

8. Appendix:

8.1 Terminology of DNS

DNS Terminology

To understand the DNS and the DNS-specific recommendations in this document, operators and administrators should be familiar with the following terms:

Resolver: A DNS client that sends DNS messages to obtain information about the requested domain name space.

Recursion: The action taken when a DNS server is asked to query on behalf of a DNS resolver.

Authoritative Server: A DNS server that responds to query messages with information stored in Resource Records (RR) for a domain name space stored on the server. A domain needs at least 2 nameserver, one master, one slave. The slave name server will keep up with master nameserver for the change of configuration of domain.

Recursive Resolver: A DNS server that recursively queries for the information requested in the DNS query.

FQDN: A Fully Qualified Domain Name is the absolute name of a device in the distributed DNS database.

Resource Record: A Resource Record (RR) is a format used in DNS messages that is composed of the following fields: NAME, TYPE, CLASS, TTL, RDLENGTH, and RDATA.

Domain: A domain name and all domain names below it, sub-domains; that is, all domain names ending with the domain name. Domains are delegated from one nameserver to another.

How to make your domain more secure: Implementation DNSSEC on your domain immediately

Zone: A database that contains information about the domain name space stored on an authoritative server. A zone is the same as a domain minus all delegated domains.

Resource Record Set: All resource records with the same NAME, TYPE, and CLASS; however, the RDATA is different. A response from DNS is always a complete Resource Record Set (or RRSet in short). An example of an RRSet would be multiple NS records for a respective zone or domain.

Delegation Signer (DS): The DS RR is a DNSSEC record type that is used to secure a delegation for a zone.

Zone Signing Key (ZSK): This is used to sign all the RRSets in a zone.

Key Signing Key (KSK): This is used to only sign the DNSKEY RRSet.

DNSKEY Resource Record: This DNSSEC RR is used to store the public keys that are used to sign the records for a zone. This RR can contain either a ZSK or a KSK.

EDNS: Extension Mechanisms for DNS (EDNS, as defined in RFC 2671) is an IETF specification written to remove DNS message size restrictions initially imposed (RFC 1035 Section 2.3.4. Size limits) on the DNS protocol. EDNS allows clients to advertise their capabilities to DNS servers and one of those capabilities that is related to DNSSEC is the ability for a client to advertise its reassembly buffer to a DNS server, for example, a DNS client can reassemble a DNS message sent over UDP that is larger (2000 bytes) than the legacy limit of 512 bytes.

DNSSEC OK (DO) EDNS header bit: This is a bit in the EDNS header that, when set to one ("1") in a DNSSEC-enabled query messages, indicates to the server that the resolver is requesting and able to accept DNSSEC RRs in the query response message.

8.2 Trust of chain

For DNSSEC to work, the recipient needs to know that the public key in use is trustworthy. The resolver asks the name server for its public key, but that public key is used to verify its own identity, which isn't very secure or verifiable.

To resolve this problem, a "chain of trust" is established. The chain starts by adding an "anchor" at the root name servers. Then each "link" in the "chain" is

How to make your domain more secure: Implementation DNSSEC on your domain immediately

signed against the previous "link." Here is our example using `www.comp116.edu`, which is an A record.

`www.comp116.edu` is signed at the nameservers for `comp116.edu`;

`comp116.edu` is signed by the TLD servers for `.edu`;

`.edu` is signed by the root nameservers.

An anchor for `.edu` is stored on the root nameservers in the form of a DS (Delegation Signer) record.

8.3 helpful scripts for network manager

Each time you edit the zone by adding or removing records, it has to be signed to make it work. So you can create a script for this so that we don't have to type long commands every time.

```
root@master# more /usr/sbin/zonesigner.sh
```

```
#!/bin/sh
PDIR=`pwd`
ZONEDIR="/etc/bind" #location of your zone files
ZONE=$1
ZONEFILE=$2
DNSSERVICE="bind9" #On CentOS/Fedora replace this with "named"
cd $ZONEDIR
SERIAL=`/usr/sbin/named-checkzone $ZONE $ZONEFILE | egrep -ho '[0-9]{10}'`
sed -i 's/'$SERIAL'/'$((SERIAL+1))'/' $ZONEFILE
/usr/sbin/dnssec-signzone -A -3 $(head -c 1000 /dev/random | shasum | cut
-b 1-16) -N increment -o $1 -t $2
service $DNSSERVICE reload
cd $PDIR
```

Save the file and make it executable.

```
root@master# chmod +x /usr/sbin/zonesigner.sh
```

Whenever you want to add or remove records, edit the `example.com.zone` and **NOT the .signed file**. This file also takes care of incrementing the serial value, so you needn't do it each time you edit the file. After editing it run the script by passing the domain name and zone filename as parameters.

```
root@master# zonesigner.sh example.com example.com.zone
```

You do not have to do anything on the slave nameserver as the incremented serial will ensure the zone is transferred and updated.

A screenshot of a Google Chrome browser window displaying a terminal session. The browser's address bar shows the URL: https://ssh.cloud.google.com/projects/comp116-199318/zones/us-east1-b/instances/instance-1?authuser=0&hl=zh_CN&projectNumber=1039789723119. The terminal window shows the following text:

```
/ This is the primary configuration file for the BIND DNS server named.
/
/ Please read /usr/share/doc/bind9/README.Debian.gz for information on the
/ structure of BIND configuration files in Debian, *BEFORE* you customize
/ this configuration file.
/
/ If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

The terminal window has a title bar with standard Linux window controls (minimize, maximize, close) and a status bar at the bottom showing "named.conf" 11L, 463C. On the right side of the screen, there is a vertical taskbar with various application icons, including a file manager, a terminal, and a web browser. At the bottom right, a system tray shows the date and time: "12:47 PM Sunday 4/29/2018".

bycom1299@instance-t: ~ - Google Chrome

Securehttps://ssh.cloud.google.com/projects/comp116-199318/zones/us-east1-b/instances/instance-17authuser=0&hl=zh_CN&projectNumber=1039789723119

options {
 directory "/var/cache/bind";

 // If there is a firewall between you and nameservers you want
 // to talk to, you may need to fix the firewall to allow multiple
 // ports to talk. See http://www.kb.cert.org/vuls/id/800113

 // If your ISP provided one or more IP addresses for stable
 // nameservers, you probably want to use them as forwarders.
 // Uncomment the following block, and insert the addresses replacing
 // the all-0's placeholder.

 forwarders {
 0.0.0.0;
 };

 //=====
 // If BIND logs error messages about the root key being expired,
 // you will need to update your keys. See https://www.isc.org/bind-keys
 //=====
 recursion no; #authoritative server only
 allow-transfer { none; }; # no transfer for all domain
 auth-nxdomain no; # conform to RFC1035
 listen-on-v6 { any; };
}

};

"named.conf.optional.original" 26L, 964C

22,56-63

All

12:51 PM
Sunday
4/29/2018

英

How to make your domain more secure: Implementation DNSSEC on your domain immediately

Fig.2 named.conf.options

```
// Do any local configuration here
//
zone "comp116.edu" IN {
    type master;
    file "/etc/bind/zones/db.comp116.edu.signed";
}; # define the domain and file path of the db of this domain

// Consider adding the 1918 zones here, if they are not used in your
// organisation
//include "/etc/bind/zones.rfc1918";

"named.conf.local" 13L, 313C
```

Fig.3 named.conf.local

```
STTL 604800
0 IN SOA ns1.comp116.edu. bjcom1299@gmail.com. (
    604800 ; Serial
    604800 ; Refresh
    604800 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL

FORIGIN comp116.edu.
comp116.edu. IN NS ns1.comp116.edu.
ns1 IN A 10.142.0.2
www IN A 10.142.0.2

"db.comp116.edu" 12L, 280C
```

Fig.4 zone file

bycom1299@instance-1: ~ - Google Chrome

Secure | https://ssh.cloud.google.com/projects/comp116-199318/zones/us-east1-b/instances/instance-17authser=08hl=zh_CN&projectNumber=1039789723119

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vula/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        0.0.0.0;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    recursion no; #authoritative server only
    allow-transfer { none; }; # no transfer for all domains
    dnsmsec-validation yes;
    dnsmsec-enable yes;
    dnsmsec-lookaside auto;
    //key-directory "keys";
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};

//

"named.conf.options" 30L, 1064C
```

25,8 All

12:47 PM
Sunday
4/23/2018

bjcom1299@instance-1: ~ - Google Chrome

Secure | https://ssh.cloud.google.com/projects/comp116-199318/zones/us-east1-b/instances/instance-1?authuser=0&hl=zh_CN&projectNumber=1039789723119

```

root@instance-1:/etc/bind/zones# ls -l
total 32
-rw-r--r-- 1 root bind 353 Apr 29 16:02 db.comp116.edu
-rw-r--r-- 1 root bind 7605 Apr 29 16:25 db.comp116.edu.signed
-rw-r--r-- 1 root bind 167 Apr 29 16:25 dsset-comp116.edu
-rw-r--r-- 1 root bind 605 Apr 29 15:55 Kcomp116.edu.+007+01610.key
-rw----- 1 root bind 1779 Apr 29 15:55 Kcomp116.edu.+007+01610.private
-rw-r--r-- 1 root bind 931 Apr 29 15:56 Kcomp116.edu.+007+63489.key
-rw----- 1 root bind 3319 Apr 29 15:56 Kcomp116.edu.+007+63489.private
root@instance-1:/etc/bind/zones#

```

6

How to make your domain more secure: Implementation DNSSEC on your domain immediately

```
Secure | https://ssh.cloud.google.com/projects/comp116-199318/zones/us-east1-b/instances/instance-1?authuser=0&hl=zh_CN&projectNumber=1039789723119
root@instance-1:/etc/bind/zones# dnssec-signzone -A -3 $(head -c 1000 /dev/random | shasum | cut -b 1-16) -N INCREMENT -o comp116.edu -t db.comp116.edu
head: cannot open '/dev/random' for reading: No such file or directory
Verifying the zone using the following algorithms: NSEC3RSASHA1.
Zone fully signed:
Algorithm: NSEC3RSASHA1: ESKs: 1 active, 0 stand-by, 0 revoked
db.comp116.edu.signed
Signatures generated: 10
Signatures retained: 0
Signatures dropped: 0
Signatures successfully verified: 0
Signatures unsuccessfully verified: 0
Signing time in seconds: 0.014
Signatures per second: 696.767
Runtime in seconds: 0.045
root@instance-1:/etc/bind/zones#
```

Fig.7 the result of dnssec-signzone command

```
Secure | https://ssh.cloud.google.com/projects/comp116-199318/zones/us-east1-b/instances/instance-1?authuser=0&hl=zh_CN&projectNumber=1039789723119
root@instance-1:/etc/bind/zones# dig DNSKEY comp116.edu. @localhost +multiline

; <<> Dig 9.10.3-P4-Debian <<> DNSKEY comp116.edu. @localhost +multiline
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 30763
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
;; QUESTION SECTION:
;comp116.edu.                IN DNSKEY

;; ANSWER SECTION:
comp116.edu.                604800 IN DNSKEY 256 3 7 (
    AWEAAc3baUf6wKjV35ogfK5S0lKozhraoQE2PwGc4X/e
    teNvYF6sewv/juY7ER4FnRj0mdDlGA3h9K+04pjamCG
    Q2FK2zc3LPV/8x908i13Q0/JUWgMWBINfdw+9ahNUA
    ZU3AkBQm2Ia1e4hTFmktKCHOspxeCLlGhgqlqv70LRe8
    vVjoaPhFYozin7Qe+DAFmNC91e8zde5lpc0cPHe534A
    23qEMuX2K8z+QeU9p/4cMBHBT+137IFXAAljY+GJ5
    b7a0S5yabt7DyYpWg3einowL6Kugyx711le94qpgg
    Ez8TzKeYDX19825pL0vtcspHwWbrkK08fc8=
    ) ; ZSK; alg = NSEC3RSASHA1; key id = 1610

comp116.edu.                604800 IN DNSKEY 257 3 7 (
    AWEAAc740o0F7TtImwSXIpaqIr8CuanYAYz9Z/Tj80
    v7S14moAdF3eoPqD33uLIYxxzi9gj3vdnBUCBdf9YDQ
    hshUpf/X7Ing5Ylma1JPCkBJkg7U6VFRGgP64yj23MK
    i6KXl07rnQSKnQ936fututfcJG2p0F5Prjzwf1blrtU
    sF4cMfVvT8Hf8m0n09AG0UFIEM+K8gDgQc311V
    0R8ezn0qltv9z0yaN4FpWcyAw6fzX0q7A98F0hA150
    rqlYhgEdVY5GGSh20AlCFTw2RbfSR9st9YFvtW1aeRY
    7PWGfCQ5382XohdPiv+Ghd2W+PRFV7KokyPVFXOGMEIz
    qRwUc3h70e1af6Xa3v1Dg1gfaqP0GofzPMWVJgaokk7L
    ph2978qem4Aof01xhJ/QW0u191hXtC0eAd0pLd5G0xDb
    NQ3g4Wh0Ks2ANadiyzDp06m3Ma1CehqkNVTla01QeEG
    CanFtB1tb1OPq/C36VAGUj+98znSiNgpzL5Ekz1gPUEG
    UyITWciI32Qy0bM4/9d3vV5jnlv0k1hGr5Cl3p398V89
    t0DP00dWYr3V8Ww6jLFX0X2HlQlndRoQz/sdn0P6
    D1tEMqg8D38uHE2PuoOmK98/Cwa7pt18Qa027Hc59D1V
    HsKy9jwCbF404s1D44Tnj09efl3
    ) ; KSK; alg = NSEC3RSASHA1; key id = 63489

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Sun Apr 29 16:24:01 UTC 2018
;; MSG SIZE rcvd: 848

root@instance-1:/etc/bind/zones#
```

Fig.8 example of dig a signed response

How to make your domain more secure: Implementation DNSSEC on your domain immediately

```
bjcom1299@instance-1: ~ - Google Chrome
Secure | https://ssh.cloud.google.com/projects/comp116-199318/zones/us-east1-b/instances/instance-1?authuser=0&hl=zh_CN&projectNumber=1039789723119

-rw-r--r-- 1 root bind 353 Apr 29 16:02 db.comp116.edu
-rw-r--r-- 1 root bind 7605 Apr 29 16:05 db.comp116.edu.signed
-rw-r--r-- 1 root bind 167 Apr 29 16:05 dsset-comp116.edu.
-rw-r--r-- 1 root bind 605 Apr 29 15:55 Kcomp116.edu.+007+01610.key
-rw-r--r-- 1 root bind 1779 Apr 29 15:55 Kcomp116.edu.+007+01610.private
-rw-r--r-- 1 root bind 951 Apr 29 15:56 Kcomp116.edu.+007+63489.key
-rw-r--r-- 1 root bind 3319 Apr 29 15:56 Kcomp116.edu.+007+63489.private
root@instance-1:/etc/bind/zones# dig A www.comp116.edu. @localhost +noadditional +dnssec +multiline

;<> DIG 9.10.3-P4-Debian <> A www.comp116.edu. @localhost +noadditional +dnssec +multiline
;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 43002
;; flags: qr aa rdq QUERY 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; RDNS: version: 0, flags: do: udp: 4096
;; QUESTION SECTION:
;www.comp116.edu.      IN A

;; ANSWER SECTION:
www.comp116.edu.      604800 IN A 10.142.0.2
www.comp116.edu.      604800 IN RRSIG A 7 3 604800 (
    20180529150527 20180429150527 1610 comp116.edu.
    U4TxgmFUIjG7GyeVVoHss7lc+xs7lt5Ij1Q38kmaRoD
    D5+Lkz26V1z+yKt6nfr5zN8S5UxqRm0aO/YQ9ha20
    +j1PmuuSITVHD4Y21EoyJd9H8Df5PK5eXGepRly5ps8
    bt9mlKVMAndvupq3MzhG3J1V1Agtr074NhRYNz=Ac2+
    xcnBul4pPrQ5Bz11M/zUzAXT+ULp4WuFbrPCvTW4qOh
    a90vg/t7f0mMyR00hcj3eQ7YmWcD1aa3eQ7OpoutaVRS
    fP19W0Qa=J20U7Oc48lMnatKYVYtpttGrcB8ay2rke
    FV54kJ8dhtPocVrg1DfR0O9g2R68h49hw= )

;; AUTHORITY SECTION:
comp116.edu.          604800 IN NS ns1.comp116.edu.
comp116.edu.          604800 IN RRSIG NS 7 2 604800 (
    20180529150527 20180429150527 1610 comp116.edu.
    E6+BvcQk418eX2RALpvnJEpIDgmUgUxXaUTNH+qr7yi
    13n2lUzCKKFF111+H1v1/R8lQl1DqR5B8z5FLODM8
    D1bX5r2pIR24Ate5ipN81m/skUC+/pucPH19gIFQDFU
    QjA1813nJD/r5k61xpyfKM+akVTJ8Ra6w1bbngQAAtHF
    BcMBaSNQnEL48bCY8IqjN5F77Dcl85KdethU2+RKN1d8
    L3jKuY2fcsUhgfoziIfgjr08H2+cnN1MK6jxbwk2cr
    1yVWmj7tmK61tp13Ro/81J2w4hOndJ8M1Qns8BLAME
    dth1KVMq7Vy5NS5FVNp88cA2wM/f35aghg= )

;; Query time: 0 msec
;; SERVER: 11f531:11
;; WHEN: Sun Apr 29 16:17:08 UTC 2018
;; MSG SIZE rcvd: 991

root@instance-1:/etc/bind/zones#
```

Fig.9 another example of dig a signed response