DLV - A decade on

Useful migration tool
Dangerous distraction
YOU DECIDE

Copyright 2007 bill manning
Some History

• The ideas behind DLV were originally / independently conceived by David Conrad and Bill Manning in the 1996/1997 timeframe.

• There was a concern that DNSSEC dependence on being able to reach a valid trust anchor, canonically the root, would become a “show-stopper” for DNSSEC deployment.
lookup chain

- As used by all Iterative Mode Resolvers (aka Caching Servers) - Start at the Root and work down to the Leaf
- The default path used by Validation (makes sense) - Start at the Leaf and work up to the Root (or Trust Anchor)
- The idea of a single Trust Anchor is the ideal in an always on, always connected network. The practical reality is that for robustness, most sites will maintain several Trust Anchors

Copyright 2007 bill manning
Question:
www.ep.net A

Lookup Chain

1. Resolver
   www.ep.net A ?
2. Iterative Mode Resolver (recursive)
   www.ep.net A ?
3. root-server
   “go ask net server @ X.gtld-servers.net” (+ glue)
4. gtld-server
   www.ep.net A ?
5. “go ask ep server @ ns.ep.net” (+ glue)
6. ep-server
   www.ep.net A ?
7. “198.32.6.80”
8. 198.32.6.80
9. Add to cache
Question:

TA for www.ep.net

1. www.ep.net 5137
   Is this a TA?

2. ep-server
   “go ask DS-6722”

3. www.ep.net TA?

4. www.ep.net TA?
   “go ask DS-1244”

5. www.ep.net TA?
   “go ask DS-6722”

6. www.ep.net TA?

7. “TA is 3995
   root-server

8. 3995

9. Add to cache

Copyright 2007 bill manning
Question: Validation Chain with DLV

TA for www.ep.net

1. www.ep.net TA?

2. 3995

3. www.ep.net TA?

4. Add to cache
   “TA is 3995”

5. 3995

Resolver

Validator (DLV)

DLV server

root-server

DS-6722(gtld)

ep-server

Copyright 2007 bill manning
Any Problems?

• What is YOUR business relationship with the DLV registry?
• When to “Jump” to the DLV registry?
Where is it defined?

- Two specifications:
  - “Preventing Child Neglect in DNSSECbis Using Lookaside Validation”; Paul Vixie, ISC, October 2004
- IETF’s RFC 4431, February 2006
- draft-weiler-dnssec-dlv-01.txt, Samuel Weiler, June 2006
- THE PREDOMINANT IMPLEMENTATION most closely follows the ISC TechNote

Copyright 2007 bill manning
Who is promoting DLV

• No apparent call for this type of service from the community - ISC driven
• There are at least five DLV registries in service now, many more can come into existence - no prior coordination with other registries is required
  – ISC implementation presumes a single DLV registry
  – No guidance on how to deal with multiple DLV registries
• DLV support has been in BIND for almost three years now.
Analogies

- The DNSSEC trust hierarchy is similar to a Certification Authority/Hierarchy.
- DLV is mostly similar to a “Web of Trust” - aka PGP.
Risks

• Users are completely dependent on:
  – ISC good will (ISC will kill DLV “when the need passes”)
  – Reachability to the DLV registry
• No registry has published Key Management rules.
  – How they protect Keys
  – Service Level Agreements
• Without DLV, are folks content with the USG being the sole signer of the root?
• All validation queries, except EXACT matches, hit the DLV registry server. High probability of server failure
Rewards

• IF you have a parent who refuses to take your DS, then a DLV registry may adopt you.

• DLV registry gains a view of parts of the tree which are signed and can be validated. For DNSSEC purposes, they become the defacto alternate root for validation purposes.
NO-OP

- No current application (save research work) does validation
- Signing and Key Management for a delegation are the hard parts - no DLV registry is needed, let alone required
My thoughts

• DLV is a nifty idea with limited practical value in today's DNS architecture

• **The risks are real**

• There is minimal value to the DLV registrant to use a DLV registry... most of the value derives to the registry

• It may be better to use resources to persuade your parents/children to use DNSSEC than “opt-out” into a third-party trust chain.

• Adding a DLV registry to your TA-list might be a reasonable short-term aid.