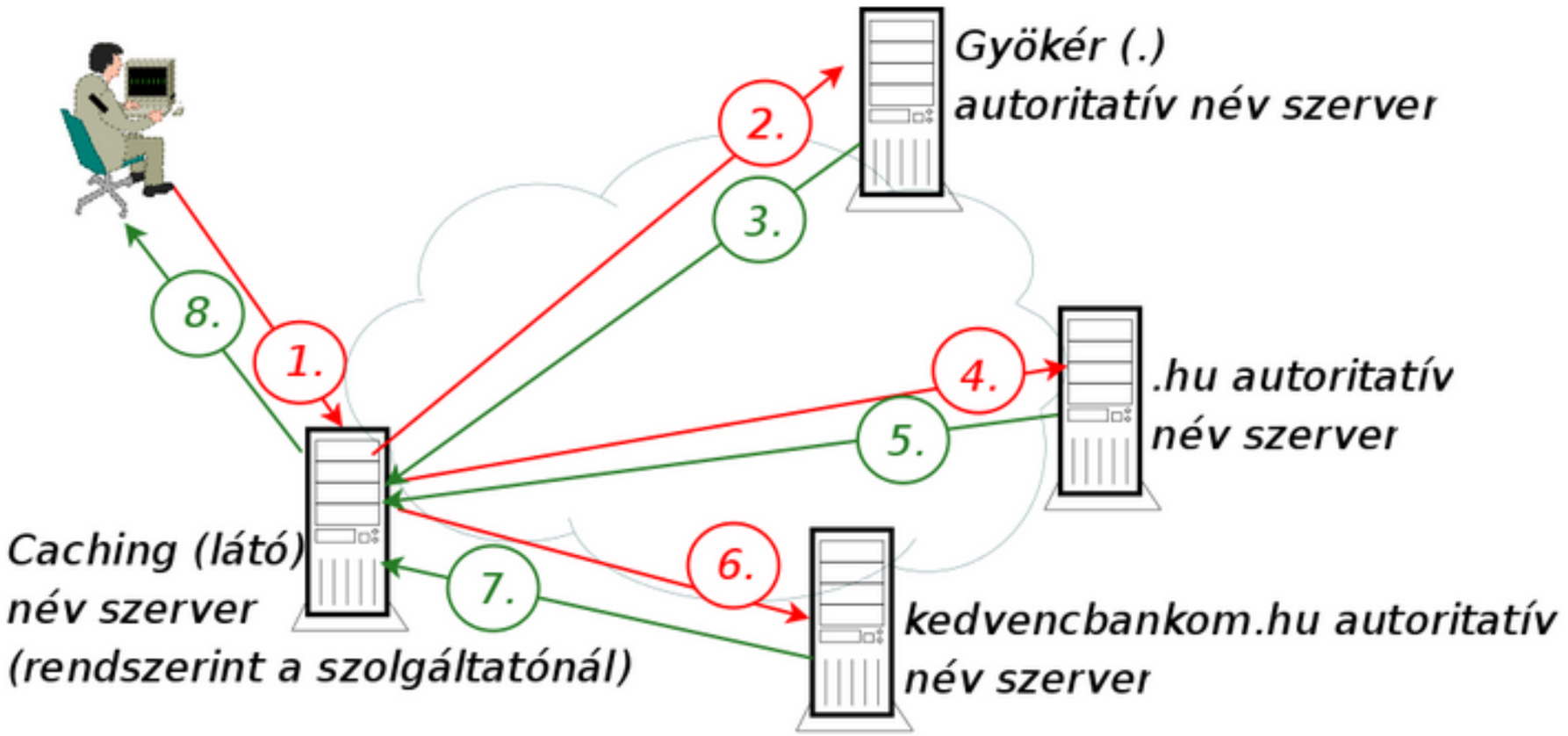
DNSSEC: motiváció és elv

Pásztor Miklós
PPKE/ITK - ISZT
pasztor@ppke.hu - pasztor@iszt.hu

Név feloldás

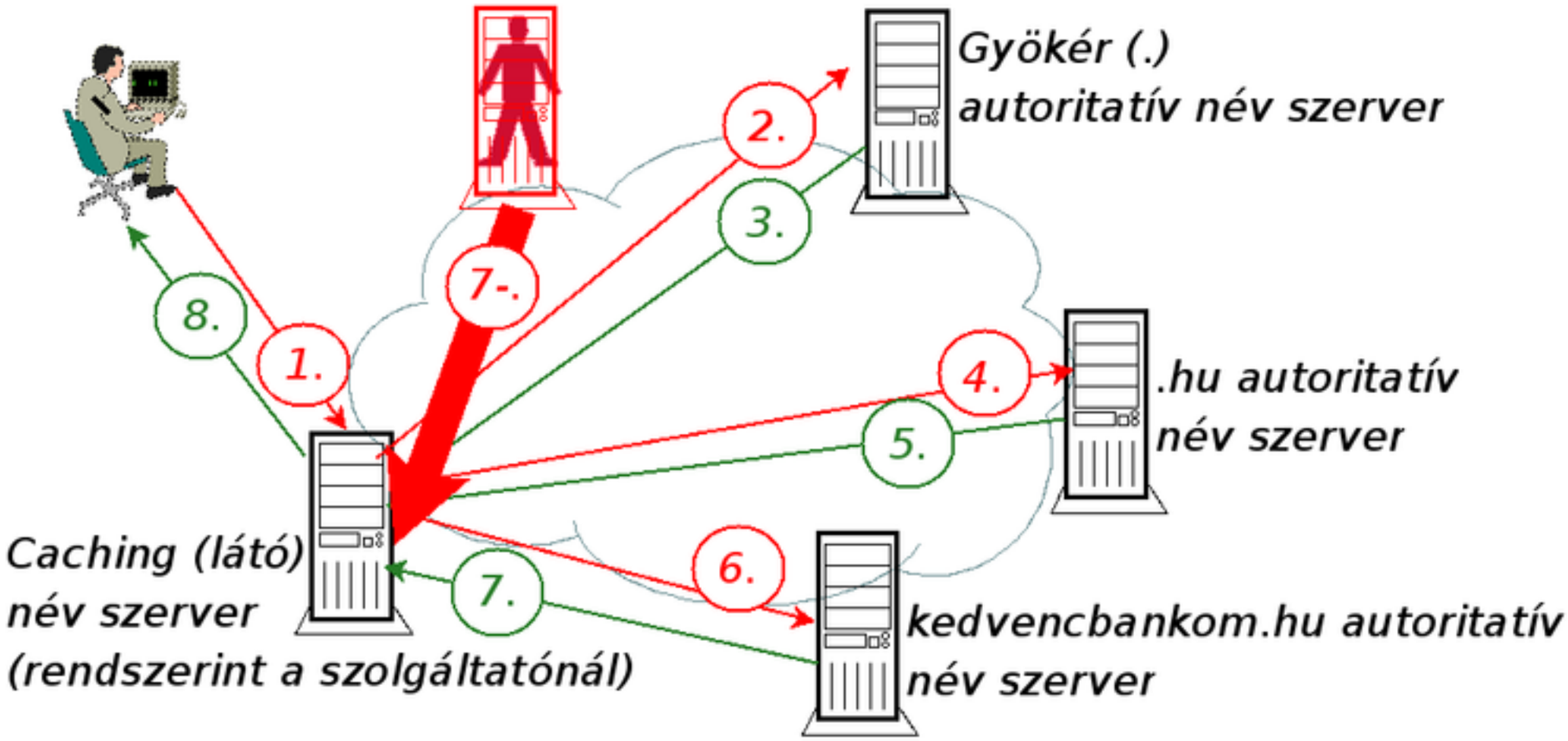


1. www.kedvencbankom.hu ?
2. www.kedvencbankom.hu ?
3. Nem tudom, de itt vannak a .hu név szerverei!
4. www.kedvencbankom.hu ?
5. Nem tudom, de itt vannak kedvencbankom.hu név szerverei!
6. www.kedvencbankom.hu ?
7. www.kedvencbankom.hu A rekordja: 111.22.33.44 (autoritatív válasz)
8. www.kedvencbankom.hu A rekordja: 111.22.33.44 (nem autoritatív válasz)

A DNS szerverek kettős feladata

- Látni
  - Az elosztott adatbázist kérdezni szerte az interneten
  - Caching, rekurzív név szerverek
- Mutatni
  - A rájuk tartozó részről a többi szerver számára adatokat szolgáltatni
  - Autoritatív név szerverek

DNS cache poisoning / cache mérgezés



1. www.kedvencbankom.hu ?
2. www.kedvencbankom.hu ?
3. Nem tudom, de itt vannak a .hu név szerverei!
4. www.kedvencbankom.hu ?
5. Nem tudom, de itt vannak kedvencbankom.hu név szerverei!
6. www.kedvencbankom.hu ?

