Practicalities

Presented by
Olaf Kolkman (NLnet Labs)

Has bind been compiled with dnssec?

```
$ ./configure --with-openssl

$ head config.log

This file contains any messages produced by compilers
while
running configure, to aid debugging if configure makes a
mistake.

It was created by configure, which was
generated by GNU Autoconf 2.61.  Invocation command line
was

  $ ./configure --prefix=/usr/local --with-openssl
```

Make your nameserver DNSSEC Aware

- For BIND: turn DNSEC with dnssec-enable option

```
options {
        ...
        dnssec-enable yes;
        ....
};
```

- For NSD: DNSSEC enabled by default

Generate Keys

```
 dnssec-keygen -a alg -b bits [-n type] [options] name

Version: 9.5.0-P2
Required options:
    -a algorithm: RSA | RSAMD5 | DH | DSA | RSASHA1 | HMAC-MD5 | HMAC-SHA1 | HMAC-SHA224 | HMAC-
SHA256 |  HMAC-SHA384 | HMAC-SHA512
    -b key size, in bits:
        RSAMD5:                 [512..4096]
        RSASHA1:                [512..4096]
        DH:                     [128..4096]
        DSA:                    [512..1024] and divisible by 64
        HMAC-MD5:   [1..512]
        HMAC-SHA1:  [1..160]
        HMAC-SHA224:            [1..224]
        HMAC-SHA256:            [1..256]
        HMAC-SHA384:            [1..384]
        HMAC-SHA512:            [1..512]
    -n nametype: ZONE | HOST | ENTITY | USER | OTHER
        (DNSKEY generation defaults to ZONE
    name: owner of the key
Other options:
    -c <class> (default: IN)
    -d <digest bits> (0 => max, default)
    -e use large exponent (RSAMD5/RSASHA1 only)
    -f keyflag: KSK
    -g <generator> use specified generator (DH only)
    -t <type>: AUTHCONF | NOAUTHCONF | NOAUTH | NOCONF (default: AUTHCONF)
    -p <protocol>: default: 3 [dnssec]
    -s <strength> strength value this key signs DNS records with (default: 0)
    -r <randomdev>: a file containing random data
    -v <verbose level>
    -k : generate a TYPE=KEY key
Output:
     K<name>+<alg>+<id>.key, K<name>+<alg>+<i
```

Generate two keys

- Generate a Key Signing Key and Zone Signing Key

```
$ dnssec-keygen -a RSASHA1 -b 2048 -f KSK example.com
Kexample.com.+005+41863

$ dnssec-keygen -a RSASHA1 -b 1024 example.com
Kexample.com.+005+58803
```

Include the keys in your zonefile

```
$TTL 100
@       100     IN      SOA     ns  (
                         zonemaster    ;
                         2008091600
                               100     ; These values
                               200     ; are to unrealistic for
                            604800     ; production zones
                               100
                               )



                        NS              ns
ns                      A               192.0.2.1
demo                    A               192.0.2.3

$include Kexample.com.+005+41863.key
$include Kexample.com.+005+58803.key
```

Sign your zone

```
$ dnssec-signzone example.com
example.com.signed
```

```
example.com.            100     IN SOA  ns.example.com. zonemaster.example.com. (
                                        2008091600 ; serial
                                        100        ; refresh (1 minute 40 seconds)
                                        200        ; retry (3 minutes 20 seconds)
                                        604800     ; expire (1 week)
                                        100        ; minimum (1 minute 40 seconds)
                                        )
                        100     RRSIG   SOA 5 2 100 20081017184752 (
                                        20080917184752 58803 example.com.
                                        mMS8by7lO9SKFv+zQHB/dd0czsmZpsvwrwil
                                        gBh12tqK/9kGtuID8f5OvERqwSDhE4e462yF
                                        sS8839JlKYndgMJu/cCY1qGIW34tad83P/yu
                                        lPWdZO0bDGB8d0BeE4Sj8TbUtSrnJb1ZvByG
                                        0IIB0JKZHRe009SBQAKfXqUnr/E= )
                        100     NS      ns.example.com.
                        100     RRSIG   NS 5 2 100 20081017184752 (
                                        20080917184752 58803 example.com.
                                        O991xgbHje/OowTz1Ea94bnNruxxzW1xf/al
                                        YQ482cPQWTeD3B6qsNIJSC3ymQcZ4ySQu4Gj
                                        mKh25Mz/uH0fsHGNrLPZuw7laEWd/H4hN1ib
                                        YPANP+AKF3yuK/h9IHc/ydNMyMLsk3woDfXc
                                        KsEHZSJeuTYgGLIRQtdfhGaQU6g= )
                        100     NSEC    demo.example.com. NS SOA RRSIG NSEC DNSKEY
                        100     RRSIG   NSEC 5 2 100 20081017184752 (
                                        20080917184752 58803 example.com.
                                        ROta6SMQWFoRrmEAdPaHIbViqNJAWYsPZYCG
                                        iGodUKVDxGPw/E77rkMdwIKJZk3n/IMHleM+
                                        ce/8v2zU3cBXtJ2BjFKiJ3quDWaJRb33DGWH
                        100     DNSKEY
```

```
osx+r8ku8fIRtfHmggn78Z986+yc0mGiddEH
G9LcAv8riwE2/+lq1BFO7Ftvg+g= )
```

Serve the signed zone

- Just point to your masterfile

```
zone "example.com" {
        type master;
        file "example.com.signed";
};
```

TEST

$ dig @192.168.2.202 example.com SOA +dnssec

```
; <<>> DiG 9.5.0-P2 <<>> @192.168.2.202 example.com SOA +dnssec
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53425
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:

example.com.            100     IN SOA  ns.example.com. zonemaster.example.com. (
                                        2008091600 ; serial
                                        100        ; refresh (1 minute 40 seconds)
                                        200        ; retry (3 minutes 20 seconds)
                                        604800     ; expire (1 week)
                                        100        ; minimum (1 minute 40 seconds)
                                        )
example.com.            100     RRSIG   SOA 5 2 100 20081017184752 (
                                        20080917184752 58803 example.com
```

```
example.com.            100     IN SOA  ns.example.com. zonemaster.example.com. (
                                        2008091600 ; serial
                                        100        ; refresh (1 minute 40 seconds)
                                        200        ; retry (3 minutes 20 seconds)
                                        604800     ; expire (1 week)
                                        100        ; minimum (1 minute 40 seconds)
                                        )
example.com.            100     RRSIG   SOA 5 2 100 20081017184752 (
                                        20080917184752 58803 example.com.
                                        mMS8by7lO9SKFv+zQHB/dd0czsmZpsvwrwil
                                        gBh12tqK/9kGtuID8f5OvERqwSDhE4e462yF
                                        sS8839JlKYndgMJu/cCY1qGIW34tad83P/yu
                                        lPWdZO0bDGB8d0BeE4Sj8TbUtSrnJb1ZvByG
                                        0IIB0JKZHRe009SBQAKfXqUnr/E= )

example.com.            100     NSEC    demo.example.com. NS SOA RRSIG NSEC DNSKEY
example.com.            100     RRSIG   NSEC 5 2 100 20081017184752 (
                                        20080917184752 58803 example.com.
                                        ROta6SMQWFoRrmEAdPaHIbViqNJAWYsPZYCG
                                        iGodUKVDxGPw/E77rkMdwIKJZk3n/IMHleM+
                                        ce/8v2zU3cBXtJ2BjFKiJ3quDWaJRb33DGWH
                                        +SaIOJgc4lHMwcTGzdogGdznCJ0xpbYmV9g8
                                        rCZV59qWJ3sferRYTvRMbEokBh0= )
                        100     DNSKEY  256 3 5 (
                                        AwEAAbMW4ddT7IZ+xHcPkbyimnQEVd/h4lPm
                                        VI2ghRdMoy3vY+Y4m0jg4YKL6DSRaWppZpF4
                                        YGVvrL/jWngKUaUOeEDjDLx3e79K9t4ncL66
                                        jKFgB1pOxUKxNSKda9nm4JbjoGZwU+AH4aGc
                                        94fKVb12+jwSx6Y9UNN4E13JHIMeQvnt
                                        ) ; key id = 58803;; Query time: 1 msec
;; SERVER: 192.168.2.202#53(192.168.2.202)
;; WHEN: Wed Sep 17 22:36:49 2008
;; MSG SIZE  rcvd: 452
```

This was the essence of serving

- You have to:
  - automate
  - automate
  - automate
  - automate
  - automate