SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 5911

Demonstracija rada protokola DNSSEC u sustavu IMUNES

Dubravko Lukačević

Zagreb, lipanj 2019.

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

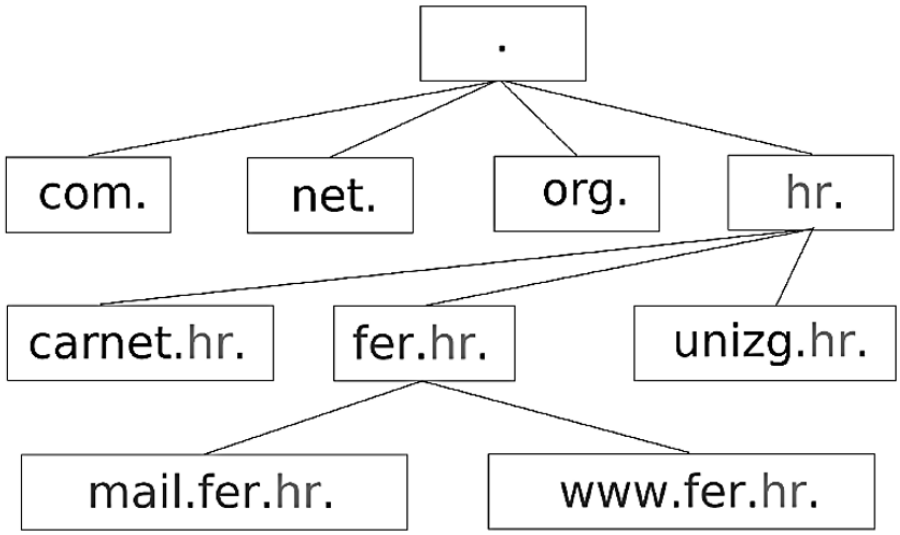
SADRŽAJ

1. Uvod

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

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

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



Slika 1.1: Primjer DNS hijerarhije, izvor [2]

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

2. Sigurnosni problemi DNS-a

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

2.1. Registracija sličnih domena

Kao jedan od čestih problema DNS-a javlja se registracija sličnih domena u svrhu prijevare, a najčešća meta za kriminalce su sustavi koji imaje veze s novcem. Prijevara se odvija tako da kriminalci registriraju domenu sličnog imena (npr. paypa1 umjesto paypal), postave jednak izgled stranice kao original i čekaju da nepažljivi korisnici ostave svoje podatke na njihovoj stranici.
Jedini način pravovremene zaštite jest da, kako bi zaštitile svoje korisnike, organizacije preventivno registriraju sve slične domene.

2.2. Lažiranje DNS odgovora

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

2.3. Trovanje DNS međuspremnika

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

3. Način rada DNSSEC-a

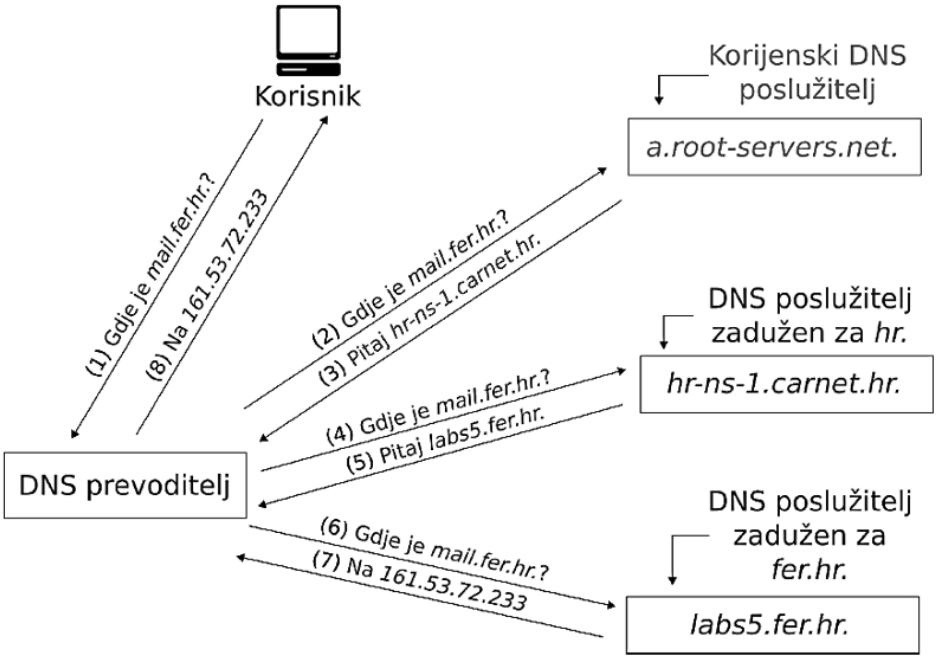
DNS sustav sastoji se od tri glavna dijela, a to su:

