DNS/DNSSEC and Domain Transfers: Are they compatible ?

Olafur Gudmundsson
Steve Crocker
Shinkuro inc.
{ogud,steve}@shinkuro.com

Background

- Shinkuro was asked by ORG to look into how DNSSEC affects transfers of signed domains,
  - In particular when Registrar operates the DNS service for the Domain holder.
- We have spend many months working out solutions that fit into the real world
  - Running DNSSEC transfer tests with early adopting registrars for org.

Approach

- This presentation is from the perspective of the DNS protocol, DNS software and is aimed at highlighting the real world issues.
- Goals:
  - Eliminate and/or minimize DNS resolution errors and service calls
  - Minimize work by “old” operators

Approach (cont)

- Assumptions:
  - All parties are willing to be minimally cooperative.
    - Without cooperation → DNS resolution errors
  - **Only DNS is being changed all other services are ignored**.

Approach (cont)

- How the behavior of certain DNS architectural elements affect the steps, at the time of:
  - DNS operator change
  - Registrar transfer
  - DNSSEC key change
- What DNS components need to be taken into account when changing operators
  - Parent/Registry/Registrar behavior
  - Authoritative server behavior
  - Resolver's behavior
  - TTL values and impact

Roles and Notation

- Domain holder: (H)
  - The entity that has the registration for a domain
- DNS operator: (O = old) (N = new)
  - Operates the DNS servers for the domain and maintains the zone
- Registrar: (R)
  - The party that the Domain holder has contracted with to register the domain
    - From H's perspective Registry is not visible.
- Parent:
  - The DNS domain that has the delegation to the zone
- Content Provider:
  - Ignored in this presentation
- Red = ERROR, Blue = Optional, Orange = not desired/partial failure

DNS control plane for domains: Record types

- **NS** lists the set of hosts that act as authoritative name servers for a zone
  - Appears in two places
    - as a hint in the parent, **unsigned**
    - Authoritative in the child, **signed**.
- **DNSKEY** the key(s) that can sign the data in the zone,
  - Resides at the child size of the delegation
- **DS** the key(s) authorized to sign the child DNSKEY set
  - Resides at the parent side of the delegation, **signed** by parent.

