“Signing a .CO domain with DNSSEC extensions”

Gonzalo Romero

Chief Security Officer (C.S.O.)

LACNIC 21 - DNSSEC Workshop

May 4th – 5th, 2.014

Agenda

- Setup (HW and SW)
- Steps to sign a .CO domain/zone with DNSSEC
- Questions?

Setup (HW and SW) – 1 / 4

- Registration of the test .CO domain
  - DNSTEST.GOV.CO
  - DNS Servers:
    - NS.DNSTEST.GOV.CO and NS2.DNSTEST.GOV.CO
    - Public IP address: w.x.y.z
- PC with UBUNTU 14.04 (fully updated)
  - OpenSSH, BIND9, AppArmor, Apache2
- File “/etc/bind/named.conf.local”
  - zone “dnstest.gov.co” {
    - type master ;
      - file “/etc/bind/db.dnstest.gov.co”;
  - };

Setup (HW and SW) – 2 / 4

- File “/etc/bind/db.dnstest.gov.co”
  - $TTL **120**
  - @ IN SOA ns.dnstest.gov.co. dnsmng.dnstest.gov.co. (
    - 2014050401 ; Serial
    - 3600 ; Refresh
    - 1800 ; Retry
    - 2419200 ; Expire
    - **120** ; Negative Cache TTL
  - @ IN NS ns.dnstest.gov.co.
  - @ IN NS ns2.dnstest.gov.co.
  - @ IN A w.x.y.z
  - ns IN A w.x.y.z
  - ns2 IN A w.x.y.z
  - www IN A w.x.y.z

Setup (HW and SW) – 3 / 4

- Create file “/var/log/query.log”
  - sudo touch /var/log/query.log
  - sudo chown bind /var/log/query.log
- File “/etc/bind/named.conf.local”
  - logging {
    - channel query.log {
      - file “/var/log/query.log”;
      - severity debug 3;
    - };
    - category queries { query.log; };
    - };

Setup (HW and SW) – 4 / 4

- Edit file “/etc/apparmor.d/usr.sbin.named” and add:
  - /var/log/query.log w,
- Reload the profile:
  - cat /etc/apparmor.d/usr.sbin.named | sudo apparmor_parser -r
- Restart BIND9
  - sudo service bind9 restart
- Validate DNS setup
  - named-checkzone dnstest.gov.co /etc/bind/db.dnstest.gov.co
- Should get as output:
  - zone dnstest.gov.co/IN: loaded serial [SERIAL]
  - OK

Steps to sign a .CO zone with DNSSEC

(0a) Establish duration (time validity) y # of ZSK and KSK keys to use

(0b) Determine if NSEC or NSEC3 to be used

(0c) Determine sizes, algorithm and HASH of the ZSK and KSK keys

1) Generate ZSK and KSK keys
2) Sign the zone and generate the “DS Records”
3) Include parameters related with DNSSEC in the BIND setup
4) Load the signed zone
5) Send “DS Records” to the .CO Root-Zone via an EPP update
6) Use a “DNS recursive resolver” to validate the signup.

Steps to sign a .CO zone with DNSSEC – 1 / 6

(0a) Establish duration (validity in time) of the ZSK and KSK keys, and how many ZSK and KSK keys will be used

- ccTLD root-level Key Rollover: ZSK (quarterly), KSK (annual)
- At least one (1) pair of ZSK y KSK keys

(0b) NSEC or NSEC3 to be used?

- NSEC is more “simple”
- NSEC3 avoids “walking through the zone”
- .CO supports both

(0c) Define sizes, algorithm and HASH of the ZSK and KSK keys

- ZSK = 1.024 bits; KSK = 2.048 bits (monthly refresh)
- Algorithm and HASH = RSA/SHA2-256

Steps to sign a .CO zone with DNSSEC – 2 / 6

(1) Generate ZSK and KSK keys, via “dnssec-keygen”

- Signup Date: **YYYY/ MM / DD**
- Create “/etc/bind/keys” folder/directory
- ZSK (quarterly):
  - sudo /usr/sbin/dnssec-keygen –a RSASHA256 –b 1024 –K /etc/bind/keys –r /dev/urandom **–I YYYY[MM+3] [DD+7]** 00 00 00 **–D YYYY []+1 []+3** 00 00 00 –n ZONE dnstest.gov.co
  - Generates files [ZSK].key and [ZSK].private
- KSK (annual):
  - sudo /usr/sbin/dnssec-keygen –f KSK –a RSASHA256 -3 –b 2048 –K /etc/bind/keys –r /dev/urandom **–I [YYYY+1] [MM] [DD+7]** 00 00 00 **–D [] []+1 []+3** 00 00 00 –n ZONE dnstest.gov.co
  - Generate files [KSK].key and [KSK].private

Steps to sign a .CO zone with DNSSEC – 3 / 6

(2) Sign the zone, via “dnssec-signzone”

- cd /etc/bind
- sudo /usr/sbin/dnssec-signzone –t –p –S –K /etc/bind/keys –d /etc/bind/keys –s **YYYY MM DD HH MM SS** –o dnstest.gov.co db.dnstest.gov.co
- Generates
  - “/etc/bind/db.dnstest.gov.co.**signed**”
- and
  - “/etc/bind/keys/**dsset**.dnstest.gov.co”,
- which contains the “DS Records”.

