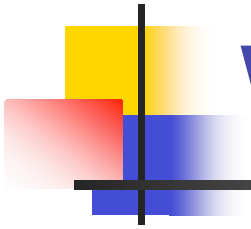
SecSpider: The DNSSEC Monitoring Project

Eric Osterweil

Dan Massey

Lixia Zhang

http://secspider.cs.ucla.edu/

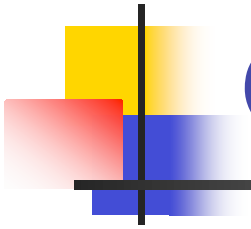


Why We Are Monitoring

- Trying to identify observable facets of DNSSEC's rollout
- Hope to find instructive insights for future systems
- Identifying elements that shed light on a design and operational practices

Motivating The Sec in DNSSEC

- We study the importance of islands and chains of trust
  - What kinds of islands are out there?
- When keeping records for their signature lifetimes:
  - Is re-signing of new data before expiration bad?
  - How often does it happen?



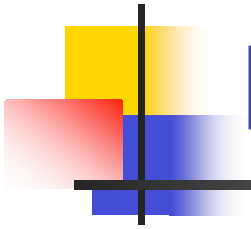
Outline

- Monitoring procedure
- Current state of our monitored set
- The way zones look so far
- Islands of trust
- Signing behavior and pitfalls
- Conclusion

Where Do We Get Our Zones?

- Each zone that we monitor was obtained in one of 3 ways
  - As a user submission
  - As the parent of a secure zone
  - It was spidered in our web crawl
  - It was NSEC walked

	#
User submission	67
Parent	33
Spidered	360
Walked	10



How We Monitor Each Zone

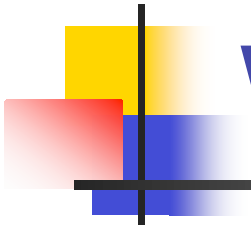
- To determine the operational status of each zone, we query each nameserver and we:
  - Note its serial number
  - Check that it supports ENDS0
  - Look for RRSIG RRs on its SOA record
  - Check to see if those signatures correspond to DNSKEYs served by the zone
  - Verify that the zone does not serve a CNAME for itself

How We Monitor Each Zone (2)

- Ensure that the zone issues a secure denial of existence for names that do not exist
- We classify zones as secure if all of their nameservers conform to the tests above
- Within each zone, each nameserver's status is enumerated on its zone-drilldown page

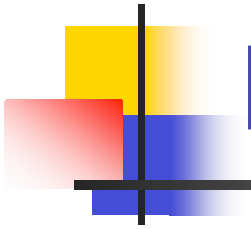
Name Servers:

Online:	NS Name:	NS IP:	Server Version:	First Queried:	Last Queried:	NS Serial Number:	EDNS0 Capable:	DNSSEC Deployed:	Pointed to by Which Zone (Parent/Authoritative/Both)?
Yes	ns0-dnssec.nic.uk.	213.248.202.150	9.3.1	Mon Nov 13 16:50:10 2006 UTC	Mon Nov 13 16:50:10 2006 UTC	2006111301	Yes	Yes	Parent
Yes	ns1-dnssec.nic.uk.	213.248.202.150	9.3.1	Mon Nov 13 16:50:11 2006 UTC	Mon Nov 13 16:50:11 2006 UTC	2006111301	Yes	Yes	Parent



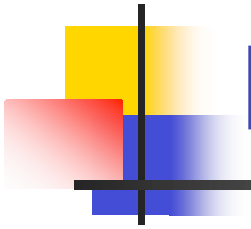
What We Are Tracking

- Currently, we track **470** zones
- Of these, roughly **276** are secure
  - i.e. they use DNSSEC with up to date signatures, etc.
- From our web crawl (of 18M zones), we estimate that the deployment status of DNSSEC is roughly 0.0015%



