Validating/Using DNS Sec

demo

February 21, 2014

Objectives

This is to demonstrate using a validating recursive DNS server.

Note that some versions of Microsoft's DNS server do not support dnssec validation. http://support.microsoft.com/kb/2028240 for more details.

Server bits

- Grab the root key
- Configure the “root anchor” in your resolver
- Two examples based on your server

Server bits: unbound - automated updates of anchor

- You can use “unbound-anchor” to download the real root.key, and set “auto-trust-anchor-file:” in unbound.conf, and let unbound update the key when necessary.

```
server:
    # The following line will configure unbound to
    # perform cryptographic DNSSEC validation using
    # the root trust anchor.
    auto-trust-anchor-file: "/var/lib/unbound/root.key"
```

Server bits: unbound - manual updates of anchor

- Alternatively download the key yourself

```
server:
    # The following line will configure unbound to
    # perform cryptographic DNSSEC validation using
    # the root trust anchor. Download it to this file:
    trust-anchor-file: "/etc/unbound/root.key"
```

profit!

- restart unbound

Server bits: bind

- Assumption is this bind is recursive caching ONLY (don't mix servers)
- Download the root key and edit named.conf

```
trusted-keys {
    // paste here the contents
};
```

profit!

- Restart bind

Client bits

if you want to run this you can ssh to ub.po.rg.net with the username that we created ssh keys for and try the dig comands.

working zone

```
$ dig @noc.po.rg.net +dnssec . SOA
$ dig +multi +noall +answer dnskey psg.com
```

failures

```
$ dig @noc.po.rg.net +dnssec www.dnssec-failed.org
```

Client bits

Your end users are likely on windows. There is nslookup but we love to hate it. We have two recursive DNS servers setup for this lab. One validates, the other doesn't. The one you got from DHCP does *not* validate. To test.

- open www.dnssec-failed.org in your browser and read the page
- change your DNS settings so your nameserver is 10.10.0.250 (or have the instructor change the DNS and refresh)
- try opening www.dnssec-failed.org again in your browser.

Client bits

concerning filtering

- Note size of responses
- DO NOT FILTER TCP/53 or fragmented UDP packets.

unreachable zones

- some zomes have expired keys or poorly setup dnssec
- without dnssec other proposed standards like DANE won't work
- if possible, enable dnssec validation and prepare your support department
- previous concern is less important these days. check if you can get wwww.dnssec-failed.org from 8.8.8.8