Pro
DNS
and BIND

Ron Aitchison

APress®

Apress is pleased to present an excerpt from:

Pro DNS and BIND

Ron Aitchison

Book Information
Pro DNS and BIND | Ron Aitchison
Published: August 2005 | ISBN: 1-59059-494-0 | $44.99 US | 608 pages

About Apress
All Apress titles are available at your favorite online and brick and mortar bookstores. Contact Apress at sales@apress.com with any questions.

Apress Inc., based in Berkeley, California, is the fastest-growing publisher of technical books in the world today. It is dedicated to meeting the needs of IT professionals, from novice to expert. Apress is dedicated to publishing titles of the highest quality and has compiled a team of authors that is a "Who's Who" of the high-tech industry.

Apress®
THE EXPERT'S VOICE™

Contents at a Glance

PART 5 ■ ■ ■ Programming

PART 6 ■ ■ ■ Appendixes

DNSSEC Lookaside Validation

The DNSSEC Lookaside Validation (DLV) service is an alternative method by which a chain of trust may be created and verified without the need to sign the parent zone file. The service makes use of a DLV RR, which is not currently defined by an RFC—its status is therefore experimental—but which is fully supported by the current (9.3+) versions of BIND. The DLV RR is functionally identical to the DS RR and may be generated by the `dnssec-signzone` utility by use of the `-l` domain-name option (see Chapter 9). A DLV RR is placed in a special signed zone called a *lookaside zone* instead of the DS RR that would normally be added to the parent zone, thus removing the need to sign the parent zone. The DLV service works by providing an alternative method to verify a chain of trust as described next.

Assume that the lookaside domain is called `dlv.example.net` and the name server is trying to verify the chain of trust for the signed zone `example.com`. In a normal sequence, when a security-aware name server tries to verify the chain of trust for `example.com`, it will first check for a trusted anchor in its `trusted-keys` clause, and if one is not found, it will issue a query to find a DS RR at the parent `.com` zone. If neither is found, the zone will be marked as insecure. DLV adds an additional step by allowing the name server to query a lookaside zone, for which it must have a trusted anchor, for the DLV RR of the zone being verified. When the verifying name server detects that the lookaside feature is enabled (by a `dnssec-lookaside` statement in `named.conf`), it will issue a DLV query with the domain name `example.com.dlv.example.net`, which, if found, and assuming the trusted anchor for `dlv.example.net` is present in a `trusted-keys` clause, the `example.com` zone is verified to be secure. Figure 11-7 illustrates the DLV process.
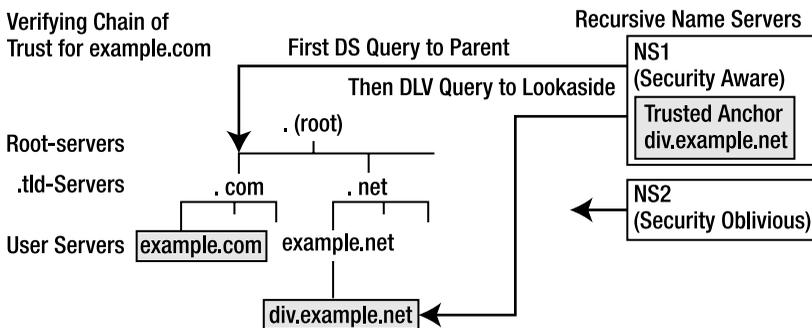

Figure 11-7. *DLV verification procedure*

The initial query will try to find a DS RR for `example.com` at the parent `.com` zone and only if that fails will the DLV query be issued to the lookaside zone. While the lookaside zone

`dlv.example.net` must be signed, the trusted anchor at NS1 means that its parent, `example.net`, does not have to be signed, as is shown in Figure 11-7.

A public pilot of DLV is currently being run by VeriSign Labs, a division of VeriSign, Inc. (`www.verisignlabs.com`), which covers *all* of the TLDs with a single trusted anchor, without the need for any of the TLD zones to be signed.

DLV Configuration

This section describes the various steps to be taken when joining the zone `example.com` to a DLV chain of trust. While the specific example of the VeriSign Pilot is used, the explanations cover the general case wherever appropriate. The lookaside zone for the VeriSign Pilot is `dlv.verisignlabs.com`.

