Internetdagarnas årliga dos av DNSSEC

Jakob Schlyter
jakob@crt.se

Internetdagarna 2002

CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

Agenda

- Status på DNSSEC inom IETF
- DNSSEC i se-zonen
- DNS och applikationer

Status på DNSSEC inom IETF

DS - Delegation Signer

- Implementerad i BIND 9.3
  - fortfarande under testning
- Har testats vid flera workshops under sommaren
  - resultaten ser lovande ut

OPT-IN

- OPT-IN är en mekanism för att slippa signera osäkra delegeringar

- Argument för
  - gör det mindre resurskrävande att införa DNSSEC i stora zoner, t.ex. .com och .net
- Argument emot
  - komplexare kod i alla klienter
  - inget skydd mot förfalskning av icke-existerade domäner

Nya standarddokument

- En ny version av RFC 2535 (“Domain Name System Security Extensions”) håller på att tas fram
  - kommer att inkludera viktiga förändringar av DNSSEC
  - inkluderar DS (delegation signer)
  - inkluderar eventuellt OPT-IN

DNSSEC i .SE

DNSSEC i .SE

- Arbetet med att införa DNSSEC i .SE drivs av IIS-stiftelsens DNSSEC-projekt
- Testdrift av DNSEC i .SE under 2003
  - Först i begränsad skala med separata namnservrar
  - Senare i den riktiga SE-zonen
- Produktionsdrift kan troligen startas under 2004

DNSSEC och applikationer

Vad är ett certifikat?

- Ett certifikat knyter kryptografiskt samman
  - en publik nyckel
  - namnet på innehavararen
  - namnet på utfärdaren samt dess signatur
  - en giltlighetstid

  - innehåller ibland också information om vad certifikatet får användas till

- Certifikatet bär sin egen säkerhet

CERT

- Defineras i RFC 2538
- CERT-posten bär ett certifikat, t.ex.
  - X.509
  - SPKI
  - PGP
- CERT-posten behöver inte DNSSEC för att vara användbar

KEY

- Defineras i RFC 2535
- KEY-posten bär enbart en publik nyckel
  - Utsprungligen både för DNSSEC själv
  - och för applikationsnycklar
- Utan en SIG-post kan inte KEY-posten autenticeras.

Restrict KEY for DNS

draft-ietf-dnsext-restrict-key-for-dnssec-03.txt

- Erfarenheter från arbetet med DNSSEC har visat att det är en dålig idé att blanda nycklar som används för DNSSEC själv med applikationsnycklar

- "Subtyping"
  - Man ställer en DNS-fråga efter {namn,klass,posttyp}
  - Det går inte att fråga efter nyckeln för en specifik applikation eftersom information om vad för applikation en KEY-post syftar på finns inuti KEY-posten

APPKEY

draft-schlyter-appkey-02.txt

- Som KEY, men bara för applikationer
- Antagligen inte en bra idé, eftersom kraven varierar mellan olika applikationer
- Har samma problem med “subtyping” som KEY
  - Hur kan man fråga efter en nyckeln som hör till en specifik applikation?
  - Kan lösas med magiska namn
    - `_ssh.host.example.com.  IN APPKEY …`
    - `_ipsec.host.example.com. IN APPKEY …`

Är många nya posttyper ett alternativ?

- Varför inte definera en ny posttyp för varje applikation?
  - "Caching servers" skall vara transparanta för nya posttyper
  - Auktoritiva servrar kan erbjuda stöd för nya posttyper med CLASS#/TYPE# syntax
  - Programvara som slår upp nya posttyper måste uppdateras
    - Kan vara en del av applikationen själv
- Varför är detta en bra idé?
  - Man kan direkt fråga efter en specifik applikationsnyckel
  - Applikationer med speciella krav behöver inte samsas om en enda posttyp

Secure Shell Fingerprint (SSHFP)

draft-ietf-secsh-dns-00.txt

- Secure Shell (SSH) kan autenticera en fjärrnod med hjälp av en publik nyckel
  - När nyckeln väl är godkänd kan den sparas för framtida uppkopplingar
  - Hur godkänner man nyckeln?

- Endast ett fingeravtryck av nyckeln behövs eftersom själva nyckeln också överförs vid uppkopplingen.

IPSECKEY

draft-richardson-ipsec-rr-00.txt

- Opportunistic Encryption (OE) for IPsec/IKE
  - OE kan transparent kryptera IP-trafik mellan två maskiner om deras nycklar finns i DNS
- OE använder idag TXT eller KEY för att för hämta
  - publika nycklar
  - parametrar om eventuell säkerhetsportal
- IKE (nyckelförhandlingsprotokollet) behöver den publika nyckeln innan autenticeringen eftersom nyckeln inte överförs vid uppkopplingen.

jakob@crt.se