VELEUČILIŠTE VELIKA GORICA

IVAN MESIĆ

DOMAIN NAME SYSTEM SECURITY EXSTENSIONS

ZAVRŠNI RAD

Velika Gorica, 2020.

VELEUČILIŠTE VELIKA GORICA

Održavanje računalnih sustava

DOMAIN NAME SYSTEM SECURITY EXSTENSIONS

ZAVRŠNI RAD

|  |  |
| --- | --- |
| Mentor: | Student: |
| Bruno Valić,  pred.,struč.spec.ing.techn.inf | Ivan Mesić, 77150342 |
|  |  |

Velika Gorica, 2020.

ZADATAK

Sažetak

Ključne riječi:

Abstract

Key words:

**Sadržaj**

[1. Uvod 1](#_Toc39773325)

[1.1. Predmet i cilj rada 1](#_Toc39773326)

[1.2. Struktura rada 1](#_Toc39773327)

[1.3. Izvori informacija i podataka 1](#_Toc39773328)

[2. Uvod u DNS tehnologiju 2](#_Toc39773329)

[2.1. Općenito o DNS-u 2](#_Toc39773330)

[2.2. Povijest i razvoj DNS tehnologije 2](#_Toc39773331)

[2.3. Hijerarhijska struktura DNS sustava 3](#_Toc39773332)

[2.3.1. Domensko ime 4](#_Toc39773333)

[2.3.2. Korijenska zona 5](#_Toc39773334)

[2.3.3. Vršna zona 6](#_Toc39773335)

[2.3.4. Zona domene druge razine 7](#_Toc39773336)

[2.4. DNS zapisi o resursima 7](#_Toc39773337)

[2.4.1. Tipovi zapisa o resursima 8](#_Toc39773338)

[2.5. DNS razrješenje 9](#_Toc39773339)

[2.6. DNS međuspremnici 11](#_Toc39773340)

[3. Ranjivosti DNS sustava 12](#_Toc39773341)

[3.1. Presretanje paketa 12](#_Toc39773342)

[3.2. Trovanje međuspremnika 13](#_Toc39773343)

[3.3. Napad uskraćivanjem usluge 14](#_Toc39773344)

[3.4. Napadi uskraćivanja usluge kroz povijest 15](#_Toc39773345)

[4. Sigurnosne ekstenzije DNS sustava 17](#_Toc39773346)

[4.1. Općenito o sigurnosnim ekstenzijama DNS-a 17](#_Toc39773347)

[4.2. Terminologija digitalnog potpisa 18](#_Toc39773348)

[4.3. Ključevi u DNSSEC-u 19](#_Toc39773349)

[4.3.1. Promjena DNSSEC ključeva 20](#_Toc39773350)

[4.3.2. Promjena ZSK ključa 20](#_Toc39773351)

[4.3.3. Promjena KSK ključa 20](#_Toc39773352)

[4.4. DNSSEC i digitalno potpisivanje 20](#_Toc39773353)

[4.4.1. DNSKEY zapis 21](#_Toc39773354)

[4.4.2. RRSIG zapis 23](#_Toc39773355)

[4.4.3. DS zapis i lanac povjerenja 25](#_Toc39773356)

[4.5. DNSSEC proces razrješenja 26](#_Toc39773357)

1. Uvod
   1. Predmet i cilj rada

U ovome radu detaljno je obrađena tema DNS (*eng*. Domain Name System) tehnologije. Posebna usredotočenost odnosi se na tehnologije koje se nazivaju sigurnosne ekstenzije DNS sustava, te nose kraticu DNSSEC (*eng*. Domain Name System Security Extensions). Ovaj rad ima težište ka detaljnom istraživanju DNS sigurnosnih ekstenzija kako bi se jasno prikazala važnost sigurnosti u slučaju kompromitiranja ili krađe podataka prilikom korištenja interneta.

* 1. Struktura rada

Rad se sastoji od šest poglavlja, te je svako poglavlje podijeljeno na potpoglavlja s ciljem što kvalitetnijeg i preglednijeg iznošenja teza. U prvom poglavlju opisan je predmet i cilj rada, struktura rada po poglavljima, te izvori potrebnih informacija. Drugo poglavlje temelji se na detaljnom opisu DNS tehnologije koji sadrži povijest, strukturu, te sigurnosne mane DNS tehnologije. Treće poglavlje temelji se na ranjivostima DNS sustava. Četvrto poglavlje donosi detaljan pregled DNS sigurnosnih ekstenzija u kojemu se nalaze važne činjenice poput nastanka, ciljeva, načina rada i složenosti DNS sigurnosne ekstenzije. Peto poglavlje prikazuje alate DNS sigurnosnih ekstenzija i njihovu primjenu. Šesto poglavlje se temelji na budućnosti DNS sustava i njegovoj primjeni u budućnosti. Na kraju rad završava zaključkom.

* 1. Izvori informacija i podataka

Izvori informacija i podataka prikupljeni su iz navedene literature, te iz provjerenih izvora nastalih istraživanjem na području računalnih mreža.

1. Uvod u DNS tehnologiju

U trenutnom poglavlju obrađen je uvod u DNS tehnologiju, te su obrađene teme poput povijesti nastanka DNS-a. Kako bi se jasno mogao prikazati razlog postojanja DNS-a, potrebno je objasniti način rada spomenute tehnologije.

* 1. Općenito o DNS-u

U današnje vrijeme uz uporabu interneta, korištenje DNS tehnologije se podrazumijeva kao osnovni servis. DNS je hijerarhijski raspodijeljena baza podataka koja pohranjuje informacije za bilo koji uređaj povezan na računalnu mrežu u svrhu međusobnog pronalaska. U spomenutom sustavu nalaze se različite informacije koje se povezuju s domenskim nazivima. Jedna od tih informacija je i povezivanje IP (eng. Internet Protocol) adresa i pripadajućih simboličkih imena.

Uz DNS tehnologiju često se može čuti i naziv „telefonski imenik interneta“. Taj pojam koristi se iz razloga jer DNS prevodi simboličko ime u jedinstvenu IP adresu. Način prevođenja može biti prikazan na primjeru simboličkog imena [www.vvg.hr](http://www.vvg.hr) u IP adresu 193.198.191.119, u obliku internet protokol verzije 4. U odnosu na izvorni telefonski imenik, spomenuti sustav ima mnogo razvijeniji način prilagodbe koji na vrlo brz način omogućava saznavanje IP adrese u slučaju promjene iste. Na taj način korisnik ne mora voditi brigu ukoliko se adresa promijenila, nego u suprotnom ima potrebu jednostavnog upisivanja simboličkog imena kako bi pristupio željenoj adresi.

* 1. Povijest i razvoj DNS tehnologije

Sami početci DNS tehnologije uvelike su povezani s nastankom današnjeg interneta. Nastanak interneta seže u 1969. godinu kada je osnovan od strane Američkog Ministarstva obrane. Projekt koji je potaknuo razvoj interneta naziva se Mreža Napredne Istraživačke Agencije Projekata (eng. Advanced Research Projects Agency, ARPAnet). ARPAnet je prvenstveno bio zamišljen kao velika mreža za dijeljenje podataka, razmjenu elektroničke pošte, te spajanje na udaljena računala. Nastavak budućeg razvoja interneta ostvaruje se izvedbom Protokola za Kontrolu Transmisije/Internet Protokola (eng.Transmission Control Protocol/Internet Protokola, TCP/IP). Upravo je spomenuti protokol omogućavao mnogim ustanovama priključak vlastitih računala i Lokalne Mreže (eng. Local Area Network, LAN) na prijašnje spomenuti ARPAnet. Takvim aktivnostima mreža se proširuje na tisuće računala, te se tijekom godina razvija u danas poznati internet.

Već tada, prilikom korištenja ARPAnet-a, započeta je zamjena numeričkih adresa sa simboličkim imenima koje je korisniku pružalo mnogo jednostavnije korištenje. Od velike je važnosti tada bilo postojanje hosts.txt datoteke, koja se danas smatra pretkom DNS tehnologije. Datoteka hosts.txt sadržavala je informacije potrebne za prevođenje simboličkih imena u adrese. Kako bi takvo prevođenje bilo moguće, svako računalo koje se nalazilo u ARPAnet-u bilo je prisiljeno zatražiti ažuriranu hosts.txt datoteku od instituta za istraživanje u Stanfordu (*eng. Stanford Research Institute*, SRI) kako bi bilo u mogućnosti vidjeti ostala računala povezana za mrežu.

Daljnje povećanje količine računala spojenih na mrežu predstavljalo je izuzetne komplikacije. Održavanje jedne, centralizirane tablice koja sadržava informacije o adresama postalo je jako sporo što je dovelo do neadekvatnosti hosts.txt datoteke. Rezultat toga je pojava bržeg i automatiziranog sustava za imenovanje adresa, danas poznatog kao DNS tehnologija.

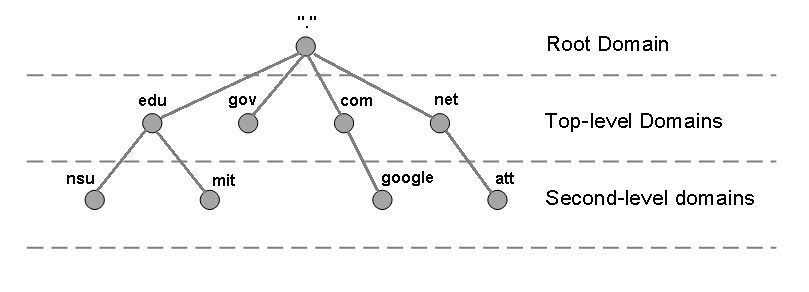
Prvu inačicu koja je i ujedno implementirana napisao je Paul Mockapetris[[1]](#footnote-1) 1963. godine, pod nazivom RFC 882 i RFC 883. Upravo je on prepoznao problematiku centralizirane tablice informacija o adresama i proizveo dinamičku DNS bazu podataka, koja na isti način postoji i danas. [1]

* 1. Hijerarhijska struktura DNS sustava

Globalni sustav domenskog imena promatra se kao hijerarhijski distribuirana baza podataka. Generalno gledajući sva računala povezana na internet posjeduju IP adresu. S druge strane također postoje računala koja posjeduju domensko ime. Takva računala dolaze u obliku web poslužitelja i predstavljaju računala s kojima korisnici žele komunicirati. Kako bi takvu komunikaciju bilo moguće ostvariti potrebno je poštivati hijerarhijsku strukturu DNS-a.

Hijerarhijska struktura domenskog imena sastoji se od tri glavne razine koje se često nazivaju i zonama te su prikazane u sljedećim točkama:

* Korijenska zona
* Vršna zona
* Zona domene druge razine

Slika 1. Hijerarhijsko stablo DNS tehnologije (izvor: [http://www.itgeared.com/articles/1354-domain-name-system-dns-tutorial-overview](http://www.itgeared.com/articles/1354-domain-name-system-dns-tutorial-overview/))

* + 1. Domensko ime

Domensko ime je simboličko ime računala koje ga jedinstveno označuje, te je u 2020 godini registrirano više od 360 milijuna domenskih imena. Domensko ime sastoji se od dvije ili više labela koje predstavljaju pojedinu razinu hijerarhijske strukture DNS-a, te od niza točaka koje služe kao „granica“ za razdvajanje spomenutih razina.

Iako labela predstavlja niz alfanumeričkih znakova maksimalne dužine od 63 znaka, prilikom stvaranja labele potrebno je koristiti neka od osnovnih pravila, te su navedeni sljedeći dozvoljeni znakovi:

* Slova od A do Z (pri čemu se ne raspoznaju mala i velika slova)
* Brojevi od 0 do 9
* Dozvoljen je jedino znak „-“

Iako je već spomenuto kako se domensko ime sastoji od dvije ili više labela odvojenih točkama, domensko ime može biti i kratkog oblika, sadržavajući svega dio određenog slijeda labela. Kada se pak govori od apsolutnoj ili potpunoj formi gdje su navedene sve labele, tada se koristi i izraz *FQDN (eng. Fully Qualified Domain Name).* Takav oblik domenskog imena može sadržavati najviše 127 podjela uz zadanu granicu od 255 znakova.

Kako bi se FQDN dodatno razlikovao od standardnog domenskog imena, važno je naglasiti da se na krajnje desnu stranu domenskog imena dodaje točka koja predstavlja korijenski poslužitelj, no u većini slučaja prilikom korištenja internet preglednika to nije praksa.

* + 1. Korijenska zona

Korijenska zona je zona najviše razine u hijerarhijskoj strukturi domenskog imena koja je kontrolirana od strane *ICANN* (eng. *Internet Corporation for Assigned Names and Numbers*) organizacije u kojoj se nalaze korijenski poslužitelji. Glavna zadaća korijenskih poslužitelja je funkcionalnost DNS-a i cijelog interneta, te je važno napomenuti kako su korijenski poslužitelji prvi korak u procesu razrješenja domenskog imena. Detaljni opis korijenskih poslužitelja objašnjen je u poglavlju 2.5. DNS razrješenje.

Često je mišljenje kako u svijetu postoji 13 poslužitelja. Iako je ta tvrdnja djelomično točna broj 13 zapravo predstavlja IP adrese korijenskih poslužitelja, dok svaki od njih posjeduje vlastitu mrežu poslužitelja raširenu po cijelom svijetu. Na taj način smanjuje se ranjivost poslužitelja u slučaju raznih napada ili pak velikih katastrofa.

U tablici 1 prikazana je lista korijenskih poslužitelja sa pripadajućim adresama i organizacijama koje ih kontroliraju.

Tablica 1. lista korijenskih poslužitelja (izvor: <https://www.iana.org/domains/root/servers>)

|  |  |  |
| --- | --- | --- |
| Ime poslužitelja | IP adresa | Organizacija |
| a.root-servers.net | 198.41.0.4 | VeriSign, Inc. |
| b.root-servers.net | 199.9.14.201 | University of Southern California (ISI) |
| c.root-servers.net | 192.33.4.12 | Cogent Communications |
| d.root-servers.net | 199.7.91.13 | University of Maryland |
| e.root-servers.net | 192.203.230.10 | NASA |
| f.root-servers.net | 192.5.5.241 | Internet Systems Consortium, Inc. |
| g.root-servers.net | 192.112.36.4 | US Department of Defense (NIC) |
| h.root-servers.net | 198.97.190.53 | US Army (Research Lab) |
| i.root-servers.net | 192.36.148.17 | Netnod |
| j.root-servers.net | 192.58.128.30 | VeriSign, Inc. |
| k.root-servers.net | 193.0.14.129 | RIPE NCC |
| l.root-servers.net | 199.7.83.42 | ICANN |
| m.root-servers.net | 202.12.27.33 | WIDE Project |

* + 1. Vršna zona

Vršna zona je područje u kojoj se nalaze domene vršne razine (*eng. Top Level Domain*). Vršne domene se nalaze na najvišoj razini hijerarhijske strukture DNS-a, te se stoga nalaze na krajnje desnom mjestu domenskog imena. Na primjeru domenskog imena [www.vvg.hr](http://www.vvg.hr), vršna domena predstavlja labelu „hr“ nakon koje slijede poddomene bez kojih vršna domena nema koristi. Za dodjelu i upravljanje domenama brine se već spomenuta organizacija *ICANN* koja vodi brigu o različitim poddomenama koje nikako ne smiju biti iste, jer bi se u protivnom vrlo lako mogla dogoditi kolizija što bi onemogućilo pravilan rad DNS sustava.

U DNS sustavu razlikuju se dvije vrste vršnih domena, pa stoga postoji mogućnost pojavljivanja geografski bazirane domene ccTLD (*eng. country code Top Level Domain*) koja predstavlja državu u kojoj se nalazi domensko ime. Spomenute domene obavezno dolaze u obliku dva znaka, te ih trenutno u svijetu postoji gotovo 250. S druge strane pak postoje i generičke domene gTLD (*eng. generic Top Level Domain*) koje se obično sastoje od 3 ili više znakova.

Tablica 2. lista vršnih domena (izvor: <https://www.worldstandards.eu/other/tlds/>)

|  |  |
| --- | --- |
| Geografske domene | |
| Ime države ili teritorija | Oznaka domene |
| Hrvatska | .hr |
| Europska unija | .eu |
| Ujedinjeno Kraljevstvo | .uk |
| Norveška | .no |
| Generičke domene | |
| Vrsta namjene | Oznaka domene |
| Komercijalna namjena | .com |
| Organizacije i udruge | .org |
| Edukacijska namjena | .edu |
| Vojna namjena | .mil |

* + 1. Zona domene druge razine

Sljedeća razina DNS hijerarhijske strukture rezervirana je za domene druge razine. Spomenuta zona nalazi se odmah nakon vršne domene, odnosno lijevo od vršne domene ukoliko se promatra kompletno domensko ime. U već spomenutom primjeru domenskog imena [www.vvg.hr](http://www.vvg.hr) domena druge razine se odnosi na oznaku „vvg“ koja predstavlja kraticu ili potpuno ime organizacije, tvrtke ili osobnog imena. Ova razina domene je vrlo bitna prilikom pretraživanja u internet pregledniku jer se upisuje u paru sa oznakom vršne domene. Te se na taj se način dobiva mnogo kvalitetniji rezultat željenog odredišta.

* 1. DNS zapisi o resursima

Svaki puta kada se pokreće zahtjev za prikupljanjem informacija o domenskom imenu, vrši se pregled kroz bazu podataka, odnosno datoteku zone (*eng. zone file*) kako bi se prikupile informacije potrebne za prevođenje potpunog domenskog imena u IP adresu. Takvi tipovi informacija nazivaju se zapisi o resursima (*RR, eng. Resource Records*). Zapisi o resursima sadrže sljedeća polja, te se pojavljuju redom koji slijedi:

* Domensko ime (*eng. Name*) – domensko ime koje sadrži RR. Uglavnom se pojavljuje u obliku FQDN-a, a ukoliko je zapisano u obliku kratkog imena tada se na kraj stavlja naziv nadležne zone.
* Životni vijek zapisa (*TTL, eng. Time To Live*) – sadrži vrijednost koja određuje koliko dugo će zapis biti pohranjen u DNS međuspremniku i izražava se u sekundama.
* Klasa (eng. *Class*) – označava klasu mreže. U današnje vrijeme dolazi jedino kao internet vrijednost.
* Tip zapisa (*eng. Type*) – govori o kojem tipu podatka se radi (tipovi podataka su detaljno opisani u potpoglavlju 2.4.1).
* Podatak o zapisu (*eng. RDATA*) – vrijednost za vezani tip zapisa.

U tablici 3 navedena su polja RR-a sa primjerima pripadajućih atributa.

Tablica 3. Komponente zapisa o resursima

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Domensko ime | Životni vijek zapisa | Klasa | Tip zapisa | Podatak o zapisu |
| [www.vvg.hr](http://www.vvg.hr) | 3600 | IN | A | 193.198.191.119 |

* + 1. Tipovi zapisa o resursima

Kada se govori o tipovima zapisa o resursima, tada postoji preko trideset tipova, no trenutno se koristi nekoliko osnovnih koji su opisani u sljedećim točkama:

* A – adresa koja korespondira sa domenskim imenom, te dolazi u obliku IPv4 adrese.
* AAAA – adresa koja ima istu funkciju kao i gore navedena adresa, samo što dolazi u obliku IPv6 adrese.
* CNAME (*eng. Canonical name*) – zamjensko ime koje je pridruženo domenskom imenu zbog lakšeg prepoznavanja raznih servisa ili uređaja, te na taj način preuzima sva svojstva izvornog domenskog imena.
* MX (*eng. Mail Exchange*) – koristi se za definiranje poslužitelja elektroničke pošte nadležnih za pripadajuće domensko ime.
* NS (*eng. Name Server*) – ispisuje imena svih DNS poslužitelja za pripadajuću domenu. Ovaj zapis omogućuje drugim poslužiteljima da pronađu autoritativni poslužitelj za pripadajuću domenu.
* SOA (*eng. Start of Authority*) – zapis koji definira ključne karakteristike i atribute za dotičnu zonu ili domenu. Također sadrži informacije o količini zaprimljenih upita i razne brojače potrebne za komunikaciju između glavnog i redundantnog poslužitelja.
  1. DNS razrješenje

Proces slanja i obrade zahtjeva, te njihovo vraćanje u obliku odgovora naziva se DNS razrješenje. Kao što je u uvodu već spomenuto, glavna zadaća DNS sustava je pretvorba domenskog imena u IP adresu što ujedno predstavlja DNS razrješenje.

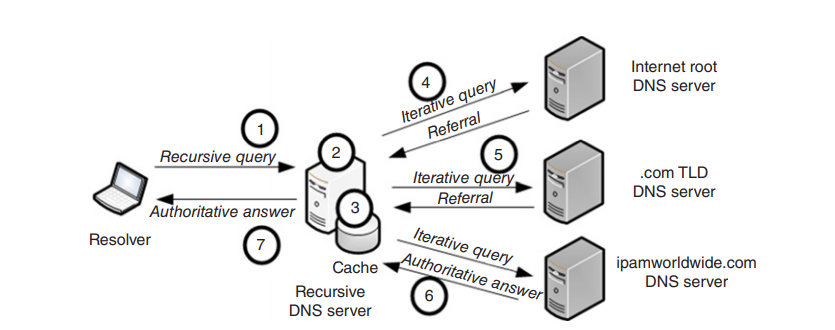
Svaki DNS sustav obavezno je sastavljen od tri dijela:

* DNS prevoditelj (*eng.resolver*) - program koji se nalazi na korisničkom računalu, poziva se od strane internet preglednika, te predstavlja prvi korak u formiranju DNS upita.
* Rekurzivni DNS poslužitelj (*eng. recursive*), poslužitelj koji nakon dobivenog upita prolazi kroz hijerarhijsko stablo i vraća odgovore DNS klijentu. Dotični poslužitelj je u većini slučaja dodijeljen od pružatelja internet usluga.
* Autoritativni DNS poslužitelj (*eng. authoritative*), poslužitelj koji odgovara na upite rekurzivnih poslužitelja i vraća konačni odgovor ili zbog nemogućnosti pronalaska tražene informacije vraća referencu na drugi autoritativni DNS poslužitelj.[2]

DNS razrješenje sastoji se od mnogo koraka koji se vrše prolaskom kroz hijerarhijsko stablo u svrhu pronalaska potrebnih informacija. S obzirom da je DNS sustav raspodijeljen na mnogo različitih poslužitelja, razrješenje ne može biti završeno na temelju samo jednog upita i odgovora, već zahtjeva veći opseg međusobne komunikacije. Iznimno razrješenje je moguće dobiti nakon samo jednog upita, no tada se tražena informacija nalazi u DNS međuspremniku o kojem se govori u poglavlju 2.5.

Ukoliko se govori o tipovima DNS rezolucije, tada postoje dva osnovna tipa prolaska kroz DNS hijerarhiju:

* Iterativni – DNS poslužitelj prima upit od strane klijenta te odmah vraća odgovor ukoliko je podatak spremljen u međuspremniku ili odgovara imenom drugog autoritativnog poslužitelja koji sadrži više informacija o traženom upitu.
* Rekurzivni, DNS poslužitelj prima upit od strane klijenta. Poslužitelj preuzima posao pronalaska informacija prolazeći kroz kompletnu DNS hijerarhiju dok ne dobije potpuni odgovor, te ga vraća nazad do klijenta.



Slika 2. DNS rezolucija (izvor: Dooley, Michael; Rooney, Timothy: DNS Security Management)

Slika 2. prikazuje skup rekurzivnih i iterativnih upita. Važno je napomenuti kako rekurzivni upit postoji samo na relaciji klijent – rekurzivni poslužitelj iz razloga što bi poslužitelji postali preopterećeni prilikom preuzimanja uloge u pronalaženju traženih informacija.

S obzirom da je DNS razrješenje vrlo složen skup upita i odgovora prikazan je na primjeru sljedećih točaka:

* Klijent pokreće rekurzivni upit za razrješavanjem domenskog imena [www.vvg.hr](http://www.vvg.hr) u smjeru rekurzivnog DNS poslužitelja. Klijent zna koji DNS poslužitelj kontaktira temeljeno na ručno podešenoj IP adresi ili pomoću DHCP-a[[2]](#footnote-2).
* Rekurzivni poslužitelj pretražuje vlastiti međuspremnik.
* Ukoliko pronađe informaciju o traženom upitu vraća odgovor i ovdje proces prestaje.
* U slučaju da odgovor nije pronađen rekurzivni poslužitelj šalje iterativni upit prema korijenskom poslužitelju koji također ne zna odgovor na traženi upit, ali izvršava delegaciju na vršnu zonu pronalaskom „hr“ labele.
* Rekurzivni poslužitelj tada šalje iterativni upit poslužitelju vršne zone koji isto tako ne zna potpuni odgovor u okviru [www.vvg.hr](http://www.vvg.hr) domenskog imena i stoga vrši delegaciju na zonu domene druge razine pronalaskom „vvg“ labele.
* Poslužitelj zadužen za zonu domene druge razine vraća autoritativni odgovor prema rekurzivnom poslužitelju u obliku IP adrese 193.198.191.119.
* Rekurzivni DNS poslužitelj odgovara klijentu odgovorom u obliku IP adrese i u tom trenu završava DNS razrješenje.
  1. DNS međuspremnici

U prethodnom poglavlju detaljno je opisano DNS razrješenje temeljeno na iterativnim i rekurzivnim upitima, uz pretpostavku da svaki novi upit predstavlja novi prolazak kroz hijerarhijsko stablo počevši od upita formiranog od klijenta prema korijenskom poslužitelju. Ukoliko bi se takav tip prakse upotrebljavao u stvarnosti to bi uvelike rezultiralo povećanim vremenom čekanja prilikom pretraživanja domenskog imena, te bi dovelo do nepotrebnog opterećenja DNS poslužitelja.[2]

Prilikom prijašnjih iskustava praksa je pokazala kako je vrlo česta pojava da korisnik u kratkom periodu vremena šalje sličan ili isti DNS upit. Upravo zbog toga svi moderni DNS poslužitelji su opremljeni DNS međuspremnicima (*eng. cache*). U međuspremnicima se nalaze sve informacije vezane za nedavne DNS upite koji omogućavaju dobivanje odgovora ili barem dijela traženog odgovora. Isto tako međuspremnici se nalaze i na strani DNS klijenata što dodatno skraćuje vrijeme pronalaska odgovora na postavljeni upit, te rasterećuje DNS poslužitelje.[2]

DNS međuspremnici u modernom DNS sustavu nose vrlo važnu ulogu, bez kojih je gotovo nezamislivo kvalitetno funkcioniranje DNS sustava. No međuspremnici imaju svoje ranjivosti poput napada na DNS sustav pod nazivom „trovanje međuspremnika“ kojem su vrlo podložni, te će se o spomenutom više govoriti u nastavku ovog rada.

1. Ranjivosti DNS sustava

DNS sustav je neizostavna komponenta bez koje je gotovo nemoguće zamisliti rad interneta. Uz prednosti i mogućnosti koje spomenuti sustav pruža svakodnevnim korisnicima interneta vežu se i mnogi sigurnosni problemi, te će o istima biti više govora u ovom poglavlju. U ranim početcima, pitanje sigurnosti nije bilo od velike važnosti iz razloga što sam internet nije bio namijenjen širokoj javnosti. No, kako je s vremenom širenje interneta u komercijalne svrhe postao sveopći pojam, zahtjevi za sigurnosne mjere zaštite podataka postali su obavezni.

Na zaštitu kojom danas raspolaže DNS ponajviše je utjecalo izvršavanje napada koji su kao glavnu zadaću imali prisiljavanje određenih poslužitelja da prihvate lažne zapise. Na taj način klijenti su preusmjeravani na pogrešne adrese prilikom čega su postajali lake mete zlonamjernih napadača.[2]

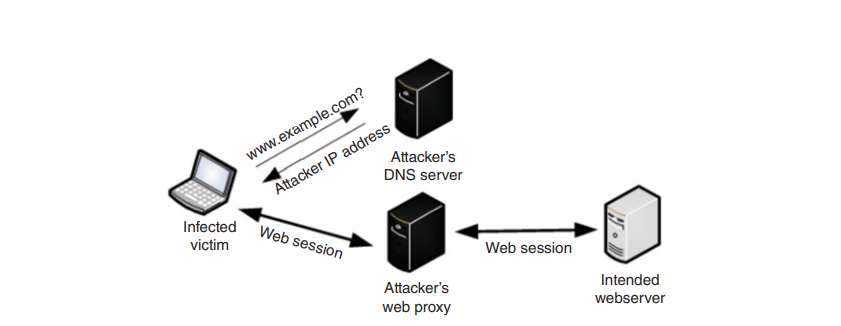
Kroz povijest DNS sustav susretao se sa mnogo tipova napada, te će neki od njih u nastavku biti detaljnije opisani.

Najistaknutiji tipovi napada na DNS sustav su:

* Presretanje paketa
* Napad uskraćivanjem usluge
* Trovanje međuspremnika
  1. Presretanje paketa

U slučaju kada se napadač nalazi u položaju u kojem ima pristup prometu mreže, koju koristi DNS klijent, tada mu se pružaju mogućnosti presretanja DNS paketa. Slikovito bi se takav tip napada mogao opisati kao „čovjek u sredini“ (*eng. man in the middle*), što prikazuje slika 3. Ovaj napad mnogo ovisi o sposobnosti napadača kojom pretpostavlja IP adresu DNS poslužitelja.

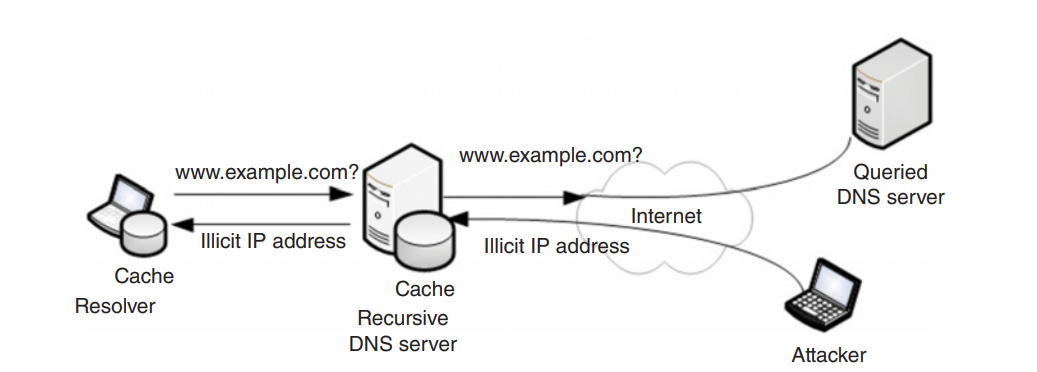
Sada kada se napadač nalazi između klijenta i DNS poslužitelja, te je otkrio identitet DNS poslužitelja, u mogućnosti je presretati upite upućene prema DNS poslužitelju jer se predstavlja kao DNS poslužitelj. Rezultati ovog napada otvaraju vrata mnogo ozbiljnijim oblicima novih napada poput uskraćivanja usluge i trovanjem međuspremnika o kojem će biti više govora u nastavku rada ili pak prikupljanju povjerljivih informacija od strane klijenta.



Slika 3. DNS presretanje paketa (izvor: Dooley, Michael; Rooney, Timothy: DNS Security Management)

* 1. Trovanje međuspremnika

Kao što je prethodno spomenuto DNS klijenti i rekurzivni DNS poslužitelji koriste međuspremnike za pohranjivanje izvršenih upita u svrhu poboljšanja performansi DNS razrješenja. Ukoliko napadač uspije u namjeri da se pozicionira između klijenta i DNS poslužitelja, te na taj način prekine njihovu komunikaciju, stavlja se u poziciju u kojoj može odgovarati na klijentove upite. Odgovori su u tom slučaju lažne informacije koje na posljetku završavaju u klijentovom međuspremniku. Lažne informacije dobivene od strane rekurzivnog poslužitelja klijent kasnije nesvjesno koristi u svrhu zlonamjernih radnji, s obzirom da vjeruje kako je informacija došla iz smjera stvarnog DNS poslužitelja.[3]



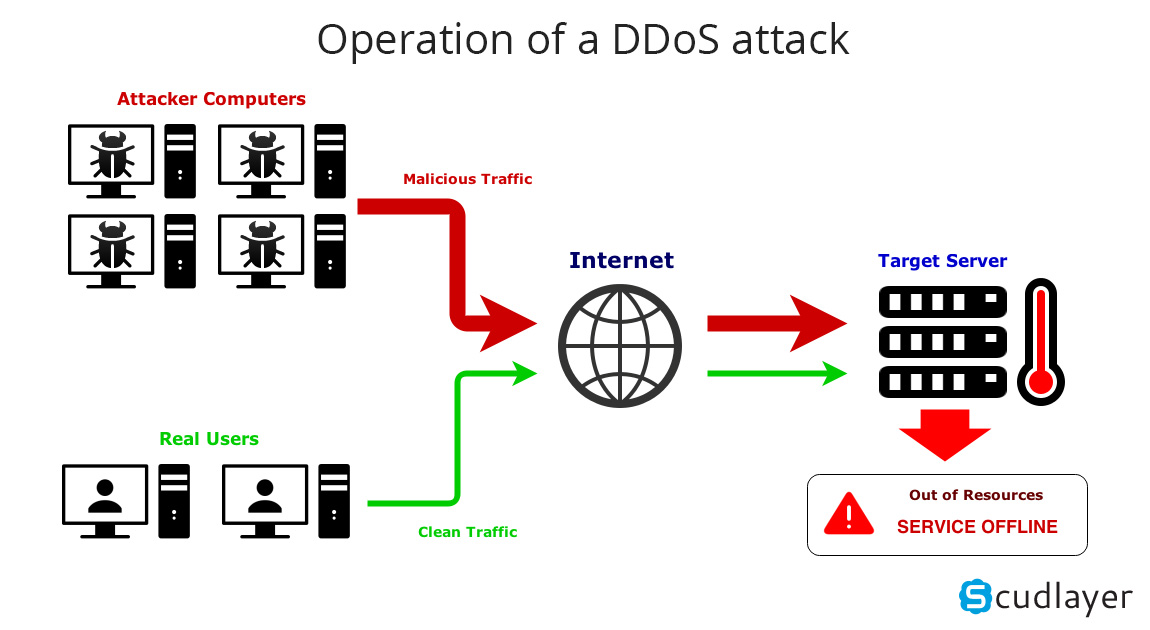
Slika 4. Trovanje međuspremnika (izvor: Dooley, Michael; Rooney, Timothy: DNS Security Management)

U slučaju kada se napadač pozicionirao između dva DNS poslužitelja, tada se lažne informacije pohranjuju u međuspremnik poslužitelja koji šalje upit nadređenom poslužitelju i svi sljedeći upiti istog oblika usmjereni prevarenom poslužitelju dobiti će lažni odgovor iz njegova međuspremnika.[4]

Ovaj tip napada često vodi do nesvjesnog usmjeravanja klijenata na pogrešne adrese čineći tako veliku mrežu napadača pogodnu za izvršavanje napada uskraćivanjem usluge o kojem će biti više govora u sljedećem poglavlju.