The DLV system, like all other DNSSEC systems, starts with a signed zone. The `example.com` zone is signed in the normal way as described earlier using the `dnssec-signzone` utility with the addition of a `-l dlv.verisignlabs.com` option to create a DLV RR with the correct name (`example.com.dlv.verisignlabs.com`). Creation of this DLV RR is the only reason the zone needs to be re-signed. This step is actually not required for the current VeriSign Pilot project, which creates 'the DS' RR automatically when a zone is submitted for addition to the pilot project. The process is described in full, since other DLV services may, however, require a DLV RR to be supplied.

Assuming the same configuration as the last example but using only the new KSK from the rollover (`key-tag` is `50148`), the zone signing would use the following command:

```
# dnssec-signzone -o example.com -t -l dlv.verisignlabs.com \
-k Kexample.com.+005+50148 master.example.com Kexample.com.+005+39539
master.example.com.signed
Signatures generated:                    20
Signatures retained:                      0
Signatures dropped:                       0
Signatures successfully verified:         0
Signatures unsuccessfully verified:       0
Runtime in seconds:                   0.357
Signatures per second:               53.079
```

As noted previously, joining the VeriSign Pilot does not require a DLV RR, and since this is the only reason for re-signing the zone, it may be omitted if that is the only objective. The \ indicates that the line has been split for presentation reasons only, meaning the first and second lines actually appear as a single line to the operating system. The `-l dlv.verisignlabs.com` argument defines the name of the lookaside zone that will be appended to this zone name (defined by the `-o example.com` argument) when the DLV RR is created. This option causes `dnssec-signzone` to create a new file called `dlvset-example.com.`, which contains a formatted DLV RR as shown here:

```
example.com.dlv.verisign.com. IN DLV 50148 5 1 (0CAE34D
    C1BDE4A5D12A777A8DEC3B703E516DC71)
```

This DLV has been edited to use multiple lines using the normal zone file method of enclosing in parentheses for presentation reasons only, and from inspection and comparison with the DS RR from the previous example files, it may be seen to be functionally identical.

Depending on the operational or business requirements of the lookaside zone service operator, the DLV RR may need to be sent by a secure process. While the data itself is not sensitive, secure transmission allows the recipient to authenticate the *sender*, not just the data. In the case of the VeriSign Pilot, the DLV RR is synthesized when the zone is registered on the project's secure web site (https://www.dlv.verisignlabs.com). The submitted zone is inspected by VeriSign software by querying for DNSKEY RRs at the zone apex, and it will automatically create and add to its database a DLV RR for any DNSKEY RR with a flags field value of 257 (the SEP or KSK bit is set). This type of procedure may or may not become common practice, but it certainly demonstrates a level of automation that would also be practical for DS RRs.

■**Note** The VeriSign Pilot *requires* that the DLV RR points to a KSK; that is, the DNSKEY RR has a flags value of 257 as described earlier (the SEP bit is set)—therefore a separate KSK and ZSK are required per the recommended practice.

