DNSSEC

22. 4. 2010

Pavel Tuček
xtucek1@fi.muni.cz

Obsah

Co je DNS a co zajišťuje?

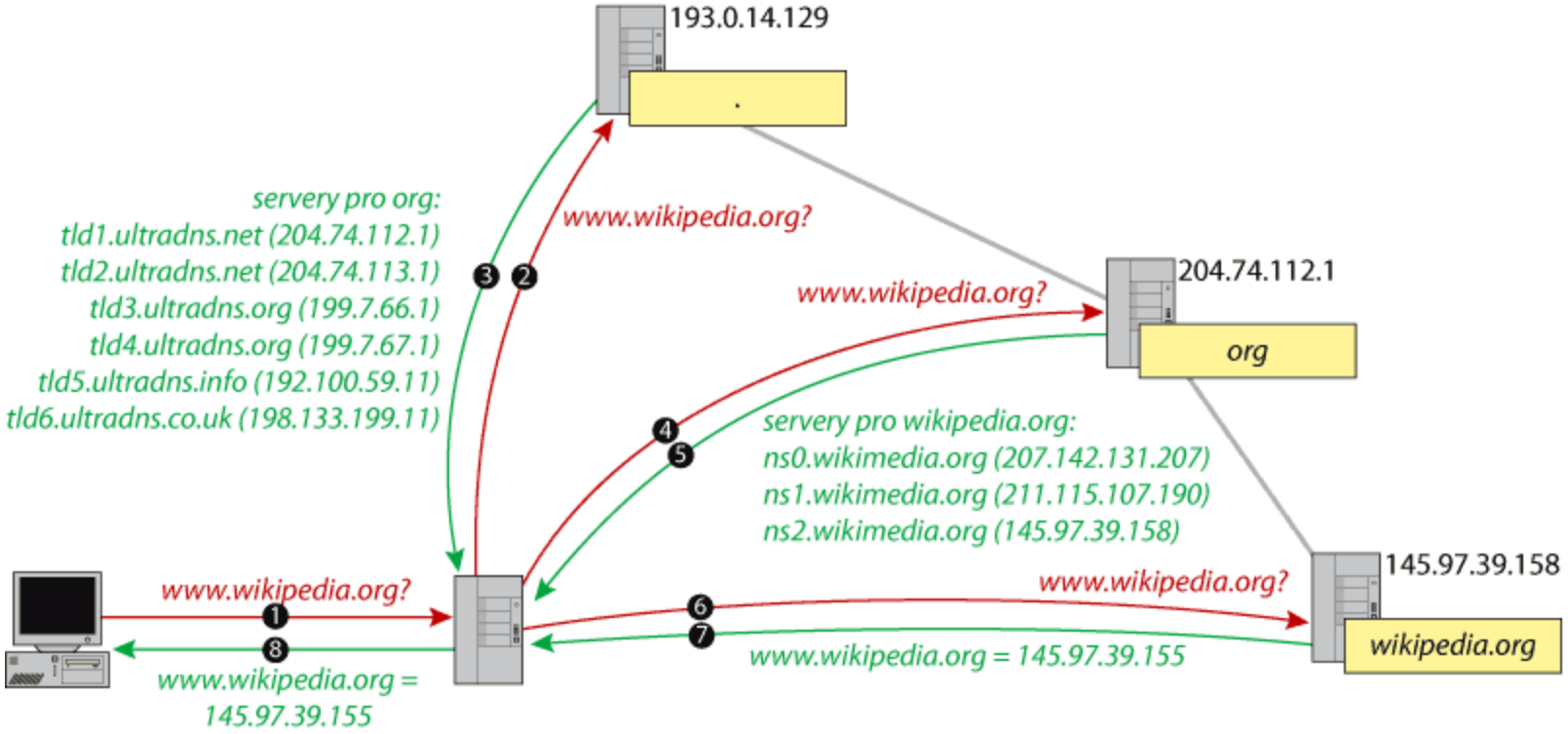
DNS = Domain Name System

Základní záznamy, se kterými se na DNS setkáváme (pro doménu ics.muni.cz):

