CARNET

DNSSEC

NCERT-PUBDOC-2017-11-347

CERT.hr

Sadržaj

Dokument je izradio Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

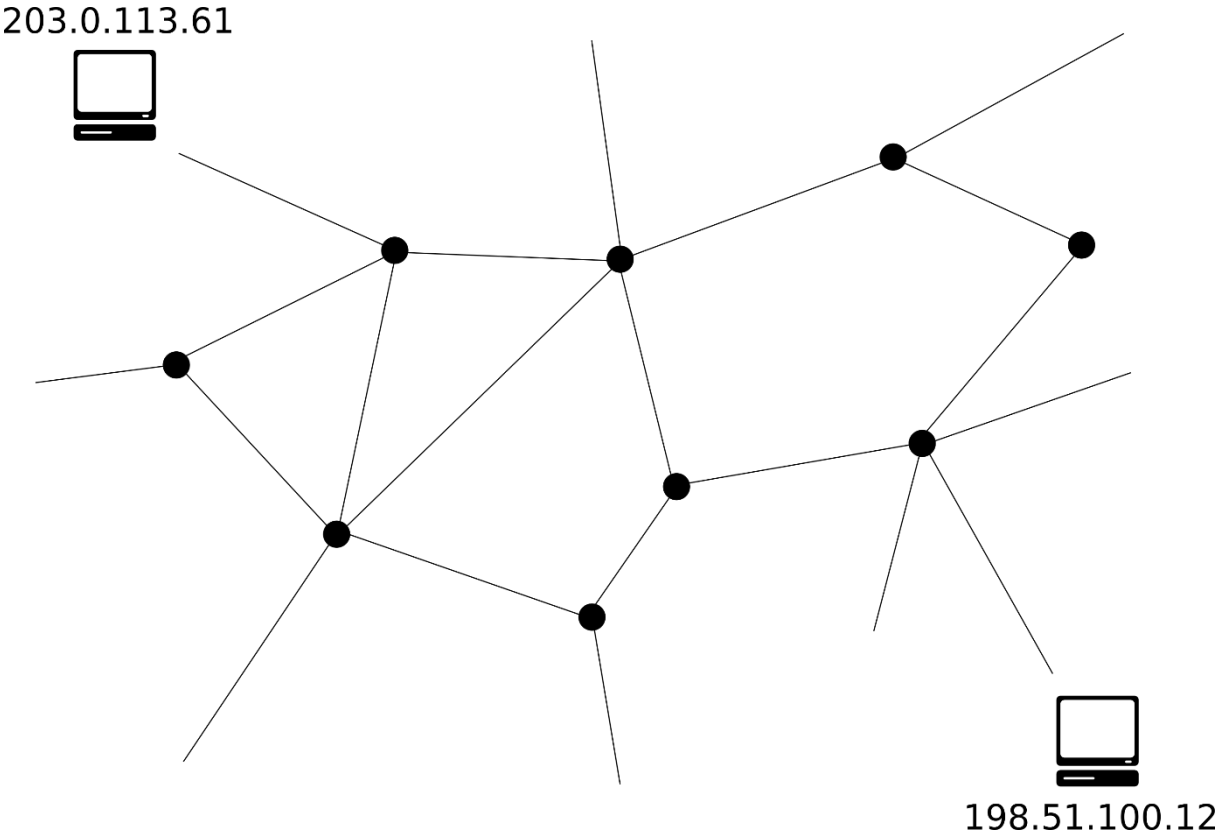
1 Uvod

DNSSEC je sigurnosna nadogradnja DNS protokola koja osigurava autentičnost i integritet DNS odgovora. Za razumijevanje DNSSEC-a preduvjet je osnovno razumijevanje Interneta, IP adresa i DNS-a. Stoga će uvodno biti objašnjeni ti pojmovi i mehanizmi.

1.1 Internet i IP adrese

Internet je **mreža povezanih računala i računalnih mreža**. Svako računalo uključeno u Internet mora imati jedinstvenu adresu, tzv. **IP (eng. *Internet Protocol*) adresu**. IP adrese računala nužne su za njihovu komunikaciju na Internetu, isto kao što su za slanje i primanje pošte nužne ulične adrese pošiljatelja i primatelja.

Za razliku od uličnih adresa, IP adrese su zapravo samo brojevi koje je moguće zapisati na različite načine – primjeri IP adresa u njihovom uobičajenom zapisu su 203.0.113.61 (za IP verziju 4) i 2001:db8:85a3::8a2e:370:7334 (za IP verziju 6). Slika 1 prikazuje dva računala spojena na Internet i njihove IP adrese (IP verzija 4).



Slika 1 - Primjer dva računala na Internetu i njihovih IP adresa

Za razliku od, primjerice, telefonskih brojeva koji imaju neku hijerarhiju (385 – Hrvatska, (0)1 – Zagreb, 61 centrala, daljnji brojevi – broj susjedstva, zgrade i korisničkog priključka…), **brojevi u IP adresama većinom nemaju značenje**. Rezultat toga je da, iako su IP adrese nužne za komunikaciju, one su ljudima izrazito **nepraktične za pamćenje**. Ono što je ljudima praktično za pamćenje su imena – primjerice *mail.fer.hr.*

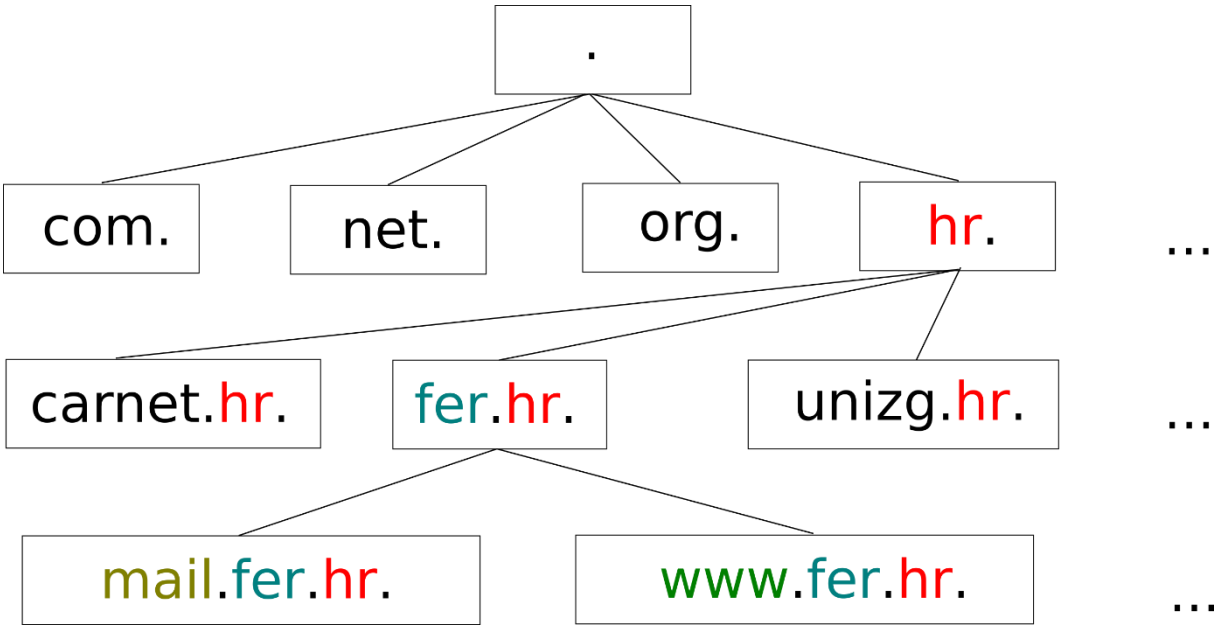
1.2 *Domain Name System* (DNS)

Kako se IP adrese ne bi morale pamtiti, rješenje je **DNS (eng. *Domain Name System*)** – sustav koji povezuje simbolička imena s IP adresama. Primjerice, pomoću DNS-a se ime *mail.fer.hr.* prevodi u IP adresu 161.53.72.233. Upravo zbog toga se DNS često naziva **„telefonskim imenikom" Interneta** – on osigurava da ljudi mogu pamtiti tzv. domenska imena (eng. *domain name*), a da zatim računalo ta imena automatski prevodi u IP adrese. Uz to, DNS može povezati domenska imena i s drugim informacijama, primjerice s proizvoljnim tekstualnim zapisima.

DNS je **hijerarhijski** i **decentralizirani** sustav. Imena koja DNS prevodiu 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.

Kontrola nad tim imenima također prati istu hijerarhiju. Organizacija zvana IANA (eng. *Internet Assigned Numbers Authority*) nalazi se na vrhu hijerarhije – ona je povjerila kontrolu nad *hr.* domenom (tj. nad imenima koja završavaju s *.hr.*) Hrvatskoj državi (tj. konkretnije CARNetu). Zatim, Hrvatska država (preko CARNeta) povjerava FER-u kontrolu nad *fer.hr.* domenom. FER onda može uređivati zapise u *fer.hr.* domeni, primjerice može reći da ime *mail.fer.hr.* odgovara IP adresi 161.53.72.233. Uz to, FER može nastaviti hijerarhiju tako da dalje povjeri kontrolu nad dijelovima domene – na primjer, FER može Zavodu za elektroničke sustave i obradbu informacija (ZESOI) povjeriti kontrolu nad domenom *zesoi.fer.hr.*

Slika 2 prikazuje DNS hijerarhiju kroz nekoliko domena. **Vrh hijerarhije** u DNS-u označava se točkom, i s obzirom na to da hijerarhija ima strukturu stabla, **naziva se korijenom DNS-a**.



Slika 2 - DNS hijerarhija

1.3 DNS prevođenje

Postupak pretvorbe domenskog imena u IP adresu (ili neki drugi DNS zapis) zove se **DNS prevođenje (eng. *DNS resolution* ili *DNS lookup*).**

Slika 3 prikazuje na primjeru kako se, u pravilu, provodi postupak prevođenja domenskog imena u IP adresu. Korisnička računala obično izravno komuniciraju **samo s DNS prevoditeljima**, strojevima koji zapravo **obavljaju glavni dio posla**. Iz perspektive korisničkog računala, ono samo pošalje upit DNS prevoditelju te zatim dobije odgovor. Ono što se zapravo odvija je sljedeće (opis prati sliku 3):

1. **Korisnik pošalje upit DNS prevoditelju** („Gdje je *mail.fer.hr.*?“).

2. **DNS prevoditelj pošalje taj isti upit jednom od korijenskih (vršnih) DNS poslužitelja** – poslužitelja koji se nalaze na vrhu hijerarhije („Gdje je *mail.fer.hr.*?“).

3. Korijenski DNS poslužitelj ne zna koja je točno adresa od *mail.fer.hr.*, ali zna da je za *hr.* domenu (tj. za sva imena koja završavaju s *.hr.*) zadužena Hrvatska država, tj. glavni hrvatski DNS poslužitelji. Zato, **korijenski DNS poslužitelj odgovara DNS prevoditelju imenom i adresom jednog od glavnih hrvatskih DNS poslužitelja**, i kaže mu da pita njega („Pitaj *hr-ns-1.carnet.hr.*“).

4. **DNS prevoditelj sada šaljeisti taj upit** poslužitelju na kojeg ga je korijenski DNS poslužitelj usmjerio, **jednom od glavnih hrvatskih DNS poslužitelja** („Gdje je *mail.fer.hr.*?“).

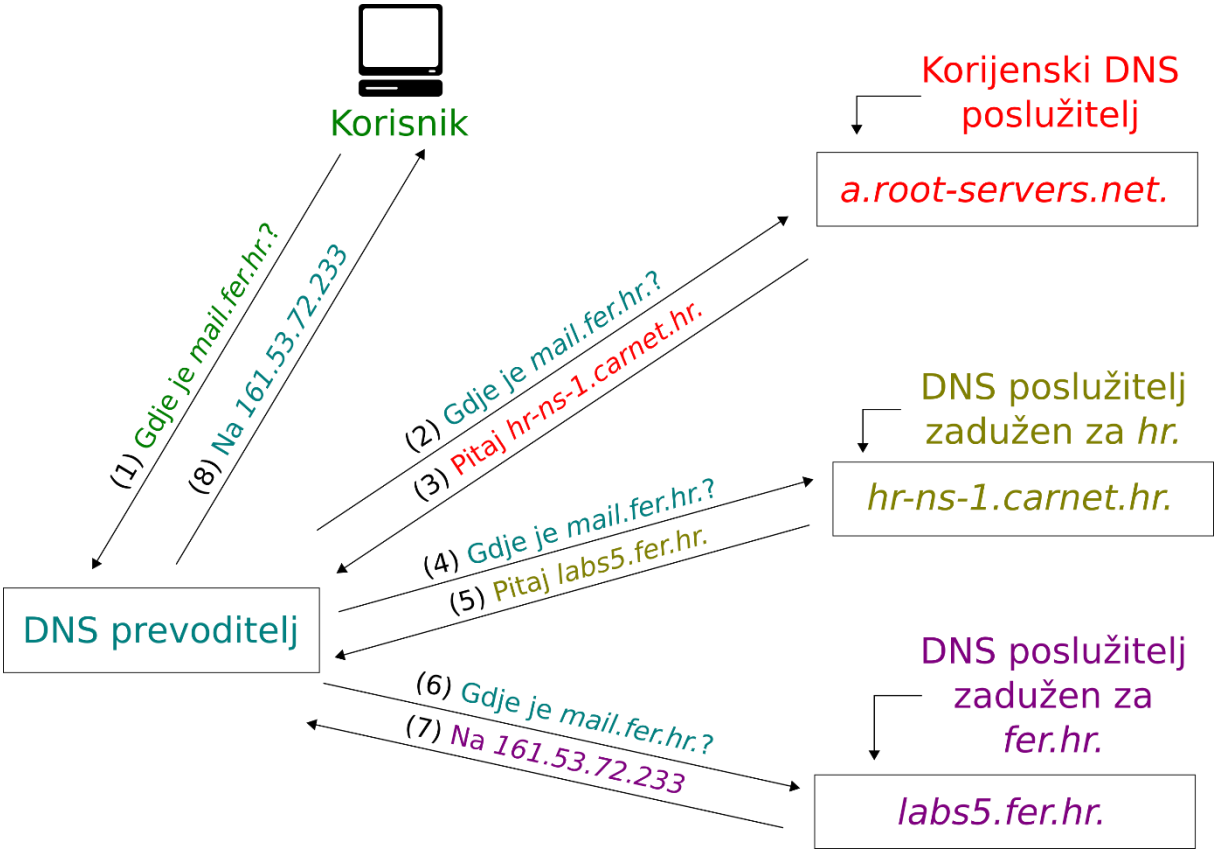
5. Ni glavni hrvatski DNS poslužitelj ne zna koja je točno adresa od *mail.fer.hr.*, već samo zna da je za *fer.hr.* domenu (tj. za sva imena koja završavaju s *fer.hr.*) zadužen Fakultet elektrotehnike i računarstva, tj. glavni DNS poslužitelji od FER-a. Zato, **glavni hrvatski DNS poslužitelj odgovara DNS prevoditelju imenom i adresom jednoga od glavnih FER-ovih DNS poslužitelja**, i kaže mu da pita njega („Pitaj *labs5.fer.hr.*“).

6. **DNS prevoditelj sada šalje isti taj upit** poslužitelju na kojeg ga je glavni hrvatski DNS poslužitelj usmjerio, **jednom od glavnih FER-ovih DNS poslužitelja** („Gdje je *mail.fer.hr.*?“).

7. **FER-ov DNS poslužitelj** zna točnu adresu od *mail.fer.hr.* i **odgovara DNS prevoditelju s tom adresom** („Na *161.53.72.233.*“).

8. Konačno, **DNS prevoditelj sada šalje tu adresu korisničkom računalu** koje je pokrenulo cijeli ovaj proces, svojim prvim upitom („Na *161.53.72.233.*“).

Ovaj proces je koristan, jer u pravilu veći broj korisnika komunicira s jednim DNS prevoditeljem. To omogućava DNS prevoditelju da, jednom kada prođe prethodno navedeni proces, spremi odgovor na neko vrijeme („*mail.fer.hr.* se nalazi na *161.53.72.233*“), i svim ostalim korisnicima koji pošalju upit za isto ime odgovori **bez ponavljanja cijelog procesa prevođenja**. Spremnik u kojem se ti odgovori spremaju kod DNS prevoditelja zove se **DNS međuspremnik (eng. *DNS cache*)**.



Slika 3 - DNS prevođenje

2 Sigurnosni problemi DNS-a

DNS kao sustav dobro odrađuje posao za koji je namijenjen, ali postoji više sigurnosnih problema. Ovo poglavlje će dati osnovni pregled dva sigurnosna problema DNS-a koje predstavljaju ozbiljne prijetnje za sigurnost na Internetu.

2.1 Registracija sličnih imena u svrhu prijevare

Jedan od sigurnosnih problema DNS-a je registracija sličnih imena u svrhu prijevare. Uzmimo za primjer domenu *paypal.com.* koja pripada poznatom *online* sustavu za plaćanje *PayPal*.

Kao sustav koji barata novcima, *PayPal* je meta za kriminalce koji na razne načine žele preoteti novac od korisnika. Jedna od metoda koja im to omogućava je i registracija sličnih domena – konkretnije, u ovom slučaju bi kriminalci mogli pokušati registrirati domenu *paypa1.com.* (umjesto zadnjeg slova „*l*“ piše broj „*1*“ koji izgleda vrlo slično). Kada bi uspjeli registrirati tu domenu, na nju bi mogli postaviti svoju lažnu web stranicu i žrtvama slati elektroničku poštu s poveznicama na nju. Njihov očekivani rezultat je da žrtve vide tu poveznicu te da ju otvore bez da primijete da je slovo „*l*“ zamijenjeno brojem „*1*“, misleći da je to prava *PayPal* web stranica na pravoj *paypal.com.* domeni. Na primjer, URL lažne eeb stranice mogao bi biti:

https://www.paypa1.com/signin?country.x=HR&locale.x=en_HR

dok je URL prave webstranice (za koju korisnici mislite da joj pristupaju):

https://www.paypal.com/signin?country.x=HR&locale.x=en_HR .

U pravilu, jedini način pravovremene zaštite je da organizacija (u ovom slučaju *PayPal*) preventivno registrira sve potencijalno slične domene.

2.2 Lažiranje DNS odgovora

Drugi sigurnosni problem DNS-a je lažiranje DNS odgovora. Lažiranje DNS odgovora zapravo predstavlja cijelu klasu sigurnosnih problema koji se svi svode na to da, u konačnici, na neki način korisnik dobije lažnu informaciju u DNS odgovoru.

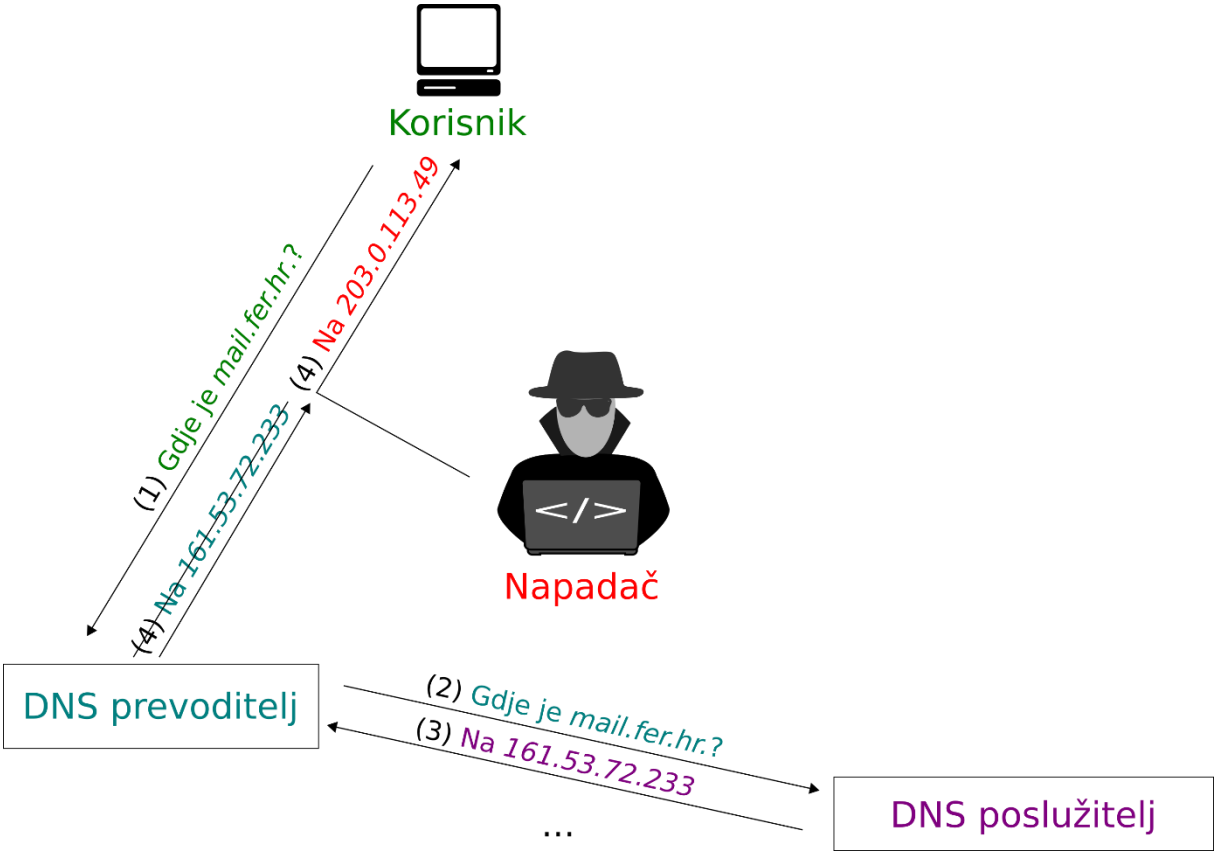
Jedan od faktora koji omogućava lažiranje DNS odgovora je činjenica da **DNS promet nije zaštićen**. Primjerice, svi DNS upiti i odgovori prikazani na slici 3 u prošlom poglavlju mogu biti **presretnuti i izmijenjeni**. Ovaj problem nije svojstven samo DNS-u – isto vrijedi i za druge nezaštićene protokole na Internetu, pa su zato potrebni dodatni zaštitni mehanizmi. Na primjer, i HTTP protokol (korišten za pregledavanje web stranica) podložan je istim problemima, pa se zato preporučuje korištenje HTTPS protokola (zapravo većinom isti protokol, samo zaštićen).