7-. www.kedvencbankom.hu A rekordja:
111.6.6.6 (autoritatív válasz) !!!

DNS cache poisoning (2.)

- Becsempészhetnek a 3-. és 5-. lépésben is rosszindulatú rekordot
- A nyílt rekurzív szerverek növelik a veszélyt
- 2008. júliusában Dan Kaminsky felfedezte, hogy nagyobb a fertőzés veszély mint gondolták: nem nehéz jó választ elhitetni
  - A gyártókat összehívta, bemutatta a felfedezését
  - Több név szerver program új változattal jött ki, mire nyilvánosságra hozta a felfedezést
    - Több véletlen a kérdés rekordban

A cache poisoning nehézség

- Ha a cache-ben van egy rekord, TTL ideig várni kell, míg újra esélyünk van, hogy megfertőzzük
  - 24 óra gyakori
- A DNS kérdés tranzaction ID-jét el kell találni
  - 16 bitnyi, 65536 lehetőség van
  - Lehet sok százszor, vagy ezerszer próbálkozni
  - Így sincs túl sok esély...
  - *Vagy mégis ?*

1. könnyítés: birthday attack

- Mi a valószínűsége, hogy a jelenlevők közt van két ember, aki a hónap ugyazon napján született?
- Valószínűleg a legtöbben meglepődnek, hogy milyen nagy!

```
#!/bin/perl
#   Mi a valószínűsége, hogy mindenki különböző napon született? ($p)
$N=31;$p=1;for $i (1..$N) { $p=(($N-$i)/$N)*$p;$r=1-$p;print $i+1, ":\t$p\t$r\n"}

2:      0.967741935483871       0.032258064516129
3:      0.905306971904266       0.0946930280957337
...
7:      0.481708424598635       0.518291575401365
...
16:     0.00864440401314186     0.991355595986858
17:     0.00418277613539122     0.995817223864609
...
32:     0       1
```

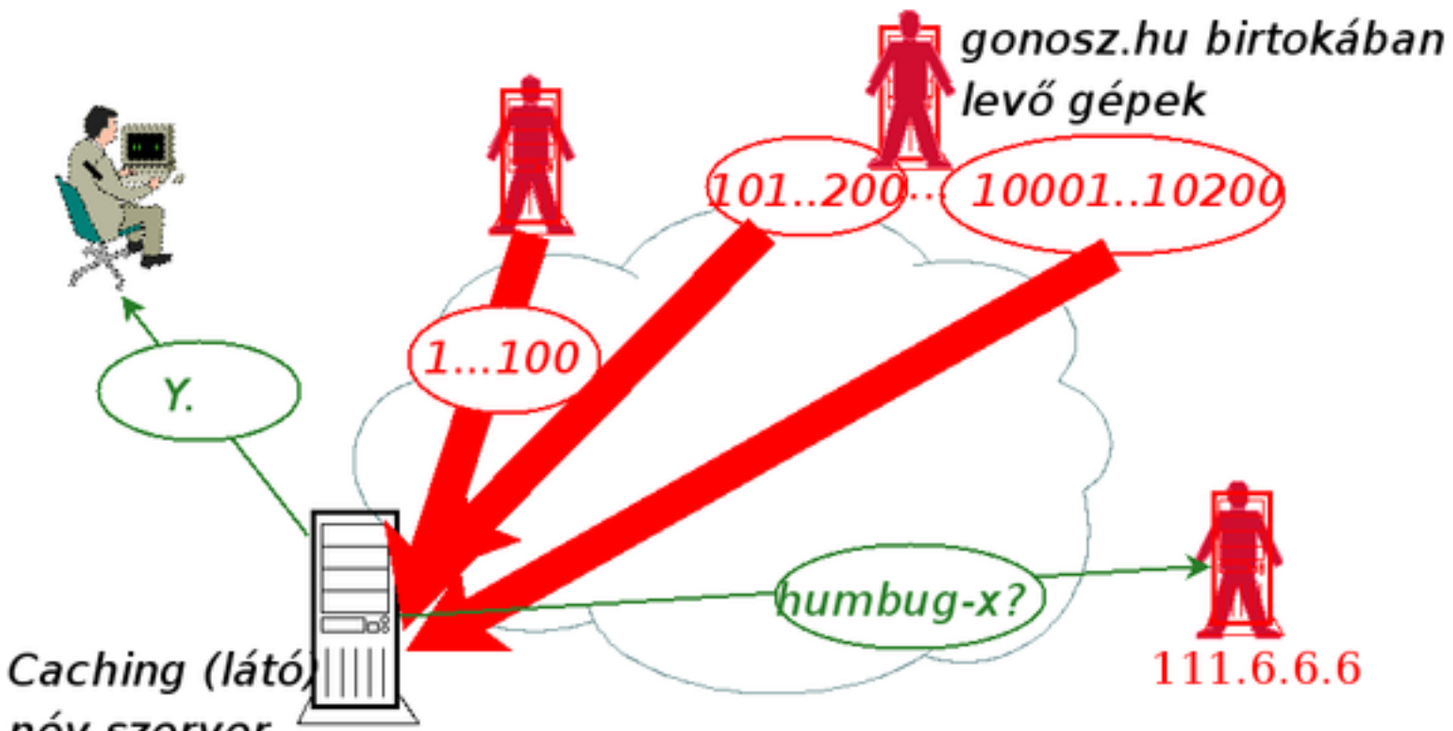
- Ha sok ID **bármelyikét** elég eltalálni, könnyebb a dolgunk!
  - 65536 eset esetén 0,5-nél nagyobb valószínűséghez 302, 0,9-nél nagyobbhoz 550 próbálkozás kell

2. könnyítés: Kaminsky felfedezése

- Nem www.kedvencbankom.hu-t, hanem
  - humbug-1.www.kedvencbankom.hu, vagy
  - humbug-2.www.kedvencbankom.hu, vagy
  - ... vagy
  - humbug-100.kedvenvcbankom.hu

  valamelyikét ,,kötjük el"
- Ez elég!

Hogyan működik?



1..100 humbug-1.www.kedvencbankom.hu,...humbug-100.www.kedvencbankom.hu ?

101..200. humbug-1-et nem tudom, de
a név szervere www.kedvencbankom.hu, IP címe 111.6.6.6!!!

... é.í.t...

9901..10000. humbug-99-et nem tudom, de
a név szervere www.kedvencbankom.hu, IP címe 111.6.6.6!!!

A humbux-x kérés jelzi a támadónak, hogy sikerrel járt.

Az Y.-ik lépésben a cache-ből
a fertőzött tartalmat adja a látó név szerver!!!

Mi van veszélyben?

- *,,A DNS azért szuper, mert folyamatosan, a felhasználók számára transzparansen működik, pedig minden levél küldésnél és fogadásnál, web lap letöltésnél stb. szerepe van."*
- Következmény: **minden** veszélyben van
- Web
- SIP
- A leveleinket mások olvashatják, módosíthatják
  - Elfelejtett jelszó? Kattintson ide! ...
- CA-knál tanúsítvány kérés/ellenőrzés: legtöbbször levelezésen alapul
- Bővebben pl.: http://www.doxpara.com/DMK_BO2K8.ppt

Hogyan lehet cache poisoning ellen védekezni?

- Nagyobb TTL a ,,klasszikus" poisoning ellen védett, Kaminsky ellen hasztalan!
- A 2008. júliusi DNS szoftver upgrade-ek a legfontosabb lépés
  - A kérdés tranzaction ID-je is és a forrás UDP port is legyen véletlen szám
- Ellenőrizzük a látó névszervereinket pl.:
  - https://www.dns-oarc.net/oarc/services/porttest
  - http://entropy.dns-oarc.net/test/
- Ne bízzunk a DNS-ben!
- A fontos tanúsítványokat ,,kézzel" (pl. telefonon) ellenőrizzük

Cache poisoning ellen sokat tehetnek a routerek gazdái!

