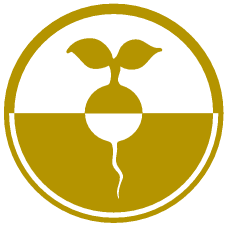


DNSSEC
Tekniken och standarden

Jakob Schlyter <j@crt.se>

http://www.crt.se/~jakob/
sip:jakob@crt.se

Agenda

- Säker delegering
- Om konsten att inte signera allt
- Nycklar för applikationer
- DNS – PKI eller nyckelhink
- Applikationer som använder DNSSEC

Delegering i DNSSEC – traditionell delegering

- Förälderns signatur lagras hos barnet

- Fördelar
  - Fungerar utmärkt vid normal drift
- Nackdelar
  - Fungerar riktigt dåligt vid onormal drift

Oplanerade nyckelbyten

- Vad gör man när förälderns nyckel röjs?
  - Genererar en ny nyckel
  - Signerar om barnens nycklar
  - Distribuerar de nya signaturerna
  - Väntar på att samtliga barn aktiverat de nya signaturerna
  - Ta bort den röjda nyckeln

Oplanerade nyckelbyten

- Tar detta lång tid?
  - För crt.se. går det fort (inga underdomäner)
  - För ericsson.se. går det inte lika fort (få underdomäner)
  - För se. börjar det blir komplicerat (xx 000 underdomäner)
  - För com. är det i praktiken omöjligt (x 000 000 underdomäner)

Signaturen hos föräldern

- Om man istället skulle lagra förälderns signatur över barnets nyckel hos föräldern?
  - dvs SIG(KEY(crt.se)) lagras hos se.

- Fördelar
  - Föräldern kan byta nyckel när som helst
    - utmärkt vid röjda nycklar
    - enklare vid omsignering
- Nackdelar
  - Föräldern blir ansvarig (”authorative”) för signaturer som egentligen borde ligga hos barnet

Delegering i DNSSEC - fingeravtryck hos föräldern

- Istället för att signera barnets nyckel, signerar föräldern ett fingeravtryck (”hash”) av barnets nyckel

- Fördelar
  - Bättre uppdelning av data
    - DS + SIG(DS) lagras alltid hos föräldern
    - KEY + SIG(KEY) lagras alltid hos barnet
  - Beroendet mellan förälder och barn minskar
    - Föräldern kan enkelt byta nyckel
- Nackdelar
  - Programvara måste skrivas om

Selektiv signering

- All data behöver inte vara signerad
  - Signering medför risk för NXT-traversering
- I praktiken nödvändigt för att inför DNSSEC i mycket stora zoner
  - com.
  - net.
  - org.
- Fördelar
  - Man kan blanda signerad och osignerad data i samma zon
- Nackdelar
  - Programvara måste skrivas om

Att signera tomrum

- Exempel på NXT
  - alpha.sigz.net. A 10.0.0.1
    SIG A ...
    TXT ”alpha”
    SIG TXT ...
    NXT gamma.sigz.net. A SIG NXT
    SIG NXT ...

    beta.sigz.net.
    gamma.sigz.net. A 10.0.0.3
    SIG A ...

Att signera eventuellt tomrum

- Exempel på NXT + NOSIG
  - alpha.sigz.net. A 10.0.0.1
    SIG A ...
    TXT ”alpha”
    NXT gamma.sigz.net. A NXT NOSIG
    SIG NXT ...
    beta.sigz.net. A 10.0.0.2
    gamma.sigz.net. A 10.0.0.3
    SIG A ...

Observation: Vad är DNS bra på?

- Uppslagning – inte sökning
- Kompakt data
- Publik data
- Stabil data

Reflektion: Vad mer skall man lagra i DNS?

- Nycklar och certfikat?
  - för maskiner?
    - SSH nycklar
    - certifikat för IPsec
  - för människor?
    - PGP nycklar
- Telefonnummer?
  - ENUM
    - +46 31 701 42 13
    - 3.1.2.4.1.0.7.1.3.6.4.e164.arpa. NAPTR ... sip:jakob@crt.se ...
- Hockeyresultat?

