Securing DNS

DNSCurve & DNSSEC

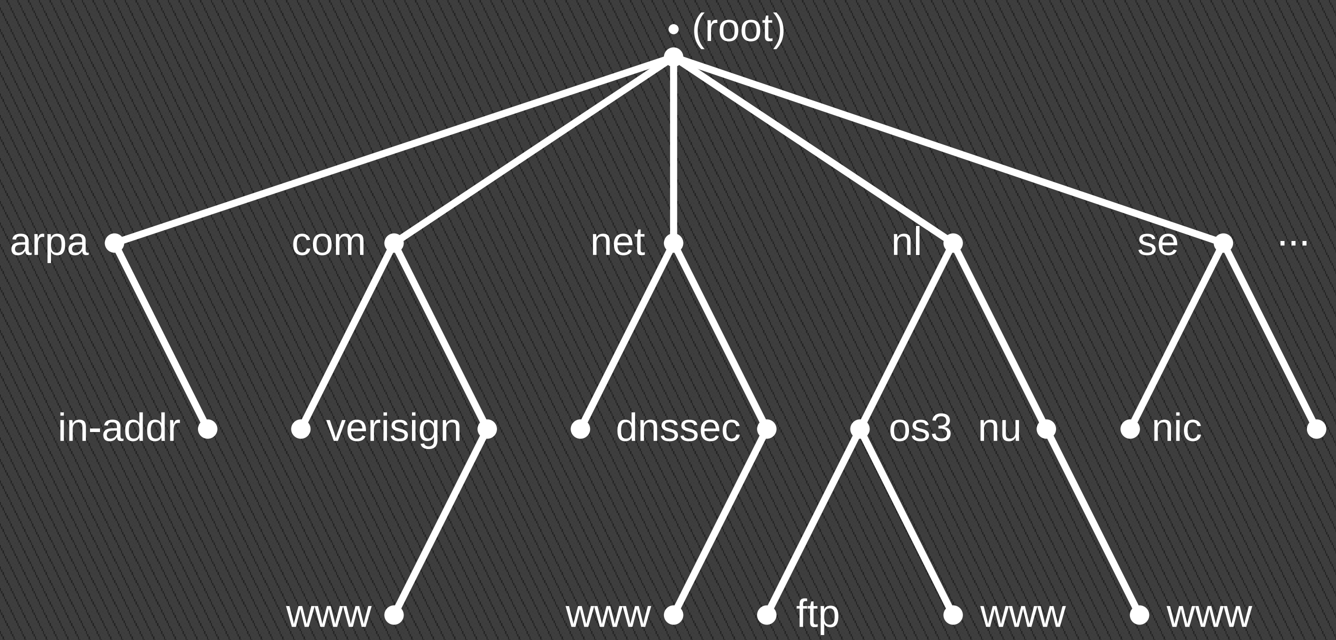
Master
System and Network Engineering

2009-07-01
Cornel de Jong

The Domain Name System

- Domain Name Space and Resource Records
- Name servers
- Resolvers

- Used for:
- Browsing
- Mail
- VoIP
- Etc…



Research question

“ *What consequences do the differences in design of DNSCurve and DNSSEC have on the implementations* ”

Sub questions

- Hardware / software requirements
- Tooling
- Transport protocol
- CIA Triangle
- Cryptographic algorithms
- Key revocation
- Overhead
- Maturity
- Interim solutions

History

ORIGINAL DNS

RFC 882	November	1983
RFC 1034 – 1035	November	1987

DNSSEC

RFC 2065	January	1997
RFC 2535	March	1999

Extensions

RFC 2671	August	1999
RFC 3833	August	2004

DNSSEC-bis

RFC 4033 – 4035	March	2005
RFC 5155	February	2008
DNSCurve		2008

Threats according to RFC 3833

- Packet interception: Man-In-The-Middle attacks
- ID guessing and query prediction
- Name chaining: Cache poisoning
- Betrayal by trusted server
- Denial-of-Service
- Wildcards insertion

DNSCurve vs DNSSEC

- The DNSCurve project adds link-level public-key protection to DNS messages using elliptic curve cryptography. (Curve25519)

- DNSSEC provides message authentication and integrity verification through cryptographic signatures.
- Authentic DNS source
- No modifications between signing and validation
  - It does not provide authorization
  - It does not provide confidentiality

(Borrowed from Olaf M. Kolkman NLnet Labs)

Hard- software requirements

DNSCurve:

- DNSCurve Cache (recursive)
- DNSCurve Forwarder (authoritative)

DNSCurve Stand-alone forwarder

"DNSCurve cache / forwarder software is, at the time of this writing (June 2009), undergoing development and testing."

