DNSSEC Non-deployment, What Can be Done?

Edward Lewis
ICANN

RIPE 87 DNS WG Session
29 November 2023

A little history DNSSEC, for perspective

- ~1990, a researcher reported cache poisoning as a vulnerability in the DNS
- ~1993-~1998, work within the IETF, implemented by a contractor developed the first two versions of DNSSEC
- 1 April 1998 (IETF 41) a small meeting addresses “why is no one using DNSSEC?”
- An effort to fix and promote DNSSEC began
- 25 years have passed, we still ask this question: “Why is almost no one using DNSSEC?

A realization

- The assumption has been that operators need more education, more training, more tools, more complex processes to automate DNSSEC. “We need a business case!”
- Measuring deployment of RPKI over the past few years show that it too has been slow going
- Maybe, just maybe, the problem isn’t operators, it’s the protocols
  - I mean, it’s a pattern, it’s not only DNSSEC that suffers low deployment, many new improvements do

Presentation Expectation Setting

- This slide deck is presenting observations, not solutions
- The goal is to kick off and/or continue discussions to improve the state of DNSSEC
  - Raising deployment numbers is not the primary goal
  - Raising the usefulness of DNSSEC is the goal, which ought to result in a rise in deployment numbers
- I'm still in learning mode, I hope for this to start conversations

Operators are not all the same

- The label “operator” covers many groups
  - DNS hosting service operators (commercial, multi-tenant)
  - ISP operators, serving recursive DNS and some hosting
  - Top-level domain and RIR operators (driven by a database)
  - Public DNS (public recursive service) providers
  - Individual operators (do-it-yourself)
  - In-house operations (run as part of a larger organization)
- Operators may be
  - Experts in delivering a service, not matter what it is
  - Experts in the service they deliver (DNS operator)

What do operators want?

- I'm not an operator so my opinion (alone) is probably wrong
- But I've been talking with operators, used to work with some, and have learned quite a bit and this is ongoing
- Operator Goals
  - Rule #1 – Keep it running!
  - Rule #2 – When it breaks, get it running fast!
- Keeping in mind, operators don't necessarily decide what to run, some are tasked to run something for someone else

Does this mean operators won't change things?

- Operators do make changes – tech-refresh is one example
- Part of Keep It Running means maintenance over long timescales
- What are the rules for making an operational change?
  - Reason #1 – It increases or preserves value (revenue) of the service
  - Reason #2 – It decreases resources needed (cost) of providing the service
- Hidden here – operators provide services, value to customers (their customers own the service, relying customers consume)

DNS Operators

- The DNS field is only about 20-25 years old, which is coincidently about the same as the DNSSEC deployment era
- DNS operations is still evolving, has become a subset of operations-in-general
- A reason why DNSSEC is hard to operate is that it was designed before DNS operations was an established field
  - The DNS itself is no operator “joy ride”
- Maybe just about everything about DNSSEC ought to be refactored given DNS operations experience

Operational Reality

- Operators are staffs of humans
  - Employees change jobs, even from one operator to another
  - Training a new person must be simple
  - Timing of activities (like key rolls) is influenced by staff retention time
- Operators report to service owners or service regulators
  - Many unique situations exist, operators may have to work around specific guidelines unrelated to technical needs
- Operators face a wide range of environments

What would make a protocol deployable?

- I'm not entirely sure yet, still working on it, but here are clues:
  - Simplicity: when it is clear what has to be done, it's easy to manage it
  - Clarity: when it breaks, it is easy to isolate the root cause and determine the path to recovery
  - "Complexity causes centralization" – observation from one operator, if it takes an expert to manage it, few can manage
- Consider these as "sound bites" – overall qualities in what ever is needed to improve the state of DNSSEC

Back to DNSSEC, where did it go wrong?

- The ideals of DNSSEC are solid
  - Authenticity of data in a response (the “truth”)
  - Integrity of data in a response (the “whole truth”)
  - Signing negative answers (including secured NXDOMAIN!)
- In the 1990’s
  - Solid understanding of the DNS protocol (beyond documents)
  - Solid understanding of digital signatures
  - Solid understanding of scalable key distribution
- Still it went wrong
  - Already mentioned we didn’t have operations to build upon

1990's Network Environment

- Host security extremely weak
- Zone administrators ran everything, their own servers
- End-to-end networking still the norm
- Network abuse was "DoS" (not yet DDoS)
- Cryptography
  - Code availability
  - Patents
  - Legal restrictions

1990's Network Environment – Host Security

- Weak host security led to a rule against on-line private keys
  - All signatures must be pre-computed
  - For negative answers, could not include the query in the response
  - Hence NSEC and NSEC3's approaches
- What if we have on-line keys?
  - Some commercial service providers have this already
  - Tailored-to-the-query responses mean no re-fits to NSEC/NSEC3
  - Stretching – could improve internal zone storage, response rates

1990's Network Environment – Zone administration

- DNSSEC was designed assuming the zone admin did everything, maintain and sign the data, run servers and interact with the parent zone
  - The parent-child relationship was assume to be direct (no registrars)
- What if we recognize roles of registrars and DNS hosters?
  - Registrars have EPP for provisioning, why not DNS hosters?
  - Can Zone admin (registrant) designate a DNS operator? More than one DNS operator?

1990's Network Environment – Zone administration, more what if?

- What if DNSSEC came after EPP?
  - We could push child-parent provisioning into an appropriate channel
  - Dynamic Update might be an acceptable alternative to EPP, perhaps its role in provisioning DNSSEC might have been enlarged
    - Dynamic Update was used to provision delegation information in registries, with IXFR used to update servers
  - Might not need a KSK/ZSK split in keys

- Secure Dynamic Update is an DNS mechanism for provisioning
  - Perhaps an alternative to the more-generalized EPP

1990's Network Environment – End-to-end networking

- End-to-end networking was threatened (and it's gone now)
  - Middleboxes or firewalls
  - Enforcing expected behaviors limits innovation
  - Expectations include DNS over UDP, 512 byte limit
    - We've won that specific battle, mostly
  - Fragmentation (of UDP) has become a concern
- What if we could move to a stream-based DNS protocol?
  - New transport (binding) would have new expectations
  - Size limits, fragmentation would not be as concerning
  - Although stream-based protocols would mean more load on servers

1990's Network Environment – Network abuse was DoS not DDoS

- The threat model didn't foresee DDoS
  - DDoS is boosted by DNSSEC via larger response sizes
- What if we were more concerned by response size?
  - Digital signatures will add size to an unsigned response
  - It's possible to limit the gain
  - However, in post-quantum, might not be able to do this
  - Of course, post-quantum is still an unknown world
  - Significance of double-signing to algorithm roll, multi-signer

1990's Network Environment – Cryptography

- Code availability
  - There was no OpenSSL or other generally available software libraries
  - Hardware Security Modules weren't known (if they existed)
- Patents
  - RSA had a patent over it until the late 90's
  - Only DSA was available during initial protocol development
- Legal restrictions
  - Cryptographic technology was subject to export restrictions

1990's Network Environment – Cryptography – What if?

- What if we knew more about having multiple DNSSEC Security Algorithms at once? Changing from one to another?
- What if we knew there would be a "basket" of widely known, commonly available algorithms?
- What if we knew operators would "go simple" and choose just one DNSSEC Security Algorithm at a time?

Where Do We Go From Here?

- What needs to be solved?
  - To improve the deployment of DNSSEC, address operator needs
  - Child-parent provisioning (DNSKEY/DS record)
  - Multiple-back end provider use cases
  - Switching algorithms
  - Avoiding mistakes
  - Recovering from mistakes (Mean Time To Repair or MTTR)

Different Ways to Get There

- First, we do need to know where ”there” is
  - A notion of “requirements”
- Tweak current records to handle new assumptions
  - Fast, records are deployed, but code still needs to be rolled out
  - Causes uncertainty in debugging, don’t know if code is old or new
  - Examples: IETF “compact denial” and “generalized notify”
- Create new records and code paths
  - Clean start, clearer
  - But needs new code to roll out, and a transition plan/motivation

A Consideration

- The IETF delivers documents describing protocols
  - Request for Comments
  - These are sort of specifications, perhaps erring on too general
  - Guides for software developers
- Missing: Operational Profiles
  - There are operational guides
  - Describing default settings, current operationally active parameters
- Perhaps there is a need for an operational profile series for DNSSEC (and other parts of DNS)
  - A way to simplify the choices to be made in operations

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: edward.lewis@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg