

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 5911

Demonstracija rada protokola DNSSEC u sustavu IMUNES

Dubravko Lukačević

Zagreb, svibanj 2019.

*Umjesto ove stranice umetnite izvornik Vašeg rada.
Da bi ste uklonili ovu stranicu obrišite naredbu \izvornik.*

SADRŽAJ

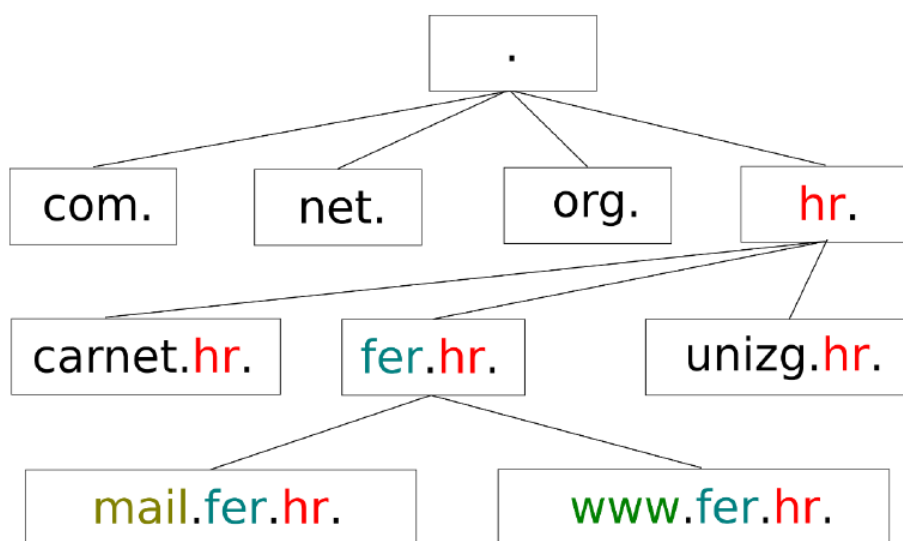
1. Uvod	1
2. Sigurnosni problemi DNS-a	3
2.1. Registracija sličnih domena	3
2.2. Lažiranje DNS odgovora	3
2.3. Trovanje DNS međuspremnik	4
3. Način rada DNSSEC-a	5
4. Uspostava DNSSEC-a	7
5. Zaključak	8

1. Uvod

Domenski sustav imena (engl. Domain Name System, kratica DNS) je sustav koji prevodi IP-adrese u simbolička imena, što nam omogućuje da lakše zapamtimo adresu neke stranice jer pamtimo smisleno simboličko ime umjesto numeričke IP-adrese. Zbog toga se za DNS često kaže da je "telefonski imenik" Interneta.

"DNS je hijerarhijski i decentralizirani sustav. Imena koja DNS prevodi u pravilu su sastavljena od više dijelova te, za razliku od IP-adresa, ti dijelovi imaju hijerarhijsko značenje. Primjerice, ime mail.fer.hr. sastoji se od tri dijela – mail, fer i hr. S desna na lijevo – hr označava Hrvatsku, fer označava Fakultet Elektrotehnike i Računarstva (FER) u Hrvatskoj, a mail označava poslužiteljsko računalo zaduženo za elektroničku poštu na FER-u." [1] Krajnji desni dio domenskog imena naziva se vršna domena ili TLD (eng. top-level domain), u ovom slučaju to je vršna domena hr. Sve domene u domenskom imenu koje su lijevo od TLD-a predstavljaju poddomene, pri čemu je najviše moguće 127 razina poddomena. Vrh hijerarhije DNS-a označava se točkom i naziva se korijenom DNS-a jer hijerarhija ima strukturu stabla. Primjer DNS hijerarhije prikazan je na Slici 1.1. "Za hrvatsku vršnu domenu .hr zadužen je poslužitelj dns.srce.hr kojim upravlja HR-DNS služba za CARNet." [2]

Problem nastaje kada gledamo sigurnost DNS-a, naime DNS je ostao nepromijenjen od ranih 1980-ih kada je osmišljen pa je normalno da sada postoje neke sigurnosne prijetnje. Jedan od glavnih problema je taj što DNS za slanje poruka koristi nepouzdanu uslugu UDP protokola, čije se poruke mogu lako lažirati. Upravo zbog toga nastalo je sigurnosno proširenje za DNS (enlg. DNS Security Extension, kratica DNSSEC).



Slika 1.1: Primjer DNS hijerarhije, izvor [2]

DNSSEC je sigurnosna nadogradnja DNS protokola koja osigurava autentičnost i integritet DNS odgovora koristeći digitalni potpis koji je baziran na kriptografiji javnog ključa, o čemu će biti više govora kasnije u ovom radu. Razvoj DNSSEC-a započeo je 1993. godine, korijenska domena potpisana je 15.7.2010. godine, a u vrijeme pisanja ovog rada (prva polovica 2019. godine) još uvijek nisu potpisane sve domene.

2. Sigurnosni problemi DNS-a

Kao što je već spomenuto, DNS je relativno star protokol i nije imao nikakve sigurnosne nadogradnje otkako je osmišljen pa su se pojavili sigurnosni problemi i u ovom poglavlju ukratko su opisani neki od njih kako bi se stekao dojam koliko su ti problemi ozbiljni i što točno sprječava DNSSEC, odnosno zašto nam je potreban.

2.1. Registracija sličnih domena

Kao jedan od čestih problema DNS-a javlja se registracija sličnih domena u svrhu prijevara, a najčešća meta za kriminalce su sustavi koji imaju veze s novcem. Prijevara se odvija tako da kriminalci registriraju domenu sličnog imena (npr. paypal umjesto paypal), postavljaju jednak izgled stranice kao original i čekaju da nepažljivi korisnici ostave svoje podatke na njihovoj stranici.

Jedini način pravovremene zaštite jest da, kako bi zaštitile svoje korisnike, organizacije preventivno registriraju sve slične domene.

2.2. Lažiranje DNS odgovora

DNS promet nije zaštićen i zbog toga se javlja sljedeći sigurnosni problem, odnosno skup problema kojima je zajedničko da na kraju korisnik dobije lažnu informaciju u DNS odgovoru jer je DNS upit ili odgovor u nekom trenutku presretnut u izmijenjen. Nadalje zbog korištenja nesigurnog UDP transportnog protokola napadaču omogućuje da lažira otkud poruka dolazi, a kao posljedica toga ako napadač zna kako izgleda DNS odgovor, može ga lažirati i ukoliko lažni odgovor stigne prije pravog, žrtva će prihvatiti taj lažni odgovor.

2.3. Trovanje DNS međuspremnik

Ovaj napad se izvodi nakon napada opisanog u prethodnom potpoglavlju i predstavlja jako ozbiljnu sigurnosnu prijetnju DNS sustavu. Kada se napadač ubaci u komunikaciju tokom DNS prevođenja on može odgovarati na upite umjesto DNS poslužitelja kojem je upit zapravo upućen te se odgovori koje napadač pošalje spremaju u DNS međuspremnik. Zbog toga će svi sljedeći isti upiti od poslužitelja dobiti lažan odgovor koji je spremljen u međuspremniku. Očito je da spremanjem samo jednog lažnog odgovora u međuspremnik na DNS poslužitelju kojeg koristi velik broj klijenata može biti prevaren velik broj ljudi.

3. Način rada DNSSEC-a

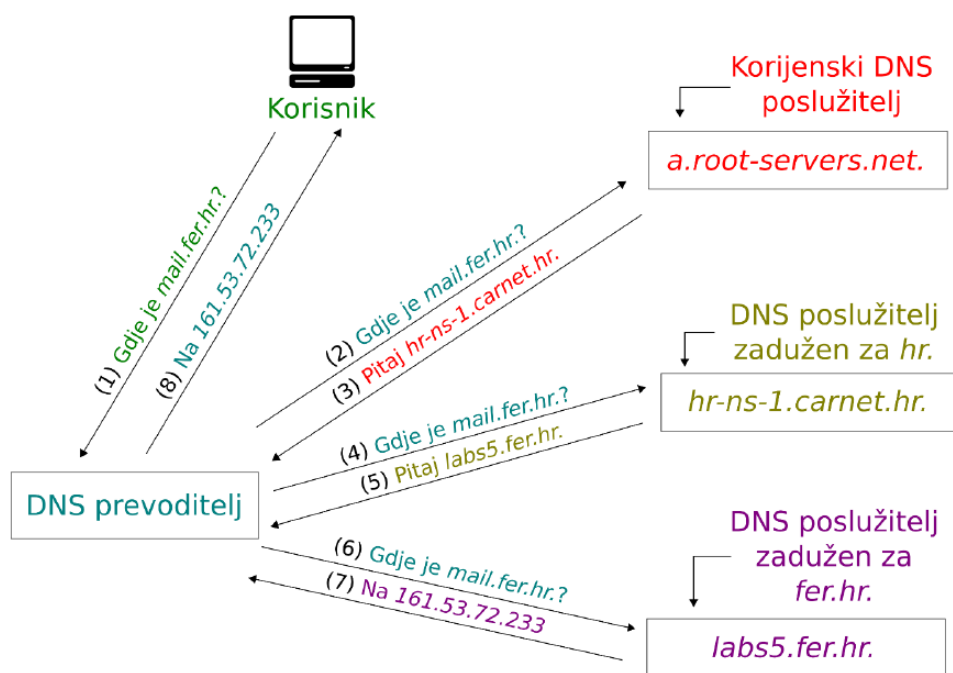
DNS sustav sastoji se od tri glavna dijela, a to su:

1. DNS klijent - nalazi se na klijentskom računalu, šalje DNS zahtjev
2. rekurzivni DNS poslužitelj - poslužitelj koji za zadani upit obavlja pretraživanje i vraća odgovor natrag klijentu
3. autoritativni DNS poslužitelj - poslužitelj koji odgovara na upite rekurzivnog poslužitelja tako što mu vrati konačan odgovor na upit ili referencu na neki drugi autoritativni DNS poslužitelj

Slika 3.1 ilustrira DNS prevođenje za slučaj kada klijent DNS prevoditelju pošalje upit za mail.fer.hr. Kada DNS poslužitelj dobije odgovor na traženi upit, taj odgovor se sprema u DNS međuspremnik kako bi drugim korisnicima koji pošalju isti upit mogao odgovoriti bez ponavljanja cijelog postupka prevođenja. Također zapis se nakon nekog vremena briše iz DNS međuspreminka kako ne bi došlo do zastarjevanja.

DNSSEC nije novi protokol, već samo uvodi sljedećih šest novih vrsta zapisa resursa:

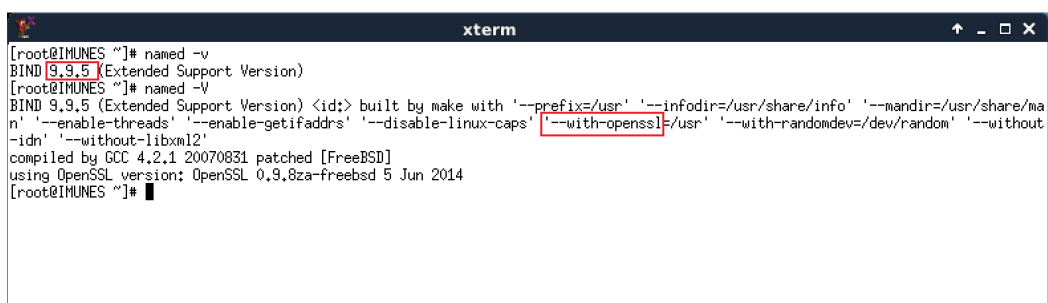
1. RRSIG - digitalni potpis
2. DNSKEY - javni ključ
3. DS - parent-child
4. NSEC - dokaz nepostojanja
5. NSEC3 - dokaz nepostojanja
6. NSEC3PARAM - dokaz nepostojanja



Slika 3.1: DNS prevođenje, izvor [1]

4. Uspostava DNSSEC-a

Za početak potrebna nam je 9.9 ili novija inačica BIND-a koju imamo već instaliranu kada preuzmemo i pokrenemo pripremljeni paket IMUNES-a za rad u virtualnom okruženju (http://www.imunes.net/dl/IMUNES_security.ova), ali ako se želimo uvjeriti možemo to učiniti s naredbom "named -v". Sljedeća bitna stvar je da kada pokrenemo naredbu "named -V" provjerimo koje su zastavice već postavljene, ako je postavljena zastavica "--with-openssl" onda je DNSSEC podržan i spreman je za daljnji rad, a ako nije onda je neophodno da nadogradimo sustav na noviju inačicu.



```
[root@IMUNES ~]# named -v
BIND 9.9.5 (Extended Support Version)
[root@IMUNES ~]# named -V
BIND 9.9.5 (Extended Support Version) <id> built by make with '--prefix=/usr' '--infodir=/usr/share/info' '--mandir=/usr/share/man' '--enable-threads' '--enable-getifaddrs' '--disable-linux-caps' '--with-openssl=/usr' '--with-randomdev=/dev/random' '--without-idn' '--without-libxml2'
compiled by GCC 4.2.1 20070831 patched [FreeBSD]
using OpenSSL version: OpenSSL 0.9.8za-freebsd 5 Jun 2014
[root@IMUNES ~]#
```

Slika 4.1: Potrebna inačica i zastavice

Na sustavu koji podržava DNSSEC sljedeći korak je omogućiti DNSSEC validaciju, za to je potrebno dodati sljedeću liniju koda u konfiguracijsku datoteku DNS poslužitelja:

```
options { dnssec-validation auto; };
```

5. Zaključak

Zaključak.

Demonstracija rada protokola DNSSEC u sustavu IMUNES

Sažetak

Sažetak na hrvatskom jeziku.

Ključne riječi: Ključne riječi, odvojene zarezima.

Demonstration of DNSSEC protocol using IMUNES system

Abstract

Abstract.

Keywords: Keywords.