DNSSEC on the Recursive Resolver

Tom Daly

Dynamic Network Services, Inc.

tom@dyn-inc.com

DYNAMIC NETWORK SERVICES INCORPORATED

Why do you care?

- Customers are going to ask.
- Operational requirements:
  - More CPU to check sigs
  - More bandwidth to transfer record signatures
- CapEx to bring your recursive farms up to speed for this.

DNSSEC Components

- Authoritative DNS with signed zones
- **Recursive DNS with trust anchors installed**
- DNSSEC validating clients

A Focus on the Recursive side

Authoritative DNS Server
(DNSSEC signed zones)

Recursive DNS
Security Oblivious

DNS Client
(Windows, Mac, Linux, etc)

Focus has been on this part! And much progress made!

This doesn't address security over the last mile...

- If you're concerned about DNS security between the security aware recursive and the stub resolver...

- ***Run your own validating recursive***
- ***Within the secure bounds of your own network***

Trust Anchors

- Secure Entry Points into DNSSEC land.
- Obtaining them is a manual process (some automation is possible)
- IANA DNSSEC testbed (http://ns.iana.org) for the root zone
- ITAR (http://itar.iana.org) for TLDs
- DLV (http://dlv.isc.org) for domains, if they contribute.
- Individually signed keys obtained OOB

Configuring BIND

```
options {
    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside . trust-anchor dlv.isc.org.;
};
trusted-keys {
    dlv.isc.org. 257 3 5 "BEAAAAPHMu/5onzrEE7z1egmhg/WPO0+juoZ…
    se. 257 3 5 “AwEAAdKc1sGsbv5jjeJ141I…
};
logging {
    category dnssec { somewhere; };
};
```

Please!

- Check your firewalls and ACLs
  - A UDP DNS frame might be more than 512 bytes.
  - TCP DNS exists, and DNSSEC may need it if EDNS fails.

Testing DNSSEC

- Use dig
- dig +dnssec @resolver <hostname>
- Look for the +ad bit to be set in your answers.

Normal DNS Query

```
; <<>> DiG 9.4.2 <<>> @localhost nic.se
; (2 servers found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28929
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;nic.se.                                IN      A

;; ANSWER SECTION:
nic.se.                 60      IN      A       212.247.7.218

;; AUTHORITY SECTION:
nic.se.                 3372    IN      NS      ns.nic.se.
nic.se.                 3372    IN      NS      ns3.nic.se.
nic.se.                 3372    IN      NS      ns2.nic.se.
```

DNSSEC Requested, Not Signed

```
; <<>> DiG 9.4.2 <<>> +dnssec @localhost intrnet.org
; (2 servers found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61756
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;intrnet.org.                   IN      A

;; ANSWER SECTION:
intrnet.org.            60      IN      A       216.177.0.100

;; AUTHORITY SECTION:
intrnet.org.            86400   IN      NS      ns2.p13.dynect.net.
intrnet.org.            86400   IN      NS      ns1.p13.dynect.net.
```

DNSSEC Requested, Signed, No Local Trust Anchor

```
; <<>> DiG 9.4.2 <<>> @localhost nic.se +dnssec
; (2 servers found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42878
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nic.se.                                IN      A

;; ANSWER SECTION:
nic.se.                 60      IN      A       212.247.7.218
nic.se.                 60      IN      RRSIG   A 5 2 60 20090619131501
20090609131501 37253 nic.se.
hulbMfNtT9IeKwJJR/ltYyDHPvEZjdeMU/mw4Dz0hv5FYdDlXVnG3T+m
T0ySswCRvePnDO0U8D+0I6Iqzps9E2rq7r6GoBs0m+HbAkc6AS6nZalK
uO/T+qE9hgaNv1TD6Y4d4PUo0UAK1IBb2whSz/IbuzmCcLfpDY2xN8Xr HIg=
```

