DNSSEC

CaribNOG 5
April 2013

Juan Alejo Peirano
jpeirano@lacnic.net

Topics

- Introduction
  - DNS packet format
  - Vulnerabilities in DNS
- DNSSEC Overview
  - Use of DNSSEC
  - Resource Records: DNSKEY, RRSIG, DS, NSEC
  - Resource Records Sets
  - Trust Chain
- DNSSEC Application in LACNIC

lacnic

Introduction

- DNS Packet

  Header

  - Protocol Header (Flags)

  Question Section

  - Query we send to the DNS server

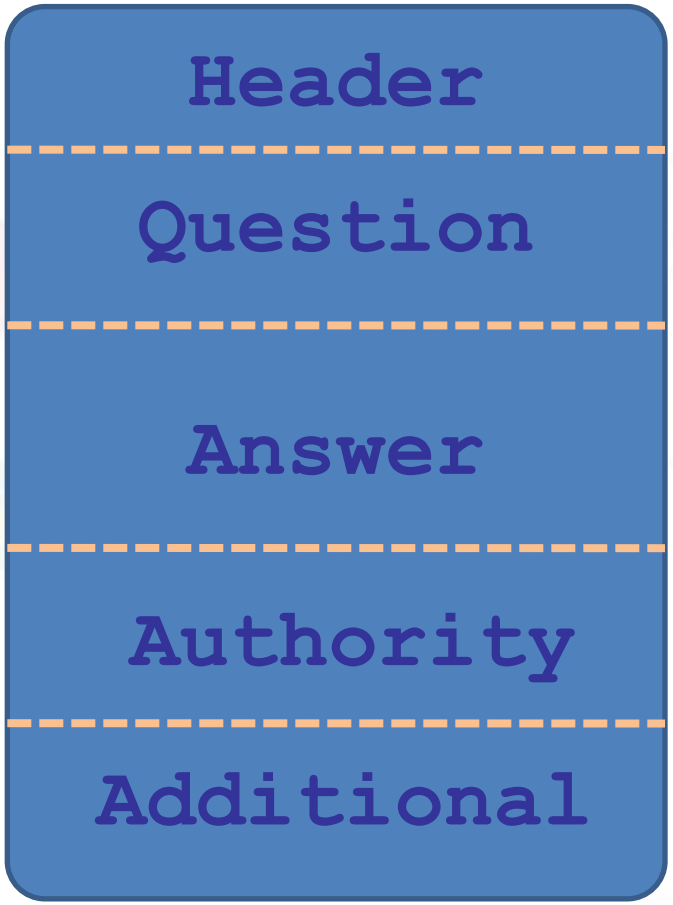
  Answer Section:

  - Resource Records that answer the query (if available)

  Authority Section:

  - Resource Records pointing to authoritative servers (optional)

  Additional Section



Introduction

- *Vulnerabilities in DNS*
  - DNS transmitted data is more prone to spoofing as it is mostly transported over UDP
    - Between master and slave (AXFR)
    - Between master and clients (AXFR)
  - Currently the DNS protocol does not have a way to validate information found in a query response
    - It is vulnerable to different poisoning techniques
  - Slaves servers do not have a way to authenticate the master servers.

lacnic

DNSSEC

- DNSSEC will protect us from data corruption and spoofing
  - It provides a way to validate both the integrity and the authenticity of the records contained in a DNS zone
    - DNSKEY, RRSIG, NSEC
  - It provides a way to delegate trust in public keys (trust chain)
    - DS
  - It provides a way to authenticate zone transfers between masters and slaves servers
    - TSIG

lacnic

DNSSEC

- DNSSEC is not a new protocol
- It is a set of EXTENSIONS added to the well known DNS protocol
  - The new RRs are
    - DNSKEY: DNS Public Key
    - RRSIG: Resource Record Signature
    - DS: Delegation Signer
    - NSEC: Next Secure
  - New Flags
    - AD: Authenticated data
    - CD: Checking disabled

lacnic

DNSSEC

- RRSets: Resource Record Sets
  - DNSSEC woks by signing RRSets and not individual RRs
  - A RRSet is a group of RRs that share characteristics
    - Class
    - Type
    - Name

lacnic

DNSSEC

- Example:
- Resource Record, a five value tuple:
  - www.example.com 86400 IN A 200.40.100.141
    - Name – www.example.com
    - Class – IN
    - Type – A
    - TTL – 86400 seconds
    - Value – 200.40.100.141

lacnic

DNSSEC

- RRSet
  - example.com
    - www 86400 IN A 200.40.241.100
    - www 86400 IN A 200.40.241.101
- Name, type and Class are the same in both RRs