* 1. Napad uskraćivanjem usluge

Napad uskraćivanjem usluge DDoS (*eng.Distributed Denial of Service*) je napad koji je usmjeren na određeni poslužitelj ili mrežu, s krajnjim ciljem ometanja ispravnih funkcija istih. DDoS napad obavlja se preplavljivanjem konstantnih lažnih upita usmjerenih prema poslužitelju ili mreži što u konačnici dovodi do uskraćivanja usluge.



Slika 4. Napad uskraćivanjem usluge (izvor: <https://medium.com/@kapil.sharma91812/understanding-ddos-attack-15dd2cbce2a>)

U slici 4. prikazan je primjer napada uskraćivanjem usluge. Poslužitelj koji se nalazi na desnoj strani predstavlja internet poslužitelj na kojem se uz pretpostavku nalazi internet trgovina određene tvrtke koja prodaje svoje proizvode. U lijevom donjem kutu slike, također uz pretpostavku nalaze se kupci koji putem svojih računala pregledavaju i kupuju proizvode u spomenutoj trgovini. U gornjem lijevom kutu nalazi se potencijalni napadač koji iz određenog razloga želi napasti internet trgovinu. U današnje vrijeme razlozi napada su mnogobrojni, no često oni proizlaze kao pokušaj iznuđivanja otkupnine ili raznih ucjena.

Napadač u ovom slučaju koristi vlastito računalo i određenu skriptu kako bi preplavio poslužitelj internet trgovine mnogobrojnim lažnim upitima. Ovakav tip napada nije uobičajeni DDoS napad jer se izvršava sa jednog računala, što većini poslužitelja ne predstavlja veliki problem s obzirom na mogućnost zatvaranja veze od strane napadača. Ono što poslužitelju predstavlja problem jest istovremeni napad velikog broja računala koordiniranih od strane glavnog računala ili napadača. Takav tip napada omogućuje se uporabom štetnog programa (*eng. malware*) koji bez pristanka korisnika rezultiraju raznim neželjenim radnjama poput krađe povjerljivih podataka, a u ovom slučaju iskorištavanje računala u svrhu raznih upita prema internet poslužiteljima. Rezultat takvog napada jest iskorištavanje resursa poput procesora ili radne memorije poslužitelja što u konačnici dovodi do onemogućavanja usluge od strane poslužitelja.

* 1. Napadi uskraćivanja usluge kroz povijest

Prvi napad uskraćivanja usluge dogodio se prije gotovo trideset godina, kada je sredinom 1999. godine skupina od 114 računala uz posjedovanje zlonamjerne računalne skripte pod nazivom „Trin00“ izvršila napad na računala u vlasništvu Sveučilišta u Minnesoti *MIT* (*eng. University of Minnesota*). Rezultat potonjeg napada bio je preplaviti Sveučilišna računala lažnim paketima podataka u svrhu sprječavanja postupanja s legitimnim zahtjevima. Napad je trajao kontinuirano dva dana, a danas se pamti kao prvi napad koji je predstavio taktiku uskraćivanja usluge.[8]

Sljedeći bitan napad uskraćivanjem usluge dogodio se 2002. godine i bio je usmjeren prema korijenskim poslužiteljima. Cilj ovog napada bio je učiniti korijenske poslužitelje nedostupnima, što bi na posljetku rezultiralo ograničavanje rada interneta. S obzirom kako je mreža korijenskih poslužitelja široko raširena, te upravo u svrhu sprječavanja zlonamjernih napada posjeduje sustav redundancije, ovaj napad nije imao velikog utjecaja na funkcionalnost no nedvojbeno je pridonjeo povećanju iskustva u spomenutim napadima.[9]

Sljedeći napad uskraćivanjem usluge koji stoji kao prvi uspješni napad velikih razmjera, dogodio se u listopadu 2016. godine. Upravo je taj napad bio usmjeren prema tvrtci Dyn koja u svome vlasništvu posjeduje *DNS* poslužitelje nadležne za većinu *DNS* infrastrukture. Rezultat ovog napada bio je uskraćivanje usluga velikih tvrtki poput Twitter-a, Netflix-a, Reddit-a, Github-a, te velikog broja ostalih tvrtki sa sjedištem u Europi i Sjedinjenim Američkim Državama. Zanimljivost u ovom napadu jest što je kao zlonamjernu računalnu skriptu pod nazivom „Mirai botnet“ koristio za upravljanje internet stvarima *IoT (eng. Internet of Things).* Upravo je korištenje internet stvari uvelike pogodovalo uspješnosti ovog napada jer su takvi tipovi uređaja znatno manje zaštićeni, te im je lakše pristupiti. Shodno tome više od 100000 uređaja internet stvari sudjelovalo je u *DDoS* napadu ostvarivši tako izuzetno velik broj upita usmjerenih prema *DNS* poslužiteljima, jačine 1,2 Tbps.[3]

1. Sigurnosne ekstenzije DNS sustava

U prethodnom poglavlju spomenuti su neki od najčešćih napada koji se izvršavaju u svrhu zlonamjernih aktivnosti, te se na taj način iskorištavaju ranjivosti DNS sustava. Pošto je postupak DNS razrješenja vrlo složen proces prevođenja domenskog imena u ispravnu IP adresu dobivenu od autoritativnog poslužitelja, mnogi od pojedinih koraka u procesu razrješenja mogu biti kompromitirani od strane raznih napada.

U trenutcima kada su poslovanje, ugled i povjerljivost podataka od velike važnosti, sigurnost istih ne smije biti upitna. Kako bi se takva pitanja otklonila dolazi do pojave sigurnosnih ekstenzija DNS sustava, kojima je glavna zadaća eliminirati sumnje negativne DNS sigurnosti.

* 1. Općenito o sigurnosnim ekstenzijama DNS-a

Sigurnosne ekstenzije DNS-a predstavljaju postupak u kojem DNS poslužitelj provjerava autentičnost i integritet rezultata koji dolaze od strane potpisane zone, u svrhu sprječavanja raznih kompromitirajućih DNS odgovora. Svi odgovori i rezultati od strane sigurnosnih ekstenzija su kriptografski digitalno potpisani, te na taj način dokazuju svoje izvorno podrijetlo od upitanog DNS poslužitelja.

Kako bi sigurnosne ekstenzije opravdavale svoju ulogu primarno se moraju fokusirati na tri glavna cilja:

* Autentikacija izvora zaprimljenih DNS podataka – potvrda da zaprimljeni podatci dolaze samo od strane autoritativnih poslužitelja nadležnih za traženu DNS zonu
* Integritet podataka – provjera i potvrda da podatci, odnosno odgovori zaprimljeni od strane DNS prevoditelja su isti onim podatcima koji su poslani od strane DNS poslužitelja nadležnog za traženu DNS zonu, te da nisu promijenjeni prilikom prijenosa.
* Dokaz o nepostojanju *PNE* (*eng. Proof of Nonexistence*) – potvrda nepostojećeg domenskog imena (*eng. NXDOMAIN*) u slučaju negativnog odgovora.

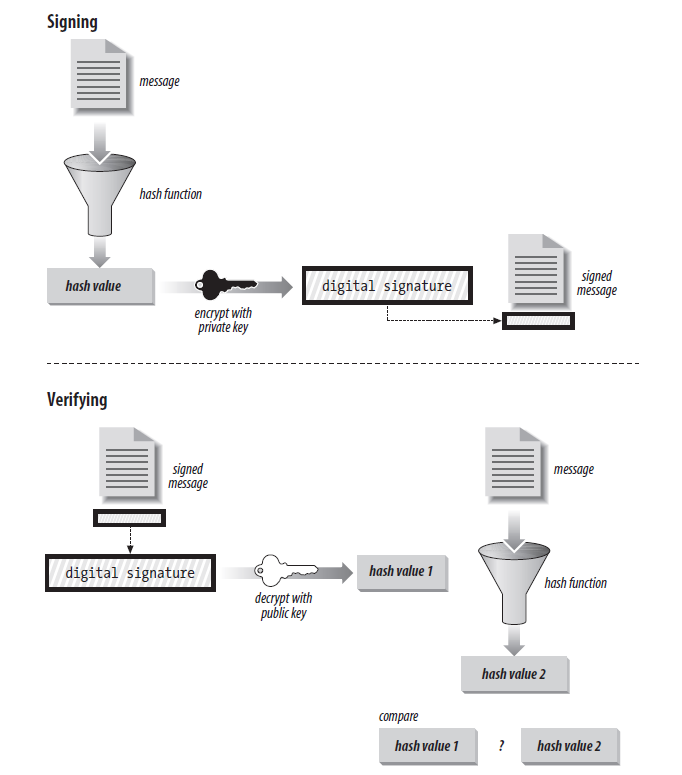
Prije svega, važno je napomenuti da u svrhu izvršavanja gore navedenih ciljeva obje strane, odnosno autoritativni poslužitelj i DNS prevoditelj moraju biti konfigurirane za podršku sigurnosnih ekstenzija DNS-a. Baza podataka u kojoj su spremljeni zapisi o resursima mora biti digitalno potpisana pri čemu postaje sigurna točka za slanje informacija. Na drugoj strani također se mora nalaziti DNS prevoditelj koji je konfiguriran za podršku DNSSEC-a, te na taj način postaje sposoban za provjeru autorizacije odgovora zaprimljenih od strane autoritativnih poslužitelja.

* 1. Terminologija digitalnog potpisa

Sigurnosne ekstenzije DNS sustava koriste digitalni potpis koji predstavlja matematičku tehniku u svrhu pružanja autentikacija i integriteta raznih digitalnih dokumenata i poruka. U današnjem vremenu kada je fizička razmjena dokumenata vrlo minorna, digitalni potpis ulijeva primaocu digitalnih dokumenata veliko povjerenje u podrijetlo i otklanjanje sumnje u promjenu podataka prilikom prijenosa. Digitalni potpis primarno se sastoji od sljedećih svojstva:

* Asimetrična kriptografija – također poznata i po nazivu kriptografija javnog ključa koja uključuje generiranje dva različita ključa, javni i tajni ključ.
* Hash funkcija – funkcija koja prevodi poslanu poruku u skup znakova fiksne duljine (*eng. digest*). Jedan od najčešćih hash algoritama je SHA 1 koji uvijek proizvodi skup slova i brojeva od 160 bitova bez obzira na duljinu poslane poruke.

Provedba procesa digitalnog potpisa započinje na strani pošiljatelja koji šalje određenu poruku primatelju uz uvjet dostupnosti javnog ključa. Poslanu poruku obrađuje hash funkcija u svrhu dobivanja skupa znakova. Pošiljatelj potom enkriptira dobiveni skup znakova uz pomoć tajnog ključa iz čega proizlazi digitalni potpis. Nakon toga oba entiteta, izvorna poruka i digitalni potpis se zajedno šalju primatelju kako bi obrnutim postupcima utvrdio legitimnost primljene poruke. S jedne strane primatelj koristi isti hash algoritam kao i pošiljatelj kako bi dobio skup znakova, dok s druge strane koristi javno dostupni ključ u svrhu dekripcije digitalnog potpisa čiji je rezultat isto tako skup znakova. U konačnici primatelj posjeduje dva skupa znakova dobivenih iz prethodnih procesa, te nad njima vrši usporedbu. Ako su oba skupa jednaka primatelj je u mogućnosti potvrditi da se poruka nije promijenila prilikom prijenosa, te da dolazi od poznatog pošiljatelja.



Slika 5. Proces digitalnog potpisivanja (izvor: Liu, Cricket; Albitz, Paul: DNS and BIND)

* 1. Ključevi u DNSSEC-u

U sigurnosnim ekstenzijama *DNS-a* razlikuju se dva tipa javnih ključeva. Iako imaju različite uloge, oba ključa se nalaze u *DNSKEY* zapisu pod kraticama *ZSK* (*eng. Zone Signing Key*) i *KSK* (*eng. Key Signing Key. ZSK* ključ koristi se prilikom procesa potvrde digitalnog potpisa potrebnog za potpisivanje zone odnosno *RRSET-a*. S druge strane *KSK* ključ ima za zadaću samo potpisati *ZSK* ključ. Razlog korištenja dvije vrste javnih ključeva jest razdvojiti skupinu funkcija u svrhu smanjenja kompleksnosti zadaća povezanih sa ažuriranjem ključeva i ponovnim potpisivanjem *DNS* zona.

*KSK* ključ se koristi za potpisivanje *DNSKEY* zapisa i predstavlja ključ koji se prosljeđuje nadređenoj zoni u obliku *DS* zapisa opisanog u poglavlju 4.3.3, te na taj način tvori jednu vrstu sidra povjerljivosti (*eng. Anchor of Trust*) za uspostavljanje lanca povjerenja.

* + 1. Promjena DNSSEC ključeva

Isti javni ključevi u *DNSSEC-u* ne smiju imati neograničeni vijek trajanja. Kako bi se povećala sigurnost koju pruža *DNSSEC,* preporučljivo je što češće vršiti promjenu javnih ključeva. U inačici RFC 4641 *DNSSEC* dokumentacije stoji kako veća vjerojatnost kompromitiranja, nezgoda ili pak kriptoanaliza ovisi o periodu korištenja javnih ključeva.[7] No u istom dokumentu također stoji kako nije preporučljivo imati jednak razmak između promjene javnih ključeva, već je preporučljivo isti proces ponoviti u okviru deset dana prije ili poslije zakazanog roka.

* + 1. Promjena ZSK ključa

Promjenu *ZSK* ključa potrebno je vršiti češće od *KSK* ključa. Razlozi češće promjene *ZSK* ključa u odnosu na *KSK* ključ su manja veličina samog ključa i mani utjecaj na *DNS* hijerarhijsku strukturu. Naime prilikom promjene *ZSK* ključa izmjene se događaju samo unutar zone gdje se nalazi *ZSK,* dok s druge strane *KSK* ključ ima utjecaja na *DS* zapis u nadređenoj zoni u kojem se također nalazi.

Razlog smanjene veličine *ZSK* ključa je njegova uloga u procesu potvrde digitalnog potpisa. Naime kada bi navedena tvrdnja bila suprotna, *DNS* poslužitelji bi se neprestano suočavali sa velikom količinom podataka, što bi uvelike usporilo performanse istih. No zbog njegove smanjene veličine mnogo je podložniji kompromitiranju, te je stoga preporučljivo se pridržavati uputa iz prethodnog poglavlja.[5]

* + 1. Promjena KSK ključa

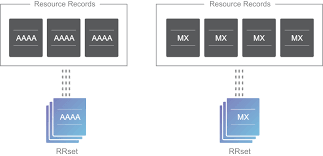
*KSK* ključ nije potrebno mijenjati tako često kao *ZSK* ključ iz razloga što se ovaj tip ključa koristi za provjeru vrlo male količine podataka, što mu dopušta veću dužinu znakova. Važno je znati kako se prilikom promjene *KSK* ključa izvršava interakcija između nadređene zone, te je u tom slučaju moguća odgoda vremena provjere.[5]

* 1. DNSSEC i digitalno potpisivanje

Kao što je već spomenuto, glavno načelo DNSSEC-a jest pružiti autorizaciju i integritet podataka. Kako bi ta zadaća mogla biti izvršena potrebno je omogućiti digitalno potpisivanje svih zapisa o resursima koji potječu od autoritativnih poslužitelja. Kao i u izvornom primjeru digitalnog potpisivanja DNSSEC koristi kriptografski par ključeva od kojih privatni ključ ostaje u tajnosti i koristi se za potpisivanje DNS zone, dok se javni ključ koristi u svrhu provjere valjanosti i javno je dostupan. Ovim postupkom dolazi do pojave četiri dodatna zapisa koji su navedeni u sljedećim točkama:

* RRSIG (eng. resource record signature)
* DNSKEY (*eng. DNS key record*)
* DS (*eng. delegation signer*)
* NSEC (*eng. Next Secure*)

Uz proces digitalnog potpisivanja putem DNSSEC-a pojavljuje se pojam *RRSET* (*eng. Resource Record Set*) koji predstavlja skupinu zapisa o resursima sa istim domenskim imenom, klasom i tipom zapisa. Za primjer se može navesti veći broj poslužitelja elektroničke pošte koji pripadaju istoj domeni, te se zbog svojih svojstava promatraju kao jedan *RRSET*. Korištenjem spomenutih skupina zapisa povećavaju se performanse, te je moguće uvelike uštedjeti na vremenu procesa potpisivanja zapisa iz razloga što se ono odvija na razini *RRSET-a*, a ne na temelju individualnog zapisa o resursu.



Slika 6. Primjer skupine zapisa (*RRSET*) (izvor: <https://www.cloudflare.com/dns/dnssec/how-dnssec-works/>)

* + 1. DNSKEY zapis

U sigurnosnim ekstenzijama DNS-a, svaka zona posjeduje par ključeva koji su sa istom povezani. Kao što je već spomenuto, taj par ključeva dijeli se na javni i tajni ključ. Tajni ključ obavezno se mora nalaziti na sigurnom mjestu, te je u većini slučaja on pohranjen u datotečnom sustavu DNS poslužitelja. S druge strane javni ključ dolazi zajedno sa domenskim imenom koje je ujedno i njegov vlasnik, a nalazi se primjeru novog *DNSKEY* zapisa i koristi se za provjeru digitalnih potpisa. *DNSKEY* zapis obično se sastoji od dva tipa ključeva pod kraticom *KSK* i *ZSK*. Upravljanje i uloga ovih tipova ključa detaljno je opisano u poglavlju 4.3.

