Why Monitoring is Important

• Distributed systems have different problems when viewed from different vantage points
  – It is important for zone admins to know their data is being served properly to resolvers in different places
  – It is important for resolvers to know if any availability problems they see are local or global
• Monitoring answers these immediate questions, and can generate aggregate and historical information
• In other words, monitoring can help the DNSSEC rollout
Outline

• How DNSSEC works
• What can go wrong
• What SecSpider can help with
• Summary
DNSSEC

- DNSSEC provides *origin authenticity, data integrity, and secure denial of existence* by using public-key cryptography
- **Origin authenticity:**
  - Resolvers can verify that data has originated from authoritative sources.
- **Data integrity**
  - Can also verify that responses are not modified in-flight
- **Secure denial of existence**
  - When there is no data for a query, authoritative servers can provide a response that proves no data exists
How DNSSEC Works

• Each DNSSEC zone creates one or more pairs of public/private key(s)
  – Public portion put in DNSSEC record type DNSKEY
• Zones sign all RRsets with private key(s) and resolvers use DNSKEY(s) to verify RRsets
  – Each RRset has a signature attached to it: RRSIG
• So, if a resolver has a zone’s DNSKEY(s) it can verify that RRsets are intact by verifying their RRSIGs
Signing Example

Using a zone’s key on a standard RRset (the NS)

Signature (RRSIG) will only verify with the DNSKEY if *no* data was modified.
Getting the Keys

• Until a resolver gets the DNSKEY(s) for a zone, data can be spoofed
• How can a resolver know that the DNSKEY(s) themselves are not being spoofed?
• DNSSEC zones securely delegate from parents to children
• Zones that have no secure parents are called trust anchors
• When a zone is a trust anchor the zones that it delegates to form an island of security
What Can Go Wrong

• Getting the keys for a zone should be simple
  – Reality: cache problems, PMTU problems, etc

• Verifying data seems as simple as following the delegation hierarchy
  – Reality: the hierarchy is underdeveloped (for now)

• Getting valid data should be as easy as verifying RSA signatures
  – Reality: signatures on data do not prove that the data is valid
Specifically…

• In this talk we pick one of these: availability
  – We discuss all 3 of these issues in our 2008 IMC paper “Quantifying the Operational Status of the DNSSEC Deployment”

• Availability is important because getting DNSSEC keys is not always as easy as one would hope
  – And clearly this is a precondition for verifying RRSIGs
SecSpider

SecSpider the DNSSEC Monitoring Project

Check out our blog

To add a zone for monitoring, please submit below:

Zone to add:  Submit

Vouch for or against a zone's production status

Search for zone:

Zone: secspider.cs.ucla.edu  Submit

http://secspider.cs.ucla.edu/
What We Track

• We currently try to track as many DNSSEC zones as we can find
  – We take user submissions, crawl various sources, do NSEC walking, etc.
  – We have been monitoring since 2005
• We track all zones in our corpus from a set of distributed pollers
• From these vantage points we can observe many facets of DNSSEC zones
Distributed Polling

- We use distributed pollers to measure consistency (or inconsistencies)
- For example: DNSKEY RRsets spoofing at one poller will not fool others, and discrepancies can be seen
- In addition, network issues can cause some vantage points to be unable (or less able) to access DNSSEC information
  - We call this *availability dispersion*
Availability Dispersion

- SecSpider does PMTU walking to each zone whenever there is trouble retrieving DNSKEYs.
- Some polling locations have serious PMTU problems that disrupt availability.
Whose Problem is it?

• Without a monitoring system, how can zone administrators *know* there is a problem?
  – With SecSpider, zone admins can see issues and correct them

• How can resolvers know *why* they are having a problem
  – With SecSpider, people can (sometimes) see if their problems are local or global
How to Use SecSpider

- From our front page, submit your zone
- After the next polling cycle, you will see your zone on our web site
- For DNSKEYs (for example) check their consistency
Zone secspider.cs.ucla.edu.

Zone status as of: Thu Oct 9 02:27:30 2008 UTC
Seen by 100% of active pollers.

Reason for Monitoring this Zone: User Request
Parent Zone: cs.ucla.edu.

Data files for:
DS records (signed)
DNSKEY records (signed)

Trust Anchor:

<table>
<thead>
<tr>
<th>Consistency</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>secspider.cs.ucla.edu</td>
</tr>
</tbody>
</table>

Summary:

<table>
<thead>
<tr>
<th>Property</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDNS0 capable</td>
<td>Yes</td>
</tr>
<tr>
<td>DNSSEC deployed</td>
<td>Yes</td>
</tr>
<tr>
<td>Production zone</td>
<td>Yes</td>
</tr>
<tr>
<td>User Production</td>
<td>N/A</td>
</tr>
</tbody>
</table>

DS Records from parent zone:
Consistency: 100%

<table>
<thead>
<tr>
<th>Key Tag</th>
<th>Digest</th>
<th>Verified (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
</tr>
</tbody>
</table>

DNSKEYs:
Consistency: 100%

<table>
<thead>
<tr>
<th>Key Tag</th>
<th>Key Type</th>
<th>Algorithm</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>secspider.cs.ucla.edu.44736</td>
<td>ZSK</td>
<td>RSASHA1</td>
<td>AwEAAwZPD1Ns1HxJujgZ8vAzBogwT6L9n5VzycR29hGZkR8yYLCbczz14V/Pe094RCFqYMhJDhlyyg2Hk</td>
</tr>
<tr>
<td>secspider.cs.ucla.edu.59317</td>
<td>KSK</td>
<td>RSASHA1</td>
<td>AwEAAwWjhb000eqgyBUUq/ppwiNi3zXB37h12S4Gy1f0txUFUqY7JX6z2Bvu4W92n37/Tu/i8US6gCQd4nXfrFus5d6tNgMX7Q5262HZnJz2JL3ENHUC0nHA2N2TVpe2R3291cs</td>
</tr>
</tbody>
</table>

RRSIGs

<table>
<thead>
<tr>
<th>Key Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>secspider.cs.ucla.edu.44736</td>
</tr>
<tr>
<td>secspider.cs.ucla.edu.59317</td>
</tr>
</tbody>
</table>
Secure Delegation Hierarchy
Summary

- The DNSSEC rollout has gotten a shot in the arm, but open issues remain.
- A distributed monitoring system can help and is here today.
- We can track zones and highlight configuration and availability problems to aid early adopters.
- But also, distributed monitoring is a general tool whose utility is not limited to the early stages of the rollout.
  - As new problems arise, monitoring will allow us to see them and address them.
Thank you