DNSSEC

- Zone Signing
  - Public/Private keys are created for each zone
    - The *Public Key* is published in DNS using the DNSKEY record. It is also used to verify the signatures of the RRSets
    - The *Private Key* is used to sign the RRSets in the zone
  - A RRSet can have multiple signatures generated using different key-pairs

lacnic

DNSSEC

- Trust Chain
  - DS “Delegation Signature” Record
    - DS records sign the keys in their child zones
    - Is a way to verify the DNSKEY, as it is signed when the parent zone is signed.
    - DS record contains a HASH of the DNSKEY record content
    - In parents zones DS Records are signed with the parent zone keys
    - The root of DNS is also signed. The DS Record for “(dot)” is obtained out-of-band and installed locally in each server.

lacnic

```
juan@juan-VirtualBox:~$ dig +dnssec www.lacnic.net

; <<>> DiG 9.8.1-P1 <<>> +dnssec www.lacnic.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58843
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 8,
ADDITIONAL: 19

;; ANSWER SECTION:
www.lacnic.net.         60    IN    A     200.3.14.147
www.lacnic.net.         60    IN    RRSIG A 8 3 60 20130511152306
20130411142935 3690 lacnic.net. GxGqBvFrqSrpyv4
+RQOCWWOxCOOU1tQn8ep+ZWNEyFCMRbdLARROWJEe
yEcAVIuqcTqmISaDhLfQqlkk81GL6K12Eqx6Kl8XnVMu6MCQIcJdqGLS
yOBfIjkugEVKmqVr3bZoufaOVdksPIG3sda+8LiaVEO5Y6RExH5x+YLd
dyzyAYVZA015rVxJ/MQz/VJUdzYrK/0trZKf4AQLCsV0uqV97DrXc7Ho
L5PCINz31Ps+ZF6qhr8AawazhUFsiuSdJuJB+W82shBWx/cKavwoQvmY
i5HqWlroHrV/jsxPDt5Xvj/rG/9ajZ3is9shqCJbWhP0222arHJTKhPP qyf63Q==
www.lacnic.net.         60    IN    RRSIG A 8 3 60 20130511152306
20130411142935 25014 lacnic.net.
L6jMelnFMhhifegdf2QZBXoCZ48tkFSBTncOxAy8wYoYt+h6AUHKBd18
NRRDXox1E6tu2vYl2zMYKjGFONC9B8nXTLX1pmchM6MPNnmd2adgquan
blsaQliDTrtBrzmroqwkxzum4PS7LGot+cIaCVoyn6NWFNuZHj2xP5Ue
BR2bGWsy0m3/Idm5PvYciV42ApntWgX1YJ6+TxqomPQ/ig2xKeNRMUYY
o7By58pOkMcvs24TOI8kDq9WH/rlClX97Yp5HsXIAS5ot6UrKaxrjJeT
xh5I66CF7sYOgSS0lY9WEaYvowV8D426rPktZ2P4+OWMlADmzXSVD7Wy Tm1dmw==
```

RRSIG 1

RRSIG 2

```
;; AUTHORITY SECTION:
lacnic.net.        7200  IN    NS    NS2.lacnic.net.
lacnic.net.        7200  IN    NS    NS2.DNS.BR.
lacnic.net.        7200  IN    NS    ns.lacnic.net.uy.
lacnic.net.        7200  IN    NS    SEC3.APNIC.net.
lacnic.net.        7200  IN    NS    NS.lacnic.net.
lacnic.net.        7200  IN    NS    TINNIE.ARIN.net.
lacnic.net.        7200  IN    RRSIG NS 8 2 7200 20130511150959
20130411144709 3690 lacnic.net. G5L0S2GN3/G2r1VT9GJjNqNu4/aLfsSD0
+wgTuuFYKOEuYmmqoZzXPRM
+SyK+TTv5eg2Amc6JI5GviL8xajtc8L7uSMg56GFrCtbAoQSvYuh9Y/+
IFwtfEmRbAHBKhEXFtfkb0MV+eAq+T5vN2CzCfCBBrKhLDxDvJ3+cZqS
QgdgDEft6iiMy3Yk4VVZ8gA2VyONEImR7nF/aAKYZPSNJ19caS/7xAxZ
ottu4PEdDEjUQTIwJc51QqJZN6TT7IJZ+9arQ6ea6jPRL92BHb7eJKuD lGJVcl5+
0Gs+9cWDL3JANaSAqzjkSCjXdnV7qh6TF3fh+YOp+owpfT45 NW24cg==
lacnic.net.        7200  IN    RRSIG NS 8 2 7200 20130511150959
20130411144709 25014 lacnic.net.
lwRRw5MGThBbEfkGSmV7QqTvbcVlI2gOHIapDouYhE6+c4EsFpv3pw7n
OBJofM1hkcv4OoSIlTN0kvn5G5/Jb/SENupZTgj1VIttlFaQdiaBfTIZ
6Xo58SzLUaAToMYvOoCZc9kld/570wjjCJQtGk9V683flwkwBIXc9Aep
lRlY3/qFqxhabByc8geWoN59qe40iK/fRUZ3rc2way9jbgkPbLCZDD7Z
Cd5OdwnXkP2dZjlAulEUz+wOY8P7A+pgRs9Z1gANbMUruKhbxM422Kg3
jwhNMHryml4UJDPK5vuS2H5cjFQG/sljzf163vxPGt1w+fGHbuaM9HSZ cnXzqA==
```