Steps to sign a .CO zone with DNSSEC – 4 / 6

(3a) Include DNSSEC related configuration parameters in the BIND setup

- File “/etc/bind/named.conf.**local**”
  - zone “dnstest.gov.co” {
    - type master ;
      - // file “/etc/bind/db.dnstest.gov.co”;
      - file “/etc/bind/db.dnstest.gov.co.**signed**”;
      - dnssec-secure-to-insecure yes;
      - auto-dnssec **allow**;
      - allow-update {
        - 127.0.0.1; # IP’s which will make “nsupdate” calls to update the zone
    - };
  - };

Steps to sign a .CO zone with DNSSEC – 5 / 6

(3b) Include DNSSEC related configuration parameters in the BIND setup

- File “/etc/bind/named.conf.**options**”
  - options {
    - directory “/var/cache/bind”;
    - dnssec-validation auto
    - auth-nxdomain no;
    - // listen-on-v6 { any; };
    - dnssec-enable yes;
    - sig-validity-interval 30; # Unit = Days
    - sig-signing-nodes 100; # Default = 100
    - sig-signing-signatures 100; # Default = 10
    - key-directory “/etc/bind/keys/”;
  - };

Steps to sign a .CO zone with DNSSEC – 6 / 6

(4) Load the signed zone

- “sudo service bind9 restart” and validate “/var/log/syslog”

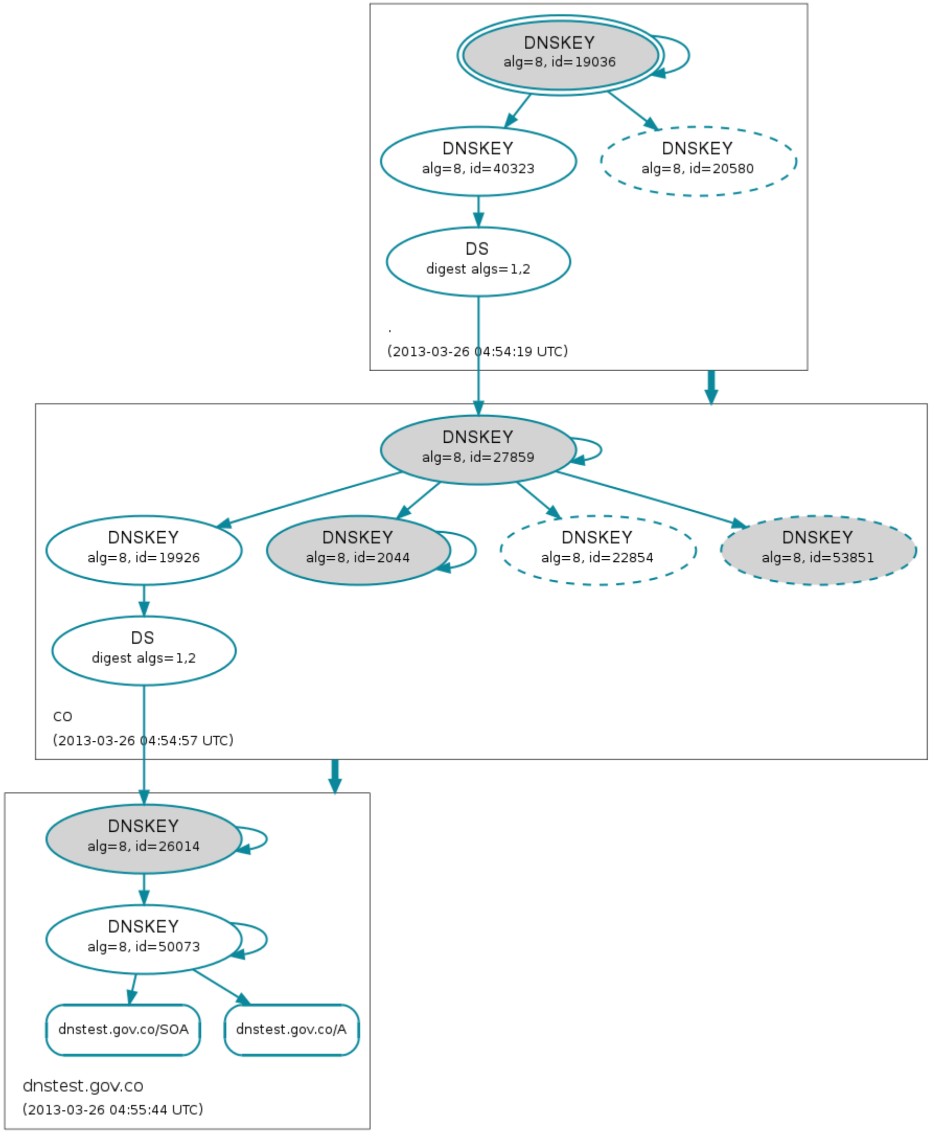
(5) Send DS Records to .CO Root-Zone via an EPP update

