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`.

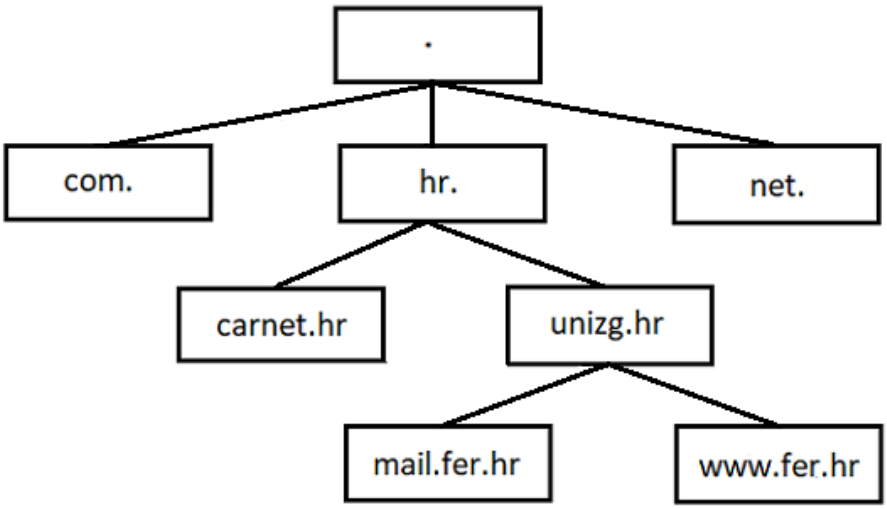
SADRŽAJ

1. Uvod

Domenski sustav imena (engl. Domain Name System, kratica DNS) je sustav koji povezuje IP-adrese i 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 koji imaju hijerarhijsko značenje. Uzmimo za primjer ime www.fer.hr. koje se sastoji od tri dijela – www, fer i hr, pri čemu hr označava Hrvatsku, fer označava Fakultet Elektrotehnike i Računarstva u Hrvatskoj, a www označava poslužiteljsko računalo na FER-u. Krajnji desni dio domenskog imena naziva se vršna domena ili TLD (engl. top-level domain), u ovom slučaju to je vršna domena hr. Sve domene u domenskom imenu koje su lijevo od TLD-a predstavljaju poddomene. 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.

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

DNSSEC je sigurnosna nadogradnja DNS protokola koja osigurava autentičnost i integritet DNS odgovora koristeći digitalni potpis koji je baziran na kriptografiji javnog ključa. 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

Detalji o konceptima i implementaciji DNS-a nalaze se u dokumentima RFC 882 i RFC 883 (izvorni tehnički podaci), odnosno RFC 1035, RFC 1123 i RFC 2181 (dopune i konačni opis pravila za oblikovanje domenskih imena). RFC (kratica od engl. Request for Comments) dokumente izdaje Internet Engineering Task Force (IETF).

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 od čega nas točno štiti 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.com umjesto paypal.com), 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.

