

DNSSEC pro běžného uživatele

Ondřej Caletka

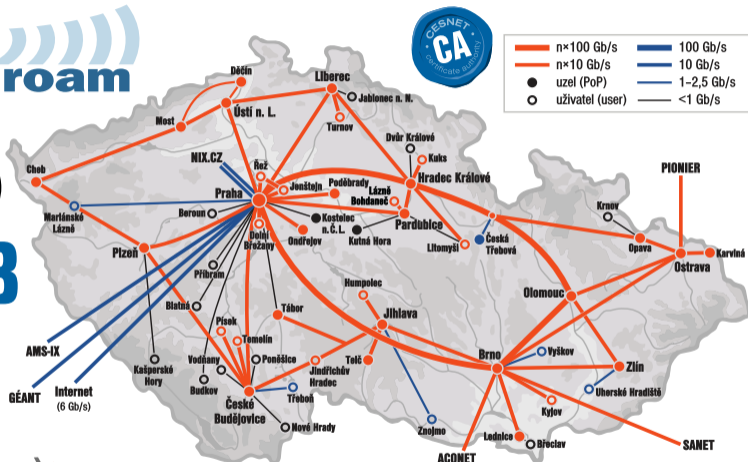


6. června 2015



Uvedené dílo podléhá licenci Creative Commons Uvedte autora 3.0 Česko.

O sdružení CESNET



Mezi uživateli je rozšířeno mnoho **polopravd, omylů a mýtů** o tom, jak funguje systém DNS a jeho rozšíření DNSSEC. Propadají pak mylnému dojmu, že DNSSEC nic neřeší a že se jím nemá cenu zabývat.

Opak je pravdou

- DNS je klíčovým prvkem architektury Internetu, jak ho známe
- na jeho bezchybné funkčnosti závisí všechny¹ internetové služby
- přitom je náchylný k *nedetekovatelné* manipulaci
- jediný úspěšný útok může unést celé části DNS stromu (třeba .com)
- šíření malwaru pomocí falešných domén se pravidelně objevuje
- DNSSEC **jedinou možností** jak manipulaci detekovat

¹Skype se nepočítá 😊

Příklady únosů DNS

DNSChanger

- trojský kůň pro Windows
- aktivní 2007 - 2011
- změnil nastavení rekurzivních DNS serverů v OS
- přidával reklamy do webových stránek

rom-0 exploit

- útok na levné domácí routery
- změna adresy rekurzivního DNS serveru v routeru
- náhrada populárních stránek za výzvu k upgradu Flash přehrávače

Oběť změny DNS



The screenshot shows a web browser window with the address bar containing `http://www.seznam.cz/`. The browser's menu bar includes "Soubor", "Nástroje", and "Nápověda". The page content features a dark header with the text "Home / Downloads / Flash Player Pro /" and a large white heading "Update Your Flash Player". Below this is a red square with a white "f" logo and the word "Pro" in the bottom right corner. To the right of the logo, the text "Please Update Your Flash Player (RECOMMENDED)" is displayed. A list of benefits follows, including downloading movies, watching 1080i HD video, faster playback in Firefox, Chrome, and Internet Explorer, and total privacy. At the bottom, there are two buttons: a yellow "Install" button and a grey "Remind me later" button.

http://www.seznam.cz/

Soubor Nástroje Nápověda

Home / Downloads / Flash Player Pro /

Update Your Flash Player



Please Update Your Flash Player (RECOMMENDED)

- Download any Movie, Video, TV shows From Any Website
- Watch any Video in Full 1080i HD
- Faster Playback and Streaming in Firefox, Chrome and Internet Explorer
- Total Privacy - Prevent Others From Tracking What You are Watching

Install **Remind me later**

Co je vlastně DNSSEC

- systém end-to-end zabezpečení autenticity DNS zpráv
- majitel domény podepisuje, kdokoli může validovat
- hierarchická delegace důvery
 - v nadřazené zóně je umístěn otisk klíče (DS záznam)
 - otisk klíče kořenové zóny je součástí výbavy každého validátoru
- i u nepodepsané domény probíhá validace nadřazených zón
 - až po podepsanou informaci, že další zóny podepsány nejsou

Součástí specifikace DNSSEC není **křišťálová koule**. Validátory manipulaci detekují, ale nejsou schopny zmanipulovaná data opravit.

