Centar Informacijske Sigurnosti

Sigurnosne ekstenzije DNS sustava

lipanj 2011.

CIS-DOC-2012-06-052

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Kako bi stupili u kontakt s nekom osobom na Internetu ili koristili neku uslugu ili resurs, potrebno je unijeti Internet adresu te osobe, usluge ili resursa i to u obliku simboličkog imena ili broja. Ta adresa mora biti jedinstvena kako bi se računala znala međusobno razlikovati pri uspostavi međusobne komunikacije. Neprofitna organizacija ICANN[1] (eng. *Internet Corporation for Assigned Names and Numbers*) zadužena je za koordinaciju spomenutih jedinstvenih identifikatora računala. Bez te koordinacije ne bi postojao globalni Internet.

Ako pri unosu koristimo simboličko ime, ono se prvo treba prevesti u broj, budući da računala rade s pravim IP(eng. *Internet Protocol*) adresama[2]. Sustav koji je zadužen za prevođenje simboličkog imena u njemu pridruženu IP adresu zove se DNS (eng. *Domain Name System*) sustav. Nedavno su otkrivene značajne ranjivosti ovog sustava koje zlonamjernim korisnicima omogućuju preuzimanje kontrole nad Internet sjednicom kako bi, na primjer, korisnika preusmjerili na svoju lažnu stranicu i ukrali mu korisničko ime i lozinku.

Ovakve ranjivosti povećale su interes za uvođenjem tehnologije poznate pod nazivom sigurnosne ekstenzije DNS sustava ili skraćeno DNSSEC (eng. *Domain Name System Security Extensions*) čiji je cilj pružiti sigurnost DNS sustavu i spriječiti spomenute napade.

U drugom poglavlju ovog dokumenta dan je pregled povijesti DNS sustava, njegove osnove i sigurnosni problemi. Treće i četvrto poglavlje dokumenta donose opis sigurnosnih ekstenzija DNS sustava te se navode njihovi ciljevi i način rada. Također je dan kratki pregled alata koji se koriste za implementaciju sigurnosnih ekstenzija DNS sustava te su navedeni problemi DNSSEC-a. Na kraju su dana predviđanja stručnjaka o budućnosti sigurnosnih ekstenzija DNS sustava te zaključak.

[1] ICANN je privatna neprofitna organizacija smještena u Los Angelesu zadužena za koordinaciju identifikatora na Internetu i osiguravanje stabilnih i sigurnih operacija nad njima.

[2] IP adresa je jedinstvena brojčana oznaka računala na Internetu.

2. DNS

DNS je distribuirani hijerarhijski sustav Internet poslužitelja u kojem se nalaze informacije povezane s domenskim nazivima, među kojima je i povezanost IP adresa i njihovih simboličkih imena.

DNS se često naziva "telefonskim imenikom Interneta" budući da prevodi simbolička imena u IP adrese. Na primjer, DNS sustav može prevesti simboličko ime www.primjer.com u IP adrese 192.0.43.10 (IPv4) i 2620:0:2d0:200::10 (IPv6). [1]

Ipak, za razliku od telefonskog imenika, DNS sustav se puno brže i lakše prilagođava promjenama. Time se olakšava pristup zatraženoj usluzi nakon što usluga promijeni IP adresu. Naime, korisnik ne mora znati da se IP adresa promjenila, on i dalje može koristiti simboličko ime bez ikakvih problema.Većina korisnika danas uvelike iskorištava tu činjenicu prilikom korištenja URL[3] (eng. *Uniform Resource Locator*) nizova koji imaju neko smisleno značenje i adresa elektroničke pošte te se pri tom ne zamaraju detaljima kako računalo zapravo locira zatražene usluge.

2.1. Povijest DNS-a

Povijest Interneta seže u 1960-te godine, kada nastaje ARPAnet[4], mreža namijenjena razmjeni datoteka, programa i elektroničke pošte te spajanju na udaljena računala. Već tada se počelo numeričke adrese zamjenjivati jednostavnijim nazivima koji su bliži korisniku i lakše pamtljivi. Da bi ta zamjena bila moguća, svako računalo u ARPAnet mreži moralo je zatražiti od instituta za istraživanje u Standfordu (*Stanford Research Institute, SRI*) datoteku *hosts.txt* koja je povezivala simbolička imena s adresama za ARPAnet mrežu. Da bi računala u ARPAnet mreži "vidjela" ostala računala priključena na mrežu, morala su imati posljednju verziju datoteke *hosts.txt*. S druge strane, institut SRI je morao biti obavješten o svakom novom računalu u mreži, kako bi ga mogao dodati u datoteku *hosts.txt* i poslati novu verziju te datoteke svim računalima na mreži.

Brzi razvoj mreže u narednih deset godina, tijekom kojeg je u ARPAnet uključeno na tisuće računala, doveo je do pojave Interneta. Također, takav nagli razvoj rezultirao je i neodrživošću sustava temeljenog na datoteci *hosts.txt* te se pojavila potreba za bržim i skalabilnijim sustavom za prevođenje simboličkih imena u numeričke adrese.

Ideju DNS sustava i prvu implementaciju napisao je Paul Mockapetris[5] (slika 1) 1984. godine na zahtjev Jona Postela[6]. Ta verzija DNS sustava poznata je pod nazivom *Jeeves*, a koristili su je SRI i University of Southern California's Information Sciences Institute.

Iste godine Douglas Terry, Mark Painter, David Riggle i Songnian Zhou, četvorica studenata na fakultetu u Berkleyju, napisala su prvu Unix implementaciju. Ta implemetacija nazvana je Berkeley Internet Name Domain (BIND) i danas prevladava kao najkorišteniji DNS program na Internetu. [1]

[3] URL (eng. *Uniform Resource Locator*) je Web adresa određenog resursa na Internetu.

[4] ARPAnet je preteča Interneta, bila je to velika rasprostranjena mreža koju je razvilo američko Ministarstvo obrane, a uspostavljena je 1969. godine.

[5] Paul Mockapetris, rođen 1948. godine, smatra se izumiteljem DNS sustava.

[6] Jon Postel (1948-1998) je američki znanstvenik koji je mnogo pridonio razvoju Interneta.

Slika 1. Paul Mockapetris, izumitelj DNS sustava
Izvor: Information Sciences Institute

2.2. Struktura DNS sustava

2.2.1. Domensko ime

Domensko ime je simboličko ime računala na internetu koje ga najčešće jednoznačno identificira (postoji mogućnost da više računala dijeli jedno domensko ime). Domensko ime sastoji se od jedne ili više labela, odvojenih točkama, npr. *primjeri.com*.

Labela je niz alfanumeričkih znakova pri čemu je dopušten i znak "-". Pravilo stvaranja labele poznato je pod nazivom LDH (eng. *letters, digits, hyphen*) pravilo. Labela ne smije počinjati ili završavati znakom "-", a velika i mala slova se ne razlikuju. Maksimalna dopuštena duljina labele iznosi 63 znaka. [2]

Kao što je već prije rečeno, labele se odvajaju točkama i na taj način tvore domensko ime. Domensko ime u kojem su navedene sve labele zove se FQDN (eng. *Fully Qualified Domain Name*) ime i predstavlja punu stazu unutar DNS hijerarhije. Maksimalna duljina FQND-a jest 255 znakova.

Krajnja desna labela domenskog imena naziva se vršna domena ili TLD (eng. *top-level domain*), npr. domensko ime *primjeri.com* pripada vršnoj domeni *com.*

Hijerarhija domena čita se s desna na lijevo. Sve domene lijevo od TLD-a u domenskom imenu predstavljaju poddomene, pri čemu je moguće 127 razina poddomena.

Krajnja lijeva labela naziva se kratko ime računala.

2.2.2. Vršne domene

Za dodjelu domena i upravljanje domenama zadužena je neprofitna organizacija ICANN. Ona brine o upravljanju domenama i IP adresama. Naime, domenska imena su grupirana u nekoliko vršnih domena, unutar kojih ne smije doći do kolizija, tj. za pravilan rad DNS sustava unutar jedne vršne domene ne smiju postojati dvije iste poddomene.

