DNSSEC: Securing the DNS and beyond

Presented by
Paul Wouters
seceng, Red Hat Inc.
Topics

- DNSSEC theory in 7 screen shots
- DNSSEC software: validating, signing
- Converting applications to use DNSSEC
- Using DNSSEC for non-DNS purposes
  - TLSA, SSHFP, IPSECKEY, <your crazy idea here>
DNSSEC in 7 screen shots
Image a DNS RRset

[paul@thinkpad ~]$ dig fedoraproject.org

; <<< DiG 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<< fedoraproject.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61882
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fedoraproject.org.

;; ANSWER SECTION:
fedoraproject.org. 44 IN A 209.132.181.16
fedoraproject.org. 44 IN A 85.236.55.6

;; Query time: 95 msec
;; SERVER: 193.110.157.123#53(193.110.157.123)
;; MSG SIZE  rcvd: 78

[paul@thinkpad ~]$
Add DNS signature record
Also signature for NXDOMAIN

[paul@thinkpad ~]$ dig +dnssec doesnotexist.fedoraproject.org
; <<< DiG 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<< +dnssec doesnotexist.fedoraproject.org
; global options: +cmd
; Got answer:
; -=>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 49754
; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

; AUTHORITY SECTION:
fedoraproject.org. IN SOA ns04.fedoraproject.org. hostmaster.fedoraproject.org. [...] fedoraproject.org. IN RRSIG SOA 5 2 300 20120923193204 20120824193204 7725 [...]
docs.fedoraproject.org. IN NSEC download.fedoraproject.org. CNAME RRSIG NSEC
docs.fedoraproject.org. IN RRSIG NSEC 5 3 86400 20120923193204 20120824193204 7725 [...] fedoraproject.org. IN NSEC aaaa.fedoraproject.org. A NS SOA MX AAAA RRSIG NSEC DNSKEY fedoraproject.org. IN RRSIG NSEC 5 2 86400 20120923193204 20120824193204 7725 [...]
Publish the public key used in DNS

```
[paul@thinkpad ~]$ dig +dnssec -t dnskey fedoraproject.org

; <<< Dig 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<< +dnssec -t dnskey fedoraproject.org
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47954
; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

; ANSWER SECTION:
fedoraproject.org. 257 3 5 AwEAAAdTXJc0joiKGfTvLX+LxGpKvPv0oJEst9PR8TCCvXGVp7h3BY3 u
XLkjc0uT0aopCp2KF8zHgNgpMK03plf94pn9gJZszxflqKs1yH2Knyn 0 a/6550p0j6jRhqAP5grX01lZ4B4H1llzhGx1Q1Bz7t0r1wAaoj
MJzLug ChRJs8GV+3LUQz6T8z1RQF33dt9UMH5EAsFAqf/TsbfJYxdGozi3 nFlw7A745+0bMLNX0qW3FcYPVzhH0807/7WpxmqM6
/ET8 VegWIs8hE nZNDDNHFyPbY9B10IrFCpE03ALgFMeggA8wmeQaX+O4Duupx5G0mdTC 04GSpM1YH6c=
fedoraproject.org. IN DNSKEY 256 3 5 AwEAAAcWN0Wl5pC1310OP2r8nStL60Zjb/2J0L0ytaMVap0L44z0YVwft u
7pu0hx3cnIM1aj00sEsWbg2/10HyC+38cYqJDXb5dFg1zGztOS5xNz7r 9hzSRK5N2jkycdj/BoBy34Y+XGpDqf4G4I97++8sIzSr6060TmGA
KTvM9V iL3ByeCN
fedoraproject.org. IN RRSIG DNSKEY 5 2 300 20120923193204 20120824193204 7725 fedoraproject.or
g. ZTebel_04w5px0g065qDxa8P1xUDnSd1Qj1InCrPOLAMrPcB51euL6n 1Dpe2aXRW2N78fApF+PocRURS1o6Q55GtGd060nPUENLC
U4yvjs1V1PZ ZLTVV+nf44dL4yIxExo2h5t0DXXVe09ngene9w6i+1/Hg9ITNtLjBy8p bHY=
fedoraproject.org. IN RRSIG DNSKEY 5 2 300 20120923193204 20120824193204 16207 fedoraproject.o
rg. U1sP5Sb6e0/0b9TyyFbcnTLClddtyg96LFVFe0PEFUQ/6mykltL5Nh9J7 7x3Zh35vsaaTT/fyAvVn9elsIXk/GZr22/2mmAcvf0dIB
9J/E/EXdBGch AI1q70j8LSkemMx5V7eK4Yld83s2+000vnaatIs1S4s6E0jCz6N00Ly9h UzjfMFouB0eqTEJjwBHDDiQuK140rLGTAzm/ L
+t/9xAmTRPwJc4h2k3j wYMeIcr1ab6HMJAJzarGxmJPPeYzi96g4WzFnX1OFqaKFr5no7V4fFg EUTmT7vHcc1u/ryY+0c9XvakndjG
V0lr6njIfAxculF5qNgNvzGAmcy 8dl+rg==
```

[paul@thinkpad ~]$
Hash of public key goes to parent

[paul@thinkpad ~]$ dig +dnssec -t ds fedoraproject.org @a0.org.afilias-nst.info.
;; >> DiG 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<>> +dnssec -t ds fedoraproject.org @a0.org.afilias-nst.info.
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<<< opcode: QUERY, status: NOERROR, id: 44034
;; flags: qr aa rd: QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;fedoraproject.org. IN DS

;; ANSWER SECTION:
fedoraproject.org. 86400 IN DS 42429 7 2 6107F37FB56D27D257598BF01180A0C12D1A0E3785B5D6BFF2D41A7A0 F4120BB7
fedoraproject.org. 86400 IN DS 27768 7 2 E3F2AD57448C1E62FC60C4C06E3F4845E19B1892
E13F6DA9087549A9 522152FD
fedoraproject.org. 86400 IN RRSIG DS 7 2 86400 20120830160604 20120809150604 4818 org. JJ4CnhBbi06fi/JkwoI1rWgu+DbxrdZ3UaWLFFl8myxegZlfqovvwzDSu ivW9bHyHRwwYgXUwB+ueH0gyL9KpDTZH0RwVovcNmFHM73NHuI2j0Fj HZ8pkRMAdVFwRv5Scy/UVTV5gGRfKREpNwSrwp5SSEJAB13XnDR7L2E38SE HkU=

;; Query time: 11 msec
;; SERVER: 199.19.56.1#53(199.19.56.1)
;; MSG SIZE rcvd: 300
Build DS -> DNSKEY trust chains

DNSData: $ dig dnskey > root.key
Data: $ drill -S dnssec.se -k root.key -4

--- Number of trusted keys: 2
--- Chasing: dnssec.se. A

DNSSEC Trust tree:
dnssec.se. (A)
    |---Existence is denied by:
    |---dnssec.se. (NSEC _adsp._domainkey.dnssec.se. NS SOA TXT RRSIG NSEC DNSKEY SPF )
    |    |---dnssec.se. (DNSKEY keytag: 30332 alg: 5 flags: 256)
    |    |---dnssec.se. (DS keytag: 2467 digest type: 1)
    |    |    |---se. (DNSKEY keytag: 12318 alg: 5 flags: 256)
    |    |    |    |---se. (DNSKEY keytag: 59747 alg: 5 flags: 257)
    |    |    |    |    |---se. (DS keytag: 59747 digest type: 2)
    |    |    |    |    |    |---. (DNSKEY keytag: 50398 alg: 8 flags: 256)
    |    |    |    |    |    |    |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
    |    |---dnssec.se. (DS keytag: 2467 digest type: 2)
    |    |    |---se. (DNSKEY keytag: 12318 alg: 5 flags: 256)
    |    |    |    |---se. (DNSKEY keytag: 59747 alg: 5 flags: 257)
    |    |    |    |    |---se. (DS keytag: 59747 digest type: 2)
    |    |    |    |    |    |---. (DNSKEY keytag: 50398 alg: 8 flags: 256)
    |    |    |    |    |    |    |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)

