DNSSEC trigger

or how to get DNSSEC on ::1

Wouter Wijngaards & Olaf Kolkman
Executive Summary

How to get DNSSEC to your machine, without too much of a headache

dnssec-trigger

Run Unbound Locally

Catch reconfig (DHCP etc)

Try to penetrate

If all fails call user
Initial configuration

Unbound Anchor

Root Key

Unbound

Unbound specific

Dynamic configuration

unbound-control sets Forwarding Config

/etc/resolv.conf

dnssec-trigger daemon

incoming DHCP info

Machine specific

DNS Probes

user space

Dynamic configuration

Thursday, November 3, 2011
Probing Strategy

- Use Cache from DHCP
- Full resolver mode, querying authority servers directly
- Port 80 and 443 to an NLnet Labs resolver
- All IPs in resolv.conf are tried in parallel, first response wins
Normal Operation

Reprobe
Probe results
Hotspot signon
Quit

results from probe at 2011-10-27 10:52:42

authority 199.7.83.42: OK
cache 192.0.21: error timeout

DNSSEC results fetched direct from authorities
Probe Expectations

- EDNS support
- RRSIGs
- DNSKEY and DS
- Lengthy Packets (>512)
- Transparent Proxy that is transparent to DNSSEC

And it will PReobe AGAIN

If insecure against its will

exp backoff
Trouble

For when you really have to turn off DNSSEC validation

Probe fails to detect DNSSEC support, pop-up dialog.

No Pop Ups during DNSSEC operations

Only during probing operation

For when you really have to turn off DNSSEC validation.
Network Manager
Netconfig
WSALookupService (XP,Vista,7)
Scripts, ifconfig, ipconfig
GTK2
unity
Windows Native
Cocoa OS X
0.7 installer might fail; ignore the failure message
I WANT YOU running dnssec-trigger

Mailing list for user experiences
http://open.nlnetlabs.nl/mailman/listinfo/dnssec-trigger

Webpage
http://nlnetlabs.nl/projects/dnssec-trigger/
If you use our software then consider to support NLnet Labs’ mission Financially:
http://www.nlnetlabs.nl/labs/contributors/

Questions: olaf@nlnetlabs.nl
or wouter@nlnetlabs.nl

That's it folks

© 2006-2010 NLnet Labs

Thursday, November 3, 2011