DNSSEC az időben

Pásztor Miklós

ISZT

2016. március, Debrecen

Miről lesz szó?

1. DNSSEC terjedés
2. A regisztrátorváltás problémája
3. Eljárásrend DNSSEC-cel védett domain módosításakor
4. Mekkora baj a hiba?

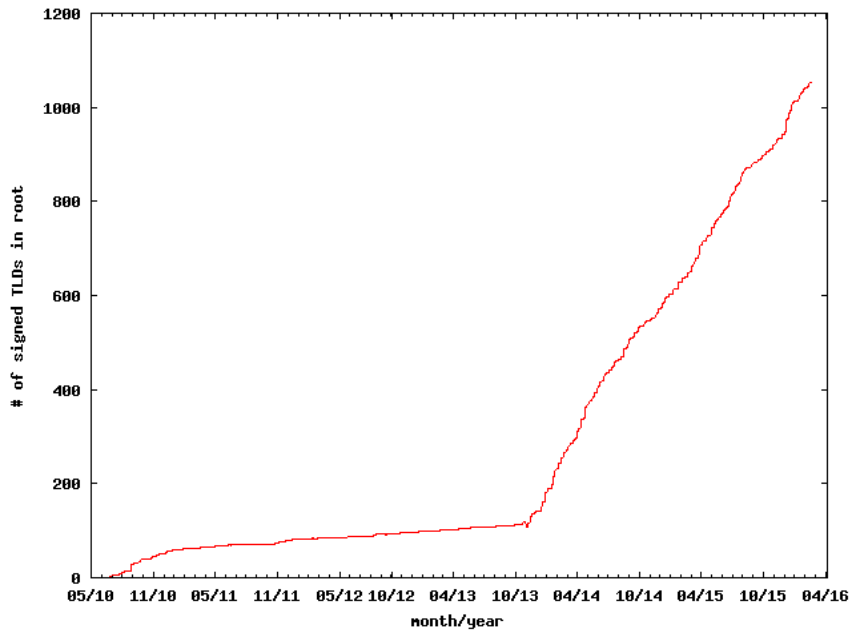
DNSSEC terjedés a világban

- 1999: RFC2535, az első DNSSEC RFC
- 2005: RFC4033-RFC4035, máig érvényes alapjai a DNSSEC működésnek
- 2005: .se bevezeti a DNSSEC-et
- 2010: A gyökér (.) domainban bevezetik a DNSSEC-et
- 2013: A google publikus rekurzív névszerverei (8.8.8.8, 8.8.4.4) is DNSSEC-cel működnek

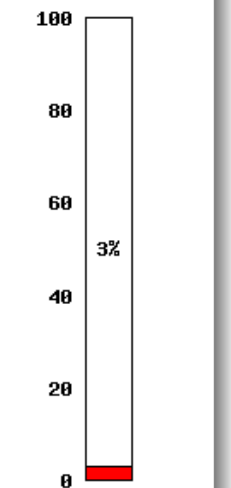
2016. márciusi állapot

- A TLD-k 91%-a DNSSEC-cel védett
  - → Ehhez nagyban hozzájárul, hogy a kb. 1000 új TLD-nél kötelező volt
- A másodlagos domain-oknak csak 3%-a védett DNSSEC-cel
- Forrás: http://rick.eng.br/dnssecstat/

DNSSEC-cel védett TLD-k



SLD-k



DNSSEC terjedés a .hu alatt

- 2011 április: kísérleti DNSSEC szolgáltatás
- 2014 október: az éles .hu zóna DNSSEC-cel működik
- 2015 február: a gyökér zónába bekerül a .hu-hoz tartozó DS rekord
- 2015 augusztus: a .hu és a nyilvános SLD-k alá elfogadunk DNSSEC delegálásokat
  - → Az első nap egyetlen DNSSEC-cel védett delegálás: `niif.hu` !
- 2016 március:
  - → a DNSSEC-cel védett domain-ok aránya 689/93 ezer, 13% !
  - → a .hu autoritatív névszerverekhez intézett kérdések 3,24%-a `DS`