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

Slika 3.1 ilustrira DNS prevođenje za slučaj kada klijent DNS prevoditelju pošalje upit za mail.fer.hr. Kada DNS poslužitelj dobije odgovor na traženi upit, taj odgovor se sprema u DNS međuspremnik kako bi drugim korisnicima koji pošalju isti upit mogao odgovoriti bez ponavljanja cijelog postupka prevođenja. Također zapis se nakon nekog vremena briše iz DNS međuspremnika kako ne bi došlo do zastarijevanja.
DNSSEC nije novi protokol, već samo uvodi sljedećih šest novih vrsta DNS zapisa:

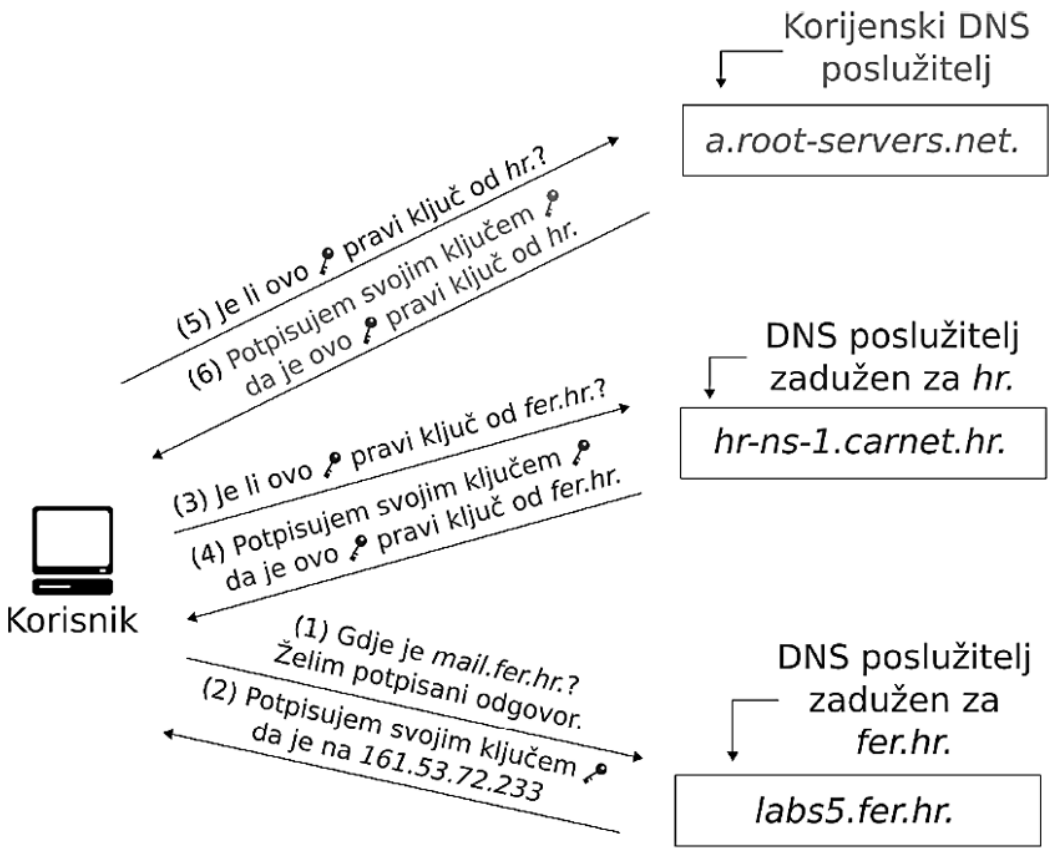
1. Resource Record Signature (RRSIG) - zapis koji sadrži digitalni potpis DNS odgovora koji koriste rekurzivni DNS poslužitelji, kada je DNSSEC uspostavljen svaki DNS odgovor dolazi s najmanje jednim RRSIG potpisom
2. DNS Public Key (DNSKEY) - zapis koji sadrži javni ključ kojim se provjerava digitalni potpis
3. Delegation Signer (DS) - zapis kojim nadređeni DNS poslužitelj podređenom poslužitelju povjerava kontrolu nad domenom niže razine, sadrži siguran sažetak javnog ključa podređenog DNS poslužitelja i ime domene koja se povjerava
4. Next Secured record (NSEC) - dokaz nepostojanja DNS zapisa
5. NSEC record version 3 (NSEC3) - poboljšani oblik NSEC zapisa

