

Overvejelser omkring DNSSEC i Danmark

DANSK INTERNET FORUM

Svenne Krap, svenne@krap.dk
København, 18. juni 2009

Nærmest utekniske

Overvejelser omkring DNSSEC (i Danmark)

DANSK INTERNET FORUM

Svenne Krap, svenne@krap.dk
København, 18. juni 2009



Agenda

De 5 hv-spørgsmål

1) Hvorfor?

2) Hvordan?

3) Hvad?

4) Hvornår?

5) Problemer?

HVORFOR?

KOMMUNIKATION

- Mindst 2 parter
- Er sikre på hinandens identitet
- Har passende hemmelighed

HVORFOR?

KOMMUNIKATION

- Mindst 2 parter
- Er sikre på hinandens identitet
- ~~Har passende hemmelighed~~

HVORFOR?

KOMMUNIKATION

- Mindst 2 parter
- Er sikre på hinandens identitet
- ~~Har passende hemmelighed~~

Fx.

Netbanker, Webshops, Nyhedssites, Email, VPN

HVORFOR? (del 2)

DNS = telefonbog

www.dk-hostmaster.dk = 193.163.102.23

1) Spørg "oraklet" (rodzonen)

DK? → a.nic.dk

2) Spørg a.nic.dk

DK-HOSTMASTER.DK ? → auth01.ns.dk-hostmaster.dk

3) Spørg auth01.ns.dk-hostmaster.dk

WWW.DK-HOSTMASTER.DK == 193.163.102.23

Ingen verifikation af udsagn!

HVORFOR? (del 3)

For fjenden er missionen:

Sørg for at sende fejlagtig information som modtageren stoler på

Sørg for at kunne opsnappe og modificere information "på vej"

HVORFOR? (del 4)

Hvad med SSL, VPN og andet crypto – er det ikke nok ?

- kan være forældet*
- kan være sat forkert op
- kan have uopmærksom bruger

→ Vi har brug for mange LAG af sikkerhed!

*

Cæsar's encryption: født 56 f.k.

Brugt i 2006 af mafiaen (som blev fængslet)

MD5: født 1994, R.I.P 1/3/2005

Angrebet dec 2008 (RapidSSL skandalen)

SHA1: født 1995, R.I.P 2004-2010

HVORDAN?

KRYPTOGRAFI

- hulens svær matematik
- public-key crypto
 - privat nøgle (hemmelig)
 - offentlig nøgle (el. certifikat)

En privat nøgle kan underskrive en udtalelse, som den offentlige nøgle kan verificere (men ikke genskabe).

→ En udtalelse kan være en anden's offentlige nøgle

HVORDAN? (del 2)

DNSSEC

En **åben standard** til at underskrive et hierarki af andres nøgler og slutteligt et fakta omkring et opslag

- starter med "orakel" = kendt god underskrift
- hvert niveau underskriver næste niveau
- sidste niveau underskriver data

= SIKRER* at du får korrekt information.

HVAD?

- 1) Værktøjer til at genere DNSSEC data
- 2) Nameservere, der understøtter at formidle DNSSEC
- 3) Resolvere der forstår DNSSEC

Ad 2)

- * Bind 9.6 (nov 2008)
- * Windows Server 2008 R2

Ad 3)

- * Windows 7
- * Unbound (unix)

HVAD?

- 1) Værktøjer til at genere DNSSEC data
- 2) Nameservere, der understøtter at formidle DNSSEC
- 3) Resolvere der forstår DNSSEC

Ad 2)

- * Bind 9.6 (nov 2008)
- * Windows Server 2008 R2

Ad 3)

- * Windows 7
- * Unbound (unix)

- + signering af rod-zonen - ultimo 2009
- + signering af relevant 2. level zoner (.dk) – 2010

HVORNÅR?

- signering af rod-zonen - ultimo 2009
- signering af relevant 2nd level zoner (.dk) - 2010

Nuværende projekter:

- Brasilien (br)
- Bulgarien (bg)
- Tjekkiet (cz)
- Puerto Rico (pr)
- Sverige (se)
- .org (Afilias) – fullblown 2010
- RIPE (reverse)

Fremtidige:

- Verisign (.com, .net m.f.) indenfor 24 mdr. (målt fra februar 2009)

PROBLEMER?

1) sikkerhed er svært (unintended consequences)



PROBLEMER?

2) standarden er ung (og allerede i anden udgave)

- fejl i matematikken
- ukendte angreb
- Inkompatibilitet
 - 2 typer x509, openPGP

1. udgave, 1995 RFC2065

→ RFC2535 (1999)

Skaleringsproblemer

2. udgave (marts 2005)

+ SHA256 (maj 2006)

+ NSEC3 (feb 2008)

PROBLEMER?

2) standarden er ung (og allerede i anden udgave)

This sounds **simple** but it has deep reaching consequences in both the protocol and the implementation—which is why it's taken more than a year to choose a security model and design a solution. We **expect it to be another year before DNSSEC is in wide use** on the leading edge, and at least a year after that before its use is commonplace on the Internet.

Paul Vixie, June **1995**

PROBLEMER?

2) standarden er ung (og allerede i anden udgave)

We are still doing basic research on what kind of data model will work for DNS security. After three or four times of saying “NOW we’ve got it, THIS TIME for sure” there’s finally some **humility** in the picture “Wonder if THIS’ll work?”

Paul Vixie, **November 2002**

PROBLEMER?

3) nøglehåndtering

Mange nøgler pr. organisation, skal skiftes regelmæssigt

→ langt større administrativt arbejde end i dag

→ vokser eksplosivt

PROBLEMER?

4) Indskrænknings

Man bør atid kunne indstille sin computer til at accpeterer data uden signering (DNSSEC)

- test data
- interne data
- forkert opsatte servere
- censur-mulighed

Alternativer?

Dan Bernstein (djb) har med hjælp af EU midler implementeret sit forslag **DNSScurve**.

- ser umiddelbart lettere ud at administrere
- MEN
 - nyt forslag, ikke så meget forskning endnu
 - kommer sent på markedet, får måske aldrig nogen betydning
 - hjælper ikke hvis DNS-serveren er Owned

Mere info

- <http://www.dnssec.net>
- <http://www.dnssec.net/dns-threats>
- <http://en.wikipedia.org/wiki/Dnssec>
- relevante RFC'er