Another Way To Chain: NSDS

Dan Kaminsky

Chief Scientist

Recursion Ventures

The Good News

- The DNS Root is being signed!
  - DNS has scaled magnificently for 25 years by there being one agreed upon root
  - DNSSEC can share in the scalability by having only one set of keys to trust
- DNSSEC can actually be pretty simple now
  - Before: Ask a question, get an answer
    After: Ask a question, get an answer and a signature
  - Before: Ask a question, get a referral
    After: Ask a question, get a referral and a signature

A Slight Complexity

- Referrals now contain DS records
  - Before: “Here is the next host to talk to.”
  - After: “Here is the next host to talk to, and here’s the key to expect.”
- Really, this is *very much just like normal DNS works*
  - Everyone wants DNSSEC to be this big crazy thing.
  - Really, it’s just DNS with keys. That’s why it’s going to work.

Building A Chain

- Getting the key into the root was a bit tricky, but we did it
  - 6 hours in Culpeper, Virginia, USA
- Getting DS records from TLDs to the root appears relatively straightforward
  - Not *that* many TLDs, and there are direct relationships

A Temporary Issue

- Getting DS records from SLDs to TLDs is being a little bit of a headache
  - Registrar/registry split means there are no direct relationships
  - Under this split, there are two kinds of hosting
    - "Full" hosting – the registrar runs the authoritative name server
    - "Delegated" hosting – the registrar delegates the zone to the registrant's authoritative name server

State of Secure Hosting

- 1) Very few registrars will have "full" hosting live on July 15th for hosting DNSSEC signed records
  - **This is OK!**
  - **Really!**
  - July 15th is about the root being signed. This is the *start* of an extended process, not least of which is the engineering of much easier to deploy DNSSEC servers
    - What's better than political pressure? Easy to deploy code!

A Temporary Condition

- 2) Only a few registrars will be ready, on July 15th, to absorb the DS records of their delegated customers
  - Only ~20% of the Alexa 10,000 will be able to push DS records. 80% will not.
  - **This will get better over time.**
  - It is, however, a real impediment for early adopters.

How Technologies Grow

- Early Adopters are key
  - Code does not come out of nowhere.
  - The game is to provide this relatively small community a relatively vast frontier for innovation
  - There is a **lot** of ground to cover with DNSSEC
  - When is it ready for people to start playing with it?

The Date

- July 15th, 2010.
  - Ready or not, here they come.
  - One way or another, we should be ready for them.
  - We just did a tremendous amount of very good work! And we, like it or not, are going to get a tremendous amount of press for it.
  - **Is it possible for us to make sure early adopters can still participate, even if their particular registrar hasn't upgraded yet?**

Introducing NSDS

- Consider the NS Name
  - Always supplied by the user
  - Always opaque to the registrar
  - Always submitted to the registry via a secure path (EPP)
    - This path respects the registrant/registrar relationship!
- Consider the DS record
  - DS records are not complicated
  - Three ints and a hash string.
- **A DS record can pretty easily fit into a NS Name.**

Bits and Bytes

- **nsds-v1-60485-5-2-D4B7D520E7BB5F0F67674A0CCEB1E3E0614B93.nsds-C4F9E99B8383F6A1E4469DA50A.domain.com**
  - No label allowed to exceed 48 bytes
  - Total length well below 256 character limit
  - Versioning allows upgrade
  - Metadata (60485, 5, 2) only present on leftmost label
  - This is essentially a port to DNSSEC of one of Dan Bernstein's ideas for DNSCurve

The General Idea

- The general idea
  - A specially formatted NS Name is sent through the registrar, through EPP, to the registry
  - The registry detects the specially formatted name, and expands it inline as if there was a DS record in the submission

The Perfect Is The Enemy Of The Good

- This isn’t the most perfect thing that has ever been proposed
  - That’s OK. The Internet doesn’t really run on the most perfect technologies, does it?
    - Token Ring
    - ATM

Still Need To Work With Registrars

- NSDS doesn’t at all obviate the need to work with registrars
  - We still need to work towards full hosters signing all their records
  - First class support for DS transfer is better than a failsafe
  - Easy to sunset the failsafe at the (now fully compliant) registrar

This is really easy to implement.

- There is one moving part
  - The registry
- There is one point of code modification
  - The EPP parser
- There is very little code to write
  - There are hard things to do in this world
  - Writing a translator between NSDS and DS is not one of them.
    - Three ints and a hash string.
- We get 100% feature compliance
  - The output is fully functional
  - The input is fully secure

Bottom Line

- A choice
  - We can go live for 20% of early adopters
  - We can go live for 100% of early adopters
- No matter what, the signing of the root is a revolution for opening DNSSEC up for business
  - This small bit of code would win us 5x the support on Day One
  - Over the next year, many things will happen to make DNSSEC more exciting and less expensive to deploy
    - The more early adopters, the faster this happens
  - **We can have 5x the early adopters!** But we need this small change.