIG NSEC	OK	Y	Y	Y		Y	
	300	RRSIG	NSEC 10 3 300 20110321231808 20110214231808 42697 berkeley.edu. cmstKEKH0hIUfa4lJIDodcNZUL6XNzlx A227/gVLObvVKP0ZFksQTNqAnALI4WJd oi4od/ubNm9zA5H+gI+ALoJR/wFihgog pVKK9tvSDSFkO1j65W5TfKrf38CGDm/S VW3yhW0suHt3S9ylY5iub5ERG6Wvh9PX BLo4QXojo7A=	OK	Y	Y	Y		Y	
cs.berkeley.edu	300	NSEC	cs-kickstart.Berkeley.EDU. NS RRSIG NSEC	OK				Y		Y
	300	RRSIG	NSEC 10 3 300 20110321231808 20110214231808 42697 berkeley.edu. cmstKEKH0hIUfa4lJIDodcNZUL6XNzlx A227/gVLObvVKP0ZFksQTNqAnALI4WJd oi4od/ubNm9zA5H+gI+ALoJR/wFihgog pVKK9tvSDSFkO1j65W5TfKrf38CGDm/S VW3yhW0suHt3S9ylY5iub5ERG6Wvh9PX BLo4QXojo7A=	BOG				Y		Y

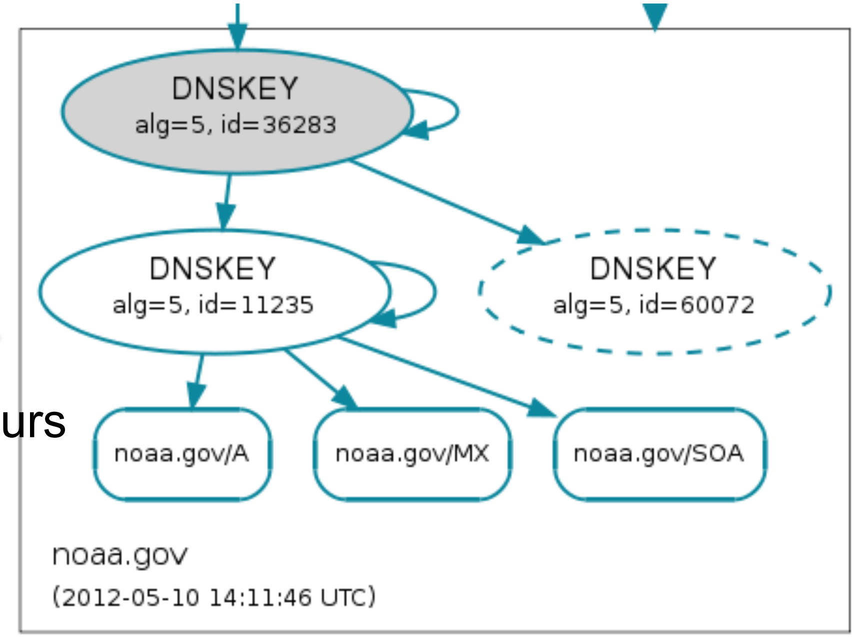
Why Temporal Analysis?

- Snapshot of behaviors exhibited by authoritative servers at a given time is insufficient
- Timing is critical because of caching behavior



TTL of RRsets: 1 day

~16 hours



http://dnsviz.net/d/noaa.gov/T6roZw/dnssec/

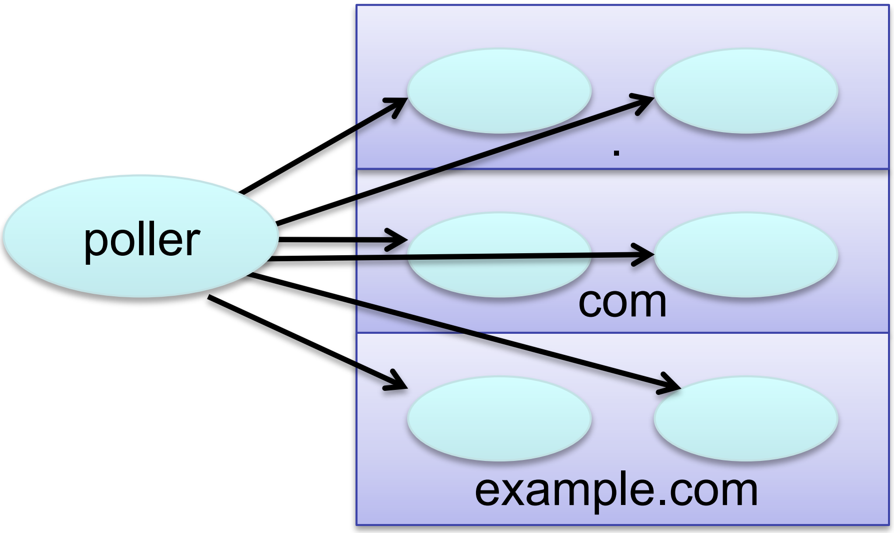
http://dnsviz.net/d/noaa.gov/T6vMow/dnssec/

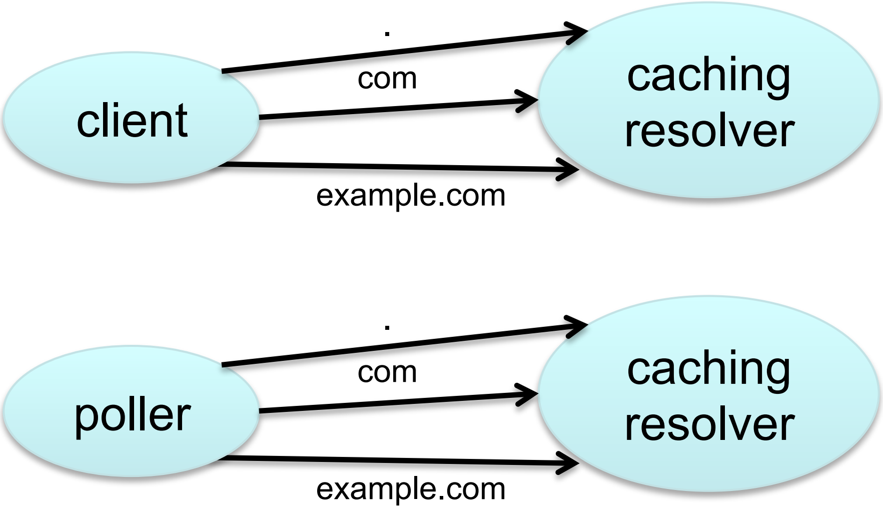
Active DNS Measurement Perspectives

- From single vantage point, using delegation chain
  - Comprehensive analysis across authoritative servers
  - Follows server and name dependencies
  - Provides snapshot of behavior at a given time
  - Periodic polling
  - Currently implemented by DNSViz (http://dnsviz.net/)

- From single vantage point, targeted
  - Analysis from perspective of caching resolver, initiated by poller or client (e.g., Web browser)
  - Cache inspection
  - On-demand
  - Work-in-progress for DNSViz

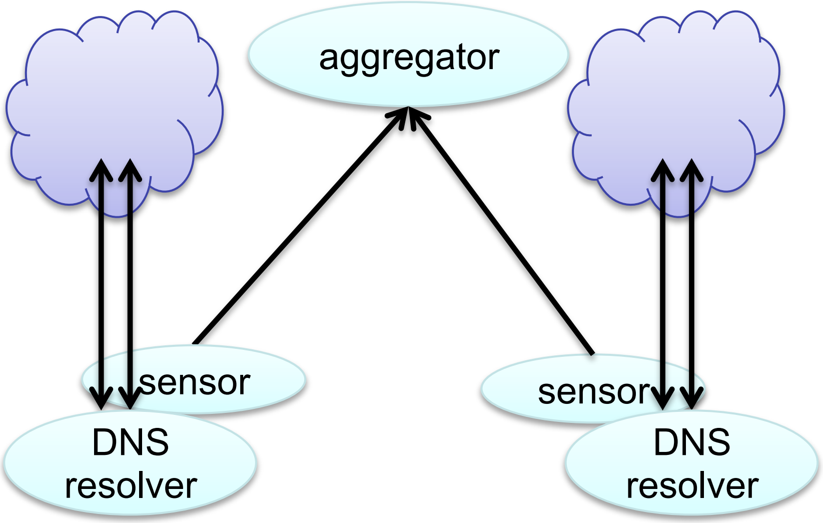
.



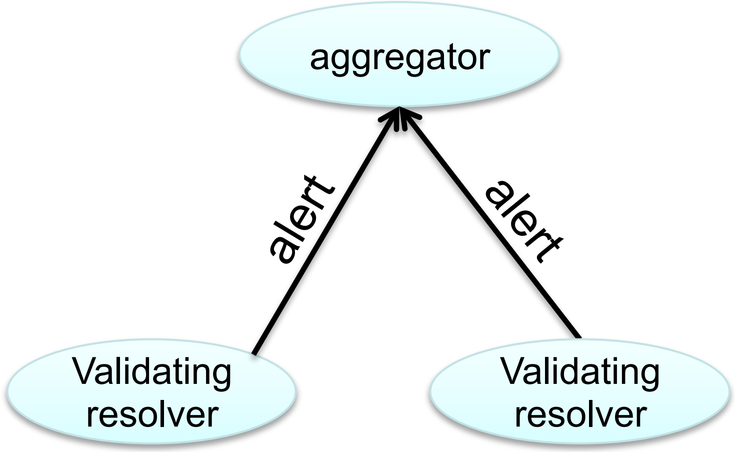


Passive DNS Measurement Perspectives

- Passive observation, traffic replication
  - Implemented by SIE.
  - Storing DNSSEC context allows real-time detection of misconfiguration and discrepancy.



- Passive observation, detection and alerts
  - Sensors or validating resolvers detect problems at resolver in real-time and notify poller for comprehensive analysis.



Measurement Scoreboard

Baseline quantitative measurements		
Responsiveness – is the service up?	Active	
Timeliness – what is its response time?	Active	
Qualitative analysis		
Behavioral analysis		
Response completeness	Active	
Response correctness	Active	
Response consistency	Active	
Comprehensive analysis		
Consideration of all dependent names	Active	
Consideration of all dependent servers	Active	
Temporal analysis		
Consideration of caching behavior	Active – partial	Passive
Consideration of historical behavior	Active – partial	Passive
Timely identification and notification of problems		Passive

Conclusions

- Qualitative measurement will aid DNSSEC deployment by helping identify and troubleshoot validation failures.
- Active measurement supplemented by passive measurement can provide rapid detection of DNSSEC misconfiguration, breaches, and other anomalies, appropriately classify their impact, and offer remedies.