Securing DNS

DNSCurve & DNSSEC
The Domain Name System

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

- Used for:
  - Browsing
  - Mail
  - VoIP
  - Etc…
“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
<table>
<thead>
<tr>
<th>Type</th>
<th>RFC</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORIGINAL DNS</td>
<td>882</td>
<td>November 1983</td>
</tr>
<tr>
<td></td>
<td>1034 - 1035</td>
<td>November 1987</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>2065</td>
<td>January 1997</td>
</tr>
<tr>
<td></td>
<td>2535</td>
<td>March 1999</td>
</tr>
<tr>
<td>Extensions</td>
<td>2671</td>
<td>August 1999</td>
</tr>
<tr>
<td></td>
<td>3833</td>
<td>August 2004</td>
</tr>
<tr>
<td>DNSSEC-bis</td>
<td>4033 - 4035</td>
<td>March 2005</td>
</tr>
<tr>
<td></td>
<td>5155</td>
<td>February 2008</td>
</tr>
</tbody>
</table>
|                 | 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
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

From Jun 17, 2009, 09:03:42 To Jun 17, 2009, 13:03:42 UTC

Percent of Queries

Time, UTC

Courtesy of: Duane Wessels and Sebastian Castro
Traffic after DNSSEC signing

Queries at yyz1.afilias-nst.info on 2009-06-02

Data © 2009 Afilias-PIR
Overview

**DNSCurve**
- Relatively new (2008)
- Lack of formal specification
- Elliptic curve cryptography
- Transport security
- No algorithm rollover
- DNS packets encrypted
- On-the-fly
- No key rollover

**DNSSEC**
- First discussed in 1993
- Specified in several RFCs
- RSA cryptography
- Data integrity
- MANDATORY vs OPTIONAL
- DNS packets unencrypted
- Pre computation
- Annual KSK key rollover
- Monthly ZSK key rollover
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 ?