authoritative servers

RRSIG 1

RRSIG 2

lacnic

DNSViz

A DNS visualization tool

Go to domain name... Go »

lacnic.net

Updated: 2013-04-12 19:26:08 UTC (25 minutes ago) Update now

« Previous analysis | Next analysis »

2013-04-12 Go »

DNSSEC | Responses | Servers | Analyze

Tweet +1

DNSSEC options (show)

Notices

RRset status

Secure (4)

DNSKEY/DS/NSEC status

Secure (10)

Delegation status

Secure (2)

DNSKEY legend

Full legend

Published only

SEP bit set

Revoke bit set

Trust anchor

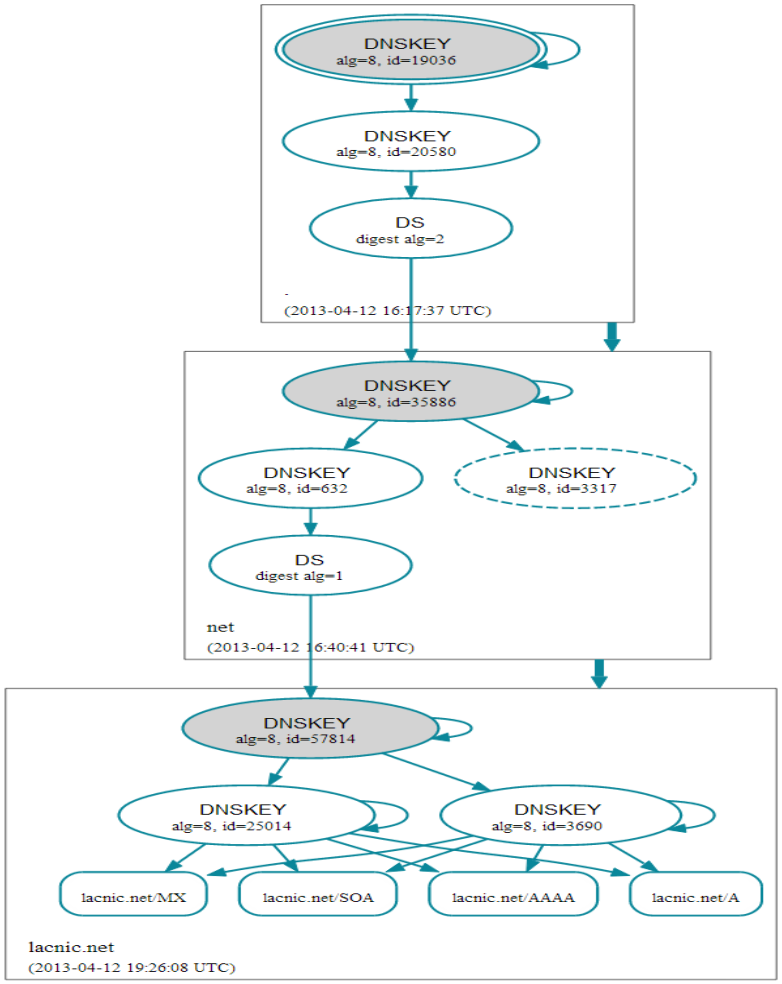
See also

DNSSEC Debugger by Verisign Labs.

DNSSEC Authentication Chain

Download: png | svg

Mouse over and click elements in the graph below to see more detail.