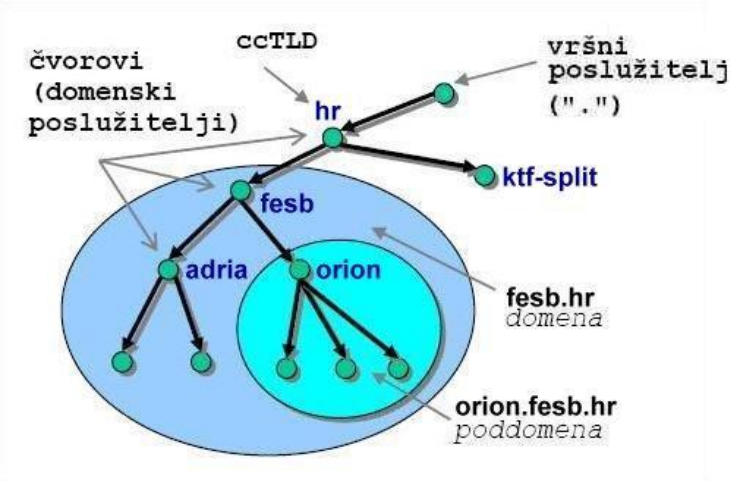
Zbog toga se vršne domene strogo kontroliraju, a postoje 2 tipa imena vršnih domena [2]:

1. **geografski bazirane domene** tzv. ccTLD (eng. *country code TLD*) su domene koje predstavljaju državni dvoznakovni kod temeljen na ISO-3166 standardu, a danas ih je u uporabi preko 243. Primjeri takvih domena su: .hr, .us, .de, .jp, .co.uk, i druge.
2. **generičke domene**, tzv. gTLD (eng. *generic TLD*) su domene koje se obično sastoje od tri ili više znakova. Primjeri takvih domena su: .com, .net, .org, .info, .biz, .edu i druge.

2.2.3. Domenski registri

Domenski registri su baze podataka o domenama i odgovarajućim IP adresama. Svaki registar upravlja DNS poslužiteljima za specifični TLD. Za ccTLD-ove su obično nadležne vlade pojedinih država, dok je za gTLD nadležan isključivo ICANN koji regulira upravljanjem 13 vršnih DNS poslužitelja (engl. *root servers*). [2]

Za hrvatsku vršnu domenu .hr zadužen je poslužitelj dns.srce.hr kojim upravlja HR-DNS služba za CARNet. Primjer DNS hijerarhije prikazan je na slici 2.



Slika 2.DNS hijerarhija
Izvor: Računalne mreže | Eldis Mujarić, dipl. ing.

2.2.4. DNS razrješenje

Funkcionalni DNS sustav nužno se sastoji od tri dijela [2]:

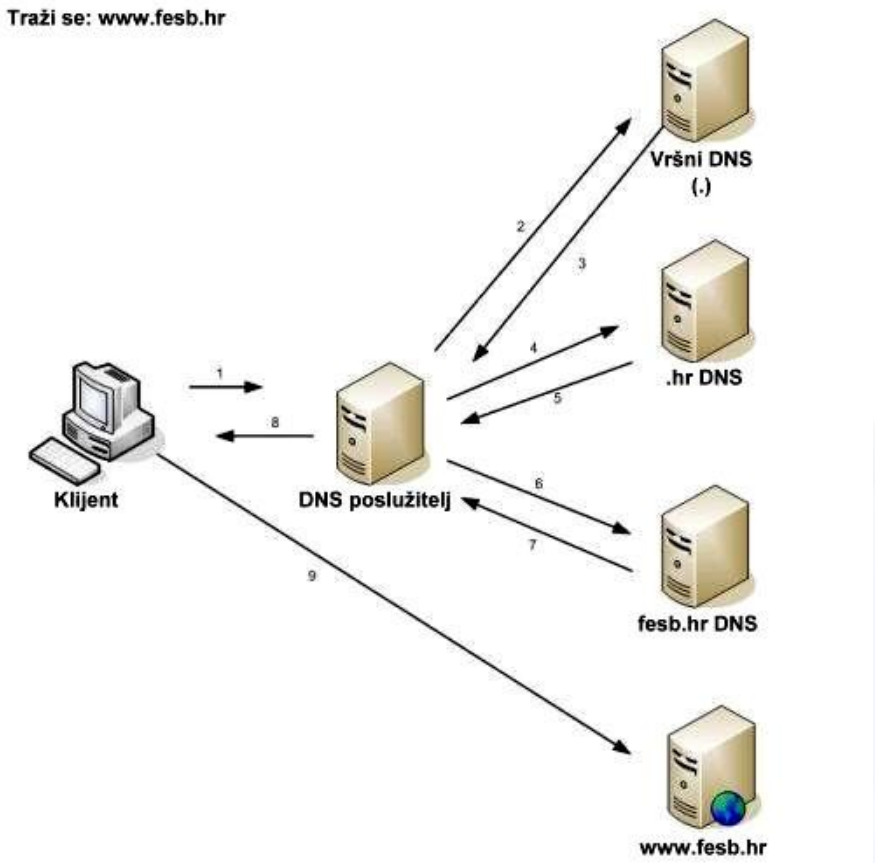
1. **DNS klijent** (eng. *resolver*) - program koji se izvršava na klijentskom računalu i koji formira određeni DNS zahtjev.
2. **Rekurzivni DNS poslužitelj** (eng. *recursive*) - poslužitelj koji nakon dobivenih upita za klijenta obavlja pretraživanje kroz DNS stablo i vraća odgovore natrag klijentima.
3. **Autoritativni DNS poslužitelj** (eng. *authoritative*) - poslužitelj koji odgovara na upite rekurzivnih poslužitelja te vraća ili završni odgovor ili, zbog delegiranja. referencu na neki drugi autoritativni DNS poslužitelj.

Proces primanja zahtjeva, obrade zahtjeva i vraćanja rezultata naziva se DNS razrješenje. Svaka potraga za nekom informacijom kreće od vrha DNS stabla. Prolazak kroz DNS stablo jest silazak po granama stabla gdje je svaki čvor jedan poslužitelj nadležan za svoj dio prostora. Dakle, DNS stablo je zapravo hijerarhijski skup DNS poslužitelja gdje svaka domena i poddomena ima jednog ili više autoritativnih DNS poslužitelja.

Postoje dva tipa obilaska DNS stabla:

1. **Iterativni** - Klijent šalje upite, a poslužitelj odgovara ili odgovorom na zahtjev ili imenom drugog DNS poslužitelja koji ima više podataka o traženom upitu.

2. **Rekurzivni** - Klijent šalje rekurzivni upit, poslužitelj preuzima posao pronalaženja informacija o traženom upitu Poslužitelj obrađuje informacije i šalje nove upite drugim poslužiteljima sve dok ne sazna informaciju koju traži. Dakle, klijent šalje svega jedan zahtjev te dobiva ili točnu informaciju koju je tražio ili poruku o grešci. Proces je prikazan na slici 3.



Slika 3. DNS razrješavanje rekurzivnim obilaskom
Izvor: Računalne mreže | Eldis Mujarić, dipl. ing.

2.2.5. DNS međuspremnik

Način pretraživanja DNS stabla prikazan u prethodnom podpoglavlju smatra se neučinkovitim, budući da se za svaki upit nanovo prolazi kroz DNS stablo. Time se poslužitelj previše opterećuje, a samo pretraživanje predugo traje.

U praksi se pokazalo da se često šalju isti ili slični DNS upiti u vremenski bliskim periodima, pa se problem predugog pretraživanja riješio dodavanjem međuspremnika. Većina rekurzivnih DNS poslužitelja danas ima interne međuspremnike u koje pohranjuju informacije o nedavnim DNS upitima. Svaki podatak u međuspremniku ima svoje "vrijeme života" ili TTL (eng. *Time To Live*) čime se osigurava da zastarjeli podaci nestaju iz spremnika i ne zauzimaju bespotrebno memoriju. Prekratko vrijeme života znači intenzivno osvježavanje podataka i zagušenje mreže, dok predugo vrijeme života onemogućuje osvježavanje podataka pa je potrebno pronaći sredinu između te dvije krajnosti. [2]

2.3. Sigurnosni problemi DNS protokola

Iako DNS sustav nudi brojne prednosti i olakšava korisnicima svakodnevnu upotrebu Interneta, uz njega su vezani i brojni sigurnosni problemi. Na sigurnost DNS sustava mogu utjecati brojne

stvari: starije inačice operacijskih sustava, ne-periodična nadogradnja programa na posljednje inačice istih, pogrešne postavke poslužitelja itd.

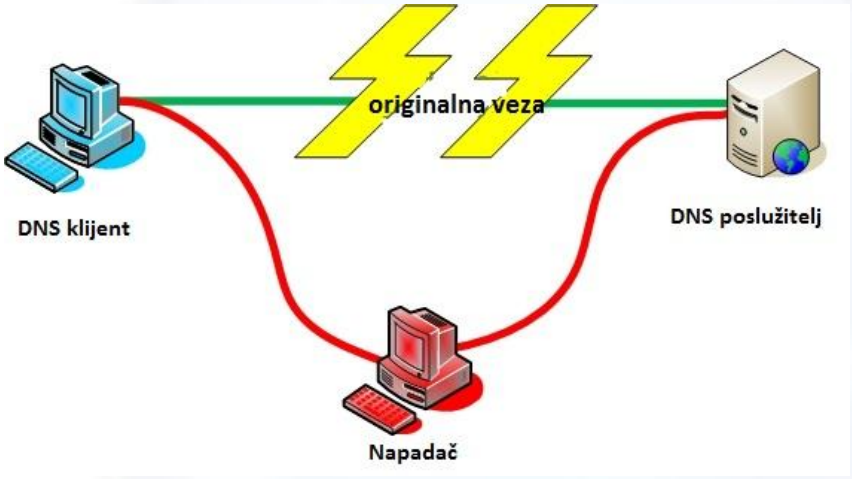
U ovom poglavlju navedeno je samo nekoliko sigunosnih problema DNS sustava. Naime, DNS sustav originalno nije uključivao sigurnost, budući da je pri njegovu stvaranju naglasak bio na skalabilnosti raspodijeljenog sustava. Sigurnosne ekstenzije DNS sustava nastoje dodati sigurnost DNS sustavima. O njima će više riječi biti u sljedećem poglavlju.

2.3.1. Presretanje paketa i napad identifikacijom

Ako napadač može prisluškivati (eng. *sniff*) promet na mreži koju koristi DNS klijent, onda može presretati DNS pakete kao i iskoristiti tu mogućnost za izvođenje napada "čovjek-u-sredini" (eng. *man in the middle*), kao što to prikazuje slika 4.

Jednom kada se napadač nalazi između DNS klijenta i DNS poslužitelja, on može presretati upite poslane DNS poslužitelju. Također, omogućeno mu je da se predstavlja kao DNS poslužitelj pa će DNS klijent vjerovati da svi paketi koje primi od napadača zapravo dolaze od DNS poslužitelja kojem je poslao upit.

Pri tom je pravi DNS poslužitelj ili žrtva napada uskraćivanjem usluge (eng. *Denial of Service attack, DoS*) ili se napadač jednostavno nalazi bliže klijentu od DNS poslužitelja. [3]



Slika 4. Napad "čovjek-u-sredini"
Izvor: OWASP (The Open Web Application Security Project)

Da bi se predstavljao kao DNS poslužitelj, napadač se ne mora nužno nalaziti između DNS klijenta i DNS poslužitelja. U tom slučaju napadač mora predvidjeti 16 bitni identifikacijski broj upita DNS klijenta. Budući da se komunikacija između DNS klijenta i DNS poslužitelja odvija putem nekriptiranih UDP[7](eng. *User Datagram Protocol*) paketa, nije teško preslušati (eng. *sniff*) nekoliko paketa i pretpostaviti sljedeći identifikacijski broj. S druge strane, nekada ni prisluškivanje paketa nije potrebno za uspješno pogađanje identifikacijskog broja, budući da se sa što većim brojem istovremenih DNS upita koje DNS poslužitelj obrađuje, vjerojatnost uspješnog pogađanja identifikacijskog broja povećava (jer postoji samo 2^{16} mogućih kombinacija).

Cilj oba ovdje spomenuta napada jest prikupiti informacije kako bi se olakšao napad trovanjem DNS međuspremnika. [3]

[7] UDP (eng. *User Datagram Protocol*) je protokol koji se nalazi u dijelu transportne razine OSI modela, te je jedan od temeljnih Internet protokola. Spada u skupinu bespojnih protokola.

2.3.2. Trovanje DNS međuspremnika

Napad trovanjem DNS međuspremnika (eng. *cache poisoning*) predstavlja ozbiljnu prijetnju sigurnosti DNS sustava. Ovaj napad se izvodi nakon napada opisanih u prethodnom podpoglavlju. Naime, nakon što se napadač ubaci u komunikaciju između DNS klijenta i poslužitelja (ili između rekurzivnog i autoritativnog DNS poslužitelja), te "utiša" DNS poslužitelj kojem je upit upućen, može odgovoriti na klijentov upit i time dodati informaciju u klijentov međuspremnik. Klijent može iskoristiti tu zlonamjernu informaciju budući da vjeruje da je odgovor stigao od pravog DNS poslužitelja. Ako se napadač ubacio između dva DNS poslužitelja, lažni podaci bit će spremljeni u međuspremnik poslužitelja koji je uputio upit, i svi sljedeći isti upiti upućeni prevarenom poslužitelju dobit će lažan odgovor iz njegova međuspremnika.

Ova metoda lažiranja DNS zapisa rezultira time da se nesvijesni klijenti preusmjeravaju na lažne adrese i time postaju laka meta napadačima.

2.3.3. Napad uskraćivanjem usluge

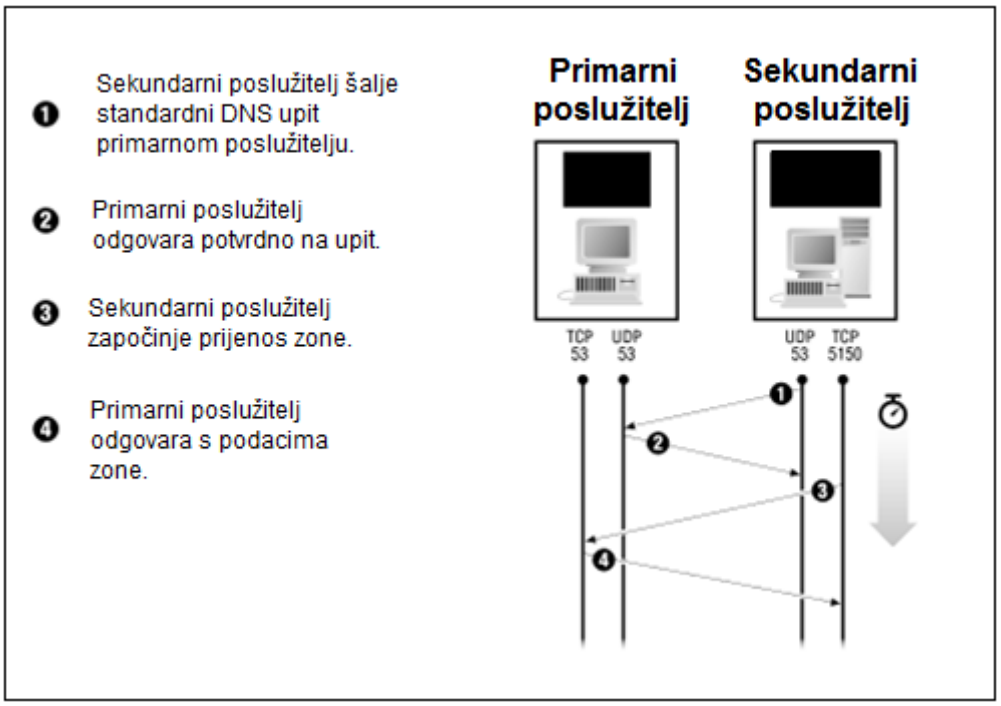
DNS sustav napadači često koriste za izvođenje DoS napada, budući da su odgovori DNS poslužitelja uglavnom veći od primljenih upita. Zbog toga napadač može iskoristiti DNS poslužitelj za umnažanje kako bi izveo napad uskraćivanjem usluge usmjeren protiv drugih mreža ili računala. [3]

2.3.4. Krađa zone

Zona je dio neke domene ili cijela domena. Za svaku zonu postoji DNS poslužitelj koji je zadužen za nju i koji se naziva primarni poslužitelj. Ostali poslužitelji u toj zoni koji podatke o zoni ne čuvaju kod sebe, nego ih primaju od primarnog poslužitelja nazivaju se sekundarni poslužitelji. Sama replikacija podataka, odnosno prijenos zone započinje standardnim DNS upitom (dakle UDP). Na dobiveni zahtjev DNS poslužitelj u slučaju da klijent ima dozvolu odgovara potvrdno, te se klijent ponovno spaja - ovaj put radi pouzdanosti ostvaruje TCP[8](eng. *Transmission Control Protocol*) vezu i prenosi čitavu zonu kroz istu vezu, zatvarajući je po završetku. Nakon toga dotični sekundarni poslužitelj odbacuje svoje stare podatke i učitava nove, ponavljajući proces kako je definirano vremenom osvježavanja. Prijenos zone prikazan je na slici 5.

Ako se lažni DNS poslužitelj uspije predstaviti kao sekundarni poslužitelj i zatraži prijenos podataka o zoni od primarnog poslužitelja govori se o krađi zone. Naime, ti podaci mogu se iskoristiti za daljnje napade, kao na primjer za trovanje DNS međuspremnika DNS klijenata i drugih DNS poslužitelja i slično. [3]

[8] TCP (eng. *Transmission Control Protocol*) je jedan od osnovnih protokola unutar IP grupe protokola, a spada u skupinu spojnih protokola.



Slika 5. Prijenos zone
Izvor: Building Internet Firewalls, Chapter 8

2.3.5. Sigurnosna ranjivost Microsoft Windows DNS klijenata

Sustavi na kojima su instalirani sustavi Windows 98, NT, 2000 ili XP osobito su ranjivi na napade budući da DNS klijent na ovim operacijskim sustavima prihvaća odgovore s bilo koje IP adrese. To znači da bilo koji poslužitelj može odgovoriti na upit i odgovor će biti prihvaćen dok god je u ispravnom formatu i ima ispravan identifikacijski broj. [3]

3. Sigurnosne ekstenzije DNS sustava

Sigurnosne ekstenzije DNS sustava ili skraćeno DNSSEC dodaju komponentu sigurnosti DNS sustavima i trenutno obavljaju tri funkcije:

1. osiguravanje sigurnog prijenosa zone,
2. sigurno ažuriranje zapisa zone i
3. očuvanje integriteta zone.

DNSSEC je u svom sadašnjem obliku dostupan još od 2003. godine, dok je formalno standardiziran 2005. godine. Standardizirala ga je organizacija IETF[9] (eng. *Internet Engineering Task Force*). [4]

3.1. Razlog nastanka sigurnosnih ekstenzija DNS sustava

Iako je u prethodnom poglavlju spomenuto nekoliko sigurnosnih problema s kojima se susreće DNS sustav, u ovom poglavlju će se pokušati dati detaljniji pregled problema koji je doveo do pojave DNSSEC-a.

[9] IETF je otvorena organizacija za standardizaciju koja razvija i promiče internet standarde.

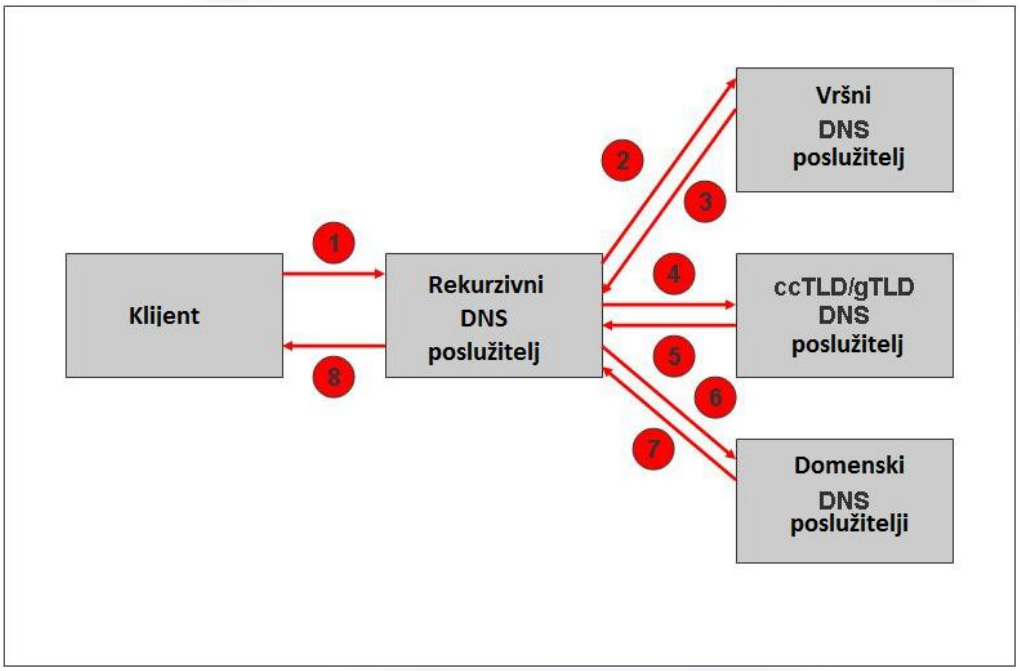
Kada korisnik spojen na Internet želi pristupiti nekoj usluzi ili resursu kao što je Internet stranica, ili želi poslati poruku putem elektroničke pošte, danas koristi simboličko ime povezano uz tu uslugu ili resurs, npr. *google.com*.

No, mreže u svom radu ne koriste simbolička imena, nego IP adrese. Stoga je prvi korak u pristupanju željenoj usluzi ili resursu slanje DNS upita putem kojeg se saznaje IP adresa koja je povezana s danim simboličkim imenom.

Sam postupak dohvaćanja odgovora na poslani DNS upit može biti dosta složen. Željeni rezultat tog upita je točna i valjana IP adresa dobivena od autoritativnog poslužitelja zone u kojoj se nalazi tražena usluga ili resurs. Adresa se također može dobiti i od poslužitelja koji se nalazi između DNS klijenta i autoritativnog poslužitelja, a koji koristi međuspremnik i ima traženu adresu pohranjenu i njemu u trenutku stizanja upita. Pojednostavljena verzija ovog procesa je prikazana na slici 5.

Nažalost, svaka strelica sa slike 5. može biti kompromitirana. I time cijeli pokušaj pristupa nekoj usluzi ili resursu postaje kompromitiran. Naime, iako HTTPS[10](eng. *Hypertext Transfer Protocol Secure*) i SSL[11](eng. *Secure Sockets Layer)* certifikati omogućuju sigurnost na mreži, u ovom slučaju su nemoćni budući da je DNS razrješenje prvi korak. A ako je odgovor koji se dobije DNS razrješavanjem oštećen ili namjerno izmjenjen, tada se daljnjim koracima nikada ne pristupa pravoj usluzi koja je zatražena i time HTTPS i SSL certifikati nemaju nikakav utjecaj. [5]

Sigurnosne ekstenzije DNS sustava omogućuju da korisnik bude siguran da je dobio ispravnu IP adresu od DNS poslužitelja i da je dobio upravo uslugu ili resurs koji je i zatražio.



Slika 6. Pojednostavljeni primjer DNS upita i odgovora
Izvor:Ron Aitchison - Choosing a DNSSEC solution

3.2. Ciljevi sigurnosnih ekstenzija DNS sustava

Sigurnosne ekstenzije DNS sustava imaju 3 cilja [5]:

1. autentifikacija izvora podataka,
2. integritet podataka i
3. dokaz o nedostupnosti (eng. *Proof of Non-Existence*, PNE).

[10] HTTPS (eng. *Hypertext Transfer Protocol Secure*) je komunikacijski protokol namijenjen sigurnoj komunikaciji preko računalne mreže.

[11] SSL (eng. *Secure Sockets Layer*) je transportni protokol koji omogućava sigurnu komunikaciju preko Interneta za razne aplikacije, npr. elektroničku poštu, Internet preglednike itd

Pod pojmom autentifikacije izvora podataka podrazumijeva se da postoji čvrsti dokaz da primljeni DNS podaci potječu od autoritativnog poslužitelja za traženu domenu.

S druge strane, korištenjem DNSSEC-a može se dokazati da su podaci koje DNS klijent primi jednaki podacima koje je autoritativni DNS poslužitelj poslao kao odgovor na poslani upit. Taj integritet podataka očuvan je i u situacijama kada između autoritativnog DNS poslužitelja i DNS klijenta postoji rekurzivni poslužitelj s međuspremnikom.

Treći cilj sigurnosnih ekstenzija DNS sustava jest sprječavanje napada u kojima napadač klijentu kao odgovor na poslani upit javlja da tražena IP adresa ne postoji. Korištenjem DNSSEC-a je moguće dokazati da je pristigli odgovor o nepostojanju tražene usluge ili resursa ispravan i da potječe od autoritativnog DNS poslužitelja za tu domenu.

3.3. Način rada sigurnosnih ekstenzija DNS sustava

Rad sigurnosnih ekstenzija DNS sustava temelji se na upotrebi kriptografskog procesa povezanog s procesom povjerenja (eng. *trust process*).

Zona zaštićena DNSSEC-om ima svoj digitalni potpis[12]. Zona se potpisuje korištenjem asimetričnog kriptosustava. Ti sustavi temelje se na korištenju tajnog ključa koji je poznat samo vlasniku i javnog ključa, koji je javno poznat i koristi se za dešifriranje podataka šifriranih tajnim ključem. Time se omogućuje autentifikacija izvora podataka, budući da samo on poznaje svoj tajni ključ, samo je on mogao poslati dobivene podatke.

Da bi rad DNSSEC sustava bio moguć, stvoreni su dodatni tipovi DNS podataka [4]:

- RRSIG (eng. *Resource record signature*) - koristi se kao DNSSEC potpis za skup podataka zaštićenih sigurnosnim ekstenzijama DNS sustava,
- DNSKEY (eng. *DNS Key record*) - DNS zapis koji sadrži kriptografske ključeve koji se koriste za potpisivanje zapisa zone,
- DS (eng. *Delegation signer*) - zapis koji se koristi za utvrđivanje DNSSEC ključa potpisivanja delegirane zone,
- NSEC (eng. *Next-Secure record*) - zapis čija je uloga pružanje dokaza da traženo domensko ime ne postoji,
- NSEC3 (eng. *NSEC record version 3*) - poboljšani oblik NSEC zapisa, s većom pouzdanošću i
- NSEC3PARAM (eng. *NSEC3 parameters*) - zapis koji sadrži parametre potrebne za rad NSEC3 zapisa.

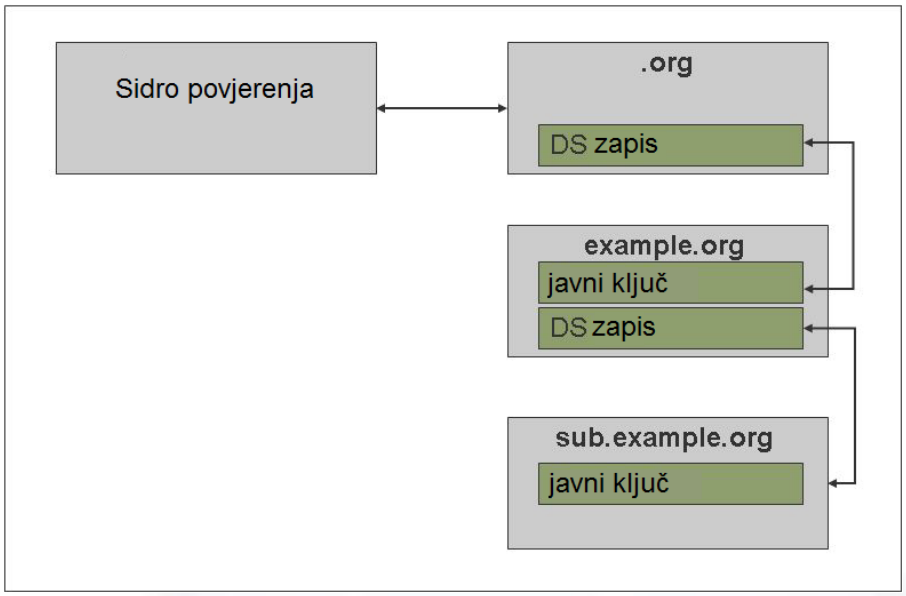
Svaki odgovor na DNS upit sadrži RRSIG zapis kao dodatak zatraženom podatku. To je zapravo digitalni potpis odgovora kojeg šalje DNS poslužitelj. Verifikacija digitalnog potpisa obavlja se korištenjem odgovarajućeg javnog ključa koji se nalazi u DNSKEY zapisu. DS zapis koristi se pri autentifikaciji DNSKEY-ja putem lanca povjerenja (eng. *trust chain*) o kojem će riječi biti nešto kasnije. Preostala tri tipa DNS podataka (NSEC, NSEC3 i NSEC3PARAMS) koriste se pri dokazivanju nedostupnosti.

Na izlazu prvog koraka u radu DNSSEC-a nastaje potpisani DNS odgovor s pridruženim javnim ključem. Ali, da bi korisnik mogao vjerovati informaciji koju je primio tim odgovorom, mora moći vjerovati izvoru pridruženog javnog ključa. To se omogućuje drugim korakom u radu DNS sustava, takozvanim procesom povjerenja.

Proces povjerenja omogućuje primatelju DNS zapisa da slijedi javne ključeve sve do "sidra povjerenja" (eng. *trust anchor*). To su u principu javni ključevi domena u DNS hijerarhiji koji su dobiveni putem nekog izvora koji nije DNS, čime se osigurava veća sigurnost cijelog sustava. Spomenuta sidra se obično dohvaćaju preko operacijskog sustava ili nekog drugog povjerljivog izvora. [5]

Pri procesu praćenja javnih ključeva potrebno je prolaziti kroz lanac povjerenja u kojem svaka roditeljska zona sadrži DS zapis kojim se potvrđuje valjanost određenog javnog DNS ključa. Prolaženjem kroz lanac u jednom trenu se dolazi do sidra povjerenja koje odgovara imenu promatrane zone. Proces korištenja lanca povjerenja prikazan je na slici 6.

[12] Digitalni potpis - metoda kojom se osigurava integritet podataka te koja se koristi za provjeru autentičnosti sudionika u internet komunikaciji.



Slika 7. Proces korištenja lanca povjerenja
Izvor:Ron Aitchison - Choosing a DNSSEC solution

3.4. Složenost DNSSEC-a

U prethodnom poglavlju dan je pojednostavljeni način rada sigurnosnih ekstenzija DNS sustava. Ipak, u stvarnosti je riječ o vrlo kompleksnoj tehnologiji. U ovom poglavlju dat će se pregled nekoliko važnih procedura uz koje se vežu problemi, a koje su potrebne za funkcioniranje sigurnosnih ekstenzija DNS sustava. [5]

1. **Promjena zone**

   Svaki put kada se nešto u zoni promjeni, potrebno ju je ponovo potpisati. Pri potpisivanju zone privatni ključevi trebaju biti na mreži (eng. *on-line*), što predstavlja sigurnosni problem.

2. **Periodičko ponovno potpisivanje**

   Potpisi zona imaju vremenska ograničenja. Zbog toga je, čak i ako se zona nije mijenjala, potrebno provesti novo potpisivanje zone prije nego vremensko ograničenje starog potpisa istekne.

3. **Višestruki ključevi**

   Iako je moguće koristiti DNSSEC samo s jednim ključem, većina sustava koristi barem dva. Svaki ključ ima vlastitu ulogu pri potpisivanju i zahtjeva redovito održavanje, pri čemu se sami procesi održavanja mogu razlikovati za različite ključeve.

4. **Održavanje ključeva** (eng. *key maintenance or key rollover)*

   Iz sigurnosnih razloga potrebno je periodički mijenjati ključeve koji se koriste za potpisivanje. Budući da je DNS sustav globalan, a koristi i međuspremnike, potrebno je uvesti nove ključeve u sustav nešto prije samog potpisivanja. Stari ključevi se isključuju iz upotrebe nakon kraćeg vremena od prestanka njihovog korištenja. Zbog te specifičnosti sustava, u nekom trenutku u sustavu se istodobno mogu naći novi ključ, trenutni ključ i prethodni ključ, što pridonosi složenosti održavanja sustava.

5. **Lanac povjerenja**

   Prilikom promjene ključeva potrebno je propagirati tu informaciju kroz lanac povjerenja. Kako se sustav sastoji od puno domena, a svaka ima svoje ključeve i može biti dio lanca povjerenja nekoliko drugih poddomena, pojavljuje se potreba da se propagacija informacija obavlja što brže i u što kraćem roku.

Budući da se DNSSEC oslanja na proces povjerenja, veliki naglasak se postavlja na pažnju kojom se rukuje privatnim ključevima. Naime, ako je jedan ili više ključeva koji se koriste za potpisivanje domene kompromitiran (tj. ukraden od strane zlonamjernog korisnika), zlonamjeni korisnik može učiniti veliku štetu prije nego se krađa uopće primjeti. Stoga je, uz već spomenuto održavanje ključeva, sigurno upravljanje tajnim ključevima osnova uspješnog DNSSEC korištenja.

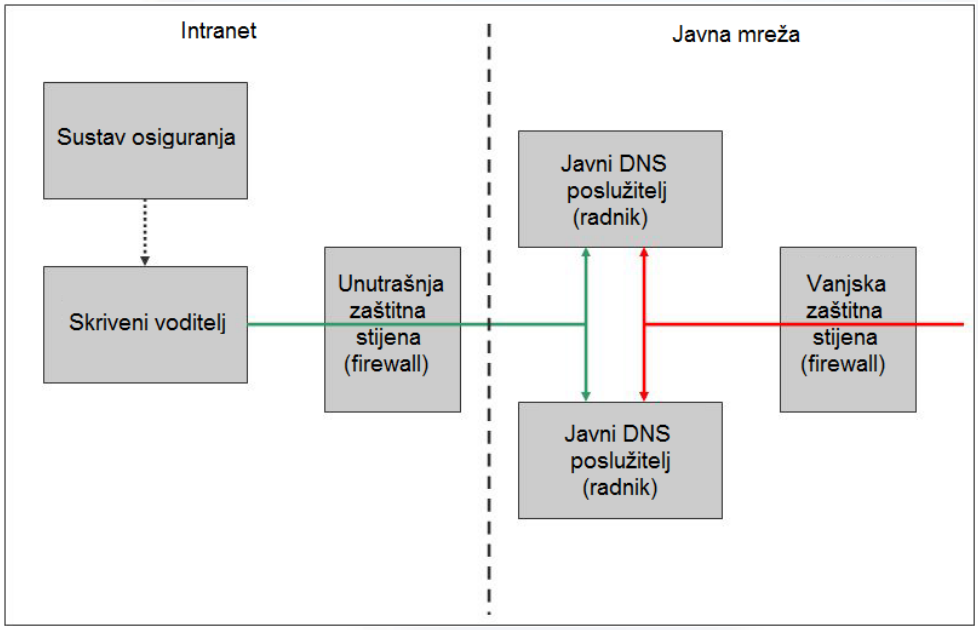
6. **Skriveni voditelj** (eng. *Hidden master*)

   Iz sigurnosnih razloga tajni ključevi nikada ne smiju biti pohranjeni na javnom poslužitelju. Zbog toga se u rad DNS sustava s DNSSEC-om uvodi dodatni poslužitelj nazvan skriveni voditelj čija je uloga potpisivanje zone. Datoteke zone potpisane na skrivenom voditelju prenose se na javne DNS poslužitelje radnike (eng. *DNS slave servers*). Arhitektura skrivenog voditelja prikazana je na slici 7.

7. **Ključevi na mreži**

   Čak i pri korištenju konfiguracije skrivenog voditelja potreban je veliki oprez pri rukovanju ključevima. Ostavljanje privatnih ključeva *on-line* unutar normalnog datotečnog sustava cijelo vrijeme predstavlja prijetnju sigurnosti. Umjesto toga, ključevi bi trebali bit prisutni samo pri potpisivanju i automatski se sigurno pohraniti pri završetku procesa potpisivanja.

   Ovaj problem postavlja dodatne zahtjeve na DNSSEC implementaciju, osobito ako se zone često mijenjaju. Tada se ključevi često koriste pa su često prisutni na mreži. Ako je to slučaj, jedino sigurno rješenje je korištenje nekog HSM (eng. *hardware security module*)[13] modula pomoću kojega ključevi nikada nisu izloženi.



Slika 8. Konfiguracija skrivenog voditelja
Izvor: Ron Aitchison - Choosing a DNSSEC solution

[13] Slopovski sigurnosni moduli (eng. *hardware security module*) ili skraćeno HSM moduli su vrsta sigurnih kriptoprocesora čiji je cilj upravljanje ključevima te ubrzanje kriptografskih procesa kao što su digitalni potpisi, provjere valjanosti i integriteta prilikom pristupa ključevima poslužiteljskih aplikacija itd.

3.4.1. Ključevi u DNSSEC-u

Sigurnosne ekstenzije DNS sustava imaju jednu glavnu zadaću - osigurati sigurnost DNS sustava. Kao što je pokazano u prethodnom tekstu, za obavljanje ove zadaće DNSSEC koristi asimetrični sustav za šifriranje. Vitalni dio tih sustava predstavlja tajni ključ korisnika. U DNSSEC-u postoje 2 vrste ključeva koje se koriste. To su [4]:

- KSK (eng. *Key Signing key*) ključ i
- ZSK (eng. *Zone Signing key*) ključ.

Dvije vrste ključeva su u upotrebi kako bi se osigurao što veći stupanj sigurnosti sustava. Naime, kriptografski ključevi se s vremenom mogu kompromitirati, što u ovom slučaju znači da napadač može korištenjem nekih metoda saznati ili pogoditi tajni ključ kojim se potpisuju DNS zapisi, čime se narušava sigurnost koju bi DNSSEC trebao nuditi korisnicima.

Zbog toga DNSSEC koristi ZSK, čije je vrijeme upotrebe kratkotrajno, kako bi periodički potpisivao DNS zapise. Za potpisivanje samih ZSK ključeva, čime se omogućava njihova provjera valjanosti, koriste se KSK ključevi, čije je vrijeme upotrebe duže.

Naime, ZSK ključevi se često mijenjaju kako bi se otežalo njihovo pogađanje i time smanjila vjerojatnost napada. S druge strane, KSK ključevi se mijenjaju dosta rjeđe (otprilike svakih godinu dana). Budući da oni potpisuju ZSK, a ZSK potpisuje DNS zapis, u stvari je za provjeru valjanost DNS zapisa bitan samo KSK.

I upravo se samo KSK u formi DS zapisa prosljeđuje roditelju u lancu povjerenja, koji potpisuje DS zapis svojim KSK ključem. Njegov KSK ključ potpisan je njegovim ZSK ključem i tako dalje sve prema vrhu, gdje se nalazi već prije spomenuto sidro povjerenja.

4. DNSSEC alati

Implementacija sigurnosnih ekstenzija DNS sustava zahtijeva dodatnu programsku podršku i na strani klijenta i na strani poslužitelja. Danas postoji velik broj i komercijalnih alata i alata otvorenog koda (eng. *open source*) koji omogućuju implementaciju sigurnosnih ekstenzija DNS sustava. Neki od poznatijih su navedeni u nastavku. [4]

- **Windows 7 i Windows Server 2008 R2**

  Ovi operacijski sustavi, proizvodi tvrtke Microsoft Windows, dolaze s podrškom za DNSSEC i omogućuju razlikovanje sigurnih i nesigurnih odgovora primljenih od rekurzivnog DNS poslužitelja.

- **BIND**

  BIND je najkorišteniji DNS program na Internetu i njegove najnovije inačice uključuju i DNSSEC.

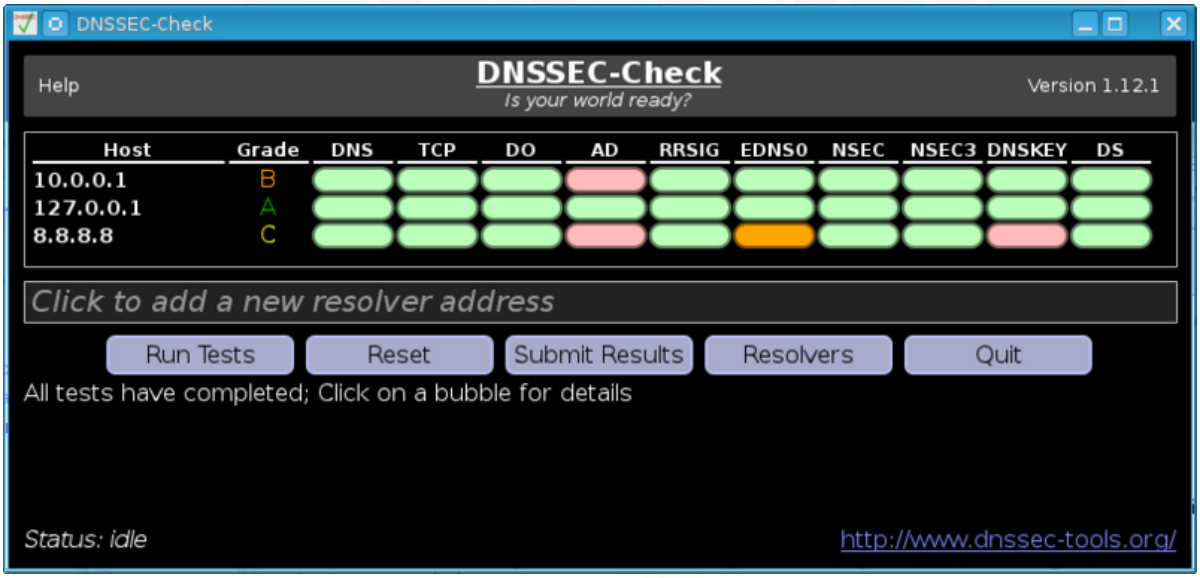
- **Idns**

  Idns je proizvod tvrtke NLnetLabs koji također nudi potporu za DNSSEC procese potpisivanja i provjere valjanosti.

- **DNSSEC-Tools**

  U posljednje vrijeme DNSSEC-Tools je postigao veliku popularnost među korisnicima. Riječ je o alatu otvorenog koda koji nudi velik izbor različitih programskih biblioteka i alata koji olakšavaju instalaciju i upotrebu sigurnosnih ekstenzija DNS sustava.

  Na slici 9. prikazano je sučelje jedne od aplikacija koju nudi DNSSEC-Tools. Riječ je o aplikaciji DNSSEC-Check koja omogućuje korisniku da provjeri koliko su sigurnosne ekstenzije DNS sustava podržane u nekom sustavu.



Slika 9. Izgled sučelja DNSSEC-Check alata
Izvor: Wikipedia, DNSSEC-Check

- **Zone Key Tool**

  Zone Key Tool je alat namijenjen korištenju u sredinama s manjim do srednjim brojem zona. Omogućuje automatsko mijenjanje ključeva zona kao i automatsko ponovno potpisivanje zona.

- **Unbound**

  Unbount je također proizvod tvrtke NLnetLabs. To je zapravo rekurzivni DNS poslužitelj s međuspremnikom koji omogućuje provjeru valjanosti DNS zapisa koje prima.

- **OpenDNSSEC**

OpenDNSSEC je nastao kao rješenje problema čestog mijenjanja zona, kada ključevi stalno moraju biti dostupni u sustavu. Naime, OpenDNSSEC prima nepotpisanu zonu, dodaje digitalni potpis i ostale potrebne DNS zapise i prosljeđuje potpisanu zonu autoritativnom DNS poslužitelju. Svi ključevi se čuvaju u HSM modulu i pristupa im se pomoću PKCS#11 sučelja.

Odabir alata uvelike ovisi o zahtjevima samih korisnika. Ipak, osnovne dvije karakteristike koje treba uzeti u obzir su razina automatiziranosti i razina upravljanja ključevima. Razlog zbog kojeg DNSSEC postoji jest zaštita i povjerenje, što se na kraju svodi na zaštitu privatnih ključeva. Ako alat kojeg koristimo ima slabo razvijen taj segment DNSSEC-a, npr. korisnik mora ručno upravljati ključevima, kontrola pristupa privatnim ključevima je loše izvedena i slabo se provodi, nije podržana arhitektura skrivenog voditelja itd., najčešće je riječ o slabom DNSSEC alatu. [5]

Druga spomenuta karakteristika koju je poželjno uzeti u obzir pri odabiru DNSSEC alata jest DNSSEC automatizacija. Naime, DNSSEC uključuje velik broj redovitih procesa koje je potrebno obaviti za očuvanje sigurnosti sustava, a uz to se često događa da je vrijeme u kojem se svi ti procesi moraju obaviti dosta ograničeno ili izuzetno kratko (npr. pri krađi ključeva). Zbog toga je poželjno imati sustave koji su dosta automatizirani, čime se smanjuje i mogućnost da čovjek slučajno napravi pogrešku pri obavljanju tih poslova i time dovede sigurnost sustava u opasnost.

Iako je idealno rješenje DNSSEC alat koji nudi i dobro upravljanje ključevima i dobru automatizaciju, to ponekad nije praktično rješenje pa je potrebno u obzir uzeti i neka druga.

Ako je potrebno birati između dobre automatizacije i dobrog upravljanja ključevima, preporuča se odabrati sustav s dobrim upravljanjem ključeva, budući da je uvijek lakše proširiti znanje o DNSSEC-u i obaviti neki posao umjesto računala, nego saznati o krađi ključeva kada je već prekasno. [5]

5. Problemi i budućnost

Sigurnosne ekstenzije DNS sustava, kao i sve nove Internet tehnologije, predstavlja nešto novo i zahtjeva nove, drugačije rutine za održavanje. Također, korist koja bi se trebala dobiti korištenjem DNSSEC-a se ne može osjetiti preko noći. Alati za implementaciju su još uvijek u fazi razvoja, a sam sustav je dosta složen i zahtjeva dobro poznavanje problematike te je sklon greškama.

Stoga se postavlja pitanje kada implementirati DNSSEC - odmah, ili još malo pričekati da se sustav razvije. Odgovor na to pitanje nije jednostavan. Naime, trebalo bi se pripremiti za DNSSEC već sada, a zatim čekati da se proizvođači ključeva u potpunosti prilagode DNSSEC-u te da i ostatak industrije postane spreman.

Također, DNSSEC još uvijek nije za sve korisnike. Budući da je implementacija DNSSEC-a relativno skupa i vremenski zahtjevna, implementacija se za sada obavezno preporuča onim poduzetnicima koji mogu mnogo izgubiti zbog napada trovanjem međuspremnika. Pod takve organizacije spadaju sve one koje koriste podatke za prijavu (eng. *login credentials*), financijske informacije, povjerljive podatke itd.

Organizacije koje implementiraju DNSSEC zasada neće osjetiti veliku korist, budući da je za sigurnost cijele DNS komunikacije potrebno da svi DNS poslužitelji u hijerarhiji nekog zahtjeva omogućuju DNSSEC, što, zasada, još nije slučaj.

S druge strane, danas je već dosta vršnih domena implementiralo DNSSEC. Neke od njih su .org, .com, .net, kao i geografske domene .br (Brazil), .bg (Bugarska), .se (Švedska), itd.

Od studenog 2011. godine više od 25% vršnih domena koristi DNSSEC, a taj broj je u porastu. [4]

Budući da DNSSEC rješava problem sigurnosti DNS sustava, zasigurno predstavlja pravi put usprkos trenutnim nedostacima. Bez sigurnosnih ekstenzija DNS sustava banke, *on-line* trgovine, vlade i obični korisnici računala biti će i dalje podložni prijetnjama s kojima se DNS sustav ne može nositi niti je namijenjen da ih spriječava. Bez metode za provjeru valjanosti informacija pronađenih u DNS poslužiteljima, napadačima se olakšava posao. Zbog svega nabrojenoga znanstvenici se slažu u zaključku da su sigurnosne ekstenzije DNS sustava budućnost. I da će korak po korak postajati sastavni dio Interneta sve dok se jednog dana korisnici ne okrenu unatrag i upitaju kako su uopće mogi živjeti bez njih. [3]

6. Zaključak

DNS sustav je jedan od ključnih elemenata koji su omogućili da se Internet razvije u ovo što je danas. DNS sustav se koristi u skoro svim interakcijama koje koriste simbolička imena umjesto IP adresa i bez njega bi takva Internet komunikacija bila otežana ili uopće ne bi postojala.

Ipak, pri nastanku DNS sustava nije se razmišljalo o sigurnosti. U vrijeme kada je DNS sustav nastao, prije više od 30 godina, okruženje za koje je nastao bilo je drugačije, puno manje i puno sigurnije.

Nažalost, danas je situacija drugačija. Međuspremnici koji se koriste u DNS sustavima postali su meta napada zlonamjernih korisnika. Ti napadi mogu biti iskorišteni u različite opasne svrhe, a DNS sustav je jedan od središnjih dijelova Interneta i nije ga moguće lako zamijeniti. Zbog toga se razvila potreba za sredstvom koje će omogućiti daljnju upotrebu DNS sustava, ali s povećanom dozom sigurnosti.

Stoga su razvijene sigurnosne ekstenzije DNS sustava čija je zadaća spriječiti napadače u iskorištavanju ranjivosti DNS sustava. Dvije najpoznatije ranjivosti DNS sustava koje DNSSEC nastoji ukloniti su ranjivosti na napad trovanjem međuspremnika i napad uskraćivanjem usluge. DNSSEC ih nastoji ukloniti omogućavanjem provjere autentičnosti i integriteta odgovora koji dolazi od DNS poslužitelja.

Nažalost, zbog raspodijeljene prirode DNS sustava, DNSSEC je potrebno implementirati na velikom broju DNS poslužitelja da bi njegova korist došla do izražaja. Zbog toga projekt uvođenja sigurnosnih ekstenzija DNS sustava u uporabu ne spada u kategoriju programa koji brzo vraćaju svoja ulaganja. Ali, ako se uspije ostvariti, u konačnici će rezultirati velikom dobiti za sve korisnike Interneta, jer će značajno pridonijeti sigurnosti svih korisnika na Internetu.

Zbog toga uvođenjem sigurnosnih ekstenzija DNS sustava u svoje okruženje organizacije ne štite samo sebe i korisnike svojih podataka, već pomažu u izgradnji globalno sigurnog sustava.

7. Leksikon pojmova

DNS

DNS (*eng. Domain Name System*) je distribuirani hijerarhijski sustav Internet poslužitelja u kojem se nalaze informacije povezane s domenskim nazivima, tj. o povezanosti IP adresa i njihovih logičkih (simboličkih) imena.

http://hr.wikipedia.org/wiki/DNS

Domensko ime

Domensko ime je simboličko ime računala na internetu koje ga najčešće jednoznačno identificira (postoji mogućnost da više računala dijeli jedno domensko ime). Domensko ime sastoji se od jedne ili više labela, odvojenih točkama, npr. *primjeri.com*.

http://www.scribd.com/doc/48742258/DNS-prirucnikkuharica

DNSSEC (Sigurnosne ekstenzije DNS sustava)

Sigurnosne ekstenzije DNS sustava (eng. *Domain Name System Security Extensions*) ili skraćeno DNSSEC dodaju komponentu sigurnosti DNS sustavima i trenutno obavljaju tri funkcije: osiguravanje sigurnog prijenosa zone, sigurno ažuriranje zapisa zone i očuvanje integriteta zone.

DNSSEC je u svom sadašnjem obliku dostupan još od 2003. godine, dok je formalno standardiziran 2005. godine. Standardizirao ga je IETF (eng. *Internet Engineering Task Force*).

http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

Napad trovanjem međuspremnika

Napad trovanjem međuspremnika (eng. *cache poisoning*) je napad kojim zlonamjerni korisnici ubacuju lažne podatke u međuspremnik DNS poslužitelja. Na taj način zaraženi DNS poslužitelj na upite odgovara lažni podatkom i preusmjerava korisnika na krivu IP adresu gdje je podložan napadima.

http://en.wikipedia.org/wiki/DNS_spoofing

DoS napad (Napad uskraćivanjem usluge)

Dos napad (eng. *Denial of Service*) je napad u kojem se obično namjernim generiranjem velike količine mrežnog prometa nastoji zagušiti mrežna oprema i poslužitelji. Isti postaju toliko opterećeni da više nisu u stanju procesirati legitimni promet što na kraju ima za posljedicu da legitimni korisnici ne mogu koristiti mrežne usluge poput maila weba i sl.

http://www.kvalis.com/component/quickfaq/4-Sigurnost%20na%20mre%C5%BEi/13-%C5%A0to%20je%20DoS%20napad?%20DDoS?

Lanac povjerenja

Lanac povjerenja (eng. *chain of trust*) se uspostavlja provjerom valjanosti svake komponente nekog sustava odozdo prema gore. Njime se osigurava upotreba samo povjerljivog i sigurnog programskog ili sklopovskog rješenja.

http://en.wikipedia.org/wiki/Chain_of_trust

ARPAnet

ARPAnet je preteča Interneta. Bila je to velika rasprostranjena mreža koju je razvilo američko Ministarstvo obrane. Uspostavljena je 1969., a služila je kao osnova za testiranje novih mrežnih tehnologija. Povezivala je mnoga sveučilišta i istraživačke centre. Prva dva čvora ARPANET-a bili su Sveučilište Los Angeles u Kaliforniji i Institut za istraživanja Sveučilišta Stanford, a nedugo potom spojilo se i Sveučilište Utah.

http://hr.wikipedia.org/wiki/ARPANET

FQDN

FQDN (eng. *Fully Qualified Domain Name*) je oblik ljudima prihvatljivog zapisa IP adrese, pri čemu predstavlja apsolutnu stazu unutar DNS hijerarhije. Takvo ime je maksimalne duljine 255 znakova, Da bi se FQDN dodatno razlikovao od labela odnosno standardnih, ne nužno potpunih, domenskih imena česta je konvencija dodavanja dodatne točke (znaka ".") na kraj domenskog imena.

http://mreze.layer-x.com/s050201-0.html

ccTLD

Geografski bazirane domene, tzv. ccTLD (engl. *country code TLD*) domene su domene koje predstavljaju državni dvoznakovni kod temeljen na ISO-3166 standardu, a danas ih je u uporabi preko 243. Primjeri takvih domena su: .hr, .us, .de, .jp, .co.uk, itd.

http://mreze.layer-x.com/s050202-0.html

gTLD

Generičke domene, tzv. gTLD (engl. generic TLD) domene koje se obično sastoje od tri ili više znakova. Primjeri takvih domena su: .com, .net, .org, .info, .biz, .edu, .travel, itd.

http://mreze.layer-x.com/s050202-0.html

ICANN

ICANN (eng. *Internet Corporation for Assigned Names and Numbers*) je privatna neprofitna organizacija smještena u Los Angelesu zadužena za koordinaciju identifikatora na Internetu i osiguravanje stabilnih i sigurnih operacija nad njima. Organizacija je osnovana 18. rujna 1998. godine, a ugovor kojim je postala zadužena za potpunu kontrolu nad upravljanjem internet identifikatorima potpisan je 29. rujna 2006. godine.

http://en.wikipedia.org/wiki/ICANN

Digitalni potpis

Digitalni potpis (eng. digital signature) je matematički algoritam za dokazianje autentičnosti digitalne poruke ili dokumenta.Valjan digitalni potpis pruža primatelju razlog za vjerovanje da je poruku poslao poznati pošiljatelj i da poruka nije mijenjana pri prijenosu.

http://en.wikipedia.org/wiki/Digital_signature

8. Reference

[1] Wikipedia: DNS,
http://en.wikipedia.org/wiki/Domain_Name_System, 06. 2012.

[2] Dinko Korunić: DNS priručnik,
http://www.scribd.com/doc/48742258/DNS-prirucnikkuharica, 06. 2012.

[3] SANS Institute: DNS, DNSSEC and the Future
http://www.sans.org/reading_room/whitepapers/dns/dns-dnssec-future_1054. 06.2012.

[4] Wikipedia: DNSSEC,
http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions, 06. 2012.

[5] Ron Aitchison: Choosing a DNSSEC solution,
http://www.zytrax.com/books/dns/info/choosing-dnssec-solution.pdf, 06.2012.