Analysis of DNSSEC Signing Methods for Very Large Zones

or...what's a TLD to do?

Joe Gersch
DNS-OARC
May 2010

SECURE64

SOFTWARE CORPORATION

Sorry I can’t be in Prague

- In case you forgot what I look like....

...or maybe not....

SECURE64

Issues with Large Dynamic Zones (TLD's)

- Time required to:
  - initially sign the zone
  - load the zone and start the name server
  - send AXFR packages to secondary servers
    - and the time at secondary site to receive large AXFR
  - periodically re-sign the zone
  - finish a key rollover
- DDNS lockout during signing, re-signing, zone transfer
- Serial number management
- Size: memory, file

SECURE64

Example: 15 Million RR's

"this is going to take a while..."

- Signing: (assume 5k/second) = 50 minutes
- load & startup: 10 to 30 minutes

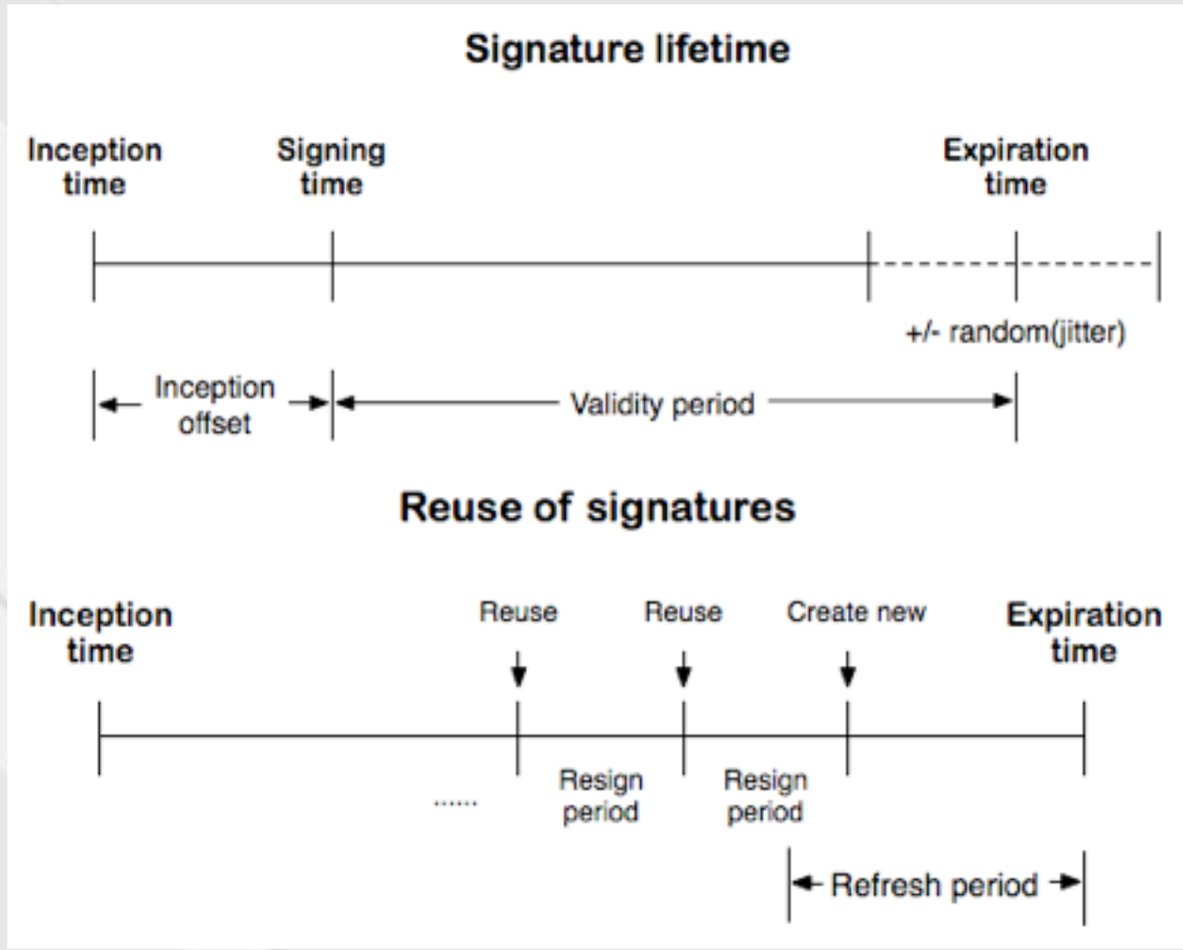
- Current solutions:
  - use NSEC3 to opt-out unsigned delegations. Much less to sign, typically only a few minutes.
  - add more horsepower to the signing engine

- But... NSEC3 is a delaying tactic only. Eventually there may be a preponderance of signed delegations. Then what?