- A záznam (**a**dress record)
  - `wsus IN A 147.251.12.110`
- AAAA záznam (IPv6 address record)
  - `wsus IN AAAA 2001:718:1c01:1:02e0:7dff:fe96:daa8` *(vymyšlená)*
- CNAME (**c**anonical **name** record)
  - `sus IN CNAME wsus`
- NS záznam (**n**ame **s**erver record)
  - `dior IN NS ns.ics.muni.cz`
    `IN NS ns1.ics.muni.cz.`
- PTR záznam (**p**oin**t**er record)
  - `10 IN PTR dior.ics.muni.cz.` *(v zóně 6.251.147.in-addr.arpa)*

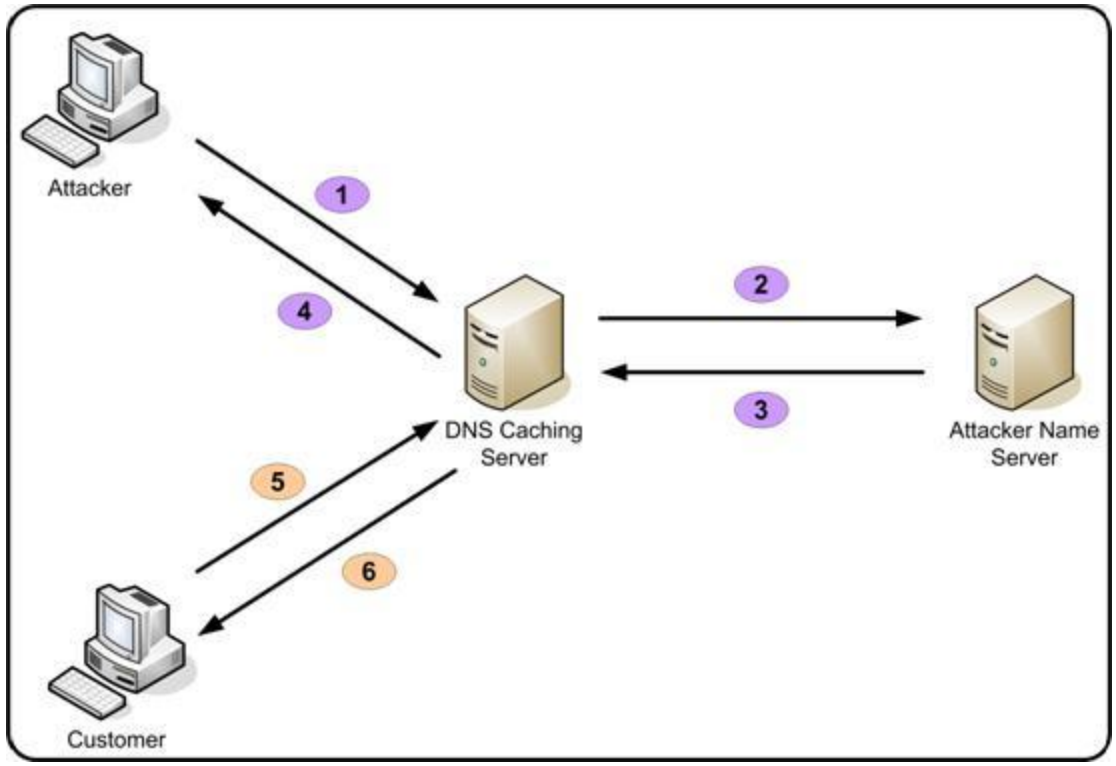
Z dalších záznamů známe: MX (**m**ail e**x**changer record), SOA (**s**tart **o**f **a**uthority record), SRV (**srv**ice record),...

Průběh dotazu www.wikipedia.org

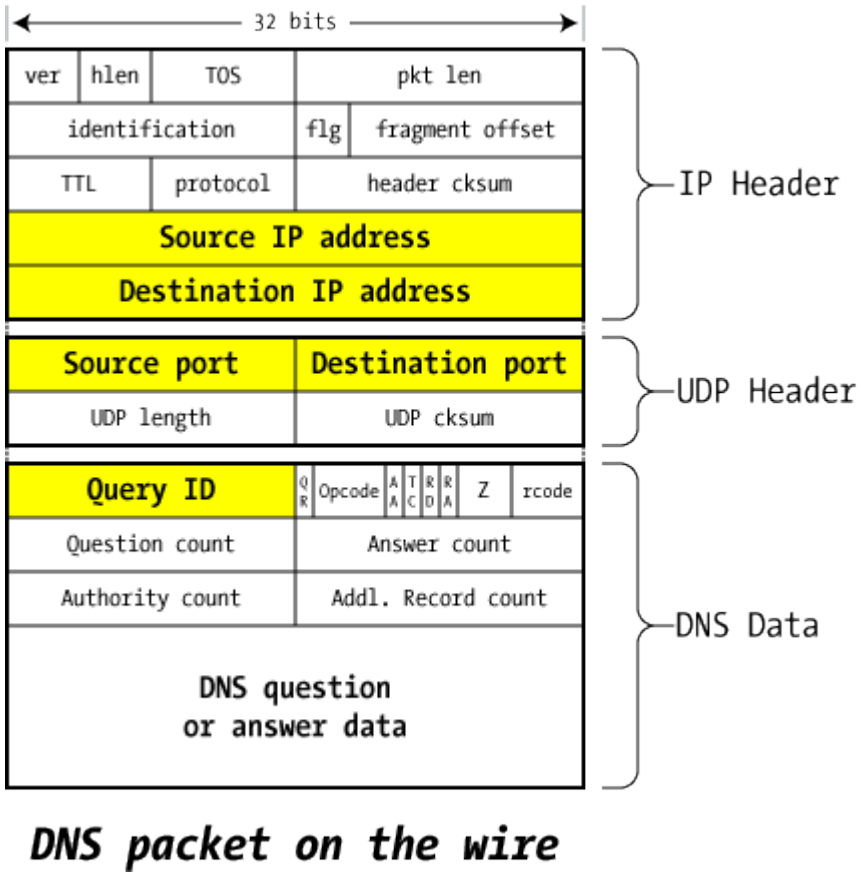


Co je za problém se současným DNS?

Na první problém upozornil již v roce 1990 Steven M. Bellovin a zatím poslední útok se nazývá DNS Cache poisoning – otrávení lokální cache DNS. Útok se objevil v polovině roku 2008 a jednalo se o největší problém DNS za celou jeho existenci.



Cache poisoning



DNS packet on the wire

Pole Query ID je dlouhé 16 bitů.

$2^{16} = 65536$

Co přináší DNSSEC

DNSSEC přináší rozšíření DNS o autentizovaný původ DNS odpovědí, autentizované popření existence a integritu dat. (RFC 4033-4035)

DNSSEC využívá infrastrukturu veřejných klíčů (PKI).

DNSSEC rozšiřuje současnou sadu záznamů o další čtyři:

- SIG záznam (**Sig**nature record)
  - `wsus IN SIG A 5 3 3600 20100501120000 20100401120000 (2539 ics.muni.cz Tjpdt...H6D)`

`5`	použitý algoritmus (RSA/SHA1)
`3`	počet domén ve jméně, které se podepisuje (kořenová se nepočítá)
`3600`	doba životnosti záznamu
`20100501120000`	doba ukončení platnosti záznamu
`20100401120000`	doba zahájení platnosti záznamu
`2539`	značka pro rychlejší nalezení klíče
`ics.muni.cz`	doménové jméno podepisujícího
`Tjpdt...H6D`	vlastní podpis (v kódování BASE64)

Co přináší DNSSEC

DNSSEC rozšiřuje současnou sadu záznamů o další čtyři:

- KEY záznam (**Key** record)
  - ```
    ics.muni.cz.
    IN   KEY   256 3 1 AQDv...GiDx
    IN   KEY   256 3 5 CLgC...Yb6n
    SIG KEY    1 2 3600 20100501120000 20100401120000 (2539 ics.muni.cz
    BH1x...7Wq3)
    ```

  První dvě položky (příznak a protokol) jsou pevně dané, následuje algoritmus, pro který se klíč používá a hodnota klíče (v BASE64). Můžeme tedy rozlišit klíč pro podepisování informací v doméně (zone signing key, ZSK) a klíč pro podepisování jiných klíčů (key signing key, KSK).

- DS záznam (**D**elegation **S**igner record)
  - ```
    muni.cz.   IN   DS   2539 1 1 239...1a9
    ```

  Záznam obsahuje značku klíče, algoritmus, pro který se klíč používá, typ otisku a otisk ověřující platnost klíče, ke kterému se vztahuje.

Co přináší DNSSEC

DNSSEC rozšiřuje současnou sadu záznamů o další čtyři:

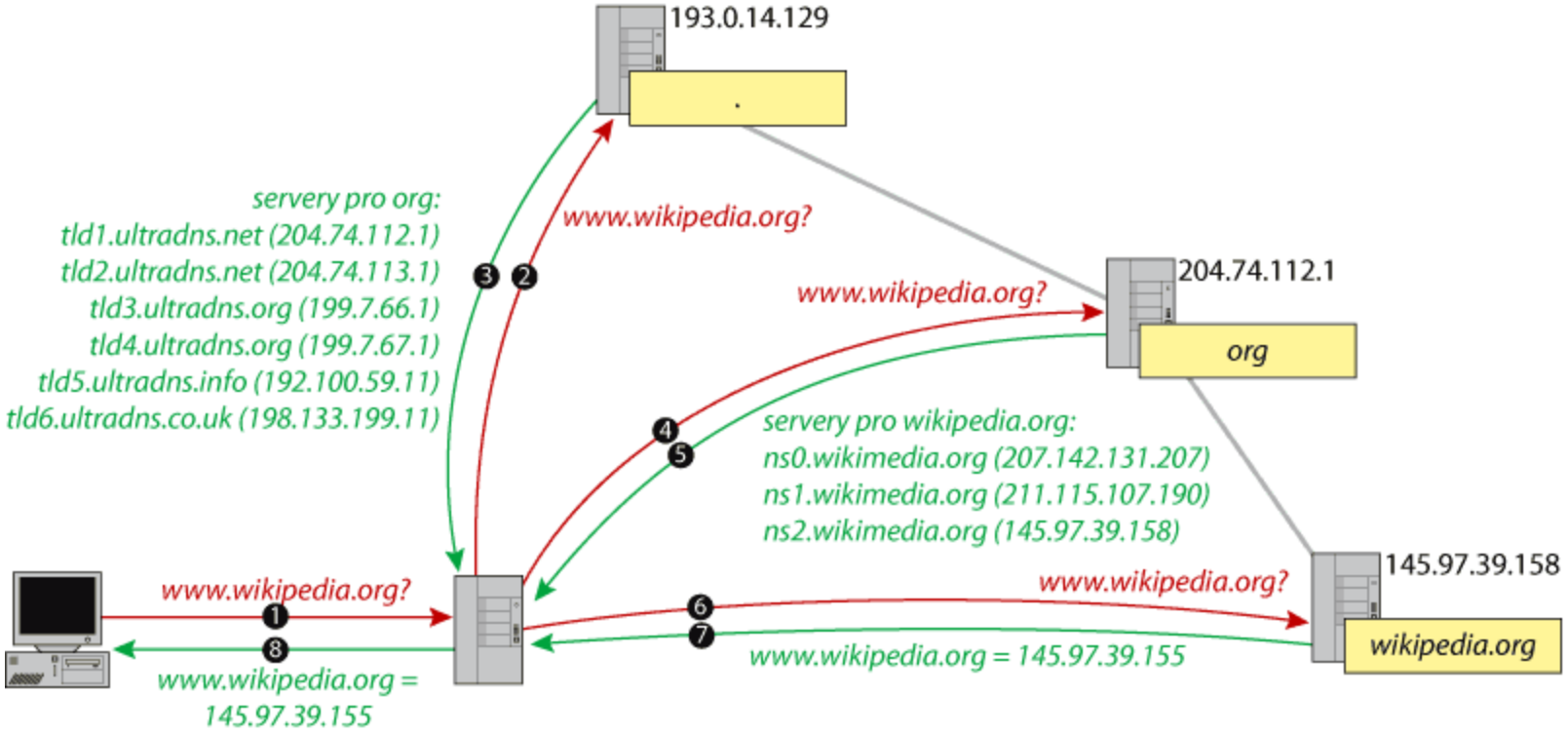
- NSEC záznam (**Next Sec**ured record)
  - `wsus IN NSEC www.ics.muni.cz. A NSEC SIG`
    `SIG NSEC 5 3 3600 20100501120000 20100401120000 (2539`
    `ics.muni.cz Tjpdt...H6D)`