NSEC Walking

- In each secure zone we walk NSEC records to look for secure delegations
- Large zones can be prohibitively expensive to walk
  - Some may inflate their zones so that walking is prohibitively expensive
- We resort to randomized NSEC walking

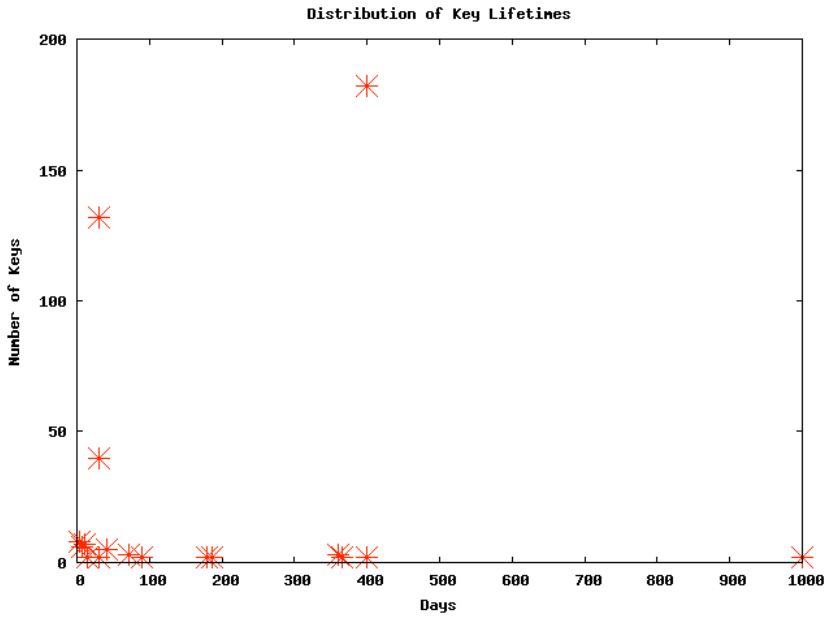


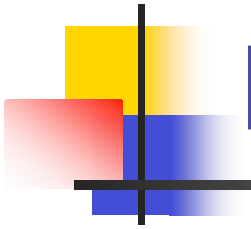
Randomized NSEC Walking

- Faced with many large secure zones we choose to make random jumps
- After a number of NSEC walks (starting at a zone's apex) we randomly create a string and append the zone's name to it
- Essentially, after some number of NSEC records, we jump forward
  - We repeat this until we wrap around to the apex

Keys

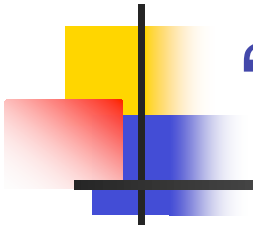
- We track 447 DNSKEY records
- All but 2 are RSA/SHA1
- Signature lifetimes vary between 3 and 1,000 days
- 80.04% keys signed for either 30 or 400 days





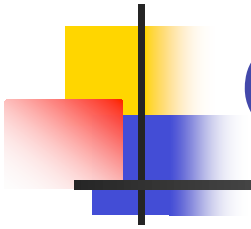
Nameservers in Zones

- We see an average of 3.6 nameservers per zone
- 24 zones have some nameservers that are secure and some that are not secure
  - We classify these zones as insecure
- 269 (out of 470) authoritative zones have NS RRsets that match the set served by their parents



“No [Zone] is an Island…”

- Delegation is a large part of the security model of DNSSEC
- Keeping track of the delegation hierarchy of the DNSSEC deployment
  - The state of the deployment falls far from the original vision

