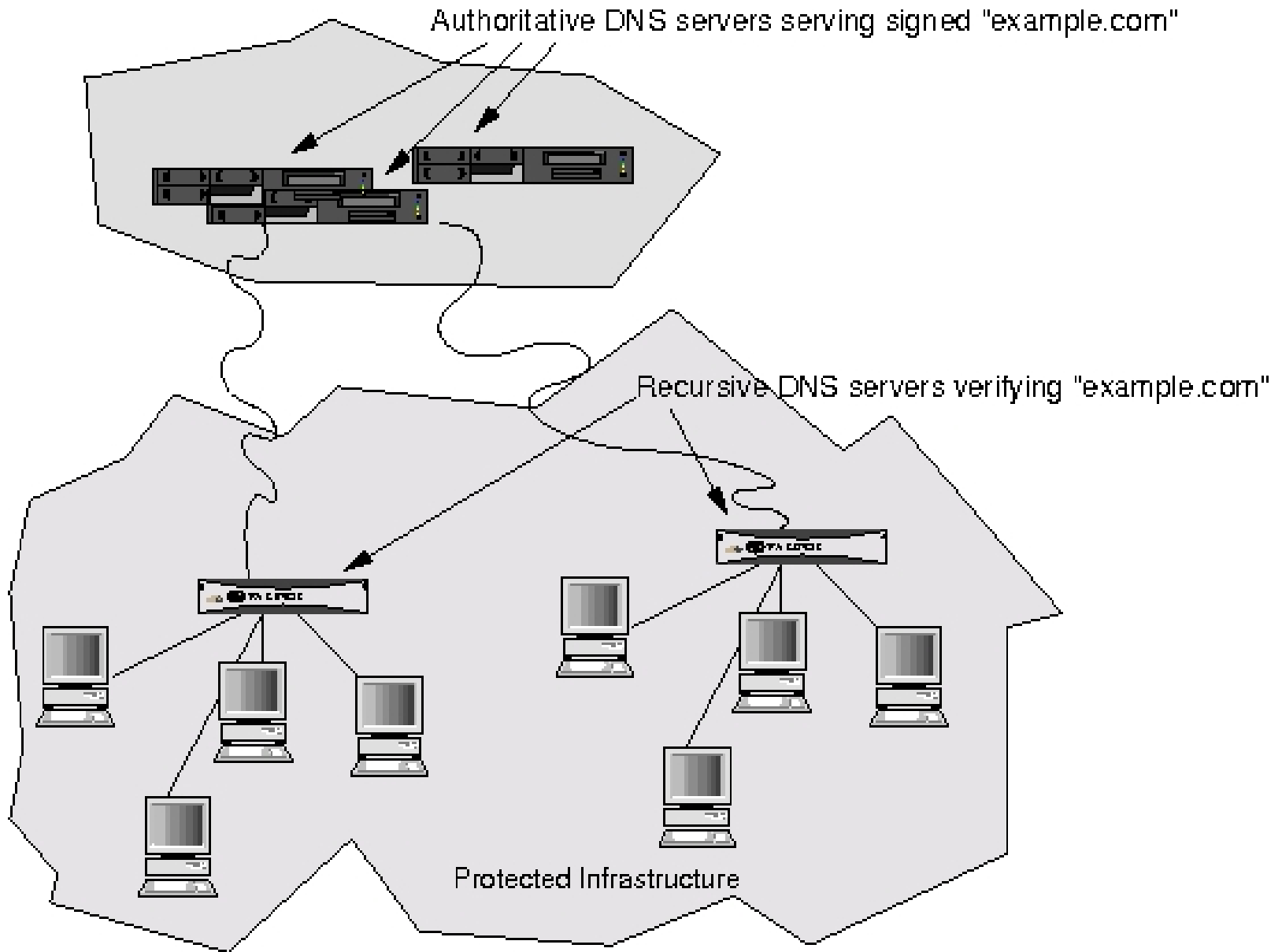


DNSSEC software at NLnet Labs

Jelte Jansen

jelte@nlnetlabs.nl



Overview

- Unbound – *DNSSEC Resolver*
 - Client side validation
- NSD – *DNSSEC Authority Server*
 - Serving signed zones
- LDNS – *Tool Library and DNSSEC Signer*
 - Signing, deploying, debugging

Introduction

- **Why these products?**
 - Code diversity in DNS server monoculture
 - Alternative choice for BIND 9
- **Basic Ideas**
 - Open Source – BSD license
 - Open Standards – RFC compliant
 - IPv6 and DNSSEC supported by default
- **About NLnet Labs**
 - A non-profit, public benefit foundation
 - Sponsored by NLnet foundation

Unbound Features



Architected &
Prototyped with:

VeriSign

EP.NET

nominet

kirei

- DNS Recursive Resolving Server
 - Open source: BSD license
 - Recursion and Caching
 - IPv4 and IPv6 dual stack support
 - DNSSEC validation
 - NSEC, NSEC3, DLV, SHA256
- Tools
 - Unbound-checkconf
 - Unbound-host: validated host lookup
 - Unbound-control: remote control of server
- Documentation
 - man pages, website unbound.net and in code (doxygen)
- Thread support (optional): scalable performance

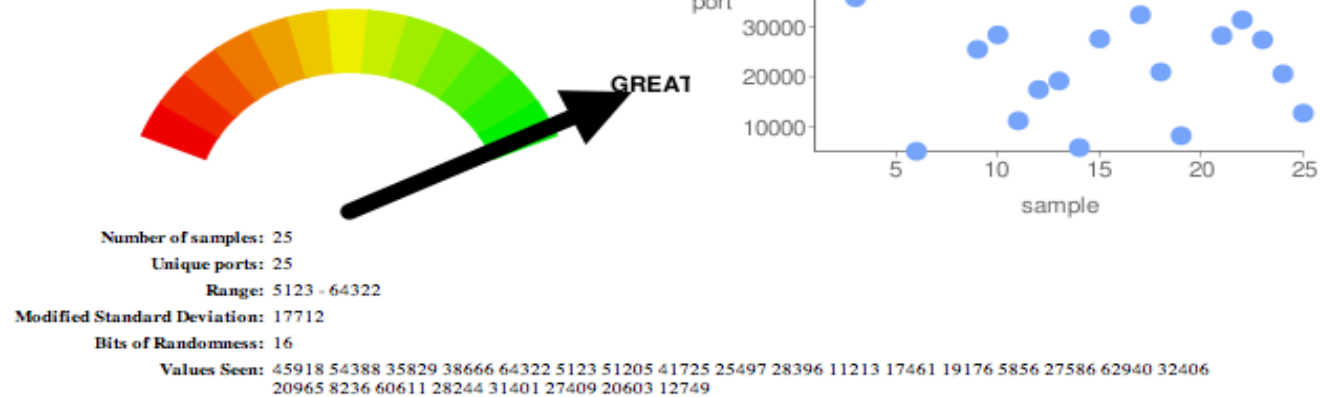
Features: More

- Trust anchors: *feature rich*
 - DS and DNSKEY, Zone-format and bind-config
- Authority service: *minimal*
 - Localhost and reverse (RFC1918) domains
 - Can block domains
- Extended statistics support (munin, cacti)
- contrib/*update-anchor.sh* script
 - Update trust anchors securely from daily cron job.
- Stop domain name rebinding attacks
- Access control for DNS service
 - not open recursor

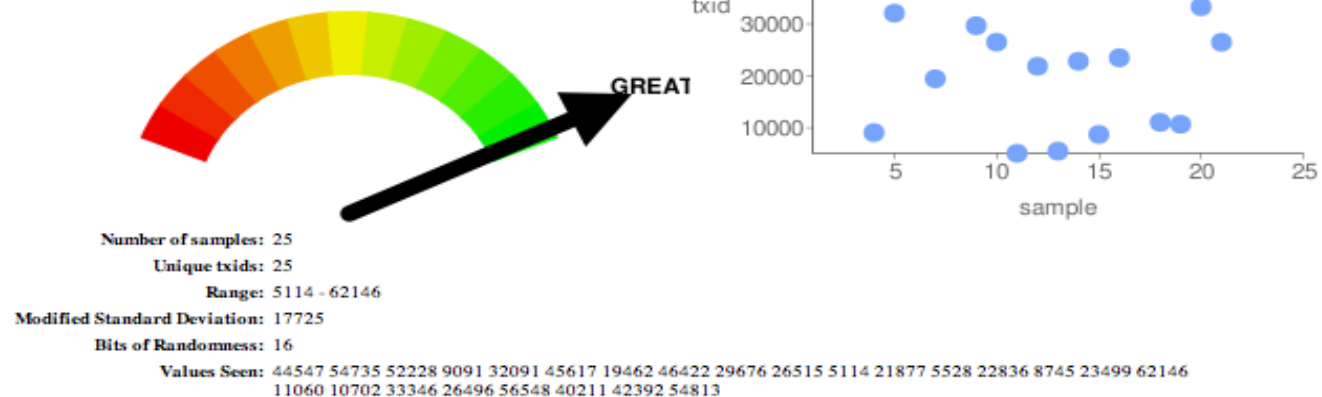
Features: Paranoia

- Forgery resilience: *full featured*
 - Scrubber filters packets for out-of-zone content
 - Follows RFC2181 trust model
 - Follows all recommendations from dnsop draft
 - Query name matching
 - Strong random numbers for ID
 - UDP source port random
 - IP source address random
 - RTT banding
- Experimental 'Kaminsky' mitigation
 - dns-0x20 full support
 - draft-wijngaards-dnsex-resolver-side-mitigation

