Contents

- Small DNS introduction.
- MIM attack.
- What is DNSSEC?
- Why DNSSEC helps.
Anatomy of a DNS Packet

ID was never meant as anti spoof mechanism.

Question

Answer

Authority
Which server is authoritative for this info

Additional
Extra info that may be handy

Optimazation.
Real Life DNS Packet

% dig a www.govcert.nl

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39349
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;www.govcert.nl.

;; ANSWER SECTION:
www.govcert.nl. 3600 IN A 62.112.232.131

;; AUTHORITY SECTION:
govcert.nl. 3597 IN NS ns2.asp4all.nl.
govcert.nl. 3597 IN NS ns3.asp4all.nl.
govcert.nl. 3597 IN NS ns1.asp4all.nl.
Players in the DNS World

Resolver

- Sits on your local PC.
- Converts from and to DNS format.

Cache

- Cache answers.
- (Optimization)

Name Server

- Gives back the final answer.
A Query in Action

www.govcert.nl. IN A?

This is the hard part of DNS. Its called: recursive resolving.

Resolver  →  Cache  →  Name Server

www.govcert.nl. 3600 IN A 62.112.232.131
A Spoof in Action

www.govcert.nl. IN A?

- If the cache accepts it, *all* resolvers will get the wrong answers for 3600 sec.
- If the resolver accepts it, it will mess up this query.

- Simple to do on a wireless LAN.
- *Much* harder on the Internet.
Resolving: Following Delegations

.(root)

.nl NS ns1.nic.nl

.nl

govcert.nl NS
ns1.asp4all.nl

govcert.nl

.be

.nl

.nlnetlabs.nl

govcert.nl

.nl NS ns1.nic.nl
DNSSEC to the Rescue - Basics

- DNSSEC adds public key cryptography to the DNS.
- Public keys are published in the DNS.
- Public keys chained via “Chain of Trust”.
- Each “answer” is signed.
- Documented in RFCs: 4033, 4034 and 4035 (just released).
- Private key(s) used to sign DNS data offline.
DNSSEC - Chain of Trust

- DNSKEY APQ...
- .nl DS ...
- .RRSIG(.nl DS)

- (root)

- .nl
  - DNSKEY APQ...
  - govcert.nl DS ...
  - .nl RRSIG (govcert.nl DS)

- .be

- govcert.nl
- nlnetlabs.nl

- govcert.nl DNSKEY APQ...
- nlnetlabs.nl DNSKEY APQ...
DNSSEC - Example Packet

;; -->HEADER<<- opcode: QUERY, rcode: NOERROR, id 15280
;; flags: qr aa rd ; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; nlnetlabs.nl. IN SOA

;; ANSWER SECTION:
nlnetlabs.nl. 86400 IN SOA open.nlnetlabs.nl. hostmaster.nlnetlabs.nl. 2005041500 28800 7200 604800 18000
nlnetlabs.nl. 86400 IN RRSIG SOA RSASHA1 2 86400 (20050514235004 20050414235004 43791 nlnetlabs.nl.
 AT1AQdbbHuIF6wGQwUvOIUlzXS/NjdaqW+AYI6sYp5A
 aXbzbUubVYjKMA9zHktIzmTyzl6vx2v9oxamWpMwalq2
 0Mq1/EVjWtR+asKQ/hQwXNNC9Ci2YsKoWk0Qrgx4Pkt
 J+z8qtDxppUDepxd6V+DiMXMA0ytnY9fZNUQLlnlqM=)
A Spoof in Action, DNSSEC Enabled

www.govcert.nl. IN A?

**Resolver** → **Cache** → **Name Server**

www.govcert.nl. 3600 IN A 62.112.232.131

127.0.0.1

www.govcert.nl. 3600 IN RRSIG “A 62.112.232.131”

- Resolver/Cache already knows DNSKEY of govcert.nl.*
- RRSIG does not validate.
DNSSEC - Ponder and Discuss

- Roll out on the Internet is hard (look at IPv6).
- Root should be signed first (or a big TLD).
- Globally updating anchored root key(s) is difficult.
- No real incentive for roll out, unless something “major” happens.
- .SE has advanced plans for DNSSEC deployment.
Documentation

RFC 4033 (Introduction, quite readable).

NSD/BIND9 DNSSEC enabled.

http://www.dnssec.net
http://www.dnssec-deployment.org