Simplified model

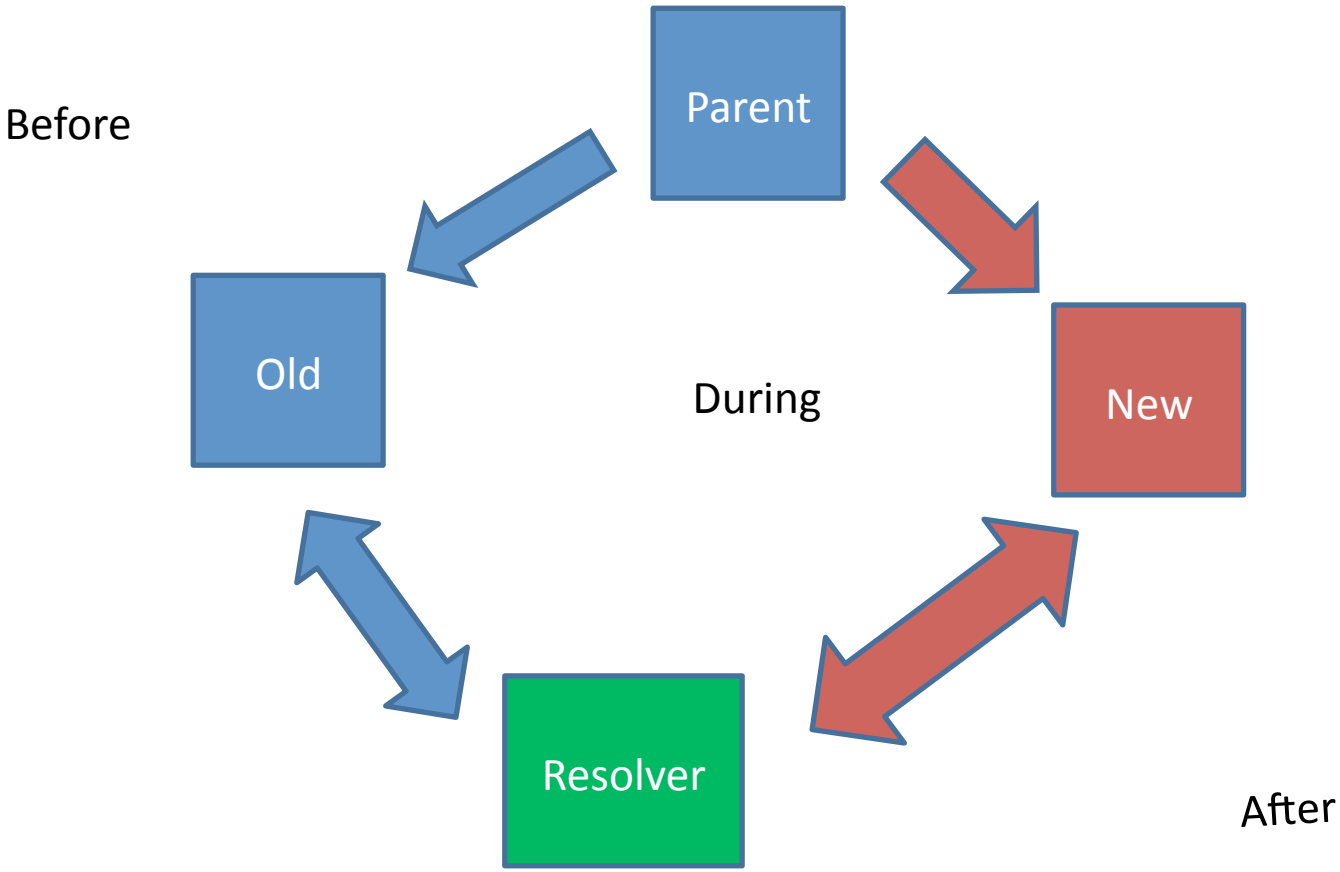
- New operator creates and loads a zone
  - Data is **available** but not **visible** as parent points to old operator.
- Moment of DNS change:
  - When parent **changes NS** set to point to new operator.
- New operator's data becomes **visible**

–BUT

Complication #1: TTL

- All DNS RRsets can be stored and reused by DNS resolvers/caches for certain time after reception.
  - Resolvers that **know about** old operator will keep asking old operator until the NS set expiries .
    - Until NS set expires the only reason for resolver to ask parent any question about the domain is to refresh the DS record.

DNS Operator Change: what happens



Complication #2: Resolver behaviors

- Centricity:
  - Some resolvers only use the NS set from the child
  - Others just use the one from the parent
- TTL stretching:
  - When an **identical** copy of a cached RRset from the same source is seen
    - some resolvers use the new copy to refresh the TTL
    - ➔ resolvers can be sticky to old operator.
- Error recovery:
  - Even when NONE of the authoritative servers answers resolvers will not ask parent for newer copy of NS.
    - This is common operator mistake/…….
    - asking parent **repeatedly** will only yield same bad data,
      - » Only causes extra load

DNS operator change (script)

- Domain holder (**H**) is using **O** as DNS operator
- **H** asks **N** to become *new DNS operator*
- **H** assists **N** in instantiating a copy of the zone
  - **O** may or may not be involved.
- **N** gives **H** a new NS set.
- **H** via **R (registrar)** to changes the NS set to point to **N**
- **H** asks **O** to change its NS set to **N**'s
  - This is optional for **O**
- **H** waits for old copies of NS sets to expire i.e. new NS set to become *globally visible*.
- **H** asks **O** to stop DNS service
  - **O** should stop service as soon as possible.

