



UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE
-Savremene informacione tehnologije-

DNSSEC kao zaštita DNS servisa na internetu

- Master rad -

Mentor:

Prof. Dr Mladen Veinović

Student:

Aleksandar Kostadinović

Br. indeksa: 410365/2013



Beograd, 2014.

Sadržaj

Sadržaj	1
1. Metodologija istraživačkog projekta	3
1.1. Uvodne napomene	3
1.2. Predmet istraživanja	3
1.3. Ciljevi i zadaci istraživanja	4
1.4. Metode istraživanja	4
1.5. Hipotetički okvir	5
2. DNS – Domain Name System	6
2.1. Šta je i kako radi DNS sistem	6
2.2. Hijerarhijska podela DNS servera	8
3. Slabosti i nedostaci DNS sistema i servera	11
3.1. Cache poisoning (Kaminsky bug)	12
3.2. Posledice Cache Poisoning-a	15
4. Pojam DNSSEC i njegova geneza	17
4.1. Istorijat DNSSEC	17
4.2. Šta je DNSSEC i kako štiti DNS zone	18
4.3. Pregled stanja uvođenja DNSSEC u svetu	23
5. Uvod u tehnologiju DNSSEC-a	27
6. Kako DNSSEC radi	28
6.1. DNSSEC tehnologija	28
6.1.1. Server na kome se kreira i drži DNS zona	29
6.1.2. Softver pomoću koga se digitalno potpisuje DNS zona	34
6.1.3. Uređaji za generisanje i čuvanje tajnih softverskih ključeva za potpisivanje zone	38
6.1.4. Serveri za razrešavanje DNS upita korisnika i verifikaciju DNSSEC potpisa	42

7. Slabosti DNSSEC-a.....	44
7.1. Visoki troškovi	44
7.2. Komplikovanost sistema	44
7.3. Podložnost DDoS napadima.....	45
8. Forenzička analiza HSM uređaja i DNS servera.....	49
8.2. Forenzička analiza u opštem slučaju	49
8.3. Forenzička analiza HSM uređaja	50
8.4. Forenzička analiza DNS servera	51
9. Studija slučaja uvođenja DNSSEC	55
9.1. Studija slučaja SurfNET i DNSSEC	55
9.2. Vremenski plan uvođenja DNSSEC u DeNIC	59
10. Zaključak	61
Literatura	63
Indeks pojmova	64

1. Metodologija istraživačkog projekta

1.1. Uvodne napomene

DNS (Domain name system) je nastao zbog osobine čoveka da znatno lakše pamti imena nego kombinacije brojeva i tako umesto samo IP adresama obeležio računare i pamtljivim imenima. Tako uprošćeno posmatrano DNS je ništa drugo do distribuirani imenik IP adresa i imena servera i servisa na internetu. I pored toga što ovo deluje kao jednostavna uloga važnost DNS servisa je neizmerno velika i kompletan današnji internet je zasnovan na njemu.

Početak korišćenja DNS-a vremenski koincidira sa početkom korišćenja prvih računarskih mreža. Tada je zbog malog broja računara u prvim eksperimentalnim mrežama bilo moguće zapisati sva imena računara i njihove IP adrese i jedan tekstualni fajl koji se zvao hosts čija se kopija nalazila na svakom od računara u toj mreži.

Sa rastom veličine mreže i brojem računara u toj mreži i današnjem internetu, bilo je potrebno zameniti hosts fajl drugačijim sistemom jer bi veličina hosts fajla rasla do neslučenih razmera. Tada je nastao DNS onakvim kakav je danas. Sistem distribuiranih servera podeljenih hijerarhijski, koji kada se svi zajedno sabere sadrže podatke o svim imenima servera i servisa u svim javnim domenskim prostorima na svetu, ali ni jedan server sam nema sve podatke koji su mu potrebni.

DNS sistem nije imao evoluciju načina rada kroz vreme, nije se menjao kroz vreme, pa samim tim njegova konstantnost i po malo zastarelost ga čini ranjivim na nekoliko nivoa. Tema ovog rada je jedna od ranjivosti DNS sistema i analiza jednog od načina da se ta slabost ojača i zaštititi. Figurativno rečeno svaki lek ima i svoje nuspojave pa će i o tome biti reči u ovom istraživanju.

Iako je DNS servis najšire moguće korišćen, među običnim korisnicima on je gotovo potpuno nepoznat, pa čak i među populacijom koja se konkretno bavi informatikom, ovaj servis je pomalo u magli kada je vladanje njime u pitanju. DNS servisom se obično bave mrežni i sistem administratori kojima je to specijalnost, pogotovo kod velikih internet i hosting provajdera ili kod nacionalnih registara Internet domena. Zbog ovog generalnog nepoznavanja ne pridaje se dovoljna pažnja potencijalnim problemima i manipulacijama koje mogu nastati zlomernim korišćenjem DNS servera, a čije žrtve obično budu obični korisnici.

1.2. Predmet istraživanja

Osnovni predmet istraživanja ovog rada je korišćenje kriptografskih metoda i digitalnih potpisa da bi se zaštitio jedan od osnovnih sistemskih servisa na internetu. Najpre će biti istraženi osnovni pojmovi samog sistema, a centar istraživanja će zauzeti komparativna analiza nekoliko

različitih implementacija zaštite DNS servisa korišćenjem DNSSEC (Domain Name System Security Extensions).

Pored osnovnog predmeta istraživanja u radu će biti istražen i sam DNS servis da bi se njegovim potpunim razumevanjem lakše shvatile njegove slabosti, a kroz te slabosti i sam osnovni predmet istraživanja koji štiti od jedne od tih slabosti.

Takođe, u radu će se koristiti studije slučaja koje će pokazati potrebu za uvođenjem DNSSEC-a kao i studije slučaja organizacija koje su dokumentovale svoj proces uvođenja DNSSEC ekstenzija.

1.3. Ciljevi i zadaci istraživanja

Cilj istraživanja je da otkrije koji način korišćenja DNSSEC-a je najisplativiji u smislu hardversko-softverskih, ljudskih i finansijskih resursa. Koliko je DNSSEC upotrebljiv i koliko se koristi u stvarnosti.

Istraživanje treba da pokaže da li i sam DNSSEC ima svoje slabosti, da li njegovim korišćenjem i šticevanjem jedne slabosti otvaramo neku drugu slabost u nekom drugom sistemu ili servisu koji se koristi na internetu. Istraživanje takođe treba da pokaže i korisnost uvođenja DNSSEC, iskorišćenost zaštićenih i potpisanih DNS zona, finansijsko opterećenje kao i uticaj na performanse kompletnog DNS sistema, i da li sve to ima smisla u poređenju sa pretnjom od koje DNSSEC štiti, zatim koliko je njegovo korišćenje ispraćeno od proizvođača softvera i operativnih sistema, kao i koja je budućnost ovakvog načina zaštite DNS sistema.

1.4. Metode istraživanja

Da bi se ostvarilo ovo istraživanje koristiće se opšte i osnovne naučne metode istraživanja. Od osnovnih metoda istraživanja biće potrebno koristiti indukciju, dedukciju, analizu i klasifikaciju. Od opštih naučnih metoda biće korišćene statističke metode i komparacija studija slučaja.

U istraživanju će dominantna metoda prikupljanje postojećih podataka, bazična statistička obrada i interpretacija podataka. Na osnovu svih prikupljenih podataka i nakon kompletne opservacije stanja koristiće se induktivne i deduktivne metode da bi se izvukli zaključci koji će potvrditi ili opovrgnuti osnovnu i druge hipoteze koje se nalaze u radu.

Podaci za statističku analizu biće prikupljeni najčešće sa interneta ali sa internet prezentacija organizacija čiji kredibilitet kao i kredibilitet podataka se ne može dovoditi u pitanje (ICANN, IANA, RIPE, EU Rid i slično).

Pošto implementiranje DNSSEC-a nije ni malo jeftino zbog hardvera i softvera koji je potreban, nije ni malo jednostavno zbog politika i pravila koje svaka organizacija koja uvodi DNSSEC mora da donese da bi implementacija bila valjana i da bi uspešno dokumentovala sve slučajeve korišćenja ili eventualnih problema koji mogu da eskaliraju. Iz tih razloga nije moguće uraditi na mikro nivou samu implementaciju već će biti korišćena tuđa iskustva a uglavnom nacionalnih registara domenskih imena i iskustva univerziteta sa eksperimentalnim implementacijama DNSSEC.

Informacije o implementacijama u nacionalnim registrima internet domena su pribavljene najčešće direktno od osoba ili timova koji su sprovodili uvođenje DNSSEC-a, a informacije o primeni DNSSEC na univerzitetima i kampusima je pribavljano iz javnih repozitorijuma sa Interneta. Naknadno su ove informacije ujednačavane i standardizovane radi lakšeg upoređenja u ovom istraživanju.

1.5. Hipotetički okvir

Ovo istraživanje treba da pokaže ili opovrgne tačnost opšte i nekoliko pojedinačnih hipoteza. **Opšta hipoteza** je „DNSSEC je generalno koristan dodatak DNS serverima i da se njegovim korišćenjem podiže nivo bezbednosti korisnika pogotovo kada koriste servise i web sajtove koji zahtevaju prenos poverljivih informacija između korisnika i servera (ebanking i plaćanje preko interneta i sl.)“.

Pojedinačnih hipoteza ima nekoliko i one su sledeće:

1. Treba takođe pokazati da li je DNSSEC isplativ kao zaštitno sredstvo i da li je dovoljno iskorišćen.
2. Da li je moguće korisnije organizovati DNS zone i servere tako da se smanje troškovi implementacije i održavanja kao i rizici upotrebe?
3. Da li je i kako moguće zaštititi i sam DNSSEC od slabosti koje se javljaju njegovom primenom?

2. DNS – Domain Name System

2.1. Šta je i kako radi DNS sistem

Kao što je u uvodu istraživanja pomenuto, DNS sistem postoji od samih početaka računarskih mreža i danas je sastavni deo globalne računarske mreže, a isto tako i malih unutrašnjih mreža koje nisu povezane sa Internetom iz bezbednosnih razloga. Da bi se raščlanili pojmovi vezani za DNS potrebno je razumeti sledeće na samom početku. DNS je generičko ime za sam proces, DNS server je softver na nekom hardverskom uređaju, koji pruža uslugu DNS servisa. Ta tri pojma se prepliću i potrebno je jasno znati na šta se odnosi koji od njih sistem, servis ili server.

DNS servis služi za prevođenje alfa-numeričkih (slovnih naziva kao na primer www.nba.com) u brojeve nazive u formatima IPv4 i/ili IPv6. Ovo je potrebno zbog veće asocijativnosti ljudi ka alfa-numeričkim nazivima nego ka samo numeričkim i zbog lakšeg pamćenja [1]. Time je jasno da je osnovna funkcionalnost DNS-a slična telefonskom imeniku. Međutim, zbog ogromnog broja računara na mreži, i zbog veličine baza na DNS serverima koje uparuju nazive i IP adrese, potrebno je ovaj sistem podeliti na slojeve i distribuirati baze podataka hijerarhijski na više različitih servera.

Korisnik koji na primer, želi da napravi upit za neki web sajt (na primer www.primer.rs), odgovor može dobiti na nekoliko načina. Prvi način je jako redak, a on podrazumeva da je korisnik, ili sistem administrator u kompaniji u kojoj korisnik radi, uneo predefinisane vrednosti za određene domene u sam Hosts fajl. Ovo se radi najčešće u slučaju nekih unutrašnjih servisa za koje nije pametno ili praktično oglašavati na javnoj internet mreži.

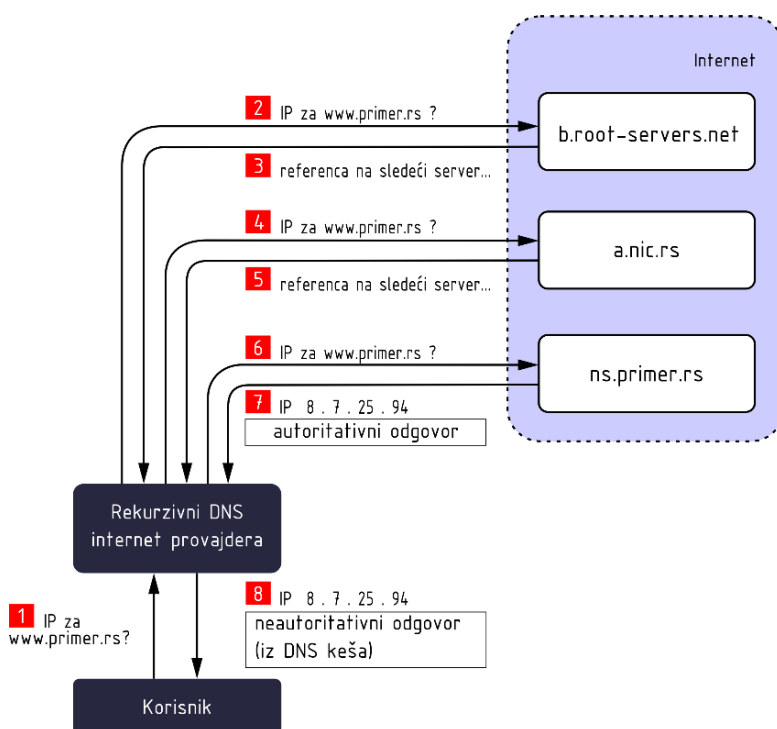
```
$# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
#      102.54.94.97      rhino.acme.com      # source server
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
```

Primer 1. – Sadržaj hosts fajla na Windows računarima

Drugi način na koji korisnik može dobiti odgovor je direktno iz keša servera provajdera ili kompanijskog servera. Ovo je slučaj ukoliko je neko već pitao za taj domen ranije i server je zapamtio odgovor na neko vreme radi brže reakcije ka novim korisnicima koji pitaju za isti domen.

Treći način opisuje potpuni proces komunikacije DNS servera i on se zove rekurzivni način. Korisnik šalje upit za web sajt www.primer.rs ka DNS serveru svog internet provajdera, koji zatim prosleđuje svoje pitanje ka root serverima koji su na samom vrhu lanca. Root serveri upućuju DNS server internet provajdera da pita server koji je autoritativan za .rs domen. Zatim, DNS server za .rs domen upućuje DNS server provajdera ka DNS serveru nadležnom za sam rnds.rs domen, koji će na kraju dati odgovor gde se nalazi www zapis u njegovoj tabeli. Taj odgovor se na kraju prosleđuje korisniku kao konačan [15].

Drugi i treći način korišćenja DNS upita se može videti na slici ispod, A sama hijerarhija DNS servera i njihove nadležnosti i autoritativnosti su objašnjeni u narednom poglavlju.

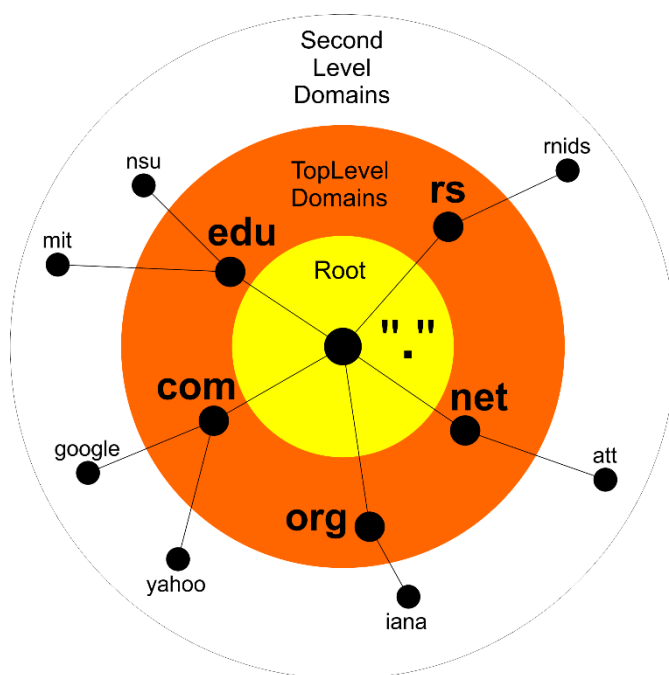


Slika 1. – Grafički prikaz rekurzivnog upita kroz mrežu DNS servera [18]

Zbog ovoga se često kaže da su DNS serveri jedna posebna mreža sebe, koja međusobno komunicira, jer kada jedan DNS server nema informaciju o nečemu, on pita sledeći server i tako dok ne dobije informaciju koja IP adresa odgovara uz traženi naziv.

2.2. Hijerarhijska podela DNS servera

Spisak računara na internetu koji bi se mogao naći u bazama DNS servera je ogroman, pa samim tim nije moguće izvesti da svaki server ima sve podatke u sebi. Iz tog razloga podaci su hijerarhijski podeljeni po nivoima i na samom dnu po domenima i svaki server je autoritativan za neki sloj, grupu servera ili domen. Šema DNS servera po slojevima se nalazi na slici 2.



Slika 1. – Šema DNS servera podeljenih po slojevima i grupama za koje su autoritativni

Najviši nivo servera su takozvani root serveri. U njihovim tabelama su upisani autoritativni DNS serveri za Top Level Domene (TLD), za generičke Top Level Domene (gTLD) i za Country Code Top Level Domene (ccTLD). Opis i primeri ovih domenskih prostora je u indeksu ovog rada.

Od ovih servera počinju svi upiti naniže ka ciljanoj informaciji za domen, pa samim tim bez ovih servera DNS lanac bi bio presečen. Postoji 12 organizacija koje upravljaju root DNS serverima, a verovanje da na svetu postoji samo 13 ovih servera je netačna.

Duplikati ovih servera objavljeni kroz takozvani anycast sistem se nalaze svuda po svetu, te root DNS servera zaista ima oko 140 trenutno. Osnovna lista root DNS servera se nalazi u tabeli 1 ispod a na slici 3 se može videti geografski raspored root DNS servera.

Tabela 1. – root DNS serveri sa IP adresama i organizacijama koje njima upravljaju [10]

Ime servera	IP Adrese	Upravljanje
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201	University of Southern California (ISI)
c.root-servers.net	192.33.4.12	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defence (NIC)
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:3::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project



Slika 2. – Geografski prikaz root DNS servera [10]

Na lestvici niže se nalaze DNS serveri odgovorni za Top Level Domene (.com, .net, .info ...), za Country Code Top Level Domene (.rs, .cpđ, .se, uk ...) i za nove generičke Top Level Domene koji su trenutno u procesu usvajanja (.gmail, .dell, .book ...). Za ove DNS servere su zadužene organizacije kojima je ICANN po ugovoru delegirao odgovarajuće domenske prostore na upravljanje. Tako na primer svakim nacionalnim domenom (ccTLD) upravlja odgovarajuća nacionalna organizacija koja bi trebalo da je ustrojena po pravilima ICANN-a, te u Srbiji domenskim prostorom upravlja RNIDS, u Nemačkoj DeNIC, u Francuskoj Afnic i tako redom. Organizacije koje su dobile pravo upravljanja Top Level Domenima su na primer

Networksolutions za .com, zatim VeriSign za .net domen i Public Internet Registry za .org domenski prostor. Kada su u pitanju novi generički Top Level Domeni različite kompanije su licitirale za odgovarajuće domenske prostore koji su im interesantni pa su shodno tome dobijali pravo da upravljaju tim domenskim prostorom.

Korak niže se nalaze najčešće DNS serveri internet i hosting provajdera koji pružaju usluge krajnjim korisnicima ili DNS serveri velikih organizacija i kompanija koji sami upravljaju svojim domenskim prostorom.

Tako, prema šemi sa slike 1., kada neki računar pita DNS server za odgovarajući domen, on dobija odgovore redom od najvišeg nivoa pa sve niže dok ne dobije tačnu informaciju koja ga interesuje, bilo da je to www zapis to jest adresa nekog web sajta ili da je MX zapis što upućuje na adresu nekog servera za elektronsku poštu ili neki drugi tip zapisa koji odgovara nekom posebnom servisu ili serveru.

Ovakvom raspodelom odgovornosti DNS servera omogućava se da svaki server sadrži set podataka koji nije prevelik za upravljanje ni zbog odgovornosti ni zbog korišćenja resursa, postiže se redundantnost i otpornost na situacije u kojima neki od servera prestaju da rade.

3. Slabosti i nedostaci DNS sistema i servera

Kao i praktično svaki ljudski proizvod, ako smo u domenu samo informatike, hardver ili softver, tako i DNS sistem ima svoje nedostatke, slabe strane, koje se pokazuju ređe same od sebe u radu sistema ili češće njih otkrivaju stručnjaci za bezbednosne propuste, bilo da su namere stručnjaka vezano za bezbednosna otkrića dobre ili loše.

Dodatna otežavajuća okolnost vezana za DNS sistem je to što je on takav od početka računarskih mreža i interneta, jako je malo evoluirao i jako se malo menjao jer bi između ostalog te promene pravile još veće gotovo tektonske promene u samom internet sistemu. Naravno, promene je moguće praviti na mikro nivou na samim DNS serverima kao i u organizacionom smislu.

Slabosti DNS sistema ima puno ali se mogu podeliti u nekoliko kategorija. Podela je izvršena prema tome kako slabost utiče na DNS sistem. Kategorije slabosti bi bile sledeće:

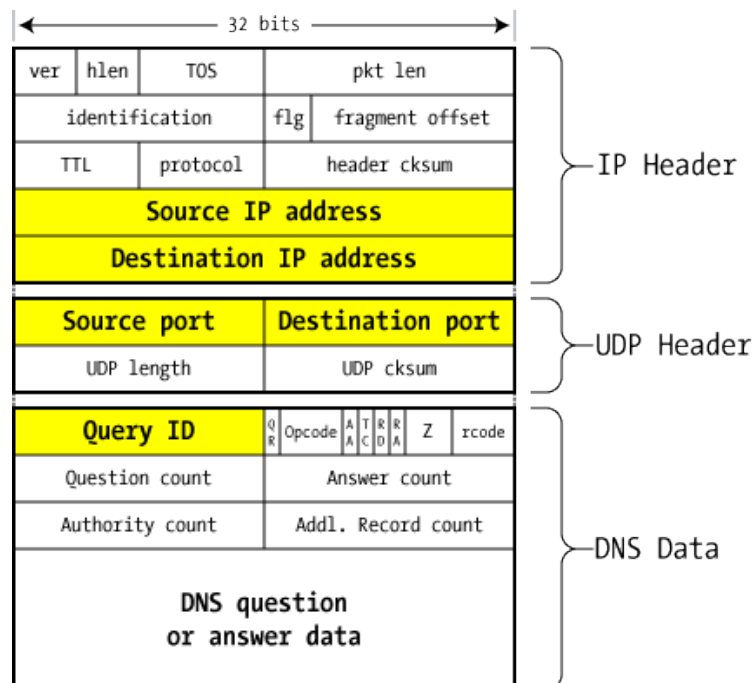
- **DoS i DDoS (Denial of Service i Distributed Denial of Service)** – ovo je najopštija slabost sistema, kojoj su podložni i svi ostali sistemi koji funkcionišu na internetu. Ova slabost se bazira na tome da sistem ne može da odgovori na dovoljan broj zahteva koji su mu poslani, ne može da zatvori započete komunikacije koje ostaju otvorene i vremenom se resursi potroše i server ostaje u stanju u kome ne može da ostvari svoju namenu.
- **Slabosti kod dinamičkog ažuriranja DNS servera** – DNS sistem ima mogućnost da dinamički ažurira svoje zapise u bazi tako što prepoznaje kada je neki računar čija adresa se nalazi u bazi promenio IP adresu ukoliko adrese dobija od nekog DHCP sistema. Dinamičko ažuriranje pruža mogućnost da se unesu neispravne i lažne adrese maskirajući se kao ispravan sistem koji daje svoju dinamičku konfiguraciju.
- **„Curenje“ važnih informacija** – Zlonamerni napadač može koristeći setove komandi ili slabosti u prepunjavanju specijalnih memorijskih bafera da dođe do podataka važnih za bezbednost DNS servera ili do podataka korisnika koji se nalaze na tim serverima a nisu namenjene za javnost.
- **Lažiranje podataka** – U ovu kategoriju spadaju slabosti koje omogućavaju da krajnji korisnik bude prevaren od strane „Rogue“ servera korišćenjem „spoof-ovanih“ lažiranih IP adresa a takođe i postoji opasnost od takozvanog napada „Man in the Middle“ gde se napadač postavlja između korisnika i DNS servera i lažira podatke da bi prevario krajnjeg korisnika.
- **Cache poisoning (Kaminsky attack)** – Ova slabost predstavlja jednu od najopasnijih narušenih bezbednosnih tačaka. Slabost podrazumeva da zlonamerni korisnik može da izmeni podatke u kešu DNS servera i samim tim krajnjem korisniku isporučuje lažirane podatke. Više o ovoj slabosti i načinima da se prevaziđe biće reči u narednim poglavljima [22].