6. NSEC3 parameters (NSEC3PARAM) - zapis sadrži parametre koji su potrebni NSEC3 zapisu da bi radio ispravno



Slika 3.1: DNS prevođenje, izvor [1]

Na slici 3.2 možemo vidjeti kako izgleda provjera ispravnosti potpisa, odnosno DNSSEC validacija. Kao što se vidi na slici, proces provjere staje kod korijenskih DNS poslužitelja jer za njih ne postoji nadređeni DNS poslužitelj, stoga nije moguće provjeriti autentičnost njihovog ključa na ovaj način. Korisnik ima odgovornost da na siguran način pribavi ključ korijenskih poslužitelja (ne putem DNS-a) te tako osigura da se ovaj proces završi s ključem kojem korisnik vjeruje pa je onda i sigurno da je primljeni DNS odgovor ispravan. Zato kažemo da je ključ korijenskih DNS poslužitelja izvor ili sidro povjerenja DNSSEC-a, a takav lanac digitalnih potpisa koji počinje ključem korijenskih DNS poslužitelja i završava potpisanim DNS odgovorom naziva se lancem povjerenja jer kada se pribavi ključ korijenskih poslužitelja ispravnost svih drugih potpisa provjerava se lančano.



Slika 3.2: DNSSEC provjera ispravnosti potpisa, izvor [1]

Kako bi se ostvarila potpuna sigurnost, provjera potpisa mora se odvijati na računalu krajnjeg korisnika jer jedino tako se sa sigurnošću može tvrditi da DNS odgovor nije bio lažiran niti u jednom dijelu procesa.
Kada završi provjera DNS odgovora zaštićenog DNSSEC-om rezultat mogu biti četiri stanja za DNS odgovor, koji su navedeni i ukratko opisani u nastavku.

1. Sigurno - ako postoji ispravan lanac potpisa skroz do ključa kojemu korisnik vjeruje te možemo reći da je DNS odgovor zaštićen

2. Nesigurno - ispravan lanac potpisa postoji samo do nekog trenutka u kojem je potvrđeno da tražena domena nije zaštićena te se potvrđuje da je stanje nesigurno, a s time i da postoji mogućnost napada, ali nije moguće odrediti događa li se stvarno napad zbog nezaštićene domene niže razine

3. Lažno - lanac potpisa nije ispravan jer neki od potpisa nije ispravan ili DNS odgovor nije potpisan, a lanac povjerenja potvrđuje da bi trebao biti potpisan iz čega se zaključuje da se događa napad ili da nešto nije ispravno konfigurirano

4. Neodređeno - ako ne postoji ključ kojemu korisnik vjeruje pa nema kako potvrditi ispravnost lanca potpisa, događa se kada korisnik nije sigurno preuzeo ključ korijenskih DNS poslužitelja pa zato ne može donijeti nikakav zaključak

