DNSSEC

Ochrana proti vyčtení obsahu zóny

Jan Včelák • jan.vcelak@nic.cz • 31. května 2016

CZ.NIC | SPRÁVCE DOMÉNY CZ

DNSSEC

- Autentizace a integrita zónových dat
- RFC 4033, 4034, 4035
- Používá kryptografii veřejným klíčem
- Navrženo pro offline podepisování

- Nové typy záznamů:
  - `DNSKEY` – data veřejného klíče
  - `RRSIG` – podpis záznamu
  - `DS` – otisk klíče delegované zóny
  - `NSEC` – ukazatel na další záznam

Podepisování záznamů (1)

```
example.org.          MX    10 mail.example.org.

example.org.          AAAA  2001:db8::1

www.example.org.      AAAA  2001:db8:100:1
                      AAAA  2001:db8:200:1

mail.example.org.     AAAA  2001:db8::2
```

Podepisování záznamů (2)

```
example.org.          MX    10 mail.example.org.
                      RRSIG MX …
example.org.          AAAA  2001:db8::1
                      RRSIG AAAA …
www.example.org.      AAAA  2001:db8:100:1
                      AAAA  2001:db8:200:1
                      RRSIG AAAA …
mail.example.org.     AAAA  2001:db8::2
                      RRSIG AAAA …
```

```
example.org. RRSIG MX 13 2 60 20160613114720 20160530114720
             11685 example.org.
             0c980nNguC8rT/+CRqtLS37OGIe8nl7a6DpqLa8VW4xK
             VlBP/MtdTBB9ANs9urh6LcmVvypODBbxJVr8aIOt8Q==
```

Popření existence jména

1. Vezmeme všechna jména v zóně:

   `example.org  www.example.org  mail.example.org`

2. Vypočítáme hash každého jména:

   ```
   H(example.org)      = jgo6vjps28
   H(www.example.org)  = i7kgftt9rd
   H(mail.example.org) = p1cgc8lh6p
   ```

3. Seřadíme hashe:

   `i7kgftt9rd` → `jgo6vjps28` → `p1cgc8lh6p`

4. Vytvoříme „NSEC“ záznam pro každou po sobě jdoucí dvojici hashů:

   ```
   NSEC: i7kgftt9rd → jgo6vjps28
   NSEC: jgo6vjps28 → p1cgc8lh6p
   NSEC: p1cgc8lh6p → i7kgftt9rd
   ```

Popření existence jména s NSEC

- Nehashuje jména v zóně
- Seřazená jména:

  `example.org` → `mail.example.org` → `www.example.org`

- Vytvořené NSEC záznamy:

```
example.org.        NSEC  mail.example.org. …
mail.example.org.   NSEC  www.example.org. …
www.example.org.    NSEC  example.org. …
```

- Dotaz na neexistující jméno:

```
$ kdig +dnssec jabber.example.org
;; ->>HEADER<<- opcode: QUERY; status: NXDOMAIN; id: 17418
example.org.  NSEC   mail.example.org. …
example.org.  RRSIG  NSEC 13 2 60 20160613114720 …
```

Vyčtení obsahu zóny s NSEC

- „Zranitelnost“, kterou zavádí DNSSEC
- Pro každé jméno v zóně stačí jeden dotaz na server:

1. `$ kdig +short example.com NSEC`

   `mail.example.org.` `NS SOA MX AAAA RRSIG NSEC DNSKEY`
2. `$ kdig +short mail.example.com NSEC`

   `www.example.org.` `AAAA RRSIG NSEC`
3. `$ kdig +short www.example.com NSEC`

   `example.org.` `AAAA RRSIG NSEC`

Popření existence jména s NSEC3 (1)

- RFC 5155
- Alternativa NSEC (nikoli náhrada)
- Jména jsou hashována funkcí SHA-1
- Volitelně sůl, volitelné více iterací
- Nové typy záznamů:
  - `NSEC3` – náhrada NSEC používající hashovaná jména
  - `NSEC3PARAM` – parametry pro hashování

Popření existence jména s NSEC3 (2)

- Parametry pro hashování:

  `example.org.  NSEC3PARAM  1 0 10 C01DCAFE`

- Hashe jmen v zóně:

  `example.org` → `JGO6VJPS28F77L9B92O0MHJTRRJTAJBD`

  `www.example.org` → `I7KGFTT9RDLD87MK004U761N0GDPUP8B`

  `mail.example.org` → `P1CGC8LH6P81PEEUOBR7G4BFBCFLU4AM`

- Výsledný NSEC3 řetěz:

```
I7KGFTT9.example.org. NSEC3 1 0 10 C01DCAFE JGO6VJPS …
JGO6VJPS.example.org. NSEC3 1 0 10 C01DCAFE P1CGC8LH …
P1CGC8LH.example.org. NSEC3 1 0 10 C01DCAFE I7KGFTT9 …
```