DNSSEC a .hu regisztrációnál

- A `szuperkft.hu` zónát DNSSEC szerint kell konfiguálni
- A regisztrátor a regisztrációs felületen domain módosítást kezdeményez
  - → Bebillenti a DNSSEC chceckbox-ot
- A regisztrációs rendszer képezi a `szuprekft.hu` `DS` rekordját a zónában levő `DNSKEY` rekordból, és ellenőriz
- A regisztrációs adatbázisba és a `.hu` zónába bekerül a `DS` rekord

Regisztrátorváltás

- A `.hu` zónát több mint 100 regisztrátor szervezet kezeli
- Gyakran kérnek domain tulajdonosok regisztrátorváltást
  - → Ilyenkor a tulajdonosnak csak az új regisztrátorral kell felvennie a kapcsolatot
- Valójában nem is a regisztrátorváltás, hanem a DNS operátor váltás okoz gondot
  - → Nem lehet baj, ha a `szuperkft.hu` zóna névszerverei változatlanok, nem a regisztrátor kezelésében, hanem saját (vagy más külső) cég kezelésében vannak
  - → Viszont regisztrátorváltás nélkül is baj lehet, ha például egy másik külső cég veszi át a DNS szolgáltatást, az autoritatív névszerverek kezelését

Milyen baj lehet DNSSEC nélküli esetben?

- A `www.szuperkft.hu A` rekord cache-elve van egy rekurzív névszerverben
- A rekurzív névszerver felhasználói a változtatás után is a régi értéket kapják
  - → Elavult információkat kapnak
  - → Lehet, hogy a régi címen már nem is működik semmi
- Védekezés
  - → A DNS operátor váltás után egy ideig ne változzanak a tényleges (pl. `A`, `MX`) rekordok
  - → Párhuzamosan működjön egy ideig (TTL ideig) a régi és az új helyen pontosan ugyanaz a szolgáltatás
  - → Változás előtt vegyük le a szolgáltatásokhoz tartozó rekordok TTL idejét, és várjuk ki a régi TTL időt

Milyen baj lehet DNSSEC esetén?

- Lehet, hogy bizonyos információkat a régi, másokat az új névszerverektől kapunk
- A DNSSEC ellenőrzés megbukhat — ilyenkor nem elavult, hanem semmilyen információt nem kapunk, mert meghiúsul a névfeloldás
- A régi védekezési módok mind csődöt mondanak!
- Például:
  - → A `szuperkft.hu` eddig is DNSSEC-cel védett volt, `DS` rekordjának TTL-je 1 nap
  - → A regisztrátor óvatlanul módosítja a `DS` és `NS` rekordokat a `.hu`-ban
  - → Egy új `A` rekord aláírás ellenőrzése megbukik akár 1 teljes napon át a régi, cache-ben levő `DNSKEY`-vel!

A DNSSEC megszüntetés

- A `szuperkft.hu` domain `DNSKEY` rekordjait nem vehetjük ki addig a zónából, amíg a `.hu`-ban ott a megfelelő `DS` rekord
- Akkor is baj lehet, ha egy időben vesszük ki a zónából a DNSSEC rekordokat az apuka zónában levő `DS` rekorddal
  - → Ilyenkor előfordulhat, hogy a `DS` rekord még a cache-ben van
    - A validáló rekurzív névszerver csak akkor fogja feloldani a neveket, ha megfelelő `DNSKEY` rekordo(ka)t és aláírásokat talál a zónában
- A DNSKEY rekordokat, aláírásokat viszont büntetlenül be lehet vezetni egy zónában, amíg nincs az apuka (`.hu`) zónában a `DS` rekord

Sorrendek DNSSEC bevezetésekor és megszüntetéskor

Bevezetés

1. Generálunk kulcsokat, aláírjuk a zónát
2. Szolgáltatjuk a DNSSEC-cel védett zónát
3. Tesztelünk, figyelünk
4. Bevezetjük az apuka zónába a megfelelő `DS` rekordot

Megszüntetés

1. Kivesszük az apuka zónából a `DS` rekordot
2. Várunk
3. Kivesszük a zónából a DNSSEC rekordokat
4. Szolgáltatjuk a DNSSEC nélküli zónát

