SecSpider: Distributed DNSSEC Monitoring

Eric Osterweil

Michael Ryan

Dan Massey

Lixia Zhang

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

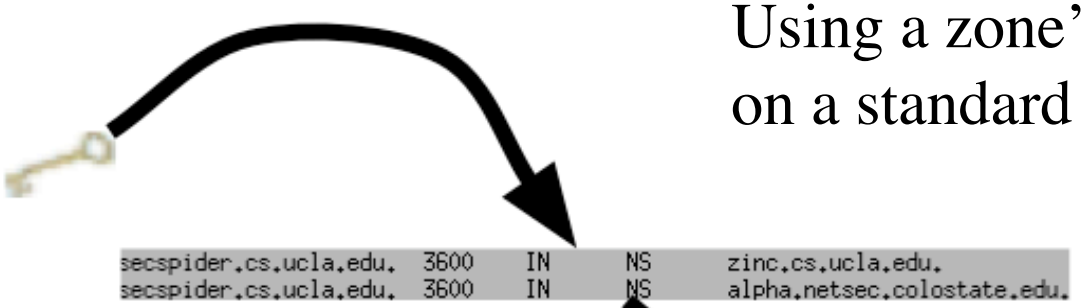
- DNSSEC provides *origin authenticity, data integrity,* and *secure denial of existence* by using public-key cryptography
- Origin authenticity:
  - Resolvers can verify that data has originated from authoritative sources.
- Data integrity
  - Can also verify that responses are not modified in-flight
- 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)



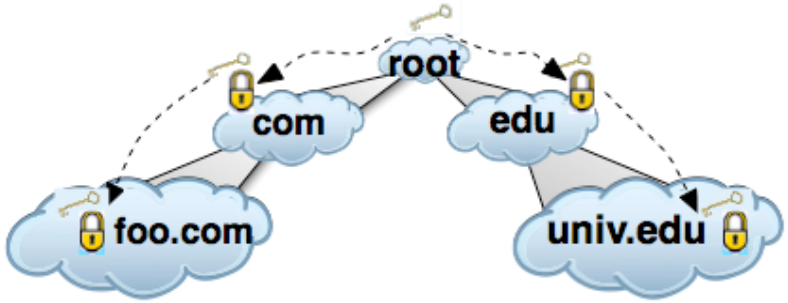
```
secspider.cs.ucla.edu.  3600    IN      NS      zinc.cs.ucla.edu.
secspider.cs.ucla.edu.  3600    IN      NS      alpha.netsec.colostate.edu.
```

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

```
secspider.cs.ucla.edu.  3600 IN NS alpha.netsec.colostate.edu.
secspider.cs.ucla.edu.  3600 IN NS zinc.cs.ucla.edu.
secspider.cs.ucla.edu.  3600 IN RRSIG NS 5 4 3600 20080324024800 (
                                20080322024800 44736 secspider.cs.ucla.edu.
                                E4msde1nzVlfGvwDo2X6jLU5d9Xrk37lrYRCZN6yq5ad
                                mABa3B3KgKl13u2VBXDujJZucHSwPQMBy+JOmotZOggf
                                SgQWUYm86v8G7ABHHcI+YFD3z3eqSoAoBAE5ysafop1u
                                g7tw1J4xd/IADIVeu1HnVIKRSycILXzvCwcaDWwAd610
                                9oJUBSMgWZjGzYeJO9Rz0oUUqIqtn9PgVOzdTm+WnRC3
                                LEz50fdoP743QvPhe7RrF9w1KA3MOptTiQA++W8GgO85
                                NhbJ7MD99nEYaEv3+GuDCTkCy5ZOWoI/2Bcjq1NGBDLo
                                71lo6udu72i1tpyRfTEEQUirpInlZ9+IMw== )
```

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*

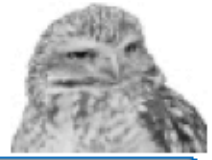
What Can Go Wrong

- 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 discus all 3 of these issues in our 2008 IMC paper "Quantifying the Operational Status of the DNSSEC Deployment" http://irl.cs.ucla.edu/papers/imc71-osterweil.pdf
- 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

