DNSSEC Algorithm Roll in .ORG: Maintenance in the Time of COVID

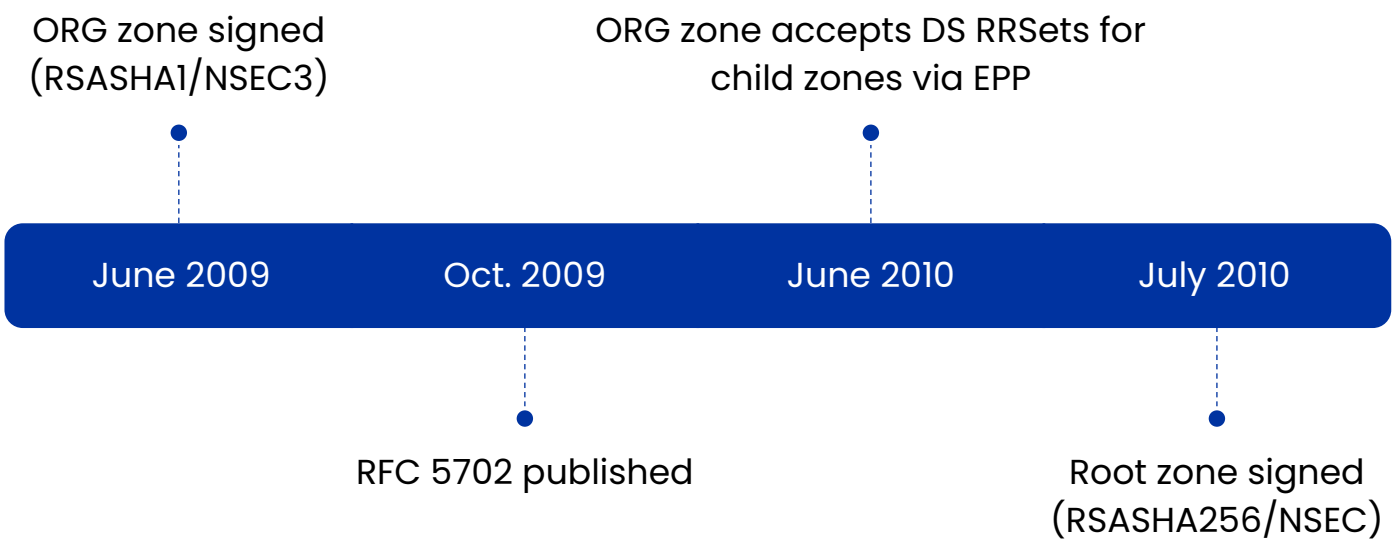
Suzanne Woolf, Joe Abley

DNSSE Workshop

Virtual ICANN 69

21 Oct. 2020

IN THE BEGINNING...



WHAT DID WE WANT TO ACHIEVE?

- **ORG had an enormous DNSKEY RRSet**
  - Enormous enough that some guy called Geoff Huston once wondered aloud on stage in various conferences how .ORG even worked at all *for an entire year* to see if we would react
  - We should really make that smaller…
  - … but we'll wait because we wouldn't want to deprive Geoff of comedic material

- **ORG is signed using algorithm 7 (RSASHA1)**
  - Rijmen, Oswald, "Update on SHA-1" January 2005
  - Wang, Yin, Yu, "Finding Collisions in the Full SHA-1" August 2005
  - Wang, Yao, Yao, "Notes on the Wang et al. 2^{63} SHA-1 Differential Path", August 2005
  - … and many other old-time favourites, including…
  - Leurent, Peyrin, "From Collisions to Chosen-Prefix Collisions – Application to Full SHA-1" April 2019
  - Leurent, Peyrin, "SHA-1 is a Shambles First Chosen-Prefix Collision on SHA-1 and Applications to the PGP Web of Trust" January 2020

- **ORG is signed using NSEC3**
  - Negligible and increasingly unimportant protections against zone-walking
  - Opt-out sections make aggressive negative caching difficult
  - Complicates provisioning since zone size depends on DNSSEC uptake in children

WHERE WERE WE HEADING?

