Research Project 1 - DNSCurve Analysis

In cooperation with ON2IT B.V.

Michiel Timmers - michiel.timmers@os3.nl

Universiteit van Amsterdam (UvA)
System and Network Engineering
February 4 2009

What is wrong?

July 2008 - CERT announced that Dan Kaminsky had found a fundamental problem in the DNS protocol

Privacy: Sniffing

Legacy: DNS was never meant to last this long

What is DNSCurve?

DNSCurve adds link-level public-key protection to DNS packets by using the elliptic-curve library "NaCl"

- Confidentiality
- Integrity
- Availability

How can I deploy it?

DNSCurve for incoming DNS data

- Upgrade your DNS cache to a DNS cache that supports DNSCurve

DNSCurve for outgoing DNS data

- Upgrade your DNS server to a DNS server that supports DNSCurve
- Install a DNSCurve forwarder

- Install the DNSCurve forwarder on a new IP address.
- Configure the DNSCurve forwarder to forward to your existing DNS server's IP address.
- Add, in your DNS data, a special DNSCurve server name for the DNSCurve forwarder.
- Add the same DNSCurve server name in your parent DNS data.
- After a week, remove the old non-DNSCurve server names.

uz5ptjftdvugccb1sbb3im9etbtfnu0mh2vsicfqa1ohme9qi940st.os3.nl

Implementation status and issues

So can I deploy DNSCurve today? NO!

- The NaCl elliptic-curve library isn't released yet.
- DNSCurve forwarder source code still needs a lot of programming

But what about DNSSEC?

DNSCurve and DNSSEC have complementary security goals

- DNSSEC project adds public-key signatures to DNS records
- DNSCurve adds link-level public-key protection to DNS packets

Recommendations & Further research

Recommendations

- Finish the code and make it publicly available
- More documentation

Further research

- DNSCurve and DNSSEC influences on each other
- How to make a DNS server support DNSCurve


DNSCurve: Usable security for DNS:
http://dnscurve.org


NaCl: Networking and Cryptography library:
http://nacl.cr.yp.to


Michiel Timmers: RP1 - DNSCurve Analysis:
https://www.os3.nl/2008-2009/students/michiel_timmers/rp1

Thanks Jeroen Scheerder of ON2IT B.V!

Questions?