

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

FENG WANG

MENTOR: MING CHOW

Abstract

The Domain Name System(DNS) is the fundamental part of Internet. DNS protocol resolves domain names to IP addresses. The original protocol is simple but not safe, there are more and more DNS abuse incidents. The most famous DNS abuse is DNS spoof, you will get the malicious domain record then go to a wrong site but with legitimate domain name. DNS Security Extensions (DNSSEC) is a specification which aims at maintaining the data integrity of DNS responses. This paper gives us an overview of DNSSEC specification, including the purpose, principle and key features. We will show how to build a secure DNS server with DNSSEC extension step by step. Then we will simulate hacker's method of DNS spoof and see how the new DNS server reacts. Finally, the paper will propose the practical recommendations and tips for successfully implementation of DNSSEC in the normal user domain.

1. Introduction

It would be easy to make the argument that DNS is perhaps one of the fundamental protocols on the Internet. DNS resolves unintelligible IP addresses to easily readable domain names. But DNS is susceptible to a range of easy attacks, from simple denial of service to serious hijacking and cache-poisoning attacks. The DNS query is sent into the void, and the response is blindly sent back with no authentication or verification. An attacker could make a continuous stream of bogus data at a DNS server hoping to confuse legitimate replies with malicious ones. We need a mechanism of certainty of signing and verifying records.

2. To the community

This paper deals mainly with a famous DNS security specification and its implementation for real domain system. The purpose of this paper to show the steps to make domain system more secure and easiness to do the upgrade. When all the website implements its DNSSEC, the world of website will be more secure: a whole range of cyber-attacks become much more difficult to orchestrate.

3. DNS and DNSSEC

DNS is a globally distributed, scalable, hierarchical, and dynamic database that provides a mapping between hostnames, IP addresses (both IPv4 and IPv6), text records, mail exchange information (MX records), name server information (NS records), and security key information defined in Resource Records (RRs). The information defined in RRs is grouped into zones and maintained locally on a DNS server, so it can be retrieved globally through the distributed DNS architecture.

DNS primarily translates hostnames to IP addresses or IP addresses to hostnames. This translation process is accomplished by a DNS resolver (this could be a client application such as a web browser or an e-mail client, or a DNS application such as BIND) sending a DNS query to a DNS server requesting the information defined in a RR.

DNSSEC (Domain Name System Security Extensions) adds resource records and message header bits which can be used to verify that the requested data matches

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

what the zone administrator put in the zone and has not been altered in transit. DNSSEC doesn't provide a secure tunnel; it doesn't encrypt or hide DNS data. It was designed with backwards compatibility in mind. The original standard DNS protocol continues to work the same.

DNS Security Extensions (DNSSEC) aims at enabling the data integrity of DNS responses. DNSSEC signs all the DNS resource records (A, MX, CNAME etc.) of a zone using PKI (Public Key Infrastructure). Now DNSSEC enabled DNS resolvers (like Google Public DNS) can verify the authenticity of a DNS reply (containing an IP address) using the public DNSKEY record.

4. Adding DNSSEC to your domain

4.1 set up a domain to play

After installing BIND software on your linux box, by default, all the configuration files of BIND software will be installed on /etc/bind directory of your system.

There are 3 files are very important:

named.conf,named.conf.options,named.conf.local.

The named.conf file is just a wrapper, it includes named.conf.options and named.conf.local.

named.conf.options says how bind will work, authoritative or resolver mode.

named.conf.local says that where is the zone file for local domain for the bind to explain.

In this thesis, my bind will work at authoritative mode only, I defined a fake domain for demonstration: comp116.edu. Its zone file is db.comp116.edu under the subdirectory of /etc/bind/zones.

4.2 add DNSSEC

4.2.1 enable DNSSEC

Now we can add DNSSEC to our bind. This is really simple: just add some lines of words to named.conf.options. 1, dnssec-validation yes; 2, dnssec-enable yes; 3, dnssec-lookaside auto. The first line tells bind should use chain-of-trust to validate dnssec responses from other server. It is always used in ISP's resolver name

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

server and all server need to trust TLN serves. The second line tells bind to give the signed authoritative responses to queries. The third line give the newbies of DNSSEC a solution to avoid manually key management.

4.2.2 generate the key

After enabling DNSSEC on bind system, then we can generate the key to sign our demo domain. Since DNSSEC uses the PKI infrastructure, so we will generate the public key and private key. These are two sets of keys: ZSK and KSK. ZSK is used by recursive server to validate zone data RRset; KSK is used by recursive server to validate DNSKEY RRset.