  Obsahuje informaci o doménovém jménu, které následuje za aktuálním (u posledního pak odkazuje na první) a seznam typů záznamů definovaných pro aktuální jméno.

- NSEC3 záznam (**Next Sec**ured record) (RFC 5155)
  - `63ag+..fee IN NSEC iIo2...lOu A NSEC SIG`
    `SIG NSEC 5 3 3600 20100501120000 20100401120000`
    `(2539 ics.muni.cz Tjpdt...H6D)`

  Obsahuje hash doménového jména, které následuje za aktuálním (opět místo otevřeného záznamu obsahuje hash) a seznam typů záznamů definovaných pro aktuální jméno.

Překlad DNS jména a jeho ověření



Překlad DNS jména a jeho ověření

V našem případě by ověřování A záznamů pro www.wikipedia.org postupovalo následně:

1. klient získá A záznamy a SIG záznam pro www.wikipedia.org
2. k jeho ověření potřebuje ZSK domény wikipedia.org (KEY záznam a jeho SIG)
3. k jeho ověření potřebuje KSK domény wikipedia.org
4. k jeho ověření potřebuje DS záznam pro wikipedia.org, který je uložen v doméně org
5. k jeho ověření potřebuje ZSK domény org
6. k jeho ověření potřebuje KSK domény org
7. k jeho ověření potřebuje DS záznam pro org z kořenové domény
8. pro jeho ověření potřebuje ZSK kořenové domény
9. pro jeho ověření potřebuje KSK kořenové domény, který by se měl dozvědět jinou cestou (např. z konfiguračního souboru)

Rozšíření DNSSEC

První země, které přijaly DNSSEC:

- Brazílie,
- Bulharsko,
- Česká republika (2.),
- Puerto Rico
- a Švédsko (1.).

Začátkem roku 2010 přešli na DNSSEC dva velcí doménoví registrátoři Active 24 a WEB4U, takže počet zabezpečených domén .cz stoupl ze 1400 na 94 tisíc. ČR je v současné době světovou velmocí v rámci DNSSEC.

Zavedení DNSSEC v kořenové (root) úrovni DNS během roku 2010.

Dotazy?

Dotazy?

Zdroje informací

[1] RFC2535 - Domain Name System (DNS) Security Extensions
http://tools.ietf.org/html/rfc2535

[2] RFC4033 - DNS Security Introduction and Requirements
http://tools.ietf.org/html/rfc4033

[3] RFC4034 - Resource Records for the DNS Security Extensions
http://tools.ietf.org/html/rfc4034

[4] RFC4035 - Protocol Modifications for the DNS Security Extensions
http://tools.ietf.org/html/rfc4035

[5] RFC5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
http://tools.ietf.org/html/rfc5155

[6] Domain Name System Security Extensions; Wikipedia, The Free Encyclopedia
http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions