Qualitative DNS Measurement Perspectives

Casey Deccio
Sandia National Laboratories
ISC/CAIDA Data Collaboration Workshop
Oct 22, 2012
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

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
Example: fbi.gov

Expired RRSIG

DS
digest algs=1,2

gov
(2011-11-11 00:39:07 UTC)

DNSKEY
alg=7, id=60816

DNSKEY
alg=7, id=58969

DNSKEY
alg=7, id=39214

fbi.gov/A
fbi.gov/MX
fbi.gov/SOA

fbi.gov
(2011-11-11 00:39:13 UTC)

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

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

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.
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”

<table>
<thead>
<tr>
<th>Name</th>
<th>TTL</th>
<th>Type</th>
<th>Data</th>
<th>Status</th>
<th>192.35.225.133</th>
<th>192.5.4.1</th>
<th>128.223.32.35</th>
<th>128.32.136.14</th>
<th>128.32.136.6</th>
<th>128.32.136.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>cs.berkeley.edu</td>
<td>300</td>
<td>NSEC</td>
<td>cs-kickstart.berkeley.edu, NS RRSIG NSEC</td>
<td>Empty Ans</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>cs.berkeley.edu</td>
<td>300</td>
<td>NSEC</td>
<td>cs-kickstart.Berkeley.EDU, NS RRSIG NSEC</td>
<td>OK</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>cs.berkeley.edu</td>
<td>300</td>
<td>RRSIG</td>
<td>NSEC 10 3 300 20110321321308 20110214231808 42697 berkeley.edu. cmstKEKH0thUfa4UJDodcNZUL6XNzix A227/gVLObwVKP0ZFsQTNgAnAL14Wjd ol4oddubNm9zASH+gI+AloJr/wfihgog pVKK9tvDSDFk0j655STKf38CGDm/S VW3yhW0suHt3S9yIY5Iub51ERG6Wvh9PX BLo4QXojo7A=</td>
<td>OK</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>cs.berkeley.edu</td>
<td>300</td>
<td>RRSIG</td>
<td>NSEC 10 3 300 20110321321308 20110214231808 42697 berkeley.edu. cmstKEKH0thUfa4UJDodcNZUL6XNzix A227/gVLObwVKP0ZFsQTNgAnAL14Wjd ol4oddubNm9zASH+gI+AloJr/wfihgog pVKK9tvDSDFk0j655STKf38CGDm/S VW3yhW0suHt3S9yIY5Iub51ERG6Wvh9PX BLo4QXojo7A=</td>
<td>BOG</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

[Image of the table with data]
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

noaa.gov
(2012-05-09 21:57:58 UTC)

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

noaa.gov
(2012-05-10 14:11:46 UTC)

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?
  - 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
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.