DNSCurve Server

J. Scheerder*
jeroenscheerder@on2it.eu

November 7, 2008

1 Introduction

In the recent past fundamental design flaws in the DNS protocol have been exposed[1].

DNSCurve[2] is a proposal to address these fundamental problems. It promises to guarantee confidentiality and integrity of DNS traffic, as well as protect against attacks on service availability.

A DNSCurve-aware server will offer these benefits to DNSCurve-capable clients. Adding DNSCurve funcationality to existing DNS software would therefore be beneficial.

It may however be non-trivial, if possible at all, to update DNS server software to include DNSCurve functionality:

- Servers can run complex, tailored software, with no room for experiments (and service downtime).
- Servers can run software that would be modifiable in principle, but has become unmaintained (obsolete) in practice.
- Servers can run closed-source software from a vendor unwilling or unable to add DNSCurve functionality.
- Servers may be special requirements that prohibit modification.

Regardless of this, a DNS server can still be effectively enhanced with DNSCurve functionality by interposing a DNSCurve-aware forwarder. Queries that before would go directly to the DNS server now are routed through the forwarder that transparantly can authenticate and encrypt DNS queries when possible.

2 Goal

Implement a DNSCurve-aware DNS service.

3 Tasks

Either:

- Add DNSCurve functionality to existing DNS server software by
  - Rounding up the neccessary DNSCurve technology.
  - Examining existing DNS recursors (such as tinydns, PowerDNS Server, BIND, NSD, MaraDNS, Nominum ANS …)
  - adding DNSCurve functionality to one or more of these.
- Implement a DNSCurve forwarder to transparently front existing DNS servers by
  - Rounding up the neccessary DNSCurve technology.
  - Design and implement a DNSCurve-aware DNS forwarder.

*ON2IT b.v., Waardenburg, The Netherlands.

[1] Widely reported as the "Kaminsky Bug".

[2] See http://dnscurve.org/.