Primjer *DNSKEY* zapisa je sljedeći:

tvrtka.hr 3600 IN DNSKEY 257 3 5 AQPWA4BRyjB3eq YNy/oykeGcSXjl+HQK9CciAxJfMcS1vEuwz9c+QG7sEJnQuH5B9i5o/ ja+DVitY3jpXNa12mEn

*DNSKEY* zapis sastoji se od četiri polja koja ujedno tvore i svojstva dotičnog zapisa. Svojstva zapisa detaljno su opisana u sljedećoj tablici u svrhu prikaza njihovih uloga. Bitno je napomenuti kako kako se prva četiri atributa ne promatraju budući da oni pripadaju jednom *RRSET-u.*

|  |  |  |
| --- | --- | --- |
| Vrsta svojstva | Primjer svojstva | Opis svojstva |
| Polje zastavica | 0, 256, 257 | Sastoji se od dva okteta, odnosno 16-bitnog polja koja specificiraju ulogu javnog ključa. U polju zastavica jedino bitovi 7 i 15 imaju vrijednosti 0 i 1. Ukoliko bit 7 ima vrijednost 1 ključ se može koristiti za potpisivanje zone (*ZSK*) i tada svojstvo iznosi 256. Ukoliko također bit 15 ima vrijednost 1 , dolazi do pojave sigurnosne točke ulaza *SEP* (*eng. Secure Entry Point*) koja određuje koji od *DNSKEY* zapisa odgovara *KSK* ključu, u ovom slučaju to je zapis sa *SEP* zastavicom. |
| Protokol | 3 | Ovaj tip svojstva je uvijek iste vrijednosti jer potječe iz starije verzije *DNSSEC-a* gdje su se ključevi mogli koristiti u različite svrhe. |
| Vrsta algoritma | 5 | Specificira algoritam korišten pri izradi digitalnog potpisa, te mora biti jednak kao i algoritam u kasnije spomenutom *RRSIG* zapisu. |
| Javni ključ | AQPWA4BRyjB3eqYNy/oykeGcSXjl+HQK9CciAxJfMc1vEuwz9c+QG7sEJnQuH5B9i5o/ja+DVitY3jpXNa12mEn | Sadrži koje u sebi sadrži javni ključ enkodiran putem sustava Base64[[3]](#footnote-3) |

* + 1. RRSIG zapis

Kako je već spomenuto *DNSSEC* koristi digitalni potpis u svrhu autentikacije prilikom slanja potrebnih informacija. Upravo se prilikom spomenutog potpisivanja koriste *RRSIG* zapisi u kojima se nalazi digitalni potpis potreban za proces autentikacije. U tu svrhu *RRSIG* zapisi se sastojeod svojstava koja su prikazana u tablici 4. Primjer *RRSIG* zapisa je sljedeći:

odjel.tvrtka.hr. 3600 RRSIG A 5 3 3600 20200601235559 20200515235559 3674 tvrtka.hr ZZP9AV28r824SZJqyIT +3WKkMQgcu1YTuFzpLgU3EN4USgpJhLZbYBqTHL77mipET5aJr8 OdRxZvfFHHYV6UGw==

|  |  |  |
| --- | --- | --- |
| Naziv svojstva | Primjer svojstva | Opis svojstva |
| Vrsta algoritma | 5 | Upućuje koja vrsta algoritma je korištena za enkripciju pri izradi digitalnog potpisa, te je jednaka vrijednosti algoritma korištenog u *DNSKEY* zapisu. U ovom slučaju se radi o *RSA/SHA-1[[4]](#footnote-4)* algoritmu. |
| Broj labela | 3 | Broj labela od kojih je sastavljeno domensko ime |
| Izvorni *TTL* | 3600 | Prikazuje vijek trajanja zapisa koje potječe od izvornog zapisa. |
| Vrijeme isteka potpisa | 20200601235559 | Vrijeme kada zapis istječe, te je izraženo u formatu GGGGMMDDHHMMSS |
| Vrijeme početka potpisa | 20200515235559 | Vrijeme kada zapis počinje, te je izraženo u formatu GGGGMMDDHHMMSS |
| Oznaka ključa | 3674 | Oznaka ključa derivirana iz javnog ključa koja korespondira sa tajnim ključem korištenim za digitalno potpisivanje. Svrha ove oznake je pronalazak ispravnog ključa ukoliko ih postoji više od jednog. |
| Naziv podrijetla potpisa | tvrtka.hr. | Identificira naziv vlasnika *DNSKEY* zapisa koji je potreban za potvrdu digitalnog potpisa. |
| Polje potpisa | ZZP9AV28r824SZJqyIT+3WKkMQgcu1YTuFzpLgU3EN4USgpJhLZbYBqTHL77mipET5aJr8OdRxZvfFHHYV6UGw== | Sadrži digitalni potpis tajnog ključa zone potpisanih zapisa enkodiranog putem sustava Base64 |

* + 1. DS zapis i lanac povjerenja

U teoriji sigurnosnih ekstenzija *DNS-a* također postoji još jedan vrlo bitan pojam pod nazivom lanac povjerenja (*eng. Chain of Trust*). Kako je vidljivo iz prijašnjeg teksta svaki *RRSET* u potpisanoj zoni posjeduje *RRSIG* zapis s kojim je povezan. Kako bi provjera *RRSIG* zapisa bila moguća, svaka zona ima zadaću isporučiti svoj javni ključ putem *DNSKEY* zapisa.

No iz sigurnosnog aspekta u svakom trenutku postoji mogućnost neovlaštenog pristupa *DNS* poslužitelju u svrhu zlonamjernih radnji. Takve radnje mogu imati za cilj izmjenu podataka u zoni i potpisati *DNS* zonu sa potpuno različitim generiranim parom ključeva.

Kako bi se takvim radnjama stalo na kraj, javni ključ je potrebno certificirati od strane višeg autoriteta. Viši autoritet potvrđuje činjenicu kako javni ključ u *DNSKEY* zapisu, određenog domenskog imena uistinu pripada njegovoj zoni, a u ovom slučaju spomenuti viši autoritet je nadređena zona, odnosno zona vršne razine u obliku hr. oznake. Prije provedbe certificiranja, viši autoritet zahtjeva jednu vrstu dokaza kojim se dokazuje identitet osoba nadležnih za tvrtka.hr domenu, dobiven prilikom kreiranja domene. Potom slijedi generiranje para ključeva, nakon čega se javni ključ šalje u smjeru nadređene zone zajedno za dokazom o identitetu. Jednom kada nadređena zona zaprimi dobivene podatke, dolazi do stvaranja novog *DS* zapisa potpisanog tajnim ključem u njenoj zoni.

*DS* zapis također posjeduje svoja svojstva koja su objašnjena u tablici 5, a prikazana u sljedećem primjeru:

tvrtka.hr 3600 DS 15480 5 1 F340F3A05DB4D081B6D3D749F300636DCE3D

|  |  |  |
| --- | --- | --- |
| Naziv svojstva | Primjer svojstva | Opis svojstva |
| Oznaka ključa | 15480 | Kao i kod *RRSIG* zapis, pomaže pri pronalasku *DNSKEY* zapisa potrebnog za digitalno potpisivanje. |
| Vrsta algoritma | 5 | Također ima istu svrhu kao i kod *DNSKEY* i *RRSIG* zapisa, te govori koja je vrsta algoritma korištena u *DNSKEY* zapisu. |
| Tip skupa znakova (*eng.digest*) | 1 | Identificira koji je algoritam korišten za izradu skupa znakova. |
| Skup znakova | F340F3A05DB4D081B6D3D749F300636DCE3D | Stvarni skup znakova dobiven na temelju *KSK* ključa *DNSKEY* zapisa iz prethodog algoritma. |

Kada se prati proces provjere *DNSKEY* zapisa, uvijek se promatra od strane nadređene zone. Prvi korak u tom procesu jest provjera *RRSIG* zapisa koji potpisuje *DS* zapis. Uz pretpostavku kako je *DS* zapis digitalno potpisan, DNS poslužitelj pretražuje DNSKEY zapis u podređenoj zoni uz pomoč oznake ključa i vrste algoritma opisanih u tablici 5. Nakon što je pronašao DNSKEY zapis, poslužitelj provlači isti zapis kroz algoritam potreban za dobivanje skupa znakova. Nakon dobivenog skupa znakova vrši usporedbu sa skupom znakova iz DS zapisa, te ako se oba skupa podudaraju DNSKEY zapis je autentičan i može se koristiti za proces provjere RRSIG zapisa.