DNSSEC Application in LACNIC

- ZONES ADMINISTRATED BY LACNIC

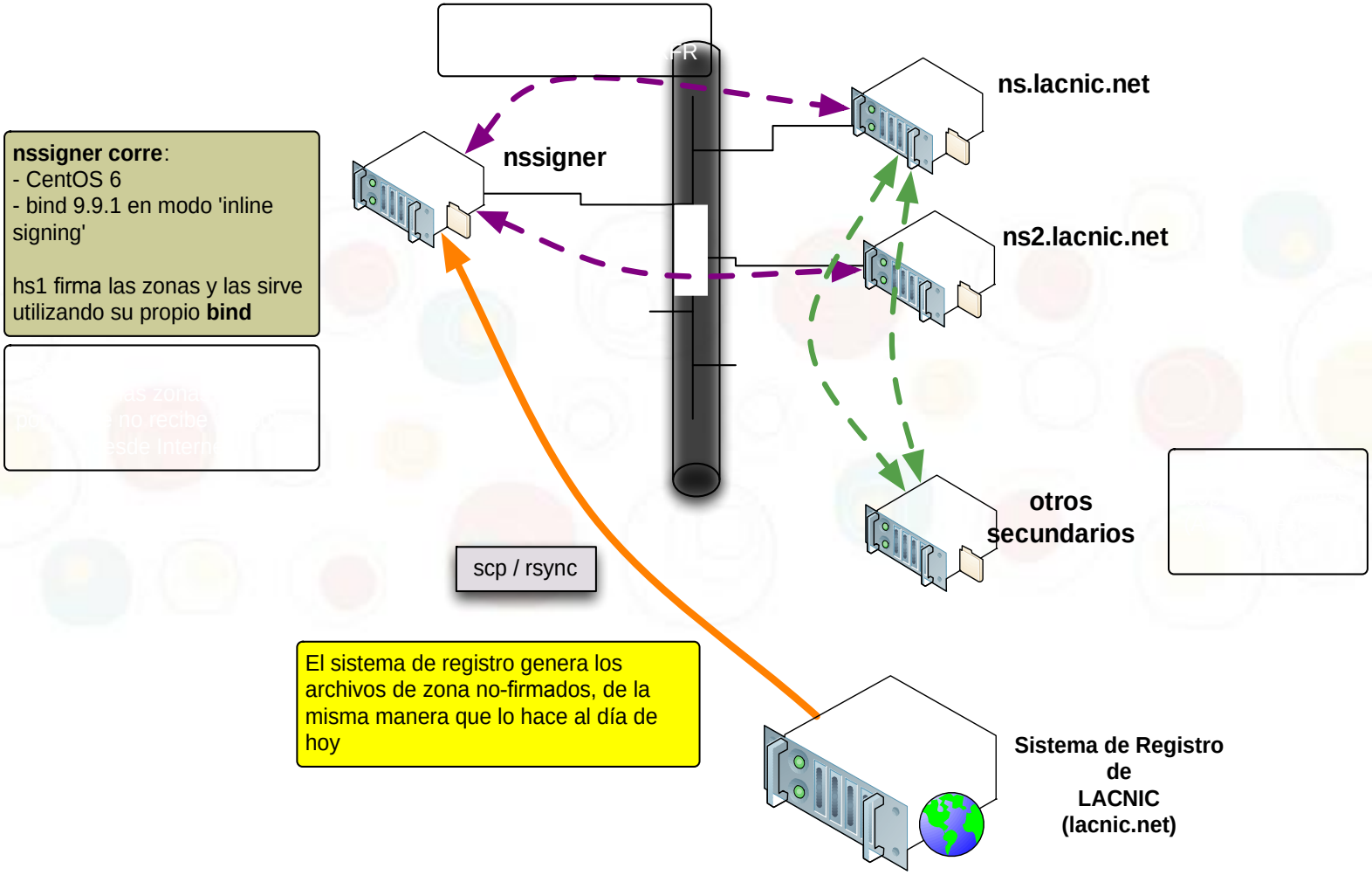
Reverse Zones

177.in-addr.arpa
179.in-addr.arpa
181.in-addr.arpa
186.in-addr.arpa
187.in-addr.arpa
189.in-addr.arpa
190.in-addr.arpa
191.in-addr.arpa
200.in-addr.arpa
201.in-addr.arpa
2.1.1.0.0.2.ip6.arpa
3.1.1.0.0.2.ip6.arpa
0.8.2.ip6.arpa

Direct Zones

programafrida.com	lacnic.net
programafrida.net	flip-6.net
programafrida.org	flip-6.org
lacnog.net	flip-6.com
lacnog.com	portalipv6.net
lacnog.org	proyectoamparo.net
fridaprogram.com	lacnic.net.uy
fridaprogram.org	lacnic.org.uy
fridaprogram.net	lacnic.uy
lacnic.org	certi6.com

DNSSEC Application in LACNIC



DNSSEC Application in LACNIC

- Nssigner Server
  - Hidden Signer
    - Generates and stores all the criptographic keys. Configured with BIND 9.9.2 in “inline-signing” mode. It is not directly exposed to internet
- Ns1.lacnic.net/ns2.lacnic.net
  - DNS servers administrated by LACNIC
- Secondary servers
  - DNS servers NOT administrated by LACNIC, with replicated information from ns1 and ns2
- Registry Service Server
  - LACNIC memebers specify their own DNS servers.

lacnic


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
TASHAKKUR ATU
YAQHANYELAY
SUKSAMA
EKHMET
BÏYAN
SHUKRIA
TINGKI
GRAZIE
MEHRBANI
MAAKE
KOMAPSUMNIDA
GOZAIMASHITA
EFCHARISTO
JUSPAXAR
PALDIES
BOLZÏN
MERCI