DLV Howto

Duane Wessels
The Measurement Factory/CAIDA

October 15, 2007

What Is DLV?

- DNSSEC Look-aside Validation
- A way to authenticate DNS records/zones before the root and TLD zones become signed.
- `http://www.aptld.org/meeting/2007/02_Bali/dlv-at-ten.pdf`
- `http://www.isc.org/pubs/tn/index.pl?tn=isc-tn-2006-1.html`
- `https://secure.isc.org/ops/dlv/index.php`
  - from where most of this talk is lifted

For Zone Owners

- Create a KSK and a ZSK
- Put the keys in the zone
- Sign the zone
- Send your DS RRs to a DLV registry
- Wait
- Test

Create a KSK

```
$ dnssec-keygen \
        -r /dev/random \
        -f KSK \
        -a RSASHA1 \
        -b 1024 \
        -n ZONE \
        life-gone-hazy.com
Klife-gone-hazy.com.+005+42217

$ cat Klife-gone-hazy.com.+005+42217.key
life-gone-hazy.com. IN DNSKEY 257 3 5 AwEAAdcNkWB6m ... KVIH5q3j
```

Create a ZSK

```
$ dnssec-keygen \
        -r /dev/random \
        -a RSASHA1 \
        -b 1024 \
        -n ZONE \
        life-gone-hazy.com
Klife-gone-hazy.com.+005+11622

$ cat Klife-gone-hazy.com.+005+11622.key
life-gone-hazy.com. IN DNSKEY 256 3 5 AwEAAbxTXHa4p ... OHQSARlH
```

Put the keys in the zone

```
# co -l /etc/namedb/master/life-gone-hazy.com

# cat Klife-gone-hazy.com.+005+*key >> /etc/namedb/master/life-gone-hazy.com

# rndc reload
server reload successful

# ci -u /etc/namedb/master/life-gone-hazy.com

$ dig +short @127.0.0.1 life-gone-hazy.com dnskey
256 3 5 AwEAAbxTXHa4p ... OHQSARlH
257 3 5 AwEAAdcNkWB6m ... KVIH5q3j
```

Sign the zone

```
# dnssec-signzone \
        -l dlv.isc.org \
        -r /dev/random \
        -o life-gone-hazy.com \
        -k Klife-gone-hazy.com.+005+42217 \
        /etc/namedb/master/life-gone-hazy.com \
        Klife-gone-hazy.com.+005+11622
/etc/namedb/master/life-gone-hazy.com.signed

# $PAGER /etc/namedb/master/life-gone-hazy.com.signed

# $EDITOR /etc/namedb/master/life-gone-hazy.com.signed
    (increment serial)

# $EDITOR /etc/namedb/named.conf

    zone "life-gone-hazy.com" {
        type master;
        file "master/life-gone-hazy.com.signed";
    };

# rndc reload
server reload successful

$ dig +short @127.0.0.1 life-gone-hazy.com rrsig
;; Truncated, retrying in TCP mode.
SOA 5 2 3600 20071111202739 20071012202739 11622 life-gone-hazy.com. s1WN63w9 ... uaE=
```

Send the DLV RRset to ISC

```
$ mail dlv-registry@isc.org < dlvset-life-gone-hazy.com.
```

- Or another DLV registry?

Wait

- What next?
- ISC will authenticate you. How?

Configure DLV in your resolver

- BIND 9.3.3 or later
- `--with-openssl`
- Secondary nameservers must also support DNSSECbis
  - Otherwise you get "CNAME and other data" errors.

Fetch ISC's key

```
$ cd /tmp

$ wget http://www.isc.org/ops/dlv/dlv.isc.org.named.conf
$ wget http://www.isc.org/ops/dlv/dlv.isc.org.named.conf.asc

$ wget http://www.isc.org/about/openpgp/pgpkey2006.txt
$ gpg --import pgpkey2006.txt

$ gpg --verify dlv.isc.org.named.conf.asc
gpg: WARNING: unsafe ownership on configuration file ‘/home/wessels/.gnupg/options’
gpg: Signature made Fri Sep 21 03:06:53 2007 PDT using RSA key ID 1BC91E6C
gpg: Good signature from "Internet Systems Consortium, Inc. (Signing key, 2006) <pgpkey2006@isc.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 445B 7704 FB95 28F3 882D  D8D3 2334 124E 1BC9 1E6C

$ sudo mv dlv.isc.org.named.conf /etc/namedb
```

- PGP Web of trust, etc, etc...

Add the ISC DLV key to named.conf

```
# vi /etc/namedb/named.conf

    options {
        ...
        dnssec-enable yes;
        dnssec-validation yes;        // BIND 9.4 and later
        dnssec-lookaside . trust-anchor dlv.isc.org;
    };

    include "dlv.isc.org.named.conf";

# named-checkconf
```

Sanity Checks

- Make sure your firewall allows port 53 TCP!
- Make sure your firewall accepts IP fragments!

Test

```
# dig +dnssec isc.org soa

; <<>> DiG 9.3.4 <<>> +dnssec isc.org soa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43626
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;isc.org.                       IN      SOA

;; ANSWER SECTION:
isc.org.                3525    IN      SOA     ns-int.isc.org. hostmaster.isc.org. 2007101400 7200 3600 24796800 360
isc.org.                3525    IN      RRSIG   SOA 5 2 3600 20071112233224 20071013233224 32934 isc.org. GjfPQRRHaPS

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Oct 14 10:39:00 2007
;; MSG SIZE  rcvd: 257
```

Debugging

```
logging {
   channel dnssec_log {
        file "/var/log/dnssec.log" size 20m;
        print-time yes;
        print-category yes;
        print-severity yes;
        severity debug 3;
    };
    category dnssec { dnssec_log; };
};
```

```
14-Oct-2007 10:35:57.877 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: looking for DLV isc.org.dlv.isc.org
14-Oct-2007 10:35:57.877 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: DLV isc.org found
14-Oct-2007 10:35:57.877 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: dlv_validator_start
14-Oct-2007 10:35:57.877 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: restarting using DLV
14-Oct-2007 10:35:57.877 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: attempting positive response validat
14-Oct-2007 10:35:57.877 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: dlv_validatezonekey
14-Oct-2007 10:35:57.877 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: Found matching DLV record: checking
14-Oct-2007 10:35:57.878 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: verify rdataset (keyid=32934): RRSIG
14-Oct-2007 10:35:57.878 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: verify rdataset (keyid=52849): succe
14-Oct-2007 10:35:57.878 dnssec: debug 3: validating @0x81d5800: isc.org DNSKEY: marking as secure
14-Oct-2007 10:35:57.878 dnssec: debug 3: validator @0x81d5800: dns_validator_destroy
14-Oct-2007 10:35:57.878 dnssec: debug 3: validating @0x8220000: isc.org SOA: in fetch_callback_validator
14-Oct-2007 10:35:57.878 dnssec: debug 3: validating @0x8220000: isc.org SOA: keyset with trust 7
14-Oct-2007 10:35:57.878 dnssec: debug 3: validating @0x8220000: isc.org SOA: resuming validate
14-Oct-2007 10:35:57.879 dnssec: debug 3: validating @0x8220000: isc.org SOA: verify rdataset (keyid=32934): success
14-Oct-2007 10:35:57.879 dnssec: debug 3: validating @0x8220000: isc.org SOA: marking as secure
```

Final Thoughts

- Keep in mind, when you enable DLV in your caching resolver, the DLV registry gets to spy on your DNS queries!

The End