DNSCurve Resolver

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 resolver will recognize and benefit from DNSCurve-capable servers. It may be non-trivial, if possible at all, to update DNS resolver software on network clients:

- Clients can run embedded, unmodifiable software. Consider ATMs, for example.
- Clients can run software that would be modifiable in principle, but has become unmaintained (obsolete) in practice.
- Clients can run closed-source software from a vendor unwilling or unable to add DNSCurve functionality.
- There may be special requirements that prohibit modification.

Regardless of this, clients can still benefit from DNSCurve by using a DNSCurve-aware recursing, resolving DNS service (that typically also acts as a DNS cache).

2 Goal

Implement a DNSCurve-aware DNS resolver.

3 Task

Implement a recursive DNS server (a DNS cache) that supports DNSCurve by

- Rounding up the neccessary DNSCurve technology.
- Examining existing DNS recursors (such as dnscache, PowerDNS Recursor, BIND, MaraDNS, Nominum CNS, Unbound, …)
- Either add DNSCurve functionality to one or more of these, or design and implement a DNSCurve-aware recursive DNS server from scratch.

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

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

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