To configure the name server to use the DLV service requires two changes to the named.conf file. The first involves definition of the lookaside zone name (in a dnssec-lookaside statement), and the second requires the inclusion of a trusted anchor for the DLV zone. The trusted anchor for the pilot project (at the time of writing there were two such anchors) may be obtained from https://www.dlv.verisignlabs.com/trusted.html. This is a secure web page, and users are recommended by text on the page to verify the security certificate—a simple but effective authentication process—before using the public keys defined, which may be simply cut and pasted into the named.conf file as shown in the following fragment:

```
// named.conf DLV fragment
...
options {
   ....
   dnssec-lookaside "." trusted-anchor "dlv.verisignlabs.com";
   ....
};
trusted-keys{
dlv.verisignlabs.com. 257 3 5
                 "AwEAAbw2HZErA6PpTSVdEbdvY1I1ly3gTFAhJPAsC7oa
                 tIr/P3hDqz7sUjDy4rVHQPNjKvQMv2vOAqTyrykryO2l
                 9WGmbKZjsXyK219AiAHvSC44TsiskIN8IP28KkM1CWg+
                 1O8FbPJGVbZ3OH1leRapnCCi2Z5qOdhecgFQWag/FupH
                 oqN7snieYsUdby/9ZO9dLDdQeL9xJn1CVtiMcxfB5/ju
                 KJ/V9bF7WIsdLKlootqniS42cjsyGGwxsfZxHQ3mH/GO
                 df1KnGs8ENBnpxSytJk4qOgYP5AkNAPTGOj1Kdma2f9v
                 i6wZAIYVkcQPKusBTYbUclFrIXnKGtPHH3Cny1s=";
dlv.verisignlabs.com. 257 3 5
                 "AQPAQR5KGn12Q/IPhkGMv6ZlAI57rw44/7csvZjuOvWD
                 bFuOGOCwwiRVa7FTh2MQIkCgUjqJ2ZTKTAyBMSadqFoV
                 Cc/CI6CFuQN+inmNNkGZsn5lE8qIoJkMIyl+/vO/OwhL
                 OCurFhObuyNJKouKqoO9wi3pOKrWQRkbnLWlcqeqfsAN
```

```
                    Gpxi27TveSm3x3pS8f9ZXHQvz5yFethXitHDQuYl+apF
                    ODsZ/TfXE9dl7+oR+5hzbzIMbPBByuqna4/ZFCcwJL2W
                    hEArHFQSpkzUaVX2ugBZ48HOM9XqG8aUCkElRAkxrawf
                    5x3bm6y3UmoQPvTQL8T71BZ6Cku84FyDGUoh";
```
```
};
```

The VeriSign DLV Pilot provides support to cover the whole hierarchy of the domain name to the root and therefore recommends a dnssec-lookaside statement with a . (root) domain as shown in the preceding example. The effect of this definition is that every secure zone for which there is no parent DS RR and no trusted anchor will incur a DLV query to the domain dlv.verisignlabs.com, which may be an unacceptable overhead. If the user wants to limit this process to only the .com domain, the following alternative statement could be used:

```
dnssec-lookaside ".com" trusted-anchor "dlv.verisignlabs.com";
```

In this case, only domain names ending with .com will incur a DLV lookup. Similarly, this could have been limited to .at or .org domains or multiple dnssec-lookaside statements used to select only the .de and .org domains, depending on requirement. The trusted anchor name of dlv.verisignlabs.com is unique to the current VeriSign Pilot project and references entries (in the preceding case two) in the trusted-keys clause with the same name.

DLV Service

There is nothing magical about a DLV service. A DLV service uses a standard name server with a standard signed zone file and could be created for use by any affinity group as an alternative to multiple trusted anchors for each member of the group. To illustrate creation of a DLV service, assume an affinity group comprised of the domains example.org, example.com, and example.net decide to set up a DLV service that will hosted by dlv.example.com. In the absence of any special software as used by the VeriSign Labs Pilot, each member domain will create a DLV RR by the zone signing process described using a -l dlv.example.com argument. The DLV RRs are sent to the domain administrator for dlv.example.com by a process that will authenticate the sender, such as secure e-mail. A zone file comprising the supplied DLV RRs will be created as shown here:

```
; zone fragment for dlv.example.com
$TTL 1d ; zone default
$ORIGIN dlv.example.com.
@       IN SOA ns1.dlv.example.com. hostmaster.dlv.example.com. (
                2005032902 ; serial
                10800      ; refresh (3 hours)
                15         ; retry (15 seconds)
                604800     ; expire (1 week)
                10800      ; minimum (3 hours)
                )
        NS ns1.dlv.example.com.
        NS ns2.dlv.example.com.
ns1     A  192.168.254.2
ns2     A  192.168.254.3
; DLV RRs for affinity group
```

```
example.com.dlv.example.com. IN DLV 37558 5 1 (CCCCCCCCCCCC)
example.org.dlv.example.com. IN DLV 42134 5 1 (DDDDDDDDDDD)
example.net.dlv.example.com. IN DLV O2557 5 1 (EEEEEEEEEEEEE)
....
```

A ZSK and KSK for the `dlv.example.com` zone will be created using the `dnssec-keygen` utility and added to the zone file as described earlier, and the zone will be signed with the `dnssec-signzone` utility using both KSK and ZSK as normal. The public key of the KSK for `dlv.example.com` is distributed to be used as a trusted anchor by all the members of the affinity group; thus a single trusted anchor is used to replace the alternative of three trusted anchors, which would otherwise be required.

The zone `dlv.example.com` would be delegated from `example.com` and an authoritative-only name server (see Chapter 7) created to support the service. Finally, each member would add the trusted anchor for `dlv.example.com` in a `trusted-keys` clause in their `named.conf file`, and to invoke the service each member would further add the following three lines to the `options` clause in the same `named.conf` file:

```
dnssec-lookaside "example.com" trusted-anchor "dlv.example.com";
dnssec-lookaside "example.net" trusted-anchor "dlv.example.com";
dnssec-lookaside "example.net" trusted-anchor "dlv.example.com";
```

The specification of `dnssec-lookaside` says that any domain *at or below* the defined domain name will use the lookaside zone defined in the `trusted-anchor` option, which means that only domain names ending with `example.com`, `example.org`, or `example.net` will incur a DLV lookup. However, the specification also says that the *deepest* domain name (which actually means the one with the most labels) defined in a `dnssec-lookaside` will be used for the lookaside query. So if a name server that included the previous three lines also wished to use, say, the VeriSign DLV Pilot service, it would *add* the following statement to invoke that DLV service:

```
dnsssec-lookaside "." trusted-anchor "dlv.verisignlabs.com";
```

The effect of this statement would be that any secure domain that does not end with `example.com`, `example.org`, or `example.net` would incur a DLV lookup to the `dlv.verisignlabs.com` lookaside domain, whereas only our three target domains, `example.com`, `example.net`, and `example.org`, would query the `dlv.example.com` lookaside domain. It is therefore possible to support a number of concurrent DLV services, each of which may target specific markets or affinity groups prior to the widespread availability of signed TLDs.

Summary

This chapter describes the theory and implementation of DNSSEC (colloquially known as DNSSEC.bis), which represents the second generation of standards used to ensure the authenticity and integrity of data supplied from a suitably configured authoritative name server to a security-aware requesting name server. DNSSEC standards use public key (asymmetric) cryptography to ensure that the data supplied in response to a query for, say, `www.example.com`, could only have come from the domain `example.com` (authenticity), that data received by the querying name server is the same as the data sent by the queried name server (data integrity), and that in the event `www.example.com` does not exist, it can be proven that such is the case

(proof of nonexistence or denial of existence). Transaction security, used to secure operations such as DDNS or zone transfer, is covered in Chapter 10.

The chapter described the establishment of islands of security whereby single, unconnected zones may be secured, or a group of such isolated islands that are part of an affinity or common interest group, such as an enterprise network, may be secured. In this case, to get security coverage the zone requires a trusted anchor—the public key used to sign the secured zone—which is obtained by a secure process that authenticates the source and is then configured into all security-aware name servers that wish to validate responses for the zone using a `trusted-keys` clause. Securing the zone involves the use of a private key to digitally sign all the RRsets in the zone using an RRSIG RR type. Once established, secure zones can be linked together into chains of trust using their delegation points; thus if `example.com` is secured, it may be linked to the `.com` gTLD or it may be securely delegated to `sub.example.com`. This process is accomplished using the Delegated Signer RR, which is added to the parent domain and secures the delegation to the child domain. The public keys used in signing are defined in the zone file using DNSKEY RRs and are categorized as either a Zone Signing Key, which is used to sign the records within the zone file and a Key Signing Key, which is used to sign only the DNSKEY RRs used in the signing process and may be used externally as either a trusted anchor or referenced by a DS RR. While the standards allow a single DNSKEY RR to be used for both ZSK and KSK purposes, this not a recommended practice. Proof of nonexistence is provided by the NSEC RRs, which chain together all the RRs within the zone file. Cryptographic keys need to be changed either periodically to minimize risk or immediately in the case where a key is known to be compromised. This process, called key rollover, may use either a prepublish or double-signing strategy, both of which were described. Finally, examples illustrating the implementation of DNSSEC and covering all the preceding points were presented.

DNSSEC provides very positive benefits but does introduce new levels of discipline, particularly with regard to time—signatures (RRSIG RRs) in secured zone file have a finite validity period and thus require to be re-signed at periodic intervals. If the signatures are allowed to expire, the data from the zone will be marked as bogus by receiving security-aware servers.

The next chapter describes, with examples where appropriate, the statements and clauses used in `named.conf`, the configuration file that controls BIND's operational behavior.