213.154.224.48 Source Port Randomness: GREAT



213.154.224.48 Transaction ID Randomness: GREAT



NSD

- Authoritative Server
 - Lean and mean
 - Only authoritative. Limited Statistics. User is smart.
 - Less code means less security problems
 - Less code means faster
 - BSD license
- Features
 - Chroot, DNSSEC, NSEC, NSEC3, TSIG, IPv6
 - High performance, like 200k queries/second
 - Primary and secondary (AXFR, IXFR, NOTIFY)
 - AXFR fallback, and source interface config

NSD ctd.

- Status: 3.2.1 stable.
- Architecture:
 - Server processes use a precompiled copy-on-write database in memory to answer queries
 - Zone parsing, loading and transfer performed by separate processes from actual DNS server
- Deployed on root, TLD servers, like .se
- Get it here
 - <http://nlnetlabs.nl/nsd>, or use package installer

NSD Tested

- Operating Systems
 - Solaris
 - Linux
 - FreeBSD
 - Mac OS/X
- Hardware
 - i386, 32/64
 - Powerpc, Alpha
 - Sparc64
- Interoperability
 - Wire differences
 - with Bind 8, 9
 - Interop. OK
 - Details documented

LDNS

- Tool library
 - simplify DNS tools written in C
 - BSD license
 - RFC compliant
 - IPv4 and IPv6 Support
 - DNSSEC, NSEC, NSEC3, TSIG Support
 - Online documentation, manuals
 - Inspired by Net::DNS and Net::DNS::SEC (perl lib we also maintain)

LDNS signer

- **ldns-signzone**: full featured zone signer
 - Crypto based on OpenSSL
 - Hardware signers supported via openssl engines
 - NSEC and NSEC3 signing
 - SHA-256 (for DS records)
- Library
 - Signing routines can be called from the library

Tools for signing

- **ldns-verifyzone**: check if RRSIG and NSEC, NSEC3 are ok
- **ldns-key2ds**: convert DNSKEY to DS, for when a public KSK is published at parent
- **ldns-rrsig**: printout readable expiration dates
- **ldns-nsec3-hash**: print NSEC3 hash of one name
- **ldns-revoke**: set rfc5011 REVOKE flag on key
- **ldns-keygen**: generate keys, can use a hardware random device

LDNS based: drill

- Like dig
 - Inspired the idea of LDNS
 - Helped debugging NSD, BIND
- Debugging tool for DNS (SEC)
 - Can perform a trace of the DNSSEC chain of trust and printout:

```
;; Chasing: www.frobbit.se. A
```

```
DNSSEC Trust tree:
www.frobbit.se. (A)
|---frobbit.se. (DNSKEY keytag: 52320)
    |---frobbit.se. (DNSKEY keytag: 20833)
    |---frobbit.se. (DS keytag: 20833)
        |---se. (DNSKEY keytag: 21297)
            |---se. (DNSKEY keytag: 8779)
            |---se. (DNSKEY keytag: 49678)
;; Chase successful
```

More tools

- **ldns-chaos** – Shows some information about a nameserver
- **ldns-keyfetcher** – Fetches DNSSEC public keys for zones
- **ldns-read-zone** – Reads a zone file and prints it with 1 RR per line. Can also canonicalize and sort the zone, or only output dnssec or non-dnssec data
- **ldns-update** – send a dynamic update packet
- **ldns-walk** – 'Walks' a DNSSEC-NSEC zone
- **ldns-zsplit** – Splits a zone file in smaller parts
- **ldns-zcat** – Concatenates zone file parts split with ldns-zsplit
- **ldns-compare-zones** – See the differences between zones (added/removed names, added/removed rrs for names)
- **ldns-notify** – send message to slave name servers that updates are available

Under development: Autotrust

- Current beta: 0.2.0
- RFC 5011 (draft-timers) implementation
- Add-on to validator (Bind, Unbound)
 - Run from cron once per day, week
 - Writes trust anchor files
- Option to work with plain key rollover
 - No REVOKE bits need to be published
 - Keep list of keys in missing state in check

Questions