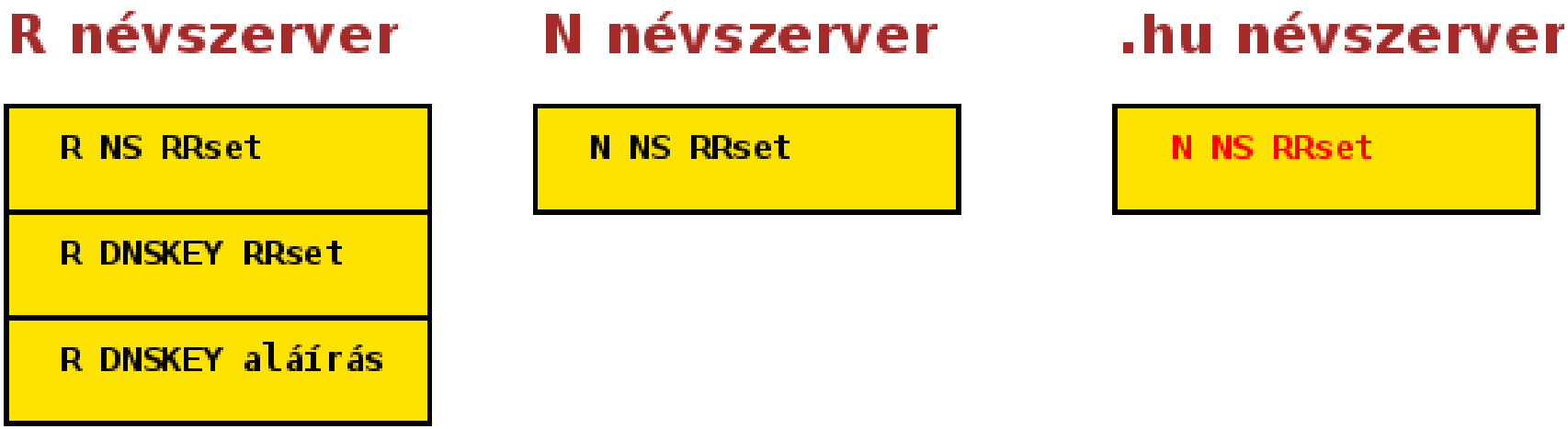
DNSSEC megszüntetés, 1. fázis

- Kezdetben a `.hu` alatt a régi (R) szolgáltatóhoz tartozó `NS` és `DS` rekordok vannak
- Az új (N) szolgáltató már bekonfigurálta DNSSEC nélkül a domain-t

DNSSEC megszüntetés, 2. fázis

- Az új regisztrátor módosítja a domain-t úgy, hogy az `NS` RRset a régi marad
- A delegálás DNSSEC nélküli. Kikerül a `DS` rekord a `.hu` zónából
- A következő lépés előtt várni kell legalább a régi `DS` TTL idejének és a régi `DNSKEY` rrset TTL idejének maximumát

DNSSEC megszüntetés, 3. fázis



- A `.hu` zónába bekerülnek az új szolgáltatóhoz tartozó `NS` rekordok

DNS szolgáltatóváltás a DNSSEC működés ideiglenes szüneteltetésével

- Nem lesznek DNSSEC hibák, ha
  - → Az új DNS operátor először is kiveszi a `.hu` alól a `DS` rekordot
  - → Vár a `DS` rekord TTL idejéig
  - → Módosítja az `NS` RRset-et a `.hu` alatt
  - → Vár (régi) `NS` TTL ideig,
  - → Ezek után vezeti be az új `DS` rekordokat.
- Hátrány: lesz egy idő, amikor a zóna DNSSEC szempontból védtelen
- Ha a zónában vannak DNSSEC-et feltételező szolgáltatások (pl. SSHFP vagy DANE), akkor ezek ezalatt az idő alatt nem fognak működni

Szolgáltatóváltás DNSSEC szüneteltetéssel, 1. fázis

- Kezdetben a `.hu` névszerverben a régi (R) szolgáltatóhoz tartozó `DS` és `NS` rekord van
- Az új (N) szolgáltató is bekonfigurálta már a zónát
  - → Az új szolgáltatónál a DNSSEC is be lehet konfigurálva, ez a folyamatban nem okoz zavart

Szolgáltatóváltás DNSSEC szüneteltetéssel, 2. fázis

- Az új regisztrátor kiveszi a régi `DS` rekorodot a régi `NS` RRset változatlanul hagyásával
- A következő lépés előtt a régi `DS` rekord TTL idejét várni kell

