Looking at TLD DNSSEC Practices

Edward Lewis, Neustar
Presented at APRICOT 2012
March 1, 2012

neustar

Why do this?

- DNSSEC is new, a major change to DNS operations, and the problem to be solved is hard to quantify. The problem is known, but the size and shape is not.
- TLD operators are at the cutting edge in this field, have the most collective experience
- Although running a TLD is not the same as running DNS for all, we at least have working examples to examine

Secondary Motivation

- By looking across the board at TLD operational patterns we can identify
  - "The norm"
  - How closely the norm is to what was anticipated in development
  - Who the outliers are
- For outliers, naming names is not the goal
  - We all have our reasons

Initial Questions

- What are the common key parameters?
  - DNSSEC "algorithm", length, duration
  - Frequency of key changes and methods
  - How many keys, signatures are published
- NSEC vs. NSEC3 choices, NSEC3 values
- Of lower concern - a measure of adoption
  - Because TLDs have different goals than the general DNS operator population

Method

- AXFR the root zone daily
  - Exclude 11 test IDN zones
- Retrieve records at each TLD apex
- Make sure there's a good collection each day
- Look at snapshots and trend data
- Deeper inspections of data as interest rises
- *Compare results to expectations*

Results

- Numbers, stats...
- Similarity in many operational aspects
- Close adherence to Conventional Wisdoms
- Patterns of operations emerging over time
  - I.e., some "experiment" before settling into a rut
- A few situations that I'd label (but not judge) as "odd"
  - Regulatory restrictions, budget limitations exist

About "CW"

- Conventional wisdom means knowledge that is generally held but not necessarily backed up by firm proofs
- In DNSSEC, a lot of parameters fit CW, starting from the workshop era
- This doesn't mean they are unfounded
  - There is some crypto science pointing to the algorithms and bit lengths
- But, these choices are untested as far as real security events

About the numbers

- The analysis covers data from June 21, 2011 to February 1, 2012 in these slides
  - Not long enough to capture annual events
- There is 1 root and 312 delegations covered
  - 11 test IDN TLDs are omitted
  - 1 zone discontinued DNSSEC in June
  - 2 zones were added in December, one signed
  - "302" is the base number of zones, "79" were signed at one point or another

Key Management Trends

Date (1st of -)	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb
Zones	299	300	300	300	300	300	302	302
Signed	64	65	65	68	73	75	78	78
with DS	59	60	61	61	62	68	71	71
without DS	5	5	4	7	11	7	7	7
RSA-SHA1-NSEC	9	9	9	9	9	9	9	9
RSA-SHA1-NSEC3	29	29	29	29	31	31	31	31
RSA-SHA256	23	24	24	27	30	33	35	35
RSA-SHA512	3	3	3	3	3	3	3	3
1024b ZSK	62	63	63	65	70	71	75	75
2048b KSK	56	57	56	59	65	67	72	72
1024b KSK	3	3	3	3	3	3	3	3
2Kb KSK/1Kb ZSK	55	56	55	57	63	64	70	70

Adoption Rate

- Motivation of engineers:
  - Big jumps made in Sept, Nov, and Dec
  - No one worked in January (and in summer)
- Net gain of 14 signed (15 newly, 1 ended)
- Want percentages?
  - 26% are signed, 24% have DS records
  - Other sources indicate some ccTLDs are as high as 15%, the larger gTLDs well under 1%

Key Mgmt Parameters

- What kinds of keys do I use?
  - Root/TLDs stick to one algorithm at a time
- What key length(s)?
  - Usually one size for KSK (SEP) and another for ZSK
- How often do I change keys?
  - Some variation here
- How many keys are active/published?
  - Have a ready "backup" or not?

Which DNSSEC Algorithm?

- All TLDs each use one RSA algorithm (no DSA)
- 78 zones, 40 RSA/SHA1, 35 RSA/SHA256
  - RSA/SHA-1 is still #1, but little gain
  - RSA/SHA-256 shot up by 50%
  - RSA/SHA-256 defined after RSA/SHA-1
- Conventional wisdom is to use RSA/SHA-256 if starting today, no rush to convert from RSA/SHA-1
  - TLDs reflect this

Key Lengths

- Conventional wisdom from the development days was to use 1024 bits for ZSK, 2048 bits for KSK
- Of the 78 signed zones, 70 do just that
  - 75 zones use a 1024 bit ZSK
  - 72 zones use a 2048 bit KSK
  - Only 1 zone uses neither

Records Published

- In DNS responses, size matters and a wish is to keep them small
- I tried adding up the number of days each record in a set was seen and dividing this by the days the zone was signed
- E.g., Signatures per set
  - Using the SOA as a measure
  - 76 of 78 zones averaged 1.0-1.1 signatures/day
  - Mostly just one active ZSK at a time