Popření existence jména s NSEC3 (3)

- Dotaz na neexistující jméno:

```
$ kdig +dnssec jabber.example.org
;; ->>HEADER<<- opcode: QUERY; status: NXDOMAIN; id: 18949
p1cgc8lh….example.org. NSEC3 1 0 10 C01DCAFE I7KGFTT9…
p1cgc8lh….example.org. RRSIG NSEC3 13 3 60 20160613183207…
```

- Výpočet hashe dotazovaného jména:

```
$ knsec3hash c01dcafe 1 10 jabber.example.org
75O1MHAPQLNKL6J5R5JFBI7FQ3CCUQRT
```

Vyčtení obsahu zóny s NSEC3

- Výčet zóny je náročnější než u NSEC, ale pořád možný
- Offline útok pomocí slovníku nebo hrubou silou
- Wander, M., Schwittmann, L., Boelmann, C., and T. Weis, *GPU-Based NSEC3 Hash Breaking*, in IEEE Symp. Network Computing and Applications (NCA), 2014.
- Bernstein, D., *Nsec3 walker*, 2011, http://dnscurve.org/nsec3walker.html.

```
$ collect example.org > example.org.collect
$ unhash < example.org.collect
p1cgc8lh… mail.example.org.
found 1 names (33%) using 229919 hash computations
i7kgftt9… www.example.org.
found 2 names (66%) using 575464 hash computations
…
```

Popření existence jména s NSEC5 (1)

- Pouze návrh, https://datatracker.ietf.org/doc/draft-vcelak-nsec5/
- Použití „hashovací funkce s veřejným klíčem“:
  - EC VRF (Verifiable Random Function), křivky secp256r1 a Ed25519
  - RSA FDH (Full Domain Hash)
- Nové typy záznamů:
  - NSEC5KEY – veřejný klíč pro ověření NSEC5 hashů
  - NSEC5PROOF – důkaz správnosti hashe, syntetizován za běhu
  - NSEC5 – ekvivalent NSEC a NSEC3

Popření existence jména s NSEC5 (2)

- Dotaz na neexistující jméno:

```
$ kdig +dnssec jabber.example.org
;; ->>HEADER<<- opcode: QUERY; status: NXDOMAIN; id: 3123
jabber.example.org.   NSEC5PROOF 13893 mRXmnCOlChdrcrNca…
rv053a7j….example.org NSEC5 13893 0 VA8VPGO2…
rv053a7j….example.org RRSIG NSEC5 13 3 60 20160613183207 …
```

- Ověření hashe:

```
$ kdig +dnssec example.org NSEC5KEY > nsec5key
$ nsec5hash nsec5key jabber.example.org mRXmnCOlChdrcrNca…
T58GPMS0I3556B2FCB7DILID2N51B9UI5R5JFBI7FQ3CCUQRTA8V
```

- Vyčtení zóny je stejně náročné, jako bez DNSSEC

Popření existence s online podepisováním (1)

- Myšlenka: Vymýšlet si NSEC/NSEC3 a podepisovat je za běhu
- Podepisovací klíč musí být na všech serverech
- RFC 7129 (informační):
  - Minimally Covering NSEC Records
  - NSEC3 White Lies
- https://datatracker.ietf.org/doc/draft-valsorda-dnsop-black-lies/:
  - Compact DNSSEC Denial of Existence (Black Lies)

- Knot DNS používá v modulu pro online podepisování metodu Black Lies

Popření existence s online podepisováním (2)

- Minimally Covering NSEC:

```
$ kdig +dnssec jabber.example.org
;; ->>HEADER<<- opcode: QUERY; status: NXDOMAIN; id: 27146
jabbeq\255…\255.example.org NSEC \000.jabber.example.org …
```

- NSEC3 White Lies:

```
$ kdig +dnssec jabber.example.org
;; ->>HEADER<<- opcode: QUERY; status: NXDOMAIN; id: 11204
aods75b3…3kd.example.org  NSEC3 1 0 - AODS75B3…3KF …
```

- Black Lies:

```
$ kdig +dnssec jabber.example.org
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 41805
jabber.example.org. NSEC \000.jabber.example.org …
```

Shrnutí

- DNSSEC umožňuje vyčíst obsah zóny. Vadí to?
- „Zranitelné“ metody:
  - NSEC
  - NSEC3
- „Bezpečné“ metody:
  - NSEC5
  - Minimally Covering NSEC
  - NSEC3 White Lies
  - Compact DNSSEC Denial of Existence (Black Lies)

Děkuji za pozornost!

Jan Včelák • jan.vcelak@nic.cz