SECURE64

Re-Signing

- How to shorten the time to re-sign a large zone
  - Partial Signing
    - (jitter & refresh)
    - incremental signing
    - continuous signing



- Still have to load data
  - unless signed in memory

SECURE64

Thanks to OpenDNSSEC project for timeline

Why is this important?
DDNS Lockout during Signing/Re-Signing

- Periodic dynamic updates (1 per minute) put on hold. An hour delay may be intolerable.

Does Jitter Really Help?

- Yes, but....
- See simulation data in next slides

- It can spread out the load, but pay attention to the parameters to see how load can vary

- Still have to load/axfr large zone which will hold off DDNS

SECURE64

Re-Signing with Jitter (discrete dynamic model)

10 day lifetime, 5 day safety factor (refresh), 3 day jitter, daily resign

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	sign																											
2		resign expires 7																										
3			resign expires 8																									
4				resign exp 9																								
5					resign exp 10																							
6						resign exp 11																						
7							resign exp 12																					
8								resign exp 13																				
9									resign exp 14																			
10										resign exp 15																		
11	33.3%	33.3%	33.3%	33.3%	33.3%						resign exp 16																	
12	33.3%	33.3%	33.3%	33.3%	33.3%	33.3%						resign exp 17																
13	33.4%	33.4%	33.4%	33.4%	33.4%	33.4%	33.4%						resign exp 18															
14														resign exp 19														
15															resign exp 20													
16						11.1%	11.1%	11.1%	11.1%	11.1%						resign exp 21													
17						11.1%	22.2%	22.2%	22.2%	22.2%	22.2%						resign exp 22												
18						11.1%	22.2%	33.3%	33.3%	33.3%	33.3%	33.3%						resign 23											
19							11.1%	22.2%	22.2%	22.2%	22.2%	22.2%	22.2%						resign 24										
20								11.2%	11.2%	11.2%	11.2%	11.2%	11.2%	11.2%						resign 25									
21											3.7%	3.7%	3.7%	3.7%	3.7%						resign 26								
22											3.7%	11.1%	11.1%	11.1%	11.1%	11.1%						resign 27							
23											3.7%	11.1%	22.2%	22.2%	22.2%	22.2%	22.2%						resign 28						
24												7.4%	18.5%	25.9%	25.9%	25.9%	25.9%	25.9%						resign 29					
25													11.1%	18.5%	22.2%	22.2%	22.2%	22.2%	22.2%						resign 30				
26														7.4%	11.1%	12.4%	12.4%	12.4%	12.4%	12.4%						resign 31			
27															3.7%	4.9%	8.6%	8.6%	8.6%	8.6%	8.6%						resign 32		
28																1.2%	4.9%	12.3%	12.3%	12.3%	12.3%	12.3%						resign 3	
29																	3.7%	11.1%	19.7%	19.7%	19.7%	19.7%	19.7%						
30																		7.4%	16.0%	23.4%	23.4%	23.4%	23.4%	23.4%					
31																			8.6%	16.0%	20.1%	20.1%	20.1%	20.1%	20.1%				
32																				7.4%	11.5%	14.4%	14.4%	14.4%	14.4%	14.4%			
33																					4.1%	7.0%	11.1%	11.1%	11.1%	11.1%	11.1%		
34																						2.9%	7.0%	13.5%	13.5%	13.5%	13.5%	13.5%	
35																							4.1%	10.7%	18.5%	18.5%	18.5%	18.5%	
36																								6.6%	14.4%	21.1%	21.1%	21.1%	
																									7.8%	14.5%	19.3%	19.3%	
																										6.7%	11.5%	15.2%	
																											4.8%	8.5%	

3-day jitter, 10 day life
5 day refresh, daily re-sign:
varies from 4% to 26%

example 2

10 day lifetime, 5 day safety factor (refresh), 10 day jitter, daily resign

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	sign																											
2		resign expires 7																										
3			resign expires 8																									
4				resign exp 9																								
5					resign exp 10																							
6						resign exp 11																						
7							resign exp 12																					
8								resign exp 13																				
9									resign exp 14																			
10										resign exp 15																		
11	10.0%	10.0%	10.0%	10.0%							resign exp 16																	
12	10.0%	10.0%	10.0%	10.0%	10.0%							resign exp 17																
13	10.0%	10.0%	10.0%	10.0%	10.0%	10.0%							resign exp 18															
14	10.0%	10.0%	10.0%	10.0%	10.0%	10.0%	10.0%							resign exp 19														
15	10.0%	10.0%	10.0%	10.0%	11.0%	11.0%	11.0%	11.0%							resign exp 20													
16	10.0%	10.0%	10.0%	10.0%	11.0%	12.0%	12.0%	12.0%	12.0%							resign exp 21												
17	10.0%	10.0%	10.0%	10.0%	11.0%	12.0%	13.0%	13.0%	13.0%	13.0%							resign exp 22											
18	10.0%	10.0%	10.0%	10.0%	11.0%	12.0%	13.0%	14.0%	14.0%	14.0%	14.0%							resign 23										
19	10.0%	10.0%	10.0%	10.0%	11.0%	12.0%	13.0%	14.0%	15.1%	15.1%	15.1%	15.1%							resign 24									
20	10.0%	10.0%	10.0%	10.0%	11.0%	12.0%	13.0%	14.0%	15.1%	16.3%	16.3%	16.3%	16.3%							resign 25								
21					1.0%	2.0%	3.0%	4.0%	5.1%	6.3%	7.6%	7.6%	7.6%	7.6%							resign 26							
22					1.0%	2.0%	3.0%	4.0%	5.1%	6.3%	7.6%	9.0%	9.0%	9.0%	9.0%							resign 27						
23					1.0%	2.0%	3.0%	4.0%	5.1%	6.3%	7.6%	9.0%	10.5%	10.5%	10.5%	10.5%							resign 28					
24					1.0%	2.0%	3.0%	4.0%	5.1%	6.3%	7.6%	9.0%	10.5%	12.1%	12.1%	12.1%	12.1%							resign 29				
25						1.0%	2.0%	3.0%	4.1%	5.3%	6.6%	8.0%	9.5%	11.1%	11.9%	11.9%	11.9%	11.9%							resign 30			
26							1.0%	2.0%	3.1%	4.3%	5.6%	7.0%	8.5%	10.1%	10.9%	11.8%	11.8%	11.8%	11.8%							resign 31		
27								1.0%	2.1%	3.3%	4.6%	6.0%	7.5%	9.1%	9.9%	10.8%	11.9%	11.9%	11.9%	11.9%							resign 32	
28									1.1%	2.3%	3.6%	5.0%	6.5%	8.1%	8.9%	9.8%	10.9%	12.1%	12.1%	12.1%	12.1%							resign
29										1.2%	2.5%	3.9%	5.4%	7.0%	7.8%	8.7%	9.8%	11.0%	12.2%	12.2%	12.2%	12.2%						
30											1.3%	2.7%	4.2%	5.8%	6.6%	7.5%	8.6%	9.8%	11.0%	12.1%	12.1%	12.1%	12.1%					
31												1.4%	2.9%	4.5%	5.3%	6.2%	7.3%	8.5%	9.7%	10.8%	12.0%	12.0%	12.0%	12.0%				
32													1.5%	3.1%	3.9%	4.8%	5.9%	7.1%	8.3%	9.4%	10.6%	11.8%	11.8%	11.8%	11.8%			
33														1.6%	2.4%	3.3%	4.3%	5.6%	6.7%	7.9%	9.1%	10.3%	11.5%	11.5%	11.5%	11.5%		
34															0.8%	1.7%	2.7%	3.9%	5.1%	6.3%	7.5%	8.7%	9.9%	11.1%	11.1%	11.1%	11.1%	
35																0.9%	2.0%	3.2%	4.4%	5.5%	6.7%	7.9%	9.1%	10.4%	11.6%	11.6%	11.6%	11.6%
36																	1.1%	2.3%	3.5%	4.6%	5.8%	7.0%	8.2%	9.5%	10.7%	11.8%	11.8%	11.8%
																		1.2%	2.4%	3.6%	4.8%	6.0%	7.2%	8.4%	9.6%	10.8%	11.9%	11.9%

10-day jitter, 10 day life
5 day refresh, daily re-sign:
converges to ~ 12%

Rollover & Jitter

- Rollover:
  - Either a full re-sign, or
  - partial re-sign with jitter, but you can’t throw away old keys until all data is signed a bit at a time.
    - Do you really want to wait 10 days?

SECURE64

The deeper issue: AXFR after re-sign

- On the sending side
  - May take 1 hour to do a full AXFR
  - then a whole lot of IXFR activity that was held off

- On the receiving side:
  - ISP may be secondary for many TLD's, all tying up time & bandwidth for large zone transfers from all these sources. May not be able to receive that much data (timeouts).

SECURE64

Potential Solution

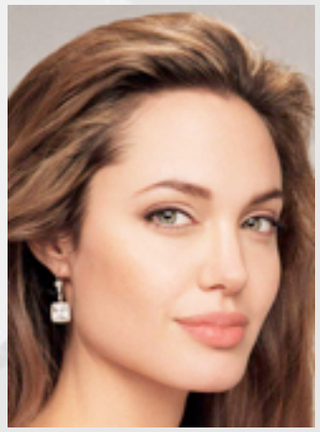
- IXFR rather than AXFR
  - after a re-signing, send only the changes
  - especially useful with NSEC3 for now, or partial re-signings later
- Incremental or Continuous Signing
  - when a dynamic update comes in, re-sign a subset of data and include this in the IXFR package.
  - serial numbers will stay in sync
  - Example:
    - sign 10,000 RR's each time a DDNS update arrives (takes 2 seconds). If 1 update per minute, the entire zone will be re-signed in 25 hours.
    - A rollover can finish in a timely manner

SECURE64

Thanks

- Interested in anyone else looking at these issues
- other ideas, approaches, experiments

...with thanks to my wife
for letting me stay up so late...



SECURE64