- 3rd level “non-commercial” (EDU/GOV/ORG/MIL.CO) records:
  - Email to dnssec@cointernet.com.co from WHOIS Registrant addresses
- Commercial and 2nd level: via the Registrars

(6) Use “DNS Recursive Resolver” to validate the zone signup

- “dig +dnssec +multiline” enables the validation flag: “AD” => signed OK (authenticated query)
- DNS-OARC (https://www.dns-oarc.net/oarc/services/odvr)
  - dig @149.20.64.20 dnstest.gov.co +dnssec +multiline
- DNSVIZ.NET (http://www.dnsviz.net)
- CZ.NIC DNSSEC-Validator (http://www.dnssec-validator.cz)

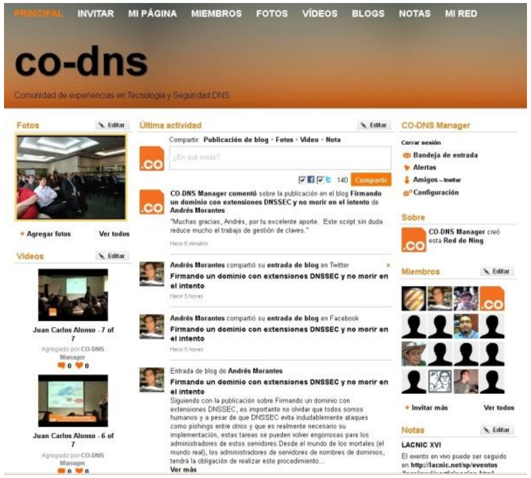
DNSVIZ.NET – dnstest.gov.co



CO-DNS – Virtual Community related with DNS IT and Security topics

- CO-DNS
  - http://co-dns.cointernet.com.co
- How to be a member?
  - Send an email to

  Gonzalo@COInternet.CO



co-dns

Comunidad de experiencias en Tecnología y Seguridad DNS

Fotos

Videos

Juan Carlos Alonso - 7 of 7

Agregado por CO-DNS Manager

0 0

Juan Carlos Alonso - 6 of 7

Agregado por CO-DNS Manager

0 0

Última actividad

Compartir: Publicación de blog · Fotos · Video · Nota

¿En qué estás?

CO-DNS Manager comentó sobre la publicación en el blog **Firmando un dominio con extensiones DNSSEC y no morir en el intento** de **Andrés Morantes**

"Muchas gracias, Andrés, por tu excelente aporte. Este script sin duda reduce mucho el trabajo de gestión de claves."

Hace 6 minutos

Andrés Morantes compartió su **entrada de blog** en Twitter

Firmando un dominio con extensiones DNSSEC y no morir en el intento

Hace 5 horas

Andrés Morantes compartió su **entrada de blog** en Facebook

Firmando un dominio con extensiones DNSSEC y no morir en el intento

Hace 5 horas

Entrada de blog de **Andrés Morantes**

Firmando un dominio con extensiones DNSSEC y no morir en el intento

Siguiendo con la publicación sobre Firmando un dominio con extensiones DNSSEC, es importante no olvidar que todos somos humanos y a pesar de que DNSSEC evita indudablemente ataques como pishings entre otros y que es realmente necesario su implementación, estas tareas se pueden volver engorrosas para los administradores de estos servidores.Desde el mundo de los mortales (el mundo real), los administradores de servidores de nombres de dominios, tendrá la obligación de realizar este procedimiento...

Ver más

CO-DNS Manager

Sobre

CO-DNS Manager creó esta **Red de Ning**

Miembros

Notas

LACNIC XVI

El evento en vivo puede ser seguido en **http://lacnic.net/sp/eventos**

Questions?

.CO

Thank you!