DS Records

- How many KSKs are represented as a DS record?
  - This is a measure of how many KSK's are active, measured for the 63 zones always-signed zones
  - 4 never had a DS, 56 avg'd 1, 4 av'd 2, 1 avg'd 3
- While calculating this number
  - Most TLDs have 2 DS record per KSK, some just 1
  - CW is to publish 2, BIND tools do this by default
  - (This is one measure I need to do more work on)

The DNSKEY set

- KSK (SEP) in the DNSKEY set
  - For 1,2,3: 44 zones, 29 zones, and 1 zone
- ZSKs
  - For 1,2,3: 45 zones, 33 zones, and 1 zone
  - Non-integer "averages" reflects rollover "speed"
- Signatures
  - 48 sign with all KSKs, 2 with just active one
  - 18 sign with KSKs and active ZSK, 11 w/all ZSK
  - Only KSK-generated signatures s are needed

Waiting to Add DS

- Only 11 zones were seen to add DNSSEC and then a DS record, how long was the wait?
  - One was immediate (an entirely new zone)
  - Seven fell into 9-23 days
  - Three ranged from 43 to 68 days
  - Rough average/mean, 21 days
- Knowing some other history
  - 3 zones were signed all of 2011, but no DS record

KSK Lifetimes

- Not enough data yet
- No DS record "came and went"
- Conventional wisdom is that KSK's live 1 or more years, so this is expected

- One notable event, one zone converted from a "Common Signing Key" to a KSK/ZSK approach, now all zones use KSK/ZSK (at the TLD level)

ZSK Key Lifetimes

- Keys visible (DNSKEY)
  - 14 ~month, **20~2mos**, 15 ~3 mos, 6 4+mons
  - 24 can't really be determined yet
- Keys used (SOA RRSIG)
  - **34 ~month**, 6~2mos, 14 ~3 mos,
  - 25 can't really be determined yet
- For further study, how long does a key remain in "retirement", how long in "preview"

Other DNSKEY Parameters

- The more one analyzes the data, the more there is to discover
  - what "exponent" is used?
  - choice of TTL of DNSKEY set and impact on changes
- And there are other, non-DNSKEY, parameters to examine

Signature - to be done

- I didn't look for this yet, but there's something to say
  - Signature Durations
  - Whether "jittering" is used or not
  - One zone sets the expiration date to be the last second of the calendar year, no matter when the signature is generated

NSEC vs. NSEC3

- NSEC and NSEC3 provide negative answer proofs. NSEC3 was added to limit disclosure of zone data
- The NSEC zone count rose from 15 to 17
  - Net gain of 2
- The NSEC3 zone count rose from 50 to 62
  - Net gain of 12
- TLDs are sensitive to data disclosure

NSEC3PARAMs

- Iterations (RFC recommends "low")
  - **4@0**, **20@1**, 16@2-9, **14@10**, 4@12
  - 1 each at 15, 17, and 150
- Salt lengths (in bytes)
  - **4@0**, 14@2-3, **31@4**, 2@5-6, **8@8**, 2@10-16
- Salt Values
  - Not unique to each zone, not always random
  - Examples: BA5EBA11, 5CA1AB1E, BADFE11A

Changing Salt

- RFC 5155 says to change the salt
  - SHOULD periodically, RECOMMENDS every "re-signing" (but many registries are incremental)
- From observations of record lifetimes
  - 50 zones have not changed (at least since June 22)
  - 3 change daily (all periods are "roughly")
  - 4 change monthly
  - 1 changes at 2 months
  - 3 change at 3 months

Results (so far)

- TLDs do DNSSEC:
  - RSA SHA-256, 1K ZSK, 2K KSK
  - One ZSK active and present, one KSK active and present
  - NSEC3 with 1 iteration, 4 byte (8 hex char) salts, rarely changed
  - Wait a few weeks after signing to add a DS record in the root
- That's what they do...is it right for everyone?

Commentary

- This work wasn't a "discovery" but "looking for confirmation" of previously held conventional wisdom based on workshops
- Unfortunately, there were few surprises
  - Unfortunate because it means that no one is challenging the Conventional Wisdom
- Fortunately, there were few surprises
  - Fortunate because TLDs appear to be taking the correct, conservative approach to security

Finally

- Why perform this "astronomy"-like survey instead of just asking the operators?
  - It's quicker to collect data
  - It's more accurate than documentation
  - It's repeatable, can be altered as new questions rise
- I'd like
  - To talk to operators who seem to fit "outlier" cases to understand why - curious, not judging

Discussion, Questions

- Feedback?
- Suggested measurements?
- How unique is this to TLDs?
- ...

- And, thanks for listening