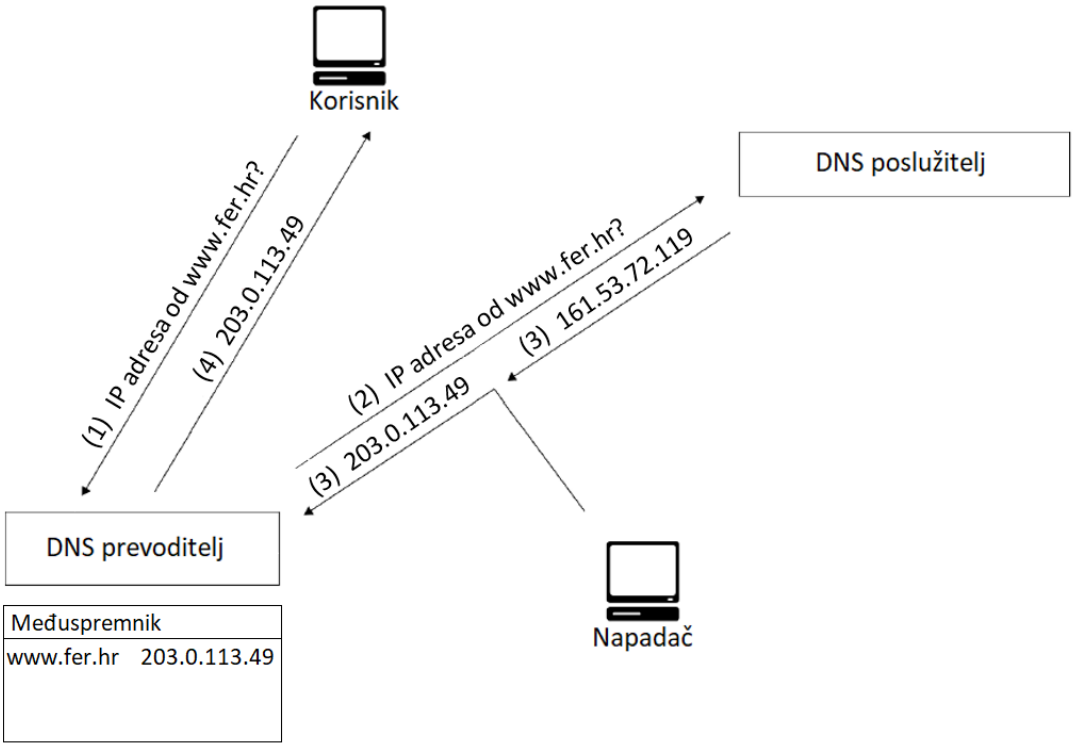
2.2. Lažiranje DNS odgovora

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 i 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. Ako se napadač ubaci u komunikaciju između klijenta i DNS poslužitelja ili između rekurzivnog i autoritativnog DNS poslužitelja, tada napadač 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.



Slika 2.1: Primjer trovanja DNS međuspremnika

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 preslikavanje simboličkog imena u IP-adresu 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 ima određeni rok trajanja koji se provjerava prilikom dohvaćanja i ako je taj rok prošao zapis se briše iz međuspremnika i potrebno je ponoviti proces sa slike 3.1. Tako se sprječava zastarijevanje zapisa u međuspremniku.

DNSSEC je predstavljen dokumentima RFC 4033, RFC 4034 i RFC 4035 te su u njima opisani način rada i novi zapisi koje DNSSEC uvodi, a kasnije u dokumentima RFC 6014, RFC 6840 i RFC 6944 objašnjeni su implementacija i korišteni kriptografski algoritmi za generiranje ključeva. DNSSEC nije novi protokol, već samo sigurnosno proširenje protokola DNS i kao takvo uvodi sljedećih šest novih vrsta DNS zapisa:

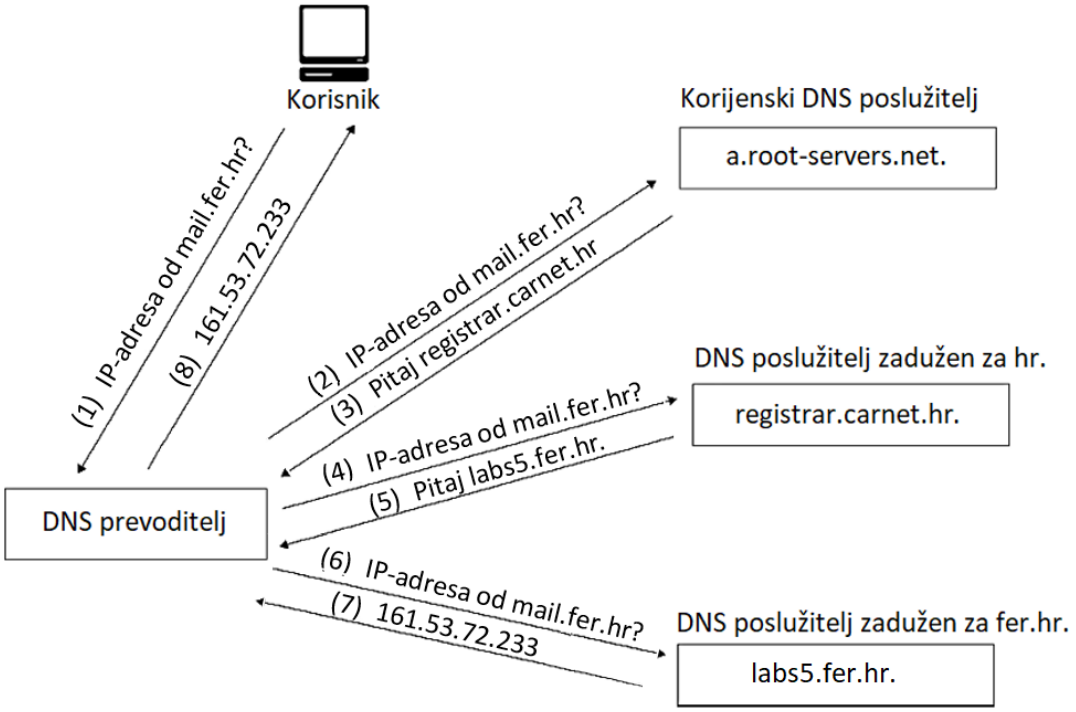
1. "Resource Record Signature" (RRSIG) - zapis koji sadrži digitalni potpis DNS odgovora, kreiran i poslan od strane autoritativnog DNS poslužitelja, a koriste ih rekurzivni DNS poslužitelji za verifikaciju DNS odgovora, kada je DNSSEC uspostavljen svaki DNS odgovor dolazi s najmanje jednim RRSIG potpisom
2. "DNS Public Key" (DNSKEY) - zapis koji sadrži javni ključ zone te se njim 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

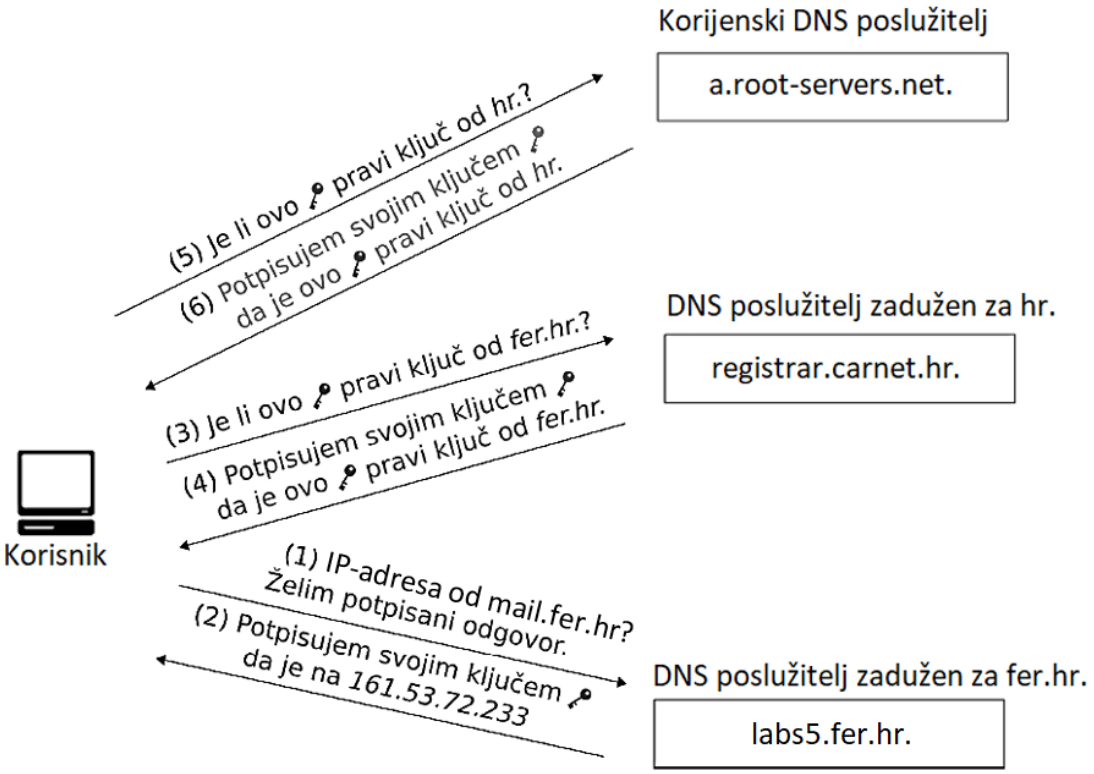
6. "NSEC3 parameters" (NSEC3PARAM) - zapis sadrži parametre koji su potrebni NSEC3 zapisu da bi radio ispravno



Slika 3.1: DNS razlučivanje

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 niz 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

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.

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[1] i pripremljeni paket podataka koji uključuje IMUNES i sve potrebne alate predviđen za otvaranje pomoću VirtualBox-a[2]. Nakon što pokrenemo spomenuto virtualno okruženje potrebna nam je 9.9 ili novija inačica BIND-a, to se provjeri upisivanjem u terminal naredbe:

```
# named -v
```

Trebali bi dobiti ispis:

```
BIND 9.14.1 (Stable Release)
```

Sljedeća bitna stvar je pokretanje naredbe

```
# named -V
```

i provjera koje su zastavice postavljene. Ako je postavljena zastavica (ako se nalazi u ispisu) `-with-openssl` onda je DNSSEC podržan i spreman je za daljnji rad, a ako nije onda je neophodno da nadogradimo sustav na noviju inačicu.

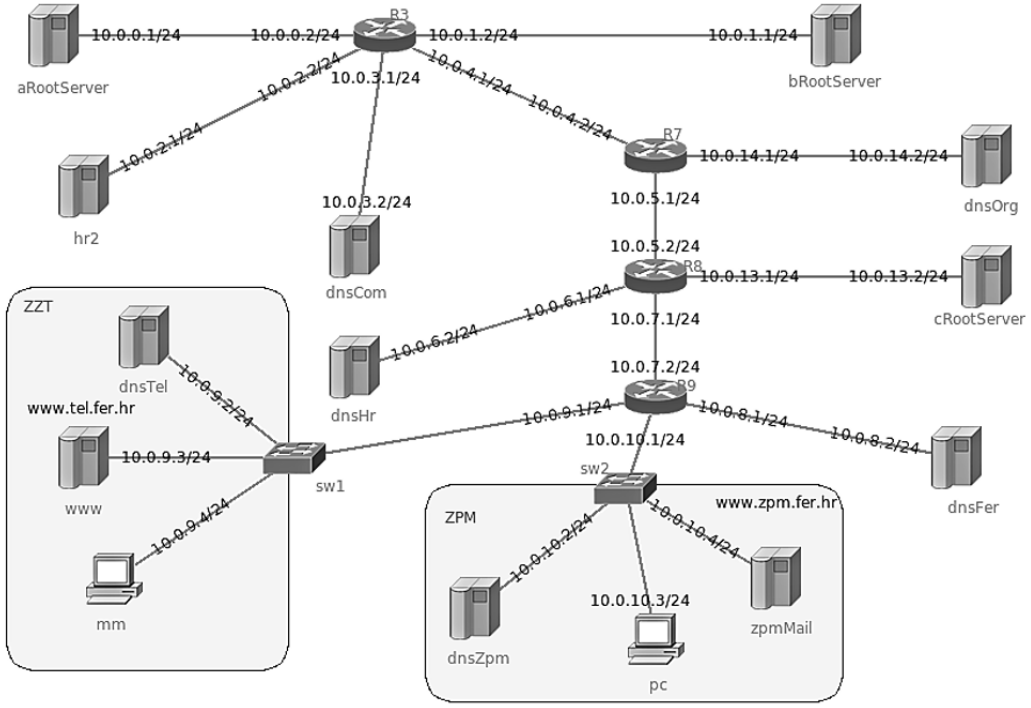
Na slici 4.1 prikazana je mreža koja je korištena u ovom završnom radu. Za sustav koji podržava DNSSEC sljedeći korak je omogućiti DNSSEC validaciju. Na disku pronađemo mapu u kojoj se nalaze konfiguracije DNS poslužitelja (nastavak .conf) te za svaki poslužitelj otvorimo tu datoteku programom za uređivanje 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. Ako želimo uspostaviti DNSSEC validaciju prvo je

[1] VirtualBox, `https://www.virtualbox.org/wiki/Downloads`
[2] IMUNES, `http://www.imunes.net/dl/IMUNES_security.ova`

potrebno omogućiti sami DNSSEC, a za to služi `dnssec-enable yes`.



Slika 4.1: Prikaz korištene mreže

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 skripte prikazan je u nastavku.

```
#! /bin/sh
error() {
    echo $*
    exit 2
}
dns_servers="aRootServer bRootServer cRootServer dnsCom dnsOrg \
             dnsHr hr2 dnsFer dnsTel dnsZpm cache"
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
    # Stop named on all DNS servers
    himage ${i}@${eid} killall -9 named 2> /dev/null
    hcp rndc.key ${i}@${eid}:/usr/local/etc/namedb/rndc.key
done

for i in $dns_servers $hosts
do
    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
    # Start named on all DNS servers
    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
```

Pomoću alata `dig` (domain information groper) i opcija koje pruža možemo temeljito ispitati rad DNS poslužitelja, za što se inače koriste naredbe `host` i `nslookup`. Za naše potrebe `dig` je primjereniji jer, za razliku od naredbi `host` i `nslookup`, `dig` ima opcije koje podržavaju DNSSEC.

Pošaljimo sada s računala `mm` upit za `www.tel.fer.hr`. U konzolu pokrenutu na računalu `mm` unesemo naredbu:

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

Pri čemu je `@10.0.9.2` IP-adresa poslužitelja kojem šaljemo upit za simboličko ime `www.tel.fer.hr`, `A` označava da želimo saznati IP-adresu, zastavicom `+dnssec` kažemo da želimo da nam se pošalju i DNSSEC zapisi, a zastavica `+multiline` je tu samo kako bi dobili ljepši ispis kroz više redova. U nastavku su prikazana najbitnija polja odgovora na navedeni upit.

```
; (1 server found)\newline
;; 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
```

Obratimo pažnju na 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 barem jedan RRSIG zapis kojim rekurzivni DNS poslužitelj verificira dobiveni odgovor.

Sljedeći korak je stvaranje ključeva, a navedeni postupak potrebno je ponoviti za sve glavne ("master") DNS poslužitelje u našoj mreži, a "slave" poslužitelji (to su u ovom slučaju `bRootServer`, `cRootServer` i `hr2`) će ih sami dohvatiti s glavnih poslužitelja. 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
```

Pri čemu naredba `dnssec-keygen` generira ključeve, s `-a RSASHA256` odabiremo algoritam koji se koristi, zastavicom `-b` i brojem nakon nje određujemo željenu veličinu ključa, a zastavicom `-f` u drugoj linija koda kažemo da želimo KSK ključ i naposljetku navedeno je buduće ime ključa.
Iz ispisa naredbe `ls` vidimo da su se stvorile četiri nove datoteke koje sadrže ključeve.

```
Khr.+008+01701.key       Khr.+008+18640.private   named.conf
Khr.+008+01701.private   hr                       named.root
Khr.+008+18640.key       localhost.rev
```

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 4.2 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.

RNDC (Remote Name Daemon Control) je pomoćni program za kontrolu servera u BIND-u. Potrebno je stvoriti `rndc` konfiguracijske datoteke pomoću istoimenog alata. `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, dodijeliti joj ime `bind.keys` i u nju kopirati korijenski javni KSK ključ unutar bloka `managed-keys`. To izgleda otprilike ovako:

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

Ovime smo uspostavili međusobno povjerenje između zona jer će sada DNS poslužitelji vjerovati ključevima koje smo ranije generirali. To možemo provjeriti pozivom naredbe:
`# himage dnsTel cat /var/named/etc/namedb/managed-keys.bind`
U ispisu vidimo njegov KSK ključ, nakon njega polje u kojem piše `trusted since` i današnji datum nakon toga. Isto ćemo dobiti pozivom naredbe na bilo kojem virtualnom čvoru, `dnsTel` je uzet samo kao primjer.

Sljedeći korak je ujedno i zadnji korak, a to je stvaranje DS zapisa iz KSK javnog ključa također za svaki glavni ("master") DNS poslužitelj. Javni ključevi imaju nastavak ".key", a ako otvorimo datoteku, unutra piše je li ključ KSK ili ZSK. Recimo za stvaranje DS zapisa za `dnsFer`:
`dnssec-dsfromkey Kdnsfer.+008+40120.key`
Pri čemu je `dnssec-dsfromkey` naredba koja generira DS zapis, a nakon nje zadajemo ime ključa iz kojeg želimo generirati DS zapis. Nakon izvršavanja naredbe u terminalu se ispiše generirani DS zapis koji je potrebno kopirati (za ovaj primjer) u konfiguracijsku datoteku `fer` i u konfiguracijsku datoteku DNS poslužitelja koji se u hijerarhiji nalazi iznad njega, u ovom slučaju to je `hr`. Oblik zapisa u konfiguracijskoj datoteci:

```
tel.fer.hr. IN DS 37201 8 1 9F72A0C55ABA3B44A6CF65BA6043EDFBCD612B1D
tel.fer.hr. IN DS 37201 8 2 5E2113CD53FBF735B5B2830D0C8D2D27E342D...

zpm.fer.hr. IN DS 57802 8 1 357C1BFF0073D6F4A3792C5B3A83D9E490B74853
zpm.fer.hr. IN DS 57802 8 2 4BA423ED40F29533BBD808AA7F024CC31FE89...
```

```
fer.hr. IN DS 27247 8 1 601D63EBBFB347B42143170114D40887146B87A3
fer.hr. IN DS 27247 8 2 762C0FDBA866BFD394BF450E120348DD88C1C...
```

Tako ćemo u datoteku `root` dodati DS zapis za `hr`, `com` i `org`, u datoteku `hr` zapise za `hr` i `fer.hr` i tako dalje. Poslužitelji koji nemaju nikoga ispod sebe u hijerarhiji imat će samo svoj DS zapis.

5. Rezultati

DNSSEC nije novi protokol pa nije za očekivati neke velike razlike u zapisima. Razlika je samo u nekoliko zastavica i novih zapisa, ali to uvelike utječe na sigurnost. Ispravnost rada DNSSEC-a najbolje se može testirati alatom `delv`. `Delv` je sličan već spomenutom `dig-u`, samo što je posebno prilagođen za DNSSEC. BIND inačice novije od 9.10 imaju već instaliran alat `delv`, ali ako nemate dovoljno novu inačicu BIND-a nadogradnja je jednostavna. Potrebno je prvo obrisati trenutnu inačicu (vjerojatno 9) i nakon toga instalirati novu inačicu, npr. trenutno najnoviju 9.14.1 naredbama

```
pkg_imunes delete bind9
pkg_imunes install bind914
```

U nastavku su navedene neke naredbe kojima možemo provjeriti funkcionalnost DNSSEC-a te očekivani i dobiveni odgovori.

Ako traženi zapis postoji i prolazi DNSSEC validaciju trebamo dobiti poruku `fully validated`, kao što dobijemo kada na poslužitelju `dnsTel` pošaljemo upit za `A` zapis računala `www.tel.fer.hr`, odnosno tražimo njegovu IP-adresu naredbom:

```
root@dnsTel# delv @127.0.0.1 www.tel.fer.hr A +multiline
```

u nastavku je prikazan odgovor koji dobijemo:

```
; fully validated
www.tel.fer.hr. 60000 IN A 10.0.9.3
www.tel.fer.hr. 60000 IN RRSIG A 8 4 60000
                      20190613120058 20190603073058 48270 tel.fer.hr.
                      csh3XrTJJluQBwze4FRuKQyCbAGJPCU1SfHFtFpIvtnB
                      89fJ0A/4dr7fb8X1lP9f+vTZjiPkMZd7IgfhLq0ppCka
                      eVx5n4VlkvT4JWKfe7zLK64SV+cJN2fkgxu2XxXO53s
                      Ps4j+QHsL4F3r29eJqAj+x7rxgBVNmpyky9Gt9k= )}
```

Vidimo da smo uz traženu IP-adresu dobili i RRSIG zapis. Ranije je objašnjeno da svaka potpisana zona generira barem jedan RRSIG zapis te i po tome možemo zaključiti da je zona koju ispitujemo potpisana.

Kada pokušamo dohvatiti zapis koji ne postoji, kao što je `A` zapis za domenu `tel.fer.hr`, očekivano dobijemo negativan odgovor koji je također potpisan:

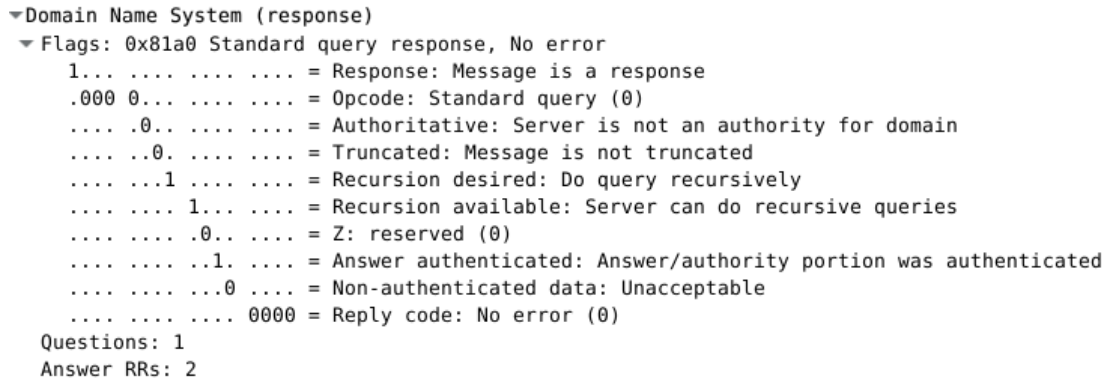
```
root@dnsTel:/ # delv @127.0.0.1 +root=tel.fer.hr tel.fer.hr A +multiline
;; resolution failed: ncache nxrrset
; negative response, fully validated
; tel.fer.hr.           3200171710 IN \-A ;-\$NXRRSET
; tel.fer.hr. SOA dnsTel.tel.fer.hr. root.dnsTel.tel.fer.hr.tel.fer.hr
2002102804 28 14 3600000 0
; tel.fer.hr. RRSIG SOA ...
; tel.fer.hr. RRSIG NSEC ...
; tel.fer.hr. NSEC dnsTel.tel.fer.hr. NS SOA MX RRSIG NSEC DNSKEY TYPE65
534
```

Vidimo NSEC zapis koji je, kao što smo već rekli, dokaz nepostojanja te iz toga i poruke `fully validated` zaključujemo da i u ovom slučaju sve funkcionira kako bi trebalo.

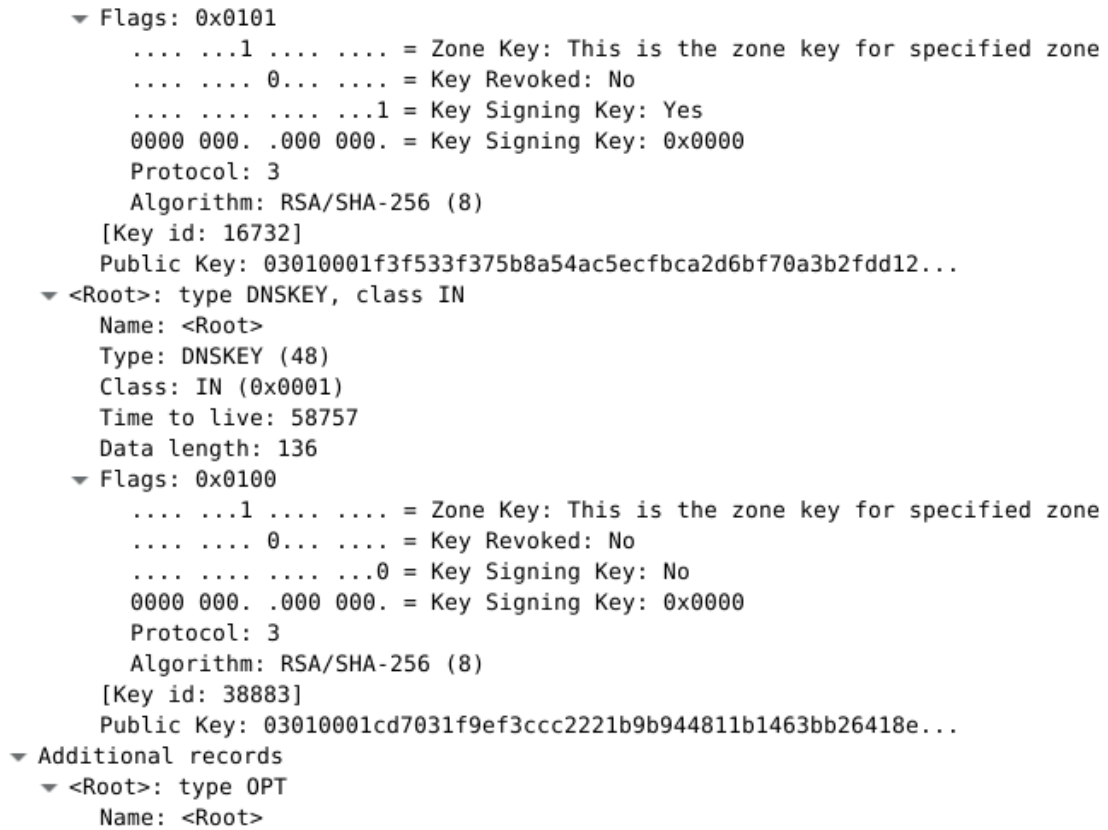
Rezultate možemo pogledati i u alatu `Wireshark`. Za primjer snimimo mrežni promet na računalu `mm`. Desnim klikom miša na računalo `mm` dobit ćemo izbornik u kojem odaberemo `Wireshark -> eth0 (10.0.9.4/24)`, tako smo započeli snimanje mrežnog prometa na sučelju `eth0` računala `mm`. Zatim pokrenemo konzolu na računalu `mm` i pošaljemo upit na `dnsTel` o ključevima korijenskog poslužitelja pomoću alata `dig` i sljedeće naredbe:

```
dig @10.0.9.2 . dnskey
```

Zaustavimo snimanje prometa i pogledamo što sve sadrži DNS odgovor. Kao što smo već rekli, DNSSEC nije novi protokol, već proširenje protokola DNS i zato u polju protokol očekivano piše DNS. Na slikama 5.1 i 5.2 vidimo postavljene zastavice i vrijednosti polja za dobiveni DNS odgovor. Među njima su zastavica `answer authenticated` koja nam govori da je poslužitelj potvrdio autentičnost podataka, zastavice koje govore da se u odgovoru nalaze ZSK i KSK ključevi, naveden je algoritam koji se koristio pri generiranju ključeva, vidimo ispis ključeva i još neke druge dodatne zapise kao što je inačica EDNS-a koja se koristi.



Slika 5.1: DNSSEC zastavice u alatu Wireshark



Slika 5.2: Prikaz KSK i ZSK ključeva u alatu Wireshark

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. Potrebno je omogućiti DNSSEC, postaviti odgovarajuću opciju validacije, generirati ključeve koji su dovoljno sigurni za vaše potrebe, redovito ih mijenjati, pažljivo testirati i onda još sve skupa održavati.

Podrška od strane DNS poslužitelja koji su nadležni za određenu domenu je samo jedna polovica DNSSEC-a, drugi dio čini podrška na strani korisnika i rekurzivnog DNS prevoditelja. Potrebno je posebno konfigurirati DNS prevoditelj da traži i provjerava DNSSEC potpise jer gotovo sav često korišteni softver podržava korištenje DNSSEC-a (kako sa strane poslužitelja i prevoditelja, tako i sa strane korisnika), ali provjera DNSSEC potpisa nije automatski uključena niti na jednom često korištenom operacijskom sustavu.

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.

LITERATURA

[1] Internet Engineering Task Force. Requirements for Internet Hosts – Application and Support, 1989. URL https://tools.ietf.org/html/rfc1123.

[2] Internet Systems Consortium Inc. BIND DNSSEC Guide, 2014. URL https://ftp.isc.org/isc/dnssec-guide/dnssec-guide.pdf.

[3] Laboratorij za sustave i signale Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu. Sigurnosne ekstenzije DNS sustava, 2011. URL https://www.cis.hr/files/dokumenti/CIS-DOC-2012-06-052.pdf.

[4] Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu. DNSSEC, 2017. URL https://www.cert.hr/wp-content/uploads/2017/11/DNSSEC_0.pdf.

[5] P. Hoffman. Cryptographic Algorithm Identifier Allocation for DNSSEC, 2010. URL https://tools.ietf.org/html/rfc6014.

[6] P. Mockapetris. DOMAIN NAMES - CONCEPTS and FACILITIES, 1983. URL https://tools.ietf.org/html/rfc882.

[7] P. Mockapetris. DOMAIN NAMES - IMPLEMENTATION and SPECIFICATION, 1983. URL https://tools.ietf.org/html/rfc883.

[8] P. Mockapetris. DOMAIN NAMES - IMPLEMENTATION and SPECIFICATION, 1987. URL https://tools.ietf.org/html/rfc1035.

[9] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. DNS Security Introduction and Requirements, 2005. URL https://tools.ietf.org/html/rfc4033.

[10] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. Resource Records for the DNS Security Extensions, 2005. URL https://tools.ietf.org/html/rfc4034.

[11] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. Protocol Modifications for the DNS Security Extensions, 2005. URL https://tools.ietf.org/html/rfc4035.

[12] R. Elz, R. Bush. Clarifications to the DNS Specification, 1997. URL https://tools.ietf.org/html/rfc2181.

[13] S. Rose. Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status, 2013. URL https://tools.ietf.org/html/rfc6944.

[14] S. Weiler, D. Blacka. Clarifications and Implementation Notes for DNS Security (DNSSEC), 2013. URL https://tools.ietf.org/html/rfc6840.

[15] Nick Sullivan. DNSSEC: An Introduction. https://blog.cloudflare.com/dnssec-an-introduction/, 2014. Online; pristupljeno: 20. svibnja 2019.

Demonstracija rada protokola DNSSEC u sustavu IMUNES

Sažetak

Ukratko su objašnjeni najvažniji pojmovi vezani za DNS, siurnosni problemi koji se javljaju i sigurnosno proširenje DNSSEC te način rada DNSSEC-a i zašto je bitan. Nakon toga prikazan je jedan način konfiguracije potrebnih datoteka. Uspostava DNSSEC-a nije nimalo jednostavna i lako se mogu dogoditi pogreške, a svaka i najmanja pogreška prouzročit će neispravan rad sustava. Iz tog razloga DNSSEC još uvijek nije implementiran na velikom broju DNS poslužitelja i zato je u ovom radu prikazano korak po korak kako implementirati DNSSEC, a nakon toga i kako provjeriti funkcionira li sustav ispravno, odnosno potpisuju li se zone i validiraju li se DNS odgovori.

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

Demonstration of DNSSEC protocol using IMUNES system

Abstract

The most important terms regarding DNS are explained, the security problems that arise, the security extension DNSSEC, the principles of how it works and why it is important. Afterwards, one way to configure the necessary files is shown. Setting up DNSSEC is not simple and mistakes can easily happen and even minor mistakes can cause the system to work incorrectly. For that reason DNSSEC is still not implemented on a large number of DNS servers and that is why this paper shows step-by-step instructions how to implement DNSSEC and how to verify if the system is working properly, meaning whether the zones are being signed and the DNS responses are being validated.

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