3.1. Cache poisoning (Kaminsky bug)

U julu 2008. godine CERT (Computer Emergency Response Team stacioniran u Karnegi Melon univerzitetu u Picburgu) je objavio da je Den Kaminski pronašao veliki propust u DNS sistemu i većini DNS servera koji omogućava napadaču da „zatreje“ keš DNS servera neispravnim podacima i na taj način prevari krajnje korisnike koji prave upit ka tim serverima. Ovaj propust je obuhvatao skoro sve DNS servere osim nekoliko koji nisu bili ni zastupljeni u nekom ozbiljnom broju na internetu, te je na samom početku pristupa ovom problemu zavladała panika. Ovaj fundamentalni propust se nalazio u samom DNS protokolu tako da su njegovom implementacijom serveri praktično nasledili taj propust od samog početka umrežavanja računara.

Nakon objavljivanja ovog propusta u DNS protokolu Den Kaminski je radio u tajnosti sa proizvođačima DNS softvera sa ciljem otklanjanja propusta iz softvera DNS servera, međutim to nije u potpunosti bilo moguće jer je propust u samom DNS protokolu, koji nije moguće izmeniti a da se pri tome ne prave ogromne izmene u načinu funkcionisanja modernog interneta.

Da bi se podrobnije objasnio ovaj propust neophodno je najpre je potrebno razumeti kako izgleda jedan DNS paket i koji su njegovi osnovni delovi. Na slici ispod je šematski predstavljen jedan DNS paket sa svim svojim sastavnim delovima, a žutom bojom su obeleženi delovi koji su uzrok ove slabosti protokola.



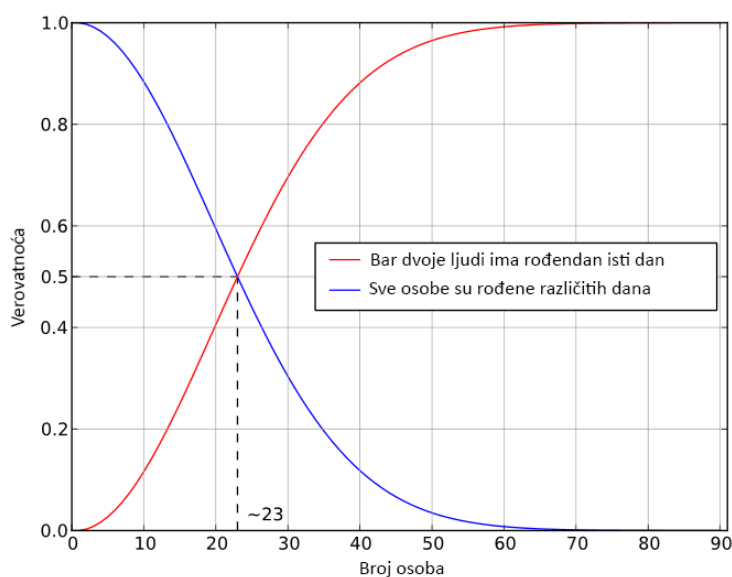
Slika 4. – Izgled paketa jednog DNS upita sa svojim sastavnim delovima (žuto obeleženi su segmenti potrebni za iskorišćavanje Kaminsky propusta)

Source/Destination IP adresa – Ovaj podatak je bitan jer pokazuje koji računar komunicira sa serverom. Moguće je falsifikovati Source adresu (takozvani spoofing) ali je besmisleno menjati destination adresu jer onda paket neće stići na željeno mesto, u ovom slučaju DNS server.

Source/Destination port number – U ovom delu paketa zapisani su portovi po kojim komuniciraju računar i DNS server. Startni DNS port na kome komunikacija počinje i koji server osluškuje je 53 ali se komunikacija može voditi i po drugim portovima.

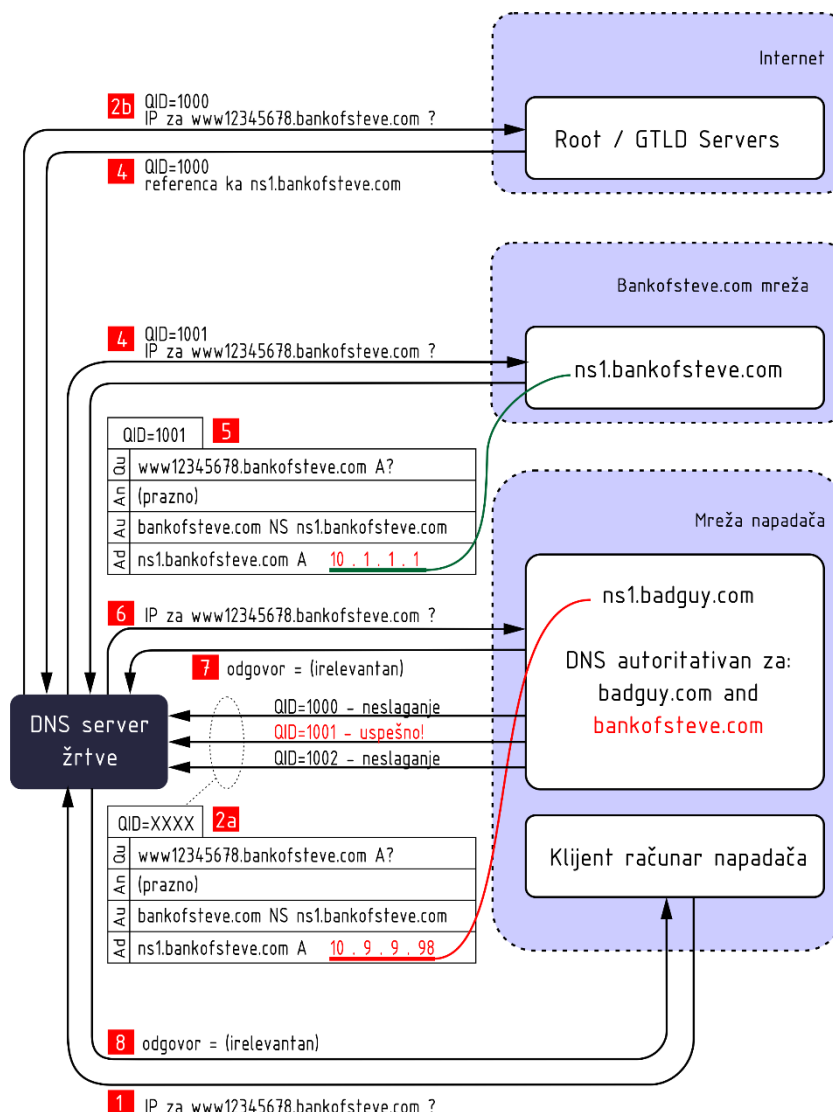
Query ID – Ovaj podatak ima najveću ulogu u stvaranju propusta na DNS protokolu. Query ID je jedinstven broj upita, i njega je potrebno pogoditi da bi se mogao utisnuti lažni podatak u keš DNS servera.

„Trovanje“ keša DNS servera počinje tako što DNS server internet provajdera (rekurzivni server koji šalje upite) šalje upit u ime klijenskog računara da bi mu pronašao podatak gde se nalazi odgovarajući www zapis. Napadač šalje veliki broj informacija serveru nazad sa lažiranim IP podacima uz domen i sa nasumičnim Query ID informacijama dok ne pogodi odgovarajući ID. U tom trenutku se u kešu servera smešta lažirani podatak za traženi domen koji će trajati neko unapred zadato vreme (ttl-time to live) i za čiji upit će svi korisnici koji pitaju taj server dobiti lažni odgovor [2]. Pogađanje Query ID nije toliko teško ni statistički posmatrano a ni analitički. Na primer, neki serveri daju ID upitima redom u inkrementima po 1, pa je moguće prateći prethodne brojeve lako pogoditi naredne ID upita ka serveru. Statistički posmatrano pogađanje Query ID je olakšano korišćenjem takozvanog *rođendanskog paradoksa*. Naime, iako deluje malo logično zbog broja dana u godini, ali je dokazano da u nasumično odabranoj grupi ljudi od 30 šansa da dvoje imaju rođendan istog dana je 70%. Sa povećanjem ovog broja šansa se drastično povećava tako da prema grafikonu ispod, u grupi od 60 i više ljudi šansa da dvoje imaju rođendan istog dana je praktično 100%.



Slika 5. – Grafički prikaz rođendanskog paradoksa

Šematski prikaz opisanog napada na slabost DNS servera „Kaminsky Bug“ je grafički prikazan na komunikacionoj šemi na slici 6.



Slika 3. – Grafički prikaz menjanja keša DNS servera „Cache Poisoning“

Nakon napada i ostavljanja na serveru lažiranih podataka, svaki klijent koji pravi DNS upite preko tog DNS servera (obično su u pitanju DNS serveri internet provajdera) za domen koji je cilj napada dobiće lažirane IP adrese i biće poslat na pogrešan web sajt ili web servis.

Preduslova koje napadač mora da ispuni da bi napad bio uspešan nema previše i nisu teški za ispunjavanje. Najpre je potrebno da instalira DNS sever koji će glumiti lažni autoritativni server za neki domen. Ovo je bitno jer će se sa tog servera slati lažirani odgovori ka DNS serveru čiji keš treba da bude izmenjen. Zatim, potrebno je da se server i radna stanica pomoću kojih se napada DNS server budu logički i fizički blizu ciljanog servera. Ovaj deo uslova je bitan jer je potrebno da na poslat zahtev lažni autoritativni server odgovori brže od pravog autoritativnog servera. Ako ovaj deo uslova nije ispunjen pravi server će odgovarati nekoliko milisekundi brže

i neće biti moguće u ciljani DNS server utisnuti lažirane podatke. Ako su ova dva uslova ispunjena napadač ima velike šanse da ostvari napad i da navede korisnike na pogrešne IP adrese.

3.2. Posledice Cache Poisoning-a

Da bi se shvatile potencijalne posledice napada na DNS server i promena njihovih zapisa, najpre je potrebno analizirati internet saobraćaj i servise u današnjem trenutku i shvatiti koliko je potencijalnih mesta na kojima je moguće iskoristiti ovu prevaru. U radu će biti pobrojane samo one najveće opasnosti i posledice, jer samim širenjem interneta u funkcionalnom smislu će se javljati vremenom i nove kritične tačke na kojima je moguće zlonamerno koristiti ovaj propust.

Prva kritična oblast je oblast elektronskog poslovanja i pogotovo elektronskog bankarstva. Scenario koji bi mogao da bude iskorišćen u ovom slučaju je sledeći. Korisnik ukucava adresu banke sa ciljem da plati račune preko interneta. Napadač je već promenio zapise na DNS serveru koji će koristiti za upit korisnik. Takođe, napadač je napravio lažni web sajt (jako sličan pravom serveru banke, obično se razlika ne može primetiti) na serveru ka kome sada vode lažni zapisi na DNS serveru. Korisnik ne sluteći da je na web sajtu koji kontroliše napadač ukucava svoje kredencijale za pristup svom nalogu elektronskog bankarstva.

Naravno, pošto je web sajt lažiran, on će prijavljivati grešku prilikom unosa kredencijala, jer se iza njega ne nalazi sistem koji prepoznaje korisničko ime i šifru korisnika, ali i pored prijavljene greške napadač je snimio uneto korisničko ime i šifru korisnika. Nakon ovoga napadač može da se uloguje na pravi sajt banke sa kredencijalima korisnika i da prebacuje novac ili plaća ono što želi sa računa. Najčešće korisnik ne primeti da je prevaren, misleći da nešto sa sajtom banke nije u redu, sve dok sa račune ne počne da nestaje novac u različitim pravcima.

Druga potencijalno kritična oblast je širenje zlonamernih programa (malware - malvera) kao što su kompjuterski virusi, trojanski konji, crvi, keylogger-i ransomware-i slično. Na način sličan kao u prethodnom scenariju, napadač može napraviti neki lažiran sajt, maskirati ga kao sajt sa koga se skida softver, ili sajt proizvođača antivirus programa, ili bilo koji slični web sajt sa koga se može distribuirati softver. Korisnik će ne sluteći da je na pogrešnoj lokaciji snimiti na svoj računar sa napadačevog sajta neki program i time inficirati svoj računar.

Nakon toga u zavisnosti od tipa malvera, virus će se širiti među drugim računarima u kontaktu sa računarom žrtve, trojanski konj može prikupljati informacije kao što su šifre, bankovni računi i slično i slati napadaču, moguće je vršiti industrijsku špijunažu u velikim kompanijama, ili u skladu sa najnovijim trendovima, napadač će iskoristiti ransomware program koji će šifrovati sve fajlove na računaru žrtve do neupotrebljivosti i tražiti da žrtva plati neku svotu novca da bi mu fajlovi bili vraćeni nazad.

Treća kritična oblast je širenje lažnih informacija. Potencijalni scenario može da se odnosi na bilo koju nestabilnu geografsku oblast, gde bi stanovnicima bila servirana informacija koja bi ih pobudila na proteste ili sprečila da se pojave na protestima, u zavisnosti od toga koji je cilj napadača. Na ovaj način lažiranjem novinskih i informativnih sajtova moguće je uticati na velike mase ljudi i proizvesti željeni efekat, a geografski kriznih oblasti u svetu u ovom trenutku ima dovoljno da bi ovakva prevara mogla da se iskoristi.

Kao što je već ranije pomenuto sa pojavom novih servisa i mogućnosti na internetu, koje za svoj rad koriste DNS servis, javljaće se i nove mogućnosti zloupotrebe bazirane na „Kaminski bug“ propustu.

4. Pojam DNSSEC i njegova geneza

Sama skraćenica DNSSEC podrazumeva skup sigurnosnih dodataka za DNS servere kojim se uslovno rečeno potpisuje zona i svaki podatak u njoj na DNS serveru sa ciljem da se nedvosmisleno i jednoznačno označi da je ona zaista sa pravog autoritativnog servera a ne sa nekog lažiranog podmetnutog od strane napadača [21].

Važno je znati da je DNSSEC kao ideja nastao pre nego što je otkriven konkretan propust u bezbednosti DNS protokola, jer se osnovano sumnjalo da do tog propusta može doći i da će pre ili kasnije biti otkriven, a onda je prvobitno rešenje i prvobitna ideja prilagođeno otkrivenom problemu.

4.1. Istorijat DNSSEC

Iako je propust u DNS javno objavljen 2008. godine, ideja o korišćenju DNSSEC datira mnogo ranije. Naime u nekim dokumentima koje je objavila organizacija koja upravlja internetom ICANN pominje se da je vlada SAD znajući da DNS protokol u sebi nema sigurnosnih i bezbednosnih elemenata razmišljala o načinu da se ovaj sistem zaštititi. Prve ideje su se javile početkom devedesetih godina dvadesetog veka, ali pošto tada nije bila uočena jasna opasnost po DNS sa tim se nije previše žurilo.

Ozbiljniji rad na definisanju samog DNSSEC i njegovih pravila i strukture je prvi put zaokružen 2005. godine sa objavljivanjem IETF RFC 4033, 4034 i 4035. RFC je dokument objavljen od Internet Engineering Task Force koji sadrži tehničke i organizacione podatke vezane za neki novi sistem koji se uvodi i javan je po svojoj prirodi. Narednih godina je ovaj standard dopunjen sa još dva dokumenta RFC 5011 i RFC 5155 kojim je dopunjen nivo privatnosti i sistem razmene i obnavljanja ključeva za potpisivanje, koji su takođe vremenom usavršavani i dopunjeni novim dokumentima [3].

I razvoj DNSSEC i njegovo usvajanje kao standarda je išlo prilično sporo. Za to ima mnogo razloga. Najpre nije bilo prevelike potrebe za uvođenjem DNSSEC dok se nije javila direktna opasnost, a onda je bilo kasno da se nešto tako veliko uradi na brzinu. Zatim, sistem kao DNS koristi jako veliki broj heterogenih organizacija i korisnika i bilo je potrebno da se DNSSEC zadovoljava potrebe i mogućnosti što većeg broja njih. Usporevajući faktor je i to što je na DNS servis oslonjen ceo internet i svaki poremećaj rada korišćenjem neke nove tehnologije bi bio tektonski poremećaj. Dalje, u ovaj razvoj je bilo potrebno da se uključe i kompanije koje razvijaju softver i hardver.

Kada je softver u pitanju potreban je bio softver koji će se baviti potpisivanjem podataka a koji se oslanja na DNS servere, zatim kompanije koje razvijaju softver samih DNS servera. Kompanije koje razvijaju hardver su imale nešto manje posla jer je sistem mogao da radi na

postojećim serverima ali su bili potrebni novi uređaji (tzv. HSM uređaji) na kojima će se čuvati ključevi za potpisivanje podataka na serverima, a koji će posedovati najviše standarde za bezbednost podataka. Vremenom su se javljala i jeftina rešenja koja su omogućavala sličnu funkcionalnost, pa čak i softverska rešenja koja su menjala skupi HSM hardver.

Prva zvanično potpisana javna DNS zona je bila ona od strane švedskog nacionalnog registra, pa su oni time postali i prvi ccTLD koji je uveo DNSSEC. Oni su tako 2005. godine omogućili za sve svoje ovlašćene registre potpisivanje zapisa u .se DNS zoni. U narednom poglavlju će biti više reči o trenutnom pregledu stanja sa implementacijom DNSSEC u svetu.

2008. godine je otkriven problem sa DNSSEC ekstenzijom (Hashed Authenticated Denial of Existence), koji je otkrivao korisnicima sadržaj svih podataka u potpisanoj DNS zoni. Zbog ovoga je standard menjan i unapređivan i sam sadržaj DNSSEC zapisa je u potpunosti promenjen.

Nakon što je nekoliko nacionalnih registara prethodno uvelo DNSEC u svoj sistem, prvi TLD koji je završio svoju implementaciju je bio .org. Nedugo zatim potpisan je i DNS „“ root zapis kompletnog interneta od strane ICANN.

4.2. Šta je DNSSEC i kako štiti DNS zone

Da bi odgovorili na pitanje postavljeno u podnaslovu ovog poglavlja prvo je potrebno definisati DNS zonu. DNS zona je produkt DNS servera. To je fajl generisan od DNS servera u kome su upisani podaci o imenima računara i njihovim odgovarajućim IP adresama. Sadržaj DNS zone zavisi od DNS servera koji je zonu generisao.

Ako je u pitanju root zona u njoj se nalaze podaci o autoritativnim serverima za sve Top Level Domene (i generičke i nove i nacionalne TLD). Ako je u pitanju DNS zona neke kompanije u njoj se na primer, nalaze podaci o produkcionim serverima, e-mail serverima (MX zapis) i tako dalje.

Sledeći korak u pojašnjavanju je kako DNSSEC štiti DNS zone i sam DNS sistem. Analogija se može napraviti istorijski sa slanjem pisama od jednog kralja ka drugom. Svaku poruku koju kralj pošalje drugom kralju može napisati i bilo ko drugi, ali ako na poruku stavi kraljevski pečat u vosku onaj koji dobija poruku će znati ko je tačno pošiljalac. Ako se pečat slomi, ili ne odgovara originalnom pečatu ta poruka nije validna.

Na sličan način funkcioniše DNSSEC. Rekurzivni DNS serveri koji prave upit za neki domen ka autoritativnom serveru će proveriti da li je odgovor potpisan i da li je potpis validan. Na taj način će rekurzivni DNS server biti siguran da je taj odgovor dobar a samim tim i krajnji korisnik koji je napravio početni upit za traženi domen. Ako ključ kojim je odgovor potpisan

nije dobar, ili odgovor nije uopšte potpisan, to se prosleđuje krajnjem korisniku da zna da postoji opasnost da je taj domen kompromitovan na neki način.

DNSSEC takođe podrazumeva da postoji lanac poverenja od najviših root servera pa naniže ka poslednje potpisanom serveru u nizu. Ako postoji prekid u lancu poverenja i sve karike tog lanca naniže neće biti u mogućnosti da budu verifikovane kao uspešno potpisani DNSSEC zaštitom.

Niže u tekstu je dat primer kako izgleda nepotpisan DNS zonski fajl kao i DNSSEC potpisan zonski fajl.

```
$TTL 3600
primer.rs.  600      IN SOA  test.primer.rs. admin.primer.rs. (
                                20080821  ; serial
                                7200      ; refresh (2 hours)
                                3600      ; retry (1 hour)
                                604800    ; expire (1 week)
                                600       ; minimum (10 minutes)
                                )
                                600      NS   ns1.primer.rs.
ns1          600      IN A    192.0.2.1
www          600      IN A    192.0.2.2
```

Primer 2. – Primer koda nepotpisanog DNS zonskog fajla

```
# zonesigner -genkeys primer.rs
    if zonesigner appears hung, strike keys until the program completes
    (see the "Entropy" section in the man page for details)

zone signed successfully
primer.rs:
    KSK (cur) 25816  -b 2048  08/21/08      (primer.rs-signset-3)
    ZSK (cur) 54228  -b 1024  08/21/08      (primer.rs-signset-1)
    ZSK (pub) 28878  -b 1024  08/21/08      (primer.rs-signset-2)
zone will expire in 4 weeks, 2 days, 0 seconds
DO NOT delete the keys until this time has passed.
```

Primer 3. – Primer komande za DNSSEC potpisivanje i rezultata potpisivanja

```

; File written on Sat Jul  4 10:13:30 2009
; dnssec\_signzone version 9.5.0-P2
example.net.          100      IN SOA  ns.example.net. olaf.nlnetlabs.nl. (
                        2002050501 ; serial
                        100        ; refresh (1 minute 40 seconds)
                        200        ; retry (3 minutes 20 seconds)
                        604800     ; expire (1 week)
                        100        ; minimum (1 minute 40 seconds)
                        )
100      RRSIG  SOA 5 2 100 20090803071330 (
                        20090704071330 17000 example.net.
                        TVgWsNQvsFmeNHAeccGi7+UI7KwcE9TXPuSv
                        mV9yyJwo4FvHkxVC1H+98EtrmbR4c/XcdUzd
                        fgn+q+lBqNsnbAitxFERwPxzxbX0+yeCdHbB
                        jHe7OuOc2Gc+CH6SbT2lKwViiEx3ySqqNoVs
                        coUyhRdnPV2A1LV0yd9GtG9mI4w= )
100      NS     ns.example.net.
100      RRSIG  NS 5 2 100 20090803071330 (
                        20090704071330 17000 example.net.
                        Xuw7saDDi6+5Z7SmtC7FC2npPOiE8F9qMR87
                        eA0egG0IB+xFx7pIogoVIDpOd1h3jqYivhbl
                        pCoDSBQb2oMbVy3BSX5cF0r7Iu/xKP8XrV4D
                        jNiugpa+NnhEIaRqG5uoPFbX4cYT51yNq70I
                        5mJvvajJu7UjmdHl26ZlnK33xps= )
100      NSEC   *.example.net. NS SOA RRSIG NSEC DNSKEY
100      RRSIG  NSEC 5 2 100 20090803071330 (
                        20090704071330 17000 example.net.
                        aDLo8JH5jEqD9u3Ft+7CNF8YXM9LKLKcDsLv
                        otIcpixsMSXlXFSZOIkxxkxZtwlqBwhz0nzIs
                        7M/tnvsTlfl4I5nt/VPRBY/XxanOa/3GjXLo
                        5Ukig8gX4S7s6/iTHNIFjJaxHiCtt5zwoI/H
                        TeKi9FjuH9ysHVuoHeYR06MN/LU= )
100      DNSKEY 256 3 5 (
                        AQPI4+0M1V055RS2Hqv+8w8V20Dh+SQmFzHQ
                        tZMuzLH3UxWE0GmG5GfjijandJeAZTKLpERX
                        B6RfHHTGG8lD3IOlazWN6DiVFEVzgr0otAdD
                        onfYF8gUT03ZnRcXlkJk41h12NOfq6rkODaF
                        nfMHCppI3WZ/MJqe+9hLJtis+oEsRw==
                        ) ; key id = 17000
100      DNSKEY 257 3 5 (
                        AQOzgs4qea+ImJlOCworkabHqFnvPKybVT7b
                        nDIkJ2HvXWslbwNWJ660x3N6ftpCTc9wWBMw
                        5+Xoh7ilTwFPruMa2gURwEywZaMG9ipILOXm
                        KO4a5I+8R2QTH4BM0WaIKnv5jCHose/19LL3
                        Y8MApsjP6gOWNM8b9aVTjBFnf0xEF7sOSBBB
                        E4G2/og5Fr+H8DYaotqgJ3nrzRfYA0gSXwwb
                        ) ; key id = 49656
100      RRSIG  DNSKEY 5 2 100 20090803071330 (
                        20090704071330 17000 example.net.
                        VQb1OdYAFpDk9kBPqkvuHL4W+e1Ulo/QzIOD
                        7EyeZfJHNYW8bGhyNY5uaXnf3o/tBE6tj8mY
                        1kmRJsBWQXdSjRlW3syaZD7+W93m3rS6/reI

```

```

9hBAijy2xSEEVx1LTeeLulqzzD0HMootC/cw
DuWSISpCs+9YB0sUbVsGQdzxn7E= )
100      RRSIG  DNSKEY 5 2 100 20090803071330 (
20090704071330 49656 example.net.
TpWicKxjdd5NML8pT+t1moSOGDQF+Nl4AbeO
oAher5Q8QCrX2JBiKcyi5iaTHZyg6RizFLPW
+FxfCsaMmzk0030Zu0ILlZW0AWUv4gxdmoBe
MQQ/4tuZp6Dgsh7OLl+3dU+S0QihyQUXDnkt
MKARs10tBGpuIkzpKJFBY5eEAsV9ivlXx1Wi
zrY4vMkth6NuasmpKJ0BYaonHUMwK8NzAQ== )
*.example.net.      100      IN A      192.168.2.10
100      RRSIG  A 5 2 100 20090803071330 (
20090704071330 17000 example.net.
U6uEoNwJVPFcPgfoloQfDTMgGjqeLijMqr7Q
RlPufDoy6SEYswoJWBk1mqolcCCkN051Nqmr
XD6Nr4Q6gRV/F8x41KiV+Ulu0+bnV6yog5CM
XFudPKnrMJC4Cr9mzmUfeiqX3yaKjqr46noE
37B1KrmcjJA1TIuVbLJ2dyPMxvo= )
100      NSEC   a.example.net. A RRSIG NSEC
100      RRSIG  NSEC 5 2 100 20090803071330 (
20090704071330 17000 example.net.
hYQV/LI/Uo2uCTAlXigo0tmuxiFH+MNUL265
hsNY3CHcdy4qJWV/fnAjPaNcA/oQMnhqfnWT
JBjp6RqPlTUZHkMPx1R7UbSPQSpI35lt5niE
xDQS5LHH4H+tzuV+HazcBR9rqLhEncPqgVmq
qIpsQRiJlMYnpN2bSjsdoqlJOrM= )
a.example.net.      100      IN A      192.168.2.1
100      RRSIG  A 5 3 100 20090803071330 (
20090704071330 17000 example.net.
MughSVso2OhRNFgUmI0iFmovjot4o0ZPTPnt
dZ/ef8WJoi2fCXutgz3nvQlQbWrI7sLetyCD
9oKZN15wISDW4inkrWqwt5RLvo5iagXfn7wv
CzZflPqYoDYD3XDfAbxzj1F5X8HiZQmQnQU2
PNOaVRj9I5OeiKBRKJaNPCTKXGU= )
100      NSEC   b.a.example.net. A RRSIG NSEC
100      RRSIG  NSEC 5 3 100 20090803071330 (
20090704071330 17000 example.net.
rO/aVFfYOUYk8NtiOAs2ypWuSarINWXedIoW
FTpeo3uUih900re52vlFMRay+ZanASfSS837
ic9SIVcZz3DpFhlIuDgsSEFN0zvEwptUnvCC
osDS6vgF0ZyxTW3SD4VNISTrlmxqoBD8S3kV
OxqJ0yoL0nBpskQ2U0zLawolIh4= )
b.a.example.net.      100      IN A      192.168.2.11
100      RRSIG  A 5 4 100 20090803071330 (
20090704071330 17000 example.net.
SiYt5SIoXwmR83oxjg/rT8KzdciE8UW4tv0c
B3Yl4+wFsQNb0M5pDBBP4Z2WIs+FDaP3xW7x
jFHuzYAl85yY0W6jP8nwWeNcvHcAAmhzYRT7
Isn2PKU92832xoIG9kF9Z3A6p3s= )
100      NSEC   b.example.net. A RRSIG NSEC
100      RRSIG  NSEC 5 4 100 20090803071330 (
20090704071330 17000 example.net.

```

```

KKIwCnO6wrYueT9ReasVJEXBYlhjoi/QB+7
cJAGpsxmV7dIgd2jEp8PTmdRaW6aYIPBn3nR
tIzhyNorFhocEVyBqAuPF7D58QJcJy78PA1W
6WG/5vGOWLKGMwWnLn1zBPcqifPC9BiQTyeU
dVASFlx+aN2QFZCKLGHAatwloG8= )

b.example.net.      100      IN      A      192.168.2.2
                    100      RRSIG   A 5 3 100 20090803071330 (
                    20090704071330 17000 example.net.
                    OnXyjrZUOnfW9byUBdHQbsx1JaWWZTHTmjoA
                    59zCJDslp8Ez/+UIoBHPfrxRMt//yRtIDjT0
                    fDacjTKVJ6YeRLmCEwCptYGp9MtqoL5xlleH
                    GD/Awido8GrWfGsBEr7GUbcbgPKDCeNnVzyok
                    PnG5YAG5ZilgOJh9PXijFGIHcxY= )

                    100      NSEC    ns.example.net. A RRSIG NSEC
                    100      RRSIG   NSEC 5 3 100 20090803071330 (
                    20090704071330 17000 example.net.
                    H/gWsA+mkx6M5jwfyAuC8fWDOUHHktnLFHO2
                    dNC1d23uWcZEV5DGBuQy9rcn8ikOmrFi0ABZ
                    gwufEAiARCdOgsCkNvkSzh2vprC2hYRZ3Hxt
                    CNTMsDobKontj7+lGv68V0wYY/se/38QMIYS
                    qTkEbokTpgaQRVku48kPLbvpObU= )

ns.example.net.      100      IN      A      192.168.2.203
                    100      RRSIG   A 5 3 100 20090803071330 (
                    20090704071330 17000 example.net.
                    YUj6wUw2hHpONnfN/rSJJaGve2NfA1TcROJV
                    7FdKmXrkVn+gMp2pATijqKxG6nLMI/MnAs1b
                    URYMMuBy6458y97v0687s5ba2kaUwFgmV4UO
                    n/TnAjbNBgStkSK/TTGQVK3Vxw9uefiQprxG
                    70Zlh6gLysWRgBc33JiQRvvn5nY= )

                    100      NSEC    example.net. A RRSIG NSEC
                    100      RRSIG   NSEC 5 3 100 20090803071330 (
                    20090704071330 17000 example.net.
                    NYwhLV0hgDLoHPRruKKM3QibpFX57R647/Ui
                    BTeetEyz675LvknCHkc16HDcVQTzvHs+6xZC
                    jCyauBwxcPWDVQQcZ/zakgl8pUh73w1I61H9
                    UHLLaFi+GMHfsH+jbdoNJ0wKzjNAP54hmOoM
                    0VPr11wlTFZhBAsb776sHu1CWL4= ) 639

```

Primer 4. – Primer DNSSEC potpisanog zonskog fajla

Iz prikazanih primera možemo primetiti razlike u izgledu nepotpisane i potpisane DNS zone kao i kompleksnost potpisanog zonskog fajla. Ta kompleksnost sa sobom nosi i potencijalne poteškoće koje treba razmatrati pri uvođenju DNSSEC zaštite na DNS server. Detaljnije ove pojave će biti opisane u drugom pristupnom radu zajedno sa drugim pozitivnim i negativnim aspektima ovakvog načina zaštite, kao i detaljnijim tehničkim rešenjima.

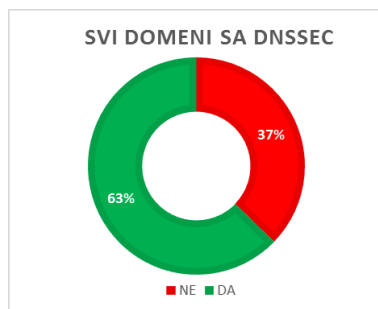
4.3. Pregled stanja uvođenja DNSSEC u svetu

Kao što je već pominjano do sada u radu, uvođenje DNSSEC je dug proces, proces koji zahteva jako puno ljudskih, računarskih i finansijskih resursa. To je dug proces posmatrano na nivou uvođenja DNSSEC u jednu organizaciju, a pogotovo na makro nivou uvođenja DNSSEC na kompletnoj internet mreži. Proces uvođenja podrazumeva najpre temeljan plan. U planu treba da bude opisan skup svih procesa potrebnih za uvođenje DNSSEC. Najpre analiza potreba, analiza i nabavka potrebnog softvera i hardvera, kao i obuka stručnjaka koji će biti zaduženi za upravljanje DNSSEC procesima i onih koji su zaduženi za DNS servere jer se sad i rad DNS servera donekle menja.

Pokazalo se do sada da je možda i najvažniji deo planiranja izrada dokumenta u kome će biti opisani svi procesi, sve moguće situacije koje je moguće predvideti kao i šta je potrebno uraditi u svakoj od tih datih situacija. Taj dokument je obično interna tajna i sa njim su upoznati samo oni koji rade na DNSSEC procesima i DNS serverima i to u meri u kojoj je potrebno da znaju ono što pokriva njihov delokrug rada. Ovaj dokument se pokazao kao jako važan zbog složenosti postupka potpisivanja DNS zona i zbog toga što se sve eventualne greške ne mogu lako ispravljati i da su sve popravke i korekcije sistema jako vremenski zahtevne. Uzimajući sve ovo u obzir nije neobično to što broj DNSSEC potpisanih zona ne raste vrtoglavo već sporo i konstantno.

Statistički pregled stanja uvođenja DNSSEC u različite domenske prostore ćemo početi sa ukupnim brojem domena koji se nalaze u root zoni i koji obuhvataju i Top Level Domene i nacionalne cc Top Level Domene kao i nove Top Level Domene koji se pojavljuju svakog dana u redosledu kako su odobreni od ICANN. Broj ovih poslednjih u detaljnijoj statistici nećemo uzimati u obzir jer kao što je pomenuto njihov broj tek počinje da raste i oni upravo sada počinju sa upotrebom te samim tim nije korektno posmatrati ih kao one domene koji na internetu postoje znatno duže. Broj novih Top Level Domena nije zanemariv, ali njihovo trajanje i tržišna zrelost jesu zanemarivi pa bez obzira na to da li su od prvog trenutka DNSSEC potpisani ili ne neće biti statistički obrađeni. Takođe u statističku obradu neće ući ni internacionalizovani Top Level Domeni (domeni na jezicima koji nisu engleski alfabet) jer ih ima jako malo a i u okviru svakog od nema previše registracija osim kod ruskog domena .pф koji je na putu da dostigne 900.000 registracija vrlo uskoro.

U root zoni na root DNS serverima nalazi se ukupno 507 naziva domena a od tog broja DNSSEC potpisano je ukupno 318. Grafički prikaz odnosa broja nepotpisanih i potpisanih domena se nalazi na grafikonu ispod [12] [16].



Slika 4. - Grafički prikaz odnosa broja svih domena sa uvedenim DNSSEC i onih koji ga nisu uveli

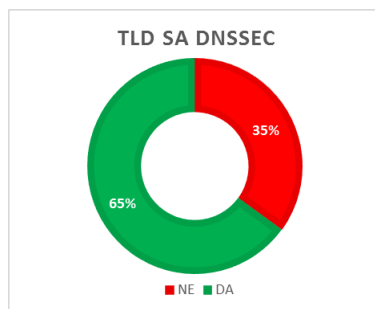
Od ukupnog broja domena upisanih u root zonu mi ćemo analizirati dve velike grupe. Najpre prvobitne osnovne Top Level Domene kojih ima 20 i koji su najzastupljeniji i najpoznatiji a i nalaze se u upotrebi najduže od svih domena. U tabeli ispod je dat spisak svih domena i odgovor da li su implementirali DNSSEC ili ne. Iz tabele i detaljnije statističke analize se može zaključiti nekoliko stvari. Možemo videti da su DNSSEC uveli oni domeni koji su najbrojniji na internetu (.com, .net, .org) jer su u želji da prošire svoje tržište i da pruže korisnicima novu bezbednosnu uslugu i da ostanu dominantni kao tržišni lideri, druga grupa domena koji su uveli DNSSEC su oni koji su imali tu obavezu od strane nekog državnog subjekta, u ovom slučaju vlade SAD, te su tako među prvima DNSSEC uveli i .edu, .gov i .mil kao i .post koji je DNSSEC uveo pod patronatom Međunarodne poštanske organizacije.

Treća grupa domena koji su uveli DNSSEC je to uradila da bi unapredila prodaju domena i priključila se prvoj grupi, kao i istakla razliku u odnosu na buduće nove domene koji stižu i nacionalne domene. U treću grupu spadaju .biz, .info, .mobi i tako dalje. Kako i kada će ostali TLD uvoditi DNSSEC zavisi od planova organizacija koje administrativno upravljaju tim domenima, njihovoj proceni tržišta kao i od toga da li će se javljati neke nove tendencije koje bi uticale na njih da pre ili kasnije uvedu DNSSEC potpisivanje zona.

Tabela 2. – Spisak potpisanih osnovnih Top Level Domena

TLD	Uveden DNSSEC	TLD	Uveden DNSSEC
aero	NE	mil	DA
biz	DA	mobi	DA
cat	DA	museum	DA
com	DA	name	DA
coop	NE	net	DA
edu	DA	org	DA
gov	DA	post	DA
info	DA	pro	NE
int	NE	tel	NE
jobs	NE	travel	NE

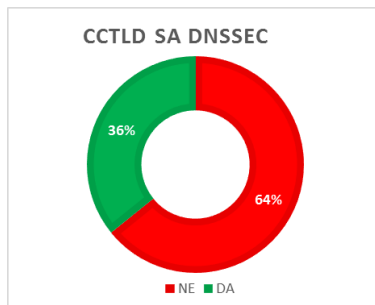
Na slici 8. se može videti jasnije odnos potpisanih i nepotpisanih TLD domena.



Slika 5. - Grafički prikaz odnosa broja TLD sa uvedenim DNSSEC i onih koji ga nisu uveli

Druga velika grupa domena koji se nalaze upisani u root zonu su ccTLD ili nacionalni Top Level Domeni. To je grupa domena dodeljena svakoj državi ili autonomnoj oblasti ponaosob na upravljanje. Uobičajen je slučaj da za svaku državu ovim domenom upravlja neka neprofitna, nevladina organizacija čiji su osnivači internet zajednica ili kompanije čiji delokrug rada se nalazi u internet komunikacijama. Naravno to nije apsolutno tako, ima izuzetaka.

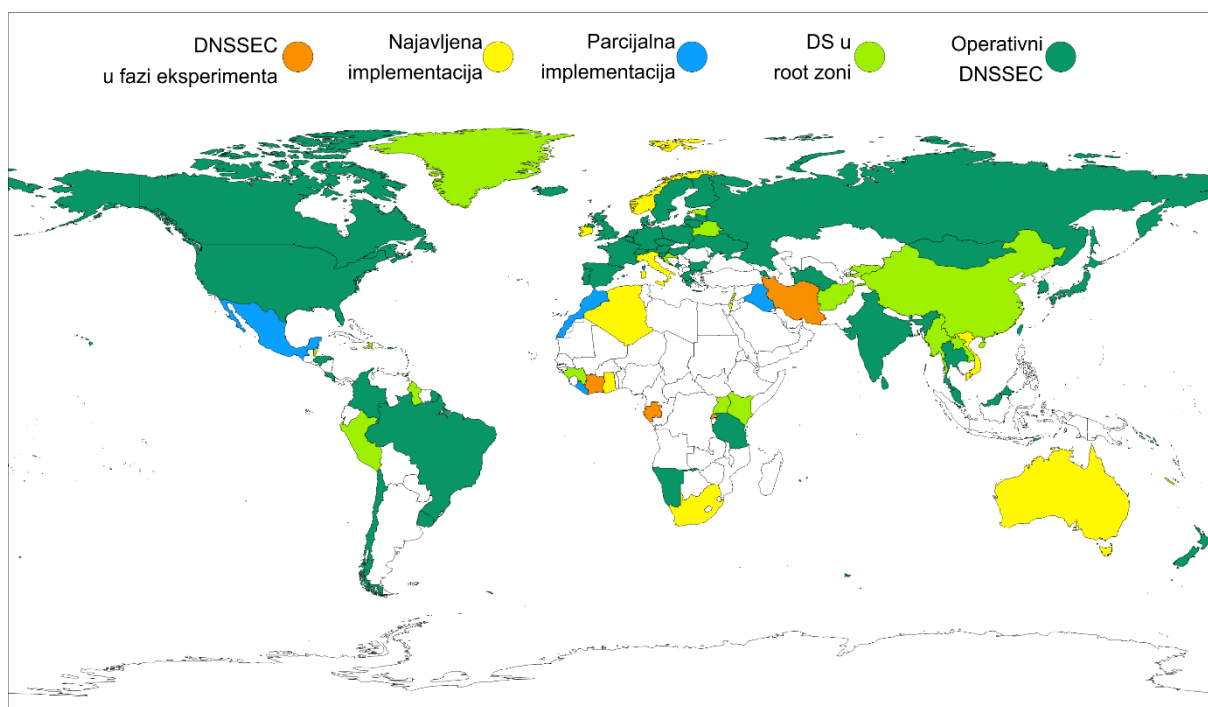
U root zoni se trenutno nalazi 254 nacionalna domena pri čemu je broj onih koji su uveli DNSSEC zaštitu 91 a preostalih 163 još uvek nisu (ovi brojevi su uzeti bez obzira da li je neki od nacionalnih domena pri kraju implementacije ili u toku planiranja jer se računaju samo oni kod kojih je DNSSEC u funkciji). Na grafikonu ispod se može uočiti odnos zaštićenih i nezaštićenih nacionalnih domena [12] [17].



Slika 6. - Grafički prikaz odnosa broja nacionalnih TLD sa uvedenim DNSSEC i onih koji ga nisu uveli

Kao što se može primetiti situacija sa nacionalnim domenima je drastično drugačija nego kada su u pitanju osnovni domeni najvišeg nivoa. Dok se organizacije koje upravljaju osnovnim domenima rukovode tržištem i odnosima na njemu, organizacije koje upravljaju nacionalnim domenima imaju drugačija pravila. Kod nekih od takvih organizacija potrebno je ispoštovati zakone i procedure pa je tim povodom ili ceo proces kraći i brži ili drastično sporiji zbog neusvojene pravne regulative. Neki od nacionalnih domena su dati na upravljanje komercijalnim organizacijama (primer crnogorski domen .me ili Tuvalu .tv) pa u njihovom slučaju tržište ponovo igra ulogu vezano za uvođenje DNSSEC. Jedan broj organizacija koje upravljaju nacionalnim domenima je zbog veliki prihoda i velikog broja registrovanih domena u mogućnosti da lako finansira i pokrije sve troškove uvođenja DNSSEC, dok druge organizacije nisu u mogućnosti. Na osnovu prethodno iznetog vidi se da nije moguće izvući

zaključak iz broja nacionalnih domena koje su uvele DNSSEC već se svaki slučaj mora posmatrati pojedinačno. Na slici ispod se vidi geografska pokrivenost kada su u pitanju nacionalni internet domeni.



Slika 7. – Geografski prikaz nacionalnih domena koje su uvele DNSSEC u različitim fazama [4]

Da li će DNSSEC biti kompletno uveden na internetu, da li će svi internet provajderi na svojim rekurzivnim DNS serverima uvesti validaciju DNSSEC potpisivanja kao i još neka slična pitanja će ostati još uvek otvorena. Odgovor na njih ne može biti dat čak ni uz izuzetno detaljnu analizu jer je previše faktora koji utiču na ceo ovaj proces (ti faktori mogu biti ne samo tehnološki i tehnički već i politički, ekonomski i sociološki) a nije moguće predvideti vrednosti tih faktora.

5. Uvod u tehnologiju DNSSEC-a

U prvom delu ovog rada ideja je bila prikazati potrebu za DNSSEC- tehnologijom i sam DNSSEC fenomenološki, kao i njegovu upotrebljivost širom interneta/sveta. U drugom pristupnom radu cilj je prikazati tehnička rešenja ove tehnologije, i to kroz oba sastavna dela, hardver i softver. Zatim, prikazati različita rešenja i pokušati ih uporediti kroz upotrebljivost, isplativost i niz drugih kriterijuma kojima je moguće uporediti ova rešenja. Kroz rad će takođe biti prikazano i na koji način DNSSEC povećava potražnju sa hardverskim i infrastrukturnim resursima, na koji način traži da mu se softver i serveri prilagođavaju, a takođe da li i koje se nove slabosti otvaraju korišćenjem ovih tehnologija a da se pre toga nisu ispoljavale.

Uvođenje DNSSEC i promene koje iziskuje se mogu uporediti sa uvođenjem armature u beton u građevinarstvu. I dalje će se praviti isti beton samo sa gvoždem unutar sebe, i dalje će se zgrade graditi odozdo na gore, i mnogo druge stvari će ostati iste, ali će zgrade biti jače, otpornije na vetrove i zemljotrese. Slično je sa DNSSEC-om. I dalje će se koristiti DNS serveri, kojima će biti dodata DNSSEC armatura, i dalje će se praviti web sajtovi i razmenjivati elektronske poruke, ali će biti znato teže lažirati adrese i korisnici će bezbednije koristiti internet.

6. Kako DNSSEC radi

Da bi DNSSEC tehnologija ispravno radila potrebno je da se koristi odgovarajući softver i hardver, kako na serveru koji digitalno potpisuje DNS zone, tako i softver na serveru koji razrešava DNS upite i vrši verifikaciju ispravnosti zapisa u zoni.

6.1. DNSSEC tehnologija

Minimalističko objašnjenje DNSSEC tehnologije bi glasil – „umesto klasičnog DNS odgovora da se ne određenoj IP adresi nalazi odgovarajući host, uz taj odgovor bi išao i digitalni potpis servera kojim se nedvosmisleno zna da je taj server autoritativan za host za čije ime je postavljen upit“. Naravno iza ovakvog odgovora se nalazi komplikovana tehnologija koja manje nego druge trpi greške i koja i po nekoliko puta usložnjava rad sa DNS serverima i po nekoliko puta povećava saobraćaj sa autoritativnih DNS servera ka rekurzivnim DNS serverima koji razrešavaju upit za krajnjeg korisnika.

Ako bi smo se trudili da pojednostavimo proces radi uvodnog objašnjenja, osnovne komponente DNSSEC tehnologije bi bile:

- server na kome se kreira i drži DNS zona
- softver pomoću koga se digitalno potpisuje DNS zona
- uređaji koji generišu i čuvaju tajne ključeve kojima se potpisuje zona
- server koji razrešava DNS upite korisnika i verifikuje DNSSEC zapis

O svakoj od ovih komponenti će biti detaljnije rečeno ponaosob u posebnim poglavljima. Možda i najbolji redosled da se krene sa objašnjenjem tehnologije je posmatrajući proces hronološki i u smislu nastajanja (DNS serveri postoje od početka interneta i kao takvi se koriste znatno pre pojave DNSSEC dodataka) i u smislu početka procesa (ako se proces nastajanja i potpisivanja jedne DNS zone posmatra od početka do kraja, na njegovom početku ali i kasnije u procesu se pojavljuje DNS server).

Dobra praksa dosadašnjih implementacija DNSSEC u svetu pokazuje da je najbolje kada su ove komponente razdvojene, to jest, kada se nalaze na različitim fizičkim ili virtuelnim mašinama. To je potrebno kako zbog upotrebljivosti tako i zbog bezbednosti celog sistema, pa je ideja rada da u skladu sa tim posmatramo ove komponente. [14]

6.1.1. Server na kome se kreira i drži DNS zona

Osnova DNS sistema bez obzira da li se koristi DNSSEC bezbednosni dodatak ili ne je klasičan DNS server koji kreira DNS zonu, na kome se ta ista zona nalazi sve do njene sledeće promene i koji odgovara na upite rekurzivnih DNS servera.

Kada je u pitanju hardver kao i u slučaju većine serverskih operativnih sistema i serverskih aplikacija kao što je DNS, poželjno je da komponente servera budu redundantne, čime se smanjuje verovatnoća otkaza. DNS serveri su kritični serveri za internet pa je po pravilu ne samo hardver na kojima se nalaze redundantan, već se uvek instaliraju po par identičnih DNS servera u slučaju preopterećenja ili potpunog otkaza jednog od njih.

Bolje rešenje od bilo koje fizičke mašine, bez obzira na kvalitet iste je virtuelna mašina. Virtualne mašine su softverski generisane simulacije fizičkih servera. One se kreiraju koristeći softver koji se kao operativni sistem instalira direktno na dva ili više fizičkih servera. Virtuelne mašine su ne samo fleksibilnije i lakše za podešavanje već su i znatno lakše za rad, za prebacivanje sa servera na server, kao i za lakše pravljenje rezervnih kopija.

Ovaj rad nema za temu virtuelne mašine jer one predstavljaju opšti pojam koji nije direktno vezan ni za DNS sistem ni za DNSSEC dodatke, pa se samim tim neće dublje ulaziti u tu oblast, a samo objašnjenje virtuelnih mašina može se naći u indeksu pojmova koji prati ovaj rad.

U narednim poglavljima biće predstavljeno nekoliko reprezentativnih primeraka softvera (DNS serverskog softvera) pomoću kog se kreiraju i održavaju DNS zone i koji odgovaraju na upite klijentima i rekurzivnim serverima. Ti serveri se za razliku od rekurzivnih (servera koji prosleđuju upite u oba smera) zovu autoritativni serveri.

- BIND

Za softver koji je napravila i usavršava organizacija Internet sistem konzorcijum, može se reći da je de fakto standard na internetu. Prema kompaniji Neustar u 2012. godini BIND je zauzimao 28% tržišta kada je 500 najkorišćenijih domena u pitanu, ali se pretpostavlja da kada se uzme u obzir kompletna internet slika da je ovaj procenat znatno veći. Softver je predviđen da radi na UNIX/Linux platformama gde je i najfunkcionalniji, ali postoje verzije i za MacOS operativni sistem, Solaris, kao i za Windows operativne sisteme.

BIND je nastao početkom osamdesetih godina prošlog veka na Univerzitetu Berkli po kome je i dobio ime *Berkeley Internet Name Domain*. Trenutno aktuelna verzija ovog softvera je 9.10.0 i datira iz aprila 2014. godine. Od 2010. godine počeo je rad na potpuno novoj verziji 10 ovog softvera a kompletiranje nove verzije se očekuje u 2015. godini. Takođe je bitno napomenuti da je ovaj softver potpuno slobodan za upotrebu i bilo kakvo nadograđivanje.

Kada su u pitanju neke standardne karakteristike, BIND podržava obe mogućnosti i da se koristi kao autoritativni DNS server ali i rekurzivni DNS server. Od verzije 9 podržava IPv6 adrese, a podržava i opciju Split horizont (objašnjenje za Split Horizont kod DNS servera se može naći u indeksu pojmova). Od verzije 9 takođe je uvedena i mogućnost koja se zove Rate Limiting koja služi da zaštiti server od amplifikovanih DDoS napada o kojima će kasnije biti reči u ovom radu. BIND serverom se može upravljati iz komandne linije direktno na serveru ili preko SSH pristupa, ali i putem veb interfejsa koji pruža dovoljno ali nešto manje opcija nego pristup preko komandne linije.

Ono što je za ovaj rad najbitnija karakteristika BIND servera je da on podržava DNSSEC u potpunosti i da je najčešće korišćeni server za DNSSEC implementacije. [5]

- Microsoft DNS

Microsoft DNS server je sastavni deo isključivo Windows Server operativnih sistema, ali nije uključen po instaliranju sistema već se naknadno dodaje kao posebna rola. Prvi put se pojavio u okviru Microsoft operativnog sistema u verziji 3.51 NT servera i odatad se koristi. Pre toga su Microsoft operativni sistemi koristili mahom Wins servis koji je zastareo i koji nije podržavao razrešavanje upita za druge operativne sisteme.

Ovaj DNS server je široko zastupljen po internetu ali se mnogo češće koristi u zatvorenim internim mrežama nego na internetu. Razlozi za to su tromost i hardverska zahtevnost pri velikom broju DNS zapisa u zoni, ali i bezbednosni problemi koji su ga pratili.

Microsoft DNS kao i BIND podržava većinu opcija koje smo gore naveli osim opcije Split Horizont a takođe se mora navesti i to da on nije besplatan jer je potrebno platiti licencu za operativni sistem u okviru koga se on nalazi, mada se ne naplaćuje dodatno. Microsoft DNS podržava DNSSEC od verzije Microsoft Server 2008 R2 a sistem rada sa ovim bezbednosnim dodacima je unapređen u aktuelnoj verziji servera Microsoft Server 2012 R2.

- PowerDNS

PowerDNS server je još jedna verzija besplatnog DNS servera namenjenog prvenstveno UNIX/Linux operativnim sistemima. Verzija za MacOS operativni sistem je još uvek u eksperimentalnoj fazi pa se ne može nazvati operativnom. Ovaj sistem je razvila PowerDNS zajednica koja postoji od kraja devedesetih godina prošlog veka. Ovaj softver je takođe besplatan i otvorenog koda, ali se napredna podrška proizvođača naplaćuje kroz servisne ugovore.

Takođe, kao i BIND, podržava sve pomenute opcije uključujući i DNSSEC dodatke. Kada je DNSSEC u pitanju važno je napomenuti da ovaj softver može da radi sa unapred potpisanim zonama na drugom softveru, ali i da ih sam on-line potpisuje i čuva ključeve. Ovaj način je

najjednostavniji za rad, ali takođe i najmanje bezbedan od svih drugih načina čuvanja ključeva za potpisivanje DNS zona.

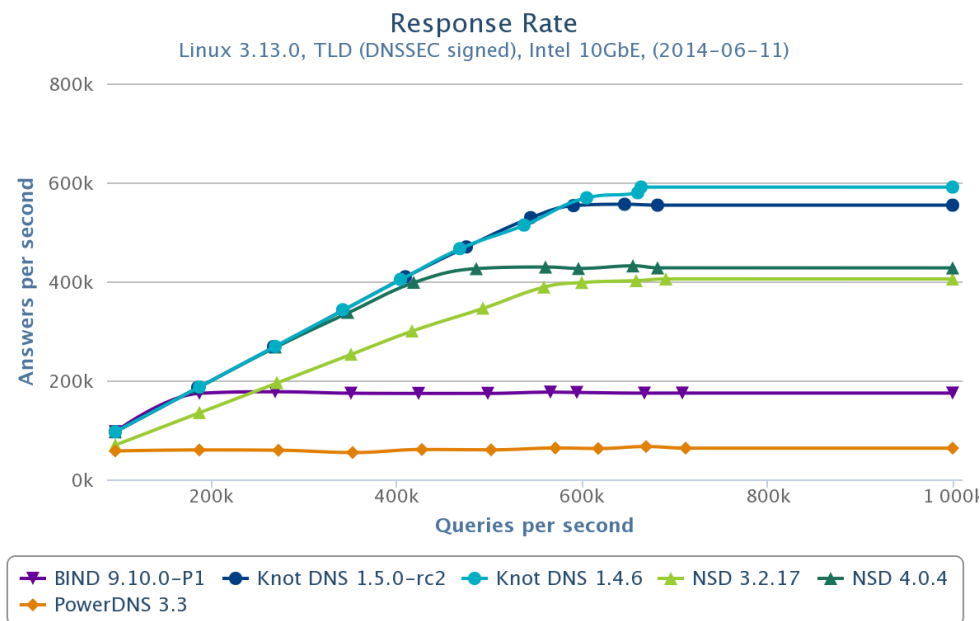
- KnotDNS

KnotDNS server je proizvod rada češkog nacionalnog internet domen registra (cz.nic), koji je nakon analize softvera na tržištu i analize svojih iskustava odlučio da napravi softver za svoje potrebe. Softver su javno objavili i besplatan je za korišćenje pod GPL licencom a može se i sam otvoreni kod skinuti sa sajta registra.

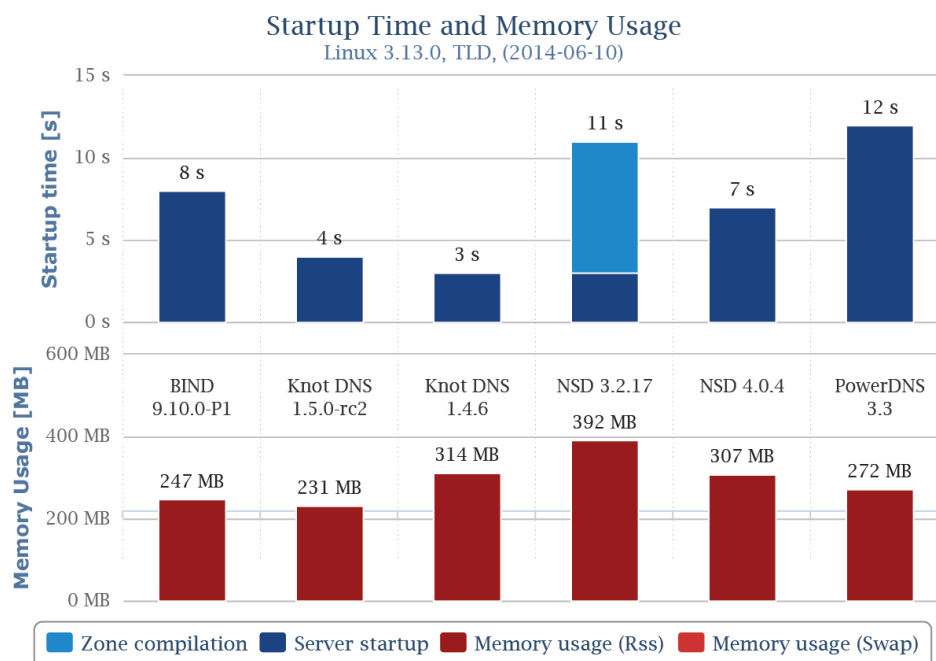
Ovaj softver je namenski pravljen kao autoritativni server visokih performansi pa samim tim ne podržava ulogu rekurzivnog servera kao ni Split Horizon kao ni neke druge koje bi usporavale rad servera i snižavale performanse. Takođe, zbog toga što je pravljen po meri češkog registra implementirane su sve opcije koje najčešće koriste ccTLD i TLD operatori u svetu.

Server u potpunosti podržava DNSSEC a od bezbednosnih opcija kao i BIND, podržava Response Rate Limiting što ga kao i prethodno štiti od amplifikovanih DDoS napada.

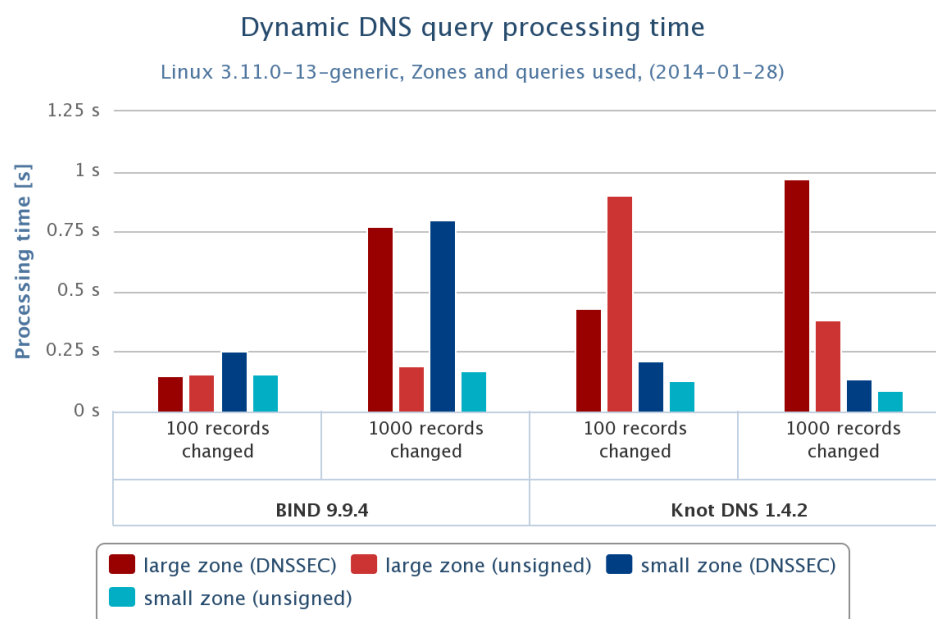
Na grafikonima 1. i 2. je prikazano poređenje reakcija servera na upit kao i potrošnja sistemskih resursa. Oba grafikona podrazumevaju da je DNSSEC na serveru implementiran. Grafikoni su preuzeti sa Benchmark dela sajta www.knot-dns.cz



Grafikon 1. – Prikaz broja odgovora servera u sekundi sa porastom broja upita u sekundi (preuzeto sa Benchmark stranice veb sajta www.knot-dns.cz)



Grafikon 1. – Prikaz brzine startovanja sistema i potrošnje memorije za zadate uslove (preuzeto sa Benchmark stranice veb sajta www.knot-dns.cz)



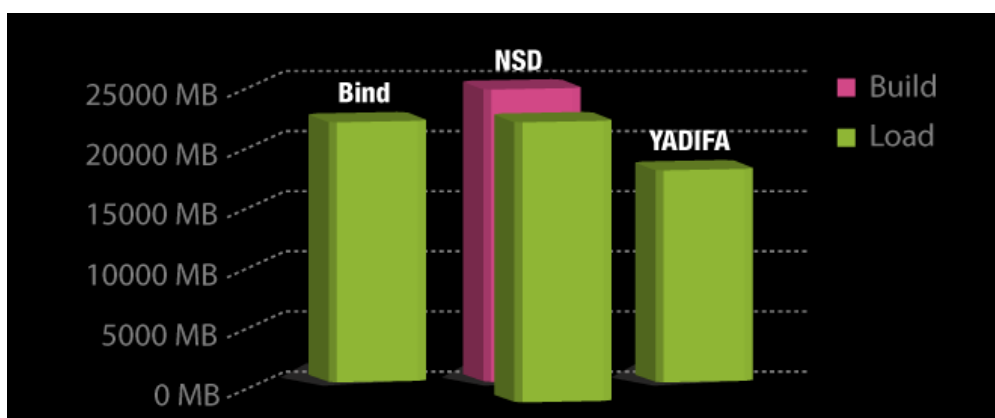
Grafikon 3. – Prikaz brzine procesiranja DNS upita za zadate uslove (preuzeto sa Benchmark stranice veb sajta www.knot-dns.cz)

- *Yadifa*

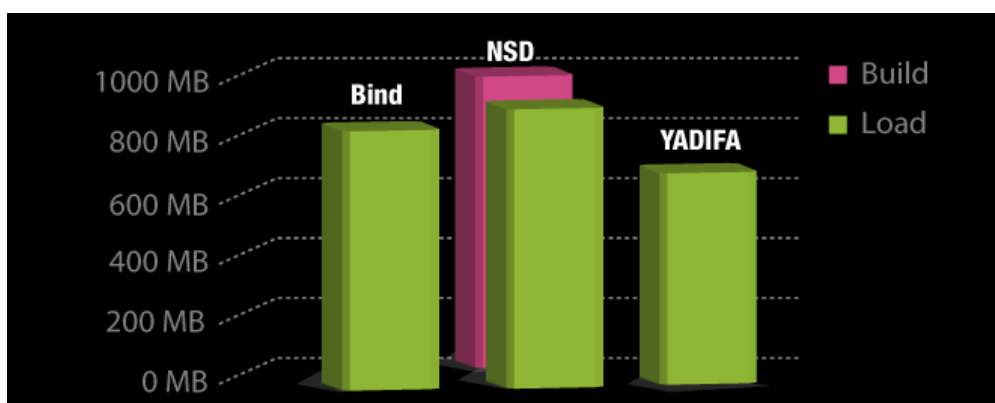
Yadifa server je slično kao i KnotDNS nastao specifično za određenu ciljnu grupu. Razvila ga je grupa autora za TLD operatora .eu domena koji se zove EURid. Samim tim slično kao i

prethodno analizirani softver, birane su opcije koje odgovaraju organizaciji EURid za njihovo upravljanje .eu domenom, tako da za razliku od KnotDNS koji je napravljen da bude maksimalno brz, Yadifa je napravljena da lako upravlja velikim zonskim fajlovima. Ovaj softver spada među najmlađe DNS servere i javno je predstavljen na ICANN konferenciji u Pragu u junu 2012. godine. Ime je dobio od skraćenice za „*Yet Another DNS Implementation For All*“. Yadifa je besplatna za upotrebu i takođe spada u grupu softvera otvorenog koda.

Kao i prethodno pomenuti KnotDNS podržava samo autoritativnu ulogu a ne i rekurzivnu, podržava DNSSEC u potpunosti kao i dinamičko ažuriranje DNS zapisa i niz drugih opcija. Poređenje Yadifa servera i nekih drugih pri pravljenju i učitavanju .com i .eu zona se može videti na sledećim grafikonima.



Grafikon 4. – Prikaz potrošnje memorije pri upravljanju zonskim fajlom .com zone
(preuzeto sa www.yadifa.eu/benchmark)



Grafikon 5. – Prikaz potrošnje memorije pri upravljanju zonskim fajlom .eu zone
(preuzeto sa www.yadifa.eu/benchmark)

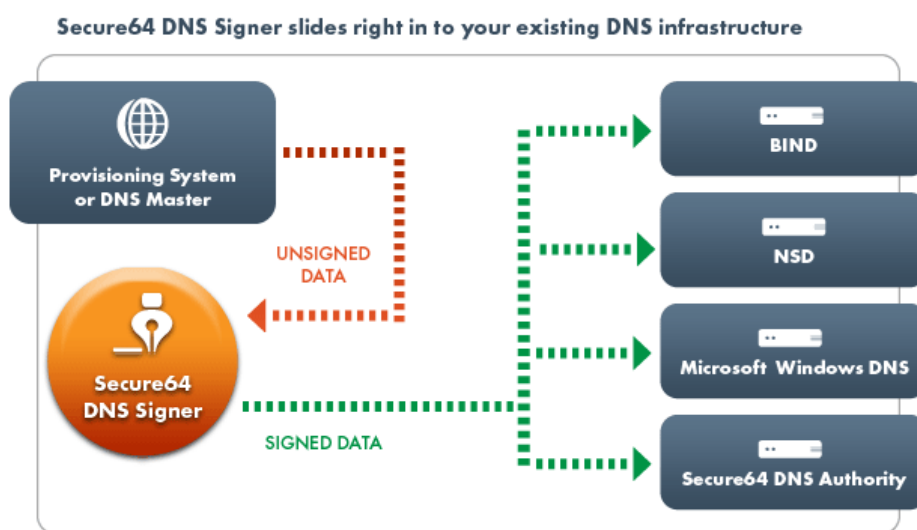
6.1.2. Softver pomoću koga se digitalno potpisuje DNS zona

U prethodnim poglavljima gde je navedeno i ukratko obrazloženo nekoliko DNS servera, rečeno je i da neki od njih u isto vreme mogu i sami da potpisuju DNS zonu koju kreiraju i da čuvaju ključeve. To je rešenje koje olakšava rad, ali ne garantuje visok stepen bezbednosti. Kvalitetnija rešenja obično sadrže poseban softver koji se idealno nalazi na nekoj drugoj fizičkoj ili virtuelnoj mašini i ima sopstvena podešavanja operativnog sistema koja se razlikuju od onih na DNS serveru, čime se podiže nivo zaštite u odnosu na prethodno integralno rešenje.

U narednim poglavljima ćemo se upoznati sa nekoliko softverskih aplikacija koja se bave primarno potpisivanjem DNS zona, ali kao i u slučaju DNS servera neki od njih imaju više uloga i pokrivaju veći deo tog procesa od uobičajenog očekivanja od te vrste softvera.

- Secure64 DNS Signer

Ovaj program za potpisivanje DNS zone je komercijalno rešenje koje je razvila kompanija Secure64. Njegova uloga je potpisivanje zone i prosleđivanje nazad serveru sa koga potiče ili prosleđivanje dalje ka serverima koji predstavljaju spoljnu infrastrukturu. Drugi pomenuti način rada podrazumeva infrastrukturu koja je optimalnija i primerenija DNSSEC implementaciji. To podrazumeva da postoji skriveni DNS server koji se u ovom slučaju zove „Hidden DNS Master“ koji kreira DNS zonu. Skriveni u ovoj rečenici podrazumeva da je server nedostupan bilo kome sa interneta već mu je moguće prići jedino iz interne mreže. Nakon toga se zona prosleđuje na u ovom slučaju Secure64 DNS Signer, ili neki drugi softver za potpisivanje zone, a on dalje potpisanu zonu prosleđuje takozvanim spoljnim DNS serverima koji služe samo da odgovaraju na upite. Šema jednog takvog sistema može se videti na slici broj 11.



Slika 11. – Šema DNS sistema sa skrivenim master serverom (slika preuzeta sa sajta www.secure64.com)

Secure64 DNS Signer spada u programe za potpisivanje koji su relativno jednostavni za implementaciju. Takođe, kako autori tvrde potpuno eliminiše potrebe za pisanjem skripti ili bilo kakvo drugo dodatno programiranje (dodatno programiranje je obično slučaj kod softvera otvorenog koda), kao i da je za implementaciju potrebno jako kratko vreme za razliku od mnogih drugih sistema jer se lako integriše u postojeću infrastrukturu, a pored toga lako se implementira rešenje za oporavak od katastrofe u slučaju drastičnih problema sa serverima koji proizvodi ista kompanija.

Ovaj softver nije besplatan, a u SAD ga koristi nekoliko državnih ustanova za potpisivanje zona njihovih DNS servera.

- OpenDNSSEC

OpenDNSSEC je celovitije rešenje od prethodnog. Pored potpisivanja zone, ovaj softver nudi i čuvanje ključeva. Iza ovog besplatnog softverskog rešenja stoji ekipa autora koju je podržao na prvom mestu švedski nacionalni internet domen registar .se ali i nekoliko drugih kao holandski NLNet Labs, SIDN, engleski Nominet, kanadski registar CIRA i mnogi drugi.

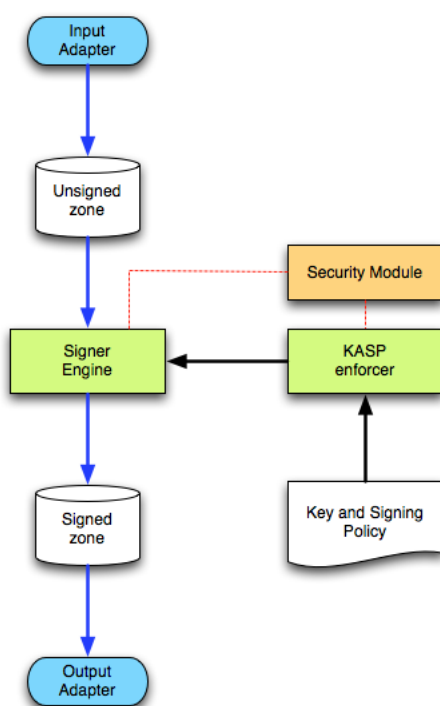
O kvalitetu OpenDNSSEC-a dovoljno govori to što su njegovi korisnici na prvom mestu ICANN koji se može nazvati nultom tačkom koja upravlja internetom i čiji serveri moraju biti zaštićeni apsolutno najvišim nivoom zaštite, zatim nacionalni registri Kanade, Francuske, Švedske, Velike Britanije, Danske, Finske, Francuske, Slovenije i niz drugih. Francuski registar pomoću ovog softvera potpisuje osim svog još pet nacionalnih domena koji predstavljaju nezavisne teritorije ali pod jurisdikcijom Francuske.

Autor ovog rada je imao privilegiju da učestvuje na kursu koji su organizovali srpski nacionalni registar RNIDS i OpenDNSSEC fondacija o principu rada i upotrebljavanju ovog softvera, kao i da upozna dvojicu od autora. Na licu mesta se moglo videti koliko je nezahtevan kada su u pitanju hardverski resursi, a i da iako se njime upravlja kroz komandnu liniju to ne smanjuje njegovu lakoću upravljanja.

Neke od karakteristika ovog softvera koje bi trebalo napomenuti su njegova skalabilnost, jer se sistem sam prilagođava memorijski uslovima potpisivanja malih i velikih zona, kako autori tvrde od nekoliko zapisa u zoni do više miliona zapisa u zoni. Druga bitna karakteristika je mogućnost potpisivanja jedne ili više zona na istoj instanci softvera, kao i mogućnost da se istim ključem potpisuje više DNS zona čime se čuva prostor, bez obzira na to da li se ključevi čuvaju na istoj mašini ili na posebnom hardveru. Bitna karakteristika je i to što može raditi na različitim distribucijama UNIX/Linux operativnih sistema pa nije potrebno dodatno obrazovanje kadrova za specifične operativne sisteme što je slučaj kod prethodno pomenutog softvera Secure64 DNS Signer.

Sastavni deo OpenDNSSEC-a koji služi za čuvanje softverskih ključeva kojima se potpisuje DNS zona (KSK i ZSK) se zove SoftHSM i on upotpunjuje ovo rešenje u integralnu celinu koja lako funkcioniše te mu nije neophodan poseban hardver za bezbedno čuvanje ključeva. Aktuelna verzija u trenutku pisanja ovog rada je 1.4.5. a aktuelna verzija SoftHSM modula je 1.3.7.

Na grafikonu ispod se može videti proces potpisivanja zone koristeći OpenDNSSEC i mogućnost korišćenja KASP (*Key and Signing Policy*) modula koji unapred određenom politikom definiše bitne karakteristike potpisivanja, kao što su dužina trajanja potpisane zone, dužina trajanja softverskih ključeva za potpisivanje zone, dužina softverskog ključa i mnoge druge.



Slika 18. – Algoritam koji prikazuje proces potpisivanja DNS zone softverom OpenDNSSEC (preuzeto sa sajta www.opendnssec.org)

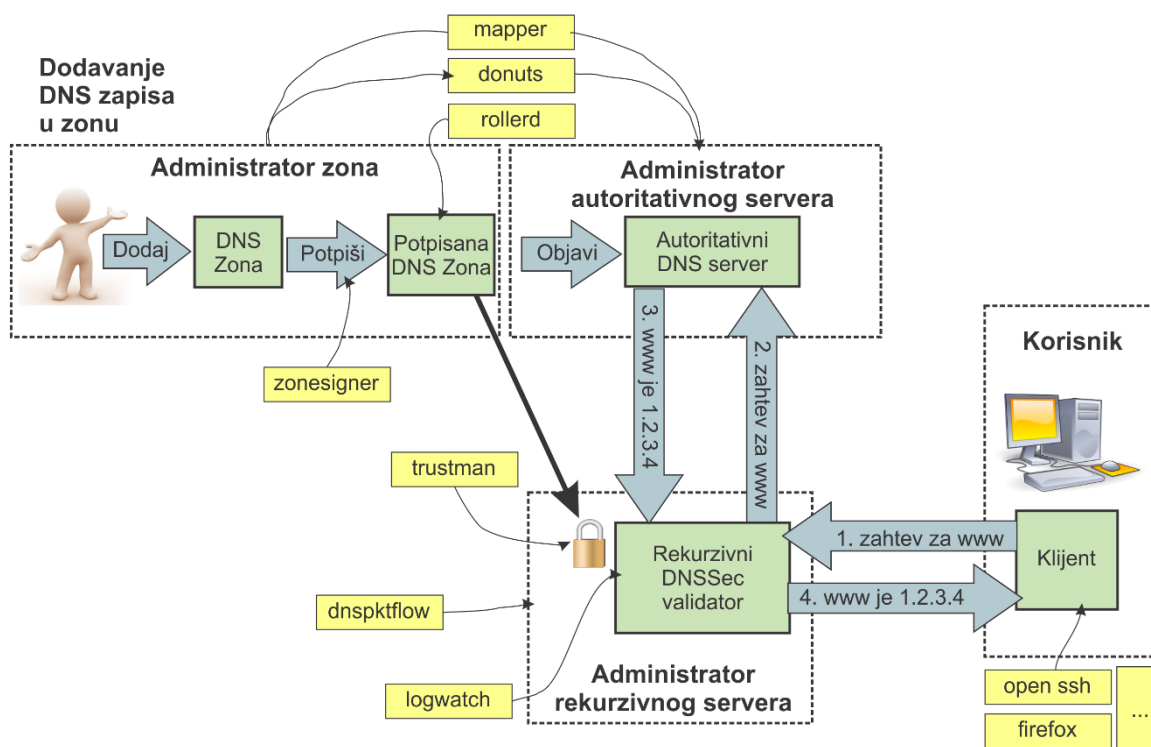
- LDNS Signer

LDNS Signer je razvijen u Holandiji i za njegov razvoj je zaslužna organizacija NLNet Labs. To je kako autori sami kažu alat za potpisivanje DNSSEC zona sa tom jedinom ulogom, ali sa svim potrebnim opcijama koje zadovoljavaju tu ulogu potpisivanja u potpunosti. Pravljen je kao i većina za UNIX/Linux operativne sisteme i takođe, kao kod većine njime se upravlja pomoću komandi preko komandne linije. Kriptografski deo ovog softvera je baziran na OpenSSL standardu, što je podrazumevalo da je nakon slabosti ovog standarda pronađene početkom 2014. godine da sam LDNS bude detaljno analiziran i otklonjeni problemi.

Pored uobičajenih opcija LDNS ima mogućnost provere i verifikacije potpisanih zona a od skora je implementirana podrška za oba IP protokola (IPv4 i IPv6). Ono što posebno odlikuje ovaj softver je što zauzima jako malo mesta na disku i u memoriji tokom rada, ali zato nije predviđen za potpisivanje jako velikih zonskih fajlova. Korišćenje ovog softvera nije lako za administratore koji nisu posebno obučeni da rade u njemu. [F]

- DNSSEC-Tools

Ovaj besplatni softver u suštini predstavlja skup alata koji se odnose na DNSSEC, ali u okviru njega postoji posebna aplikacija koja se zove zonesigner. Zonesigner se još uvek razvija, i iako nije u beta fazi on još uvek nema neku veliku upotrebnu vrednost kao prethodno pomenute aplikacije. U planu je razvoj „čarobnjaka“ koji bi u nekoliko pitanja i klikova mišem omogućio lako i brzo potpisivanje zone u 4 koraka (učitavanje zone, potpisivanje, testiranje, postavljanje na master ili slave server). Pored toga radi se na dodacima koji će i više od toga olakšavati rad administratorima. Na slici ispod se nalazi šema koja opisuje proces potpisivanja zone u slučaju aplikacije zonesigner iz DNSSEC-Tools.



Slika 19. – Proces potpisivanja DNS zone korišćenjem DNSSEC-Tools i mesto svake aplikacije u procesu (preuzeto sa sajta www.dnssec-tools.org)

6.1.3. Uređaji za generisanje i čuvanje tajnih softverskih ključeva za potpisivanje zone

Ranije je već pomenuto pri objašnjavanju da neki od softverskih paketa gore pomenutih imaju pored drugih mogućnosti i mogućnost da generišu i čuvaju ključeve za potpisivanje DNS zona. Ipak, neuporedivo je veći nivo sigurnosti kada se za tu namenu koristi specijalizovan hardver i softver, ili makar samo specijalizovan softver (kao u slučaju SoftHSM). U ovoj oblasti ima jako puno rešenja pa će u poglavlju biti pobrojane grupe tipova i specifična rešenja koja zaslužuju posebnu pažnju, takođe, pod softverom u ovom poglavlju podrazumevaće se softver integrisan u hardversko rešenje i koji je njegov sastavni deo osim kod softverskih rešenja koja se nalaze na uobičajenom hardveru koja će biti samo pomenuta i ne preterano elaborirana. [13]

- Softverska rešenja

Najreprezentativniji primerak ove grupe uređaja, a u ovom slučaju to je samo uslovno zbog toga što je samo softver u pitanju je SoftHSM koji dolazi u paketu sa pominjanim softverom OpenDNSSEC. Karakteristike ove grupe su:

- niska cena (postoje i besplatni)
- kapacitet za čuvanje ključeva je limitiran samo računarom na koji je softver instaliran
- brzina kriptografskih operacija je limitirana performansama računara na kojem se softver nalazi
- niska bezbednost zbog ne korišćenja hardvera posebno pravljenog za zaštitu

Ova rešenja mogu da se primenjuju ili u nekim malim okruženjima koja nisu od strateškog značaja (primer strateški bitnih su nacionalni internet domen registri, ovlašćeni registri za registrovanje TLD domena, veliki DNS provajderi i slično) ili se mogu koristiti u test okruženjima za ispitivanje funkcionalnosti zbog ograničenih budžeta za testiranje ali i odsustvu potrebe za visoku bezbednost DNSSEC infrastrukture.

- Hardverska rešenja

Ova rešenja se svrstavaju u više grupa prema tome koji hardver se koristi i kolika ulaganja su potrebna za kupovinu istog. Pa tako imamo:

a.) Smart kartice i USB tokeni

- Niska cena (cena ovog hardvera je jako niska delom zbog njegove jednostavnosti a delom zbog masovnosti upotrebe)
- Mobilnost (sve ove uređaje je praktično moguće lako preneti sa mesta na mesto i uključiti u drugu mrežu, iz tog razloga za njih je potrebno dodatno odrediti posebno fizičko obezbeđenje)

- Mali smeštajni kapaciteti na samom uređaju
- Mala brzina kriptografskih operacija
- Nisu podržani ili su jako slabo podržani simetrični kriptografski algoritmi

b.) PCI kartice i zasebne hardverske jedinice niže i srednje cene (kripto akceleratori)

- Značajno viša cena nego kod prve grupe hardvera (2000-20000 EUR)
- Fiksna lokacija (nisu predviđeni za prenos pa nisu mobilni već su ili ugrađeni u neki server u slučaju PCI kartica ili se nalaze u nekom serverskom ormanu kao zaseban serverski uređaj)
- Fokus nije na kapacitetu za smeštanje ključeva već na brzini operacija (drugi naziv za ovaj tip uređaja je kripto akcelerator ili SSL akcelerator)
- Jako velike brzine kripto operacija i simetričnih i asimetričnih

c.) PCI kartice i zasebne hardverske jedinice srednje cene i više cene (hardverski akceleratori)

- Najviša cena od svih pomenutih uređaja (5000-30000 EUR)
- Fiksna lokacija (nisu predviđeni za prenos pa nisu mobilni već su ili ugrađeni u neki server u slučaju PCI kartica ili se nalaze u nekom serverskom ormanu kao zaseban serverski uređaj)
- Fokus je na smeštajnom kapacitetu (moguće je bezbedno smeštanje hiljada RSA ključeva)
- Podržavaju kriptografsku akceleraciju

- Prikaz nekih modela HMS uređaja

a.) Sun Crypto Accelerator 6000 PCI Express Adapter

Kripto akcelerator tipa 6000 od kompanije Sun je hardverski dodatak (interni) za već postojeći server. Ova PCI Express kartica se ugrađuje u prvi slobodan PCI Express slot na serveru koji ima faktor x8. Na sebi ima mrežni ulaz (RJ-11) kao i USB 2.0 port za direktan pristup. Ovaj akcelerator zadovoljava standard FIPS 140-2 nivoa 3, kao što zahteva najveći broj organizacija koji radi sa poverljivim podacima.

Hardverski kartica podržava do 13000 konkurentnih sesija u sekundi po SSL standardu sa ključevima veličine do 1024 bita, a takođe poseduje i EMC standard elektromagnetne kompatibilnosti klase A. Pored namene za obradu ključeva korišćenih za DNSSEC može se koristiti i za verifikaciju PIN-ova i kreditnih kartica u finansijskim transakcijama. Na slici ispod se može videti izgled ovog adaptera.



Slika 110. - Sun Crypto Accelerator 6000 PCIe Adapter
(slika preuzeta sa sajta proizvođača adaptera www.oracle.com)

b.) Ultra Electronics AEP Keyper HSM

Keyper HSM je za razliku od prethodno pomenutog HSM uređaja (kripto akcelerator adapter) potpuni uređaj osposobljen za samostalan rad bez potrebe za nekim drugim hardverom na koji se priključuje. O kvalitetu ovog specifičnog HSM uređaja najbolje govori to što je baš on izabran nakon duge analize da bude uređaj za potpisivanje root zona interneta i čuvanje DNSSEC ključeva organizacije ICANN. Root serveri su početak lanca poverenja i bilo je potrebno odabrati najsigurniji mogući uređaj i smestiti ga na najsigurniju lokaciju da bi se izbeglo bilo kakvo kompromitovanje procesa potpisivanja i čuvanja ključeva.

Keyper HSM proizvodi engleska kompanija Ultra Electronics AEP koja za svoje uređaje obezbeđuje najviše standarde bezbednosti na osnovu kvaliteta i duge proizvodnje u ovoj oblasti. Tako i Keyper HSM ima FIPS 140-2 sertifikat nivoa 4 čime se pokazuje njegova snaga i ozbiljnost u čuvanju ključeva. Proizvođači tvrde da je to jedini uređaj na tržištu koji je do sada pokazao potrebne karakteristike za dobijanje nivoa 4 ovog FIPS sertifikata.

Uređaj takođe poseduje mrežni ulaz kao i serijski ulaz za direktan pristup i podešavanje uređaja. Karakteristika ovog uređaja koja je posebno bitna u radu sa DNSSEC ključevima je njegova mogućnost da generiše slučajne brojeve sa potpunom entropijom i za to poseduje sertifikate kao dokaz (FIPS 186-2 sertifikat 699).

Sam uređaj ako se koristi kao DNSSEC HSM dolazi sa besplatnim paketom koji je preinstaliran i zaštićen u samom uređaju. Paket je nasnimljen kao DNSSEC virtual appliance na DVD disk koji dolazi zajedno sa uređajem. Samim tim na HSM uređaju se ne nalazi bilo kakav softver jer se on učitava sa DVD uređaja, već se na uređaju nalaze snimljeni samo ključevi za potpisivanje zona (KSK i ZSK) u sigurnom okruženju. Paket koji dolazi uz uređaj sadrži sledeće:

- ISC BIND DNS Server (aktuelna verzija BIND 9)
- CEntOS (Community Enterprise Operating System) virtuelizovan sa fizičke mašine i pripremljen kao virtual appliance (virtualna mašina pripremljena za rad bez potrebe za bilo kakvom dodatnom instalacijom).
- OpenSSL
- Keyper upravljačke programe

Treba naglasiti da ni BIND ni CEntOS nisu standardne verzije već ojačane verzije sa odbačenim aplikacijama i modulima koje se ne koriste u DNSSEC procesima da bi se maksimalno povećala bezbednost samog HSM uređaja. Uređaj štiti ključeve dok god je to u mogućnosti, dok u slučaju pokušaja hemijskog ili mehaničkog napada na uređaj i pokušaja otvaranja, uređaj po osnovnom podešavanju na najsigurniji način uništava sav sadržaj koji se nalazi na njemu i ne dozvoljava nasilan pristup čuvanom sadržaju. Uvoz i izvoz ključeva sa i na uređaj se može vršiti putem kombinacije standardnih Smart kartica i PIN-a koji je vezan za karticu.

U slučaju potrebe za obradom velikog broja krypto podataka, ili velikog broja zahteva za ključevima, moguće je vezati do 16 ovih uređaja paralelno da se obezbedi ravnomerna raspodela opterećenja (load balancing) pri čemu se opterećenje preuzima i od uređaja koji su se potencijalno pokvarili u ovom lancu. Na slici ispod se može videti izgled uređaja Keyper HSM.



Slika 111. – Uređaj Keyper HSM (slika preuzeta sa sajta proizvođača www.ultra-aep.com)

6.1.4. Serveri za razrešavanje DNS upita korisnika i verifikaciju DNSSEC potpisa

U prethodnim poglavljima je već pomenuto da neki od DNS servera koji su detaljnije opisani pored ostalih uloga imaju i uloge rekurzivnih DNS servera, to jest servera koji razrešavaju DNS upite korisnika i takođe verifikuju da li je DNSSEC potpis odgovarajuće DNS zone ispravan i validan. Ovi servere najčešće srećemo kod internet provajdera kada je njihova uloga da pronađu željene adrese na internetu za klijente tog internet provajdera, ali takođe ih možemo naći i kod velikih kompanija sa puno računara koji imaju sopstvenu DNS infrastrukturu i koji koriste sopstvene servere za dalje upite na internetu.

Princip rada rekurzivnih DNS servera je da oni upite klijenata prosleđuju dalje do root DNS servera, zatim do TLD autoritativnih servera, pa onda od servera autoritativnih za upitanu zonu (primer www.rnids.rs, najpre bi bio pitan root server gde je DNS za .rs, pa zatim gde je DNS server za rnids.rs i na kraju bi taj DNS server bio upitan gde je www.rnids.rs) i tako redom do konačnog odgovora koji se prosleđuje klijentu i on biva upućen na traženu adresu.

DNS servera koji su specijalizovani da budu samo rekurzivni nema mnogo i njihova uloga je najmanje bitna u ovom procesu (daleko češće se u ovoj ulozi sreću serveri koji imaju i druge uloge, kako zbog toga što su kvalitetniji tako i zbog poznatosti i manje potrebe za dodatnom obukom zaposlenih za rukovanje) pa će samo biti pomenuti bez daljeg objašnjavanja. Možda najpoznatiji rekurzivni DNS server je Unbound koji je proizvod holandske organizacije NLNet Labs, a pored njega postoje i Nominum koji je komercijalan kao i softveri otvorenog koda kao PdnsD i DNRD (Domain Name Relay Daemon).

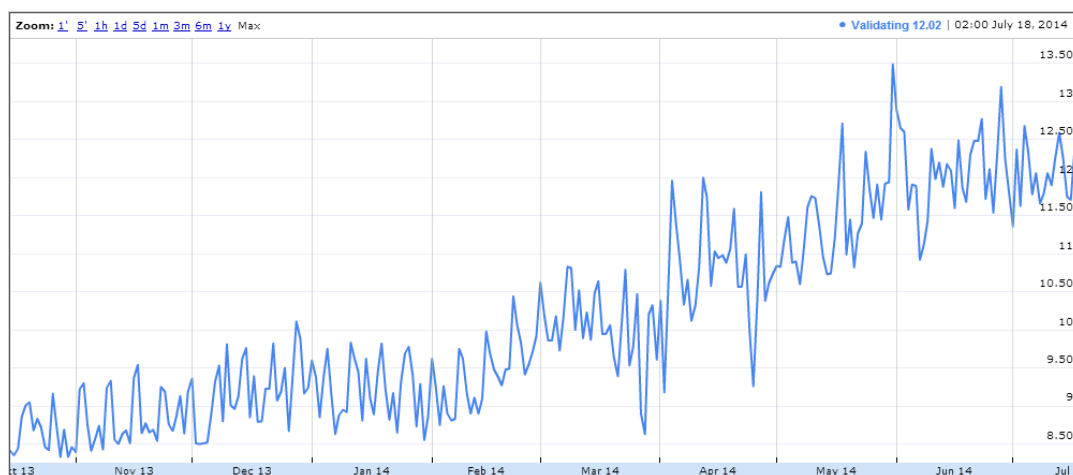
Verifikacija DNSSEC potpisa je još uvek nerešen problem. Većina DNS servera na internetu ne verifikuje DNSSEC potpise jer još uvek ne osećaju potrebu za tim, a time i izbegavaju povećan saobraćaj zbog toga što je odgovor potpisanog servera tri do četiri puta veći od odgovora nepotpisanog servera. Na svom blogu autor Geoff Huston je rekao da je od trenutka kad je najveći javni rekurzivni DNS server u vlasništvu kompanije Google počeo da radi validaciju DNSSEC potpisa procenat validiranih upita na internetu porastao sa oko 4% na oko 8%. [4]

Takođe, u priču oko verifikacije DNSSEC potpisa DNS zona se uključuju i autori operativnih sistema, kako onih otvorenog koda tako i Microsoft, pa se očekuje da verifikacija bude implementirana na sistemskom nivou, što ne isključuje validaciju na rekurzivnim DNS serverima već samo dodaje još jedan nivo sigurnosti.

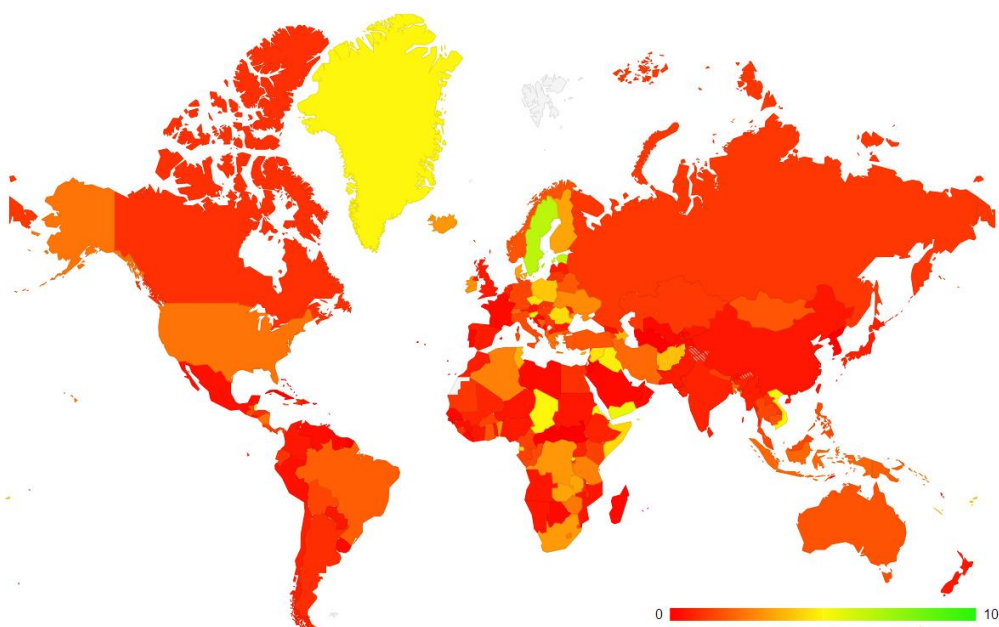
Postoje i dodaci za veb pregledače kao što su Chrome i Firefox. Najpoznatije dodatke je napravila češka grupa programera okupljena oko projekta KnotDNS. Mora se naglasiti da su ovi dodaci vrlo uskog polja verifikacije i validacije i odnose se samo na pregledače veba koji su pomenuti i takođe da verifikuju samo ono što kroz dati pregledač prolazi, te ukoliko postoji

neki dodatni softver na računaru koji koristi DNS upite (može biti bilo koji softver koji ima pravo izlaska na internet, kako zbog ažuriranja verzija ili potpisa ako je antivirus u pitanju, bankovni softver i slično) na njega verifikacija nema nikakav uticaj i njegovi upiti nisu provereni.

Na grafikonima ispod se može videti vremenski trend porasta procenta validiranih DNSSEC upita na svetskom nivou kao i mapu država sa procentualnim bojem validacija DNSSEC za odgovarajuću državu.



Slika 112. – Grafikon trenda porasta procenta DNSSEC validacija na internetu
(grafikon preuzet sa internet prezentacije www.internetsociety.org/deploy360/dnssec/)



Slika 113. – Grafički prikaz procentualne validacije DNSSEC potpisa po državama
(mapa preuzeta sa internet prezentacije www.internetsociety.org/deploy360/dnssec/)

7. Slabosti DNSSEC-a

Kao i svaki drugi servis, sistem, inovacija, tako i DNSSEC pored svih nabrojanih dobrih strana ima i slabe strane koje ga čine manje upotrebljivim, teškim za korišćenje, pa i podložnim napadima i čak oružjem za napad na druge. U ovom poglavlju će biti pobrojani glavne slabosti i nedostaci DNSSEC, a posebno će biti objašnjena uloga DNSSEC potpisanih DNS servera kao oružja u rukama hakera.

7.1. Visoki troškovi

U analizi troškova koji su neophodni da bi neka organizacija uvela DNSSEC, prema ENISA-i (European Network and Information Security Agency) organizacije se mogu podeliti na dve grupe; veliki potrošači i velike štediške. U skladu sa tim se i kreće raspon neophodnih troškova. Tako sa malopre pomenutom podelom se i kreće u implementaciju; velike štediške će se truditi da ojačaju postojeću infrastrukturu i da u nju „uglave“ DNSSEC, dok će veliki potrošači uvođenje videti kao priliku da zamene u potpunosti postojeći sistem novim u koji je integrisan DNSSEC.

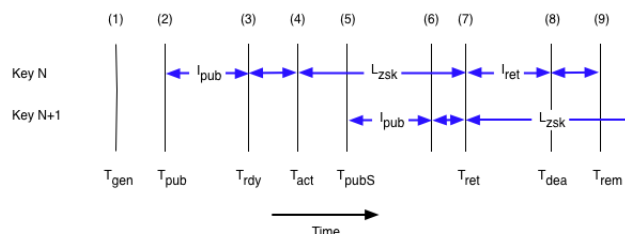
U istoj analizi troškova potrebnih za uvođenje DNSSEC procenjeno je da se oni kreću od 250.000 evra do 1.250.000 evra u slučaju DNS operatora najvišeg reda, pa do ovlašćenih registara čija cena uvođenja se kreće oko 10.000 evra. U skladu sa rastom troškova kreće se i vreme potrebno za implementaciju jer je i osetljivost sistema veća, veći je broj pravila i procedura koje treba uvesti a sa svim tim traje i vreme implementacije koje i samim povećavanjem dodatno povećava cenu. Uz pomenute troškove treba dodati i troškove obučavanja zaposlenih za rukovanje novim sistemom.

Da bi se neutralisala ova slabost visokih troškova, potrebno je dobro planirati resurse, napraviti plan potrebnih promena i onda krenuti u implementaciju da bi se izbegli neplanirani i skriveni troškovi. [19]

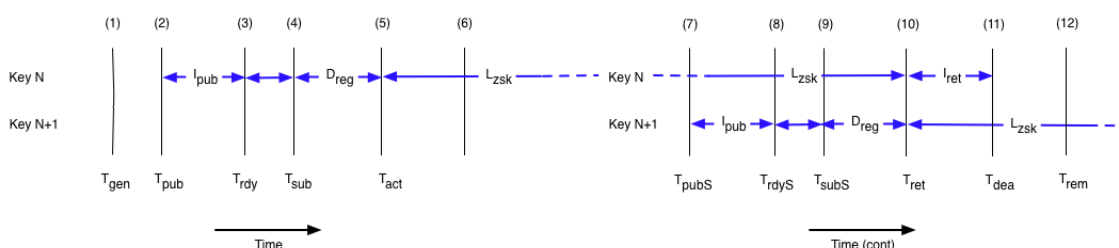
7.2. Komplikovanost sistema

Jedno od nepisanih pravila tehnike i tehnologije je da što sistem ima više komponenti to je veća verovatnoća da dođe do problema u radu. U slučaju DNSSEC to pravilo može da važi. Kao što smo videli do sada DNSSEC sistem se sastoji od više komada različitog softvera i hardvera, prisutna je i mrežna infrastruktura koja je od trenutka puštanja u rad DNSSEC opterećenija tri do četiri puta više. Bitna komponenta sistema je i vreme. Vremenski intervali generisanja zona, potpisivanja, objavljivanja zona i javnih ključeva, trajanja ključeva i ostali, moraju biti vrlo

egzaktni jer u suprotnom sistem prestaje da bude siguran i DNSSEC potpisane zone prestaju da budu validne. Na slikama ispod su prikazani tačni predefinisani vremenski intervali različitih stanja ključeva u DNSSEC (KSK key signing key i ZSK zone signing key) i na kojima se može zapaziti složenost vremenskih intervala koji svaki put moraju u potpunosti biti ispoštovani da bi sistem radio ispravno. [18]



Slika 114. – Vremenska skala koja prikazuje trajanje različitih stanja kod ključa za potpisivanje zone ZSK (preuzeto sa sajta wiki.opendssec.org)



Slika 115. - Vremenska skala koja prikazuje trajanje različitih stanja kod ključa za potpisivanje ključa kojim je potpisana zona KSK (preuzeto sa sajta wiki.opendssec.org)

Ono što predstavlja dodatni potencijalni problem je i to što svaka greška koja se napravi ili svako kompromitovanje sistema, podrazumeva promenu praktično svih podataka i resetovanje vrednosti (promene ključeva i resetovanje svih vrednosti na početne vrednosti) što predstavlja veliki zastoј u radu koji je neprihvatljiv kod sistema koji moraju da rade kontinualno po pravilu 24/7. [9]

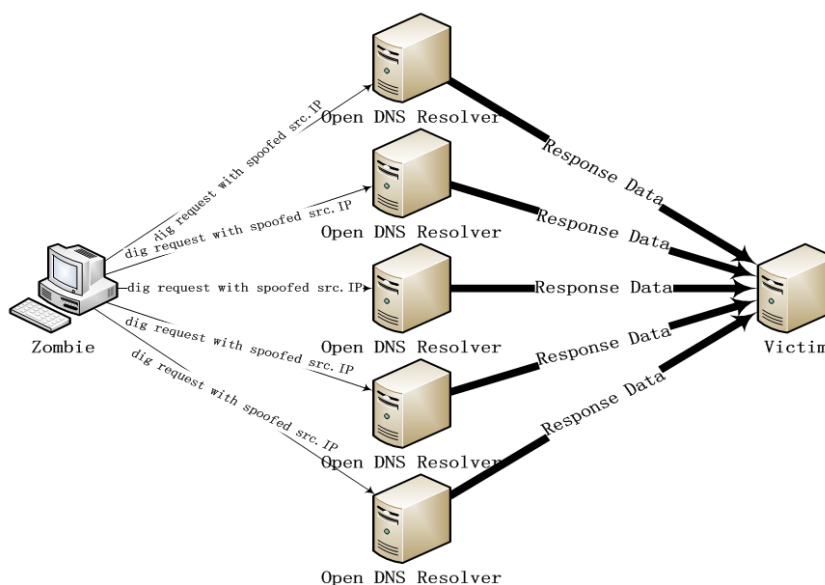
7.3. Podložnost DDoS napadima

Veliki problem svih servisa na internetu predstavljaju DoS (Denial of Service) i DDoS (Distributed Denial of Service) napadi. Ovi napadi predstavljaju opterećenje servera od strane osobe koja želi da taj servis učini nedostupnim, do trenutka kad servis prestane da pruža uslugu kojoj je namenjen. DoS napadi su jednostavniji i potiču uglavnom sa jednog izvora, dok DDoS napadi predstavljaju daleko složeniji problem jer su distribuirani i dolaze sa mnogo različitih strana.

Svaki servis na internetu je podložan ovome, ali u poslednjih par godina je zabeleženo mnogo slučajeva kada su DNS serveri iskorišćeni kao oružje za pojačavanje DDoS napada na neki treći

cilj. Ovakvi napadi se zovu amplifikovani (pojačani) DDoS napadi. Pojačani napadi se izvode tako što napadač lažira svoju IP adresu adresom žrtve i pošalje sa te adrese ogroman broj upita različitim DNS serverima.

Na upite tipa „*dig any request*“ DNS serveri odgovaraju tekstom koji je mnogo puta veći od samog upita (za upit kao što je navedeno od 20-tak bajtova dobija se odgovor od oko 2kB što je u proseku oko 100 više). Tako je napadač pojačao svoj napad koristeći DNS servere oko 100 puta. U slučaju da je DNS zona servera koji se koristi za napad DNSSEC potpisana odnos pojačanja ide od 50 do 200 puta, pri čemu se i mrežna infrastruktura oko samog DNS servera opterećuje kako upitima tako i odgovorima te samim tim blokira i sve uređaje koji nisu dovoljno jaki za propuštanje takvog saobraćaja. Na slici ispod se nalazi prikaz šeme jednog pojačanog DDoS napada.



Slika 16. – Šematski prikaz pojačanog DDoS napada (slika preuzeta sa sajta www.nsfocusblog.com)

Prava i trajna odbrana od različitih DDoS napada ne postoji. Sve se svodi na to da je potrebno posedovati velike internet linkove i jaku mrežnu infrastrukturu sa moćnim mrežnim uređajima koji mogu da izdrže napad i da preusmere saobraćaj, ali u slučaju pojačanog DDoS napada i DNS servera koristi se još jedna taktika, „rate limiting“ kojom se onemogućava sa se sa jedne adrese ili na jednu adresu šalje više odgovora nego što to server dozvoljava. Izračuna se na osnovu dosadašnjeg saobraćaja i pretpostavi se na osnovu toga da obični korisnici mogu da postave jedan broj upita u sekundi, i na osnovu toga se postavlja limit koliko upita neka adresa može da traži i koliko odgovora da dobije. Time se ne brani sam DNS server jer ga je i dalje moguće zatrpati zahtevima, ali time DNS serveri štite druge korisnike da ih neko ne bi koristio kao oružje.

Na listingu ispod dat je primer odgovora DNS servera sa DNSSEC potpisom na jednostavnu „dig any“ komandu koju zadaje napadač.

Komanda

```
dig ANY ddos.rs @1.2.3.4
```

Odgovor

```
; <<>> DiG 9.7.3 <<>> ANY ddos.rs @1.2.3.4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5147
;; flags: qr rd ra; QUERY: 1, ANSWER: 27, AUTHORITY: 4, ADDITIONAL: 5

;; QUESTION SECTION:
;ddos.rs.                IN      ANY

;; ANSWER SECTION:
ddos.rs.                4084    IN      SOA      ns-int.ddos.rs. hostmaster.ddos.rs.
2012102700 7200 3600 24796800 3600
ddos.rs.                4084    IN      A        149.20.64.42
ddos.rs.                4084    IN      MX       10 mx.rs1.ddos.rs.
ddos.rs.                4084    IN      MX       10 mx.rs2.ddos.rs.
ddos.rs.                4084    IN      TXT      "v=spf1 a mx ip4:204.152.184.0/21
ip4:149.20.0.0/16 ip6:2001:04F8::0/32 ip6:2001:500:60::65/128 ~all"
ddos.rs.                4084    IN      TXT      "$Id: ddos.rs,v 1.1724 2012-10-23
00:36:09 bind Exp $"
ddos.rs.                4084    IN      AAAA     2001:4f8:0:2::d
ddos.rs.                4084    IN      NAPTR    20 0 "S" "SIP+D2U" ""
_sip._udp.ddos.rs.
ddos.rs.                484     IN      NSEC     _kerberos.ddos.rs. A NS SOA MX TXT
AAAA NAPTR RRSIG NSEC DNSKEY SPF
ddos.rs.                4084    IN      DNSKEY   256 3 5
BQEAAAAB2F1v2HWzCCE9vNsKfk0K8vd4EBwizNT9KO6WYXj0oxEL4eOJ
aXbax/BzPFx+3q08B8pu8E/JjkWH0oaYz4guUyTVmT5Eelg44Vblkssy
q8W27oQ+9qNiP8Jv6zdOj0uCB/N0fxFVL3371xbednFqoECfSFDZa6Hw jU1qzveSsW0=
ddos.rs.                4084    IN      DNSKEY   257 3 5
BEAAAAOAhHQDBrhQbtphgq2wQUpeEQ5t4DtUHxoMVfu2hWLDmvoOMRXjGr
hhCeFvAZih7yJHf8ZGfW6hd38hXG/xyLYCO6Krpbdjwx8YMXLA5/kA+
u50WIL8ZR1R6KTbsYVMf/Qx5RiNbPCLw+vT+U8eXEJmO20jIS1ULgqy3
47cBB1zMnnz/4LJpA0da9CbKj3A254T515sNIMcwsB8/2+2E63/zZrQz
Bkj0BrN/9Bexjpiks3jRhZatEsXn3dT47R09Uix5WcJt+xzqZ7+ysyL
KOOeds39Z7SDmsn2eA0FKtQpwA6LXeG2w+jxmw3oA81lVUGef/rzeC/bB yBNs070aEFTd
ddos.rs.                4084    IN      SPF      "v=spf1 a mx ip4:204.152.184.0/21
ip4:149.20.0.0/16 ip6:2001:04F8::0/32 ip6:2001:500:60::65/128 ~all"
ddos.rs.                484     IN      RRSIG    NS 5 2 7200 20121125230752
20121026230752 4442 ddos.rs. oFeNy69Pn+/JnnltGPUZQnYz0lYGglMhS/SZKnlgyMbztT2r/2v+X1j
AkU19GRW9JAZU+x0eEj5oNAkRiQqK+D6DC+PGdM2/JHa0X41LnMIE2NX
UHDAKMmbqk529fUy3MvA/ZwR9FXurcfYQ5fnpEEaawNS0bKxomw48dcp Aco=
ddos.rs.                484     IN      RRSIG    SOA 5 2 7200 20121125230752
20121026230752 4442 ddos.rs. S+DLHzE/8WQbnSl70geMYoKvG1IuKARVlxmssce+MX6DO/J1xdK9xGac
XCuAhRpTMKElKq2dIhKp8vnS2e+JTZLrG14q/bnrmmhQ9eBS7IFmrQ6s
0cKEEyuijumOP1KCCN9QX7ds4siiTlrEOGHCaamEgrJqVxqCsgldBUrR hKk=
ddos.rs.                484     IN      RRSIG    MX 5 2 7200 20121125230752
20121026230752 4442 ddos.rs. VFqFWRPyulIT8VsIdXKMPMRJTYpdggoGgOjKJzKJs/6ZrxmbJtmAxEu
/rkwD6Q9JwsUCepNC74EYxzXFvDaNnKp/Qdmt2139h/xoZsw0JVA4Z+b
zNQ3kNiDjdV6z16ELtCVDqj3SiWDZhYB/CR9pNno1FAF2j0iJYSwiwBS Lcw=
ddos.rs.                484     IN      RRSIG    TXT 5 2 7200 20121125230752
20121026230752 4442 ddos.rs. Ojj8YCzf3jYl9eO8w4Tl9HjWKP3CKXQRFed8s9xeh5TR3KI3tQTKsSeI
JRQaCXkADiRwHt0j7VaJ3xUHa5LCKzetcVgJNPmhovValw87Hz4DU6q9
k9bbshvbYtXOF8xny/FCiR5c6NveLmvvu4xeOqSwIpoo2zvIEFFP9deR Uha=
ddos.rs.                484     IN      RRSIG    AAAA 5 2 7200 20121125230752
20121026230752 4442 ddos.rs. hutAcro0NBmVku/m+2lF8sgIYyIVWORTp/utIn8KsF1W0wwM2QMGA5C9
/rH/ZQBQn46ZMmiEm4LxH6mtaKxMsBGZwgzUEDfsvVtr+fs5NUoAlrF
wg92eBbInNdCvT0if8m1sldx5/hSqKn8EAscKfg5BMQp5YDFs1lsTauA 8Y4=
```

```

ddos.rs. 484 IN RRSIG NAPTR 5 2 7200 20121125230752
20121026230752 4442 ddos.rs. ZD14qEHR7jVXn5uJUn6XR9Lvt5Pa7YTEW94hNAn9Lm3Tlnkg11AeZiOU
3woQ1pg+esCQepKCIBlplPLcag3LHlQ19OdACrHGuzzM+rnHY50Rn/H4
XQTqUWHBF2Cs0CvfqRxLvAl5AY6P2bb/iUQ6hV8Go0OFvmMEkJonxPPw 5i4=
ddos.rs. 484 IN RRSIG NSEC 5 2 3600 20121125230752
20121026230752 4442 ddos.rs. rY1hqZAryM045vv3bMY0wgJhxHJQofkXLeRLk20LaUlmVTyu7uair7jb
MwDVCVhx7f7gRdgu8x7LPSvJKU16sn731Y80CnGwszXBp6tVpgw6oOcr
Pi0rsnzC61IarXLwNBfMLZg2Aza6SSirzOPObnmK6PLQCdmaVAPrVJQs FHY=
ddos.rs. 484 IN RRSIG DNSKEY 5 2 7200 20121125230126
20121026230126 4442 ddos.rs. i0S2MFqvHB3wOhv2IPoze/IQABM/eDDCV2D7dJ3AuOwi1A3sbyQ29XUD
BK82+mxxsET2U6hv64crpbGTNPJ30sMxNOAFA0QYphoMnt0jg3OYg+AC
L2j92kx8ZdEhxKiE6pm+cFVBHLLmXGKLdAVnffLvlGQIl5YrIyy4jiw h0A=
ddos.rs. 484 IN RRSIG DNSKEY 5 2 7200 20121125230126
20121026230126 12892 ddos.rs. j1kgWw+wFFw01E2z2kXq+biTG1rrnG1XoP17pIoT0ZHElgy7F6kEgyj
fN6e2C+gvXxOAAABQ+qr76o+P+ZUHRLUEI0ewtC3v4HzIME10Z2/NE0MH
qAEdmEemeZKn901EAOC7gZ4nU5psmuYlqxcCkUDbW0qhLd+u/8+d6L1S
nlrD/vEi4R1SL12bD5VBtaxczOz+2BEQLveUt/UusSlqhYcFjdCYbHqF
JGQziTJv9ssbEDHT7COc05gG+A1Av5tNN5ag7QHWa0VE+Ux0nH7JUy0N
chlKVecPhXJVHRF97CEH5wCDEgcFKAYyhaXXh02fqBGfON8R5mIcgo/F DRdXjA==
ddos.rs. 484 IN RRSIG SPF 5 2 7200 20121125230752
20121026230752 4442 ddos.rs. IB/bo9HPjr6aZqPRkzf9bXyK8TpBFj3HNQloqhrquMSBfcMfmJqHxKyD
ZoLKZkQk9kPeztau6hj2YnyBoTd0zIVJ5fVSqJPuNqxwm2h9HMs140r3
9HmbnkO7Fe+Lu5AD0s6+E9qayi3wOowunBgUkkFsc8BjiiGrRKcY8Ghc kak=
ddos.rs. 484 IN RRSIG A 5 2 7200 20121125230752
20121026230752 4442 ddos.rs. ViS+qg95DibkkZ5kbL8vCBpRUqI2/M9UwthPVCXl8ciglLftiMC9WUzq
U13FBbri5CKD/YNXqyvxyvmZfkQLDUMffjDB+ZGqBxSpG8j1fDwK6n1
hWbKf7QSe4LuJZyEgXFEkP16CmVyZCTITUh2TNDmRgsoxrvrOqOePWWhp 8+E=
ddos.rs. 4084 IN NS ns.isc.afiliias-nst.info.
ddos.rs. 4084 IN NS ams.sns-pb.ddos.rs.
ddos.rs. 4084 IN NS ord.sns-pb.ddos.rs.
ddos.rs. 4084 IN NS sfba.sns-pb.ddos.rs.

;; AUTHORITY SECTION:
ddos.rs. 4084 IN NS ns.isc.afiliias-nst.info.
ddos.rs. 4084 IN NS ams.sns-pb.ddos.rs.
ddos.rs. 4084 IN NS ord.sns-pb.ddos.rs.
ddos.rs. 4084 IN NS sfba.sns-pb.ddos.rs.

;; ADDITIONAL SECTION:
mx.ams1.ddos.rs. 484 IN A 199.6.1.65
mx.ams1.ddos.rs. 484 IN AAAA 2001:500:60::65
mx.paol.ddos.rs. 484 IN A 149.20.64.53
mx.paol.ddos.rs. 484 IN AAAA 2001:4f8:0:2::2b
_sip._udp.ddos.rs. 4084 IN SRV 0 1 5060 asterisk.ddos.rs.

;; Query time: 176 msec
;; SERVER: 1.2.3.4#53(1.2.3.4)
;; WHEN: Tue Oct 30 01:14:32 2012
;; MSG SIZE rcvd: 3223

```

8. Forenzička analiza HSM uređaja i DNS servera

Kako ni jedan sistem nije apsolutno bezbedan, uključujući i visoko bezbednosno standardizovane HSM uređaje, potrebno je unapred imati planove u slučajevima da se nešto nepredviđeno desi sa hardverom i softverom u lancu potpisivanja i objavljivanja DNS zona. Ovaj rad se neće baviti posebno planovima za oporavak sistema od otkaza, ali ćemo se u ovom poglavlju dotaći plana za forenzičku proveru i otkrivanje eventualnog upada na sistem kao i otkrivanje tragova ukoliko se to desilo. Pre nego što krenemo u analizu metoda forenzičke analize bilo HSM uređaja ili DNS servera poslužićemo se definicijom same forenzike kao nauke: „Kompjuterska ili digitalna forenzika označava primenu naučnih metoda u cilju identifikacije, prikupljanja i analiziranja podataka uz očuvanje integriteta originalnog dokaza i lanca nadležnosti u cilju utvrđivanja potencijalnih digitalnih dokaza“. [7]

Zatim kao sledeći korak ćemo analizirati forenzički HSM uređaje, koji su pravljani sa posebnom namenom da budu teško probojni i samim tim moraju zadovoljavati određene standarde. Samim tim je i lako otkriti ukoliko je došlo do upada u neki od ovih uređaja, ali nije lako pratiti tragove jer je sam uređaj izuzetno komplikovan. Sa druge strane, DNS serveri (pod ovim ćemo podrazumevati upad u operativni sistem i softver a ne u sam hardver, najpre jer hardver najčešće nije specijalizovan a zatim i zbog toga što je većina DNS servera implementirana kao virtuelni server) koje ćemo forenzički analizirati su manje zaštićeni ali znatno lakši za forenzičku analizu i prikupljanje tragova u slučaju upada.

8.2. Forenzička analiza u opštem slučaju

Na jednom od velikih skupova na kojima često govori, Markus Ranum, jedan od stručnjaka prve CERT organizacije u svetu je parafrazirao Bendžamina Frenklina rečima „*An ounce of prevention is worth a pound of detection* – Gram prevencije je vredan kao kilogram detekcije“. U ovoj rečenici je srž obezbeđivanja informacionih sistema. Međutim, pošto je nekada nemoguće sprečiti upad u sistem, detekcija i forenzika su jedini alat kojim možemo pronaći propust, počinioča, učiti na greškama i obezbediti se u budućnosti od sličnih upada.

Prva i možda najbitnija stvar i sam početak forenzičke pripreme pa zatim analize je obezbeđivanje mesta koje se istražuje, bilo da je ono fizičko ili virtuelno. Potrebno je zadržati što je moguće veći nivo očuvanosti samog mesta od bilo kakvih uticaja, da bi analiza bila valjana. Svaki strani, pa i uticaj samog forenzičara na mesto istrage dovodi do potencijalnog ugrožavanja dokaza i validnosti rezultata forenzičke analize. Sledeći koraci mogu zavisiti od cilja forenzičkog istraživanja, od samog mesta, od metoda ili načina rada, ali prvi korak je u svim slučajevima isti i moram biti izveden besprekorno da bi rezultati bili verodostojni i valjani.

8.3. Forenzička analiza HSM uređaja

Kao što je ranije pomenuto u prethodnim poglavljima, HSM uređaji imaju vrlo specifičnu namenu i glavna njihova karakteristika je zaštita podataka koji se na njima nalaze. Za razliku od drugih generičkih uređaja (klasični računari ili diskovi), HSM uređaji su pravljeni prema posebnim standardima. Neki od standarda se odnose na metode čuvanja podataka, šifrovanja podataka koji se nalaze na uređaju, metode pristupa podacima, ali i standarde koji se odnose na detekciju narušavanja sistema ili promene ili gubitka podataka.

Kao i u drugim oblastima tako i u ovoj postoji mnoštvo standarda ali postoje i oni koji su obavezni i bez kojih uređaji nemaju nikakvu upotrebnost vrednost. Najvažniji standard koji se odnosi na ovu oblast je FIPS 140-2 (Federal Information Processing Standard). Ova grupa standarda i pravila podeljena je na više nivoa se odnosi na zaštitu podataka generalno bez obzira da li tim podacima rukuju ljudi, računari ili specifični uređaji.

FIPS 140-2 standard je podeljen sa sledeća 4 nivoa:

Nivo 1 – Najniži nivo sigurnosti po ovom standardu. Obavezno je korišćenje barem jednog algoritma ili metoda za zaštitu koji je odobren od ove organizacije. Ne postoje specifični mehanizmi za fizičku zaštitu ovakvih uređaja. Primer uređaja ovog nivoa su obični desktop ili laptop računari.

Nivo 2 – Na ovom nivou zahtevaju se mehanizmi koji obezbeđuju fizičku zaštitu uređaja kao i načini i mehanizmi da se utvrdi ukoliko je došlo do fizičkog upada u uređaj radi krađe podataka. Ove metode mogu biti raznovrsne, od materijala na kojima se vidi pokušaj upada u uređaj do pečata ili prepreka koje je potrebno slomiti ili oštetiti da bi se došlo do podataka. Ovo znatno pomaže forenzičku istragu jer su dokazi najčešće veoma evidentni.

Nivo 3 – Ovaj nivo podrazumeva mehanizme sa prethodnog nivoa a pored toga dodati su i softverski mehanizmi koji sprečavaju napadača da dođe do kritičnih sigurnosnih parametara (to mogu biti šifre, ključevi ili slični parametri kojima se postiže zaštita podataka). Takođe, na ovom nivou se zahteva pojačavanje fizičke zaštite uređaja ne samo preprekama na kojima se prepoznaje upad u sistem već i materijalima koji štite uređaj da se naruši njegov fizički integritet (najčešće su u pitanju kućišta od izuzetno izdržljivih materijala).

Nivo 4 – Ovo je najviši nivo standarda zaštite koji neki uređaj može da dobije. Podrazumeva fizičku i softversku zaštitu sa apsolutno najvećom verovatnoćom detekcije upada, pored toga podrazumeva totalnu fizičku zaštitu uređaja ne samo pasivnim već i aktivnim metodama zaštite. Ovi uređaji se često koriste u okruženjima gde nije moguće pružiti neku dodatnu zaštitu kao na primer u zatvorenom računskom centru, pa se zbog toga zahteva ekstremno visok nivo zaštite kao i isto takav nivo prepoznavanja da se desio pokušaj ili sam upad u sistem.

Kada se ovako posmatra forenzička analiza HSM uređaja, deluje vrlo lako prepoznati narušavanje bezbednosti uređaja sa višim nivoima FIPS standarda. Međutim, da bi ste forenzičku analizu izveli u potpunosti uspešno i osim konstatacije da se upad ili pokušaj desio, potrebno je detaljno poznavanje načina rada samog uređaja da bi bilo moguće da se pokupe tragovi koji vode do počinioca.