Home | Blog | About | FAQ | Documentation | Usage | Pollers | GPG Key | IRL

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

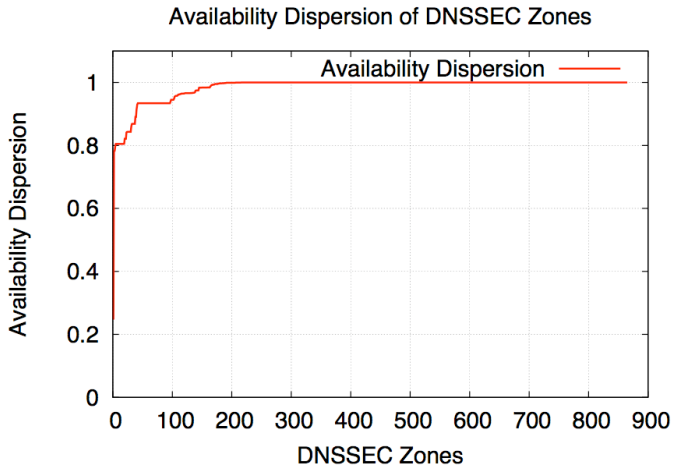
Distributed Polling

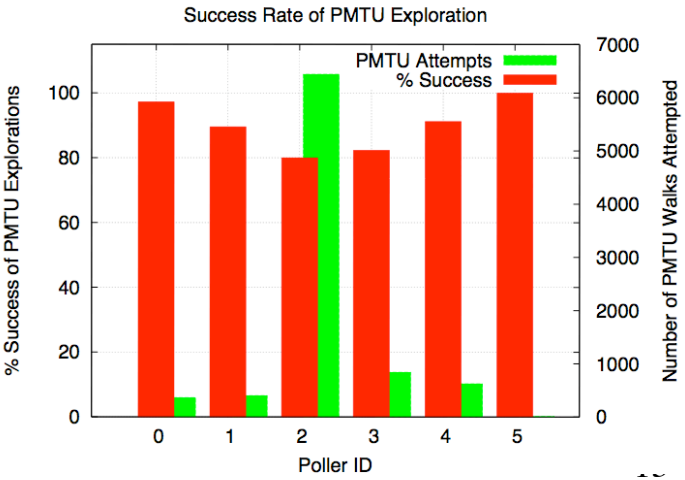
- We use distributed pollers to measure consistency (or inconsistencies)
- For example: DNSKEY RRsets spoofing at one poller will not fool others, and discrepencies can be seen

- 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

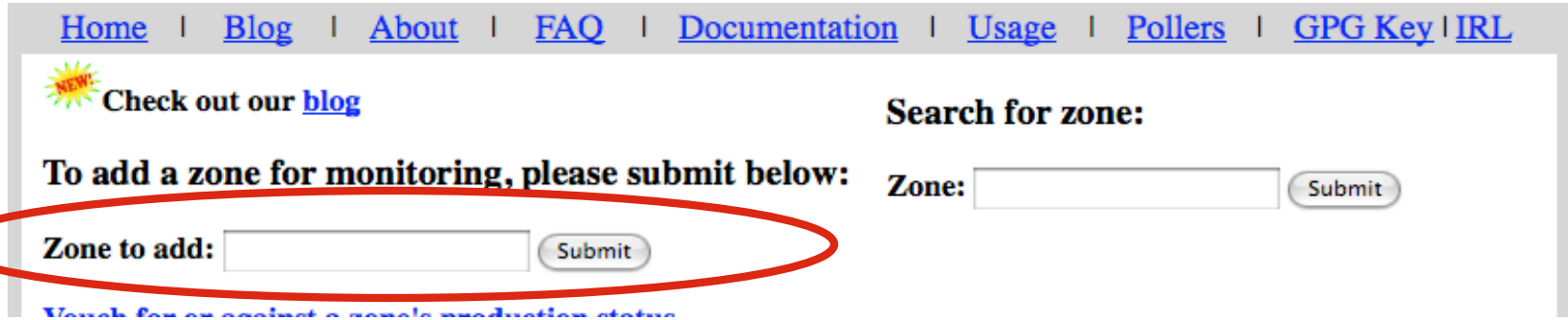




Whose Problem is it?

- 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 Drilldown Page

Zone **secspider.cs.ucla.edu.** 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:

Consistency:	Name:
100%	secspider.cs.ucla.edu.

Summary:

Property:	Status:
EDNS0 capable	Yes
DNSSEC deployed	Yes
Production zone	Yes
User Production	N/A

DS Records from parent zone:
Consistency: 100%

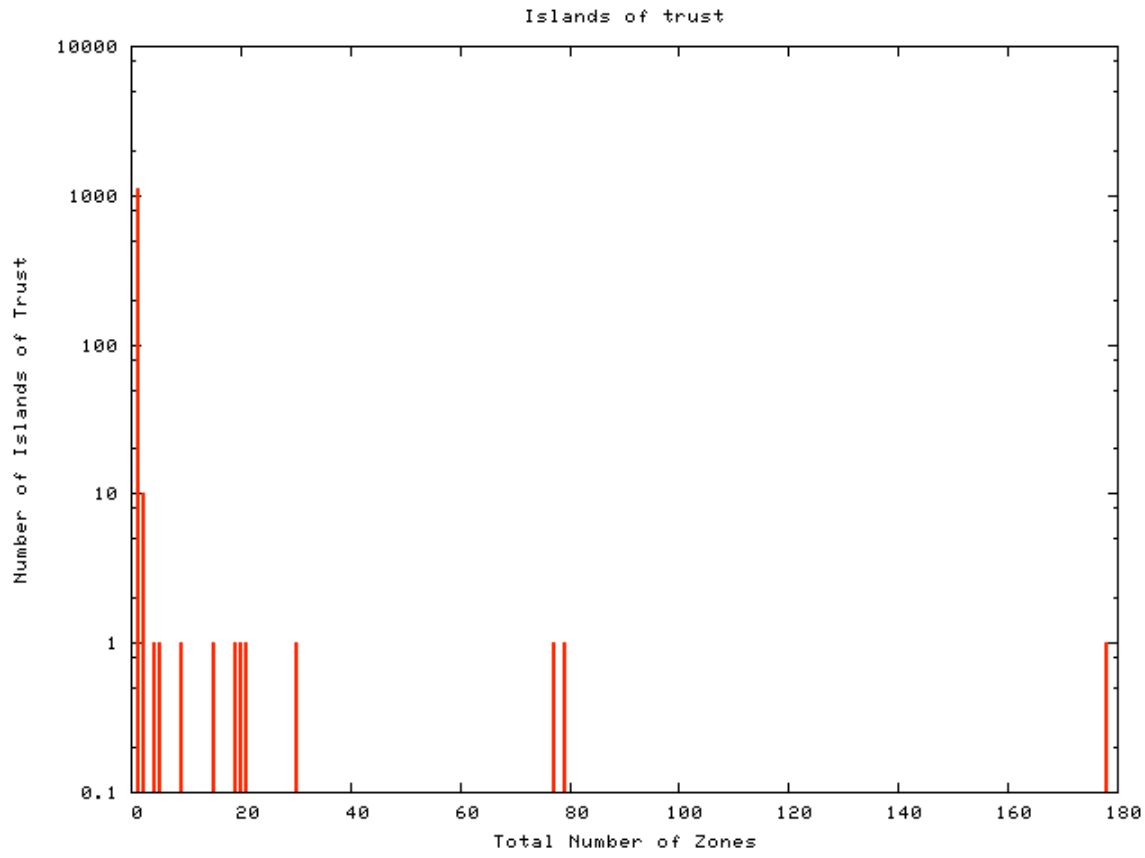
Key Tag:	Digest:	Verified (Yes/No):
N/A	N/A	No

DNSKEYs:
Consistency: 100%

Key Tag:	Key Type:	Algorithm:	Key:
secspider.cs.ucla.edu. 44736	ZSK	RSASHA1	AwEAAdWZPD1Ns1HKjugZ 8vAz8eqwT6f9n5YzyeR2 9hGZkR8YCLbccz14V//P Og4RCFQYMjDJbhMyqZHk
secspider.cs.ucla.edu. 59317	KSK	RSASHA1	AwEAAcWJhb0O0eaqyBUU q/ppiHMi3zKB37hl2S4G Y1f0txUfUQwYTjNsZHvu 4Wc2nL3Tin/ui8Us06CQ d4Ga5KfrFu5dbstgMX7Q 52O6zZh3nXZs2Jf3ENHU C0sHAZM2IVpe2R329icS

RRSIGs	Key Used:
	secspider.cs.ucla.edu. 44736
	secspider.cs.ucla.edu. 59317

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