TSIG transaction sercurity in BIND

Alessandro Dotti Contra
alessandro@hyboria.org

May 8, 2010

Abstract

This is a dry step by step guide to implement Transaction SIGnature (TSIG) based security transaction in BIND. The discussion refers to BIND version 9.

Generate the shared key for the pair of hosts

The first step is to generate a secret key that will be shared between host H1 and host H2.

You can choose an arbitrary name for the key, but a name like "H1-H2" would be preferred.

The following command will generate a 128 bits HMAC-MD5 key:

```
# dnssec-keygen -a HMAC-MD5 -b 128 -n HOST H1-H2
```

The command will generate two files: one with a private key (.private) and one with the public key. The base64 encrypted string following "Key:" in the private key's file can be used as the shared secret between H1 and H2.

```
YRW4vcK2W9257iSB5rb6RQ==
```

Adding the key to the servers' configuration

For both H1 and H2 you have to edit the `named.conf` to let BIND be aware of the key's existence:

```
key H1-H2. {
  algorithm hmac-md5;
  secret "YRW4vcK2W9257iSB5rb6RQ==";
};
```

You also need to remove world readable permission to the `named.conf` file, or include the statement above in a non world readable file and source it from the main `named.conf` (using the `include` directive).

Using the key

Let's suppose H1's address is `192.168.1.1` and H2's address is `192.168.1.2`; the following statement must be added to the H1 and H2's `named.conf` files respectively:

```
server 192.168.1.2 {
  keys { H1-H2; };
};

server 192.168.1.1 {
  keys { H1-H2; };
};
```

Multiple keys can be present, but only the first one will be used.

TSIG based access control

To use a TSIG based ACL for the `allow-{ trasfer | query | update }` directives, you must specify the name of the key to be used.

For example, the following directive:

```
allow-transfer { key H1-H2; };
```

will allow a zone trasfer only between the hosts configured to use the key H1-H2.

References

[1] BIND 9 Administrator Reference Manual