Kako ovakvih uređaja nema u onom broju u kom ima klasičnih servera i računara, i kako je cena ovih uređaja, pogotovo uređaja viših nivoa FIPS standarda jako visoka, tako su i brojevi pokušaja na ove uređaje znatno manji od drugih, ali i znatno sofisticiraniji. Naime, ako je uobičajeno da i manje vešti počinioci često pokušavaju upade na računare, servere ili veb prezentacije širom sveta, jer je broj uređaja velik, alati za napade ili krađu podataka su rasprostranjeni, tako sa druge strane napadača na ovakve HSM uređaje ima znatno manje, ali su jako vešti, veoma sofisticirani i najčešće sami prave svoje alate za napad ili krađu podataka. Znajući ovo, za uspešnu forenzičku analizu upada na neki ovakva uređaj potrebno je angažovati specifične stručnjake čija je specijalizacija vrlo uska na taj uređaj ili taj tip uređaja da bi smo došli do valjanih podataka. Često ni stručnjaci iz slične oblasti nisu dovoljno obučeni da pronađu sve tragove u uređaju kojim se pre toga nisu bavili, a time je i forenzička istraga najčešće upropašćena. Istragu takođe može da uspori i oteža to što proizvođači ovakve specifične opreme kriju podatke o arhitekturi uređaja i softvera zbog sopstvene zaštite pa je moguće tokom forenzičke analize upasti u zamku koju je postavio sam proizvođač uređaja i izgubiti željene tragove i podatke.

8.4. Forenzička analiza DNS servera

Za razliku od HSM uređaja DNS serveri se mogu nazvati obične serverske mašine, sa relativno uobičajenim operativnim sistemima i sa ne-specifičnim softverom. Najveći broj DNS servera na internetu, bez obzira da li su u pitanju autoritativni serveri ili rekurzivni serveri su u suštini na Linux operativnim sistemima, dok je po istraživanjima najveći broj unutrašnjih DNS servera u velikim kompanijama na Microsoft operativnom sistemu. Imajući to u vidu, u slučaju upada u sistem ili bilo kakvog kriminalnog pokušaja krađe ili promene podataka, forenzička istraga nakon obezbeđivanja mesta na kome će se istraga vršiti analiza samog operativnog sistema da bi se utvrdilo odakle je upad došao. Bez obzira na softver na samom DNS serveru sam operativni sistem će u svojim log fajlovima imati praktično sve podatke koji će potencijalno dati sliku o inkriminišućem događaju. Na osnovu ovih podataka možemo pokrenuti istragu odakle je počinilac došao, preko kojih ulaza ili portova je upao na sistem, da li je koristio neku posebnu slabost sistema ili je možda do podataka i kredencijala za prijavljivanje na sistem došao putem socijalnog inženjeringa. U ovim log fajlovima se mogu naći IPv4 ili IPv6 adrese prema kojima može da se vrši dalja istraga.

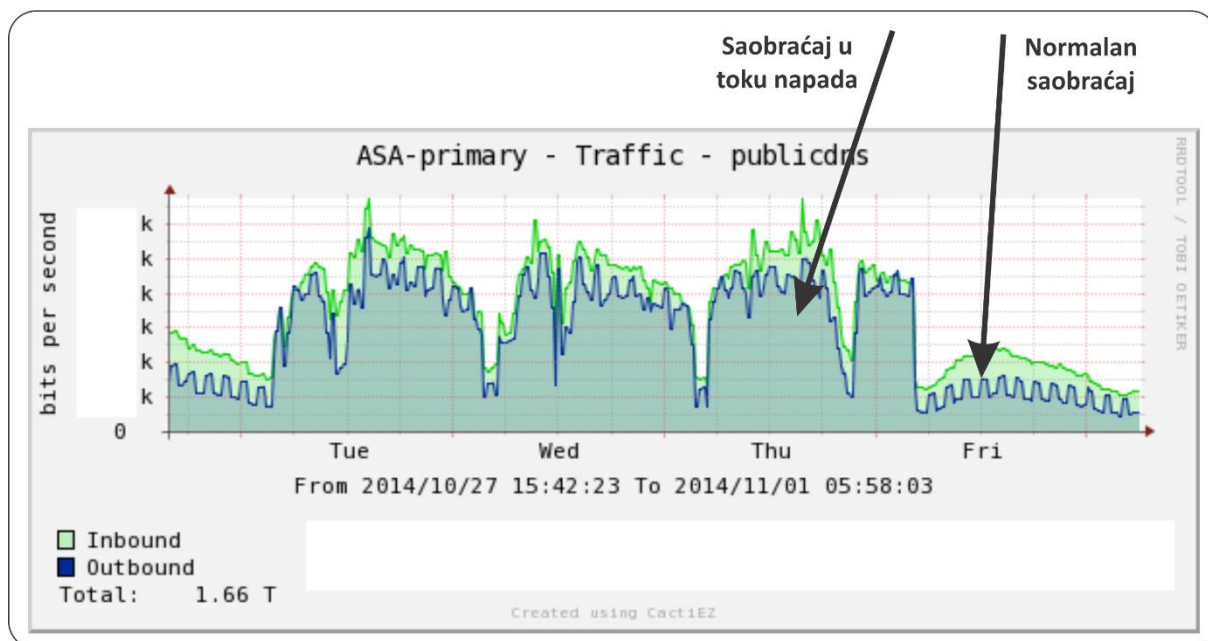
Uobičajeno je da napadači koriste lažne adrese da bi prikrili tragove ili da bi se sistemu prikazali kao da su iz njegovog bliskog okruženja, te je za dalju istragu ka spolja potrebno analizirati log

fajlove sa mrežnih uređaja koji su propustili napadača ka serveru. Do ovih log fajlova je moguće doći ukoliko su mrežni uređaji pod upravljanjem onih koji upravljaju i DNS serverom koji je napadnut, a u suprotnom svaki sledeći korak na mreži i svaki sledeći log fajl uređaja je sve teže dobiti jer ih oni koji upravljaju štite da bi zaštitili informacije o svom sistemu. Do ovakvih podataka je onda moguće doći jedino zakonskim putem uz pomoć i odobrenje organa unutrašnjih poslova ili putem sudskih odluka.

Analiza softvera za DNS servis nam može pružiti informaciju šta je bio cilj onoga koji je napao sistem. Na osnovu toga koje je zapise menjao, brisao ili dodavao može se izvući zaključak kome je i na koji način hteo da naudi ili kojim putem je hteo da nastavi svoj dalji upad u sistem.

Slično kao i u slučaju HMS uređaja potrebno je da se ovim analizama bave stručnjaci specijalizovani za različite oblasti, pa tako mrežni administratori (uobičajeno sa CISCO sertifikatima) bi se bavili analizom saobraćaja na mreži i putevima kojima je napadač došao do servera, Linux ili Microsoft administratori (uobičajeno sa RHCSA ili LPI sertifikatima za Linux operativne sisteme i MCSE i MCSA sertifikatima za Windows operativne sisteme) se bave analizom puteva kojim je napadač ušao u sistem, analizom slabosti sistema koje su dovele do upada ili lozinki koje je napadač iskoristio, a DNS administratori bi dali sliku šta je bio cilj napada ili ukoliko je DNS server oružje napada koji je dalji korak napadača.

Na slikama ispod se može videti najpre izgled saobraćaja pri normalnim uslovima i u toku napada na DNS server, zatim dve vrste logova (manje i više detaljni) koji se prikupljaju da se ustanovi odakle dolaze napadi na sam server.



Slika 17. – Prikaz internet saobraćaja preuzet sa mrežnih uređaja tokom DDoS napada na DNS server

ZenossCORE

DASHBOARD

EVENTS

INFRASTRUCTURE

REPORTS

ADVANCED

Event Console

History

Event Classes

Event Manager

Select

Export

Configure

Last updated at 10:51:20PM

Refresh

Actions

Commands

Status	Severity	Device	Component	Event Class	Summary	First Seen	Last Seen	Count
...	...							
		ASA	ASA	/Unknown	[Scanning] drop rate-1 exceeded. Current burst rate ...	10-31 05:00:26	11-01 22:50:55	1187
		ASA		/Unknown	snmp trap 1.3.6.1.4.1.9.9.41.2.0.1	08-15 11:02:39	11-01 22:50:55	780037
		ASA	ASA	/Unknown	[Scanning] drop rate-1 exceeded. Current burst rate ...	10-31 05:00:46	11-01 22:50:35	704
		ASA	snmp	/Status/Snmp	SNMP agent down	08-15 11:04:53	11-01 22:50:07	22618
		ASA	ASA	/Unknown	[Scanning] drop rate-1 exceeded. Current burst rate ...	11-01 22:50:05	11-01 22:50:05	1
		ASA		/Unknown	snmp trap 1.3.6.1.6.3.1.1.5.5	08-15 11:03:30	11-01 22:50:01	452674
		ASA	ASA	/Unknown	[Scanning] drop rate-2 exceeded. Current burst rate ...	10-31 05:13:29	11-01 22:49:15	607
		localhost	snmp	/Status/Snmp	SNMP agent down	09-25 22:58:44	11-01 22:48:52	10667
		ASA	ASA	/Unknown	Group = mgmtaccess, Username =	11-01 22:48:50	11-01 22:48:50	1
		ASA	ASA	/Unknown	Group = mgmtaccess, Username =	11-01 20:00:45	11-01 22:48:50	2
		ASA	ASA	/Unknown	Group = mgmtaccess, Username =	11-01 20:00:45	11-01 22:48:50	2
		ASA	ASA	/Unknown	Group = mgmtaccess, Username =	11-01 20:00:45	11-01 22:48:50	2
		ASA	ASA	/Unknown	IPAA: DHCP configured, no viable servers found for ...	11-01 20:00:45	11-01 22:48:49	2
		ASA	ASA	/Unknown	Group = mgmtaccess, Username =	11-01 20:00:45	11-01 22:48:49	2
		ASA	ASA	/Unknown	AAA transaction status ACCEPT : user =	11-01 20:00:45	11-01 22:48:49	2
		ASA	ASA	/Unknown	AAA retrieved default group policy (mgmtaccess) for...	11-01 20:00:45	11-01 22:48:49	2
		ASA	ASA	/Unknown	AAA user authentication Successful : local database...	11-01 20:00:45	11-01 22:48:49	2
		ASA	ASA	/Unknown	[Scanning] drop rate-1 exceeded. Current burst rate ...	11-01 18:15:14	11-01 22:46:54	5
		ASA	ASA	/Unknown	ASA-SSM-20 Module in slot 1, application up "IPS", v...	10-21 17:37:26	11-01 22:46:32	272
		ASA	ASA	/Unknown	ASA-SSM-20 Module in slot 1, application reloading "...	10-21 17:37:26	11-01 22:46:32	272
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from 38.122.147.121 to ...	11-01 22:39:49	11-01 22:39:49	1
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:39:01	11-01 22:39:01	2
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:39:01	11-01 22:39:01	1
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:39:01	11-01 22:39:01	1
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:39:00	11-01 22:39:00	1
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:39:00	11-01 22:39:00	1
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:38:51	11-01 22:38:51	1
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:38:51	11-01 22:38:51	1
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:38:51	11-01 22:38:51	1
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:38:50	11-01 22:38:50	1
		ASA	ASA	/Unknown	IDS:2005 ICMP time exceeded from	11-01 22:38:45	11-01 22:38:45	1

Slika 18. – Prikaz sadržaja log fajla sa mrežnog uređaja Cisco ASA (manje detaljan prikaz)

[Scanning] drop rate-1 exceeded. Current burst rate is 2 per second, max configured rate is 10; Current average rate is 5 per s

Device: ASA

Component: ASA

Event Class: /Unknown

Status: 0

Start Time: 2014/10/31 05:00:26.000

Stop Time: 2014/11/01 22:50:15.000

Count: 1186

Message: [Scanning] drop rate-1 exceeded. Current burst rate is 2 per second, max configured rate is 10; Current average rate is 5 per second, max configured rate is 5; Cumulative total count is 3242

Systems:

Groups:

Location:

Device Class: /Network/Router/Firewall

Production State: Production

Device Priority: Normal

[Hide details](#)

Slika 19. – Prikaz sadržaja log fajla sa mrežnog uređaja Cisco ASA (više detaljan prikaz)

Na osnovu ovakvih podataka iz log fajlova i sa grafikona saobraćaja, moguće je praviti analizu prilaza napadača DNS serveru. Neki od podataka sa slika 21. 22. i 23 su namerno obrisani zbog poverljivosti podataka na sistemu sa koga potiču ovi log fajlovi.

Packet Log Examples

Date and Time	Type	Prot Dir Query, Reply IP	R/Q	Flag	Record Domain
4/15/2014 3:16:00 PM	0710 PACKET	0000000028FB94C0 UDP Rcv 69.160.33.71	8857 R Q [0080	NOERROR]	A .ns1.offeringsmislead.com.
4/21/2014 7:18:36 AM	0714 PACKET	000000002CC599A0 UDP Snd 8.8.8.8	3434 Q [1001 D	NOERROR]	A .cdn-controltag.krxd.net.

Information: DNS Update Message Flags

- 0 (NOERROR) No error; successful update.
- 1 (FORMERR) Format error; DNS server did not understand the update request.
- 0x2 (SERVFAIL) DNS server encountered an internal error, such as a forwarding timeout
- 0x3 (NXDOMAIN) A name that should exist does not exist.
- 5. 0x4 (NOTIMP) DNS server does not support the specified Operation code.
- 0x5 (REFUSED) DNS server refuses to perform the update because
- 0x6 (YXDOMAIN) A name that should not exist does exist.
- 0x7 (YXRRSET) A resource record set that should not exist does exist.
- 0x8 (NXRRSET) A resource record set that should exist does not exist.
- 10. 0x9 (NOTAUTH) DNS server is not authoritative for the zone named in the Zone section.
- 0xA (NOTZONE) A name used in the Prerequisite or Update sections is not within the zone specified by the Zone section

Information: Record Type

- A 0x01 Host (A) record For mapping a DNS domain name to an IP address used by a computer.
- NS 0x02 Name server (NS) record For mapping a DNS domain name to the name of a computer that operates the network name service.
- CNAME 0x05 Alias (CNAME) record For mapping an alias DNS domain name to another primary or canonical name.
- PTR 0x0C (12) Reverse-lookup (PTR) record For mapping a reverse DNS domain name based on the IP address of a computer that points to the forward DNS domain name of that computer.
- 5. MX 0x0F (15) Mail exchange (MX) record For mapping a DNS domain name to the name of a computer that exchanges or forwards mail.
- SRV 0x21 (33) Service (SRV) record For mapping a DNS domain name to a specified list of DNS host computers that offer a specific type of service, such as Active Directory domain controllers.
- IXFR 0xFB (251) Incremental zone transfer (IXFR) record
- AXFR 0xFC (252) Standard zone transfer (AXFR) record
- All 0xFF (255) All records Domain
- 10.

Slika 20. – Prikaz sadržaja log fajla sa DNS servera

Na slici 24. je prikazan izgled različitih log fajlova sa jednog DNS servera koji se nalazi na CentOS Linux platformi koji prikazuje normalan rad jednog DNS servera.

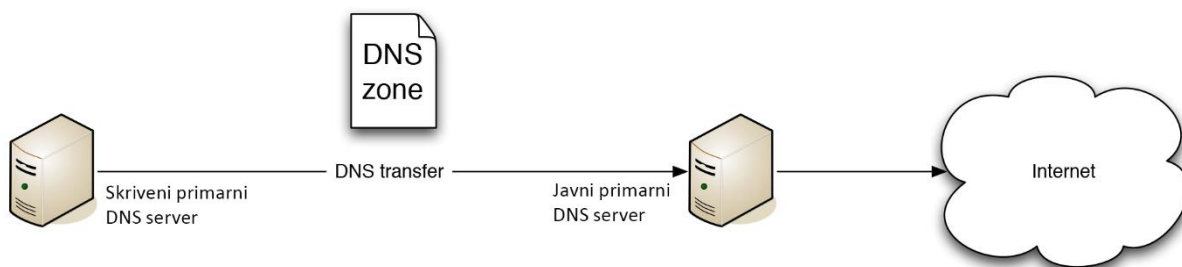
9. Studija slučaja uvođenja DNSSEC

U ovom poglavlju biće prikazana jedna studija slučaja uvođenja DNSSEC dodataka za zaštitu DNS servera u organizaciju SurfNET, i jedan sažeti prikaz vremenskog okvira uvođenja DNSSEC dodataka u nemački nacionalni registar DeNIC (u slučaju DeNIC je moguće prikazati samo vremenske okvire plana uvođenja jer su podaci o detaljima uvođenja poverljivi i nisu dostupni široj javnosti).

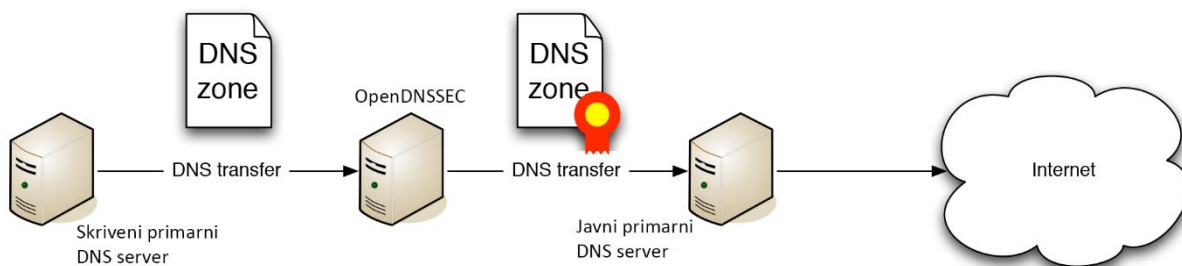
9.1. Studija slučaja SurfNET i DNSSEC

SurfNET je organizacija osnovana u Holandiji i čiji je cilj pružanje informacionih i komunikacionih usluga u holandskim akademskim, obrazovnim i naučnim institucijama. Pored toga SurfNET radi i kao registar naziva domena za sledeće domene: .nl, .com, .net, .org, .info i .eu. Cilj ovog projekta koji je idejno pokrenut krajem 2009. godine je bio da se obezbedi DNSSEC funkcionalnost za portal SURFdomeinen, čija je osnovna funkcionalnost registrovanje gore pomenutih naziva domena a koji se nalaze na serverima SurfNET organizacije. Time bi se DNSSEC uveo najpre u SURFdomeinen a zatim i u kompletan set servera SurfNET. Sam projekat je počeo 2010. godine a njegov završetak je planiran za treći ili četvrti kvartal iste godine.

Prvi koraci u realizaciji ovog projekta su bili anketiranje trenutnih i potencijalnih korisnika usluga o zainteresovanosti i upoznatosti sa DNSSEC tehnologijom, a zatim nakon pozitivnih rezultata ankete krenulo se najpre sa analizom postojećeg stanja pa zatim i planiranjem uvođenja DNSSEC. Na slikama 25. i 26. se može videti uprošćen prikaz prenošenja zone u situaciji pre uvođenja DNSSEC i prenošenja i potpisivanja zone u situaciji nakon uvođenja DNSSEC. Na obe slike može da se primeti da se zone generišu na skrivenim DNS serverima da bi se zaštitio njihov integritet a da se nakon generisanja a kasnije generisanja i potpisivanja zone ona prenosi na javni server gde mu korisnici i rekurzivni DNS serveri mogu pristupati i praviti upite ka njemu.

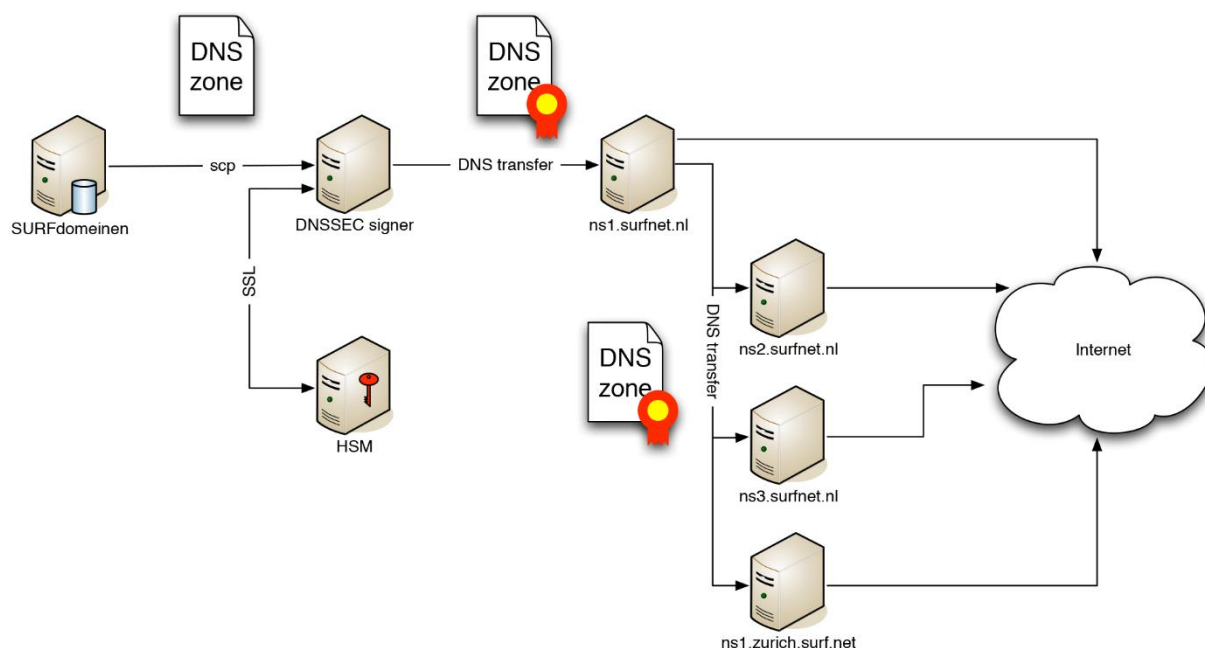


Slika 21. – Uprošćen prikaz prenosa generisane zone sa skrivenog na javni server (preuzeto sa <http://surfnet.nl>)



Slika 22. – Uprošćen prikaz prenosa generisane zone sa skrivenog na javni server i njeno potpisivanje sa OpenDNSSEC u toku prenosa (preuzeto sa <http://surfnet.nl>)

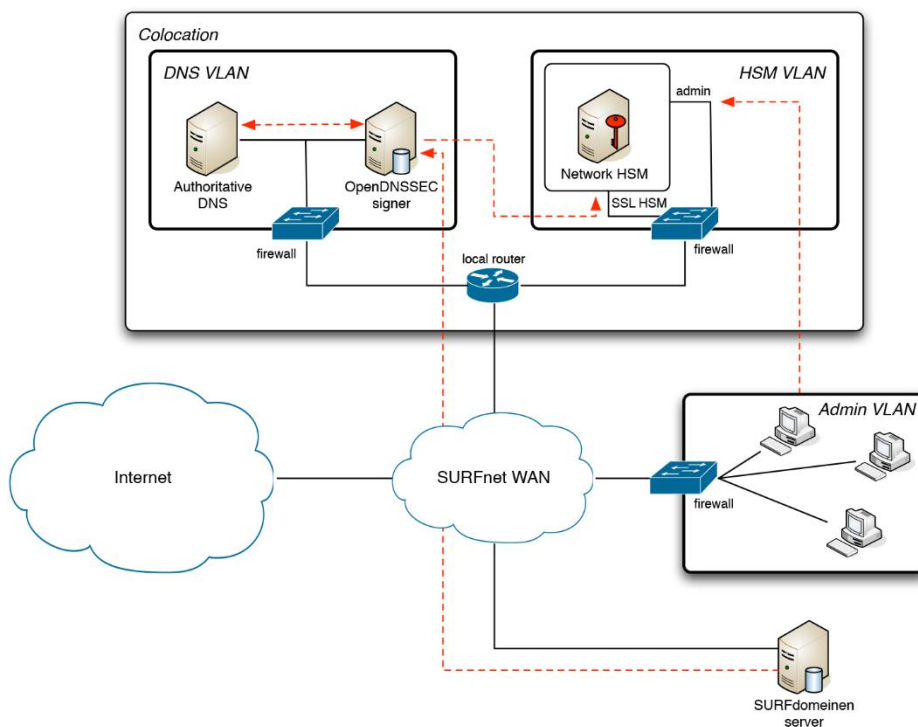
Nakon uprošćenih grubih planova kao na prethodnim slikama pristupilo se detaljnijem planiranju same infrastrukture, koje je u ovom slučaju podrazumevalo i planiranje mesta i načina za čuvanje ključeva kojima se zona i sami ključevi potpisuju. Na slici 27. se vidi sistem znatno realnije prikazan, sa dodatim HSM uređajem za čuvanje ključeva. Koji HSM uređaj je iskorišćen za čuvanje ključeva u ovom slučaju nije bilo moguće saznati jer to spada u domen poslovne tajne organizacije SurfNET.