What can go wrong:

- If O stops service before parent NS is changed:
  - Total DNS failure on all lookups
- If O stops service before all resolvers have migrated over:
  - Some resolvers may experience outage
    - Hard to diagnose as this depends on the state of local resolvers
- If O does not stop service when asked to
  - Some child-centric sticky resolvers may never discover the operator change
- N is not ready when NS is changed:
  - DNS resolution failure

TTL effects

- How fast operators can be changed: is dictated by the TTL on the DNS control plane RRsets!
- In many cases the PARENT selected TTL's dominate the wait times.
  - Many TLD's have TTL's on NS sets that are in day's

DNSSEC operator change

- Assumption:
  - New and Old DNS operators will use different keys to sign data in the zone.
- Goal:
  - Want to avoid both DNS resolution failures and DNSSEC validation errors!!
    - Follow same approach
    - During change resolvers MUST be able to validate signatures by both operators.
- Actually this is Key Rollover and Operator change rolled into one

DNSSEC preconditions

- DS set MUST contain authorization for **both** operators KSK's during the change
- **Both** DNSKEY RRset's MUST contain ZSK's for both operators during change.
- ➔ New DNSKEY and DS sets **MUST** be **globally visible**
  - before NS set in **parent** is changed.

Script: Before DNSSEC operator change

- **H** contracts with **N** to operate zone
- **N** instantiates a zone,
  - Generates new KSK and ZSK,
    - DNSKEY set includes ZSK **O** is using.
  - Provides **H** with new NS and DS records
- **H** asks **O** to add **N**'s ZSK to its copy of zone
- **H** via **R** adds **N**'s DS record to the ones for O
- **H** waits for new DS and DNSKEY to become globally visible.
  - Max(O's NS TTL, P's NS TTL, DS TTL)

Operator Change and after

- **H** via **R** changes NS set to point to **N**
- **H** asks **O** to change NS set to point to **N**
  - Optional step
- **H** waits for old NS's to expire max TTL on NS sets
- **H** asks **O** to stop service.
- **H** waits for laggard resolvers to detect change
- **H** via **R** to removes DS records for **O**
- **H** asks **N** to remove ZSK records for **O**

How can change go wrong?

- **O refuses** to add N's ZSK →
  - signed Operator Change **not possible** →
    - this behavior complicates things.
- **O** turns **off** service before changes in parent have had time to propagate
  - DNS resolution failures.
- **H** can not update DS records
  - **Operator Change not possible**

Considerations

- **H** does not wait long enough for old data for expire from the system
  - Some resolvers may experience failures
    - **This is H's choice**
- **O** does not change NS to reflect **N**
  - Mitigations:
    - O can slave from N and then things work great
    - O can lower TTL on NS and DNSKEY to force resolvers to forget its NS set.

Now back to the real world ☺

- The previous slides assumed **H** knew what to do and had the ability to do so.
  - **H** can give **N** the authorization to perform its tasks
- When Registrar is also the DNS Operator
  - Change the DNS Operator **first**
  - **Then** change the Registrar
    - ISSUE: H not able to insert new DS records before change.

Registry DNSSEC requirements

- Sign zone and process updates in near real-time.
- Accept DS records via EPP
  - Accept more than one DS record per delegation
    - Org allows 12
    - Rollovers work better if DS is published before change
  - Optional: accept DNSKEY records and generate DS records

Requirements for Registrars: DNSSEC Signed Domains

- Registrars must support DNSSEC EPP extensions
- Interfaces must be updated to accept DS records
  - add + delete operations
  - Optional: accept DNSKEY records
- Separate account for Technical Contact
  - Can only change NS and DS records

Requirements for DNS operators

- MUST accept DNSKEY record from domain holder
- Should change NS when asked
- MUST turn off service when asked **but not before.**

DNSSEC Transfer Testing for ORG

- As a demonstration that it is possible to change DNS operators and Registrars we have worked with org and two registrars
  - Names Beyond
  - DynDNS
- For each registrar there are up to 13 tests where it is the original registrar
- There are up to 4 tests where it is destination registrar.

