Lab 10.2 – More DNSSEC Options

Objective:
Perform DNSSEC key rollover.
Implement DNSSEC with Dynamic Updates
Adding trust anchors.

Background
DNSSEC (or DNS Security Extensions) provide security to the zone files.

Note:
In the steps below, we are using
myzone.net - our domain
db.myzone.net – zonefile for the domain
Kmyzone.net.+005+12345.key/private = ZSK generated
Kmyzone.net.+005+67890.key/private = KSK generated

A. **Key rollover**. This involves performing scheduled zone maintenance. There are typically two commonly used means to do this.

1. KSK rollover using Double Signing.

Double signing is the easiest way to do key rollover, but it's primarily used only for KSK rollover.

Note: when you change KSK keys, the DS record in your parent zone must be updated. Otherwise, your zone will not validate.

a. Generate a new KSK using `dnssec-keygen` (see B.1 above).
b. Insert the new key into the zone's DNSKEY RRset and use both keys for signing.

```
dnssec-signzone –o myzone.net –N increment –f <output-file> \ -k
Kmyzone.net.+005+11111 db.myzone.net Kmyzone.net.+005+67890
```

where Kmyzone.net.+005+11111 is the new KSK generated. New DS records will be added to the file dsset-<myzone.net>.

c. Send the new DS record(s) to the parent. You may need to wait until the DS is introduced and propagated and then for the TTL of the old DS to pass.
d. Remove old key and re-sign.

2. KSK rollover using Pre-Publication. You can also rollover the KSK using this method. In this method, we are publishing the new key but we will not use it for signing.

a. Generate the new KSK using dnssec-keygen (see B.1 above).

```
dnssec-keygen –K keydir –f ksk –A none <myzone.net>
rndc loadkeys example.com
```

-K key directory option in named configuration. Can be configured per zone or at the global config

b. Generate a new ZSK using `dnssec-keygen` (see B.1 above).

c. Publish both keys, but use only the old one for signing.
d. Wait at least propagation time and then the TTL of the DNSKEY RR to expire.
e. Then use dnssec-settime once you are ready to sign the zone. Use the new key for zone signing, leaving the old one published.

```
dnssec-settime –K keydir –A now Kexample.com.+005+12345

rndc loadkeys example.com
```

f. Wait for the propagation and then the maximum TTL in the old zone.
g. Set the old key to no longer sign with the key, but leaves it in the zone.

```
dnssec-settime –K keydir -I now Kexample.com.+005+12345
rndc loadkeys example.com
```

This removes all the associations to Kexample.com.+005+12345.

h. Now remove the old keys. This completely removes the keys.

```
dnssec-settime –K keydir -D now Kexample.com.+005+12345
rndc loadkeys example.com
```

Note: Changing of the ZSK can occur as often as possible without introducing changes to the parent zone.

3. Automating the Signing. Starting at Bind 9.7, meta-data is introduced into the keys.

a. Use RNDC to sign and load keys to named. Assuming that you have already configured RNDC (see Lab 5), you only need to add the option below into named.conf

```
auto-dnssec allow;
```

The auto-dnssec command is used to automate the signing and key rollover. The complete options are as follows.

```
auto-dnssec off; (default setting)
auto-dnssec allow; (this enables RNDC signing)
auto-dnssec maintain; (updates DNSSEC based on key meta-data)
```

Then you can use the following commands in

```
rndc loadkeys

rndc sign
```

b. If you are sure when you want to publish, activate and retire certain keys, you can use the timing options in the dnssec-keygen command.

```
dnssec-keygen –P now –A now+30d –I now+2y –D \

now+25mo example.com
```

This command inserts into DNSKEY RRset now, use for signing in 30 days, retire in 2 years, deletes in 2 years 1 month.

Here are some dnssec-keygen timing options

-P publish

-A activate

-I retire

-D delete

B. **(optional) Domain Look-aside Buffer**. If the parent zone isn't signed yet, you can use DLV. We are not going to do this in class, but this is more for information only.

1. Create an account with ISC DLV at http://dlv.isc.org. Once done, you can add a
2. Sign the zone with the –l option.

```
dnssec-signzone -l dlv.isc.org -r /dev/urandom -o myzone.net -k
Kmyzone.net.+005+67890 myzone.net Kmyzone.net.+005+12345.key
```

3. In the ISC DLV login page, add your zone. Then add the DNSKEY for the particular zone. Instructions will be provided on the page.

4. Download the ISC DLV's key from here. Then add it as a trusted key.

```
trusted-keys {
   dlv.isc.org 257 3 5 "<key-here";
   };
```

5. Enable DLV.

```
options {
   dnssec-lookaside . trust-anchor dlv.isc.org.;
   };
```

6. Test using the dig command.

```
dig +dnssec @localhost myzone.net
```

C. **DNSSEC and Dynamic Zones**.

1. Edit named.conf to point to add the update policy.

```
zone <myzone.net> {
      type master;
      update policy-local;
      auto-dnssec maintain;
      file "dynamic/example.com";
      key-directory "keys";
};
```

The above options in bold means:

auto-dnssec maintain = allows

2. Generate keys for the dynamic zones.

```
dnssec-keygen –K </path/to/keys> -r /dev/urandom <zonename>
dnssec-keygen –f ksk –K </path/to/keys> -r /dev/urandom \
<zonename>
```

3. Use RNDC to sign the zone.

```
rndc sign
rndc loadkeys
```

4. Add or remove zone contents using nsupdate.

```
nsupdate –l
> update add myzone.net DNSKEY 256 3 7 <key-here>
> send
```