Drugi faktor koji je nešto specifičniji za DNS je korištenje UDP transportnog protokola za prijenos DNS upita i odgovora. UDP je jednostavan transportni protokol, ali nesiguran sam po sebi jer je **moguće lažirati od kuda dolazi poruka**. Posljedica toga je da, čak i kada napadač nije u prilici izmijeniti i presresti DNS promet, i dalje ima mogućnost slanja lažnih DNS odgovora žrtvama. Ako napadač zna točno kako

odgovor treba izgledati, i pošalje ga prije pravog odgovora, **žrtva će taj lažni odgovor prihvatiti**.

Uz ovo, moguća je i situacija gdje je **DNS prevoditelj nepouzdan** i namjerno šalje lažne DNS odgovore. To se može dogoditi kada napadač na neki način preuzme kontrolu nad DNS prevoditeljem ili kada je jednostavno osoba koja upravlja prevoditeljem napadač.

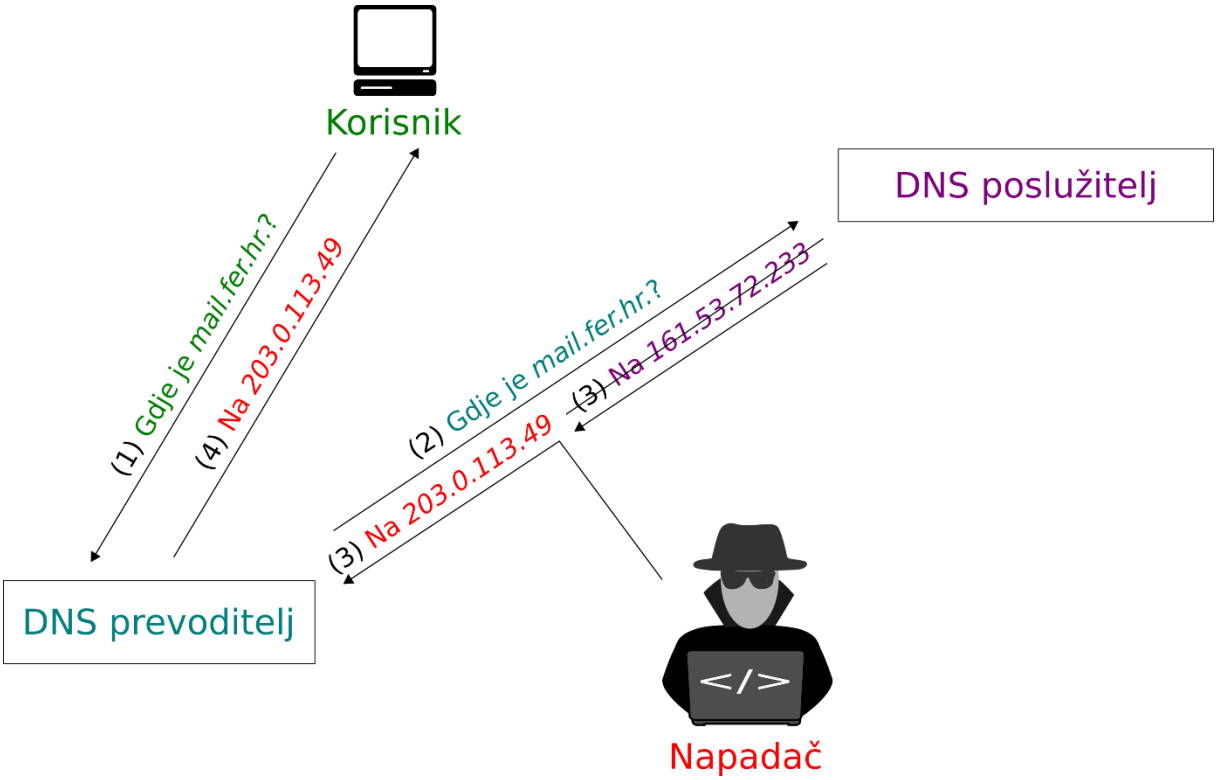
Slika 4 prikazuje primjer napada kod kojeg napadač **neposredno korisniku lažira DNS odgovor**. Prikazan je proces prevođenja imena *mail.fer.hr.* u IP adresu, kao i na slici 3, no dio kada DNS prevoditelj komunicira s DNS poslužiteljima (korijenskim, hrvatskim, FER-ovim) skraćen je zbog preglednosti. Napad se odvija u zadnjem koraku, kada DNS prevoditelj korisniku odgovara na upit. U tom koraku, umjesto da korisnik dobije pravi odgovor od DNS prevoditelja, on dobiva lažni odgovor od napadača koji sadrži lažnu IP adresu.



Slika 4 - DNS lažiranje neposredno prije korisnika

Slika 5 prikazuje sličan primjer napada, no u ovom slučaju napadač **DNS prevoditelju lažira DNS odgovor**, koji onda **posredno dolazi i do svih korisnika** koji komuniciraju s tim DNS prevoditeljem. Kao i na slici 4, prikazan je skraćeni proces prevođenja imena *mail.fer.hr.* u IP adresu. U ovom slučaju, **napad se odvija u trećem prikazanom koraku**, kada DNS poslužitelj odgovara DNS prevoditelju. U tom koraku, umjesto da DNS prevoditelj dobije pravi odgovor od DNS poslužitelja, on dobiva lažni odgovor od napadača koji sadrži lažnu IP adresu. DNS prevoditelj će spremiti tu lažnu IP adresu u svoj DNS međuspremnik, pa se zato ova vrsta napada zove **trovanje DNS**

međuspremnika (eng. *DNS cache poisoning*). Krajnja posljedica je da je **DNS prevoditelj prevaren** i u odgovorima **šalje svim svoj korisnicima lažnu IP adresu**.



Slika 5 – DNS trovanje međuspremnika (eng. *DNS cache poisoning*)

Lažiranje DNS odgovora**stvaran je i ozbiljan problem** na Internetu – pogotovo napadi trovanjem međuspremnika (*cache poisoning*). Za bolje razumijevanje te klase sigurnosnih problema i njihovih posljedica korisno je upoznati se s nekim stvarnim primjerima takvih napada.

Jedan primjer su **napadi na DNS prevoditelje brazilskih internetskih poslužitelja** iz studenog 2011. godine – više o napadima je moguće pročitati na ovoj poveznici. Napadači su uspješno izvršili napade trovanja međuspremnika (*cache poisoning*) određenih DNS prevoditelja u Brazilu i tako su **posredno napali velik broj tamošnjih korisnika Interneta**. Konkretnije, kada su žrtve pokušale pristupiti web stranicama popularnih servisa kao što su ***YouTube***, ***Gmail*** i ***Hotmail***, bile su preusmjerene na **lažne verzije web stranica**. Te web stranice su od žrtava zahtijevale da **preuzmu zlćudni softver (eng. *malware*)** prije nastavka korištenja, te u slučajevima kada su žrtve imale stare, ranjive verzije određenog softvera, računala su **čak i automatski bila zaražena** čim su lažne stranice otvorene.

Drugi primjer su napadi na nepoznate DNS prevoditelje o kojima je obavještavala organizacija CERT/CC u rujnu 2014. godine – više o napadima je moguće pročitati na ovoj poveznici. I u ovom slučaju napadači su uspješno izvršili napade trovanja međuspremnika (*cache poisoning*) određenih DNS prevoditelja i tako posredno napali veći broj korisnika Interneta. Ono što je zanimljivo kod ovog napada je koji su odgovori lažirani, tj. za koje domene – **lažirani su odgovori za domene najvećih *webmail* poslužitelja**. U članku nisu direktno imenovani servisi, no implicira se da bi to mogli biti ***Gmail***, ***Yahoo***, ***Outlook.com*** i slični. Posljedice ovog napada su najvjerojatnije bile

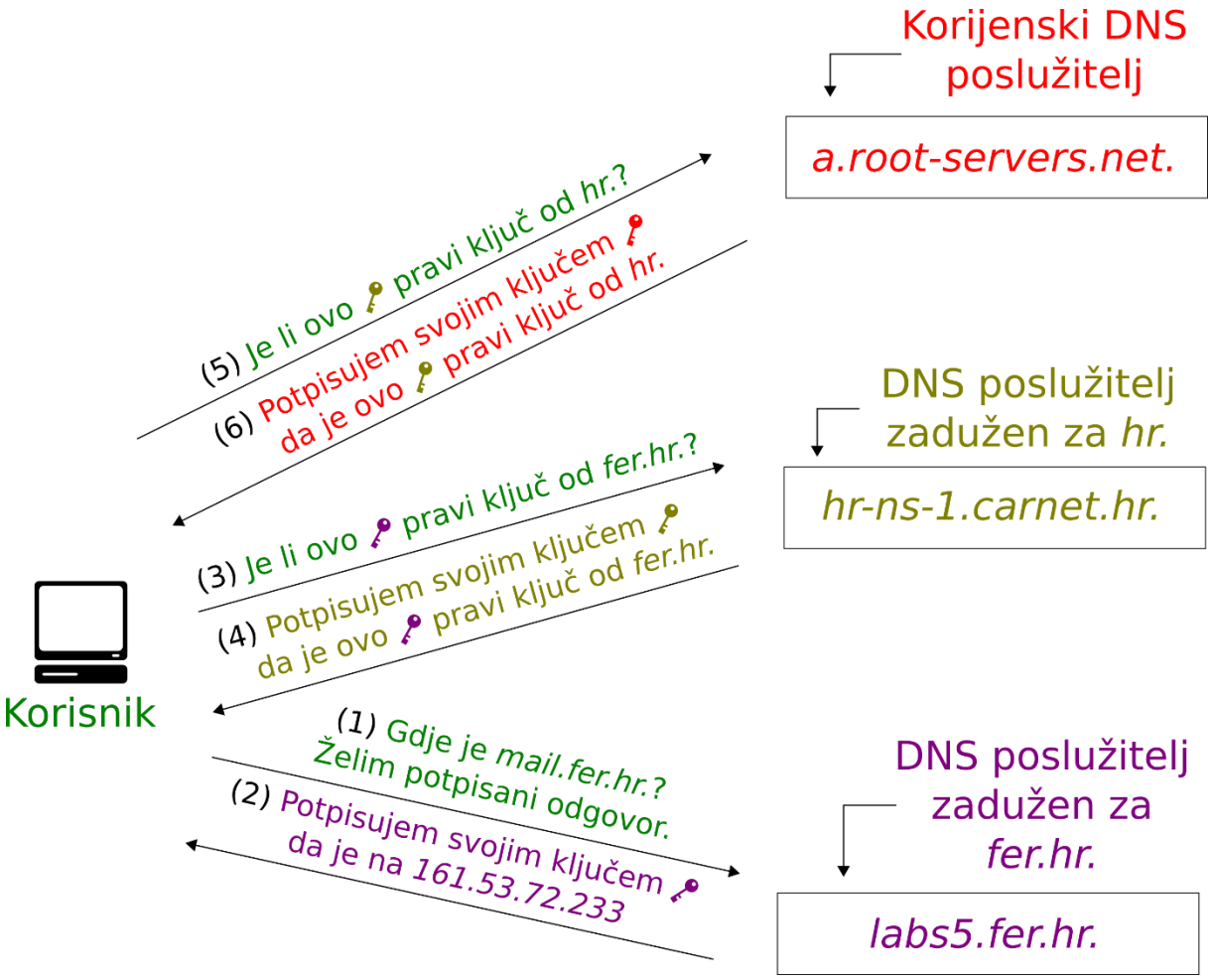
presretanje (potencijalno čitanje i izmjena) jednog dijela elektroničke pošte povezanog s navedenim *webmail* servisima.

Bitan zaključak je da je u oba slučaja **napadom na nekolicinu DNS prevoditelja** bilo moguće učiniti **veliku štetu** zbog relativnog velikog broja posrednih žrtava.

3 DNSSEC

DNSSEC je **sigurnosna nadogradnja DNS-a** čija je svrha upravo da **spriječi bilo kakvo lažiranje DNS odgovora**. Kada se koristi DNSSEC, DNS odgovori dolaze s **digitalnim potpisom** koji dokazuje da odgovor zaista dolazi od pravog DNS poslužitelja i da nije izmijenjen po putu. Tehničkim rječnikom – DNSSEC osigurava **autentičnost** i **integritet** DNS odgovora. No kako bi se korisnik uvjerio u ispravnost takvog DNS odgovora, nije dovoljno samo primiti odgovor s potpisom, već je nužno i **provjeriti ispravnost tog potpisa**.

Slika 6 prikazuje proces provjere potpisa DNS odgovora na primjeru upita za domenu *mail.fer.hr.* Proces započinje primitkom DNS odgovora s potpisom – tad korisnik prvo provjerava **je li dobiveni DNS odgovor ispravno potpisan FER-ovim (*fer.hr.*) ključem**. Ako je, tu provjera ne staje – jer korisnik u ovom trenutku nije siguran da je ključ s kojim je DNS odgovor potpisan zaista pravi FER-ov ključ. Zato, sljedeći korak je provjeravanje kod nadređenog DNS poslužitelja (*hr.*) **je li taj ključ zaista FER-ov ključ**. Ako je, ni tu provjera ne staje – na isti način potrebno je **lančano provjeriti ispravnost ključeva** sve do korijenskih DNS poslužitelja. Kod korijenskih DNS poslužitelja taj proces staje, jer u njihovom slučaju **ne postoji nadređeni poslužitelj** pa nije moguće na isti način provjeriti autentičnost njihovog ključa. Odgovornost korisnika je da **na siguran način pribavi ključ korijenskih poslužitelja** kako bi ovaj proces provjere završio s ključem kojem korisnik vjeruje i kako bi u konačnici korisnik bio siguran da je primljeni DNS odgovor zaista ispravan.



Slika 6 - DNSSEC provjera potpisa

Ovaj lanac digitalnih potpisa koji započinje s ključem korijenskih DNS poslužitelja i završava s potpisanim DNS odgovorom naziva se **lancem povjerenja**. S ključem korijenskih poslužitelja je taj lanac „usidren“ – drugim riječima, **ključ korijenskih poslužitelja je izvor povjerenja DNSSEC-a**. Jednom kada korisnik na siguran način pribavi taj ključ, može lančano provjeriti ispravnost svih drugih potpisa.

Za potpunu sigurnost, nužno je da se **provjera** je li DNS odgovor ispravno potpisan **odvija na računalu krajnjeg korisnika**. To je jedini način da korisnik bude siguran da DNS odgovor nije bio lažiran **niti u jednom dijelu procesa**. U alternativnim konfiguracijama, DNS prevoditelj provjerava ispravnost potpisa te javlja rezultat krajnjem korisniku, koji u to slijepo vjeruje. To olakšava konfiguraciju (DNSSEC je potrebno konfigurirati samo na prevoditelju, a ne i korisničkim računalima), ali **nije sigurno** jer je i dalje moguć napad na promet između DNS prevoditelja i korisnika, te čak i napad na samog DNS prevoditelja.

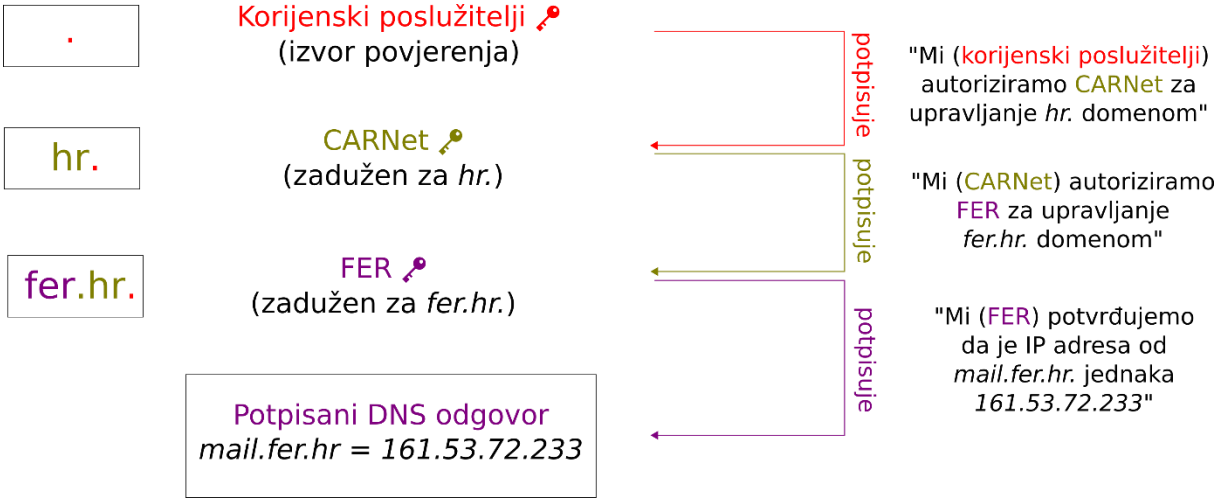
3.1 Stanje dobivenog odgovora

Kod provjere potpisa DNS odgovora zaštićenog DNSSEC-om, rezultat se **ne** svodi na uspješnu i neuspješnu provjeru. Ovisno o okolnostima, moguće je zapravo utvrditi **četiri stanja** za DNS odgovor:

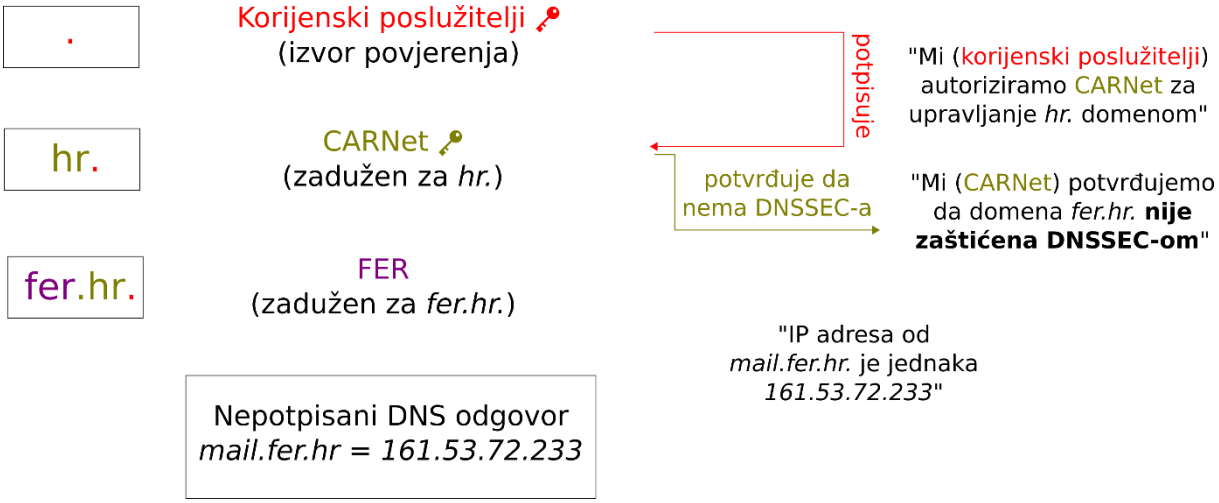
- **Sigurno**
  - Postoji ispravan lanac potpisa skroz do ključa kojemu korisnik vjeruje (što je u pravilu ključ korijenskih DNS poslužitelja).
  - **DNS odgovor je zaštićen.**
  - Prikazano na slici 7, pod pretpostavkom da korisnik **vjeruje** korijenskom ključu.
- **Nesigurno**
  - Postoji ispravan lanac potpisa do nekog trenutka u kojem je potvrđeno da tražena domena nije zaštićena DNSSEC-om.
  - Potvrđuje da je stanje nesigurno, tj. da postoji mogućnost napada – ali **nije moguće reći događa li se stvarno napad,** jer domena niže razine nije zaštićena DNSSEC-om.
  - Prikazano na slici 8.
- **Lažno**
  - Lanac potpisa nije ispravan.
  - **Neki od potpisa nije ispravan** (slika 9) ili **DNS odgovor nije potpisan**, a lanac povjerenja potvrđuje da bi trebao biti potpisan (slika 10)
  - Zaključak – **događa se napad ili nešto nije ispravno konfigurirano.**
- **Neodređeno**
  - Ne postoji ključ kojemu korisnik vjeruje s kojim bi mogao potvrditi ispravnost lanca potpisa.
  - Konkretnije – **korisnik nije sigurno preuzeo ključ korijenskih DNS poslužitelja i ne može donijeti nikakav zaključak**, makar lanac potpisa bio ispravan!
  - Prikazano na slici 7, pod pretpostavkom da korisnik **ne vjeruje** korijenskom ključu.

Ključno je razlikovati **nesigurno** stanje od **lažnog** stanja. **Nesigurno** stanje označava situaciju kada DNSSEC nije konfiguriran na domeni – u tom slučaju, DNS funkcionira kao i inače, sa svim svojim nesigurnostima. **Lažno** stanje nedvojbeno označava da se događa napad ili da je došlo do greške u konfiguraciji DNSSEC-a u nekom dijelu lanca. Uz ovakvo razlikovanje stanja, **moguće je zaštiti neke domene DNSSEC-om te i dalje koristiti nezaštićene domene kao i prije**.

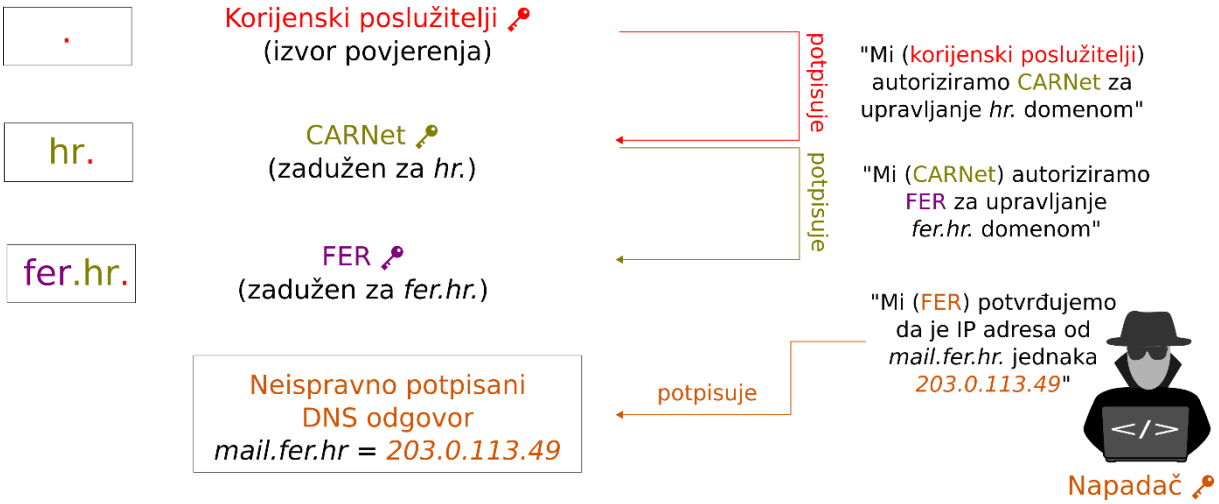
Razlika između **sigurnog** i **neodređenog** stanja je također bitna – kod **neodređenog** stanja, moguće je imati ispravan lanac kao i kod **sigurnog** stanja, samo je temeljna razlika u tome vjeruje li korisnik ključu korijenskih poslužitelja. Ako korisnik nije prethodno na siguran način pribavio ključ korijenskih poslužitelja, onda ne može vjerovati ni tom ključu, ni cijelom lancu povjerenja te konačno ni samom DNS odgovoru. **Bez povjerenja u ključ korijenskih poslužitelja, nema ni povjerenja u DNSSEC**.



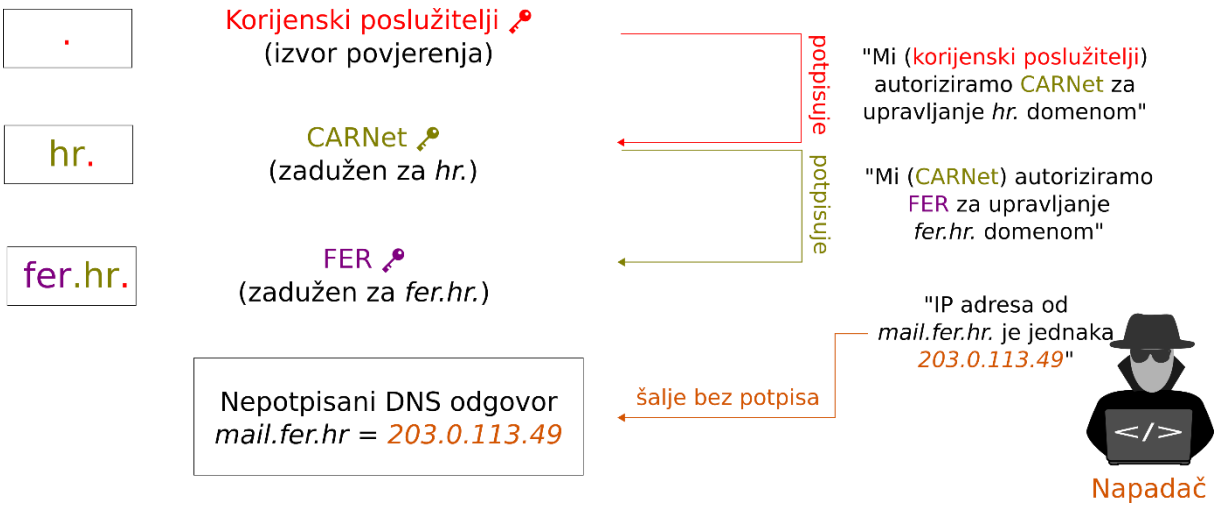
Slika 7 - Ispravan lanac potpisa, sigurno ili neodređeno stanje



Slika 8 - Ispravan lanac potpisa, nesigurno stanje



Slika 9 - Lažno stanje zbog neispravnog lanca potpisa



Slika 10 - Lažno stanje zbog nedostatka potpisa

3.2 Tehnička implementacija

S tehničke strane, DNSSEC dodaje šest novih vrsta DNS zapisa:

- *Resource Record Signature* (RRSIG) – zapis koji **sadrži digitalni potpis** DNS odgovora.
- *DNS Public Key* (DNSKEY) – zapis koji **sadrži javni ključ za provjeru digitalnih potpisa**.
- *Delegation Signer* (DS) – zapis kojim nadređeni poslužitelj na siguran način povjerava kontrolu nad domenom niže razine podređenom poslužitelju. Primarno **sadrži ime domene** koja se povjerava i **siguran sažetak (eng. *hash*) javnog ključa podređenog poslužitelja** kojemu se povjerava kontrola nad domenom.
- *Next Secure* (NSEC, NSEC3, NSEC3PARAM) – zapisi kojima se na siguran način **potvrđuje nepostojanje** DNS zapisa.

Pomoću alata i web servisa *DNSViz* moguće je na konkretnim primjerima vizualizirati kako ti DNS zapisi tvore DNSSEC lanac povjerenja. Slike 11, 12 i 13 prikazuju upravo tu vizualizaciju za tri različite domene odnosno DNS zapisa:

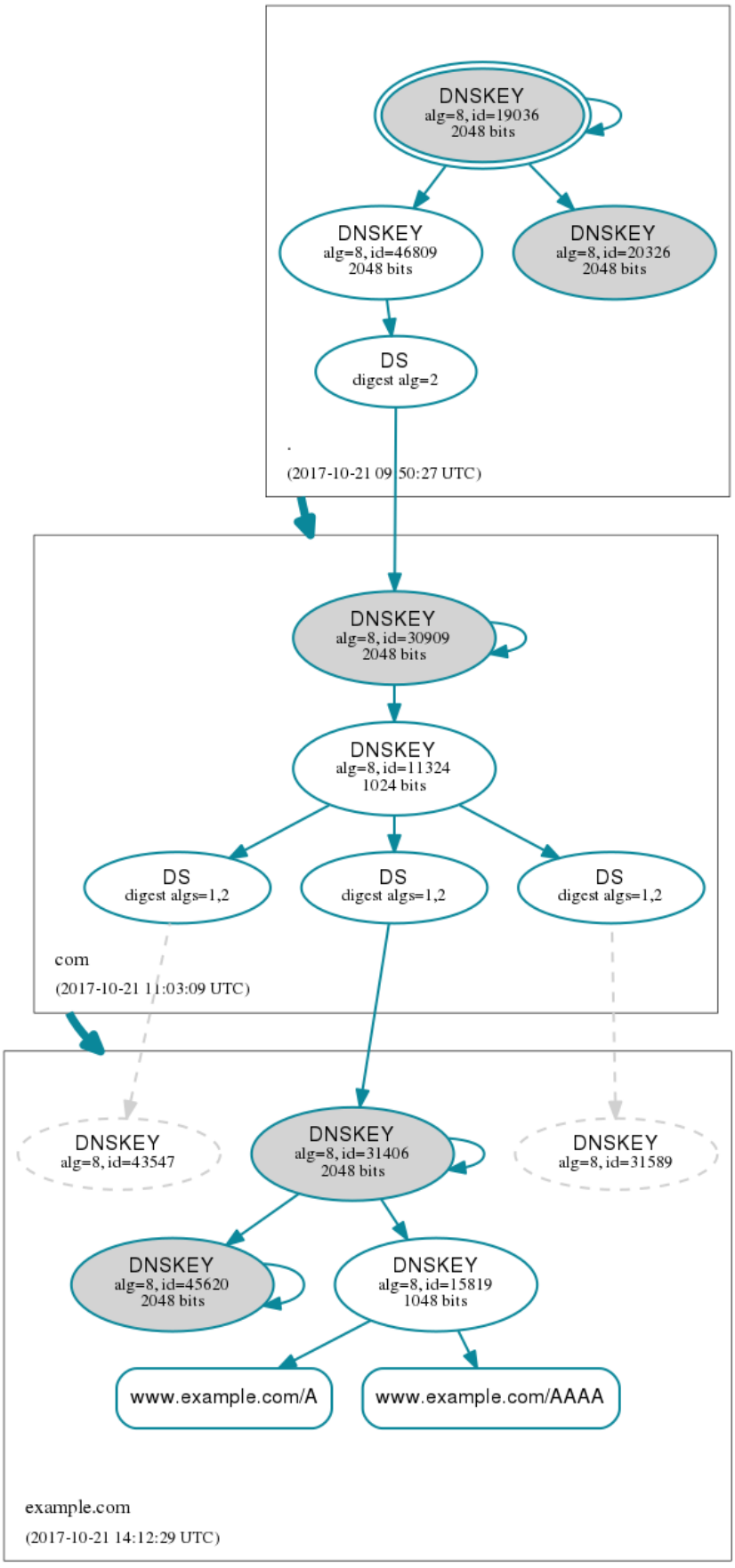
- Slika 11, *www.example.com.* – primjer ispravnog lanca i **sigurnog** stanja.
- Slika 12, *www.fer.hr.* – primjer ispravnog lanca i **nesigurnog** stanja.
- Slika 13, *www.dnssec-failed.org.* – primjer neispravnog lanca i **lažnog** stanja.

Na sve tri slike se na vrhu nalaze DNS zapisi korijenskog DNS poslužitelja. Skroz na vrhu, dvostruko zaokružen se nalazi **glavni ključ** korijenskih DNS poslužitelja. On potpisuje drugi ključ korijenskih DNS poslužitelja, koji zatim **potpisuje DS zapis**. Ova posrednost – ključ koji potpisuje drugi ključ koji zatim potpisuje zapis – postoji samo zbog lakoće održavanja i nije ključna za funkcioniranje DNSSEC-a. Potpisivanjem navedenog DS zapisa se **na siguran način povjerava kontrola** podređenim DNS poslužiteljima – na slikama su to poslužitelji zaduženi za *com.*, *hr.* odnosno *org.* domene. U tom se trenutku slike počinju značajno razlikovati.

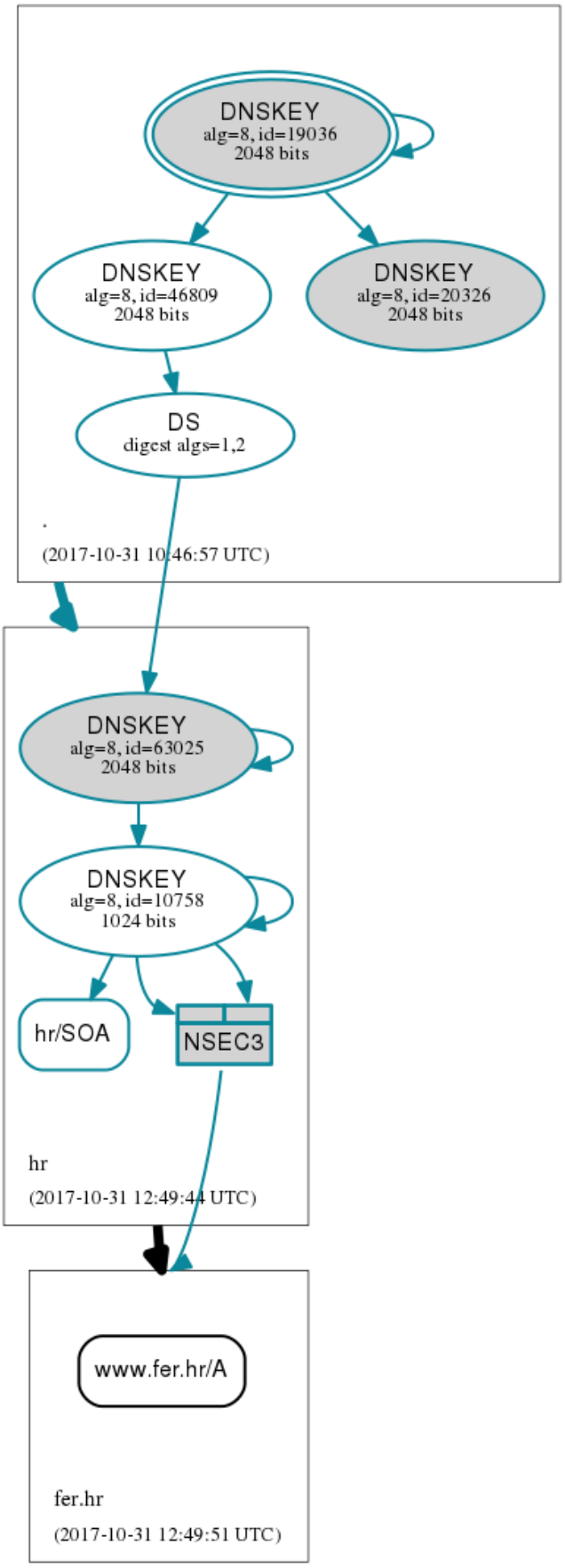
Na slici 11 **lanac se nastavlja na isti način** – isto kako su korijenski poslužitelji pomoću potpisanog DS zapisa povjerili kontrolu DNS poslužiteljima zaduženima za *com.*, tako su i ti poslužitelji povjerili kontrolu DNS poslužiteljima zaduženima za *example.com.* Konačno, isto kako su nadređeni poslužitelji potpisali DS zapise, poslužitelji zaduženi za *example.com.* potpisuju A zapis – zapis u kojemu piše koja je IP adresa od *www.example.com.* Rezultat je ispravan lanac povjerenja i **sigurno** stanje DNS odgovora.

Na slici 12 postoji značajna razlika – DNS poslužitelji zaduženi za *hr.* ne potpisuju DS zapis koji dalje povjerava kontrolu, već **potpisuju NSEC3 zapis koji potvrđuje da DS zapis za *fer.hr.* ne postoji**. To znači da DNSSEC nije konfiguriran za domenu *fer.hr.* – ona nije zaštićena, što znači da je **podložna napadima**, ali ne nužno i da se događa napad. Lanac je ispravan, ali stanje DNS odgovora je (potvrđeno) **nesigurno**.

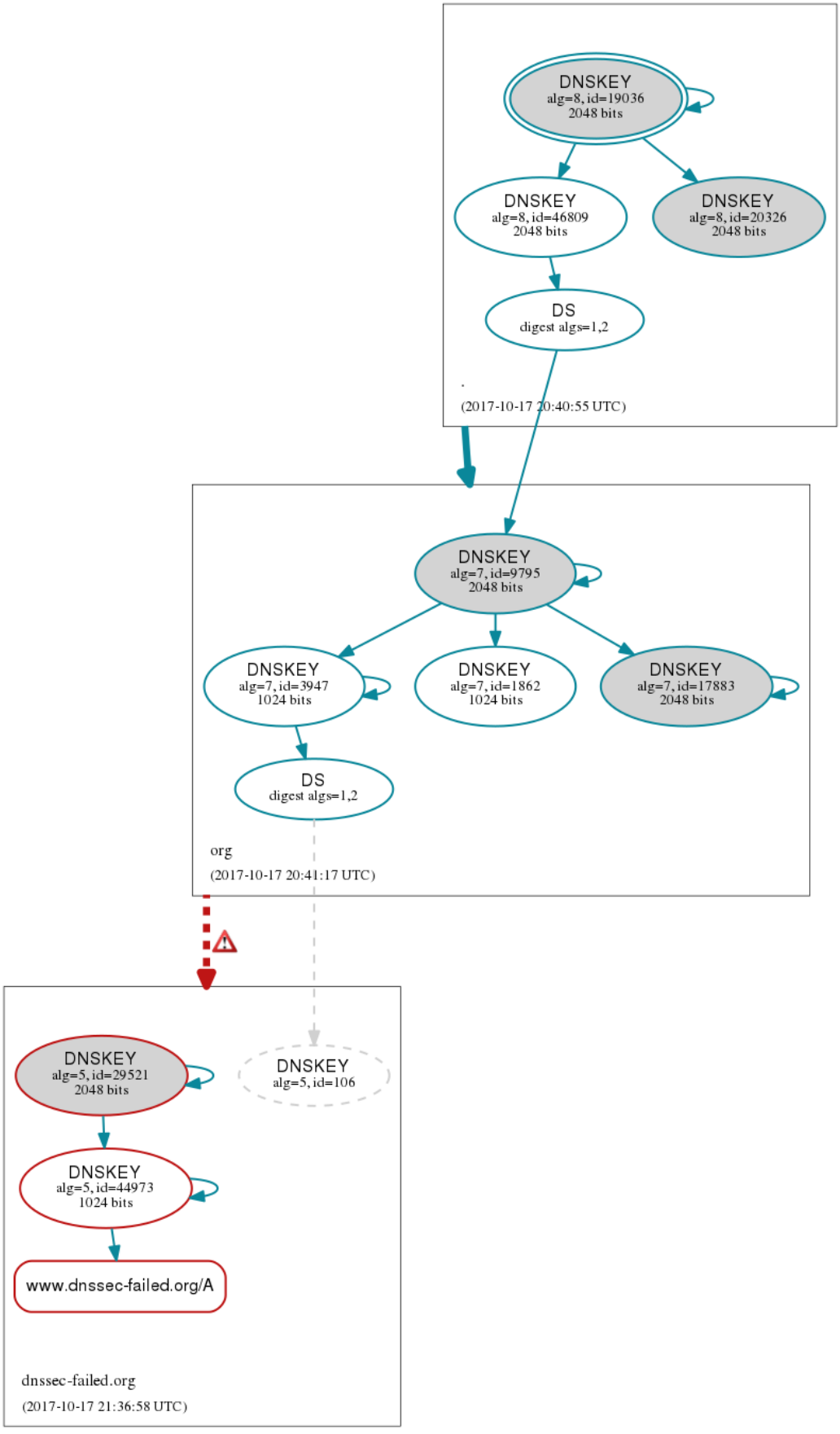
Slika 13 prikazuje domenu koja je **primjer za krivo konfigurirani DNSSEC, odnosno za napad na domenu zaštićenu DNSSEC-om**. Ključna razlika je u DS zapisu kojim DNS poslužitelji zaduženi za *org.* povjeravaju kontrolu – **kontrola je povjerena jednom ključu, no potpuni drugi ključ dalje potpisuje lanac**. Ovaj primjer prikazuje što bi se dogodilo kada bi napadač zaista pokušao lažirati potpis DNS odgovora s vlastitim, neispravnim ključem – lanac bi bio prekinut i neispravan, a stanje DNS odgovora **lažno**.



Slika 11 - Ispravan lanac potpisa, sigurno stanje za *www.example.com*



Slika 12 - Ispravan lanac potpisa, nesigurno stanje za *www.fer.hr.*



Slika 13 - Neispravan lanac potpisa, lažno stanje za *www.dnssec-failed.org*

3.3 Raširenost DNSSEC-a

Kako bi neka domena bila zaštićena DNSSEC-om, potrebno je da **cijeli lanac do nje bude zaštićen**. Primjerice, kako bi domena *zesoi.fer.hr.* (od zavoda ZESOI na FER-u) uopće mogla biti zaštićena, DNSSEC-om moraju biti zaštićeni:

- Korijen DNS-a (*„.“*)
- Hrvatska domena (*„hr.“*)
- FER-ova domena (*„fer.hr.“*)

Konkretnije, unatoč tome što su korijen DNS-a (*„.“*) i hrvatska domena (*„hr.“*) zaštićeni DNSSEC-om, FER-ova domena (*„fer.hr.“*) trenutno zaista **nije zaštićena DNSSEC-om**, tako da ni jedna domena ispod nje (uključujući *zesoi.fer.hr.*) **ne može biti zaštićena**.

Trenutno je slična situacija i kod ostalih domena:

- Kao što je već navedeno, **korijen DNS-a (*„.“*) zaštićen je DNSSEC-om**
- **Većina domena najviše razine** (kao što su *com.*, *org.*, *net.*, *hr.* …) je **zaštićena** – sveukupno oko 90% njih
    - Primjer domene najviše razine koja nije zaštićena je *aero.* – posljedica toga je da **ni jedna *<nešto>.aero.* domena ne može biti zaštićena DNSSEC-om**!
- Ispod toga, tzv. **domene druge razine** (npr. *fer.hr.*, *example.com.* …) **često ne podržavaju DNSSEC**
    - Npr. iako je *hr.* domena zaštićena DNSSEC-om, domena *fer.hr.* nije!
    - Postotak zaštićenosti varira ovisno o domeni najviše razine
        - Oko 88% zona ispod domene *gov.* su zaštićene (Američka vlada)
        - Oko 45% zona ispod domene *nl.* su zaštićene (Nizozemska)
        - Ali samo oko 0.5% zona ispod *com.* je zaštićeno – no i dalje, domena *com.* ima velik broj zona tako da tih 0.5% predstavlja otprilike 600 000 zaštićenih zona.

Podrška od strane domena (i DNS poslužitelja) je jedna polovica DNSSEC-a – drugi dio je podrška od strane korisnika i DNS prevoditelja, tj. njihovo traženje i provjeravanje DNSSEC potpisa. Gotovo sav često korišteni softver i sa strane poslužitelja i prevoditelja, i sa strane korisnika podržava korištenje DNSSEC-a. No trenutno, **provjera DNSSEC potpisa na uređaju korisnika nije uključena niti na jednom često korištenom operacijskom sustavu** (Windows, Mac, često korištene Linux distribucije, Android, iOS). Provjera potpisa odvija se na jednom dijelu DNS prevoditelja (primjerice na Googleovim javnim DNS poslužiteljima koje velik broj Android uređaja koristi), no kao što je prethodno navedeno, **to ne osigurava krajnjeg korisnika**.

Postavlja se pitanje – **zašto DNSSEC već nije konfiguriran i uključen svugdje**, i na domenama i na uređajima krajnjih korisnika? Jedan mogući razlog je to što DNSSEC nije lako konfigurirati. Događalo se da domene imaju **krivo konfiguriran DNSSEC**, zbog čega su one bile **nedostupne svim korisnicima i DNS prevoditeljima koji su provjeravali potpise, i posredno – svim korisnicima tih DNS prevoditelja**. Iz njihove perspektive, to je bio napad koji je DNSSEC spriječio, no zapravo je to bila samo greška u konfiguraciji koju nije moguće razlikovati od napada. Jedan primjer

upravo takvog slučaja je kriva konfiguracija *hbonow.com.* domene iz ožujka 2015. godine – više o tom događaju moguće je pročitati ovdje. Problem je bio sljedeći – DNS poslužitelji zaduženi za *com.* su imali DS zapis koji povjerava kontrolu nad *hbonow.com.* domenom i opisuje ispravni ključ za potpisivanje. Domena *hbonow.com.* je po tome **trebala biti zaštićena**, no njeni DNS poslužitelji **nisu potpisivali DNS odgovore**. Došlo je do greške u konfiguraciji, i svi korisnici i DNS prevoditelji koji su provjeravali DNSSEC potpise su utvrdili da je stanje DNS odgovora za *hbonow.com.* **lažno**. U konačnici, oni su ovu grešku (ispravno) **tretirali kao napad** i nisu dopuštali pristup toj domeni. U ovom slučaju, **i DNS prevoditelji mreže *Comcast* su provjeravali potpise** te zbog utvrđenog **lažnog** stanja, blokirali pristup toj domeni. Većina korisnika *Comcast* mreže koristila je upravo te DNS prevoditelje, pa je i njima bio blokiran pristup domeni *hbonow.com.*, što je jednom dijelu korisnika dalo dojam da *Comcast* namjerno blokira pristup toj domeni. Ovakvi događaji, gdje je **greška u konfiguraciji imala negativne poslovne posljedice**, jedan je od **potencijalnih razloga** koji sprječavaju velik broj organizacija da implementira DNSSEC na svojim domenama odnosno na uređajima koje proizvode.

3.4 Kako koristiti DNSSEC?

Korisnici koji se žele zaštititi od nesigurnosti DNS-a na domenama koje podržavaju DNSSEC mogu konfigurirati svoje računalo da u DNS upitima **traži potpisane odgovore** i da onda te potpise i **provjerava**.

Za korištenje DNSSEC-a na računalima s Windows, Mac i Linux operacijskim sustavima moguće je instalirati *Unbound*, programski paket koji obavlja DNS prevođenje i provjeru DNSSEC potpisa. Upute za instalaciju *Unbound*-a na Windows operacijskim sustavima je moguće preuzeti ovdje. Jednom kada je *Unbound* instaliran, zadnji korak je konfiguracija računala da koristi *127.0.0.1* kao IP adresu svog DNS prevoditelja – to je lokalna IP adresa gdje je pokrenut *Unbound*, koji će onda tražiti i provjeravati DNSSEC potpise za svaki DNS upit korisnikovog računala.

Na Linux distribucijama često nije ni potrebno instalirati nikakve dodatne programske pakete (kao što je *Unbound*), već je dovoljno samo konfigurirati postojeće. Paketi *dnsmasq* i *systemd-resolved* koji se često koriste na Linux distribucijama oboje podržavaju provjeravanje DNSSEC potpisa – sve što je potrebno je uključiti to u njihovoj konfiguraciji. No, dobro je znati da je česti problem kod ovakve konfiguracije korištenje DNS prevoditelja koji **strogo ne podržavaju DNSSEC**. Takvi prevoditelji će u prijenosu DNS odgovora maknuti sve zapise koje ne prepoznaju **– uključujući i DNSSEC potpise**. Rezultat kod krajnjeg korisnika je prividna greška u radu DNSSEC-a. Taj problem je moguće riješiti **korištenjem programskog paketa** kao što je *Unbound* (**koji samostalno obavlja DNS prevođenje**) ili **konfiguracijom svog računala da koristi DNS prevoditelje koji podržavaju DNSSEC**, primjerice Google-ove javne DNS prevoditelje na IP adresama 8.8.8.8 i 8.8.4.4 (no tada je važno biti svjestan kako to utječe na privatnost korištenja Interneta).

Za mobilne uređaje s operacijskim sustavima Android i iOS na žalost ne postoji jednostavan način za provjeravanje DNSSEC potpisa. Moguće je konfigurirati korištenje DNS prevoditelja koji provjeravaju DNSSEC potpise, no to daje samo djelomičnu zaštitu, a korisnike otvara riziku nedostupnosti domena koje imaju krivo konfiguriran DNSSEC. Za administratore DNS prevoditelja i domena, odnosno DNS

poslužitelja, dostupne su upute za konfiguraciju svih često korištenih programskih paketa. Ovdje je moguće preuzeti detaljne upute za konfiguraciju DNSSEC-a na *BIND* DNS poslužitelju/prevoditelju. Prije konfiguracije DNSSEC-a za svoje DNS prevoditelje odnosno domenu/poslužitelje, važno je biti svjestan kako će to utjecati na potencijalne korisnike – kao što je navedeno u prošlom poglavlju, greška u konfiguraciji može uzrokovati nedostupnost servisa, no kada je sigurnost bitna, taj rizik može biti u potpunosti prihvatljiv.

3.5 Zamjena korijenskog ključa

U sigurnosnim sustavima koji se oslanjaju na digitalno potpisivanje kao što je DNSSEC, **povremeno mijenjanje ključa** za potpisivanje je **dobra sigurnosna praksa**. To je preventivna mjera koja ograničava štetu u slučaju da je ključ kompromitiran, tj. da je napadač nekako došao do njega. Zamjenom ključa, stari, potencijalno kompromitirani ključ više nije aktivan i ne može raditi štetu, a mijenja se novim ključem za kojega se s visokom pouzdanošću može reći da je siguran.

Trenutni DNSSEC ključ korijenskih poslužitelja je generiran 2010. godine – u ovom kontekstu, taj ključ je relativno star, te se planira uskoro zamijeniti novim ključem. To je postepeni proces – novi ključ je generiran još u listopadu 2016. godine, a zamjena starog ključa tim novim ključem je planirana otprilike godinu dana kasnije, 11. listopada 2017. godine, kako bi svi imali dovoljno vremena za pripremu. Unatoč tom periodu za pripremu, zamjena ključa nije obavljena 11.10.2017. već je odgođena zbog informacija da velik broj DNS prevoditelja nije bio spreman za zamjenu.

Ova vijest je bitna za administratore DNS prevoditelja – nužno je pratiti novosti o promjeni ključa te držati svoje DNS prevoditelje ispravno konfiguriranima, kako bi nastavili uspješno raditi i nakon zamjene ključa korijenskih poslužitelja.

3.6 DNSSEC kao temelj sigurnosti za druge tehnologije

Osiguravanje DNS-a kao sustava koji povezuje domenska imena i zapise može biti temelj sigurnosti za mnoge druge tehnologije. Konkretno, tehnologije kojima je potrebna sigurna razmjena ključeva mogu kao svoj sigurnosni temelj koristiti DNS zapise osigurane DNSSEC-om.

Ove tehnologije su većinom još u stadiju osmišljavanja ili razvoju, no već postoji mnogo obećavajućih mogućnosti – u DNS zapise moguće je zapisati:

- TLS certifikate
  - Stavljanje TLS certifikata i u DNS zapis dodatno osigurava HTTPS, tj. sprječava lažiranje certifikata od strane zlonamjernih/kompromitiranih tijela za izdavanje certifikata (eng. *rogue certificate authorities*).
  - Za automatsko osiguravanje elektroničke pošte.
  - U pravilu za bilo koju drugu tehnologiju koja se oslanja na DNS i TLS.
- PGP javne ključeve
  - Dodatno povjerenje za ključeve, uz mrežu povjerenja (eng. *web of trust*).
- SSH otiske poslužitelja (eng. *host fingerprint)*
  - Dodatno osiguranje od napada na SSH veze, tj. od spajanja na napadačev lažni poslužitelj.

Jedan dio navedenoga razvija se i već danas je moguće koristiti kroz DANE (*DNS-based Authentication of Named Entities*) tehnologije. Vrijednost ovakvih tehnologija se već počinje prepoznavati u Europi – osiguravanje elektroničke pošte pomoću DANE-a obavezno je za sva vladina tijela u Nizozemskoj, dok će u Njemačkoj to biti obavezno za sve organizacije koje žele biti certificirane kao sigurni davatelji usluga elektroničke pošte.

4 Zaključak

DNSSEC je sigurnosni dodatak DNS-u koji osigurava autentičnost i integritet DNS odgovora te tako **štiti DNS od ozbiljnih i stvarnih sigurnosnih problema**.

Na globalnoj razini, DNSSEC **još nije u širokoj uporabi**, potencijalno jer konfiguracija DNSSEC-a nije jednostavna, a greške u konfiguraciji mogu učiniti servise nedostupnima i tako negativno utjecati na poslovanje. No u nekim kontekstima gdje je sigurnost prioritet, DNSSEC je **prepoznat kao korisno i nužno rješenje**. Primjerice, oko 88% DNS zona unutar *gov.* domene (koja pripada Američkoj vladi) potpisano je DNSSEC-om, dok je u Nizozemskoj korištenje DNSSEC i DANE tehnologija (za osiguravanje elektroničke pošte) obavezno za sva vladina tijela.

Kao krajnji korisnik, moguće je konfigurirati svoje uređaje da prilikom slanja DNS upita traže i provjeravaju DNSSEC potpise. Na taj način moguće je spriječiti bilo kakvo lažiranje DNS odgovora za domene koje su zaštićene DNSSEC-om. **Kao administrator DNS prevoditelja** je analogno moguće konfigurirati korištenje DNSSEC-a kako bi se DNS prevoditelji osigurali od napada trovanjem međuspremnika (eng. *cache poisoning*) na zaštićene domene.

Kao administrator domene odnosno DNS poslužitelja, moguće je zaštititi svoju domenu DNSSEC-om, osim u rijetkim slučajevima kada neka od nadređenih zona nije zaštićena. Sav često korišteni DNS poslužiteljski softver podržava DNSSEC i ima dostupne upute.

U konačnici, korist DNSSEC-a ne staje s osiguravanjem uobičajenih DNS odgovora. Trenutno se razvijaju (i na nekim mjestima već koriste) tehnologije koje **svoju sigurnost temelje na sigurnom DNS-u**. Ako su DNS zapisi osigurani, u njih je moguće zapisati **TLS certifikate, PGP javne ključeve, SSH otiske poslužitelja (eng. *host fingerprint*)** i slične podatke kako bi se riješio problem sigurne razmjene ključa i tako osigurale tehnologije kao što je primjerice elektronička pošta.

5 Literatura

1. **Assolini, Fabio.** Massive DNS poisoning attacks in Brazil. *Securelist.* [Mrežno] 7. studeni 2011. [Citirano: 31. listopad 2017.] https://securelist.com/massive-dns-poisoning-attacks-in-brazil-31/31628/.
2. **Atkins, Derek i Austein, Rob.** Threat Analysis of the Domain Name System (DNS). *IETF.* [Mrežno] kolovoz 2004. [Citirano: 31. listopad 2017.] https://tools.ietf.org/html/rfc3833.
3. **Boyce, Jim.** Understanding how DNS works, part 1. *TechRepublic.* [Mrežno] 20. srpanj 2000. [Citirano: 31. listopad 2017.] https://www.techrepublic.com/article/understanding-how-dns-works-part-1/.
4. —. Understanding how DNS works, part 2. *TechRepublic.* [Mrežno] 14. rujan 2000. [Citirano: 31. listopad 2017.] https://www.techrepublic.com/article/understanding-how-dns-works-part-2/.
5. **Brini, Davide.** DNSSEC verification with dig. *1.* [Mrežno] 17. studeni 2010. [Citirano: 31. listopad 2017.] http://backreference.org/2010/11/17/dnssec-verification-with-dig/.
6. **Cloudfare.** DNSSEC Complexities and Considerations. [Mrežno] [Citirano: 31. listopad 2017.] https://www.cloudflare.com/dns/dnssec/dnssec-complexities-and-considerations/.
7. —. How DNSSEC Works. [Mrežno] [Citirano: 31. listopad 2017.] https://www.cloudflare.com/dns/dnssec/how-dnssec-works/.
8. **DNSViz.** A DNS visualization tool. [Mrežno] [Citirano: 31. listopad 2017.] http://dnsviz.net/.
9. **Davids, Marco.** New e-mail security protocols mandatory within government. *SIDN.* [Mrežno] 24. listopad 2016. [Citirano: 31. listopad 2017.] https://www.sidnlabs.nl/a/weblog/new-e-mail-security-protocols-mandatory-within-government?language_id=2.
10. **Ferrari, Martín.** DNSSEC, DANE, SSHFP, etc. [Mrežno] 22. travanj 2014. [Citirano: 31. listopad 2017.] https://blog.tincho.org/posts/DNSSEC__44___DANE__44___SSHFP__44___etc/.
11. **Friedl, Steve.** An Illustrated Guide to the Kaminsky DNS Vulnerability. [Mrežno] 7. kolovoz 2008. [Citirano: 31. listopad 2017.] http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html.
12. **Gudmundsson, Olafur.** DNSSEC Done Right. *Cloudfare.* [Mrežno] 29. siječanj 2015. [Citirano: 31. listopad 2017.] https://blog.cloudflare.com/dnssec-done-right/.
13. **Höbel, Peter.** Secure email transport required by the German Federal Office. *Open-Xchange Blog.* [Mrežno] 26. svibanj 2016. [Citirano: 31. listopad 2017.] https://blog.open-xchange.com/2016/05/26/bsi/.
14. **ICANN.** DNSSEC – What Is It and Why Is It Important? [Mrežno] 29. siječanj 2014. [Citirano: 31. listopad 2017.] https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en.
15. —. KSK Rollover Postponed. [Mrežno] 27. rujan 2017. [Citirano: 31. listopad 2017.] https://www.icann.org/news/announcement-2017-09-27-en.
16. —. Root Zone KSK Rollover. [Mrežno] [Citirano: 2017. listopad 31.] https://www.icann.org/resources/pages/ksk-rollover.
17. **ISC.** BIND DNSSEC Guide. [Mrežno] 2017. [Citirano: 31. listopad 2017.] https://ftp.isc.org/isc/dnssec-guide/dnssec-guide.pdf.

18. **Internet Society.** DNSSEC Test Sites. [Mrežno] 13. lipanj 2013. [Citirano: 31. listopad 2017.] https://www.internetsociety.org/resources/deploy360/2013/dnssec-test-sites/.
19. —. State of DNSSEC Deployment 2016. [Mrežno] prosinac 2016. [Citirano: 31. listopad 2017.] https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-State-of-DNSSEC-Deployment-2016-v1.pdf.
20. **Larson, Matt.** Do you have DNSSEC validation enabled? [Mrežno] 11. svibanj 2017. [Citirano: 31. listopad 2017.] https://blog.apnic.net/2017/05/11/dnssec-validation-enabled/.
21. **Larson, Matt, i dr.** DNS Security Introduction and Requirements. *IETF.* [Mrežno] [Citirano: 31. listopad 2017.] https://tools.ietf.org/html/rfc4033.
22. **Spring, Jonathan.** Probable Cache Poisoning of Mail Handling Domains. *CERT/CC Blog.* [Mrežno] 10. rujan 2014. [Citirano: 31. listopad 2017.] https://insights.sei.cmu.edu/cert/2014/09/-probable-cache-poisoning-of-mail-handling-domains.html.
23. **Unbound.** *Unbound.* [Mrežno] [Citirano: 31. listopad 2017.] https://www.unbound.net/.
24. **Wijngaards, Wouter.** Manual for Unbound on Windows. *Unbound.* [Mrežno] svibanj 2015. [Citirano: 31. listopad 2017.] https://www.unbound.net/documentation/unbound-windows-manual-02.pdf.
25. **York, Dan.** HBO NOW DNSSEC Misconfiguration Makes Site Unavailable From Comcast Networks (Fixed Now). *Internet Society.* [Mrežno] 10. ožujak 2015. [Citirano: 31. listopad 2017.] https://www.internetsociety.org/blog/2015/03/hbo-now-dnssec-misconfiguration-makes-site-unavailable-from-comcast-networks-fixed-now/.