* + 1. NSEC zapis

Svrha *NSEC* zapisa je vrlo bitna u sigurnosnim ekstenzijama *DNS* sustava. Kao što je u uvodu spomenuto *DNSSEC* posjeduje mogućnost pružanja potvrde dokaza o nepostojanju što kasnije rezultira vrlo važnim informacijama. U slučaju kada korisnik šalje zahtjev za razrješenjem nepostojećeg domenskog imena na primjer odjel1.tvrtka.hr, u zoni koja nije potpisana, poslužitelj mu tada vraća prazan odgovor. Loša strana takvih odgovora jest što ne posjeduju nikakve zapise o resursima, te samim time ne mogu biti digitalno potpisani. Upravo tada dolaze do izražaja *NSEC* zapisi koji su potrebni za provedbu dokaza o nepostojanju. *NSEC* zapis obuhvaća prostor između dva domenska imena u *DNS* zoni, te govori koje sigurno domensko ime je sljedeće po redu, te na taj način usmjerava na domensko ime odjel.tvrtka.hr. U svrhu pronalaska sljedećeg sigurnog domenskog imena sva imena moraju biti poredana abecednim redom gledajući od desne strane potpune forme imena.

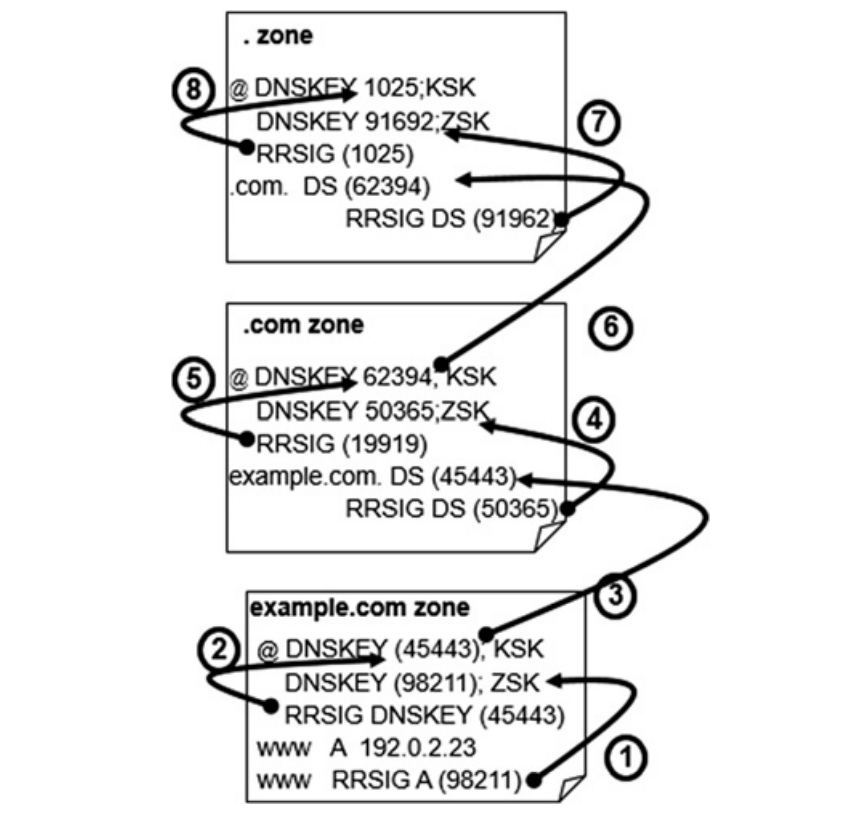
Primjer *NSEC* zapisa je sljedeći:

odjel1.tvrtka.hr NSEC odjel.tvrtka.hr. A MX RRSIG NSEC DNSKEY

Ovaj zapis govori kako se radi o *NSEC* tipu zapisa o resursu, zatim slijedi potpuna forma sljedećeg sigurnog domenskog imena koji je u abecednom poretku posljednji. Sljedeći podatci ukazuju na zapise koji se također nalaze u sljedećem sigurnom domenskom imenu, poput *A, MX, RRSIG, NSEC* i *DNSKEY* zapisa.

* 1. DNSSEC proces razrješenja

Osnovni proces *DNS* razrješenja opisan u poglavlju 2.5 ostaje prilikom *DNSSEC* procesa nepromijenjen. Također sama *DNS* rezolucija zadržava sve korake u obliku silaska kroz hijerarhijsko stablo koji su potrebni u svrhu dostavljanja odgovora na rekurzivne i iterativne upite. Vezano za *DNS* razrješenje, proces digitalnog potpisivanja i provjere istog moguće je započeti tak kada je *DNS* razrješenje završeno, te se na temelju dobivenih podataka vrši provjera.



Slika 7. DNSSEC proces (izvor: Dooley, Michael; Rooney, Timothy: DNS Security Management)

Sam proces *DNSSEC* razrješenja prikazan je u sljedećim koracima praćenim kroz prethodno objašnjeno sidro povjerenja, koje se kreće uzlazno sve do korijenske zone, uz pretpostavku kako rekurzivni poslužitelj zaprima upit [www.primjer.com](http://www.primjer.com).

U prvom koraku rekurzivni poslužitelj potvrđuje zaprimljeni odgovor u obliku A zapisa na način da dekriptira digitalni potpis odgovora što rezultira određenim skupom znakova. Nakon toga uzima izvorni odgovor korištenjem hash funkcije također dobiva skup znakova. Na posljetku vrši usporedbu nad skupovima znakova, te ako se isti podudaraju započinje proces potvrde *KSK* ključa.

U drugom koraku provodi se proces potpisivanja zone na isti način kao i u prvom koraku, osim što umjesto odgovora na upit stoji *ZSK* ključ koji je potrebno potvrditi putem *KSK* ključa i digitalnog potpisa od *DNSKEY* zapisa. nakon što su izvršene ove dvije potvrde, rekurzivni poslužitelj može potvrditi kako je odgovor potpisan od zone u kojoj se nalazi domena primjer.com. No u tom trenutku *KSK* ključ nije vjerodostojan jer nije postavljen kao sidro povjerenja.

U trećem koraku rekurzivni poslužitelj provjerava da li je domena primjer.com povezana lancem povjerenja prema nadređenoj zoni, u ovom slučaju zona vršne razine sa oznakom .com. Ta provjera se vrši putem *DS* zapisa u nadređenoj zoni. *DS* zapis tada pruža skup znakova dobivenog od *KSK* ključa iz podređene zone u svrhu provjere autentičnosti istog.

Četvrti korak pruža proces potvrde *DS* zapisa putem digitalnog potpisa *DS* zapisa i *ZSK* ključa koji se nalazi u *DNSKEY* zapisu pripadajuće zone. Dok peti korak pruža proces provjere i potvrde ključeva u zoni sa oznakom .com na isti način kao i u drugom koraku.

Ponavljajući korake sve do korijenske zone, u koracima od šest do osam, dolazi se do potvrde potpisa za korijensku zonu putem *KSK* ključa.

Opisanim procesom može se utvrditi autentičnost i integritet zaprimljenih odgovora pošto sve razine u hijerarhijskoj strukturi *DNS-a* pripadaju lancu povjerenja.[3]

Literatura

[1] Hinshelwood, David: URL:<https://www.sans.org/readingroom/whitepapers/dns/dns-dnssec-future-1054>, 6.2.2020.

[2] Korunić, Dinko: DNS priručnik: URL: <https://sysportal.carnet.hr/system/files/DNS-prirucnik-1_5.pdf>, 9.2.2020.

[3] Dooley, Michael; Rooney, Timothy: DNS Security Management

[4] Laboratorij za sustave i signale, Fakulteta elektrotehnike i računarstva, Sveučilišta u Zagrebu: URL: <https://www.cis.hr/files/dokumenti/CIS-DOC-2012-06-052.pdf>, 9.3.2020.

[5] Aitchison, Ron: Pro DNS and Bind 10

[6] Liu, Cricket; Albitz, Paul: DNS and BIND

[7] Kolkman, O; Gieben, R: DNSSEC Operational Practices, 18.2.2020.

[8] <https://securityintelligence.com/articles/what-is-a-ddos-attack/>

[9] Liska, Allan; Stowe, Geoffrey: DNS Security Defending the Domain Name System

1. Američki računalni znanstvenik koji se smatra tvorcem DNS tehnologije [↑](#footnote-ref-1)
2. Mrežni protokol za dinamičko dodjeljivanje IP adresa [↑](#footnote-ref-2)
3. Base64 je algoritam koji omogučava pretvorbu binarnih brojeva u znakove [↑](#footnote-ref-3)
4. Kriptografski algoritam koji proizvodi 160-bitnu vrijednost u obliku skupine znakova [↑](#footnote-ref-4)