Existence denied
--- Chase successful
DNSSEC Lookaside Verification

```
[paul@thinkpad ~]$ dig +dnssec -t dlv fedoraproject.org.dlv.isc.org

;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 54192
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 1

;; QUESTION SECTION:
fedoraproject.org.dlv.isc.org. IN DVL

;; ANSWER SECTION:
fedoraproject.org.dlv.isc.org. IN DVL 16207 5 1 8DD099791A2A110851FDE5D14F6C62ADC3DD7C18
fedoraproject.org.dlv.isc.org. IN DVL 16207 5 2 A7C9BF5AFE374C9650ED678F3D36931A7DE9256B86A7BC34
DGDEED7D4E492E5E
fedoraproject.org.dlv.isc.org. IN RR SIG DVL 5 5 3600 20120924203004 20120825203004 64263 dlv.isc.org. gDSDRBYb1Cr346RPL71BJ01rE6CMcrAp0cbbKHTJEuAfiTLu139rvWhn p9+t7CwzMZf5E8KJuTA9ShRPrr3X9vhbxyzMM6Cw4FzWc91iBAHwBR ScVJBVpsi4hqwGh8Xc8uX/rzKBg7Fqa+aR7qWshHHUuEJnracroSO/jkMZP Epc=

;; AUTHORITY SECTION:
dlv.isc.org. 2610 IN NS ns.isc.afilias-nst.info.
dlv.isc.org. 2610 IN RR SIG NS 5 3 3600 20120924203004 20120825203004 64263 dlv.isc.org. A20V4NhDFzJ5Yd83TEJblpq4ef0GL70CMvJttiZAvmBCqFSMXEcCZDYF IHicKDFwFrFeJA02/9MYpdVl9lCnvnxY7mEWEcWr2N2sLV0vK74mA DQHQMx0aNnHxqupFWSrBq3hPhe5H0Atd9HjHfVKBKKEQaDkcAwEDARg h/A=
```

[paul@thinkpad ~]$
DNSSEC states and bits

- Secure: validated from known trust anchor key
- Insecure: proven no trust anchor exists there
- Bogus: crypto failed, answer scrubbed (ServFail)
- Indeterminate: answers incomplete/missing

- Query using “dig +dnssec”
- Check dig output for “AD” - Authenticated Data
- Debug ServFail's using “dig +cd +dnssec”
DNSSEC in Linux distro's

- DNSSEC capable DNS resolvers
  - unbound (preferred for on the fly reconfiguration)
  - bind (named)
- DNSSEC capable DNS servers
  - All modern DNS servers (bind, nsd, powerdns)
- DNSSEC zone signers
  - opendnssec, dnssec-signzone (bind), pdns, dnssec-tools, ....
- DNSSEC utilities (dig, unbound-host, drill,..)
  - yum/apt-cache search dnssec
DNSSEC validation in Fedora / RHEL

- yum install unbound or yum install bind
- echo “nameserver 127.0.0.1” > /etc/resolv.conf
- No further configuration needed, DNSSEC enabled in default configuration since Fedora 15

- Don't actually do this on your laptop, as you depend on spoofed DNS every day!
DNSSEC resolving issues

- DNSSEC too good – protects against
  - hotspot / captive portal
  - VPN – private views
  - opendns, NXDOMAIN squatting, dns rewriting (such as done by Rogers)
- Many applications mess with /etc/resolv.conf and /etc/hosts or system32\hosts files
- We need to address these issues all at once
DNSSEC and hotspots

- NetworkManager, unbound, dnssec-triggerd
- Run DNSSEC server locally: unbound
dnssec-triggerd with NM hook to:
  - Detect hotspot via http://fp.org/static/hotspot.txt
  - use resolv.conf to temporarily bypass unbound
  - Launch browser to hotspot-nocache.fp.org
  - Detect payment / license agreement
  - Re-enable DNSSEC using unbound via resolv.conf
Hotspot detected

Web traffic hijacked
The web traffic on this network is being hijacked. Is this a hotspot?

While you login you are *insecure*, until the traffic hijacking has stopped and dnssec-trigger has detected regular web access.

*Skip* if you are not logging into a hotspot right now.

[Skip]  [Log in]
Thanks MTCC.....

probe dnssec results

dnssec-trigger 0.11
results from probe at 2012-10-02 09:45:18

http fedoraproject.org (152.19.134.146): error stream closed
http fedoraproject.org (209.132.181.16): error stream closed
http fedoraproject.org (66.35.62.166): error stream closed
http fedoraproject.org (140.211.169.197): error stream closed
cache 207.181.101.5: error no EDNS
cache 207.181.101.4: error no EDNS

DNS queries are sent to INSECURE servers. There is no web access, perhaps you must do hotspot signon. Please, be careful out there.
Enter the Access Code provided and agree to the MTCC's Internet Access Terms and Conditions before you can access the Internet.

Authentication: Complimentary access

ACCESS CODE

[ ] I agree to the Terms and Conditions

Next >>
Fallback to DNS over TCP

probe dnssec results

dnssec-trigger 0.11
results from probe at 2012-10-02 09:48:21

ssl443 66.35.62.163: error timeout
tcp80 152.19.134.150: OK
authority 192.112.36.4: error no answer, SERVFAIL
http fedoraproject.org (66.35.62.166): OK
cache 207.181.101.4: error no EDNS
cache 207.181.101.5: error no EDNS

DNSSEC results fetched from open resolvers over TCP
Or worse: cache-only

Network DNSSEC Failure

The Network Fails to Support DNSSEC

The network you are connected to does not allow DNSSEC, via the provided DNS caches, nor via contacting servers on the internet directly (it filters traffic to this end). It is not possible to provide DNSSEC security, but you can connect insecurely.

Do you want to connect insecurely?

* if you choose **Disconnect** then DNS is disabled. It is safe, but there is very little that works.

* if you choose **Insecure** then the DNSSEC security is lost. You can connect and work. But there is no safety. The network interferes with DNSSEC, it may also interfere with other things. Have caution and work with sensitive personal and financial things some other time.

Some hotspots may work after you have gained access via its signon page. Then use **Reprobe** from the menu to retry.

*Stay safe out there!*
DNSSEC and VPNs

- Openswan reconfigures unbound on the fly
  - IPsec server sends XAUTH domain name and name server parameters to openswan client (i.e. “redhat.com”, 10.11.255.156)
  - Openswan informs unbound: “unbound-control forward_add redhat.com 10.11.255.156”
  - On termination, openswan issues “unbound-control forward_remove redhat.com” and “unbound-control flush_requestlist”
DNSSEC zone signing

- `yum install opendnssec -y`
- `systemctl ods-enforcerd start`
- `systemctl ods-signerd start`
- `ods-ksmutil zone --add yourzone.com --input /var/named/yourzone.com --output /var/named/yourzone.com.signed`
- `ods-signer sign yourzone.zome` (updated named.conf, restart named, wait a few days, go to Registrar for DS, or dlv.isc.org to publish DLV)
- `ods-ksmutil key ds-seen --zone yourzone.com --keytag xxxxxx`
Convert code to use DNSSEC

- We will use libunbound as our API
- Find gethostbyname() calls (direct / indirect)
- Initialize a DNSSEC cache context
- Configure its behaviour to emulate POSIX
- Load DNSSEC trust anchor keys (root, DLV)
- Call ub_resolv() directly or via thread / callback
- Check return value for DNSSEC parameters
/* Converting gethostbyname() to libunbound with DNSSEC support */

#include <unbound.h>
struct ub_ctx* dnsctx;

int unbound_init(int verbose)
{
    dnsctx = ub_ctx_create();  /* create unbound resolver context */

    if (verbose) {
        printf("unbound context created - setting debug level high\n");
        ub_ctx_debuglevel(dnsctx, 255);
    }

    /* look at /etc/hosts before DNS lookups as people expect this */

    if ( (ugh = ub_ctx_hosts(dnsctx, "/etc/hosts")) != 0) {
        printf("error reading hosts: %s. errno says: %s\n",  
            ub_strerror(ugh), strerror(errno));
        return 0;
    }

    /* Use DHCP obtained DNS servers as forwarding cache */

    if ( (e = ub_ctx_resolvconf(dnsctx, "/etc/resolv.conf")) != 0) {
        printf("error reading resolv.conf: %s. errno says: %s\n",  
            ub_strerror(e), strerror(errno));
        return 0;
    }

...
Add trusted DNSSEC keys

/* DNSSEC root key */
static char *rootanchor = "\n
/* DNSSEC DLV key, see http://dlv.isc.org */
static char *dlvanchor = "\n
/* real errno handling code removed for clarity */

/* add trust anchors to libunbound context */
if(verbose)
    printf("Loading root key:%s\n", rootanchor);
    e = ub_ctx_add_ta(dnsctx, rootanchor);

/* Enable DLV */
if(verbose)
    printf("Loading dlv key:%s\n", dlvanchor);
    e = ub_ctx_set_option(dnsctx, "dlv-anchor:" , dlvanchor);

return 1; /* real errno handling code removed for clarity */

"unbound-hooks.txt" 223L, 6357C written
Add DNSSEC resolve call

```c
err_t unbound_resolve(char *src, size_t src_len, int af, ip_address *ipaddr)
{
    char *err = NULL;
    int qtype = 1; /* default to IPv4 */
    int e;
    struct ub_result* result;

    if(af == AF_INET6) {
        qtype = 28; /* AAAA */
    }

    e = ub_resolve(dnsctx, src, qtype, 1 /* CLASS IN */, &result);
    if(result->bogus) {
        fprintf(stderr,"ERROR: %s failed DNSSEC validation!\n", result->qname);
    }
    if(!result->havedata) {
        if(result->secure)
            sprintf(err,"Validated reply proves '%s' does not exist\", src);
        else
            sprintf(err,"Failed to resolve '%s' (%s)\n", src, (result->bogus) ? "BOGUS" : "insecure ");
        ub_resolve_free(result);
        return err;
    } else if(!result->bogus) {
        if(!result->secure) {
            fprintf(stderr,"warning: %s lookup was not protected by DNSSEC!\n", result->qname);
        }
    }
}```
replace gethostbyname()

/* Code changes to support DNSSEC in openswan's "add connection" code */

+#ifdef DNSSEC
+  if(resolvip) {
+      /* initialise our DNSSEC resolver context */
+      if(!unbind_init(verbos)){
+          fprintf(stderr,"unbind_init() failed, aborting\n");
+          return 1;
+      }
+  }
+#endif

        [.........]

               if(hostname) {
                   err_t e;
                  char b[ADDRSOT_BUF];
               +#ifdef DNSSEC
               +  if(verbos) {
               +      printf("Calling unbound_resolve() for hostname value");
               +  }
               +  e = unbound_resolve(hostname, strlen(hostname), AF_INET, &cfg->dr);
               +#else
               /* toaddr() calls gethostbyname(hostname) */
               e = ttoaddr(hostname, strlen(hostname), AF_INET, &cfg->dr);
               +#endif

        [.........]

+#ifdef DNSSEC
+  ub_ctx_delete(dnsctx);
+#endif

    exit(exit_status);
Achievement unlocked!

- Your zone is continuously signed and updated
- Your resolvers are deployed with DNSSEC
- You can handle necessary spoofed data from VPN and hotspots
- Your application is DNSSEC aware and protects against DNS spoofing and cache poisoning
- You can now use DNSSEC to securely publish your own data
non-DNS data use of DNSSEC

- TLSA – Store HTTPS certificates in DNS
- SSHFP – Store ssh known_hosts keys in DNS
- IPSECKEY – Store IPsec public RSA keys in DNS
- S/MIME – Store email public keys in DNS
- SMTP/TLSA – STARTSSL public keys in DNS

(first three are already described in RFCs, the last two are currently still drafts)
The TLSA record

2.1. TLSA RDATA Wire Format

The RDATA for a TLSA RR consists of a one-octet certificate usage field, a one-octet selector field, a one-octet matching type field, and the certificate association data field.

```
<table>
<thead>
<tr>
<th>Cert. Usage</th>
<th>Selector</th>
<th>Matching Type</th>
<th>Certificate Association Data</th>
</tr>
</thead>
</table>
```

```
_443._tcp.fedoraproject.org. 300 IN TLSA 3 0 1 F4BF2EAD76DA47E2EB64D6BD8033 \ 5B276574E8E62617908D4917F19E 75920F22
```
Adding TLSA records

- `yum install hash-slinger`
- `tlsa --create fedoraproject.org`
- `tlsa --create --insecure www.microsoft.com`
- `tlsa --verify nohats.ca`
Other data suggestions

- PGP/GPG fingerprints in DNS?
- OTR (IM) fingerprints in DNS?
- File hashes in DNS? (rpm, tripwire, IMA/EVM)
- SElinux policies via DNS?
- Software Update Versions in DNS?
- Distributed secure twitter-like publishing?
  1. tweets.fp.org. IN TXT "#dnssec in @fedora is neat!"
  2. tweets.fp.org. IN TXT "#sectorca people think I'm nuts"
Offline DNSSEC chains

- My laptop stores DNSSEC hierarchy from the root ("." ) to itself ("pwouters.redhat.com")
- Your laptop does same, from "." to "johndoe.toronto.example.ca"
- Laptops can now authenticate each other offline via adhoc/bluetooth – no internet required as long as both have the root ("." ) key.
DNSSEC and Firefox

- addon: DNSSEC Validator (labs.nic.cz)
- addon: Extended Validator (os3sec.org)
- addon: DNSSEC / TLSA validator
  - people.redhat.com/pwouters/
- All proof of concept addons to push browser vendors for native integration
DNSSEC Validation

Invalid domain name signature has been detected. It could indicate spoofed connection!

This website does not supply identity information.

Your connection to this website is not encrypted.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn’t continue.

Get me out of here!

Technical Details:

- Domain name: fedoraproject.org
- Error type: DNSSEC validation failure
- Server certificate: None
- Port: 443
- Protocol: HTTPS
TLSA / DNSSEC Validation

Domainname is secured by DNSSEC, and TLSA proved the certificate is valid (and no CA)
You are connected to

nohats.ca
which is run by
(unknown)

Your connection to this website is encrypted to prevent eavesdropping.

More Information...
Questions?
Ideas?

Contact:
pwouters@redhat.com
LetoAms on FreeNode, Twitter, etc
But djb says 'DNSSEC is evil'

- DNSSEC does not cause 51x amplification (numbers published by Dan Kaminsky and me)
- DNS privacy is more then just encryption
- DNScurve would destroy all DNS caches (causing much worse amplification)
- DNScurve causes CPU load on DNS auth servers (talk about Denial of Service attack)
- The OpenDNS business model is forging dns...
- DJB is wrong – come talk to me afterwards
But Moxie Marlinspike says 'DNSSEC and Verisign are evil'

- 200+ million domain names, can't store/verify
- X-Files was wrong, you need to trust someone
- Hierarchical trust or decentralized trust?
  - “Peer to Peer” DNS cannot work, uniqueness requires enforcement, human-readability
  - Moxie is postponing the inevitable trust. come talk to me after the presentation