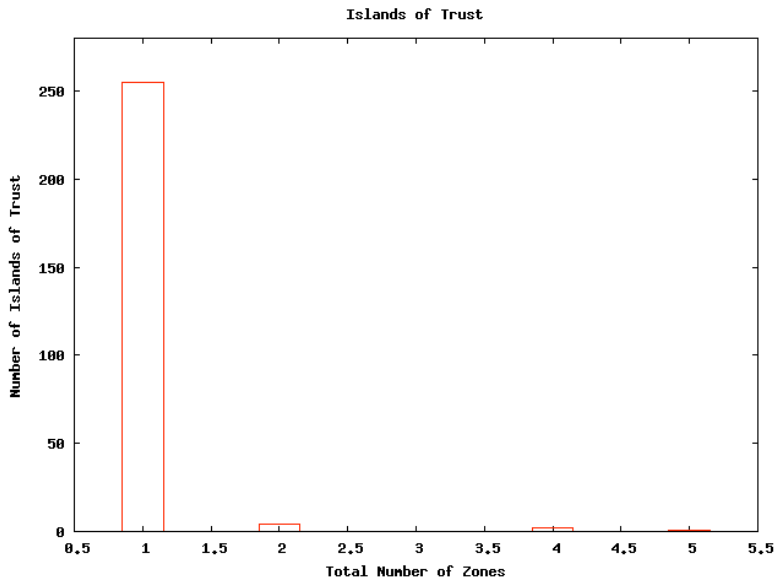


Or, maybe they are?

- From 276 secure zones, there are **262** separate islands of trust
- The largest island is **se.** and contains just **5** zones
- Islands are only formed by cryptographic delegations
  - Through DS records

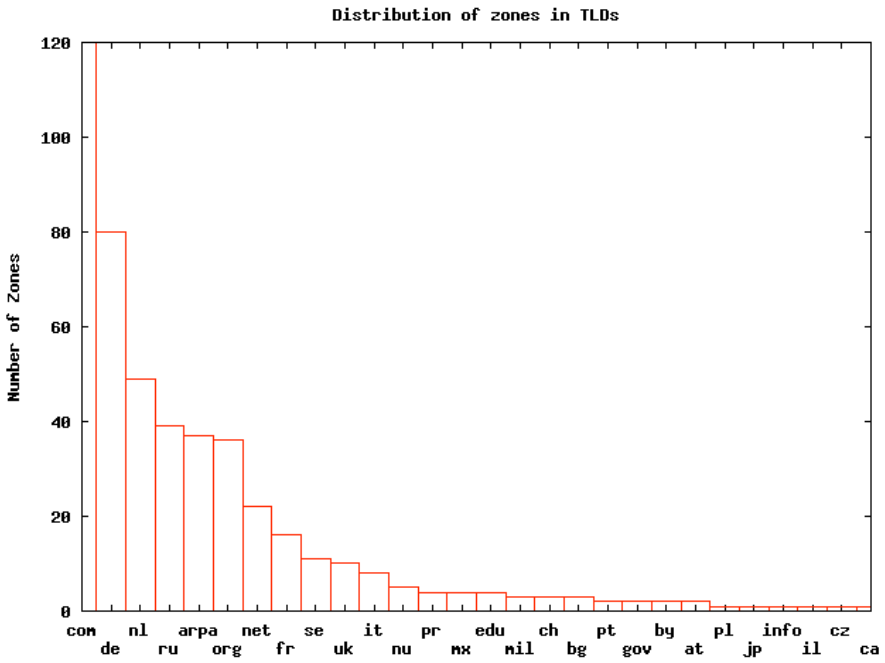
Today's Islands of Trust

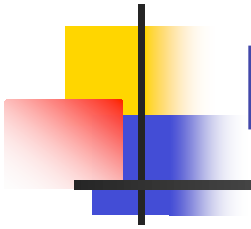
- Almost every zone is its own island
- Demonstrates lack of deployment experience managing delegation hierarchy
  - Since every zone is island, no zone is currently operating the delegation hierarchy



TLD Distribution

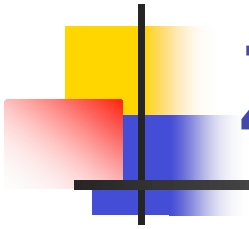
- Some TLDs have an effort to push DNSSEC
- Other TLDs are simply large and have more zones that could try DNSSEC