The bind software provides the tools to generate keys: dnssec-keygen.

```
#dnssec-keygen -f KSK -a 'your name of algorithm' -b 4096 -n ZONE your's domain
```

In this thesis, I choose NSEC3RASSHA1 algorithm, the domain is: comp116.edu.

```
#dnssec-keygen -a 'your name of algorithm' -b 2048 -n ZONE your's domain
```

In this thesis, I choose NSEC3RASSHA1 algorithm, the domain is: comp116.edu.

Then you will get 2 pair keys. Keep your private key in a private place!

After generating all the public keys, we need to include these two public keys in our zone file. You can add 2 lines to the zone file by yourself.

```
$INCLUDE name of KSK public file;
```

```
$INCLUDE name of ZSK public file;
```

4.2.3 sign RR

The bind software provides the tools to generate keys: dnssec-signzone.

This command will need a random salt for signing zone file. This salt is a randomly 16 characters in HEX. This will increase the difficulty to decipher.

You can simply give the salt such as 1234567890ABCDEF, anything you like. I use a bash script to generate this salt. Thanks for google to get this one.

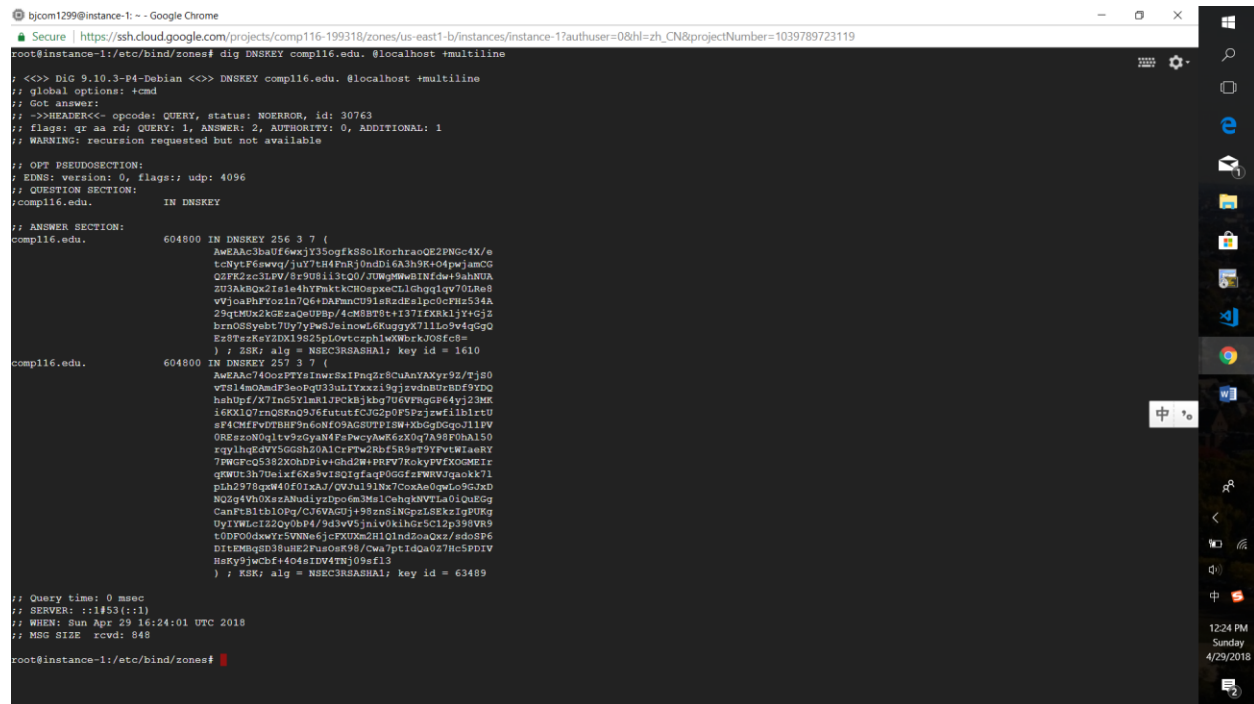
The command and its output see the figure below. You can how many signatures are generated and the algorithm. Now we will get a signed version of zone file at the same directory of original zone file.

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

Then we don't forget to revise named.conf.local, use the new signed version zone file to replace the original unsigned zone file. At last, we need to restart our DNS server software to update its new configuration.

