register.si

(r)evolucija DNSa

Benjamin.zwittnig@register.si

9.12.2013 SINOG

zgodovina

- DNS iz leta 1983/1984
  - ni (močnih) varnostnih mehanizmov
  - UDP
  - Infrastrukturna storitev
- DNSSEC
  - začetki 1997
  - Kaminsky 2008

DNSSEC

- Preprosta ideja: Odgovori dns strežnika digitalno podpisani
  - Problem: Vsi strežniki, ki gostijo neko domeno, morajo imeti isti ključ (nevarno)
- Domeno podpišemo vnaprej
  - Problem:Tudi odgovor, da nekaj ne obstaja, je pomemben

Kako preveriti podpise?

- Podpisovanje
  - ‘atom’ podpisovanja je RRSET
  - Izračunamo HASH RRET-a (SHA256, SHA1...)
  - HASH zakriptiramo z privatnim delom ključa = RRSIG
- Validator preveri podpis
  - Na enak način izračuna HASH dobljenega odgovora
  - RRSIG v odgovoru odkriptira z javnim delom ključa in dobi HASH, kot ga je izračunal podpisnik
  - Če sta HASH-a enaka, so podaki in podpis OK

Kdo naj preverja?

- Preverja naj tisti, ki dobi podatke
- Kako zaupati ključem?

Problemi

- Novi problemi
  - Podpisan odgovor ujamemo in ga podtaknemo, ko ni več ‘uporaben’
  - Kriptografski material v obtoku
- Rešitev
  - Podpisi imajo rok uporabnosti
  - Redna menjava ključev

Dodatni problemi

- Odgovori mnogo večji
  - Več prometa
  - DDoS napadi
- Večja poraba virov
- Več dela
  - Redno podpisovanje
  - Časovna usklajenost

Trenutno stanje

- Root zona podpisana od 15. julij 2010
- .si zona podpisana od 30. november 2011
- Cca. 1/3 TLDjev podpisanih
- SLD:
  - .si cca 40 od 110000
  - .se pionirji
  - .cz, .nl veliki registrarji/DNS ponudniki podpisujejo domene

Zaključek

- DNSSEC ni čudežna paličica
- Zaenkrat žal malo zanimanja
- Ni vidnih prednosti
- Novi problemi
- Naložba v prihodnost