Szolgáltatóváltás DNSSEC szüneteltetéssel, 3. fázis

- Az új regisztrátor `NS` rekord módosítást kezdeményez DNSSEC megadása nélkül
  - → Az új zónában ott lehetnek már a DNSSEC rekordok, ezek nem jutnak addig érvényre, míg a bizalmi lánc nem záródik, vagyis a `.hu` zónába nem kerülnek be az új `DS` rekordok
- A következő lépés előtt a régi NS rekord TTL idejét várni kell

Szolgáltatóváltás DNSSEC szüneteltetéssel, 4. fázis

- Az új regisztrátor DNSSEC-cel konfigurálja a regisztrátori felületen a domaint

  → Bekerül az új `DS` rekord a `.hu` zónába, újra zárul a bizalmi lánc

DNS szolgáltató váltás folyamatos DNSSEC működéssel

- El lehet érni, hogy DNS szolgáltató váltás során is folyamatosan DNSSEC szerint biztonságosan fel lehessen oldani a `szuperkft.hu` alatt levő neveket
- Az apuka zónában, a `.hu` alatt ilyenkor is háromszor kell változtatást kezdeményezni
- Az egyes lépések közt várni, hogy a cache-ekből a régi adatok kikerüljenek

DNS szolgáltató váltás folyamatos DNSSEC működéssel, 1. fázis

- Kezdetben a `.hu` névszerverben a régi (R) szolgáltatóhoz tartozó `DS` és `NS` rekord van
- Az új (N) szolgáltató is bekonfigurálta már a zónát

DNS szolgáltató váltás folyamatos DNSSEC működéssel, 2. fázis

- Az új szolgáltató a régi DNSKEY RRset-ben levő ZSK és KSK rekordokat is beteszi a saját `DNSKEY` RRset-be
- Aláírja az új KSK-val

DNS szolgáltató váltás folyamatos DNSSEC működéssel, 3. fázis

- A régi szolgáltató az új DNSKEY RRset-ben levő ZSK és KSK rekordokat is beteszi a saját `DNSKEY` RRset-be
- Aláírja a régi KSK-val

DNS szolgáltató váltás folyamatos DNSSEC működéssel, 4. fázis

- A `.hu` zónába bekerül az új `DS` a régi mellé
- Az `NS` rekord RRset még a régi
  - → Ezt az új regisztrátor úgy tudja elérni, hogy domain módosítást kér DNSSEC-cel úgy, hogy a regisztrációs rendszerben egy régi névszervert ad meg kiinduló NS-ként
- A következő lépés előtt várni kell legalább a régi `DS` TTL idejének és a régi `DNSKEY` rrset TTL idejének maximumát

DNS szolgáltató váltás folyamatos DNSSEC működéssel, 5. fázis

- A .hu zónában a régi NS RRset-et az új váltja fel
- A régi DS még bent marad az újjal együtt
  - → Ezt az új regisztrátor úgy tudja elérni, hogy domain módosítást kér DNSSEC-cel úgy, hogy a regisztrációs rendszerben egy új névszervert ad meg kiinduló NS-ként
- A következő lépés előtt várni kell legalább a maximumát a következő három értéknek:
  - → régi NS rekord TTL ideje az apuka (.hu) zónában
  - → régi NS rekord TTL ideje a régi zónában
  - → a legnagyobb TTL az aláírt régi zónában

DNS szolgáltató váltás folyamatos DNSSEC működéssel, 6. fázis

- Az új szolgáltató kiveszi a régi szolgáltatóhoz tartozó `DNSKEY` rekordokat
- Újra aláír az új KSK-val

DNS szolgáltató váltás folyamatos DNSSEC működéssel, 7. fázis

- A `.hu` zónából kikerül a régi `DS`, miután az új regisztrátor domain módosítást kért
- Ezzel lezárul a DNS szolgáltató váltás folyamata.

Kísérlet

- Szándékosan hibás DNS szolgáltató váltás
- A `DNSKEY`, `DS` rekordok is változnak
- Az `isztteszt2.hu` zóna névszerver
- Mennyi ideig, és mely rekurzív névszervereknél lesz hiba?