- **ORG had an enormous DNSKEY RRSet**
  - Identify operationally incomplete KSK rolls and complete them
  - Review pre-publication parameters for as-yet unused keys
  - Start lab testing different signer parameters to find out what else we could improve on

- **ORG is signed using algorithm 7 (RSASHA1)**
  - Plausible targets are algorithm 8 and 13
  - All the cool kids are doing algorithm 13 though, and that will help with the DNSKEY response size. Let's do that, we're cool. Algorithm 8 is lame, etc.
  - Start lab testing to find the performance implications of algorithm 7 vs. 8 vs. 13

- **ORG is signed using NSEC3**
  - NSEC is operationally less complicated
  - We're fairly sure we are no longer concerned with the zone-walking problem
  - With 10,000,000 delegations, most of which are insecure, adding NSEC + RRSIG to each one means something like 20,000,000 additional resource records and 10,000,000 additional signatures
  - Start lab testing to find the performance implications of signing the NSECs
  - Start reviewing the edge capacity forecasts for memory footprint

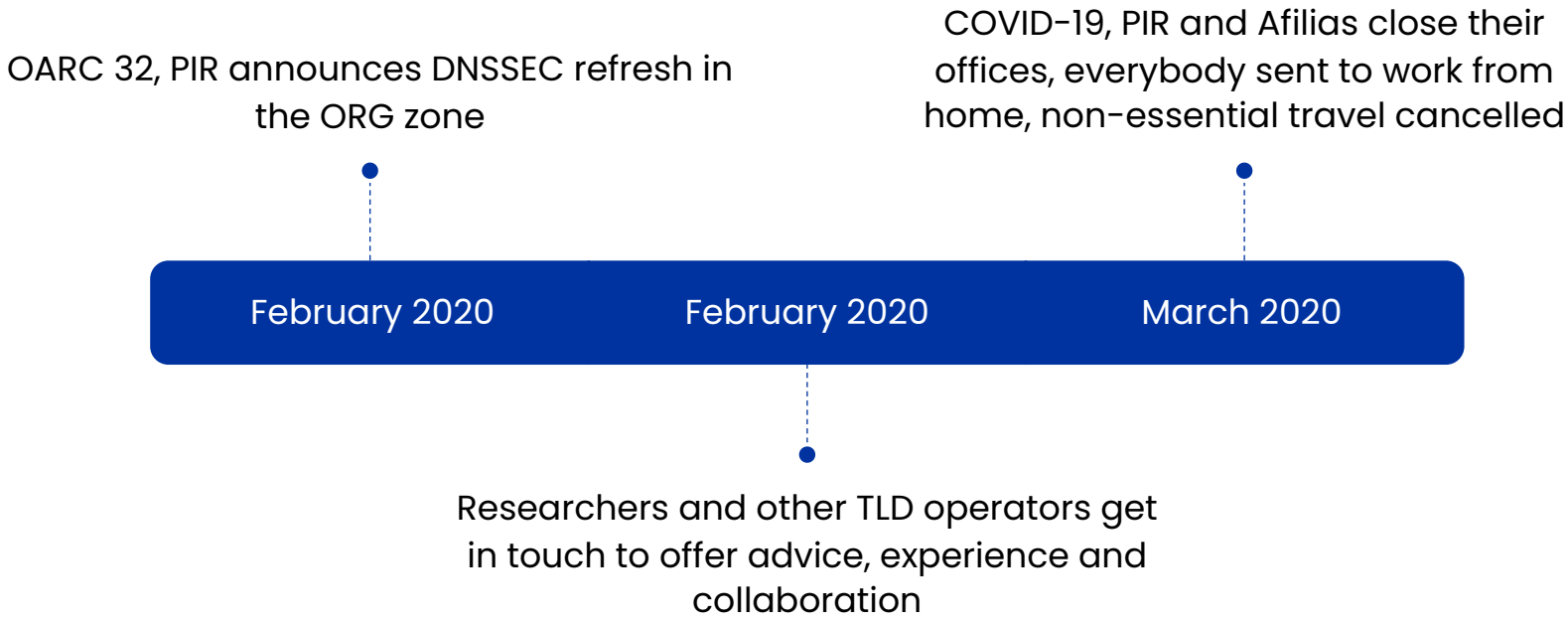
WHO SHOULD WE WORK WITH?

- **Community Engagement**
  - We want to make sure resolver operators are well aware of our plans
  - Let's review the relative differences in the validator population when it comes to 8 vs. 13
  - We should do a bunch of lab testing, and if we're going to do lab testing, we may as well make it a public lab

- **Research Opportunities**
  - ORG might have a more widespread base of dependent validators than the ccTLDs that have rolled to 13; perhaps there are interesting differences, there
  - We don't know for sure, but we think that possibly there hasn't been a production TLD roll from NSEC3 to NSEC, so perhaps that is new and exciting

- **Communications and Data Collection Partners**
  - Started talking to the good people at DNS-OARC about our plans
  - Keith and Matt offered to host a mailing list
  - We started talking about how we might contribute funds to help with data collection exercises, if researchers suggested they were interested in data

IN EARLY 2020, WE HAD IT ALL FIGURED...



BUT THEN OF COURSE

- **Huge performance impact of Algorithm 13 on Existing Signers**
  - The current signing platform in use for .ORG has unoptimized support for ECDSA, and it shows
  - The new signing platform under development for other TLDs that would very likely not have this problem is still, well, under development

- **No Travel**
  - Setting up a lab with new hardware is suddenly much more difficult
  - Crossing borders to increase edge capacity, memory footprints, etc suddenly seems difficult
  - Changes to key management that involve people handling credentials seem unwise, even if they are practical

- **No Universities**
  - Universities all over the planet start closing down and sending their students home
  - Campuses close, courses are suspended
  - Some regional universities have already cancelled lectures through the end of 2021

- **Everybody Suddenly Depends on the DNS Even More than they Used To**
  - Let's face it, this would be a particularly terrible time for anything to go wrong
  - Critical Critical Infrastructure

THAT WAS MARCH. SURELY APRIL WOULD BE FINE.

MARCH 50TH OR SO: WHAT *CAN* WE DO THIS YEAR?

- **We can review relevant parameters in the existing signers, like**
  - Key pre-publication strategy
  - Signature lifetimes and zone-wide re-sign intervals
  - ZSK rollover policies
  - TTLs

- **We can test the performance implications of a roll to algorithm 8**
  - A more incremental step than we'd wanted, but gets us away from SHA1.
  - We've already done most of this, in fact, and the differences were negligible

- **We can test the robustness of the algorithm rollover in the current signer**
  - We could do this in private and publish the results
  - We could run a public testbed

- **We can do a dry run in some smaller TLDs**
  - While we would take full precautions with *any* TLD, no matter how small, the impact of a problem in a much smaller TLD would be easier to mitigate and would affect far fewer end-users

- **We can do communications, outreach and coordination with researchers**

SUDDENLY, IT'S MARCH 235TH

- **We did a lot of outreach to various audiences**
  - RIPE dns-wg, May 2020 and Sept. 2020
  - DNS-OARC, June 2020
  - ccNSO Tech Day, ICANN 68, June 2020

- **Preparatory Work carried out by our Back-End Registry Services Provider**
  - A roll from 7 to 8 was feasible, even with the lower risk tolerance of the new world
  - Successful Lab testing of a roll from 7-8 using the same signer platform
  - Production roll from 7 to 8 using the same signer platform but for a different, small new gTLD

- **Published plans to 40 people subscribed to our org-algorithm-roll list**
  - Subscribed following earlier presentations: people listening!
  - Substantially technical audiences
  - Finalized details of incremental steps in the roll, with dates, over the summer

- **A less ambitious plan for a less forgiving time**
  - Now is not the time to "mess around"
  - Dress rehearsal for a future time when there's more room for bigger changes

THE STEPS

- **Week Ending 9/25 (schedule built by PIR and Afilias):**
  - The new Algorithm 8 KSKs were added to each zone.
  - The new Algorithm 8 ZSKs were added to each zone.
  - The DNSKEY RRSet signed by both the algorithm 7 and algorithm 8 KSK for each zone.
- **Week ending 10/9:**
  - The old algorithm 7 KSK record was removed from the DNSKEY RRSet
  - The DNSKEY RRSet is no longer signed by the algorithm 7 KSK.
- **Week ending 10/16:**
  - The old algorithm 7 ZSK record was removed on Thursday, 15 Oct 2020 from the DNSKEY RRSet.
  - The superfluous ZSK-based RRSIG on the DNSKEY RRSet has been removed.
- **Current state:**
  - Per the diagram in RFC 6781, .ORG remains in the “DNSKEY Removal” step
  - Next week, the old algorithm 7 based zone RRSIGs will be removed, which will complete the algorithm roll.
- **We’ve got this….**
  - Surely no other global problems can emerge this year, right?
  - (Fingers crossed for a few more days.)
  - All told, this has taken 11 years. Or 8 months. Or 5 weeks.
  - Main lesson: proceed cautiously, but proceed.

Questions?

Joe Abley <jabley@pir.org>
Suzanne Woolf <swoolf@pir.org>