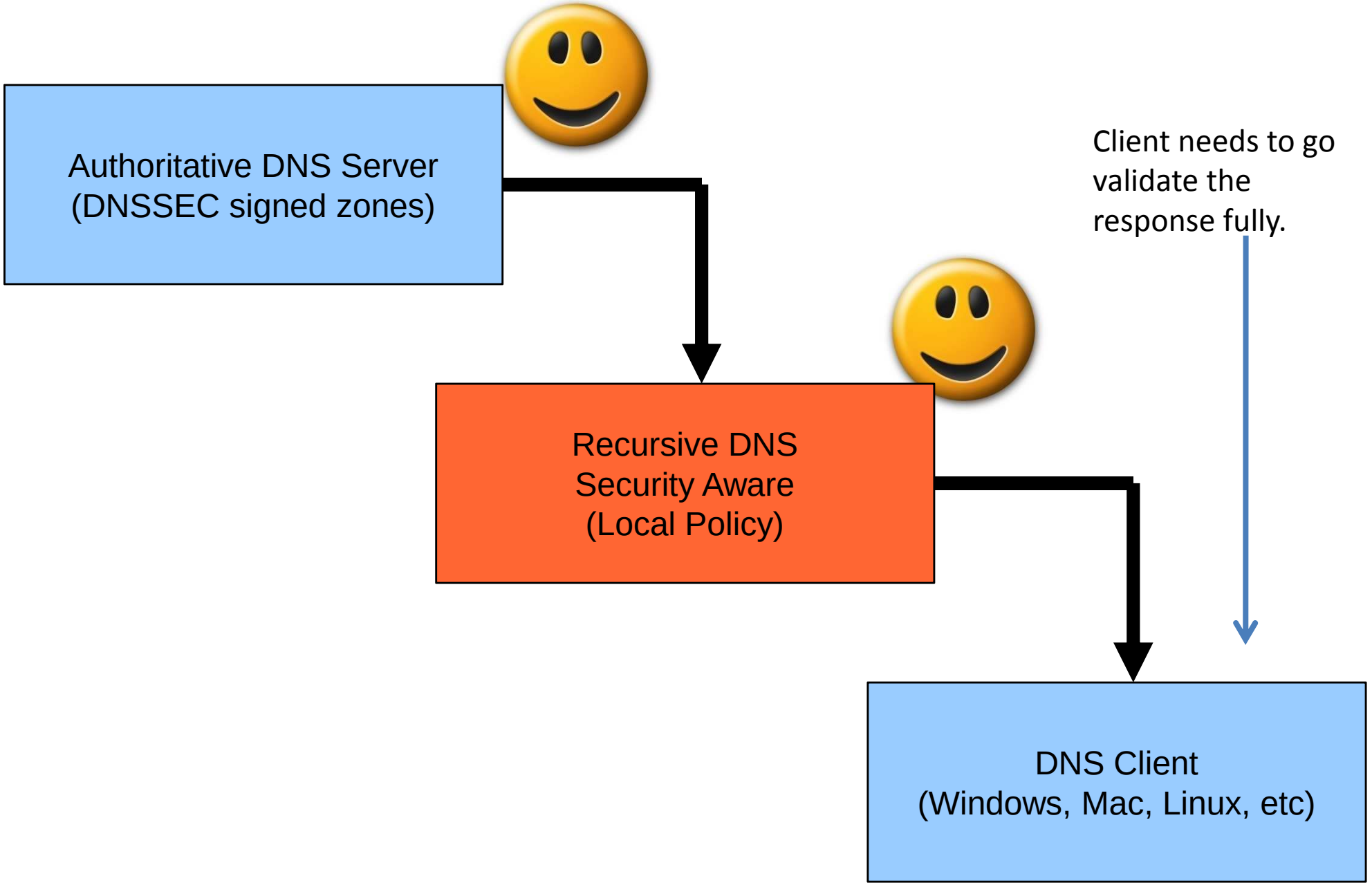
DNSSEC Requested, Signed, Resolver Validated

```
; <<>> DiG 9.4.2 <<>> @localhost nic.se +dnssec
; (2 servers found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14799
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nic.se.                                IN      A

;; ANSWER SECTION:
nic.se.                 54      IN      A       212.247.7.218
nic.se.                 54      IN      RRSIG   A 5 2 60 20090619131501
20090609131501 37253 nic.se.
hulbMfNtT9IeKwJJR/ltYyDHPvEZjdeMU/mw4Dz0hv5FYdDlXVnG3T+m
T0ySswCRvePnDO0U8D+0I6Iqzps9E2rq7r6GoBs0m+HbAkc6AS6nZalK
uO/T+qE9hgaNv1TD6Y4d4PUo0UAK1IBb2whSz/IbuzmCcLfpDY2xN8Xr HIg=
```

To fully validate…

- You’ve only been given a hint (specific to local policy) that things look good (+ad bit)
- Stub would now walk the DNSSEC chain to validate the response.
- Validate RRSIGs up the chain to a trust anchor(s) available.
- It is best to get your stub client to walk the validation chain.

Validation


Authoritative DNS Server
(DNSSEC signed zones)
Recursive DNS
Security Aware
(Local Policy)
DNS Client
(Windows, Mac, Linux, etc)
Client needs to go validate the response fully.

Next Steps

- Client resolver/stub libraries
- Application feedback

- Propagate DNSSEC validation error to user (similar to SSL in HTTP UAs)

Testing Resources

- Dyn Inc DNSSEC Testbed (http://dynamicnetworkservices.com/dnssec)

- Comcast DNSSEC Trial (http://www.dnssec.comcast.net/)

- DNS-OARC ODVR (https://www.dns-oarc.net/oarc/services/odvr)