Applikationsnycklar - APPKEY

- Det finns behov att via DNS distribuera rena publika nycklar för t.ex. följande applikationer:
  - IPsec
  - SSH
  - TLS (SSL)
- Dessa nycklar bör inte blandas ihop med de nycklar som används av DNSSEC själv, dvs KEY-poster.
- Rena publika nycklar är inte certifikat eftersom de inte bär sin egen säkerhet
  - Säkerheten uppnås av APPKEY + SIG i kombination
  - Giltlighetstiden styrs av signaturen

Sammanfattning

- DS – för bättre delegering
  - draft-ietf-dnsext-delegation-signer-02.txt
- NXT+NOSIG - för selektiv signering
  - draft-arends-dnsext-rrsets-00.txt
- APPKEY – för att lagra applikations nycklar
  - draft-schlyter-appkey-00.txt

- http://www.ietf.org/internet-drafts/

Är DNSSEC en PKI ?

- DNS ger möjlighet att distribuera data
  - DNS är världens största distribuerade databas
- DNSSEC gör att vi kan lita på att data inte är förändrad
  - Vi kan inte avgöra om data är korrekt
- DNSSEC ger ingen möjlighet till revokering
  - Kort giltlighetstid minskar behovet av revokering

DNSSEC och traditionell PKI i samverkan

- Distribution av traditionella certifikat via DNS
  - Kan göras redan idag – inte beroende av DNSSEC
  - Skalar bättre än alternativen, t.ex. LDAP, vid uppslagning
- Kan vi lita på traditionella certifikat genom att verifiera dem via DNSSEC?
  - Administratören för www.crt.se. stoppar in ett självsignerat certifikat för denna dator i DNS och signerar sedan zonen crt.se
  - Kan en webbläsare som litar på se. och därmed även crt.se. på ett säkert sätt hämta certifikatet för www.crt.se. ?
  - Kan webbläsaren lita på detta certifikat ?

Demoapplikationer för DNSSEC – Certifikat

- OpenSSL med stöd för DNSSEC och CERT-poster
  - litar automatiskt på självsignerade X.509 certifikat som hämtats och verifierats via DNSSEC
- Patchar till KDE Konqueror och Lynx
- http://www.crt.se/dnssec/apps/

Demoapplikationer för DNSSEC – IPsec

- isakmpd (IPsec/IKE) med stöd för KEY
  - publika nycklar kan hämtas via DNS
  - interopererar med Linux FreeS/WAN

- Inga certifikat behövs
  - alla publika nycklar lagras i DNS
  - kort livslängd på signaturerna eliminerar behovet av revokering

- isakmpd utnyttjar även stödet för att hämta certifikat från CERT-poster om stöd för detta finns i OpenSSL

Demoapplikationer för DNSSEC – PGP

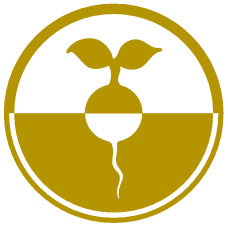
- applikationer för att hantera PGP-nycklar i DNSSEC
  - fetchpgp – hämtar PGP-nycklar från DNS
  - mkcertrr – tillverkar CERT poster
  - patchar till emacs mailcrypt

- http://www.crt.se/dnssec/apps/

sigz.net

- Testzon för DNSSEC
  - administreras av Lars-Johan Liman & Jakob Schlyter
  - frågor till <hostmaster@sigz.net>

- Vi flyttar helt enkelt . till sigz.net.
  - se. flyttas till se.sigz.net.
  - crt.se. flyttas till crt.se.sigz.net.
  - fi. flyttas till fi.sigz.net.
- Inte riktigt produktionskvalité
  - t.ex. ingen automatisk omsignering
- Mer information finns på www.sigz.net



Frågor?

Jakob Schlyter <j@crt.se>

http://www.crt.se/~jakob/
sip:jakob@crt.se