Uočimo razliku između nesigurnog i lažnog stanja. Kada je u pitanju lažno stanje, sigurno možemo reći da se događa napad ili da postoji pogreška u konfiguraciji DNSSEC-a, dok nesigurno stanje označava situaciju u kojoj DNSSEC nije konfiguriran na domeni pa DNS funkcionira normalno kao i inače.
Također postoji bitna razlika između sigurnog i neodređenog stanja, naime kod neodređenog stanja moguće je imati u potpunosti ispravan lanac kao i kod sigurnog stanja, ali razlika je u tome vjeruje li korisnik ključu korijenskih poslužitelja, ako ne vjeruje onda ne može vjerovati ni DNS odgovoru jer "bez povjerenja u ključ korijenskih poslužitelja, nema ni povjerenja u DNSSEC."[1]

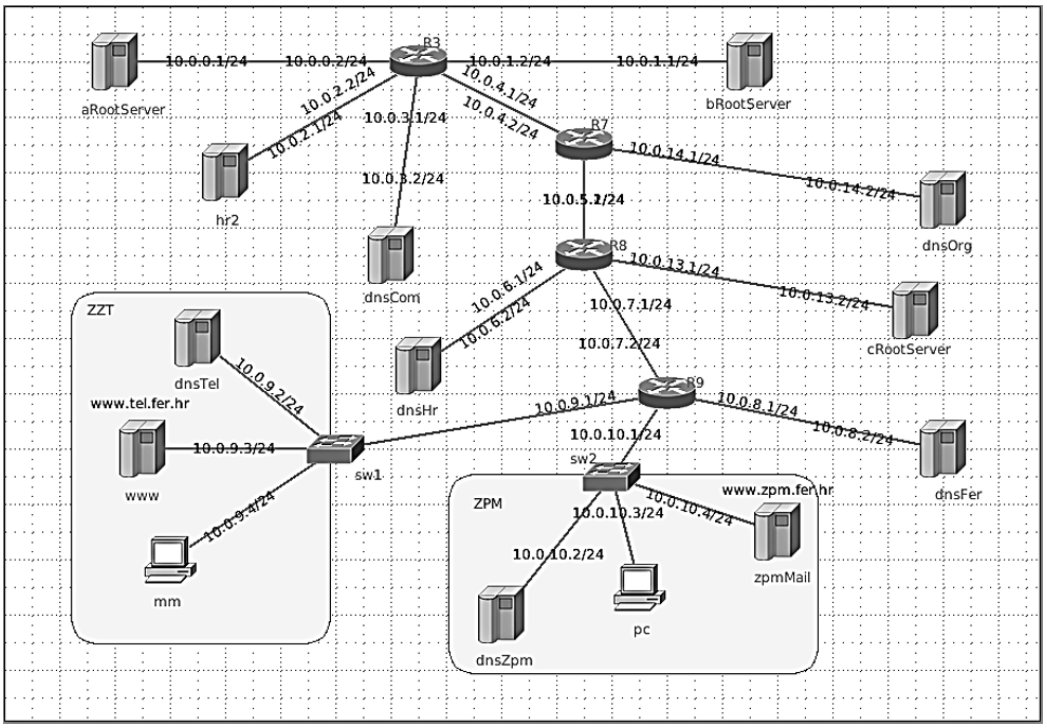
4. Implementacija DNSSEC-a u sustav IMUNES

Budući da je tema ovog rada demonstracija rada protokola DNSSEC u sustavu IMUNES, potrebni su nam program VirtualBox (`https://www.virtualbox.org/wiki/Downloads`) i pripremljeni paket podataka koji uključuje IMUNES i sve potrebne alate predviđen za otvaranje pomoću VirtualBox-a (`http://www.imunes.net/dl/IMUNES_security.ova`). Nakon što pokrenemo spomenuto virtualno okruženje potrebna nam je 9.9 ili novija inačica BIND-a, to se provjeri upisivanjem naredbe named -v u terminal. Sljedeća bitna stvar je pokretanje naredbe named -V i provjera koje su zastavice postavljene. Ako je postavljena zastavica –with-openssl onda je DNSSEC podržan i spreman je za daljnji rad, a ako nije onda je neophodno da nadogradimo sustav na noviju inačicu.