Slika 23. – Širi prikaz sistema za prenos i potpisivanje DNS zone u organizaciji SurfNET (preuzeto sa <http://surfnet.nl>)

Kao što se na slici 27. može primetiti postoji redundantnost na nivou javnih DNS servera (na slici su prikazana 3 javna DNS servera), ali pored toga postoji i unutrašnja redundantnost koja podrazumeva da je ceo sistem dupliran u dva identična data centra, te u slučaju otkaza nekog od uređaja ili servera, pa i celog jednog data centra, drugi data centar u potpunosti može preuzeti njegovu ulogu i nastaviti nesmetano rad do potpunog oporavka kompletnog sistema. Ovakav način rada je izveden pomoću „Site Recovery Manager“ opcija koje pruža VM Ware sistem za upravljanje virtuelnim mašinama.

Na prethodnim slikama šematski je prikazana postavka servera u ovoj studiji slučaja, međutim na sledećoj slici (slika 28.) moguće je videti konkretno mrežno rešenje i način na koji su serveri i administrativni računari smešteni u različite virtualne mreže pomoću mrežnih uređaja proizvođača Cisco. Vlan-ovima se opravljia ruterima kao prvim tačkama čvorišta a svaki Vlan je dodatno zaštićen posebnim firewall uređajem za kontrolu saobraćaja. Grupa u kojoj se nalaze računari kojim administratori pristupaju serverima se ne nalazi u data centrima već oni imaju pristup kroz WAN SurfNET-a ili preko interneta korišćenjem VPN tunela.

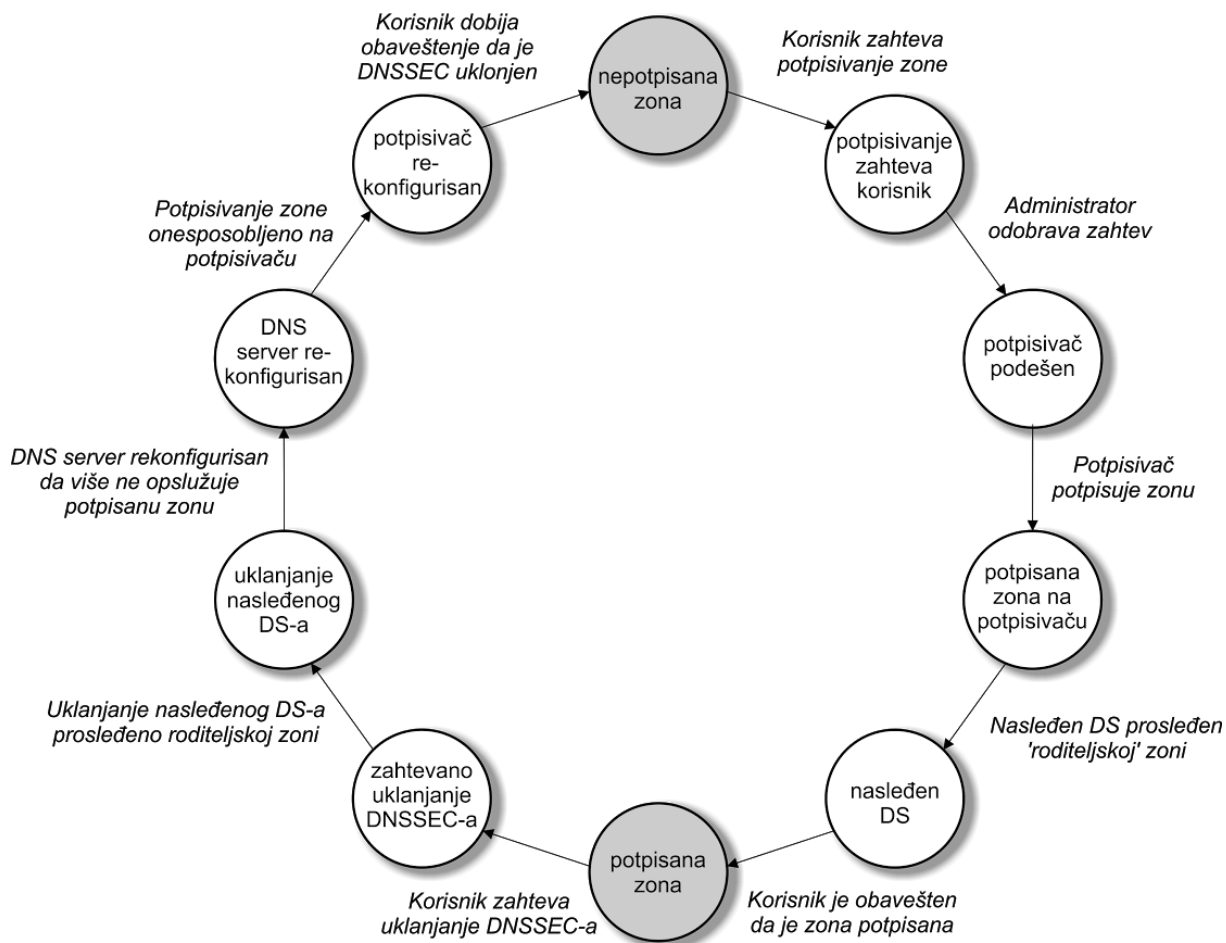


Slika 24. – Prikaz mrežnih komponenti i Vlan grupa (preuzeto sa <http://surfnet.nl>)

Pored administratora u ovom sistemu važnu ulogu imaju još dve vrste zaposlenih. To su najpre analitičari bezbednosti koji nezavisno od administratora i njihovog nadgledanja funkcionalnosti sistema na svoj način nadgledaju i analiziraju saobraćaj i potencijalne bezbednosne propuste. Treća grupa su backup administratori, čiji je zadatak da prave rezervne kopije kompletnog sistema ali i specifične kopije delova sistema i da ih nakon kreiranja testiraju da li su ispravni i konzistentni.

Takođe, povremeno backup administratori izvode probe povratka celog sistema iz rezervnih kopija da bi se proverila uspešnost celog sistema. Česta je greška verovanje da je dovoljno napraviti rezervne kopije i da je time sistem bezbedan. Bez analize svake rezervne kopije da li je sadržala apsolutno sve što je potrebno, i povremenog oporavka sistema iz takvih kopija (ovo se izvodi najčešće na test serverima da se ne remeti rad produkcionih servera) ne možemo biti sigurni da ćemo moći da oporavimo sistem posle otkaza.

Tokom razvoja projekata jedan od takođe jako bitnih delova je bio i pravljenje ciklusa po kome će korisnici moći da traže da njihov naziv domena u zoni bude potpisan ili da traže da se potpis sa njihovog naziva domena ukloni ukoliko ga više ne žele. Ciklus se može videti na slici 29.



Slika 25. – Ciklus koraka potrebnih za potpisivanje naziva domena ili za uklanjanje potpisa sa naziva domena u zoni (preuzeto sa <http://surfnet.nl>)

Na korisničkom interfejsu izgled potpisanog naziva domena DNSSEC ekstenzijom i nepotpisanog naziva domena izgleda kao na slici 30.

Zones				Zone toevoegen +
vorige pagina		volgende pagina		
Zone	Type	Gebruiker	Reseller	
dnshealth.info.	Managed	SURFnet B.V.	SURFnet B.V.	✖
dnshealth.org.	Managed	SURFnet B.V.	SURFnet B.V.	✖
vorige pagina		volgende pagina		

Slika 30. – Prikaz potpisanog domena na korisničkom interfejsu korisnika SurfNET (preuzeto sa <http://surfnet.nl>)

Projekat uvođenja DNSSEC u SurfNET je izveden između ostalog uz pomoć i asistenciju organizacije SIDN (holandski nacionalni internet domen registar) kao i organizacije NINetLabs koja je osnovana od strane internet zajednice i stručnjaka u Holandiji. Sledeći koraci su unapređivanje sistema, automatizacija, kao i poboljšavanje monitoringa i nadzora samog sistema. [20]

9.2. Vremenski plan uvođenja DNSSEC u DeNIC

Drugi deo u poglavlju studija slučaja je prikaz vremenskih okvira i događaja prilikom uvođenja DNSSEC u DeNIC (nemački nacionalni internet domen registar). Kao veliki registar, prilično zatvorenog tipa, nije bilo moguće doći do podataka o šemama sistema i načinima funkcionisanja DNSSEC sistema, ali je bilo moguće doći do podatka kako je išao vremenski tok implementacije DNSSEC jer to nije predstavljalo korporativnu tajnu.

Iako možda nema dovoljno tehničkih podataka, ali smo mišljenja da je i sam vremenski okvir značajna informacija koja bi mogla da pomogne pri planiranju budućih implementacija, kako kroz korišćenje koraka koje su oni pravila tako i kroz realno sagledavanje vremena potrebnog za određene korake u ovom procesu.

Ceo proces je počeo 24. aprila 2009. godine sastankom organizacija koje sarađuju sa DeNIC a osnovani su od strane nemačke Vlade (BSI, eco). Naredni korak je bio 2. jula iste godine koji je podrazumevao sastanke sa internet provajderima, ovlašćenim registrima i drugim zainteresovanim stranama čija je tema bila podizanje svesti o potrebi DNSSEC i bezbednijem internetu u Nemačkoj. Nakon toga narednih pet meseci je urađen upitnik o uređajima koje korisnici koriste za pristup internetu, da bi se ustanovio stepen uređaja koji su DNSSEC kompatibilni i koji ne bi predstavljali tehničku prepreku u uvođenju. Paralelno sa upitnikom rađena je i analiza softvera u istom vremenskom periodu, a njen cilj je bio da se ustanovi stanje softvera potrebnog za podršku DNSSEC kao i prevođenje već postojećeg softvera na nemački jezik.

Krajem 2009. godine podignuto je prvo test okruženje pripremljeno za prvu instalaciju DNSSEC okruženja, a mesec dana kasnije je u to okruženje instaliran DNSSEC sistem i time je zaokruženo test okruženje u kome je DNSSEC dalje razvijan za potrebe DeNIC. Nakon toga je podnet izveštaj internet zajednici koja je uključena u ovaj proces i pružena je mogućnost onima koji se još nisu pridružili da se uključe u rad. U sledećim koracima test okruženje je proširivano a na narednim sastancima su strane uključene u razvoj davale svoje izveštaje o nivou koje su postigli u implementaciji DNSSEC u svoja mikro okruženja.

Krajem 2010. godine procenjeno je da se došlo do optimalne konfiguracije DNSSEC implementacije i nakon toga je napravljen finalni izveštaj koji je podnet svim zainteresovanim i uključenim stranama u ovom procesu. Taj četvrti kvartal 2010. godine se može smatrati

početkom rada DNSSEC u DeNIC. Nakon toga su usledili sastanci koji bi uključili nove organizacije koje žele da postanu deo lanca poverenja od najviše tačke (root serveri organizacije ICANN) pa preko DeNIC i niže do veb i internet provajdera. Ovde nije kraj procesa jer je sistem potrebno konstantno usavršavati. [4]

Na ovom vremenskom planu možemo da vidimo da je čak i organizacijama kao DeNIC koje imaju znatna finansijska sredstva (DeNIC u ovom trenutku ima oko 17 miliona domena, iz čega može da se izvuče zaključak da su godišnji prihodi veći od 150 miliona evra) i veliki broj ljudi u informatičkoj delatnosti, potrebno skoro dve godine za implementaciju DNSSEC u svoj sistem. Neke organizacije su možda uspele da za kraće vreme uvedu DNSSEC ali je ovo primer uključenja cele zajednice u taj proces.

10. Zaključak

Tokom pisanja ovog rada i istraživanja koje ga je pratilo, došlo se do niza zaključaka koji su u nekim trenucima delovali i kao kontradiktorni. Prvo mora se razumeti da DNSSEC rešava samo jedan od problema koji je posledica dugogodišnjeg nerazvijanja DNS protokola (problem upisivanja u DNS keš), što pred nas stavlja pitanje kada i u kojoj meri je taj problem potrebno rešavati.

Problem koji stvara Kaminski propust nije mali, može da uzrokuje lažiranje veb prezentacija i samim tim kao što je pominjano u poglavlju 3.1. da omogući napadačima da prevare potencijalne korisnike da poveruju da se nalaze na sajtu neke banke ili da skinu softver sa sajta za koji veruju da je pouzdan a da on to nije. Međutim, postoji ogroman broj veb sajtova i drugih servisa, na koje ovaj propust nema nikakav uticaj, niti je njihov sadržaj tog nivoa da bi se napadači angažovali da ga krivotvore i nateraju korisnike na grešku. Ovo nas najpre navodi na zaključak da je u velikom broju slučajeva uvođenje DNSSEC veliko trošenje resursa, i to na više nivoa; trošenje finansijskih, ljudskih i informatičkih resursa, a da je dobit iz toga gotovo neprimetna ili da je praktično nema. Iz tih razloga još uvek postoji relativno veliki broj kako nacionalnih tako i novih TLD registara koji nisu uveli DNSSEC u svoj sistem.

Nakon sagledavanja ove situacije autor je došao na ideju koja bi DNSSEC implementaciju učinila znatno isplativijom i iskorišćenijom. Naime, na primeru .com domena u koji je na root nivou uveden DNSSEC ali je broj potpisanih naziva domena zanemarljivo mali, možemo da shvatimo koliko je DNSSEC iskorišćen. Ista ili slična situacija je i u drugim slučajevima te se može izvući zaključak da je iskorišćenost potencijala DNSSEC zanemarljivo mala. Ideja koja bi se mogla iskoristiti i koja bi podigla nivo iskorišćenosti DNSSEC je organizacionog tipa.

Ukoliko bi na primer sve banke uzele .bank domen (primer srbija.nekabanka.bank) i sam root domena .bank bio potpisan, nivo iskorišćenja bi bio 100% ili jako blizu toga jer postoji potreba da veb sajtovi banaka i e-banking sistemi budu DNSSEC potpisani. Slično bi se moglo uraditi sa novim TLD domenom .soft za softverske kompanije. Time ne bi postojala potreba da generički domeni uvode DNSSEC i prave ogromne troškove već bi se DNSSEC uvodio samo u specifične domene kod kojih je velika verovatnoća da će napadači pokušati da falsifikuju DNS zapise u kešu i navedu korisnike na pogrešan veb sajt.

Nažalost, autor veruje da ova ideja nije izvodljiva zbog nekoliko razloga. Prva je to da se moraju poštovati slobode da svaki registar TLD domena može da bira da li želi da uvede DNSSEC bez obzira na to koliko mu je ta investicija isplativa, drugo, neke su države u svojim zakonima uvele članove koje insistiraju da njihovi nacionalni registri moraju uvesti DNSSEC, treće je mogućnost korišćenja DNSSEC u promotivne svrhe (registri mogu promovisati svoj biznis time što pružaju i ovu dodatnu uslugu) a četvrto je takođe sloboda odabira korisnika da biraju domen koji žele da koriste, te nije moguće uslovljavati da koriste određenu grupu domena kao na

primer .bank (neke organizacije biraju nacionalne domene radi promovisanja svog biznisa u određenoj državi, jer pretraživači a pogotovo Google favorizuju nacionalne domene ukoliko se pretraga vrši na teritoriji te države). Uvođenje ovakve ideje se može uporediti sa dogovorom da se sve države odreknu nuklearnog naoružanja; opšte je poznato da bi to smanjilo napetosti u svetu ali ne postoji ni jedna država koja bi ga se tek tako dobrovoljno odrekla pa čak ni u slučaju da se neki drugi odreknu.

Ukoliko pretpostavimo da je DNSSEC moguće uvesti na celom internetu, to može vući neke druge posledice kao na primer povećanje internet saobraćaja na svetskom nivou (potpisane DNS zone su i do tri puta veće od nepotpisanih) kao i opterećenje DNS servera širom interneta. Pitanje je koliko je sadašnja svetska internet infrastruktura sposobna da podnese ovakav porast saobraćaja, pogotovo kad se uzme u obzir da postoje skokovi i drugih vrsta saobraćaja koji drastično opterećuju linkove (ogroman skok video i live streaming saobraćaja).

Mišljenja smo da je možda bolji put bio unapređivanje samog DNS protokola koji nije menjan od nastanka prve internet mreže, za šta neki smatraju da je kasno i da bi to moralo da promeni kompletan način funkcionisanja interneta. Kao što je došao trenutak kada je IPv4 protokol zamenjen IPv6 protokolom jer se došlo do tačke bez povratka kada više nije bilo IPv4 adresa, tako će se možda u skoroj budućnosti desiti još neki propust u DNS protokolu kada više neće biti moguće novo dodavanje ekstenzija koje štite korisnike i moraće da se pristupi otkrivanju i primenjivanju nekog novog načina da se DNS zameni.

Literatura

- [1] **Aitchison, R.**, *Pro DNS and BIND 10*, Apress 2012.
- [2] **Bauer, M.** *DNS Cache Poisoning*, Linux Journal Maj 2011.
- [3] **Crocker, S.**, *DNSSEC History, Status, Future*, Internet Dagarna Conference 2008.
- [4] DeNIC Roadmap, <http://www.denic.de/en/domains/dnssec/dnssec-testbed/roadmap.html?cHash=3486f26050ac1dc3cbe6f5842dc70494>
- [5] *Deploying DNSSEC Using BIND 9.7*, Nanog Presentation, Internet Systems Consortium, 2010.
- [6] *Deploying DNSSEC: what, how and where*, Afnic, 2014.
- [7] *Digitalna forenzika i alati*, Wikipedia Srbija, http://sr.wikipedia.org/wiki/digitalna_forenzika_i_alati
- [8] DNSSEC Deployment Initiative <https://www.dnssec-deployment.org/>
- [9] *Good practices guide for deploying DNSSEC*, Enisa, 2010.
- [10] Google Maps <https://maps.google.com/maps/ms?msa=0&msid=103993808347197645891.00043a30b2657ea61ea33&dg=feature>
- [11] http://www.circleid.com/posts/20130717_dns_dnssec_and_googles_public_dns_service/
- [12] ICANN (The Internet Corporation for Assigned Names and Numbers) <http://www.icann.org/en/news/in-focus/dnssec/deployment>
- [13] **Ivarsson J., Nilsson A.**, *A Review of Hardware Security Modules*, Certezza AB, 2010.
- [14] **Kolkman O.**, *DNSSEC HOWTO - a tutorial in disguise*, NLNet Labs, 2009.
- [15] Kurose, J. F., Ross, K. W., **Computer Networking Sixth Ed**, Pearson Education, Inc. 2013.
- [16] *Overview of DNSSEC deployment worldwide*, EURid Report, 2013.
- [17] RIPE (*Réseaux IP Européens Network Coordination Centre*) <https://labs.ripe.net/Members/gih/counting-dnssec>
- [18] **Sharma T.**, *DNS and DNSSEC Problems and Solutions*, Wegilant Net Solutions Pvt. Ltd., 2010.
- [19] *The Costs of DNSSEC Deployment*, Enisa, 2012.
- [20] **van Rijswijk R.**, *DNSSEC in SURFdomeinen*, Final report on the results of the project, 2011.
- [21] Weaver, R., Weaver, D., Farwood, D., **Guide to Network Defense and Countermeasures, Course Technology**, Cengage Learning, 2014.
- [22] Wright, C. S., **Current Issues in DNS**, SANS Institute, 2008.

Indeks pojmova

BIND – Softverska aplikacija koja obezbeđuje DNS servis. Jedan od najčešće korišćenih DNS servera na linux platformi. Pored njega poznati su takođe Power DNS, Knot DNS, Yadifa kao i Microsoft DNS.

ccTLD – (Country Code Top Level Domain) domeni najvišeg reda dodeljeni na upravljanje državama koje predstavljaju na internetu. Primeri su .rs .uk .hr .se i slični. Neke od država su uvele i internacionalizovani domen za svoju državu, na pismu koje se koristi u toj državi. Srbija je primer jedne od takvih država sa domenom .cp6

CERT-CC – (Computer Emergency Response Team Coordination Centre) je organizacija koja se bavi bezbednošću informaciono-komunikacionih tehnologija. Osnovan je 1988. godine u Picburgu na Univerzitetu Karnegi Melon, a kasnije je ime CERT postalo univerzalno za sve organizacije koje se bave bezbednošću IT u svakoj državi ponaosob. Zadatak oraganizacija CERT je pronalaženje propusta i objavljivanje da bi se pronašla rešenja, obaveštavanje o opasnostima vezanim za IT i slične bezbednose radnje. Srbija još uvek nema svoj CERT ali je trenutno u osnivanju.

DHCP – (Dynamic Host Configuration Protocol) Protokol kojim se omogućava dodeljivanje dinamičkih IP adresa računarima. Koristi se da bi se zamenilo ručno podešavanje IP adresa na svakom računaru ponaosob u velikim sistemima ili kod internet provajdera.

DoS – (Denial of Service) Napad na sistem kojim se uskraćuje mogućnost ostvarivanja servisa. Obično se vrši tako što se od servera traži da izvrši sve veći i veći broj zahteva do trenutka kad ostane bez resursa i ne može više da izvršava svoju osnovnu namenu.

DDoS – (Distributed Denial of Service) Napad na sistem kao i DoS sa tom razlikom što se izvršava sa mnogo više različitih tačaka i mnogo više različitih pravaca (vektora napada) u istom trenutku. Znatno je delotvorniji od DoS napada jer je napadača neuporedivo više.

FIPS, FIPS 140-2 - Federal Information Processing Standard predstavlja standard za sertifikaciju kriptografskih modula kako zahteva državna administracija SAD. Verzija 140-2 je aktuelna verzija standarda iz 2002. godine.

gTLD – (Generic Top Level Domain) su domeni najvišeg reda koji će se pojaviti nakon što prođu komisiju za dodelu novih domena najvišeg reda kod ICANN. Ovaj proces još traje a spekulise se da će biti završen za oko 18 do 24 meseca. U ovoj grupi domena nalaziće se oni za koje su kompanije i lokalne samouprave konkurisale. Neki su se već pojavili a ukupno se očekuje oko 1900 novih među kojima će biti i neki kao .gmail .book .dell .okinawa i drugi

ICANN - Internet Corporation for Assigned Names and Numbers je neprofitna organizacija koja je pobedila na tenderu za upravljanje internet resursima i od tog trenutka zajedno sa organizacijom IANA održava i brine o bazama podataka u kojima se nalaze imena i IP adrese računara na internetu

IP adresa – je numerička adresa dodeljena svakom uređaju da bi mogao da komunicira na internetu. Mogu biti javne i privatne kao i IPv4 ili IPv6.

IPv4 adresa – je trideset dvobitna numerička adresa dodeljena u obliku 4 osmобitna broja (192.168.1.12) čime se dobija ukupan broj od 2^{32} adresa (oko 4,3 milijarde) koje su dodeljene uređajima na mreži da bi mogli da komuniciraju. Ovaj način adresiranja je dostigao svoj maksimum i u toku je proces prelaska na IPv6 koji omogućava neuporedivo veći adresni prostor.

IPv6 adresa – je numerička adresa dodeljena uređajima na mreži u obliku sto dvadeset osmобitnog zapisa što daje 2^{128} adresa ili oko $3,4 \cdot 10^{38}$. Zapis je u obliku 8 grupa po 4 heksadecimalne cifre razdvojene dvotačkama (2001:0db8:85a3:0042:1000:8a2e:0370:7334)

TLD – (Top Level Domain) grupa domena najvišeg reda. Ovi domeni su se prvi pojavili na internetu. U ovu grupu spadaju .com .org .net . edu i još neki.

Redundantnost – sposobnost sistema da izdrži kvarove pojedinih komponenti tako što su mu kritične komponente duplirane ili triplirane (primer je server koji ima dva napajanja, u slučaju otkaza jednog drugi preuzima na sebe i poslove prvog).

Rogue serveri – To su serveri koje su instalirali zlonamerni korisnici da bi mogli da ih koriste za različite prevare. Serveri se često predstavljaju kao pravi ali u stvari imaju namenu da lažiraju IP adrese i DNS podatke, da isporučuju viruse i za druge namene.

Split Horizont – Mogućnost nekih savremenih DNS servera da daju različite odgovore na upite u zavisnosti od toga sa koje IP adrese upit dolazi.

TTL – (time to live) Vremensko trajanje nekog DNS zapisa nakon koga će biti ponovljen upit da se proverí da li se IP adresa tog zapisa promenila.