4.2.4 local test

After restarting our bind software, now our bind works at authoritative mode and ready to answer query with the signed mode. We will use the great tool: dig to test our new bind. Firstly, we will query the SOA record of our domain, then query an A record of www host under our domain. The command and its output are as the figure blow. You will see all responses are followed by its signature, and the responses are longer than the original unsigned version.



```
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# dig 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 (
    AwEAAc3baU6wzj35ogfk8S0LKozhzoQE2PWCc4K/w
    tcNytP6swvq/juYtR4PnRj0ndDi6A3h9K+04pwjamCG
    Q2FK2zc3LFV/8r908i13tQ0/JUWgWwBINFdw+9ahNUA
    ZU3AkBQx2Ie4e4hYFaktKCHOspkeCLIGHqqlqv70LRs9
    vWjoaBhPtozin7Qe+DAFmC0918adaiPccCPH534A
    29qTmWz2cczccq0P9p/4CM988t+137iEXkl3Y4G5E
    brnOSSyabt7Dy7ypwSJeinowL6KugjyX711Lo9v4qGgQ
    Ez8TszKsYDX19825pL0vtcphlWkWrkJOSfc8=
    ) ; ZSK; alg = NSEC3RSASHA1; key id = 1610
comp116.edu. 604800 IN DNSKEY 257 3 7 (
    AwEAAc74OozPTyE1nwzSKIPnq2r8CuAnYAXyr92/Tj89
    vTS14moAmdF3eoFg33uLiYxxzi9gjevdm8URBDF9YDQ
    hahUpE/X7Ing5YlMk1JPCkBJkbj706VFRqGP64yj2JMR
    16KX1Q7mQRK0p36faturfcG2p0F5P3jwE1b1et9
    sF4CMFPvDTHF9n6eNIO9AGSUTPDIW+Xbzq9Gqo311PV
    QREszonQltv9sGyaN4FpWcyAmR6eX0q7A98F0hA150
    rqv1hgEdVY5GGSh20A1CFTw2Rbf5R9sT9YFvtWiaRY
    7PWGpcQ5382X0hDfiV+Ghd2W+PRFV7RokypPVXOCMEir
    qgwUz3h7e1aifOks9vS2qigfagp0Gc2FwVUVQqoKx7L
    pLh2978qk40f0iKAJ/QVJul91Nz7CoxAe0qWLo9GJxD
    NQ2g4Wh0KszANuDiyrzDpo6m3Me1CehqkNVTLa0iQEGg
    CanFt81t10Pq/C36VAGUj+98znS1NGpZL8EzkygP0RG
    dY1TWGci22oy0B44/9d3v951niw0k1h8zC12p398V89
    t0DF00dxwYr5VNN6e3cFXDXa2H1Q1ndZoaQxZ/adoEP6
    D1tEMq8D38uWE2Fuo0s98/Cwa7ptidQa027Hc5PDIV
    HsKy9jwCbF404e1D44TNj09ef13
    ) ; RSK; 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#
```

5. Future work

I should register my domain to a DNS registration service party, such as Godaddy(www.godaddy.com). This website is the world's largest domain name Registrar. This registrar complies to DNSSEC specification recommended by ICANN(www.icann.org). By doing so, I can configure my DS record with this registrar. Then any DNS resolver server which has DNSSEC enabled can use the

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

public key of my domain to authenticate the query results of my domain. I can use <http://dnssec-debugger.verisignlabs.com> to test DNSSEC of my domain.

Unfortunately, while ICANN mandates that “Registrar must allow its customers to use DNSSEC upon request...” nearly all registrars (while technically compliant), offer no support for creating, maintaining and signing DNSSEC keys and records.

There still another thing to be done in future: Because there are more RRs in DNS, so there should be more traffic for DNS serves, what the impact to the performance of DNS server is also needed to examine.

6. Conclusions

We have shown that the basic architecture of DNS and concepts of DNSSEC. In this paper, we set up a simple domain, and add DNSSEC to this domain, and test the results of adding locally. The whole steps are very easy to understand, we need not to modify all the records of our domain except to add some new RRs related to DNSSEC. Because DNS is the basic of world of websites, if our DNS is more secure, hackers in the world will have less opportunities to make fake information. Also, we can see that, not all registrar supports DNSSEC, we need to increase awareness of DNS security problems. We also need more corporate and commercial end-users to implement DNSSEC where possible and put pressure on their domain registrars to improve support. Without awareness and demand, we will never reach the critical mass required to make secure DNS a reality.

References

- 1, Survey of DNS abuse type: https://www.sidnlabs.nl/a/weblog/survey-of-dns-abuse-types?language_id=2
- 2, Preparing for DNSSEC: <https://www.cisco.com/c/en/us/about/security-center/dnssec-best-practices.html>
- 3, Official ISC DNSSEC guide: <https://ftp.isc.org/isc/dnssec-guide/html/dnssec-guide.html>
4. DNSSEC – What Is It and Why Is It Important?
<https://www.icann.org/resources/pages/dnssec-qa-2014-01-29-en>
5. how to setup dnnsec on authoritative server.
<https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server--2>