RRset Signing

- Stale records can be replayed even after the auth servers remove the records
  - Vulnerable until the signature lifetime expires
  - Suggests the use of a very short signature lifetime
- Signing data is a computational and operational burden
  - Requires access to private keys which may (should?) be offline
  - suggests the use of a very long signature lifetime
- SecSpider tracks the trade-offs and shows potential vulnerabilities due to long signatures



Zones May Be Vulnerable

- Some zones proactively re-sign their records more often than they expire
  - RRsets become *vulnerable* when their RR values change and are re-signed *before* old values' signatures expire
- In the event that a record (NS/A/etc) is re-signed with a new value, an adversary may be able to replay old values
  - This could affect service
  - What about a DNSKEY?

DNSKEY Vulnerability

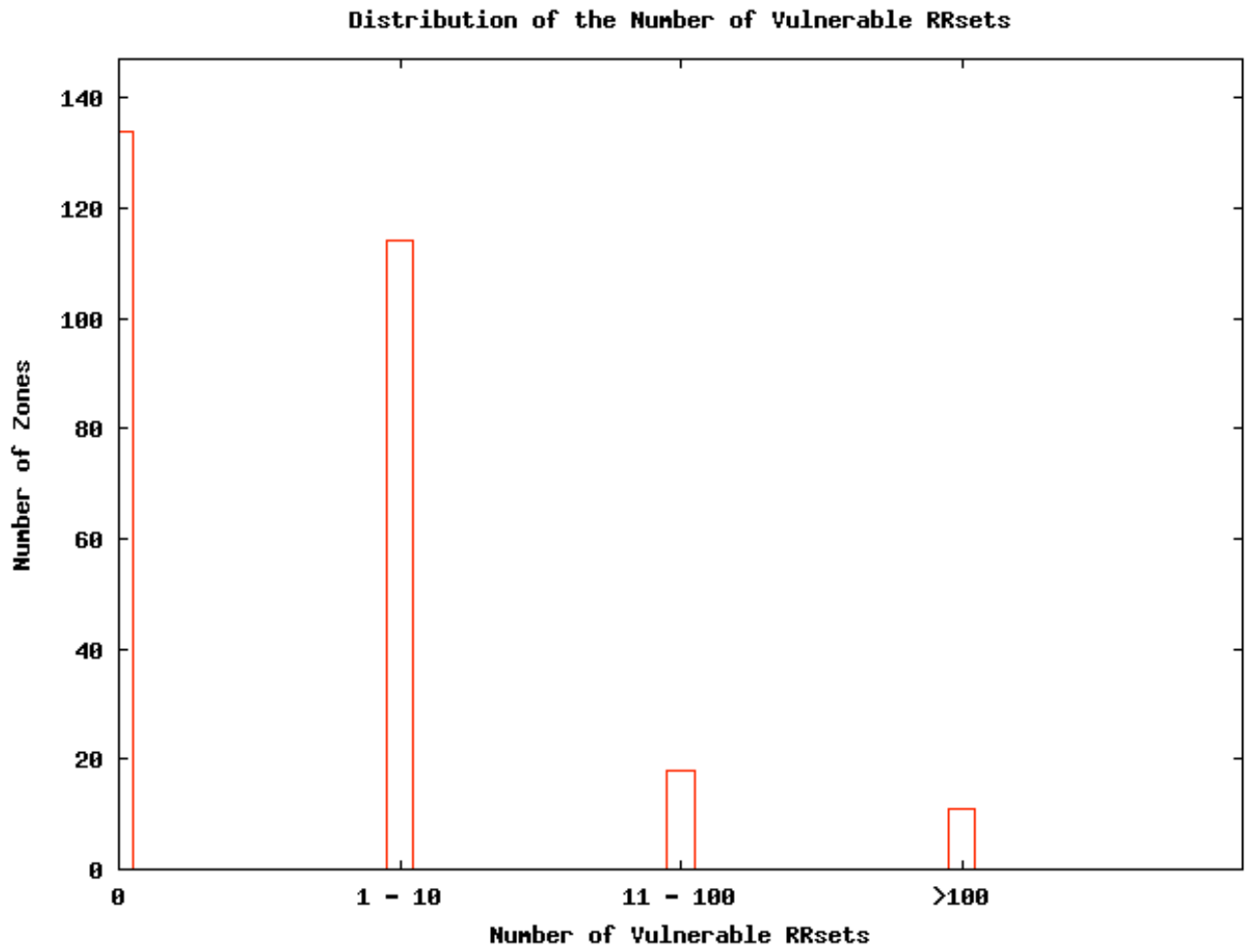
- In some cases, important sets (like DNSKEYs) can be vulnerable to replay

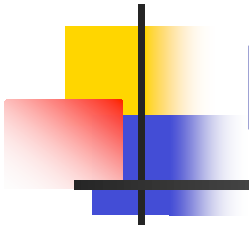
	DNSKEY	Nov 02, 2006 09:36:46 UTC	Dec 02, 2006 09:36:46 UTC	No
	NS	Nov 02, 2006 09:36:46 UTC	Dec 02, 2006 09:36:46 UTC	No
	SOA	Nov 02, 2006 03:38:40 UTC	Dec 02, 2006 03:38:40 UTC	Yes
	NS	Nov 02, 2006 03:38:40 UTC	Dec 02, 2006 03:38:40 UTC	No
	DNSKEY	Nov 02, 2006 03:38:40 UTC	Dec 02, 2006 03:38:40 UTC	Yes

Protecting the innocent

- Re-signing every night for keys with lifetimes of 1 month might be problematic when they change

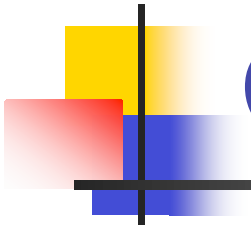
How Bad is it?


Distribution of the Number of Vulnerable RRsets
Number of Zones
140
120
100
80
60
40
20
0
0
1 - 10
11 - 100
>100
Number of Vulnerable RRsets



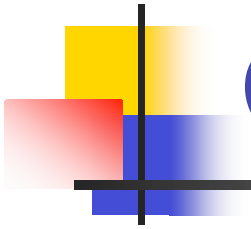
How Bad is it? (2)

- Roughly half of the monitored zones maintain signing practices that correspond to signature lifetimes
- The rest re-sign with a frequency that leaves some of their RRsets in conflict with previous values



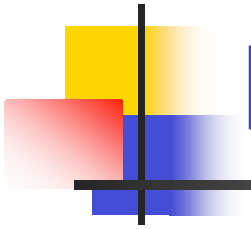
Conclusion

- We have observed that “orphaned” islands of security are essentially the norm
  - This lends credence to the notion of providing non-hierarchical (or look aside) validation of zones
- We have also seen that many zones deploy with default configurations
  - Almost all zones use RSA/SHA1
  - A significant portion of DNSKEYs are signed with the default 30 period



Conclusion (2)

- With the observations of small islands and default configurations we can see the importance of providing strong/safe defaults for critical operational practices
- Additionally, we notice that without clear re-signing guidelines, there exist unaddressed attack vectors against DNSSEC



Future Work

- Add support for
  - NSEC3
  - DLV
- Create a distributed monitoring framework
  - Poll zones from locations around the World
  - Will let as add the notion of availability to our monitoring

Come See For Yourself

SecSpider the DNSSEC Monitoring Project

Deployment status as of: ***Mon Nov 13 17:17:25 2006 UTC***

Monitoring Summary:

470 Zones

269 Zones have NS sets that match their parents' delegation set

276 DNSSEC enabled zones

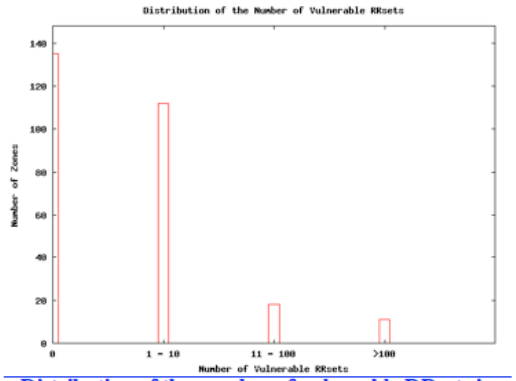
178 Zones use both KSKs and ZSKs

Distribution of key algorithms in use:

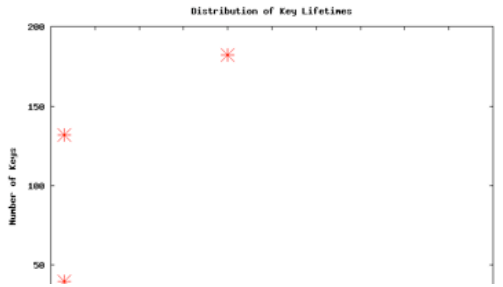
Algorithm	# Keys
RSA/MD5 [RSAMD5]	1
Diffie-Hellman [DH]	0
DSA/SHA-1 [DSA]	1
Elliptic Curve [ECC]	0
RSA/SHA-1 [RSASHA1]	445
Indirect [INDIRECT]	0
Private [PRIVATEDNS]	0
Private [PRIVATEOID]	0
Reserved 0	1
Reserved 255	0

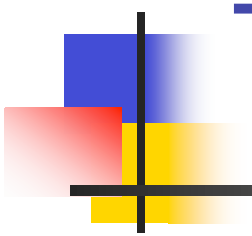
Monitored Zones: (in DNS cannonical order):

"." through "*170.32.198.in-addr.arpa.*"
"*195.in-addr.arpa.*" through "*80.in-addr.arpa.*"
"*81.in-addr.arpa.*" through "*agefal.org.*"
"*alaskaairhawaii.com.*" through "*at.*"
"*atlantadanceparty.com.*" through "*bierbijelkgerecht.com.*"



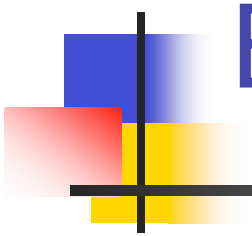
Distribution of the number of vulnerable RRsets in zones





Thank You

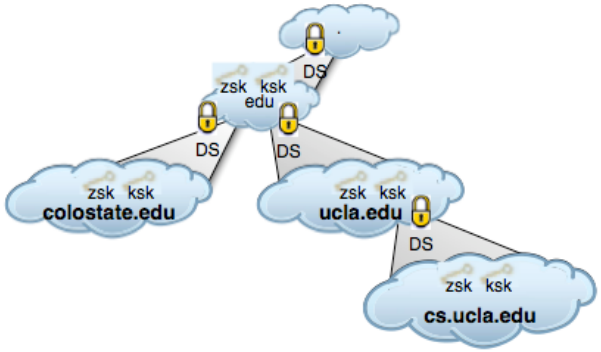
Questions?



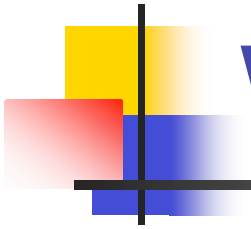
Backup

What is Trust?

- In DNSSEC resolvers identify authoritative zone data



  - Secure delegations create Islands of Security
  - Ideally, the root of an island should serve as a configurable trust anchor
  - All zones below a root should be verifiable from that root (chain of trust)



Web Crawling

- We obtained a large web crawl from a commercial search engine (http://www.infocious.com/)
- Next we mapped its URLs to 18,965,389 unique authoritative zones
- For each zone we queried for DNSKEY records.
- Whenever found, a zone with keys is added to SecSpider