- A mérgezés egyik feltétele a ,,mutató" név szerver IP címének hamisítása
- RFC2827 (BCP38): ingress traffic filtering
  - Minden interfészen csak olyan forrás címmel engedjünk be csomagot, ami onnan valóban jöhet!
- Ez nem teljes védelem
- Sok veszélytől véd, de:
  - A LAN-on még hamisíthatják a router-t!
  - A látó név szerver hálózatán hamisíthatják a név szervert!
  - A mutató név szerver hálózatán hamisíthatják a név szervert!

DNSSEC

- A cache poisoning elleni védekezés **egyik** módja
- Véd DNS elkötés ellen is: pl. Verisign wildcard, 2003
- A DNSSEC-ről az első RFC: rfc2065 (1997)
- Már 2000-ben a Networkshop-on, Gödöllőn szó volt erről: DNS biztonsági kérdések
- Lassan halad a bevezetés
  - Kaminsky felfedezése sietteti
- Sok szervezet népszerűsíti: ICANN, RIPE, EU, kormányok
- Elöl járnak a bevezetésben: .SE, .RIPE.NET, .CZ, .BG

Elv

- Az egyes DNS rekordokat nyilvános kulcsú digitális aláírással látjuk el
- A DNS delegáláshoz hasonlóan, a magasabb szinten aláírjuk a delegált zónában használt publikus kulcsot (DS rekord)
- A DNS adat **hitelességét** és **sértetlenségét** garantáljuk
- Kurrens fő RFC-k: RFC4033, RFC4034, RFC4035

RR-ek és RRset-ek

- RR: Resource Record, a DNS adatbázis egy eleme
- RRset: egy zónában RR-ek halmaza, amiknek azonos:
  - Nevük (bal oldaluk)
  - Típusuk (pl. mind NS)
  - Osztályuk (gyakorlatban mindig IN)

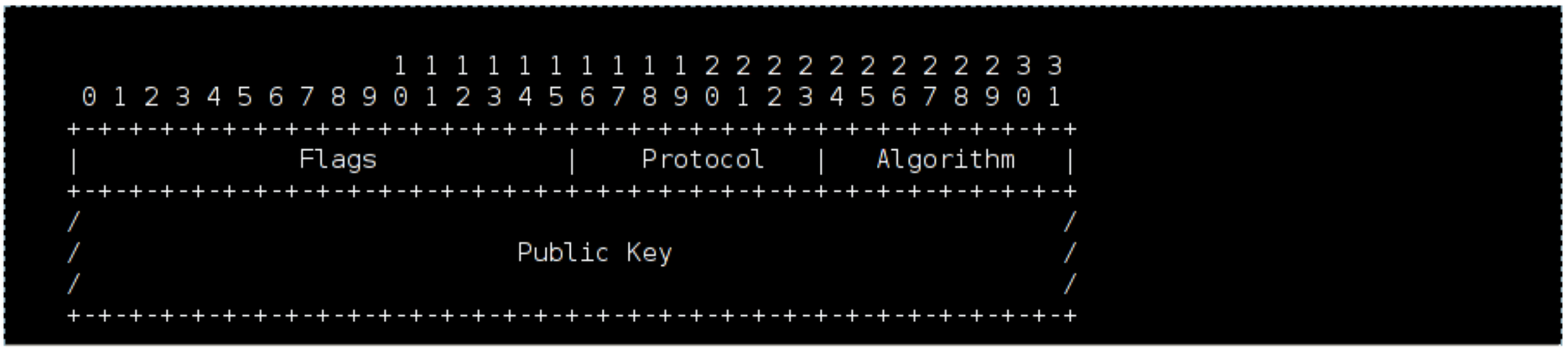
A DNSSEC kriptográfia sajátosságai

- Nincs titkosítás, csak digitális aláírás
- A DNSSEC nem PKI
- Nincs kulcs lejárati idő
  - De az aláírásnak van lejárati ideje
  - A DNS rekordoknak is (TTL)
- Nincsenek visszavonási listák (key revocation lists)
  - A DNS rekordok eleve rövid életűek (TTL)
  - Újabban (RFC5011) bevezettek egy ,,visszavont kulcs" bitet
- Csak DNS-sel kapcsolatos kriptográfia
  - Lehetnek pl. PGP, vagy SSH kulcsok a DNS-ben, de ezzel nem foglalkozik

