DNSSEC Look-aside Validation

Internet Systems Consortium

May 4, 2009

Description

- DLV is a local policy choice for resolver operators
- DLV acts as a last-resort method to discover secure entry points into a DNSSEC island
- DLV will not replace configured trust anchors
- DLV operations are secured using DNSSEC
- Web interface (https://dlv.isc.org/) allows publishers of DNS data to add, update, or remove secure entry points

Purpose

- An interim DNSSEC deployment mechanism
  - Allows use of DNSSEC with many “islands of trust”
  - Eases resolver configuration headaches
    - One trust anchor to add
    - One trust anchor to track
  - Eases deployment of DNSSEC signed zones
    - One place to add trust information
    - Automatic distribution to all users of DLV
  - DLV tracks prominent TARs, so resolver operators do not need to

DLV Fills a Gap

- Provides an interim method of deploying DNSSEC until key zones are signed
  - The Root
  - The TLDs
  - Sufficient “connectivity” in the root-based DNSSEC chain
- Signing the root is not sufficient to consider DNSSEC deployment complete.
- Policy and technical details need to be performed at each delegation point

Using - Authority

- After signing a zone, it lives in a vacuum unless its parent is
  - Signed
  - Prepared to accept DS records
- Operators of authority servers may choose to publish their DNSKEY records in various ways:
  - Parent
  - Web sites (requiring manual addition/tracking for users)
  - DLV or other Trust Anchor Repositories

Using - Authority

- DLV advantages
  - One place to publish
  - Full control over which keys are published
  - DLV will perform basic sanity checks on zones, which provides a safety check for operators

Using – Recursive

- Add a trust-anchor for dlv.isc.org zone
  - This is a standard procedure for any trust anchor
  - Must track the key to ensure continued operation
- Enable DLV operation using dlv.isc.org zone
  - `options {`
    - `dnssec-enable yes;`
    - `dnssec-validation yes;`
    - `dnssec-lookaside . trust-anchor dlv.isc.org.;`
  - `};`
  - `trusted-keys { dlv.isc.org. 257 3 5 “<key data>”; };`
  - Latest key data is published on

Operational Details

- DLV relies heavily on “aggressive negative caching”
- Each query a resolver receives will generate one or more query into dlv.isc.org
  - Asking for www.isc.org will generate the following queries, assuming nothing is found along the way:
    - www.isc.org.dlv.isc.org DLV
    - isc.org.dlv.isc.org DLV
    - org.dlv.isc.org DLV
    - dlv.isc.org DLV

Operational Details (cont)

- Using aggressive negative caching, a resolver will quickly cache enough entries to avoid asking many queries into dlv.isc.org
-

Recent Improvements

- dlv.isc.org is served by ISC's SNS@ISC product to ensure DNS query capacity
- Web-based interface for authoritative operators to enable direct control over published data
- Automated TAR tracking including PGP-based verification to ensure freshness of TAR imported data
- Email warnings to authoritative operators when problems are discovered (expired sigs, etc)

Recent Improvements

- Hardware upgraded to higher powered dedicated signer and web interface servers
- Servers have been physically relocated from ISC at Redwood City to PAIX
- Completion of these takes us into “full production” service
-

Potential Issues

- Increased load on resolvers
  - CPU usage in validating DNSSEC responses
  - Network traffic due to DNSSEC responses
  - Network traffic due to DLV queries
- Problems when dlv.isc.org zone is not reachable
  - ISC serves this on our SNS@ISC DNS service
  - Network outages will generally cause disruption of any DNS service

Future Plans

- More automation on the DLV service
  - RFC5011-style tracking of trust anchors
  - Warnings when signatures are about to expire
- More automation inside BIND 9.7
  - RFC5011 tracking of trust anchors, including those used for DLV
  - Automated signing of DNS zones
  - Automated re-signing as necessary
  - Simplified DNSSEC configuration