Na slici 4.1 prikazana je mreža koja je korištena u ovom završnom radu. Za sustav koji podržava DNSSEC sljedeći korak je omogućiti DNSSEC validaciju. Na disku pronađemo mapu u kojoj se nalaze konfiguracije DNS poslužitelja (nastavak .conf) te za svaki poslužitelj otvorimo tu datoteku programom za uređivanje teksta te unutar bloka options {...} dodamo sljedeće dvije linije koda:

dnssec-validation auto;
dnssec-enable yes;

Naredbom dnssec-validation auto omogućena je automatska validacija pretpostavljenog sidra povjerenja koje se nalazi u datoteci managed-keys. Postoje još opcije yes i no, za opciju yes potrebno je ručno postaviti sidro povjerenja, a za opciju no DNSSEC validacija je isključena. Ukoliko želimo uspostaviti DNSSEC validaciju prvo je potrebno omogućiti sami DNSSEC, a za to sluči naredba dnssec-enable yes.



Slika 4.1: Prikaz korištene mreže

Pomoću alata "dig" provjerimo trenutno stanje. Nakon pokretanja eksperimenta u sustavu IMUNES (Experiment -> Execute) u terminalu se pozicioniramo u mapu u kojoj se nalaze datoteke vezane za ovaj projekt te naredbom "./start_dns" pokrenemo skriptu start_dns.pl koja pokreće i konfigurira sve DNS poslužitelje korištene u eksperimentu. Sadržaj te skripte prikazan je u nastavku.

```
#! /bin/sh

    error() {
                echo $*
                exit 2
            }

    dns_servers="aRootServer bRootServer cRootServer \
                dnsCom dnsOrg dnsHr hr2 \
                dnsFer \
                dnsTel dnsZpm"

    hosts="mm www pc zpmMail"
```

```
if test $# -eq 1; then
        eid=$1
else
        eid=`himage -e aRootServer`
        if test $? -ne 0; then
                exit 1
        fi
fi

for i in $dns_servers
do
        himage $i@$eid killall -9 named 2> /dev/null
        hcp rndc.key $i@$eid:/usr/local/etc/namedb/rndc.key
        hcp bind.keys $i@$eid:/usr/local/etc/namedb/bind.keys
done

cd DNS_files

for i in $dns_servers
do
        himage $i@$eid mkdir -p /var/named/etc/namedb
        hcp $i/* $i@$eid:/var/named/etc/namedb
        echo Starting named on $i...
        himage $i@$eid named -c /var/named/etc/namedb/named.conf
done

echo
echo Copy/Create resolv.conf on clients:
for i in $hosts
do
        hcp resolv.$i $i@$eid:/etc/resolv.conf
done
```

Sada recimo s računala mm pošaljemo upit za "www.tel.fer.hr". U konzolu pokrenutu na računalu mm unesemo naredbu:

```
dig @10.0.9.2 www.tel.fer.hr. A +dnssec +multiline
```

U nastavku su prikazana najbitnija polja odgovora na navedeni upit.

```
; (1 server found)
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46595
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:
2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; ANSWER SECTION:
www.tel.fer.hr. 60000 IN A 10.0.9.3
```

Ovdje nam veliku ulogu igraju zastavice. Ovim korakom dobili smo zastavicu "do" (kratica od engl. DNSSEC OK) koja ukazuje na to da rekurzivni DNS poslužitelj zna kako postoji mogućnost da dobije potpisani DNS odgovor. Bit koji prikazuje zastavicu "do" prenosi se pomoću EDNS-a (kratica od engl. Extension mechanism for DNS), odnosno proširenja koje omogućuje slanje DNS zahtjeva i odgovora u većim paketima preko UDP-a. Vidimo da u ovom slučaju BIND već ima EDNS omogućen. Nakon što u potpunosti završimo konfiguraciju DNSSEC-a trebali bi ovdje vidjeti RRSIG zapis i "ad" zastavicu (kratica od engl. Authenticated Data), koja ukazuje na to da je primljeni odgovor uspješno prošao proces validacije.

Sljedeći korak je stvaranje ključeva, a navedeni postupak potrebno je ponoviti za svaki DNS poslužitelj u našoj mreži, osim za "slave" poslužitelje, a to su u ovom slučaju bRootServer, cRootServer i hr2. U nastavku je prikazano stvaranje ključeva za domenu hr. Potrebno je pozicionirati se u terminalu unutar mape u kojoj se nalaze konfiguracijske datoteke DNS poslužitelja dnsHr, a nakon toga upisati sljedeće naredbe:

```
dnssec-keygen -a RSASHA256 -b 1024 hr
dnssec-keygen -a RSASHA256 -b 2048 -f KSK hr
```

Na ovaj način dobili smo dvije vrste ključeva, KSK (kratica od engl. Key Signing key) i ZSK (kratica od engl. Zone Signing key) te od svake vrste po jedan privatni i jedan javni ključ. Slika 4.5 prikazuje kada se koristi koji ključ i koliko često se to događa.

Ključ	Upotreba	Učestalost korištenja
ZSK privatni	Koristi ga autoritativni DNS poslužitelj za stvaranje RRSIG zapisa za podatke o zoni	Relativno često, svakom promjenom podataka o zoni
ZSK javni	Koristi ga rekurzivni DNS poslužitelj za validaciju podataka iz zone	Često, kad god rekurzivni DNS poslužitelj vrši validaciju DNS odgovora
KSK privatni	Koristi ga autoritativni DNS poslužitelj za stvaranje RRSIG zapisa za ZSK i KSK javni ključ (DNSKEY)	Rijetko, kada se promijene ZSK ili KSK, npr. jednom godišnje
KSK javni	Koristi ga rekurzivni DNS poslužitelj da provjeri je li DNSKEY validan	Često, kad god rekurzivni DNS poslužitelj provjerava je li DNSKEY validan

Slika 4.2: Uloga KSK i ZSK ključeva

Ukratko, KSK ključevi (koji se rijetko mijenjaju) potpisuju ZSK, a ZSK potpisuje DNS zapis pa je zapravo za provjeru valjanosti DNS zapisa bitan samo KSK. Također samo KSK se u formi DS zapisa prosljeđuje roditelju u lancu povjerenja, koji potom potpisuje DS zapis svojim KSK ključem i tako dalje prema korijenu, odnosnu sidru povjerenja.
Nakon stvaranja ključeva potrebno je ponovno urediti named.conf konfiguracijsku datoteku za svaki DNS poslužitelj koji koristimo tako da (npr. za dnsHr) unutar bloka zone "hr" {...} unesemo sljedeće naredbe:

```
key-directory "/etc/namedb";
inline-signing yes;
auto-dnssec maintain;
```

Naredbom key-directory dodajemo put do ključa, a inline-signing služi za potpisivanje zone pomoću ključeva koji se nalaze na lokaciji navedenoj u nastavku key-directory naredbe. Inline-signing je onemogućeno po pretpostavljenoj vrijednosti i zato je potrebno izričito reći da želimo omogućiti potpisivanje zone. Naredbom auto-dnssec se zadaje način upravljanja ključevima, postoje opcije off (pretpostavljena vrijednost) za ručno upravljanje ključevima, allow dopušta ponovno potpisivanje zona kada korisnik unese naredbu rndc sign, a opcija maintain koju mi koristimo daljnju brigu prepušta BIND-u, odnosno potpisivanje i vršenje određenih korekcija odvija se automatski.

Potrebno je stvoriti rndc konfiguracijske datoteke pomoću istoimenog alata. RNDC (Remote Name Daemon Control) je pomoćni program za kontrolu servera u BIND-u. Rndc.key datoteka sadrži tajni ključ koji omogućuje povezivanje poslužitelja ako se

ključevi podudaraju. Za početak kreirat ćemo datoteke za jedan proizvoljni poslužitelj te ćemo taj ključ kopirati na sve poslužitelje. Unesimo za primjer naredbu:

himage dnsTel rndc-confgen -a

Tako smo stvorili automatsku rndc konfiguraciju na poslužitelju dnsTel koja nam je u ovom slučaju dovoljna. Ta konfiguracija je sada na virtualnom čvoru pa ćemo upotrijebiti naredbu

hcp dnsTel:/usr/local/etc/namedb/rndc.key .

kako bi datoteku rndc.key kopirali na stvarni operacijski sustav.
Nadalje, u radnoj mapi potrebno je stvoriti novu tekstualnu datoteku, nazvati ju bind.keys i u nju kopirati sve KSK ključeve po zonama tako da korijenski javni KSK ključ stavimo u managed-keys blok, a ostale u trusted-keys blok. To izgleda otprilike ovako:

```
managed-keys {
        . initial-key 257 3 8 "AwEAAfP1M/N1u...OLA6tk=";
};

 trusted-keys {
        hr. 257 3 8 "AwEAAZR2LFjTzxt0...RBjOnlMk=";
        fer.hr. 257 3 8 "AwEAAerUor/t2...n5CodQfObk=";
        tel.fer.hr. 257 3 8 "AwEAAdaIbMS...QsldEGkz1s=";
        zpm.fer.hr. 257 3 8 "AwEAAb4e83...7tSO4Twwb0=";
        com. 257 3 8 "AwEAAdTLa8DtvO...tlBhtRJE/0M=";
        org. 257 3 8 "AwEAAdGgf1H...OW 1SVs/gNyNB0=";
};
```

Ovime smo uspostavili međusobno povjerenje između zona jer će sada DNS poslužitelji vjerovati ključevima koje smo ranije generirali.

5. Rezultati

6. Zaključak

DNS protokol je nezaštićen pa postoje ozbiljni sigurnosni problemi i puno mogućnosti napada na korisnike. Zbog toga je nastao DNSSEC, sigurnosni dodatak DNS-u koji DNS odgovorima osigurava autentičnost i integritet, odnosno sprječava napadače u njihovim zlim namjerama.

Nažalost, DNSSEC još uvijek nije implementiran na većini DNS poslužitelja, a upravo to je potrebno kako bi njegova korist došla do izražaja te kako bi se izgradio globalno siguran sustav. Valja napomenuti da konfiguracija DNSSEC-a nije nimalo jednostavna u što će se brzo uvjeriti svi koje se u tome okušaju. Svaka i najmanja greška u konfiguraciji učini stranice i servise nedostupnima, a to naravno negativno utječe na poslovanje pa je upravo složenost konfiguracije glavni razlog zašto DNSSEC još uvijek nije u širokoj upotrebi.

Trenutno je moguće djelomično se zaštititi kao krajnji korisnik ako svoje uređaje konfiguriramo tako da uvijek pri slanju DNS upita provjeravaju postoji li DNSSEC potpis i ako postoji da ga provjere. Ako to učinimo spriječit ćemo lažiranje DNS odgovora barem za domene koje su već zaštićene DNSSEC-om.

Demonstracija rada protokola DNSSEC u sustavu IMUNES

Sažetak

Ukratko su objašnjeni najvažniji pojmovi vezani za DNS i njegovo sigurnosno proširenje DNSSEC te način rada DNSSEC-a i zašto je bitan, a nakon toga i jedan način konfiguracije potrebnih datoteka. Uspostava DNSSEC-a nije jednostavna i lako se mogu dogoditi pogreške, a i najmanja pogreška prouzročit će neispravan rad sustava. Iz tog razloga prikazano je korak po korak kako implementirati DNSSEC, a nakon toga i kako provjeriti radi li sve ispravno.

Ključne riječi: DNS, DNSSEC, sigurnost, DNS proširenje, IMUNES, BIND

Demonstration of DNSSEC protocol using IMUNES system

Abstract

Keywords: DNS, DNSSEC, security, DNS extensions, IMUNES, BIND