Kitérő — dnsyo

- `https://github.com/samarudge/dnsyo`
- DNS terjedés ellenőrzésére szolgáló eszköz pythonban
- Megmondja, hogy sok-sok rekurzív névszerver hogyan old fel egy-egy nevet
- Tartalmaz egy $>$ 1000 szerverből álló rekurzív szerver listát
- Ezekből 76 válaszol `AD` bittel

A kísérletünknél felhasznált rekurzív szerverek

- A dnsyo 76 szervere
  - → Természetesen `8.8.8.8` és `8.8.4.4` ott van köztük
- Az Invitel két rekurzív szervere (évek óta DNSSEC-cel működnek!)
  - → `62.77.203.10`
  - → `213.163.34.66`
- Az OARC validáló szerverei
  - → `149.20.64.20`
  - → `149.20.64.21`
- `127.0.0.1`: itt Unbound 1.4.17 fut
- IPv6 címeket nem használtunk

Az ellenőrző szkript

```
#!/bin/sh
while true; do

T=$(date +%F_%T)
for i in $(cat /var/tmp/godi-rekurziv-lista);do
 echo $i;dig a.isztteszt2.hu  @$i;done >/var/tmp/r-$T
sleep 120
done
```

- A szkript futása közben változtattuk az `isztteszt2.hu` névszervereit a `.hu` zónában
- Az `NS` és a `DNSKEY` rekordok is változtak
- Durva változtatás, nem volt másik névszerverhez tartozó `DNSKEY` rekord sem a régi, sem az új névszerverben
- Az `a.isztteszt2.hu` TTL-jét változtattuk

Tapasztalatok

TTL=86400 eset

- Sok névszervernél egyáltalán nem jelentkezett hiba
- A Google nyilvános névszervereinél egyáltalán nem volt hiba
- A hibát mutató névszerverek közül is a legtöbb egy órán belül rendbejött

TTL=300 eset

- Minden névszerver hibát (`SERVFAIL`-t) jelzett
- A Google nyilvános névszerverei egy órán belül rendben mutatták az új értéket
- A hibát mutató névszerverek közül némelyik közel egy napig nem jött rendbe

Tanulságok

- Általában nem olyan rossz a helyzet, mint amilyen lehetne
- Ha levesszük a „közönséges” (pl. `A`) rekord TTL-jét DNSSEC esetben, az csak ront a helyzeten!
- A rekurzív névszerverek védekezhetnek és némelyek valóban védekeznek bizalmi lánc megtörése ellen
  - → Az autoritatív szervertől kapott TTL-t felülbírálhatják
  - → Ha megbukik egy DNSSEC ellenőrzés, újra kérik a DNSSEC (`DS`, `DNSKEY`) rekordokat
  - → A Google nyilvános névszerverei biztosan csinálják

TTL felülbírálás

- A rekurzív névszervereket újraindíthatják
- A rekurzív névszerverben lehet minimum/maximuma a TTL-nek
- A rekurzív névszerver használhat forwardereket (DNS proxykat)
- A rekurzív névszerver lehet multihomed hoszt, amik egymástól független cache-t használnak

DNSSEC és DNS szolgáltató váltás problémájáról szóló olvasnivaló

1. Peter Koch draft-ja alapos munka (bár sajtóhibáktól nem mentes): `https://tools.ietf.org/html/draft-koch-dnsop-dnssec-operator-change-06`
2. Steve Crocker előadása: `http://conferences.npl.co.uk/satin/presentations/satin2011slides-Crocker.pdf`
3. ISOC dokumentum EPP-vel történő változtatásra: `http://wp.me/p4eijv-4lF`
4. Verisign segédlet: `https://www.verisign.com/assets/whitepaper-dnssec-transfers.pdf`
5. A .pl regisztrációs segédlet is tartalmaz DNS szolgáltató váltásra vonatkozó információt a 6. és 7. pontban.
6. Az .at segédlet nem szól a regisztrátorváltáskor fellépő nehézségekről.
7. A dyn.com szolgáltató írása lépésről lépésre leírja a DNSSEC-cel védett zónánál a szolgáltató váltás folyamatát.
8. `http://deneb.iszt.hu/~pasztor/dnssec-regisztrator-valtas.html`