Lab 8.1 DNSSEC
IN715 Networks Three

September 9, 2014

Introduction

DNS presents a significant security risk since the compromise of a DNS zone would allow an attacker to direct sensitive network traffic to a destination of her choosing.

DNSSEC is a set of measure to guard against this risk by cryptographically signing DNS records to verify their authenticity. BIND supports DNSSEC and includes tool used to implement it.

In this lab we will see how to use DNSSEC to protect our zones and our users.

1 Create encrption keys

Create keys with the following commands:

```
cd /var/named/etc
dnssec-keygen -a RSASHA1 -b 2048 -n ZONE -f KSK nw3.sqrawler.com
```

This will create public and private key files in our BIND configuration directory. In particular, it creates 2048 bit key signing keys for our zone.

Now we create zone signing keys with the command

```
dnssec-keygen -a RSASHA1 -b 1024 -n ZONE nw3.sqrawler.com
```

2 Signing the zone

We will use our keys top sign the `nw3.sqrawler.com` zone. First, we include our keys in the zone file by adding these lines to the bottom of the zone file:

```
$INCLUDE Knw3.sqrawler.com.+005+10849.key ; KSK
$INCLUDE Knw3.sqrawler.com.+005+58317.key ; ZSK
```

(Your key file names will be different.)

Now you sign your zone with the following;

```
dnssec-signzone -o nw3.sqrawler.com -k Knw3.sqrawler.com.+005+10849 \
  db.nw3.sqrawler.com Knw3.sqrawler.com.+005+58317.key
```

The -o option specifies the origin, or name, of the zone to sign, and the “db.nw3.sqrawler.com is the name of the zone file.

If you are going to use DLV, you need to add an extra option;

`-l dlv.isc.org`

to indicate that you are using the ISC DLV service.

You will now have a signed zone file, `db.nw3.sqrawler.com.signed`. You will also get a DS or DLV record file.

You will need to re-sign the zone anytime you make changes, and you will need to resign the zones at least monthly since the key signatures expire in that time by default.

3 Modify named.conf

You will need to modify the `file` attribute of your zone to use the new signed version of the zone file.

You must also add the following lines to the options sections of your configuration:

```
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
```

This will enable DNSSEC for your zone and for recursive queries.

Reload your DNS server and test with the command

`dig +dnssec www.nw3.sqrawler.com`

4 Notify the parent

To use DNSSEC, you must complete the process by registering your DS or DLV record with the appropriate party. This is your registrar in the case of a DS record, or the ISC in the case of a DLV record.