Bevezetünk új flag-eket a DNS üzenetekben

- `DO` (Dnssec Ok)
  - Kérdésben használatos: kérem a DNSSEC rekordokat is
- `CD` (Checking Disabled)
  - Te ne ellenőrizz, majd én
- `AD` (Authenticated Data)
  - Ezt ellenőriztem és rendben találtam DNSSEC szerint
- A bitek helyéhez szükség van EDNS0-ra (Extended DNS, RFC2671)
  - Szükség van az EDNS0 által bevezetett hosszabb csomagméretre is - a ,,klasszikus" DNS csak legfeljebb 512 byte hosszú csomagokat használ

DNSKEY rekord



- Protokoll: mindig 3
- Algoritmus: legtöbbször 5 (RSASHA1), lehet más
  - Az egyik algoritmussal aláírt kulcs lehet más algoritmusú...

DNSKEY flag-ek

- Bit 7 (256): Zone Key
  - Gyakorlatilag mindig áll
  - Ha nem, akkor nem szabad DNS rekordok ellenőrzésére használni
- Bit 15 (1): Secure Entry Point
  - RFC3757
  - KSK (Key Signing Key) jelölésre
    - Csak a DNSKEY RRset-et írjuk vele alá
  - Ebből keletkezik az apuka zónában a DS rekord

KSK és ZSK

- KSK Key Signing Key, viszonylag ritkán változik, hosszú
  - Csak a DNSKEY rrset-et írjuk vele alá
- ZSK Zone Signing Key, viszonylag gyakran változik, nem túl hosszú kulcs
  - RSA esetén a kulcs hosszával nő:
    - Az aláírás hossza
    - Az erőforrásigény
- Az apuka zónában a KSK-t írják alá (pontosabban a hash-ét)
- A KSK-val a zóna gazdája aláírja a ZSK-t, a ZSK-val az egyes rekordokat

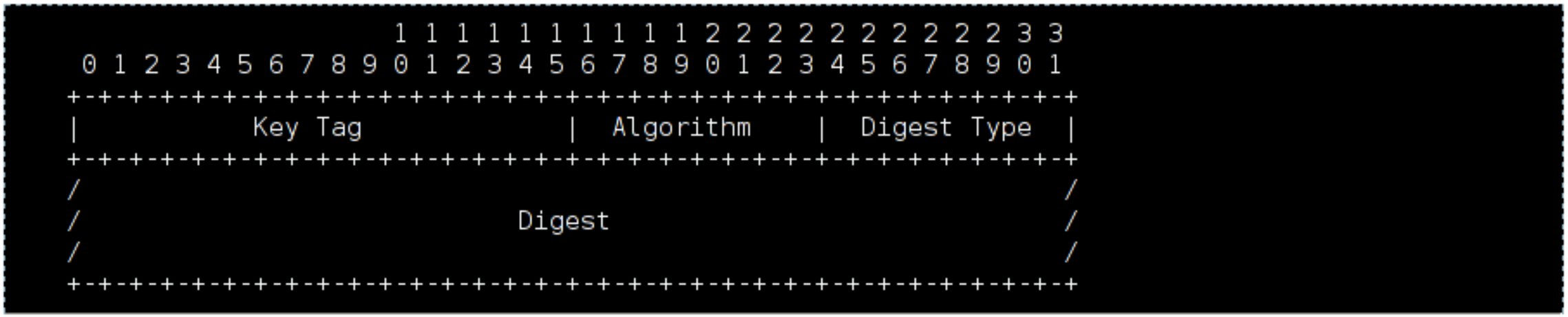
Újabb DNSKEY flag: revoke

- RFC5011
- Egy régi kulcs aláírásával be lehet vezetni új kulcsot
  - Ha ilyet egy támadó meg tud tenni, nagy baj lehet
    - Pl. visszavonhat tényleges kulcsot
  - Ezért egy ilyen új kulcs nem él azonnal, csak indít egy timer-t
- Bit 8 (512): Revoke
- Ha ilyet lát a látó név szerver **- aláírva -** , akkor visszavontnak tekinti a kulcsot
- A revoke csak akkor érvényes, ha önmagával (is) alá van írva
  - Ha több kulcs van használatban, és nem mind kompromittálódott, a támadó nem tudja mindet visszavonni

DS - Delegated Signer rekord

- A bizalmi lánc építésére szolgál
- A bizalmi lánc hierarchia megegyezik a DNS hierarchiával
  - Egyelőre ,,bizalmi szigetek"
- A delegált zóna KSK-hoz tartozó nyilvános kulcs ID-t, a kulcs hash-ét tartalmazza
- Az delegáló zóna ZSK-jával aláirandó

DS rekord formátum



- A Digest Type: rendszerint 1 (SHA-1). Elvben/később lehet más
- Algoritmus: legtöbbször 5 (RSASHA1), lehet más
- A Digest az owner name-et és az DNSKEY rekordot fogja át (nem csak a kulcsot)

Key Tag

- Segít a megfelelő kulcs kiválasztásában
- A kulcs rekord 2-byte-os darabjainak összege 1-es komplemens aritmetikával
- **Nem** egyedi, nem szabad csak erre hagyatkozni

RRSIG rekord

RRSIG rekord mezők

- Labels: hány darabból (label) állt az aláírt rekord
  - A wildcard rekordokkal kapcsolatban hasznos
- Original TTL: az aláírt rekord (RRset) ttl-je
- Signature Expiration/Inception
  - 1970 január 1 0:0:0 UTC óta eltelt idő másodpercben megadva
  - Szokás `YYYYMMDDHHmmSS` alakban írni
- Signer's Name
  - Az aláíró DNSKEY kulcs bal oldala (owner name)

Hogyan tudjuk aláírni a ,,nincs ilyen" rekordot

- Nem akarunk ,,menet közben" aláírni
  - Nagyon ,,drága" lenne minden ,,nincs ilyen" választ aláírni
  - Nincs is az autoritatív DNS szerveren titkos kulcs!
    - Legalább is *lehetőleg* nincs

NSEC (Next Secure)

```
hu.                     86400   NSEC    0-24.hu. NS SOA TXT RRSIG NSEC DNSKEY
```

- Mutatja, hogy ehhez a névhez milyen rekordok tartoznak
- Lexikografikus sorrendben mi a következő rekord
- Minden ,,klasszikus" rekordhoz legalább +2 rekord
  - NSEC
  - RRSIG NSEC
- Ezáltal a zóna mérete többszörösére nő (a csak delegálásokat tartalmazó .hu 7-szeresére)

DNS walk

- Biztonsági kockázat, amit a DNSSEC nyit
  - Ha NSEC rekordok vannak, akkor hiába tiltjuk a zóna transzfert:

```
$ldns-walk ripe.net @ns-pri.ripe.net
ripe.net.       A NS SOA MX AAAA RRSIG NSEC DNSKEY
_sip._udp.ripe.net.     SRV RRSIG NSEC
_stun._udp.ripe.net.    SRV RRSIG NSEC
adsl.ripe.net. A RRSIG NSEC
e0.adsl.ripe.net.       A RRSIG NSEC
aironet10.ripe.net.     A RRSIG NSEC
aironet11.ripe.net.     A RRSIG NSEC
aironet2.ripe.net.      A RRSIG NSEC
...
```

- A zóna *letapogatható !*

Alternatíva: NSEC3

- Régi terv, több internet draft tárgyalta
- Egész új RFC: RFC5155, 2008. március
- A szoftverek újabb változatai már támogatják (NSD, Unbound, Bind)
- Nem a neveket, hanem a nevekből képzett hash-eket tartalmazza

```
H(example)       = 0p9mhaveqvm6t7vbl5lop2u3t2rp3tom
H(ns1.example)   = 2t7b4g4vsa5smi47k61mv5bv1a22bojr

0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.example. NSEC3 1 1 12 aabbccdd (
                          2t7b4g4vsa5smi47k61mv5bv1a22bojr MX DNSKEY NS
                          SOA NSEC3PARAM RRSIG )
```

- Opt-in mechanizmust is megenged: a *következő* jelentheti a *következő DNSSEC-cel védett* rekordot
- A nem DNSSEC delegálások átugorhatók

Key rollover - KSK

- RFC4641
- A kulcsokat előre tervezett periódusonként cserélni kell
- Új KSK felvétele
  - Generálunk új KSK kulcsot
  - Aláírjuk a régi és az új kulccsal **is** a DNSKEY set-et
  - Az apuka zónába elküldjük a publikus részét, megvárjuk a DS rekordját (az apuka másodlagosainál is!)
  - Elküldjük minden más helyre, ahol esetleg trusted key-ként szerepelt
  - A régi kulcsot és aláírásait csak akkor vegyük ki, ha már lejártak a régi TTL-ek (a régi kulcs DS TTL-e, amit az apuka zóna mutatott!)
    - Itt juthat szerephez az RFC5011 szerinti revoke bit
  - A .se KSK kulcsok: http://www.iis.se/domains/sednssec/publickey
  - RIPE: https://www.ripe.net/projects/disi/keys/
  - Root (test): https://ns.iana.org/dnssec/status.html

Key rollover - ZSK

- RFC4641
- 1. módszer: double signature
  - Generáljunk új ZSK kulcsot
  - A régi és az új kulccsal is aláírjuk a zónát (double signature)
  - Várunk a régi aláírások legnagyobb TTL-je időt
  - A régi kulcsot és az aláírásait kivesszük
- 2. módszer: pre-publish
  - Generáljuk az új ZSK kulcsot
  - Várunk, míg minden másodlagos és cache tartalmazza a DNSKEY RRset-ben
  - Aláírjuk a zónát **csak** az új kulccsal
  - A régi kulcsot még megtartjuk, amíg a régi aláírások TTL-je mindenütt le nem jár
  - Eltávolítjuk a régi kulcsot a DNSKEY rrset-ből

Látó (rekurzív) név szerver konfiguráció

- Trust anchor-okat kell bekonfigurálni
  - Nyilvános KSK kulcsok, amiket pl. a ripe.net, .se stb. használ
- Azokat az aláírásokat fogja elfogadni, amiket ezektől fogva vissza tud fejteni
- A DO flag-gel jövő kéréseket a klienseknek AD bit-tel fogja megválaszolni

```
trusted-keys {
        "ripe.net.net." 256 3 1 AwEAAa9iBXsfILIS4d0A/wXPAIFst2Ma6F78Bf0bu8jmHgmZNwpbw6x0j/kLtFD65zl
        };
```

Segédeszközök

- `Net::DNS::SEC`
  - Perl modul, amivel dnssec tudású alkalmazások írhatók
- `ldns`
  - Library, c programok számára amivel dnssec tudású alkalmazások írhatók
  - Az nlnetlabs terméke
  - Lásd ldns-walk
- drill
  - dig-hez hasonló segédeszköz, DNSSEC nézegetésre
  - Ez is az nlnetlabs terméke
  - ldns-en alapul

Példa drill használatra

```
  $drill -T -t ns -k ~/dnssec/keys/Kripe.net.+005+00811.key  ris.ripe.net

;; Domain: .
;; No DNSKEY record found for .
;; No DS for net.
;; Domain: net.
;; No DNSKEY record found for net.
;; No DS for ripe.net.
;; Domain: ripe.net.
[T] ripe.net. 3600 IN DNSKEY 256 3 5 ;{id = 64728 (zsk), size = 1216b}
ripe.net. 3600 IN DNSKEY 256 3 5 ;{id = 1725 (zsk), size = 1216b}
ripe.net. 3600 IN DNSKEY 257 3 5 ;{id = 21238 (ksk), size = 2064b}
ripe.net. 3600 IN DNSKEY 257 3 5 ;{id = 811 (ksk), size = 2064b}
[T] ris.ripe.net. 0 IN DS 25861 5 1 4c856668a2dfe12981ae7f61fbb873a97bfe52cc
;; Domain: ris.ripe.net.
[T] ris.ripe.net. 3600 IN DNSKEY 256 3 5 ;{id = 20613 (zsk), size = 1216b}
ris.ripe.net. 3600 IN DNSKEY 256 3 5 ;{id = 20103 (zsk), size = 1216b}
ris.ripe.net. 3600 IN DNSKEY 257 3 5 ;{id = 25861 (ksk), size = 2064b}
ris.ripe.net. 3600 IN DNSKEY 257 3 5 ;{id = 21022 (ksk), size = 2064b}
[T] ris.ripe.net.      1800    IN      NS      sec1.apnic.net.
ris.ripe.net.  1800    IN      NS      ns-pri.ripe.net.

;;[S] self sig OK; [B] bogus; [T] trusted
```

Források

- dnssec-deployment.org
- dnssec.[net|org|com]
- dnssec-tools.org