Nejčastější příčiny nevalidních DNS dat:

- zastaralé verze rekurzivních DNS serverů
- nevhodné konfigurace firewallů
- captive portály
- chyba na straně držitele domény

Máme přece TLS

- DNSSEC chrání pouze překlad doménového jména na IP adresu, proti odklonění IP provozu je neúčinný
- je tedy nezbytné používat TLS s DNSSECem
- správně implementované TLS dokáže detekovat i únos DNS
- PKI model má však vážné trhliny
- DNSSEC je nezávislý bezpečný kanál
- spolehlivě ochrání přinejmenším proti *vzdálenému* útočníkovi

DNSSEC + TLS = DANE

- důvěryhodnost TLS spojení je dnes výlučně závislá na soustavě certifikačních autorit
- DNSSEC je důvěryhodný nezávislý kanál, kterým může majitel domény publikovat různé informace
- TLSA záznamy umožňují publikovat otisky TLS certifikátů
- výhledově nahradí *Domain Control Validated* TLS certifikáty

Jak validovat

Validace v prohlížeči

- rozšíření DNSSEC a TLSA validátor
- obsahuje kompletní DNSSEC resolver
- kontroluje, zda se prohlížeč připojuje na správnou adresu
- nezasahuje do validace TLS spojení v prohlížeči



Validace na domácím routeru

- stačí aktuální BIND nebo Unbound
- konfigurace je obvykle připravena, stačí vložit klíč kořenové zóny
- režim plné rekurze nebo forwardování na nadřazený DNS server
 - problémy s chybami v nadřazených serverech znemožňující validaci některých jmen
 - režim plné rekurze špatně škáluje, vyžaduje nezasahování ISP do udp/53 provozu



- DNSSEC z principu nechrání před útokem na poslední míli mezi validátorem a konzumentem
- specifikace nařizuje bezpečný kanál
- jsou-li pochybnosti o bezpečnosti kanálu, je nutné kritická data znovu validovat
- validace na vzdáleném serveru hlavně chrání server před otrávením své vlastní cache

Resolver na loopbacku

- snadné pro pevné instalace, obtížné pro přenosná zařízení
 - filtrovaný DNS provoz
 - přesměrování DNS provozu na polofunkční server
 - *captive portály* blokující konektivitu do přihlášení
- experimentální DNSSEC Trigger
 - automatizovaně otestuje použitelnost místního resolveru
 - podle výsledku nastaví lokální unbound na forwardování nebo plnou rekurzi
 - hot spot režim pro přihlášení ke captive portálům
 - nouzové tunelování DNS přes TLS portem tcp/443

Problém řetězení resolverů s DNSSEC

- problematická validace žolíkových domén
- chyba v nadřazeném BIND < 9. 9. 0
- automatizovaný test na <http://wildcarddnssec.jdem.cz/>

Test		Výsledek testu
1.	Zabezpečení DNSSEC *. wilda. rhybar. 0skar. cz	Úspěch. Nedostanete se na doménová jména s neplatným podpisem.
2a.	NSEC zóna s A záznamem *. wilda. nsec. 0skar. cz	Neúspěch. Váš DNS server nedokáže správně validovat A záznam, který vznikl expanzí žolíkového znaku na zóně s NSEC.
2b.	NSEC zóna s CNAME záznamem *. wild. nsec. 0skar. cz	Neúspěch. Váš DNS server nedokáže správně validovat CNAME záznam, který vznikl expanzí žolíkového znaku na zóně s NSEC.
3a.	NSEC3 zóna s A záznamem *. wilda. 0skar. cz	Neúspěch. Váš DNS server nedokáže správně validovat A záznam, který vznikl expanzí žolíkového znaku na zóně s NSEC3.
3b.	NSEC3 zóna s CNAME záznamem *. wild. 0skar. cz	Neúspěch. Váš DNS server nedokáže správně validovat CNAME záznam, který vznikl expanzí žolíkového znaku na zóně s NSEC3.
4.	NSEC s extra záznamem uvnitř žolíku www. wilda. nsec. 0skar. cz	Úspěch. Váš DNS server správně validuje CNAME záznam, obklopený žolíkovými A záznamy na zóně s NSEC.
5.	NSEC3 s extra záznamem uvnitř žolíku www. wilda. 0skar. cz	Úspěch. Váš DNS server správně validuje CNAME záznam, obklopený žolíkovými A záznamy na zóně s NSEC3.

Když něco nefunguje

- selhání validace server signalizuje návratovým kódem SERVFAIL
 - nelze odlišit o ostatních příčin selhání
 - pomocí `dig +cdflag` lze provést dotaz s vypnutou validací
- detailní analýza pomocí `unbound-host`

```
$ unbound-host -C /etc/unbound/unbound.conf \  
rhybar.cz
```

```
...
```

```
validation failure <rhybar.cz. A IN>: no keys  
have a DS with algorithm RSASHA1 from  
2001:718::53 for key rhybar.cz. while building  
chain of trust
```

Když je problém u zdroje

DNSCheck

Test domény Test nedelegované domény + FAQ

Otestujte DNS-server a najdete chyby

Název domény: ces.net
Vložte název domény pro otestování, například "ic.cz"

Testovat

V testu se vyskytují chyby
ces.net, 2013-09-26 02:04:26
Test byl proveden nástrojem DNSCheck verze 4.0

Souhrnné výsledky Detailní výsledky

- Delegace
- DNS server
 - DNS server decsys.vsb.cz
 - DNS SERVFAIL při dotazování 158.196.149.9 na SOA
 - Ďnejný server decsys.vsb.cz (158.196.149.9) neodpovídá na dotazy přes TCP
 - DNS SERVFAIL při dotazování 2001.718.1001.149.0.0.0.9 na SOA
 - Ďnejný server decsys.vsb.cz (2001.718.1001.149.0.0.0.9) neodpovídá na dotazy přes TCP
 - DNS server nsa.ces.net
 - DNS server nsa.cesnet.cz
- Konzistence
- SOA
- Konektivita
- DNSSEC

Historie testů

- 2013-09-26 02:04:26

Vysvětlení

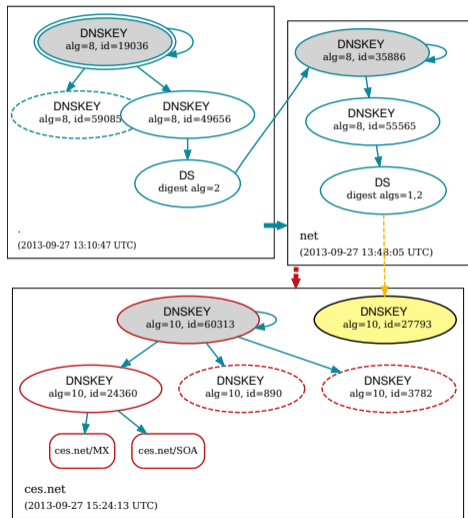
- Test je v pořádku
- Test obsahuje varování
- Test obsahuje chyby
- Test se nezaukateřil

Odkaz na tento test:
<http://dnscheck.labs.nic.cz/?time=1364259866&id=42686&view=basic&test=standard>

DNSCheck (v.4.0) plat P 2001.718.1.6. 134.136

Výběr jazyka: Cesky

CZ NIC SPRÁVCE DOMÉNY CZ



- DNSSEC je **zralá** technologie se **zcela novým** modelem důvěry
- aktivní validace do jisté míry **chrání i nepodepsané subdomény**
- manipulací s provozem **nelze** přesvědčit validátor, že daná zóna není podepsaná
- rozšíření pro validaci v prohlížeči pomůže odhalit zfušovaný internet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
<http://Ondrej.Caletka.cz>

