DNSSEC – It's Still a Journey Until We Reach the Destination

Edward Lewis

Neustar

ccNSO Panel, Cairo ICANN meeting

DNSSEC - why "now?", again

- Since the dawn of the protocol the DNS could be poisoned by an attacker winning a race
- As DNSSEC matured the race became harder for the attacker to win, too hard to make DNSSEC worth it
- But this summer someone changed the rules of the race and attackers now win consistently and DNSSEC is "worth it"

Is DNSSEC ***now*** the answer?

- DNSSEC hasn't changed, the environment has
  - But has cobwebs to dust off
- Can we "dodge" DNSSEC with something else?
  - Short term treatments, but no replacement
- Can't we just ignore the new (summer) threat?
  - Attacks are already a concern

Where is the *SuperDNSSEC* hero?

- The superhero cape and tights not quite ready
  - Software and operations are largely untested
  - A significant element (NSEC3) is not available in any ***production ready**** code base
  - Few registries have experience with DNSSEC and those with - only with "early adopter" registrants
  - Operations and process for signing, registration, validation are mostly undefined and untested
  - No one should role out anything until ***tested!***

Fitting the cape and tights

- Or, why is it still a journey to the destination?
  - We need to have a signed root, TLDs
    - It's only a start, has proven to be a "must"
  - We have to make sure the DNS supply chain elements are individually incented to deploy DNSSEC
    - Registration process (registrars), DNS service providers
  - We have to get the "end" players up and running
    - Enterprises, ISPs (on behalf of their customers)

"Sign the root and TLDs!!!"

- A nice mantra, but...
- Mantras do not get work done
  - **Registrants** have to sign/maintain their data
  - **Registrars** need to convey DNSSEC data
  - **ISP**s have to manage DNSSEC keys in caches
- "Sign the root and TLDs" is not enough!

What's a registry to do?

- Non-technical chores
  - Managing expectations
  - Helping incent (motivate) the registration chain
- Technical chores
  - Database, Registration, DNS, WhoIs, Billing
  - Examine operations of DNSSEC
  - Cryptographic key management
- Don't just solve for DNSSEC, solve for security

Managing Public Expectations

- Government agencies want security
- Anti-crime groups want protection against things like phishing, spam and such
- Net operators want protection against DDoS
- Some groups want privacy protection
- People want a reliable means of conducting commerce and getting entertainment

Incent the Registration Chain

- Fundamental rule: a (successful) change must do at least one of two things
  - Decrease cost of operations
  - Increase benefit of services
- DNSSEC costs need to be identified
- DNSSEC benefits recognized for all players
  - For some it is "clear", for others (registars) it is not
  - Individually, not just "it is good for the Internet"

Engineering Changes

- The DNS "job" will grow
  – Not just loading DNS from the database
  – DNS contents will need to be actively maintained
- DNS data (in memory/disk) and traffic grow
- New registration data fields, interfaces
  – Besides name servers, now need DNSSEC data
- May impact billing, whois, other services
  – No common recommendation here

Operational Considerations

- Management of Cryptographic Data
- Interacting with the IANA on DNSSEC data
- Signing data as it changes
- Refreshing signatures on unchanged data
- Will NSEC3's "Opt-In" be deployed?
- Be sure your service providers are ready too

Testing Changes

- Internal testing
- Testing with IANA's interface for reporting
- Have a plan for roll out and roll back
- Permit your customers (registrars) to engage in testing before they open up for business

Non-Registry Elements

- There are the elements of the DNSSEC equation beyond a registry's reach
- Registries can't do anything about this but
  - DNSSEC won't be effective until the enterprises sign their data (and they do want to)
  - DNSSEC won't be effective until the ISPs install the keys to protect the caches (and they do want to)
- All that can be done here is "encouragement"

Why is DNSSEC still a journey?

- We don't have a signed root zone
- Tools availability is still limited
- Need to fit it into operations
- Internal testing, external testing
- Establishing a supply chain for DNSSEC data

- Could be looking at 12-18 months before widespread deployment of DNSSEC

What's a Registry to Do ***Now***?

- Manage Expectations
- Understand Costs
- Understand Benefits
  - – Registries have unique arrangements
- Fight attacks in the meantime
- Make sure their operations supporters are ready for DNSSEC

NeuStar Plans

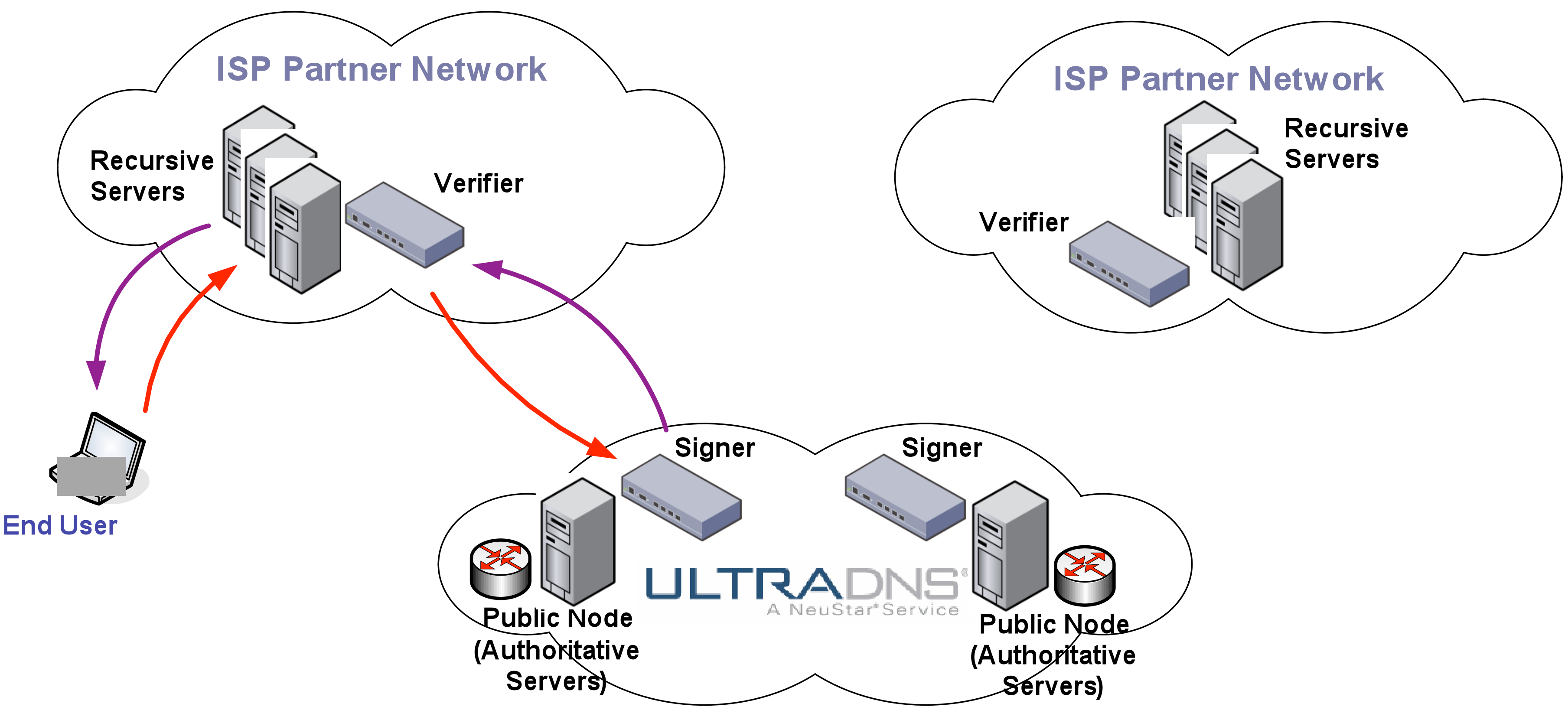
- Until summer, a patient stance on DNSSEC
  - "Cost versus benefit" balance now favors DNSSEC
- Support customers who are early adopters
  - Identifying ways to protect our customers sooner
- Immediate plans
  - Deploy a new service called **CacheDefender** to provide protection in advance of widespread DNSSEC

CacheDefender

- A new service protecting DNS traffic between participating recursive servers and NeuStar's UltraDNS servers
  - Hardware installed in front of both ends
  - Queries and responses cryptographically signed
  - Keys managed by NeuStar
- Protection extended to all zones as they are hosted on our servers

CacheDefender Architecture

***Cache Defender* Network Architecture**



Features of CacheDefender

- Deployed security while the DNSSEC journey continues
  - Not a replacement for DNSSEC
  - Point-to-point security
  - Increment to Neustar's provided services
- End-to-end protection that works with existing DNS network transport
  - Invisible to non-NeuStar hosted DNS

Out of Slides

- I believe the Q&A comes next...