Deploying DNSSec

or, How I learned to stop worrying and love the 'Net.

Erik Berls
LayerOne 2009

Why DNSSec?

- Idealized end state
- Failures of the "old" system
  - Stepping back, how services changed over time
- Stepping stones to get there

OK, but what is it?

- Signing
- Verification
- Trust Anchors
- New record types

Authoritative Servers: Some Changes

- Server setup
- Protecting the Keys
- Updates
- Routine Actions

Before making changes (aka, the paperwork)

- Assumption: You've already got a working DNS setup
- Assumption: Your software is compatible
- Assumption: Your SECONDARY's software is compatible

What keys, and what Castle?

- What zones to sign
- What zones NOT to sign

- Other considerations
  - DDNS
  - SOA serial

Setting up your server

- Traditional server setup
- Additional requirements now that we've got keys
  - Offline signing
  - Online signing - client reachable host
  - Online signing - "protected" host
- Additional details on safer

Setting up your Keying information

- (Re)Generation of your keys
  - Zone Signing Key (ZSK) - 3 Months
    - `dnssec-keygen -a alg -b bits -n type name`
    - `dnssec-keygen -a RSASHA1 -b 1024 -n ZONE worst.com`
  - Key Signing Key (KSK) - 12 Months
    - `dnssec-keygen -a alg -b bits -n type name`
    - `dnssec-keygen -a RSASHA1 -b 4096 -n ZONE -f KSK worst.com`
- Add to Zone file
  - Either $INCLUDE or appending
    - `cat Kzonename*.key >> zonefile`
    - `cat Kworst.com*.key >> db.worst`

Signing your Zone

- Really Simple with BIND9

```
dnssec-signzone -l DLV -r randomsrc -o origin -k KSK inputfile ZSK

dnssec-signzone -l dlv.isc.org -r /dev/random -o worst.com -k Kworst.com.
+005+59404 worst.com Kworst.com.+005+00393.key
```

- Options exists for further granularity
  - Incrementing Serial
  - Fine tuneing of dates
- Automation tools exist

Deploying your signed Zone file

- named.conf

```
options {
  dnssec-enable yes;
  allow-recursion { none; };
  allow-transfer { peers; };

};
```

- Copy into place and Update zone section
  - replace
    - `file "/etc/namedb/db.worst";`
  - with
    - `file "/etc/namedb/db.worst.signed";`
- Restart/Reload BIND

Verification

- Verification with logs

```
... zone ono-sendai.com/IN/external: loaded serial 2006072403
... zone worst.com/IN/external: loaded serial 2008072600 (signed)
```

- Verification with dig
  - dig +dnssec @127.0.0.1 worst.com. soa

[snip]

```
;; ANSWER SECTION:
worst.com.              3600    IN      SOA     worst.com. cyber.ono-sendai.
com. 2008072600 3600 300 2419200 3600
worst.com.              3600    IN      RRSIG   SOA 5 2 3600 20080826053942
20080727053942 393 worst.com.
ZYcLtMvobEwcvX16xNTTNuynP2kd5mu/nlsWXaox/6AKV69CFJBr8Yr0
jAtbsU+0TiGf6ntbYu57NHqVx5PfXUNjcEfPJyrgCkwcdRvzT1k+LLFB
ttvbtFnmBbZR67UAJGKPnU96nZui6L0CITNJAOTyFdNZH+SUK2OGbxT2 fTE=
```

[snip]

Ok, we're done, right?

- Hooking into the Trust Chain
  - DS
  - DLV

DS - Chaining from the parent

- The way it *should* work
- Existing trust relationships

DLV - Domain Lookaside Verification

- Submitting the dlvset
  - output from dnssec-signzonewith the -l option
- Proof!
  - DLV vendor wants to know that you really have control
  - `dlv.worst.com. IN TXT "24qxDwq6vr0Zk"`
  - https://dlv.isc.org/

Periodic Actions (Authoritative)

- Updating Zones
- Key Rotations

- Both involve signing
  - 1 hour grace
  - 30 day lifetime
  - No key expiration! (Rotation is important!)

Caching/Recursive Resolvers

- "Almost" prime time
  - Checking stats

- named.conf for DLV

```
trusted-keys {
    # from https://www.isc.org/ops/dlv/#dlv_key
    dlv.isc.org. 257 3 5 "BEA...uDB";
};

options {
    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside "." trust-anchor dlv.isc.org.;
};
```

IANA ITAR (Trust Anchors)

- Top level signed zones
- Distributed as XML but convertable to trusted-keys for BIND
- https://itar.iana.org/instructions/

Periodic actions (Recursive)

- Update Trust Anchors
  - DLV
  - IANA ITAR
  - Mailing lists & Automated updates
  - RFC 5011
- Check stats in logfile

Under the hood a bit

- New record types (RFC 4034)
  - DNSKEY

```
worst.com                3600    IN DNSKEY 257 3 5 (
                                           AwEAAdX...kiTx
                                           ) ; key id = 59404
```

  - RRSIG

```
                         3600    RRSIG   SOA 5 2 3600 20090621034710 (
                                         20090522034710 393 worst.com.
                                         S2n...n0g= )
```

  - NSEC

```
;; QUESTION SECTION:
;google.com.dlv.isc.org.                IN      NSEC

;; AUTHORITY SECTION:
[snip]
germann-family.com.dlv.isc.org. 3600 IN NSEC    greenpeas.com.dlv.isc.org.
RRSIG NSEC DLV
[snip]
```

More internals

- DS

```
worst.com.              IN DS 59404 5 1
0910CF0711809DC00BC2DCAAD34126B2E5CEEB63

worst.com.              IN DS 59404 5 2
830833F177145BB30EB28F9C5205DD3B1ED70F3F9CC13B5C5BED2BBD D0CC39E1
```

- NSEC3
  - RFC 5155
  - hashed denial of existence
- DLV

```
worst.com.dlv.isc.org.  IN DLV 59404 5 1
0910CF0711809DC00BC2DCAAD34126B2E5CEEB63

worst.com.dlv.isc.org.  IN DLV 59404 5 2
830833F177145BB30EB28F9C5205DD3B1ED70F3F9CC13B5C5BED2BBD D0CC39E1
```

Questions?

- https://dlv.isc.org/
- https://itar.iana.org/instructions/