DNSSEC:

DNS name server that supports DNSSEC

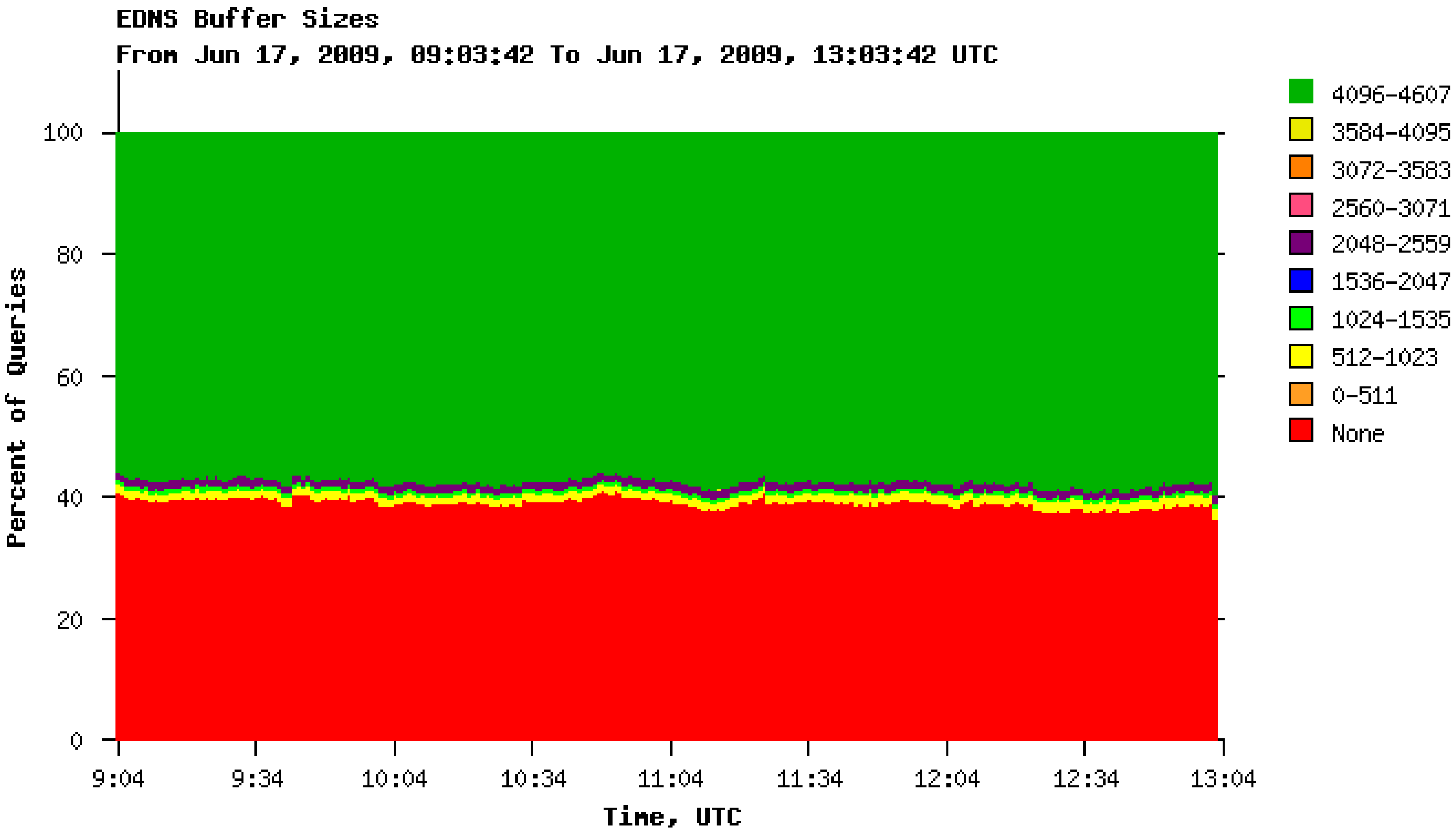
EDNS0 support, new hardware (depending on the scale of the organization)

Transport protocol

- UDP limited to 512 Bytes (RFC 1035)
- EDNS 4096 Bytes (RFC 2671)
- 512 Bytes > “Middle boxes”
- UDP vs TCP
- Amplifier → Denial of Service

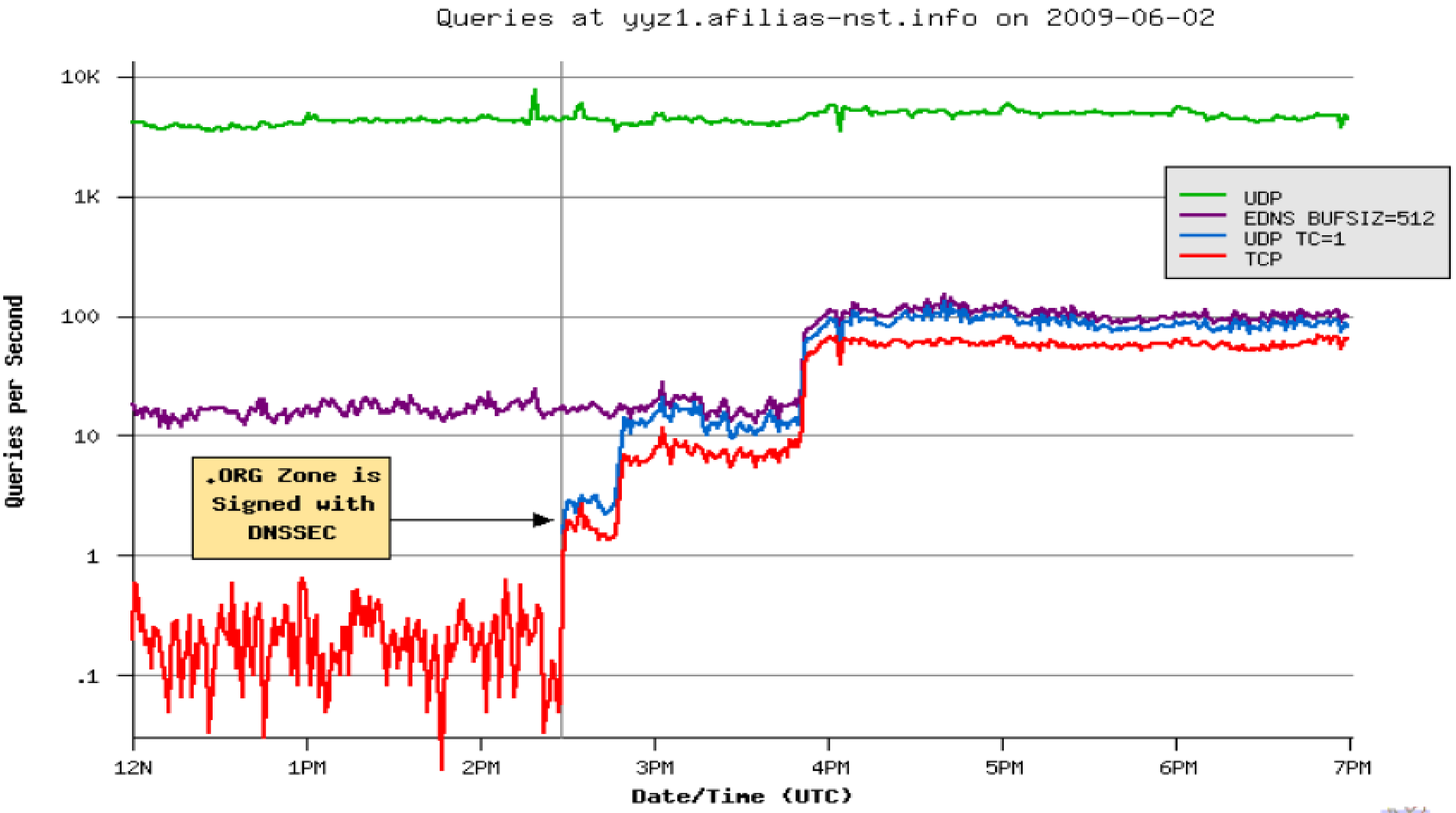
EDNS Buffer Sizes

C.root-servers.net



Courtesy of: Duane Wessels and Sebastian Castro

Traffic after DNSSEC signing



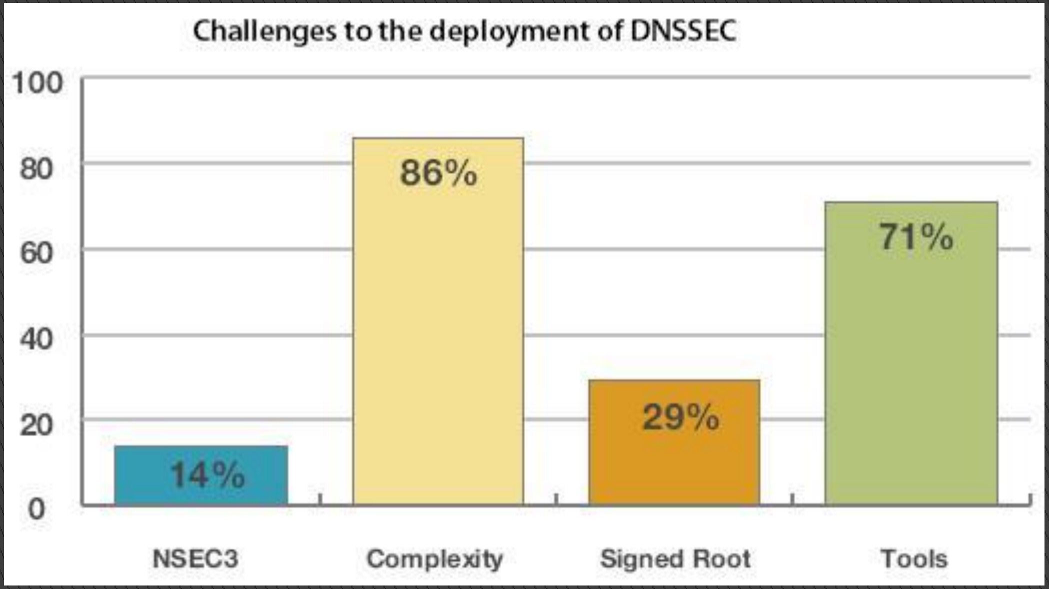
Data © 2009Afilias-PIR

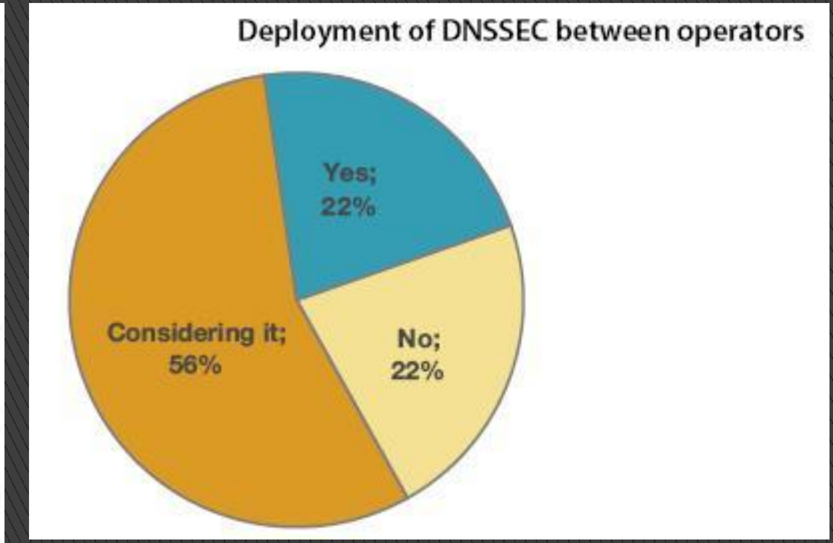
DNS-OARC

Overview

DNSCurve	DNSSEC
Relatively new (2008)	First discussed in 1993
Lack of formal specification	Specified in several RFCs
Elliptic curve cryptography	RSA cryptography
Transport security	Data integrity
No algorithm rollover	MANDATORY vs OPTIONAL
DNS packets encrypted	DNS packets unencrypted
On-the-fly	Pre computation
No key rollover	Annual KSK key rollover
	Monthly ZSK key rollover

DNSSEC deployment





Source: ENISA

Govcert Trend report 2009:

Investigation by GOVCERT.NL (April 2009) among 466 Dutch governmental organizations showed that DNSSEC was not used by any of the organizations.

(GOVCERT.NL examined the name servers of 13 ministries, 12 provinces and 441 municipalities)

Conclusions

DNSCurve is designed to authenticate and encrypt messages on-the-fly, were DNSSEC cryptographically pre-signs all DNS records.

In order to verify the integrity of the received messages DNSCurve stores the public key in the existing NS record were DNSSEC uses a special DNSKEY record.

DNSCurve seems very promising but first has to prove itself.

Future work

- DNSCurve code analysis
- DNSCurve vs DNSSEC performance tests
- Impact on embedded devices
- DNSSEC in SOHO routers (end-to-end)
- DNSTrust Trust dependencies for TLDs
- DNSSEC capable resolvers within OS’s
- Key revocation

Questions ?