Testing sheet

variant	7AcAd	Transfer of DNS operation for a signed zone
Actors		Neither operator is associated with a registrar
R	PIR/Afilias	
H	Shinkuro	This variant tests just the transfer of signed DNS service. It is assumed that other services, e.g. mail and web, are provided on separate machines and do not need to be transitioned. Initial State: domain name is registered via A and operating on c1 and c2
A	NBC	
B		
c	Shinkuro	
d	Sparta	
FQDN	dnssecxfr00378-7AcAd.org	
NS	c1, c2, d1, d2	

Step	Date/Time	Notes	Actor	Actions	Results
1			H	Request d to operate zone	Positive Ack from d with credentials
2			d	Get copy of zone and instantiate it on d1, d2. Create new ZSKs and KSKs. Replace KSKs with new KSKs. Add the new ZSKs with old ZSKs. Replace all RRSIGs with new signatures. Domain Holder gets DS records and ZSKs from d.	Verify that servers are responding authoritatively with appropriate content

Testing sheet (cont)

3		H	Tell c to add new ZSKs to keyset.	Positive Ack from c
4		c	Add ZSKs to the zone's keyset	
5		H	Tell A to update DS records at parent	
6		A	send EPP command to add new DS records to the parent	query shows new DS records at the parent
7		H	Wait for the later of two sequences: ZSK to appear in c, then for the maxTTL of ZSKs, and the DS TTL after the DS records appear at the parent.	
8	1	H	Tell c to replace name servers with d1, d2	Positive Ack from c
9		c	Replace name servers with d1, d2	query shows change at c
10		H	Tell A to replace name servers with d1, d2	Positive Ack from A
11		A	Send EPP command to registry to replace the name servers with d1, d2 at the parent	
12		R	Replace c1, c2 with d1, d2	Parent DNS and Whois both reflect the change
13	2	H	Wait for d1, d2 to appear in c and in parent	d1, d2 appear in both c and parent
14		H	Wait max(TTLs on the NS sets)	No visible result. Caches are presumably drained throughout the net
15		H	Tell c to turn off service	c Acks
16		a	c turns off service	c servers respond to queries with "notauth"
17		H	Tells d to remove old DNSKEYs and tells A to remove DS records from parent.	
18		d	DNSKEYs from c are removed from d's zone	query shows records gone
19		A	Send EPP command to remove old (c's) DS records from the parent	query shows DS records gone
20		R	Remove old (c's) DS records from the parent	Parent DNS and Whois both reflect the change

Testing Results

- Registrar interfaces needed fixing
  - All minor issues
- Most of testing performed by outsiders (us)
- Time to perform tests dominated by ORG's TTL of 1 day
- Actual tests in progress.

DNSSEC Registrar Considerations

- Registrar that operates ONLY as registrar for a domain
  - Needs to update UI and EPP with parents
    - Add/delete DS/DNSKEY

Bundled DNSSEC Registrar considerations

- Registrar that operates DNS as value added service
- Needs to understand the extra requirements that being a DNSSEC operator means
  - Must accept new DNSKEY records from domain holder
  - Transfer policies: ?
    - Block Transfers until after DNS operation has been transferred.
    - Operate DNS service for a grace period after Transfer
    - Other

Registry Policy Questions

- When can a DNSSEC domain be transferred?
  - Between DNSSEC capable registrars ?
- How many DS record are allowed ?
- Will registry lower TTL's on upon demand ?
- What certification testing is required for DNSSEC registrars?
- Does registry accept DS and/or DNSKEY records?

Conclusions

- “All at once” DNSSEC Transfer is impossible
- With “DNS first, Registration second” Transfer is: