

Departman za posleddiplomske studije
SAVREMENE INFORMACIONE TEHNOLOGIJE

MASTER STUDIJE
- Master rad -

**BEZBEDNOST RUTIRANJA I SISTEMA
IMENOVANJA DOMENA**

Mentor:
prof. dr Mladen Veinović

Student:
Đorđe Antić
Br. indeksa:
M 9368/08

Beograd, 2012.

“They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.”

“Oni koji bi se odrekli suštinske slobode da bi stekli malo privremene bezbednosti, ne zaslužuju ni slobodu ni bezbednost.”

Bendžamin Franklin (1706-1790)

Naslov rada: Obezbeđivanje rutiranja i sistema imenovanja domena

Apstrakt: Sistem imenovanja domena (DNS) je temelj na koji se oslanja većina mrežnih aplikacija, kao i sama bezbednost mreže. Međutim, sam sistem nije projektovan da bude bezbedan, što danas predstavlja potencijalno veliku pretnju za bezbednost na mreži, uz pojedince i kriminalne grupe koje iskorišćavaju njegove nedostatke. Predloženo rešenje u vidu bezbednosnih proširenja DNS-a (DNSSEC) rešava neke bezbednosne probleme, uvođenjem u sistem kriptografije javnog ključa, ali samo uz uslov da se pravilno implementira. Konfigurisanje i održavanje zona obezbeđenih DNSSEC-om može biti vrlo kompleksan zadatak. Primenom tehnologija i alata koji su ovde predstavljeni, bezbednost DNS-a se može podići na nivo koji je danas neophodan. Najzad, postoji i pitanje, političko isto koliko i tehničko, kontrole i samim tim moći koju obezbeđivanje DNS-a i Interneta donosi telu koja bi dobilo taj zadatak – pitanje koje u današnjem svetu ima veoma kontroverznu konotaciju. S druge strane, fundamentalni elementi Interneta – nazivi i adrese – su godinama izvor osnovnih strukturalnih slabosti same mreže. Rutiranje podataka na Internetu je zbog ovih slabosti izloženo kako ljudskim greškama tako i potencijalnim napadima zlonamernih pojedinaca i grupa. Iako dobro poznate godinama, ove slabosti tek u skorije vreme počinju da bivaju rešavane u vidu standarda i potencijalno trajnih rešenja. Kao najsveobuhvatnije se nameće rešenje koje predlaže SIDR radna grupa pri IETF, kojim se predviđa efektivno pokrivanje skoro svih poznatih slabih tačaka. Međutim, to rešenje donosi sa sobom i određene promene u funkcionisanju protokola rutiranja, pre svega u smislu administrativne kontrole. Potrebno je pažljivo sagledavanje svih aspekata predloženih rešenja, kako rešenje za jednu vrstu problema ne bi stvorilo probleme potpuno druge vrste.

Ključne reči: Internet, DNS, bezbednost, DNSSEC, BIND, kriptografija javnog ključa, ICANN, DHS, NSA, rutiranje, BGP, BGPsec, RPKI, digitalni potpis, digitalni sertifikat, upravljanje Internetom

Title: Securing routing and Domain Name System

Abstract: The domain name system (DNS) is the foundation on which most network applications, as well as network security, relies. However, the system itself was not designed to be secure, which represents potentially significant threat to online security today, with individuals and criminal groups exploiting the system's shortcomings. Suggested solution in the form of DNS Security Extensions (DNSSEC) resolves some of the problems, incorporating public-key cryptography into the system, but only if properly implemented. Configuration and maintaining of DNSSEC secured zones can be a very complex task. Application of technologies and tools presented in this work can increase security of DNS to a level that is greatly needed today. Finally, there is also the issue, political as much as technical, of control and power that securing of DNS provides to the body that would perform the task – issue that has a very controversial connotation in the world as it is today. On the other hand, the Internet's fundamental elements – names and addresses – were the source of basic structural vulnerabilities in the network for years. Routing on the Internet has been exposed to human errors as well as to potential attacks by malicious individuals and groups. Although well known for years, these weaknesses are being addressed through standards and potentially permanent solutions only lately. A comprehensive solution is proposed by IETF SIDR working group, which effectively encompasses almost all known weak points. However, the proposed solution changes some aspects of routing protocol, principally concerning administrative control. Thorough analysis of all aspects of proposed solutions is required, in order not to allow the solutions for existing problems to create completely different ones.

Keywords: Internet, DNS, security, DNSSEC, BIND, public-key cryptography, ICANN, DHS, NSA, routing, BGP, BGPsec, RPKI, digital signature, digital certificate, Internet governance

Sadržaj

Uvod	- 1 -
1. Sistem imenovanja domena.....	- 3 -
1.1 Struktura DNS-a.....	- 3 -
2. Bezbednosni problemi DNS-a.....	- 6 -
2.1 DNS lažiranje.....	- 7 -
3. Pregled DNSSEC-a.....	- 10 -
3.1 DNSSEC.....	- 10 -
3.2 Funkcionisanje DNSSEC-a	- 10 -
3.3 DNSSEC Lookaside Validation.....	- 13 -
3.4 Problemi DNSSEC-a.....	- 14 -
4. Implementacija DNSSEC-a	- 15 -
4.1 Generisanje kriptografskih ključeva.....	- 15 -
4.2 Potpisivanje zone	- 16 -
4.4 Prelaz između ključeva.....	- 19 -
4.4.1 Zamena ZSK ključa.....	- 19 -
4.4.2 Zamena KSK ključa	- 20 -
4.5 DNSSEC Lookaside Validation.....	- 21 -
5. Budućnost Interneta i DNS-a	- 23 -
5.1 ICANN i administracija DNS-a	- 23 -
5.2 SAD i bezbednost na Internetu	- 24 -
5.2 Alternativni DNS	- 27 -
6. Rutiranje podataka na Internetu	- 28 -
6.1 Osnove rutiranja.....	- 28 -
6.2 BGP protokol	- 29 -
6.3 Format BGP poruka	- 32 -
6.4 Odabir najpovoljnije rute.....	- 33 -
7. Bezbednosni problemi rutiranja	- 34 -
7.1 Tehničke greške	- 34 -
7.2 Lažiranje (<i>spoofing</i>)	- 35 -
8. Bezbednosna rešenja za BGP protokol.....	- 39 -
8.1 Bezbednosna rešenja SIDR radne grupe	- 39 -

8.1.1	Digitalni sertifikati	39 -
8.1.2	Obezbeđivanje prava na korišćenje adresa – RPKI	40 -
8.1.3	Obezbeđivanje porekla oglašavanja rute – ROA	42 -
8.1.4	Obezbeđivanje propagacije ruta – BGPsec.....	45 -
8.1.5	Konfigurisanje rutera za rad sa RPKI	48 -
9.	Budućnost rutiranja i Interneta	50 -
9.1	Autonomija Internet provajdera	50 -
9.2	Model poverenja i kompatibilnost	51 -
	Zaključak	53 -
	Literatura.....	55 -

Uvod

Poslednjih godina, naročito u svetlu terorizma kao pretnje, pitanje bezbednosti je postalo aktuelno u svim sferama života. Kako je Internet postao sastavni deo života većine ljudi, bezbednost komunikacija na njemu je, za razliku od godina u kojem je nastao, postala tema o kojoj se razmišlja i deluje. Da bi se Internet učinio bezbednijim, neophodno je pre svega obezbediti ključne delove njegove infrastrukture. Dva suštinska mehanizma za funkcionisanje Interneta, koje se prepliću i zajedno funkcionišu kao celina u današnjem poimanju Interneta su sistem imenovanja domena (*Domain Name System – DNS*) i rutiranje.

DNS je distribuirana baza podataka o hostovima na Internetu. Njegov zadatak je prevođenje naziva računara u IP adrese i obrnuto. Trenutni (nebezbedni) DNS ne sprečava napadače da modifikuju ili ubacuju DNS podatke. Da bi se obezbedila njegova sigurnost, DNS je proširen ekstenzijama (DNSSEC) koje funkcionišu na principu kriptografije javnog ključa. DNSSec je projektovan da zaštiti DNS od lažiranja podataka (npr. “trovanjem keša” ili preuzimanjem kontrole nad domenima), obezbeđujući njihovu autentičnost i integritet.

Pravilna instalacija, podešavanje i održavanje softvera čiji je zadatak pružanje DNS servisa je temelj za bilo kakvu zaštitu koju bi sistem trebalo da pruža. Takođe, konstantno praćenje inovacija (kao što je *DNSSEC Lookaside Validation*) i njihova implementacija mora biti deo bezbednosne prakse. Na kraju, da bi se maksimalno iskoristile prednosti obezbeđivanja DNS-a, kao i da bi najvažniji zadaci uvođenja bezbednog DNS-a bili ispunjeni, neophodno je da kompletan DNS sistem bude obuhvaćen. Ovo sa sobom povlači mnoge probleme, od kojih je najveći i najvažniji obezbeđivanje DNS *root*-a i kontrola nad *root*-om koju to donosi.

Rutiranje u okviru računarske mreže predstavlja proces odabira putanje duž koje se šalje sav mrežni saobraćaj. Internet, kao najveća, globalna računarska mreža je podeljen na autonomne sisteme i sav saobraćaj među njima se usmerava uz pomoć BGP protokola. Ovaj protokol omogućava decentralizovano usmeravanje podataka, što Internet čini ovakvim kakav je danas – potpuno decentralizovanim sistemom. Kako predstavlja suštinski mehanizam na koji se oslanja Internet, rutiranje predstavlja njegovu potencijalnu slabu tačku. Protokoli rutiranja su generalno, samim tim i BGP protokol, podložni specifičnim pretnjama i napadima koji mogu da naštetite kako pojedinačnim korisnicima tako i radu cele mreže. Malo je poznato da je pojedinim zloupotrebama moguće ostvariti značajnu kontrolu nad tokom saobraćaja na Internetu, bez znanja korisnika.

Predloženo rešenje za obezbeđenje rutiranja na Internetu oslanja se na kriptografiju javnog ključa. Reč je o infrastrukturi javnih ključeva resursa (RPKI) koja bi, uz korišćenje modifikovanih X.509 digitalnih sertifikata, trebalo da omogući autentifikaciju blokova IP adresa i brojeva autonomnih sistema u okviru protokola rutiranja, kao i proveru porekla informacija o ruti. Paralelno uz RPKI, BGPSec mehanizam bi trebalo da omogući proveru propagacije ruta.

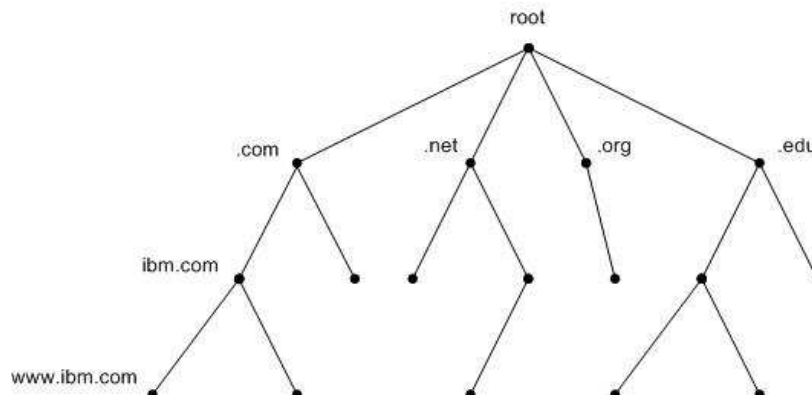
Međutim, važno je primetiti da je u predloženim rešenjima, kako za DNS tako i za rutiranje, jedan od tehničkih uslova koji se moraju ispuniti za njegovu primenu – centralizacija. U oba slučaja, ovom centralizacijom je predviđeno da autoritet za primenu obezbeđivanja bude institucija koja već ima administrativnu kontrolu nad raspodelom adresnih resursa na Internetu. Uzimajući u obzir sva poboljšanja koje bi obezbeđivanje moglo da donese, mora se postaviti pitanje mudrosti ovakve odluke, jer mehanizmi DNS-a i rutiranja nisu samo tehnička, već i institucionalna, ekonomska i politička pitanja od globalnog značaja.

1. Sistem imenovanja domena

1.1 Struktura DNS-a

DNS je globalna, hijerarhijska i distribuirana baza podataka. Ova baza podataka, koja se čuva na serverima naziva, povezuje kanonička imena, koja koristimo kao nazive domena, sa određenim podacima koji se nazivaju zapisi resursa (*Resource Records* – RRs). Zapisi koji se odnose na naziv domena mogu biti različitih tipova, ali je tip *adresa* najčešći. Skup zapisa resursa istog tipa se označava kao *Resource Record Set* (RRSet).

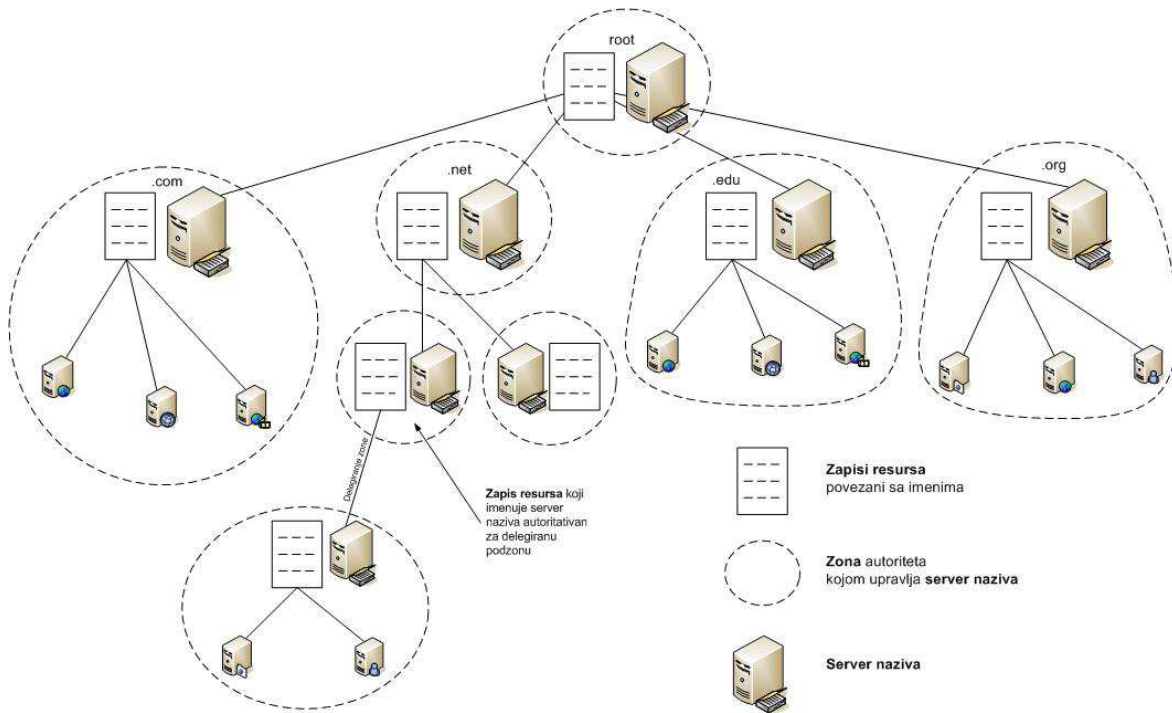
Pošto nazivi domena moraju da budu globalno jedinstveni, koristi se hijerarhijski princip davanja imena. Naziv domena se odnosi na jedan čvor u stablu koje nazivamo adresni prostor domena (*domain name space*). Ovo stablo naziva domena (slika 1.1.1) je vrlo slično fajl sistemu *Windows* ili *Linux* operativnog sistema. Svako podstablo se naziva domenom. Na primer, podstablo sa korenom u *.com* čvoru se naziva *.com* domenom i obuhvata sve nazive domena koji se završavaju sa *.com*. Čvorovi koji su direktni potomci (*child*) korenog čvora se nazivaju domeni najvišeg nivoa (*Top Level Domain* – TLD).



Slika 1.1.1 Stablo naziva domena

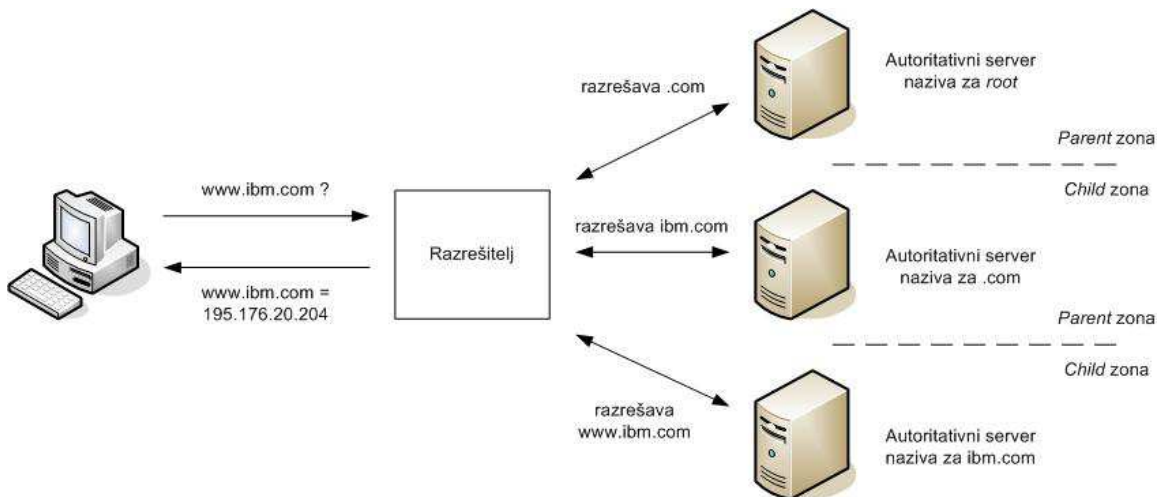
Komunikacija sa DNS bazom podataka prati klijent-server arhitekturu. Stablo naziva domena je podeljeno u zone, koje predstavljaju susedne delove stabla. Zone se određuju procesom delegiranja kojim se nekoj organizaciji daje odgovornost upravljanja pojedinim poddomenima. Zona može da sadrži informacije o domenima i njihovim poddomenima. Zone najvišeg nivoa, kao što je *.edu*, uglavnom sadrže informacije o delegiranju.

Za svaku zonu postoje autoritativni serveri (serveri naziva) koji odgovaraju na upite vezane za nazive domena u toj zoni. Serveri naziva mogu biti autoritativni i za više zona. Klijentski program za pristup DNS-u se naziva razrešitelj (*resolver*). Kada razrešitelj primi upit, on ga prvo prosleđuje jednom od *root* DNS servera koji opslužuju *root* domen. Kao odgovor, dobija se sledeći server u nizu koji je “bliži” autoritativnom serveru iz traženog upita.



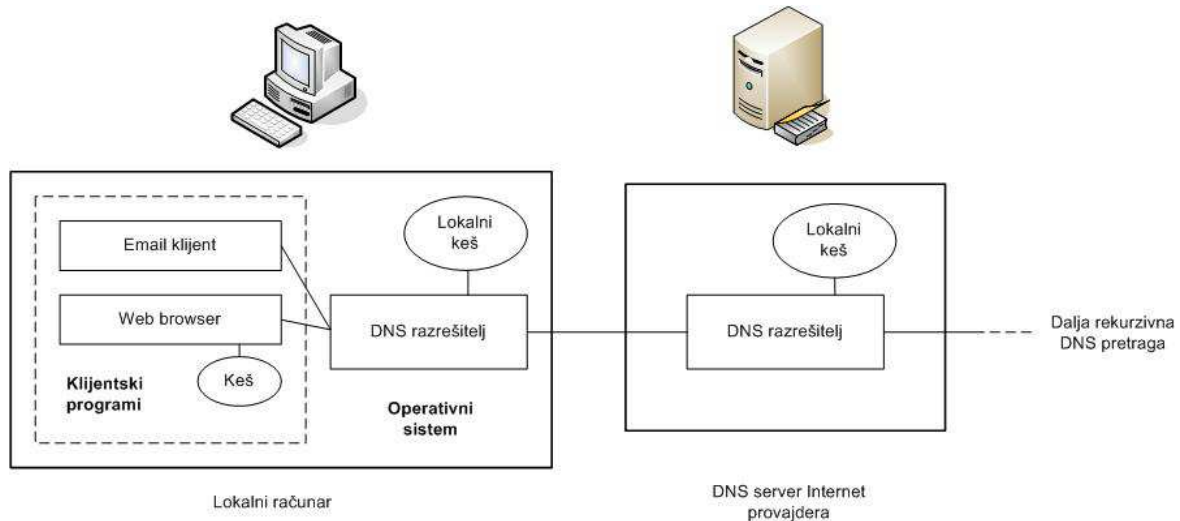
Slika 1.1.2. Adresni prostor domena

Na primeru na slici 1.1.3, razrešitelj prima upit za IP adresom za *www.ibm.com*. Razrešitelj potom prosleđuje upit *root* DNS serveru, koji kao odgovor vraća IP adresu DNS servera koji je autoritativan za *.com* zonu. Razrešitelj zatim šalje upit serveru naziva koji je autoritativan za *.com* i kao odgovor dobija IP adresu servera naziva autoritativnog za *ibm.com*. Konačno, kontaktira se DNS server za *ibm.com* koji šalje IP adresu za *www.ibm.com* za koju je i autoritativan. Ovaj odgovor se zatim vraća klijentu koji je poslao upit. Ovaj celokupni proces se naziva razrešavanje (*resolving*).



Slika 1.1.3. Razrešavanje DNS upita

Radi ubrzanja razrešivanja upita, kao i rasterećenja servera naziva na svim nivoima, koristi se tehnika keširanja rezultata upita, koji se čuvaju u memoriji određeno vreme.



Slika 1.1.4. Keširanje DNS podataka

Root serveri su od suštinskog značaja za funkcionisanje DNS sistema. Postoji 13 različitih root servera (slika 1.1.5) koji su, uz višestruku replikaciju, razmešteni po celom svetu. Uz njih, koriste se tehnike keširanja da bi se smanjio saobraćaj i broj zahteva kao i ubrzao proces razrešavanja. Kao posledica, svaki zapis resursa koji se dobije od DNS servera poseduje određeni životni vek (*time-to-live* – TTL) koji predstavlja vreme u kojem se taj zapis resursa može keširati.



Slika 1.1.5. Geografske lokacije svih root servera (Jul 2012)¹.

¹ Izvor: root-servers.org

2. Bezbednosni problemi DNS-a

Po svojoj prirodi, DNS je javni sistem, što ga čini vrlo privlačnim za zlonamerne korisnike Interneta. Postoji više aspekata kroz kojih se bezbednost DNS-a može posmatrati, od relativno jednostavnih do veoma kompleksnih. Da bi shvatili napade kojima je ovaj sistem svakodnevno izložen, moramo identifikovati sve aspekte sistema koje takvim korisnicima mogu poslužiti kao potencijalne tačke pristupa. Oni se suštinski mogu modeliti u četiri grupe:

- Administrativna bezbednost: Tiče se fizičke bezbednosti, dozvola za pristup fajlovima, konfiguracije servera, podešavanja DNS softvera (najčešće BIND-a) i sl. Administrativna bezbednost predstavlja osnovu odbrane sistema. Nijedna kriptografska tehnika ne vredi ako je osnovni sistem nestabilan ili dozvoljava neograničen pristup interesantnim fajlovima.
- Transferi zone: Predstavlja jedan od mehanizama koji administratorima omogućavaju repliciranje baze podataka sa DNS podacima. Transferi zone imaju nekoliko potencijalnih bezbednosnih problema, ali se oni lako rešavaju pravilnim podešavanjem DNS softvera.
- Dinamičko ažuriranje: Izlaže *master* fajl zone mogućem oštećenju, uništenju ili trovanju. Predostrožnosti u ovoj proceduri obuhvataju dobro projektovanje sistema, parametri DNS softvera (najčešće BIND-a), zaštitne barijere (*firewall*) i autentifikacija.
- Integritet zone: Ako je neophodno da podaci u zoni koju koristi DNS ili krajnji host budu apsolutno ispravni (tj. da odgovori na upite nisu menjani i da podaci koji se vraćaju zaista potiču od vlasnika zone), mora se koristiti DNSSEC. Njegova druga generacija, pominjana i kao *DNSSEC.bis*, predstavlja rezultat zajedničkog truda IETF²-a, *root* server operatera kao i regionalnih Internet registara.

Postoji nekoliko različitih klasa pretnji po DNS, od kojih su većina slučajevi opštih problema reflektovani na DNS, ali su neke specifične za osobenosti njegovih protokola. 1983. godine, kada je napisana prva implementacija sistema, bezbednost je bila tema koja je bila mnogo manje aktuelna nego danas. Tada je jedino bilo važno da se usled stalnog rasta mreže uspostavi skalabilan sistem koji će funkcionisati, dok se o bezbednosti nije mnogo razmišljalo. Razvojem Interneta u ono što predstavlja danas, služeći kao sredstvo komunikacije privatnim korisnicima, komercijalnom sektoru i državnim institucijama, DNS je postao meta zloupotreba. Najveću pretnju za integritet sistema predstavlja lažiranje DNS podataka.

² *Internet Engineering Task Force*. Razvija i promoviše *Internet* standarde, blisko sarađujući sa W3C i ISO/IEC.

2.1 DNS lažiranje

Lažiranje DNS podataka predstavlja promenu mapiranja naziva nekog domena sa legitimne IP adrese na adresu koju odabere napadač.

Opšti oblik lažiranja izgleda ovako:

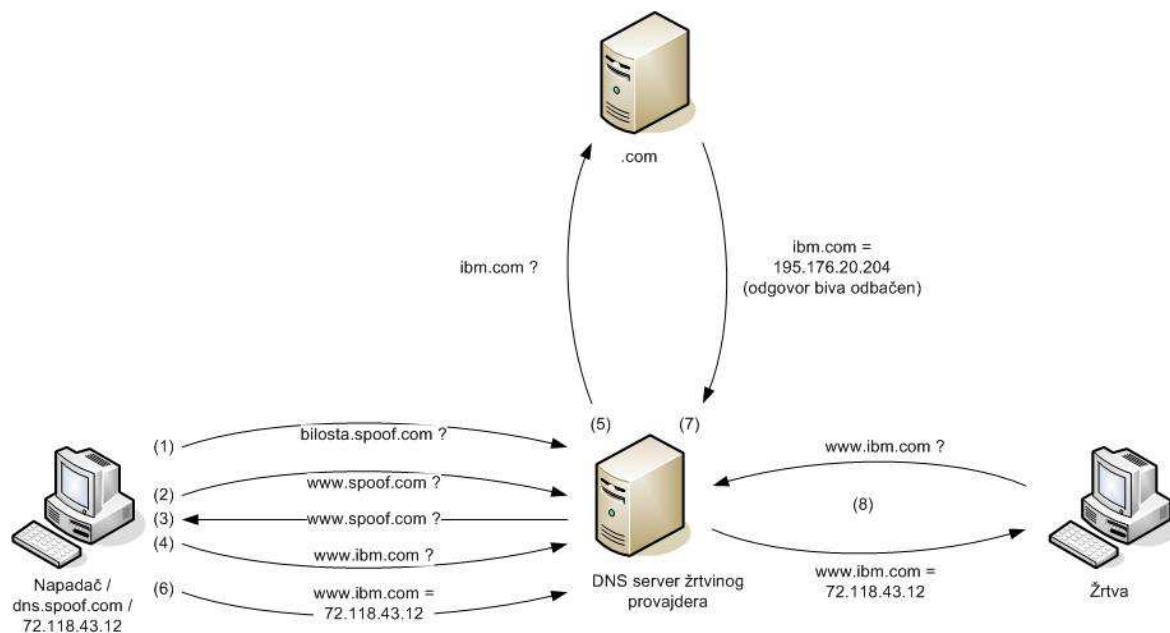
- Žrtva šalje upit, možda i na podsticaj od strane napadača ili neke treće strane; u nekim slučajevima sam upit može biti nepovezan sa nazivom koji se napada (tj. napadač samo koristi ovaj upit kao način da ubaci lažne informacije o nekom drugom nazivu).
- Napadač ubacuje odgovor, bilo putem presretanja paketa, pogađanja upita ili time što je legitimni server naziva koji je u nekom trenutku uključen u proces odgovaranja na upit koji je žrtva poslala.
- Napadačev odgovor sadrži jedan ili više zapisa resursa sa DNS nazivima u polju RDATA; u zavisnosti od toga kog je određenog oblika ovaj napad, cilj može biti da se ubace lažni podaci povezani sa tim nazivima u keš žrtve preko *Additional* dela ovog odgovora ili da se sledeća faza upita preusmeri na server koji određuje napadač (da bi se ubacili kompleksniji lažni podaci u žrtvin keš a koji mogu lako da stanu u jedan odgovor ili da bi se lažni podaci ubacili u *Authority* ili *Answer* delove odgovora gde će imati veće šanse da prevare razrešitelj).

Detaljan prikaz mogućeg scenarija DNS lažiranja dat je na slici 2.1.1. Napadač može da natera DNS server žrtvinog provajdera da pošalje zahtev za traženje adrese *www.ibm.com*. Zbog korišćenja UDP protokola, DNS server ne može da potvrdi od koga je dobio odgovor. Napadač to može da iskoristi falsifikujući očekivani odgovor i da tako ubaci drugu IP adresu u keš DNS servera.

Važno je napomenuti da svaki zahtev nosi redni broj, na osnovu koga server povezuje odgovore sa zahtevima. Da bi saznao tekući redni broj, on može da registruje domen *spoof.com*, sa adresom *72.118.43.12*. Za svoj domen napadač pravi i DNS server *dns.spoof.com*, koji ima istu adresu s obzirom da se radi o istoj napadačevoj mašini.

Prvi korak je da se od žrtvinog servera naziva traži adresa računara *bilosta.spoof.com* (1), što će kao rezultat dovesti do slanja upita autoritativnom serveru naziva za *.com* i unošenja napadačevog DNS servera u keš, kao autoritativnog za taj domen. Napadač zatim od servera naziva provajdera traži adresu *www.spoof.com* (2). Server naziva provajdera taj zahtev, naravno, šalje napadačevom DNS serveru (3). Taj zahtev nosi redni broj koji je napadaču potreban. Sledećeg trenutka, napadač šalje nov zahtev, ovaj put za *www.ibm.com* (4) i istog trenutka odgovara na sopstveni zahtev, šaljući serveru naziva falsifikovani odgovor (6) u ime servera autoritativnog za *.com*: *www.ibm.com = 72.118.43.12*. Taj falsifikovani odgovor nosi redni broj za jedan veći od broja koji je prethodno primljen. Iako je provajderov server naziva u međuvremenu poslao upit serveru naziva autoritativnog za *.com* (5), napadačev odgovor sa ispravnim rednim brojem će stići pre njegovog odgovora, i napadačev odgovor biva keširan, dok pravi odgovor biva odbačen (7) kao netražen.

Na kraju, kada odabrana žrtva ili bilo ko drugi ko u tom trenutku koristi server naziva istog provajdera zatraži adresu lokacije *www.ibm.com* (8), biće usmeren na napadačevu mašinu, gde ih može dočekati lažni *web* server.



Slika 2.1.1. DNS lažiranje

Zajedničko za sve napade lažiranjem je da poruke odgovora dozvoljavaju napadaču da unese proizvoljne DNS nazive i da obezbedi dodatne informacije za koje napadač tvrdi da su povezane sa ovim nazivima; izuzev ako žrtva zna prave podatke koji su vezani za ove nazive, biće vrlo teško odbraniti se od ovakvog napada.

Ova vrsta napada je naročito podmukla s obzirom na to da je napadaču vrlo lako da isprovocira žrtvu da pošalje upit za određeni naziv po napadačevom nahođenju, na primer postavljanjem linka u grafiku veličine 1x1 piksela (*web bug*³) koja je deo Text/HTML *email* poruke upućene žrtvi. Ako žrtvin program za čitanje pošte pokuša da prati taj link, rezultat će biti DNS upit za naziv koji je odabrao napadač.

Jula 2008, objavljeno je da ova slabost može predstavljati mnogo veći problem nego što je do tada bio. Opšti pristup problemu ostaje isti, ali razlika nastaje u sadržini falsifikovanog odgovora. Umesto da se lažira samo jedan odgovor, tj. zapis resursa sa IP adresom domena, otkriveno je da je moguće oteti kontrolu nad kompletnom zonom. Napad počinje tako što se od servera naziva traži razrešavanje nekog poddomena u okviru domena koji se napada (npr. *www12345.google.com*). Kako server naziva ne može da pronađe traženi poddomen u svojim zapisima a ni u kešu, on prosleđuje zahtev serveru višeg nivoa. Napadač ovaj put falsifikuje odgovor sa *Authority* delom (deo paketa u DNS komunikaciji), u kome se navodi da odgovor nije poznat, ali da server može da se obrati na priloženu IP adresu. Na toj adresi napadač podiže sopstveni DNS server, i konfiguriše ga da bude autoritativan za *google.com*. Ako DNS server

³ Objekat koji se postavlja u *web* stranu ili *email* poruku, obično nevidljiv za korisnika, koji pokreće neki zahtev za dohvaćanje sa *Interneta* i time, neizbežno, slanje DNS upita.

prihvati falsifikovani odgovor, ta IP adresa će biti uneta u keš i svi dalji upiti za domene u okviru *google.com* biće preusmereni na napadačevu mašinu. Ovaj napad je izuzetno opasan jer napadač na ovaj način stiče autoritet nad kompletnom zonom, sa istim privilegijama kao da je njen vlasnik, i u stanju je da kontroliše sve što je u vezi sa razrešavanjem preko tog servera naziva. Sve posle ovoga postaje trivijalno – napadač može preusmeriti *web* saobraćaj na sopstveni sajt ili rutirati svu elektronsku poštu na svoj *mail* server.

U novim verzijama većine softvera koji se koristi na DNS serverima mogućnosti za lažiranje podataka u kešu su u dobroj meri oslabljene, uvođenjem novih praksi (odabir slučajnih vrednosti za ID brojeve upita kao i za port koji se koristi). Međutim, trajno rešenje za problem lažiranja podataka će najverovatnije predstavljati predloženi standard za bezbednosno proširenje DNS-a, koji u sistem uvodi kriptografiju javnog ključa – DNSSEC.

DNSSEC obezbeđuje dobru odbranu od većine varijacija ovog napada. Proveravanjem potpisa, razrešitelj može da odredi da li su podaci vezani za neki naziv zaista uneseni od strane delegiranog autoriteta za taj deo DNS adresnog prostora. Preciznije, razrešitelj može da odredi da li je strana koja je unela podatke imala pristup navodno tajnom ključu čiji se odgovarajući javni ključ pojavljuje na očekivanoj lokaciji u DNS adresnom prostoru sa očekivanim lancem *parent* potpisa koji počinju javnim ključem koji razrešitelj već poznaje.

DNSSEC potpisi ne pokrivaju *glue*⁴ zapise, tako da i dalje postoji mogućnost napada lažiranjem koji obuhvata *glue*, ali uz pomoć DNSSEC-a je moguće otkriti ovaj napad privremeno prihvatajući *glue* da bi se preuzele potpisane autoritativne verzije istih podataka i provere njihovih potpisa.

⁴ Serveri naziva se u delegiranjima pojavljuju u formi naziva, a ne u formi IP adrese. Ovo znači da razrešitelj mora da pošalje još jedan DNS zahtev da bi saznao IP adresu servera na koji je upućen. Pošto ovo može da dovede do kružne zavisnosti (*circular dependency*) ako je server naziva na koji se upućuje ispod domena za koji je autoritativan, povremeno je neophodno da server naziva koji delegira obezbedi i IP adresu narednog servera naziva. Ovaj zapis se naziva *glue* zapis.

3. Pregled DNSSEC-a

3.1 DNSSEC

DNSSEC je predloženi standard koji modifikuje zapise resursa i protokole DNS-a da bi se obezbedila sigurnost za transakcije između razrešitelja i servera naziva. Uvođenjem podataka koji su kriptografski potpisani javnim ključem u DNS uz pomoć četiri nova zapisa resursa, DNSSEC obezbeđuje:

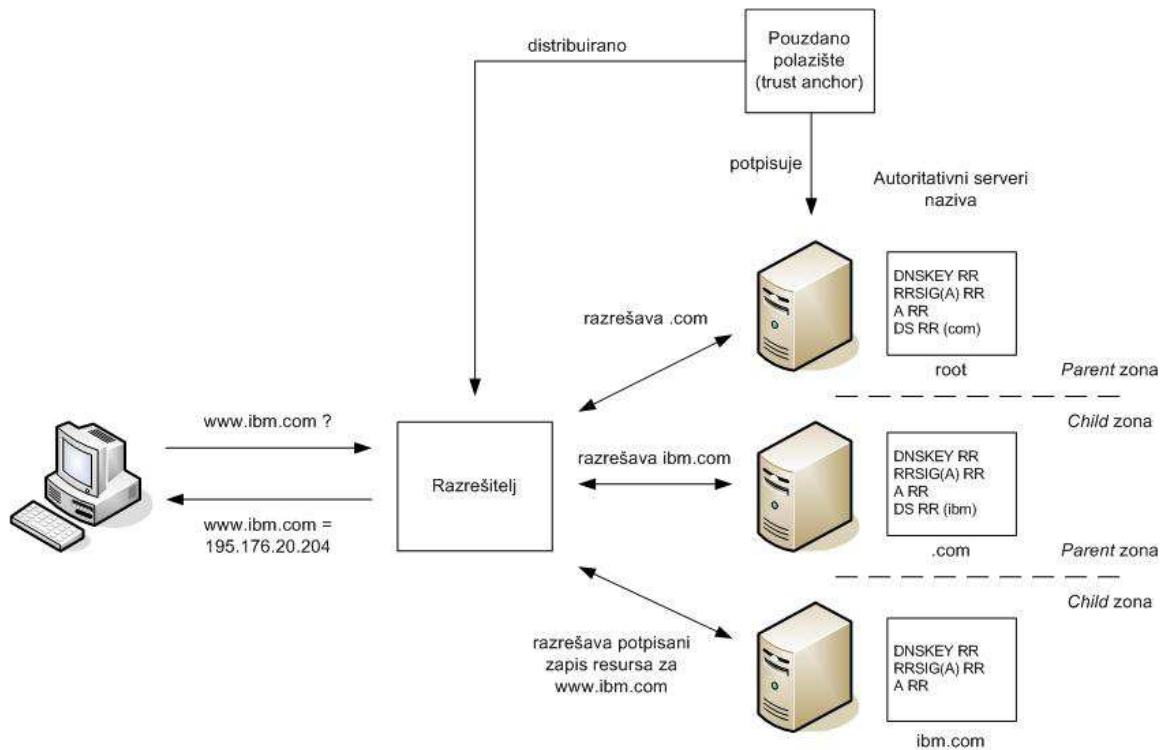
- Autentičnost izvora: Razrešitelj može da odredi da li odgovor potiče od autoritativnog servera naziva određene zone.
- Verifikaciju integriteta: Razrešitelj može da odredi da li je odgovor menjan u toku prenosa.
- Autentično poricanje postojanja: Razrešitelj može da potvrdi da je određeni upit nerazrešiv, ako ne postoji zapis resursa DNS-a na autoritativnom serveru naziva.

3.2 Funkcionisanje DNSSEC-a

DNSSEC je osmišljen da zaštiti razrešitelje od lažiranih DNS podataka, kao što je slučaj pri “trovanju” DNS keša. Svi odgovori u DNSSEC-u koji se šalju su digitalno potpisani. Proverom digitalnih potpisa, razrešitelj može da proveriti da li je primljena informacija identična (tačna i kompletna) kao informacija na autoritativnom serveru naziva.

DNSSEC uvodi četiri nova tipa zapisa resursa: Potpis zapisa resursa (RRSIG), DNS Javni ključ (DNSKEY), Potpisnik delegiranja (DS) i Sledeći bezbedan (NSEC).

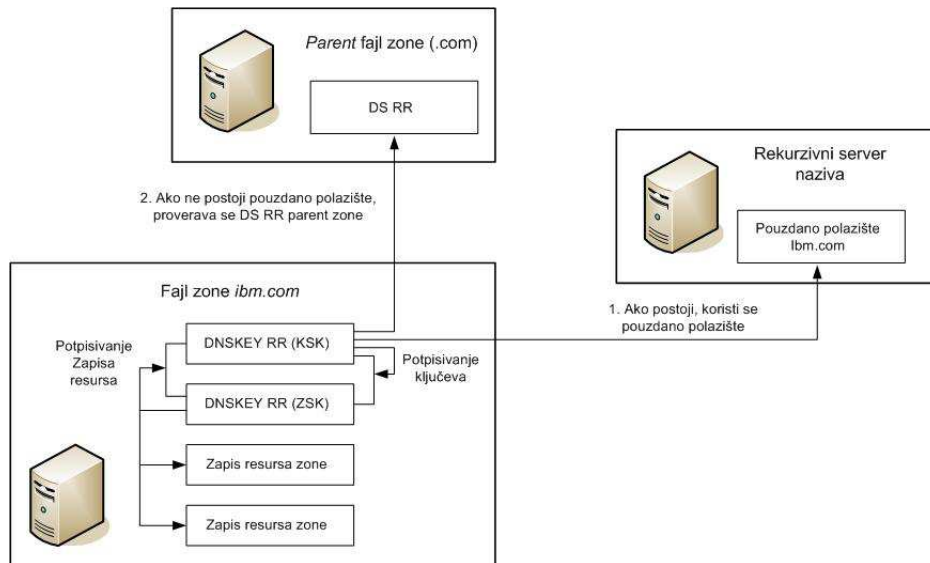
DNSSEC Server naziva za određenu zonu drži Potpis zapisa resursa (RRSIG) za različite skupove zapisa resursa (RRset) koje se na njemu drže. RRSIG predstavlja digitalni potpis koji se formira uzimanjem *hash*-a određenog skupa zapisa resursa u zoni i njegovom enkripcijom uz pomoć privatnog ključa iz kompleta kriptografskih ključeva administratora te zone. Odgovarajući javni ključ iz ovog kompleta se čuva u zapisu DNSKEY. Po primanju potpisanog DNS odgovora od servera naziva, DNSSEC razrešitelj dešifruje RRSIG uz pomoću javnog ključa zone. Razrešitelj zatim generiše *hash* RRset dela odgovora i upoređuje ga sa *hash*-om dobijenim iz RRSIG dela odgovora. Na taj način se potvrđuje ili negira integritet i autentičnost porekla različitih tipova informacija.



Slika 3.2.1. DNSSEC upit i odgovori

Kako razrešitelj dolazi do autentičnog DNSKEY ključa za određenu zonu? Zapis resursa Potpisnik delegiranja (DS) se obezbeđuje od strane *parent* zone i predstavlja tačku delegiranja između *parent* i *child* zona koja se može autentifikovati. Da bi potvrdio DNSKEY *child* zone, razrešitelj preuzima odgovarajući DS, RRSIG(DS) i DNSKEY *parent* zone. DS se verifikuje pomoću dešifrovanog RRSIG(DS) i zatim se DS podaci koriste za autentifikaciju DNSKEY podatka *child* zone. Na ovaj način, potpisani DS funkcioniše kao “sertifikat” koji se autoritativno isporučuje iz *parent* zone i vezuje *child* zonu za svoj DNSKEY. Server naziva iz *parent* zone postaje, praktično, “pouzdanost treće lice”, koje olakšava razmenu DNS informacija između razrešitelja i *child* zone. Niz ovakvih delegiranih odnosa formira lanac autentifikacije, koji predstavlja putanju koju razrešitelj može da prati od javnog ključa (tj. pouzdanog polazišta – *trust anchor*) DNS *root*-a. Na kraju, Sledeći bezbedan (NSEC) zapis resursa povezuje potpisane resurse, omogućavajući razrešitelju da pretražuje fajl zone i da odredi da li određeni domen postoji u DNS-u.

Ovde je važno napomenuti da se u praksi koriste dva tipa kriptografskih ključeva po zoni, ključevi za potpisivanje zone (*Zone Signing Keys* – ZSK) i ključevi za potpisivanje ključeva (*Key Signing Keys* – KSK). Tajni ZSK ključ se koristi za potpisivanje svih podataka zone i njegov odgovarajući javni ključ se objavljuje u vidu DNSKEY zapisa. Javni KSK ključ se takođe pojavljuje kao DNSKEY zapis, ali se njegov tajni ključ koristi samo za potpisivanje DNSKEY zapisa.



Slika 3.2.2. Potpisivanje ZSK i KSK ključevima

Dva različita ključa se koriste iz bezbednosnih razloga. Opšte pravilo u kriptografiji je da što se više podataka šifruje određenim ključem, opasnost da se ključ sazna postaje sve veća. U ovom slučaju u pitanju je tajni ključ. U DNS-u se taj ključ koristi za potpisivanje velike količine podataka jer svaka promena u zoni zahteva ponovno potpisivanje. Što je zona veća, to ima više podataka koji su dostupni za kriptanalizu. Iz tog razloga, praksa je da se ZSK ključevi menjaju relativno često. Kada bi se koristio samo jedan ključ, svaki put kada bi se on menjao, bilo bi neophodno slati DNSKEY *parent* zoni kako bi se u njoj zamenio i ponovo potpisao DS zapis za tu zonu. Da bi se ovo izbeglo, koriste se dva odvojena tipa ključeva, i *parent* zonu je potrebno kontaktirati samo pri promeni KSK ključeva, što se čini relativno retko (njime se potpisuje vrlo malo podataka). Održavanje jake bezbednosti sistema ovime postaje lakše i brže.

DNSKEY fajl (sa samim ključem u *Base64* formatu) izgleda ovako:

```
godfather.rs. IN DNSKEY 257 3 5
AwEAAeYqX0+Qw2JuhvRLLohkqIQ1F0laSn7KlwnU+kSA4ee3Wgu3yTVZ
+Eit1nh0I6sw26HyXGnVJyOg820JfegFfne90EZQ0wrzvVaIGerh127A
S2tRTJNJ1yysK8ZCA4aVCMRgO/9Aqr5L405k6YaE297Vy6IyEyqM6t6F zQ5HZ819
```

Polje koje ovde ima vrednost 257 je bitno za razlikovanje tipova ključeva. Dužine je 2 bajta, i u njemu je moguće postaviti SEP (*Secure Entry Point*) indikator. Ako je SEP indikator postavljen, to označava da je u pitanju KSK.

DNSSEC koristi i tri indikatora u DNS porukama – DO, AD i CD.

DO (*DNSSEC OK*) indikator se koristi zbog veličine DNS poruka. Veličina DNS poruke originalno je ograničena veličinom UDP paketa – 512 bajta. Ako bi se RRSIG zapisi prenosili ovakvim putem, dosta poruka bi bilo prekinuto pre kraja. Uveden EDNS0 ekstenzijom DNS-a⁵, DO indikator označava da razrešitelj podržava DNSSEC i da treba poslati takve zapise u

⁵ EDNS0 omogućava korišćenje UDP poruka dužine do 4,096 bajta. Esencijalan je za korišćenje DNSSEC-a

odgovoru. Ovim se izbegava slanje nepotrebnih poruka kao odgovor razrešiteljima koji ne koriste DNSSEC. Ovaj indikator se uvek pojavljuje u posebnom delu poruke:

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
```

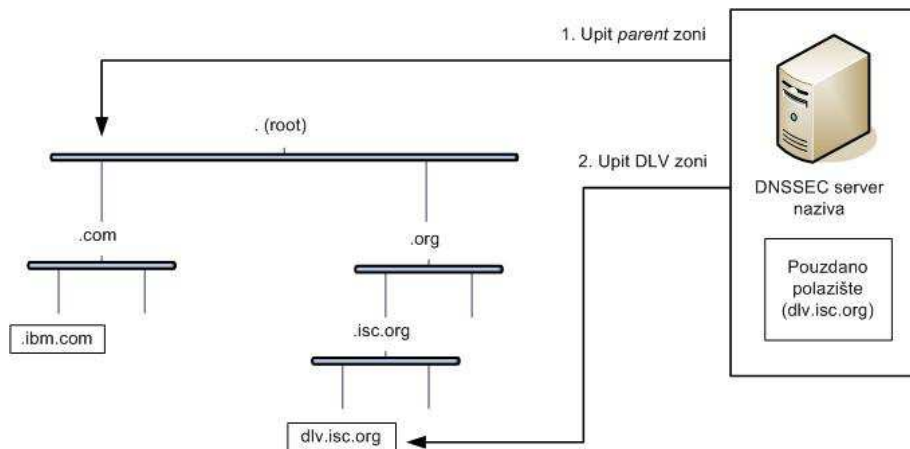
AD (*Authenticated Data*) se postavlja od strane servera naziva i označava da je server proverio sve zapise resursa koje šalje u odgovoru.

CD (*Checking Disabled*) se postavlja od strane razrešitelja, i označava da razrešitelj može samostalno da proverava DNSSEC zapise i da server to ne mora da radi.

3.3 DNSSEC Lookaside Validation

U vreme pisanja ovog rada (jun 2009.) *root* kao i većina TLD domena još uvek nisu potpisani. Jedini način za proveru potpisanih zona je održavanje obimne prekonfigurisane liste pouzdanih polazišta. Održavanje ovakve liste na svakom razrešitelju koji podržava DNSSEC predstavlja značajan problem.

DNSSEC Lookaside Validation (DLV) predstavlja alternativni metod za uspostavljanje i proveru lanca poverenja. Njime je moguće postaviti pouzdana polazišta van lanca delegiranja koji koristi DNS, tj. dozvoliti razrešiteljima da verifikuju potpisane DNS podatke zona čije *parent zone* nisu potpisane. Da bi se ovo postiglo, uveden je pojam “DLV domena” u kojima se objavljuju bezbedne tačke pristupa za zone koje nisu njegove *child zone*. One bivaju objavljene u vidu DLV zapisa resursa koji je u svemu identičan sa DS zapisom resursa, efektivno ga zamenjujući.



Slika 3.3.1 Verifikacija putem DLV-a

Na primeru na slici 3.3.1, koristi se jedan od DLV registara na Internetu (*dlv.isc.org*) a proverava se potpisana zona *ibm.com*. U slučaju da se ne pronađe pouzdano polazište u konfiguraciji softvera, server naziva će potražiti DS zapis resursa za *.com* zonu. Pošto takav zapis ne postoji, ovakav domen bi bio označen kao nebezbedan. DLV omogućava još jedan korak, slanje upita *lookaside* zoni (za koju postoji pouzdano polazište) radi dobijanja DLV

zapisa resursa zone koja se verifikuje. Kada server naziva utvrdi da je *lookaside* funkcija omogućena (opcijom u konfiguracionom fajlu), poslaće DLV upit za domen *ibm.com.dlv.isc.org* i ako bude pronađen, *ibm.com* zona biva verifikovana kao bezbedna. *Lookaside* zona *dlv.isc.org* mora biti potpisana, jer je definisana kao pouzdano polazište, dok njegova *parent* zona *.isc.org* ne mora da bude potpisana.

Osim pomenutog *Internet Systems Consortium*-ovog registra, od februara 2009. je aktivan i *Interim Trust Anchor Repository*⁶ (u beta fazi) koji održava IANA. Ovaj registar je postavljen sa ciljem da replicira informacije koje bi bile postavljene u *root* zoni da je ona potpisana i sadrži DS zapise za domene najvišeg nivoa. IANA planira da ga koristi sve do potpisivanja *root* zone.

3.4 Problemi DNSSEC-a

Pored brojnih bezbednosnih prednosti koje donosi, DNSSEC se suočava sa sopstvenim problemima:

- Da bi ostali pouzdani, javni i tajni ključevi koji se koriste za potpisivanje *root* servera moraju biti periodično menjani. Proces promene ovih ključeva i njihova bezbedna distribucija na Internetu je vrlo težak zadatak.
- DNSSEC značajno povećava veličinu DNS paketa u odgovoru; između drugih stvari, ovo čini DNSSEC DNS servere još efektivnijim kao pojačavače DoS napada.
- Provera odgovora DNSSEC-a povećava opterećenje razrešitelja, jer DNSSEC razrešitelj treba da izvrši validaciju potpisa i u nekim slučajevima treba da pošalje dodatne upite. Ovo povećanje opterećenja povećava i vreme potrebno da se pošalje odgovor originalnom DNS klijentu, što u nekim slučajevima može da dovede do *timeout*-a i ponovnog slanja upita.
- Kao i sam DNS, model poverenja DNSSEC-a je skoro potpuno hijerarhijski. Dok DNSSEC dozvoljava razrešiteljima da saznaju javne ključeve van grupe onih koji se odnose na *root*, *root* ključ je onaj koji je zaista važan. Stoga bi bilo kakav kompromis u bilo kojoj zoni između *root*-a i određenog naziva mogao da naruši sposobnost DNSSEC-a da zaštiti integritet podataka vlasnika naziva.
- DNSSEC ima specifične zahteve za vremensku sinhronizaciju između razrešitelja koji proverava i strane koja vrši DNSSEC potpisivanje. Pre DNSSEC-a, svi postupci povezani sa vremenom u DNS-u su mogli biti obavljani od strane mašine koje je radila samo sa “proteklom” ili “relativnim” vremenom. Zbog toga što je period validnosti DNSSEC potpisa baziran na “apsolutnom” vremenu, razrešitelj koji proverava mora koristiti isti koncept apsolutnog vremena kao i potpisnik zone, da bi se odredilo da li je potpis u okviru svog perioda validnosti ili je istekao. Napadač koji može da promeni razrešiteljevo poimanje apsolutnog vremena može da ga prevari koristeći potpise koji su istekli. Takođe, napadač koji može da promeni poimanje trenutnog apsolutnog vremena potpisnika zone, može da prevari potpisnika zone na taj način da generiše potpise čiji se period validnosti ne poklapa sa onim što je potpisnik nameravao.

⁶ <https://itar.iana.org/>

4. Implementacija DNSSEC-a

Da bi DNSSEC bio uspešno implementiran, neophodno je adekvatno podesiti softver koji obavlja posao servera naziva. Kao primer će poslužiti konfigurisanje BIND (*Berkeley Internet Name Domain*) DNS softvera, koji se koristi na većini servera naziva na Internetu. Njegova aktuelna verzija (BIND 9) je napisana potpuno od nule, a jedan od razloga za to je upravo dodavanje podrške za DNSSEC. Biće opisani samo delovi vezani za DNSSEC. Kompletan opis sa svim podešavanjima bi zauzeo isuviše prostora i nije tema ovog rada. Podrazumeva se predznanje o opštim mogućnostima paketa kao i o njegovoj instalaciji i podešavanju za uobičajeni rad (nebezbedan DNS).

4.1 Generisanje kriptografskih ključeva

Kao primer će biti korišćeno obezbeđivanje zone *godfather.rs*, čiji fajl zone izgleda ovako:

```
$TTL 6h
godfather.rs.      IN SOA      ns1.godfather.rs. hostmaster.godfather.rs. (
                                1
                                10800
                                3600
                                604800
                                86400 )
;
; Serveri naziva
;
godfather.rs.      IN NS       ns1.godfather.rs.
;
; Adrese za kanonicka imena
;
ns1.godfather.rs.  IN A        192.168.1.251
media.godfather.rs. IN A        192.168.1.201
proxy.godfather.rs. IN A        192.168.1.220
```

Da bi se zona obezbedila, potrebna su dva kriptografska ključa, ZSK i KSK. ZSK ključ će biti formiran uz pomoć *dnssec-keygen* alata, koji je deo paketa BIND:

```
> dnssec-keygen -a rsasha1 -b 1024 -n zone godfather.rs
Kgodfather.rs.+005+19860
```

Opcija *-a* označava da treba koristiti RSA/SHA-1 algoritam, što je obavezno. Opcija *-b* definiše dužinu ključa koga treba generisati⁷, u ovom slučaju 1024. *-n* označava tip ključa (ključ zone). Program će po generisanju ključeva prikazati njihov naziv sa oznakom algoritma (005 je RSA/SHA-1) i identifikatorom ključa (19860) koji služi za razlikovanje različitih ključeva ako u istoj zoni postoji više njih. Javni ključ će biti upisan u fajl *Kgodfather.rs.+005+19860.key* dok će tajni ključ biti upisan u fajl *Kgodfather.rs.+005+19860.private*.

Zatim će biti formiran KSK ključ. Sintaksa je slična prethodnoj komandi, osim što se koristi i opcija *-f KSK*, koja ukazuje da treba postaviti SEP indikator:

```
> dnssec-keygen -a rsasha1 -b 1024 -f KSK -n zone godfather.rs  
Kgodfather.rs.+005+26527
```

Kao rezultat se dobijaju odgovarajući javni (*Kgodfather.rs.+005+26527.key*) i tajni (*Kgodfather.rs.+005+26527.private*) KSK ključevi.

4.2 Potpisivanje zone

Pre nego se pristupi potpisivanju zone, neophodno je javne KSK i ZSK ključeve uneti u fajl zone:

```
[...]  
godfather.rs. IN DNSKEY 257 3 5  
AwEAAeYqX0+Qw2JuhvRLLohkqIQlF0laSn7KlwnU+kSA4ee3Wgu3yTVZ  
+Eit1nh0I6sw26HyXGnVJy0g820JfegFfne90EZQ0wrzvVaIGerhl27A  
S2tRTJNJ1yysK8ZCA4aVCMRg0/9Aqr5L405k6YaE297Vy6IyEyqM6t6F zQ5HZ819  
  
godfather.rs. IN DNSKEY 256 3 5  
AwEAAARuUlw2DF7GLfYBxXR6rjqV6ZQCS7Jb7/YMw7SVCmlfEgd1xgqT  
6sA3Ve6CRhkndVsg2FJQJjQSCRWsoJXlBRITeI/MFRxrWDQ9fRM0PvDr  
WofxK4V19NjoHZE/51twFQUppikmluLBNyMEakuPp0CSKp8qZe10owe/ Zwry7Jql
```

Zatim se može pristupiti samom potpisivanju, uz pomoć alata *dnssec-signzone*, takođe delu paketa BIND:

```
> dnssec-signzone -o godfather.rs. db.godfather.rs  
db.godfather.rs.signed
```

Opcija *-o* služi za definisanje naziva domena koji se potpisuje. *dnssec-signzone* će na osnovu SEP indikatora odrediti koje će zapise potpisati kojim ključem. Cela zona će biti potpisana ZSK ključem a samo DNSKEY zapisi i ZSK i KSK ključevima. Rezultat je novi fajl zone, *db.godfather.rs.signed* (potpisi i ključevi su skraćeni radi bolje preglednosti):

⁷ RSA savetuje da do 2010. godine minimalna dužina ključa bude 1024 bita:
<http://www.rsa.com/rsalabs/node.asp?id=2004>

```

; File written on Tue Jun 10 07:01:50 2009
; dnssec_signzone version 9.6.0-P1
godfather.rs.      21600 IN SOA      ns1.godfather.rs.
hostmaster.godfather.rs. (
                        1          ; serial
                        10800      ; refresh (3 hours)
                        3600       ; retry (1 hour)
                        604800     ; expire (1 week)
                        86400      ; minimum (1 day)
                        )
21600 RRSIG SOA 5 2 21600 20090716040150 (
20090616040150 19860 godfather.rs.
jnUpETJLJb9T6KGQkETjqCPN6jYwltirvYtj
[...]A9qJ7g89vjM5YVwY60adQADGqgE= )
21600 NS ns1.godfather.rs.
21600 RRSIG NS 5 2 21600 20090716040150 (
20090616040150 19860 godfather.rs.
N9BfZkoSTqvbVUMsUJgj8uJ5+n/o7eaa6gl4
[...]ZxAHcrP5f9HHxGamifj6XKpPT58= )
86400 NSEC media.godfather.rs. NS SOA RRSIG NSEC DNSKEY
86400 RRSIG NSEC 5 2 86400 20090716040150 (
20090616040150 19860 godfather.rs.
m4rH5aKuAJSJCxyFFLl2+ggw0WtuqHPl0Ql+
[...]PV5XVTzwpDF/VtLdLzjDr0UT72Q= )
21600 DNSKEY 256 3 5 (
AwEAAbrUulw2DF7GLfYBxXR6rjqV6ZQCS7Jb
[...]NyMEakuPp0CSKp8qZe10oWe/Zwry7Jql
) ; key id = 19860
21600 DNSKEY 257 3 5 (
AwEAAeYqX0+Qw2JuhvRLLohkqIQlF0laSn7K
[...]405k6YaE297Vy6IyEyqM6t6FzQ5HZ819
) ; key id = 26527
21600 RRSIG DNSKEY 5 2 21600 20090716040150 (
20090616040150 19860 godfather.rs.
XhfufsrHwvE7SyxihFvQ1rsZAJVj2KQG/ch6
[...]5202Rc2ST7g8oL/TejVhY+IrD4M= )
21600 RRSIG DNSKEY 5 2 21600 20090716040150 (
20090616040150 26527 godfather.rs.
kmrL4BR/Z6Q7cC855PDGskMdUompwOp7MLau
[...]Kpn0fmKBXauvOI385XJg4s4w9Z0= )
media.godfather.rs. 21600 IN A 192.168.1.201
21600 RRSIG A 5 3 21600 20090716040150 (
20090616040150 19860 godfather.rs.
eAzYMP/q5tr9XVwjh2rFli0yg7AfPLA6qau
[...]ZJMSQ7BP8FPZBEcwwkE2hs9ogQA= )
86400 NSEC ns1.godfather.rs. A RRSIG NSEC
86400 RRSIG NSEC 5 3 86400 20090716040150 (
20090616040150 19860 godfather.rs.
P+wZ2PN0c+5Bd+60cXV9QpkPk7a1DVgNNQSu
[...]HyLMRGiY/AiVUyqFowWrFfpS0vY= )
ns1.godfather.rs. 21600 IN A 192.168.1.251
21600 RRSIG A 5 3 21600 20090716040150 (
20090616040150 19860 godfather.rs.
VYZc4HydUmFYQcdocfEws0DzxFQfHAgbRShv
[...]Ngs15aZfERSFEq0TcnkLQn8hYJ8= )
86400 NSEC proxy.godfather.rs. A RRSIG NSEC
86400 RRSIG NSEC 5 3 86400 20090716040150 (
20090616040150 19860 godfather.rs.
V5jZYMU+/9fAE9odlBTIMs0XAqoazSnii8ZQ
[...]V0yLRhI16IolV/n843im/BiX228= )

```

```

proxy.godfather.rs.      21600 IN A    192.168.1.220
                        21600 RRSIG A 5 3 21600 20090716040150 (
                        20090616040150 19860 godfather.rs.
                        ARZ++cn7X2U0CvViT39+FgIL74F31nrDTzPI
                        [...]txTR4TpMVTuzbnRRmoSd+u6G2ZQ= )
                        86400 NSEC godfather.rs. A RRSIG NSEC
                        86400 RRSIG NSEC 5 3 86400 20090716040150 (
                        20090616040150 19860 godfather.rs.
                        h6f7hMEB2wyNjhFEYd05+G0bEYdxUbqo5L/z
                        [...]w/jzQJumkwkGTSVewZ4vEMFNpN0= )

```

Sada je neophodno aktivirati podršku za DNSSEC kao i promeniti naziv fajla zone koji se učitava u konfiguraciji BIND-a (*named.conf*):

```

options {
    directory "c:\windows\system32\dns\zones";
    recursion yes;
    dnssec-enable yes;
};

zone "godfather.rs" IN {
    type master;
    file "db.godfather.rs.signed";
};

```

Proverom uz pomoć alata *dig* (takođe deo paketa BIND) se utvrđuje ispravnost podešavanja:

```

> dig @localhost media.godfather.rs +dnssec

; <<>> DiG 9.6.0-P1 <<>> @localhost media.godfather.rs +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 972
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;media.godfather.rs.      IN      A

;; ANSWER SECTION:
media.godfather.rs.      21600 IN      A          192.168.1.201
media.godfather.rs.      21600 IN      RRSIG     A 5 3 21600 20090716040150 20090
616040150 19860 godfather.rs.
eAZYMYP/q5tr9XVwjh2rFli0yg7AfPlA6qau0qLac77VZJBCEFKBRG8ZnHAKf2L5Bnx[...]gQA=

;; AUTHORITY SECTION:
godfather.rs.           21600 IN      NS          ns1.godfather.rs.
godfather.rs.           21600 IN      RRSIG     NS 5 2 21600 20090716040150
2009
0616040150 19860 godfather.rs.
N9BfZkoSTqvbVUMsUJgj8uJ5+n/o7eaa6gl4hL0gophMQxI2x5v//7QsLEcms7nIKxg[...]T58=

;; ADDITIONAL SECTION:
ns1.godfather.rs.       21600 IN      A          192.168.1.251

```

```

ns1.godfather.rs.      21600   IN      RRSIG   A 5 3 21600 20090716040150
20090
616040150 19860 godfather.rs.
VYZc4HydUmFYQcdocfEws0DzxFQfHAgbRShv3mFl1zdzBd0KSdXeJqZUU0Mvxb[... ]YJ8=

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Jun 10 09:51:38 2009
;; MSG SIZE rcvd: 613

```

4.4 Prelaz između ključeva

Kao što je ranije navedeno, ZSK i KSK ključevi moraju biti periodično menjani. Oba ključa se menjaju na sličan način, uz određene preporuke koje se moraju poštovati. Nije dovoljno samo generisati nove parove ključeva i zameniti stare. Mora se, barem u trajanju jednog TTL vremena koje je definisano za potpisane zapise resursa, održati veza sa drugim serverima naziva koji su keširali potpisane podatke. Prostom zamenom ključeva se ti podaci više ne bi mogli verifikovati jer bi se promenili i potpisi zapisa resursa koji više ne bi odgovarali keširanim podacima.

4.4.1 Zamena ZSK ključa

U slučaju promene ZSK ključeva, najbolja praksa je korišćenje metode predobjavlјivanja. Generisanje novog para ključeva će biti samo prvi korak u prelasku između ključeva:

```

> dnssec-keygen -a rsasha1 -b 1024 -n zone godfather.rs
Kgodfather.rs.+005+47532

```

Novi ZSK ključ zatim treba dodati u fajl zone i ponovo potpisati zonu **tekućim** ZSK (19860) i tekućim KSK (26527) ključem:

```

> dnssec-signzone -o godfather.rs -k Kgodfather.rs.+005+26527 /
db.godfather.rs Kgodfather.rs.+005+19860
db.godfather.rs.signed

```

Dobijeni fajl zone će biti potpisan tekućim ZSK ali će sadržati i DNSKEY zapis resursa sa novim ZSK. Na ovaj način će novi ZSK (47532) biti dostupan svim serverima naziva koji od ovog momenta budu keširali podatke. Kako je za sve servere naziva obavezno da probaju sve raspoložive ključeve, neće biti problema sa validacijom postojećih podataka, jer je prisutan i tekući ZSK (19860):

```

; File written on Tue Jun 10 13:40:25 2009
; dnssec_signzone version 9.6.0-P1
godfather.rs.      21600   IN   SOA      ns1.godfather.rs.
hostmaster.godfather.rs. (
                        1           ; serial
                        10800        ; refresh (3 hours)
                        3600         ; retry (1 hour)
                        604800       ; expire (1 week)

```

```

                                86400      ; minimum (1 day)
                                )
[...]
21600 DNSKEY      256 3 5 (
    AwEAAZgWWGFu8eDDuWFT4bEMebMznXZjyLUP
    [...]14AYbiswrnTb4BG4o/G6kb69bQeR
    ) ; key_id = 47532
21600 DNSKEY      256 3 5 (
    AwEAAbRuUlw2DF7GLfYBxXR6rjqV6ZQCS7Jb
    [...]EAKuPp0CSKp8qZe10owe/Zwry7Jql
    ) ; key_id = 19860
21600 DNSKEY      257 3 5 (
    AwEAAeYqX0+Qw2JuhvRLLohkqIQlF0laSn7K
    [...]k6YaE297Vy6IyEyqM6t6FzQ5HZ819
    ) ; key_id = 26527
21600 RRSIG      DNSKEY 5 2 21600 20090716104025 (
    20090616104025 19860 godfather.rs.
    EARyEXZD2bLCMyIo38DEtgHx0jEYPvLBlv/a
    [...]ADQp2nuVMMHa5+lsRsinfkAU= )
21600 RRSIG      DNSKEY 5 2 21600 20090716104025 (
    20090616104025 26527 godfather.rs.
    I0jzVqWy9Rn+0CpuG9rNt9UR08hCCQItfxq2
    [...]9UiHg+gk7PhU6TucCTvWksQM= )
[...]
```

Ovakav fajl zone bi trebalo zadržati sve dok ne istekne važenje prethodno keširanih podataka, tako da svi serveri naziva imaju novu verziju podataka sa novim i tekućim ključem i tekućim potpisima. Kada se to dogodi, treba ponovo potpisati zonu, tekućim KSK (19860) i ovaj put **novim** ZSK (47532) ključem:

```
> dnssec-signzone -o godfather.rs -k Kgodfather.rs.+005+26527 /
db.godfather.rs Kgodfather.rs.+005+47532
db.godfather.rs.signed
```

Sada su svi RRSIG zapisi resursa potpisani novim ZSK. Po isteku sledećeg TTL vremena za keširanje podataka iz fajla zone, svi serveri naziva koji pristupaju zoni *godfather.rs* imaće samo verziju podataka sa novim i starim ključem ali sa novim potpisima. Stari ključ sada može biti uklonjen iz fajla zone i zona ponovo potpisana novim ZSK ključem.

4.4.2 Zamena KSK ključa

U slučaju promene KSK ključa, najbolji način da se to izvede je metodom dvostrukog potpisivanja. Počinje se generisanjem novog KSK:

```
> dnssec-keygen -a rsasha1 -b 1024 -f KSK -n zone godfather.rs
Kgodfather.rs.+005+22969
```

Ovaj ključ se zatim dodaje u fajl zone na već opisani način. Zonu zatim treba potpisati na sledeći način:

```
> dnssec-signzone -o godfather.rs -k Kgodfather.rs.+005+26527 -k /
Kgodfather.rs.+005+22969 db.godfather.rs Kgodfather.rs.+005+47532
db.godfather.rs.signed
```

Treba primetiti da se argument `-k` koristi dva puta, što označava da će DNSKEY zapisi biti potpisani tri puta, novim (22969) i tekućim (26527) KSK kao i tekućim (47532) ZSK:

```
[...]
      21600 DNSKEY      256 3 5 (
      AwEAAZgWWGFu8eDDuWFT4bEMebMznXZjyLUP
      [...]ORY14AYbiswrnTb4BG4o/G6kb69bQeR
      ) ; key id = 47532
      21600 DNSKEY      257 3 5 (
      AwEAAb6qQuRGoQ6uK7HjNP/6FnSfH90ayN4x
      [...]8sk0VblocnljqNmoF5bEtZJypH6SP99
      ) ; key id = 22969
      21600 DNSKEY      257 3 5 (
      AwEAAeYqX0+Qw2JuhvRLLohkqIQLF0laSn7K
      [...]05k6YaE297Vy6IyEyqM6t6FzQ5HZ819
      ) ; key id = 26527
[...]
```

Ono što je sada ključno je da se uspostavi lanac poverenja. Fajl sa novim KSK ključem (*Kgodfather.rs.+005+22969.key*) treba poslati svim serverima naziva kod kojih je uspostavljeno pouzdano polazište za *godfather.rs*. Zatim je neophodno obavestiti sve korisnike koji koriste *godfather.rs* kao pouzdano polazište da je dostupan novi KSK i da ga treba dodati u *trusted-keys* deo konfiguracije BIND-a:

```
trusted-keys{
    "godfather.rs." 257 3 5 " AwEAAeYqX0+Qw2JuhvR[...]5HZ819"; // stari KSK
    "godfather.rs." 257 3 5 " AwEAAb6qQuRGoQ6uK7H[...]H6SP99"; // novi KSK
};
```

Posle određenog vremena, kada se dobije potvrda da je novi KSK dodat u konfiguraciju servera, stari KSK se može ukloniti iz fajla zone i zona ponovo potpisati, na već opisani način, ovaj put samo novim KSK. Time je kompletiran prelazak sa starog na novi KSK.

4.5 DNSSEC Lookaside Validation

Kao što je ranije pomenuto, *DNSSEC Lookaside Validation* (DLV) predstavlja alternativni metod za uspostavljanje i proveru lanca poverenja. Konfigurisanje paketa BIND za korišćenje ovog sistema počinje, kao i u ostalim DNSSEC sistemima, potpisivanjem zone. Zona se potpisuje na već opisani način, osim što se dodaje i opcija `-l` kojom se definiše naziv *lookaside* zone:

```
> dnssec-signzone -o godfather.rs -l dlv.isc.org -k /
Kgodfather.rs.+005+22969 db.godfather.rs Kgodfather.rs.+005+47532
db.godfather.rs.signed
```

Formira se DLV zapis resursa, pod nazivom *dlvset-godfather.rs*:

```
godfather.rs.dlv.isc.org. IN DLV 22969 5 1 A19A6B0ED1E967B22[...]F4E55E
```

Da bi svaki server naziva bio pripremljen za korišćenje DLV servisa, neophodno je da se unesu dve izmene u konfiguracione fajlove BIND-a. Prva je da se definiše naziv *lookaside* zone u *options* sekciji:

```
options {  
    ....  
    dnssec-lookaside "." trusted-anchor "dlv.isc.org";  
    ....  
};
```

Ovde je značajno naglasiti da argument *dnssec-lookaside "."* označava da za svaku obezbeđenu zonu za koju ne postoje ni *parent* DS zapis ni definisano pouzdano polazište, treba slati upit na *dlv.isc.org*. Promenom argumenta na *.com* ili *.org* ovaj proces se može ograničiti samo za te domene.

Druga izmena podrazumeva upisivanje pouzdanog polazišta za DLV zonu:

```
trusted-keys {  
    dlv.isc.org. 257 3 5 "BEAAAAPHMu/5onzrEE7z1egmhg/WP00+juoZ  
    rW3euWEn4MxDCE1+lLy2brhQv5rN32RKtMzjHzpT59k/Vs[...]uWrBNh";  
};
```

Ovim će *dlv.isc.org* biti postavljen kao pouzdano polazište čime će lanac poverenja biti kompletiran.

5. Budućnost Interneta i DNS-a

5.1 ICANN i administracija DNS-a

Iako je opšte poznato da je Internet decentralizovan i nehijerarhijski organizovan, u njegovoj osnovi je i dalje centralizovana hijerarhija, što se najbolje vidi posmatranjem DNS-a. Potreba da se obezbedi jedinstvenost, tj. da se spreči korišćenje duplih naziva domena, stvorila je potrebu za nekom vrstom tela koje bi pratilo ili dodeljivalo imena. Međutim, kontrola nad DNS-om daje značajnu moć nad Internetom. Ko god kontroliše DNS, odlučuje koji novi TLD nazivi mogu da se uvedu (npr. novi sufixi kao što je .xxx ili .shop) i kako će imena i IP adrese biti dodeljene web sajtovima i drugim Internet resursima.

Kada je Internet još bio u začetku, DNS je održavala grupa volontera, zajedno sa Američkom Nacionalnom Naučnom Fondacijom (NSF) i civilnim i vojnim preduzimačima. Eksponencijalni rast Interneta je otežao funkcionisanje u to vreme *ad hoc* sistema za upravljanje DNS-om, i ono što su u početku bila uglavnom tehnička pitanja, postala su politički, pravni i ekonomski problemi koji su počeli da privlače zvaničnu pažnju. Naročito, od kada su atraktivni nazivi .com domena postali retki, sporovi oko ovakvih imena su postali uobičajeni i počeo je da raste pritisak da se otvore novi domeni najvišeg nivoa, kao što je .web. Iako tehnički trivijalno za implementaciju, predlog je dočekan sa neodobravanjem od strane nosioca intelektualnih svojina koji su se već suočavali sa sve većim problemima sa licima koja su registrovala nazive domena koja su odgovarala zaštitnim znacima i držala ih radi profita. Za to vreme, vlade drugih zemalja, naročito u Evropskoj Uniji, su počele da izražavaju razumljivu zabrinutost zbog kontrole koju Sjedinjene Države imaju nad kritičnim elementom globalnog komunikacionog i komercijalnog resursa, od kojeg će njihove ekonomije i društva sve više zavisiti.

Juna 1998, Američko Ministarstvo trgovine je kao odgovor na sve veću zabrinutost vezanu za DNS, donelo Izjavu o politici privatizacije adresnog prostora na Internetu, poznatu kao *DNS White Paper*⁸. Ovaj dokument je pozvao na formiranje privatne neprofitne korporacije koja bi preuzela DNS i izvršila različite reforme. Nedugo posle toga, međunarodna grupa je posle zatvorenog sastanka, objedinjena u ICANN, kao privatnu neprofitnu korporaciju sa sedištem u Kaliforniji. Nedugo zatim, Američko Ministarstvo trgovine je prenelo na ICANN većinu svojih ovlašćenja vezanih za upravljanje DNS-om.

U prve dve godine postojanja, ICANN je uveo nekoliko promena sa potencijalno dugoročnim efektima.

Uvedena je obavezna arbitraža žalbi na korišćenje zaštitnih znakova. ICANN-ova Jednoobrazna politika razrešavanja sporova⁹ (*Uniform Dispute Resolution Policy – UDRP*) zahteva od svake strane registrovane pod .com, .org i .net domenima da prihvati arbitražu pred ICANN-ovom komisijom ako bilo koji vlasnik bilo gde u svetu izrazi sumnju da je registrovani naziv sličan njihovom zaštitnom znaku. Sam UDRP dokument je veoma kontroverzan – vlasnici

⁸ http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm

⁹ <http://www.icann.org/udrp/udrp.htm>

zaštitnih znakova se žale da nije dovoljno strog; grupe za građanska prava tvrde da takav sistem krši osnovne norme fer procesa i da se komisija ne ponaša nepristrasno.

Takođe, suprotno ranijim obećanjima da će polovina Saveta Direktora biti izabrana iz nezavisnog članstva, ICANN je objavio: da neće postojati članstvo, da će samo 5 od 18 umesto 9 od 18 njegovih direktora biti slobodno izabrano, da će četiri od inicijalno izabranih direktora ostati na funkciji i da će ICANN sprovesti analizu da bi odredio da li bi uopšte trebalo da postoje nezavisno birani direktori.

Ono što predstavlja najveći problem, i što u stvari predstavlja izvor zabrinutosti, je što, istorijski gledano, nedostatak odgovornosti uvek dovodi do samovolje. Pored toga što nema odgovornost prema Vladi, ICANN nema ni mehanizme kontrole odgovornosti koji obično postoje u korporacijama ili neprofitnim organizacijama. Takođe, ICANN nema problema sa finansijama, budući da su Internet registri prihvatili ICANN-ov autoritet i uplatu povremenih priloga u zamenu za mogućnost da prodaju registracije u *.com*, *.net* i *.org* domenima.

Rezultat ovakve istorije je telo sa minimalnom odgovornošću. Ovaj problem će samo postati veći ako Američko Ministarstvo trgovine prenese ICANN-u punu kontrolu nad DNS-om, jer najvažniji deo bilo čije „kontrole“ nad *root*-om u stvari predstavlja objavljivanje podataka na koje se različite strane, od kojih su mnoge nevladine, oslanjaju.

5.2 SAD i bezbednost na Internetu

Događaj sa početka 2007. godine je samo povećao sumnje koju ova tema izaziva. Marta 2007, na godišnjem sastanku ICANN-a u Lisabonu, predsednik Kanadske Agencije za Internet registraciju, kao predstavnik registara nacionalnih domena najvišeg nivoa, je saopštio da Američki *Department of Homeland Security* želi da ključ za potpisivanje DNS *root* zone (ključ za potpisivanje ključeva zona, trenutno u rukama *VeriSign*-a) bude pod kontrolom Vlade SAD¹⁰. DHS, koja je agencija trenutno zadužena za bezbednost na Internetu, trenutno sponzorise kampanju za podršku implementacije DNSSEC-a.

Uključivanje DHS-a u razvoj DNSSEC-a nije iznenađujuće u smislu da je učešće Vlade neophodno pri istraživanju i razvoju novih tehnologija (rani Internet je dobar primer). Ali, ponovo istorijski gledano, vlade su često pokušavale da utiču na tehničke standarde u cilju zaštite domaće industrije, povećanja sopstvene moći ili sticanja ekonomske dobiti. Ono što je interesantno sa stanovišta uvođenja DNSSEC-a je interesovanje koju DHS ima za bezbednost ostalih važnih Internet standarda (kao što je inicijativa za bezbednost protokola za rutiranje, SPRI¹¹) i široko verovanje da su aktivnosti ključnih organizacija koje se bave infrastrukturom Interneta vođene interesima privatnog sektora. Uz činjenicu da je infrastruktura Interneta po svojoj prirodi međunarodna i da se globalna ekonomija oslanja na nju, zabrinutost koju ova pitanja izazivaju je razumljiva.

U to vreme *VeriSign*-ov ekspert za DNSSEC, dr *Phillip Hallam-Baker*, objavio je na IETF mailing listi¹² tekst o implikacijama potpisivanja *root*-a korišćenjem DNSSEC-a. Takođe, pozvao je na deljenje ovlašćenja za potpisivanje:

¹⁰ <http://www.heise.de/english/newsticker/news/87655>

¹¹ <http://www.cyber.st.dhs.gov/spri.html>

¹² <http://www.ietf.org/mail-archive/web/ietf/current/msg47560.html>

“...Treba uzeti u obzir da je ovo infrastruktura koja bi trebalo da bude robusna tokom nekoliko dekada, ako ne i vekova. Takođe, treba razmotriti i verovatnoću da ko god kontroliše *root*, može preduzeti neki postupak koji neka druga strana, u tako dugom vremenskom periodu, može smatrati odmetanjem.”

“Na primer, mala ali uticajna grupa glasača na jugozapadnom poluostrvu države A smatra sebe političkim prognanicima iz države B, ostrva u blizini poluostrva. Država A je u jedinstvenoj poziciji da utiče na *root* i pomenuti glasači lobiraju za izuzimanje države B. Ako bi do ovoga došlo danas, rezultat bi bio privremeno cepanje *root*-a praćeno brzim pojavljivanjem alternativne *root* strukture koja nije bila pod zloupotrebom države A. Strane imaju vlast ali nemaju moć. Ako bi *root* bio potpisan od strane jedinstvenog tela, to telo bi imalo apsolutnu moć. Odmetanju se ne bi moglo suprotstaviti cepanjem *root*-a. Danas se prostor za odmetanje drži u ravnoteži nedostatkom bezbednosti. *Root* se, konačno, definiše lokacijom na koju određeni provajder usmerava UDP pakete sa IP adresom *root* servera. Posle potpisivanja, *root* bi bio definisan poznavanjem privatnog ključa koji bi odgovarao široko distribuiranim i ugrađenim javnim ključem.”

“Uzmite u obzir činjenicu da Evropa trenutno planira kopiranje GPS satelitskog sistema po ceni od nekoliko milijardi dolara uprkos činjenici da je jedini razlog za to sprečavanje sličnog odmetanja od strane Sjedinjenih Država. Ideja da kontrola DNS *root*-a ne bi bila izložena i značajnijim geo-političkim pritiscima je naivna. 1955. bi postavljanje ovog sistema bilo obavljeno bez privlačenja nepotrebne pažnje, što nije slučaj danas.”

Februara 2009. na jednom od saslušanja pred Kongresom SAD koji se trenutno vode na temu bezbednosti na Internetu, aktuelni Direktor za Nacionalnu Bezbednost Admiral Denis Bler je izjavio da bi NSA (*National Security Agency*, kriptološka/obaveštajna agencija koja je u sastavu Ministarstva Odbrane) umesto DHS-a trebalo da postane zadužena za obezbeđivanje nacionalne telekomunikacione mreže kao i sajber infrastrukture¹³.

Ono što predstavlja problem sa poveravanjem ovog zadatka NSA leži u prirodi same agencije. Po zakonu, NSA ima zadatak da prikuplja i analizira inostrane komunikacije kao i da prikuplja inostrane signalne podatke. Pre svega, agencija je izuzetno netransparentna, bavi se zadacima koji se najčešće klasifikuju kao super-tajni i vrlo je teško pratiti njen rad. Zatim postoji pitanje poverenja, jer je Agenciji, od 2001. godine kao deo „borbe protiv terorizma“, izvršnom naredbom bez donošenja zakona, dozvoljeno da prati, bez naloga, telefonske pozive, elektronsku poštu, Internet aktivnosti, tekstualne poruke i druge komunikacije unutar SAD. Agenciji je omogućen direktan, sveobuhvatan i nenadgledan pristup svim optičkim sistemima komunikacija između velikih nacionalnih telekomunikacionih kompanija. S druge strane, svojim novim zadatkom bi ova agencija došla u sukob interesa. Sve mreže, bilo vojne, vladine, civilne ili komercijalne koriste iste računarske sisteme, iste mrežne uređaje kao i iste mrežne protokole. Ako bi Agencija pronašla bezbednosni propust u nekom sistemu, da li bi upozorila javnost i proizvođače na njegovo postojanje, omogućujući ispravljanje tih nedostataka, ili bi ćutala, omogućivši sebi iskorišćavanje te slabosti radi prikupljanja podataka od zlonamernih strana? Da li bi Agencija pomogla da se neki sistem ili mreža učini bezbednijom ili olakšala sebi zadatak prikupljanja podataka? U saslušanju pred Kongresom marta 2009, bivši šef odeljenja za Nacionalnu Sajber Bezbednost pri DHS-u Amit Joran, ocenio je da „...je obaveštajna zajednica uvek davala i da će uvek dati veći prioritet sopstvenim naporima ka prikupljanju podataka u odnosu na zadatak odbrane i zaštite vladinih i nacionalnih digitalnih sistema“¹⁴.

¹³ http://www.dni.gov/testimonies/20090225_transcript.pdf

¹⁴ <http://www.wired.com/threatlevel/2009/03/nsa-dominance-o/>

Početkom marta 2009. direktor Nacionalnog Centra za Sajber Bezbednost pri DHS-u Rod Bekstrom, je podneo ostavku¹⁵ rekavši pritom da NSA već efektivno kontroliše sve sajber napore DHS-a i da bi poveravanje pomenutog zadatka NSA bila greška jer se obaveštajni običaji dosta razlikuju od mrežne ili bezbednosne prakse. Takođe, izrazio je zabrinutost da bi „...upravljanje bezbednošću i praćenjem najvažnijih vladinih mreža od strane jedne organizacije predstavljalo značajnu pretnju po demokratske procese“.

Aprila 2009. Senatu SAD je, kao „mera protiv terorizma“, predložen Zakon o Sajber Bezbednosti (*Cybersecurity Act*¹⁶). U obliku u kakvom je predložen, on daje Vladi SAD moć nad Internetom bez presedana.

Ovaj dokument između ostalog predviđa sledeće:

- Predsednik SAD može „da proglasi vanredno stanje u sajber prostoru i da naredi ograničenje ili isključenje Internet saobraćaja ka i prema bilo kojoj mreži ili delu kritične infrastrukture informacionog sistema SAD ili federalne Vlade“ (Paragraf 18, (2)).
- Sekretar za trgovinu „će imati pristup svim relevantnim podacima vezanim za mreže koje su deo najvažnije infrastrukture, bez obzira na odredbe zakona, propisa, pravila ili politike koja bi ograničila takav pristup...“ (Paragraf 14, (b),(1)).
- Da se sprovede studija o „izvodljivosti programa za upravljanje i potvrdu identiteta za informacione sisteme i mreže Vlade i kritičnih infrastruktura“ (Paragraf 17).

Pored toga što izazivaju zabrinutost ovakve kakve jesu, pomenute odredbe nisu ni dovoljno jasno definisane. Iako je u nekim trenucima neophodno blokirati određene mreže sa kojih stiže štetan sadržaj, ovaj zakon ne daje nikakve smernice kada bi i kako Predsednik SAD odgovorno trebalo da isključi mreže koje su u privatnom vlasništvu. Ovakvo ovlašćenje odmah pokreće pitanje slobode govora, jer se ovakva moć može iskoristiti i u svrhe prinude.

Što se tiče Ministarstva trgovine, ovaj zakon dozvoljava apsolutni pristup, bez uvođenja vanrednog stanja, svim bitnim podacima, bez standarda koji bi štitali privatnost ili pravnih provera. Kako nisu postavljene jasne granice primene odredbe, ovaj zakon bi mogao i da dođe u sukob sa drugim zakonima koji štite privatne podatke ili propisima koji se tiču finansijske privatnosti.

Konačno, odredba o upravljanju i potvrdi identiteta predstavlja potencijalnu pretnju po privatnost. Nije preterano očekivati da ova studija može biti uvod za predloge kojima bi se ograničila anonimnost na Internetu. Problem je u tome što anonimnost ne mora da podrazumeva bezbednosni rizik i isključiti je kao univerzalno pravilo za sve korisnike ne bi bilo primereno niti bi moralo da poboljša bezbednost u celini.

Interesantno je napomenuti i da je predlagač ovog dokumenta Senator Dž. Rokfeler, iz jedne od najbogatijih i najuticajnijih porodica na svetu, sa širokim interesima u industrijskom, bankarskom i političkom sektoru. *Electronic Frontier Foundation*¹⁷, organizacija koja se bavi zaštitom slobode govora, privatnosti i prava potrošača, oštro se protivi ovom predlogu zakona.

¹⁵ http://www.wired.com/images_blogs/dangerroom/files/ncsc_directors_resignation1.pdf

¹⁶ <http://thomas.loc.gov/cgi-bin/query/z?c111:S.773>:

¹⁷ <http://www.eff.org/>

Imajući u vidu sve navedeno, očigledno je da na nivou Vlade SAD postoji snažna volja da se obezbedi sajber prostor. Na žalost, ono čime je ta volja motivisana ne mora biti samo bezbednost krajnjih korisnika Interneta. Stiče se utisak da se pod izgovorom “bezbednosti” pokušavaju nametnuti ideje i metode koje narušavaju osnovne principe na kojima se baziraju današnji Internet i demokratsko društvo. Ovde nisu u pitanju samo korisnici Interneta u SAD – sve mere koje se preduzmu zahvatiće Internet na globalnom nivou.

Poveravanjem ključeva za potpisivanje *root* zone nekom telu Vlade SAD, prebacivanjem nadležnosti nad sajber bezbednošću agenciji NSA i usvajanjem Zakona o Sajber Bezbednosti u sadašnjem obliku, stvorila bi se situacija u kojoj bi jako puno moći i kontrole bilo sakupljeno na uskom prostoru, sa vrlo malo mogućnosti za pozivanje na odgovornost. Ovo je tema o kojoj se mora diskutovati i na koju se mora skrenuti pažnja, jer će u vrlo bliskoj budućnosti uticati ne samo na funkcionisanje Interneta kao globalnog servisa na koji se oslanjaju sve države, već i na svakodnevne živote svih ljudi.

5.2 Alternativni DNS

Uz postojećih 13 DNS *root* servera koji rade u dogovoru sa ICANN-om, nekoliko organizacija upravlja alternativnim DNS *root* serverima. Svaka od njih poseduje sopstvenu grupu *root* servera naziva i sopstveni skup *top level* domena.

Alternativni *root* serveri najčešće obuhvataju adresiranje za sve TLD servere koje je odredio ICANN (generički *.com*, *.net*, *.org*... kao i državni *.rs*, *.uk* itd.), kao i za TLD servere za druge domene najvišeg nivoa (kao što su *.new*, *.web*, *.tech*...) koje ICANN nije definisao, već ih održavaju nezavisne organizacije. Neke, ali ne sve alternativne *root* servere održavaju organizacije koje istovremeno upravljaju i ovim alternativnim TLD domenima.

Razlozi za pokretanje alternativnog adresiranja mogu biti različiti, ali se uopšteno mogu podeliti na sisteme: Pokrenute iz idealističkih ili ideoloških razloga, kao komercijalni projekti i kao interni projekti organizacija za sopstvene potrebe. Trenutno samo mali deo provajdera koristi usluge alternativnih *root* servera, dok se većina drži servera koje je naveo ICANN. *Internet Architecture Board*¹⁸ se u dokumentu RFC 2826 snažno protivi postavljanju i korišćenju alternativnih *root* servera naziva.

Najozbiljniji projekat alternativnog sistema adresiranja na Internetu predstavlja *Open Root Server Network* (ORSN)¹⁹, koji funkcioniše od 2002. Njegova *root* zona se obično održava u sinhronizaciji sa mrežom koju koordinira ICANN. Mreže su stoga kompatibilne, iako ORSN funkcioniše potpuno nezavisno. Osnivači ORSN mreže su kao glavni razlog pokretanja naveli zabrinutost zbog uticaja koji Vlada SAD ima na ICANN. Njihov cilj je da ograniče kontrolu nad Internetom koju daju *root* serveri, ali obezbeđujući da nazivi domena ostanu nedvosmisleni.

ORSN ima dva načina rada: Nezavisan i Baziran na ICANN-u. Baziran na ICANN-u predstavlja normalni način rada i podrazumeva dnevnu sinhronizaciju, osim što se uklonjeni TLD domeni ne uklanjaju iz ORSN *root*-a. Nezavisan režim rada se ne ažurira automatski i aktivira se „...kad god politička situacija u svetu učini ovaj korak neophodnim usled postojanja mogućnosti modifikacije i/ili pada ICANN-ove *root* zone...”²⁰

¹⁸ Komitet zadužen za nadgledanje tehničkog razvoja Interneta. Nadgleda više radnih grupa, uključujući IETF

¹⁹ <http://www.orsn.org>

²⁰ <http://www.orsn.org/faq.php>

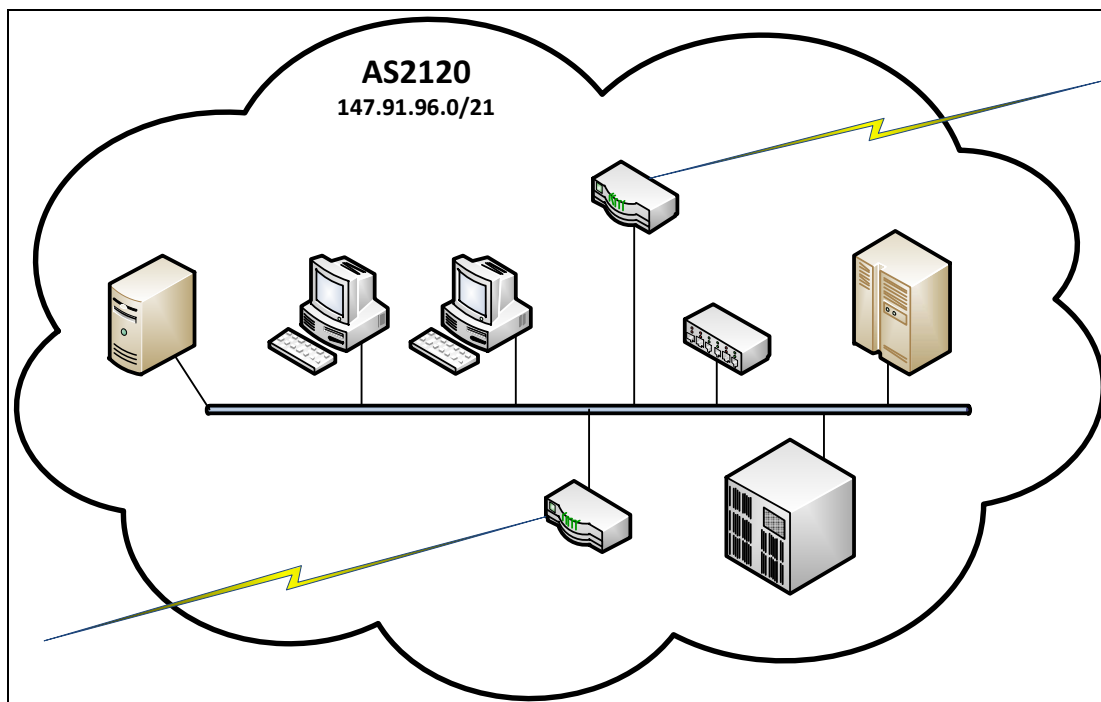
6. Rutiranje podataka na Internetu

6.1 Osnove rutiranja

Pod rutiranjem u računarskim mrežama se podrazumeva usmeravanje podataka duž određene putanje kako bi oni bili isporučeni od njihovih polazišta do odredišta. Putevi kojim će podaci biti usmereni se određuju uz pomoć uređaja pod nazivom ruteri. Ove putanje, tj. rute mogu biti statički definisane, što se koristi samo u pojedinim slučajevima. Najčešće, ruteri u zavisnosti od konkretnih mrežnih okruženja primenjuju algoritme protokola rutiranja, uz pomoć kojih dinamički pronalaze i biraju putanje kojima se usmeravaju podaci.

Današnji Internet predstavlja kompleksan sistem koji zbog efikasnosti i skalabilnosti zahteva dvoslojno rutiranje. Granica između slojeva definisana je autonomnim sistemima. Autonomni sistem (AS) predstavlja deo mreže (tj. grupu rutera) čiji nadzor, upravljanje i održavanje obavlja jedna institucija i u kojoj se primenjuju identična pravila rutiranja. Svaki autonomni sistem se identifikuje jedinstvenim AS brojem.

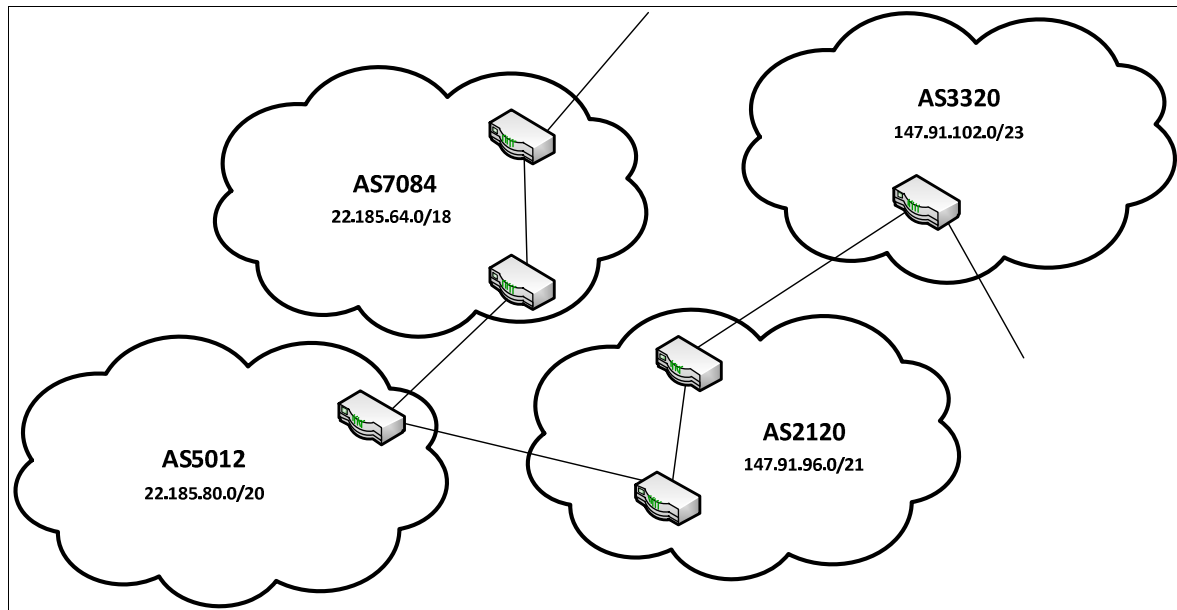
Rutiranje podataka u okviru autonomnih sistema se naziva interno rutiranje. Njime se podaci precizno usmeravaju ka odredišnom računaru. Interni protokoli rutiranja (OSPF, EIGRP...) za određivanje putanje koriste faktor cene tj. metriku. Metrika zavisi od tehničkih parametara mreže (protok ka linku, broj linkova između dve tačke i sl.).



Slika 6.1.1 Interno rutiranje

Eksterno rutiranje predstavlja rutiranje podataka između autonomnih sistema i čini noseći stub današnjeg Interneta. Njima se podaci usmeravaju grubo, na osnovu liste IP adresa (prefiksa) dostupnih unutar jednog autonomnog sistema. Parametri koji se uzimaju u obzir prilikom odabira rute nisu tehničke prirode, već su administrativni. Postoji više protokola za eksterno rutiranje ali se danas koristi isključivo BGP (*Border Gateway Protocol*).

Ovde je važno napomenuti da protokoli rutiranja, interni ili eksterni, ne rutiraju pakete podataka – oni samo razmenjuju informacije o rutiranju i rutama. Sam saobraćaj se rutira na IP sloju.



Slika 6.1.2 Eksterno rutiranje

6.2 BGP protokol

Zadatak BGP protokola je kontrola rutiranja podataka i razmena informacija o rutiranju i dostupnosti ruta. Razvijen je kao naslednik EGP (*Exterior Gateway Protocol*) protokola kako bi omogućio decentralizaciju rutiranja i omogućio bolju skalabilnost usled rasta Interneta. Skoro svi Internet provajder su obavezni da koriste BGP protokol da bi uspostavili rutiranje među sobom.

BGP verzija 4 koja je razvijena 1994. godine je i dalje aktuelna. U toj verziji je uvedeno bezklasno rutiranje (*Classless Inter-Domain Routing* – CIDR) kao i sumariizacija tj. agregacija ruta (*route summarization/aggregation*).

Bezklasno rutiranje je uvedeno sa ciljem da se uspori rast tabela rutiranja i potrošnja IPv4 adresa. U prvobitnoj arhitekturi IPv4 mreža, rutiranje se obavljalo na osnovu jedne ili više 8-bitnih grupa, što je kao rezultat imalo podelu na A, B i C klase. Bezklasnim rutiranjem je omogućeno dodeljivanje adresnog prostora na bazi bilo kog bita adrese umesto dodele 8-bitnih segmenata. U CIDR notaciji, IP adresi se pridružuje prefiks rutiranja. On označava broj vodećih bitova adrese koji određuju pripadnost delu mreže tj. rutu.

IP/CIDR	Mrežna maska	Broj hostova	Klasa
a.b.c.d/32	255.255.255.255	1	1/256 C
a.b.c.0/24	255.255.255.0	256	1 C
a.b.0.0/16	255.255.0.0	65.536	1 B
a.0.0.0/8	255.0.0.0	16.777.216	1 A
0.0.0.0/0	0.0.0.0	4.294.967.296	256 A

Tabela 6.2.1 Klase adresa i CIDR blokovi

Mrežna maska predstavlja zapis prefiksa rutiranja u vidu 4 okteta od po 8 bita. Ona pruža istu informaciju o broju vodećih bitova kao i prefiks, ali, dok su kod prefiksa svi bitovi u neprekidnom nizu, mrežna maska može obuhvatiti i bitove koji nisu deo neprekidnog niza.

212								62								45								222								
1	1	0	1	0	1	0	0	0	0	1	1	1	1	0	0	0	1	0	1	1	0	1	1	1	0	1	1	1	1	0		
RIPE NCC 212.0.0.0/8																																
Cable&Wireless 212.62.0.0/19																																
JP PTT Saobraćaja Srbija 212.62.45.0/20																																
www.singidunum.rs 212.62.45.222/32																																

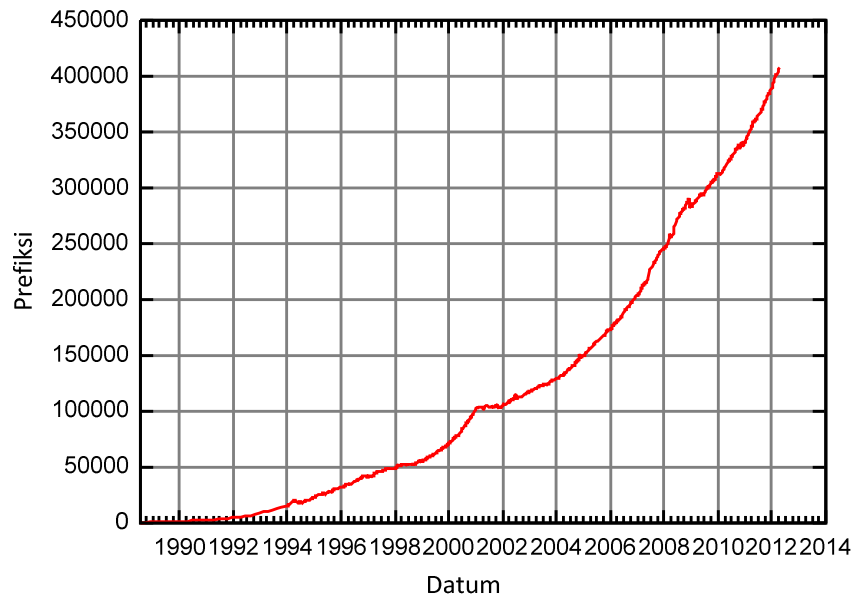
Tabela 6.2.2 Dodeljivanje CIDR blokova

Bezklasno rutiranje je omogućilo uvođenje agregacije ruta. Agregacija ruta predstavlja adresno grupisanje dve ili više mreža pod zajedničkim CIDR prefiksom. Na primer, više mreža koji se nalaze u opsegu 212.62.40.0 – 212.62.47.0 se mogu definisati kao ruta 212.62.40.0/21. Prefiks /21 označava broj zajedničkih bitova za sve obuhvaćene mreže. Umesto višestrukih unosa za svaku pojedinačnu mrežu, u tabeli rutiranja će se pojavljivati samo jedan.

Adresa	Prvi oktet	Drugi oktet	Treći oktet	Četvrti oktet
212.62.40.0	11010100	00111110	00101 000	00000000
212.62.42.0	11010100	00111110	00101 010	00000000
212.62.45.0	11010100	00111110	00101 101	00000000
212.62.46.0	11010100	00111110	00101 110	00000000
212.62.47.0	11010100	00111110	00101 111	00000000

Tabela 6.2.3 Agregacija ruta

Na Internetu se agregacija ruta koristi pre svega kao strategija za zaštitu od fragmentacije IP adresnog prostora. Primenuje se hijerarhijski sistem po kome se regionalnim i nacionalnim mrežama dodeljuje kontrola nad segmentima adresnog prostora. Praktična korist od agregacije ruta je u manjem mrežnom saobraćaju koji se odnosi na oglašavanje ruta, lakšem donošenju odluka o rutiranju i većoj efikasnosti u radu rutera, pošto se agregacijom ruta smanjuje veličina globalne tabele rutiranja.



Slika 6.2.1 Rast broja prefiksa na Internetu²¹

BGP funkcioniše putem formiranja tabele rutiranja. Tabela rutiranja se sastoji od ruta, tj. adresa odredišta i opisa putanje koja vodi do svakog od tih odredišta. Iz ovog razloga se BGP protokol naziva i protokolom vektora putanje (*path vector protocol*). BGP ruteri međusobno razmenjuju ove tabele.

Veza između BGP rutera može biti interna, u okviru istog AS, u kom slučaju ruteri razmenjuju samo rute do kojih mogu da dodju na osnovu sopstvenih veza. Ovakva komunikacija se naziva IBGP (*Internal BGP*).

U slučaju eksterne veze, jedan (mada ih može biti i više) od rutera u svakom autonomnom sistemu zastupa ceo AS pred ostatkom Interneta. Ovaj ruter se naziva *speaker* čvorom (*speaker node*) i povezuje se sa *speaker* čvorom (ruterom) u susednom autonomnom sistemu. Ovakva komunikacija se naziva EBGP (*External BGP*). *Speaker* čvorovi međusobno razmenjuju kompletne tabele rutiranja tj. rute koje je ruter prikupio samostalno ili u razmeni sa drugim BGP ruterima.

²¹ Izvor: <http://bgp.potaroo.net/>

6.3 Format BGP poruka

BGP protokol koristi četiri vrste poruka: *open*, *update*, *notification* i *keep-alive*. *Update* porukama se obavlja glavni zadatak protokola: oglašavaju se nove i povlače rute koje više nisu aktivne.

Dužina polja za povučene rute	Povučene rute	Dužina polja za <i>path</i> atributi	<i>Path</i> atributi	NLRI
-------------------------------	---------------	--------------------------------------	----------------------	------

Tabela 6.3.1 Format BGP *Update* poruke

- **Dužina polja za povučene rute** – Označava ukupnu dužinu polja „povučene rute“ ili da to polje nije prisutno
- **Povučene rute** – Lista prefiksa za rute koje se više ne koriste
- **Dužina polja za *path* atributi** – Označava ukupnu dužinu polja „*path* atributi“ ili da to polje nije prisutno
- ***Path* atributi** – Opis karakteristika rute koja se oglašava. Atributi mogu biti:
 - o Dobro poznati obavezni:
 - **ORIGIN** – Označava poreklo informacije o ruti
 - **AS_PATH** – Niz brojeva autonomnih sistema preko kojih se stiže do navedenog odredišta (prefiska). Istovremeno označava kroz koje je sve AS *Update* poruka prošla. Prilikom prolaska, svaki AS dodaje svoj broj na postojeće brojeve u ovom atributu.
 - **NEXT_HOP** – Adresa ruteru koji bi trebalo koristiti kao sledeći do odredišta zapisanih u **NLRI**
 - o Dobro poznati neobavezni
 - **LOCAL_PREF** – Stepen prioriteta na osnovu lokalno definisane politike rutiranja. Samo za UPDATE poruke ka drugim ruterima unutar istog AS.
 - **ATOMIC AGGREGATE**
 - o Opcioni prenosivi
 - **AGGREGATOR**
 - **COMMUNITY**
 - o Opcioni neprenosivi
 - **MULTI_EXIT_DISC** – Koristi se za diskriminaciju između višestrukih ulaznih i izlaznih tačaka za isti AS
 - **ORIGINATOR_ID**
- **NLRI** (*Network Layer Reachability Information*) – Sastoji se iz dva dela:
 - o **LENGTH** – Dužina prefiksa u CIDR zapisu, npr. /25.
 - o **PREFIX** – Lista prefiksa za oglašene rute, npr. 204.149.16.128.

UPDATE porukom se može oglašavati samo jedan skup path atributa, dok su višestruka odredišta moguća, pod uslovom da su im path atributi zajednički.

6.4 Odabir najpovoljnije rute

Prilikom odabira najpovoljnije rute, BGP algoritam podrazumeva da je prva ispravna putanja koju pronadje za određeno odredište ujedno i najbolja putanja. BGP zatim upoređuje trenutno najbolju putanju sa sledećom putanjom sve dok ne dodje do kraja tj. proveriti sve ispravne putanje. Odabir najbolje putanje može biti vrlo kompleksan i može zavisiti od više različitih parametara koji ne moraju biti tehnički (administrativni ili specifični za proizvođača rutera), ali određeni skup pravila se mora poštovati i to po određenom redosledu:

1. **AS_PATH atribut:** Prednost se daje putanji sa kraćim nizom AS brojeva.
2. **ORIGIN atribut:** Prednost se daje putanji sa nižim ORIGIN brojem.
3. **MULTI_EXIT_DISC atribut:** Prednost se daje putanji sa višim stepenom prioriteta.
4. **EBGP** poreklo rute ima prednost nad IBGP poreklom.
5. **Interior cost:** Prednost se daje putanji sa manjom metrikom do NEXT_HOP rutera.
6. **BGP Identifier:** Prednost ima ruta koju je oglasio BGP speaker sa nižom vrednošću (*BGP Identifier* predstavlja IP adresu rutera).
7. **IP adresa:** Prednost ima ruta dobijena od strane rutera sa nižom IP adresom

7. Bezbednosni problemi rutiranja

Kako bezbednost uopšte nije bila prioritet na Internetu, niti se na to obraćalo puno pažnje kada je BGP nastajao, ovaj protokol je do danas ostao podložan mnogim problemima sa kojima se Internet zajednica bori. Do jednako ozbiljnih problema može doći kako usled grešaka ljudi ili kvarova na opremi, tako i usled zlonamernih aktivnosti. Međutim, s obzirom na jedinstvenu ulogu koju BGP ima u globalnom Internetu, može doći i do specifičnih problema za koje u ovom trenutku ne postoje lako primenjiva rešenja.

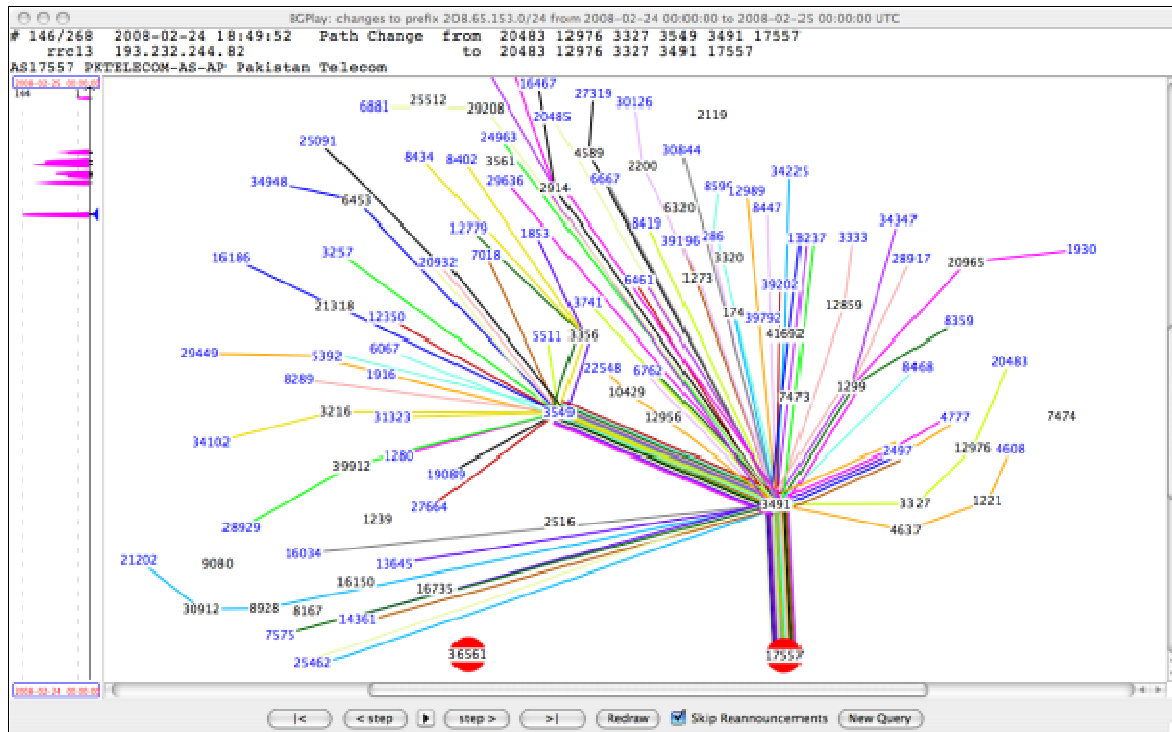
7.1 Tehničke greške

Aprila 1997. je zabeležen prvi veći incident vezan za probleme sa rutiranjem²². Ruter pod kontrolom autonomnog sistema 7007 je usled greške u samom uređaju počeo da oglašava značajan deo sopstvene tabele rutiranja ka internetu, stvarajući crnu rupu (saobraćaj koji je greškom stizao do 7007 je odbacivan bez ikakvih poruka o grešci). Rute koje su oglašavane su bile deagregirane do prefiksa /24, što je specifičnije od ruta koje postoje na ostatku interneta. Uz to, sporni ruter je polje AS_PATH u svakoj oglašenoj ruti prepisao sa 7007. Svi BGP ruteri na Internetu koji su dobili ove rute birali su njih kao najbolje i usmeravali saobraćaj ka autonomnom sistemu 7007. Ovo je dovelo do prekida saobraćaja na kompletnom Internetu u trajanju od nekoliko sati.

Februara 2008. Vlada Pakistana je donela odluku da cenzuriše pristup sajtu YouTube, iz političkih razloga²³. Prateći nalog, jedan od tamošnjih provajdera, Pakistan Telekom (AS17557), konfigurisao je svoje BGP rutere da interno oglašavaju rutu 208.65.153.0/24 (prefiks YouTube-a). Iz nepoznatih razloga, ova ruta je oglašena i ka nadprovajderu PCCW (AS 3491) koji je propagirao dalje ka ostatku Interneta. Kako YouTube (AS36561) oglašava svoj prefiks kao 208.65.152.0/22 (manje specifičan), svi ruteri do kojih je stigla sporna ruta (oko dve trećine Interneta) su je odabrali kao najbolju i usmerili saobraćaj namenjen YouTube-u ka Pakistanu. YouTube nije bio dostupan oko dva sata, koliko je trebalo da se problem uoči, pronadje uzrok, prekine sa spornim oglašavanjem (isključivanjem Pakistana sa Interneta) i da se oglase jednako specifične (/24) i specifičnije rute (/25) koje bi zamenila pogrešne.

²² <http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html>

²³ http://www.renesys.com/blog/pakistan_blocking_order.pdf

Slika 7.1.1 Incident sa Pakistan Telekom-om²⁴

7.2 Lažiranje (*spoofing*)

Lažiranje (*spoofing*) predstavlja polazište za najozbiljnije pretnje po komunikaciju na Internetu. Imajući ovo u vidu, arhitektura BGP protokola je posebno ranjiva, jer je zasnovana na poverenju. Ako u komunikaciji između dva rutera jedan od njih oglasi da je baš on najbrži i najefikasniji putanja za isporuku podataka do određenog odredišta, drugi ruter koji je povezan sa njim će mu poverovati. Ne postoje mehanizmi kojim bi se bez svake sumnje utvrdilo da li je ruter stvarno taj za koji tvrdi da jeste, da li su informacije koje šalje tačne niti da li je ovlašćen da šalje takve informacije.

Maja 2003. jedan manji provajder sa Floride je počeo da oglašava blok IP adresa 192.153.43.0/24. Međutim, pomenuti blok je bio dodeljen kompaniji Nortrop Gruman, velikom vojnom preduzimaču. Ova kompanija poseduje veliku IP mrežu i sopstveni autonomni sistem tako da bi bilo kome ko vrši nadzor bilo jasno da nešto nije u redu. Nažalost, niko to nije primetio, sve dok sa otegot bloka IP adresa nije počela da stiže ogromna količina neželjene elektronske pošte – spam.

Tehnika koju su koristili spameri nije bila izuzetak, ona se često koristi za pomenute namere. Spameri su pronašli blok IP adresa koji je dodeljen ali nije bio u upotrebi ili nije oglašavan na Internetu. Zatim su preuzeli vlasništvo nad tim blokom preregistrujući DNS domen koji je bio upisan kao *whois* kontakt za vlasnika tog bloka. Time su stvorili sebi mogućnost da šalju i primaju elektronsku poštu sa ovog domena. Ovo im je omogućilo da “dokažu” vlasništvo

²⁴ <http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>

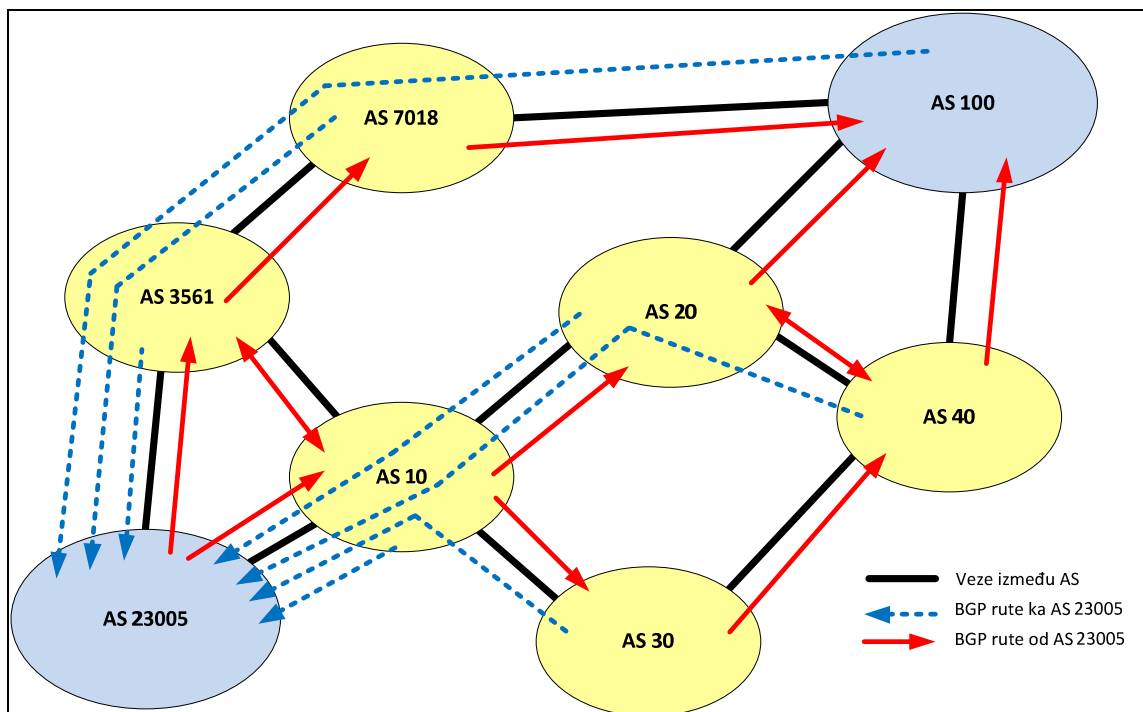
nad pomenutim blokom adresa i da zahtevaju od svog nadprovajdera da prosleđuje njihova BGP oglašavanja za oti blok.

Kao posledica, IP blok sa koga su stizale *spam* poruke je dospao na crnu listu organizacija koje prate aktivnosti spamera kao što su Spamhaus i Spews. Spameri su nesmetano nastavili sa aktivnostima sve dok kompaniji Nortrop Gruman nisu počele da stižu žalbe, posle čega su primetili otmicu bloka. Kompanija je preduzela mere da povрати vlasništvo nad adresama ali je trebalo da prodje dva meseca od početka incidenta dok lažno oglašavanje nije prekinuto.

Ovakvo otimanje IP adresa, međutim, deluje kao trivijalan problem u odnosu na potencijal koji zloupotreba BGP protokola može da ima. Aleks Pilosov i Toni Kapela su na DEFCON-u 16, 2008. godine demonstrirali metodu kojom su uspeli da neotkriveni presretnu internet saobraćaj u obimu za koji se mislilo da nije dostupan nikome van obaveštajnih agencija. Predstavljena je taktika u kojoj se BGP protokol navodi da dozvoli napadaču praćenje nešifrovanog internet saobraćaja bilo gde u svetu, pa čak i da ga modifikuje pre nego što stigne na odredište. U suštini, u pitanju je *man-in-the-middle* napad zbog koga BGP ruteri preusmeravaju podatke ka napadačevoj mreži.

Tehnika koju su koristili Pilosov i Kapela ne iskorišćava bilo kakvu grešku ili nedostatak BGP-a, već koristi uobičajeni način na koji BGP funkcioniše. Prvi korak je bio navođenje internet saobraćaja ka njihovoj mreži (AS100). Ovo su postigli tako što su mrežu koju su napadali oglašavali preko svoje mreže, ali uz kraći AS_PATH atribut i/ili specifičniji prefiks nego što je to zaista bio slučaj. Ruteri koji su dobijali ova oglašavanja su birali njihovu mrežu kao najpovoljniju za tranzit do mreže žrtve (AS23005).

U normalnim okolnostima AS23005 oglašava 10.10.220/22 i tranzit saobraćaja ka njemu je u skladu sa pravilima rutiranja u odnosu na topologiju mreže:



Slika 7.2.1 Tranzit ka AS23005

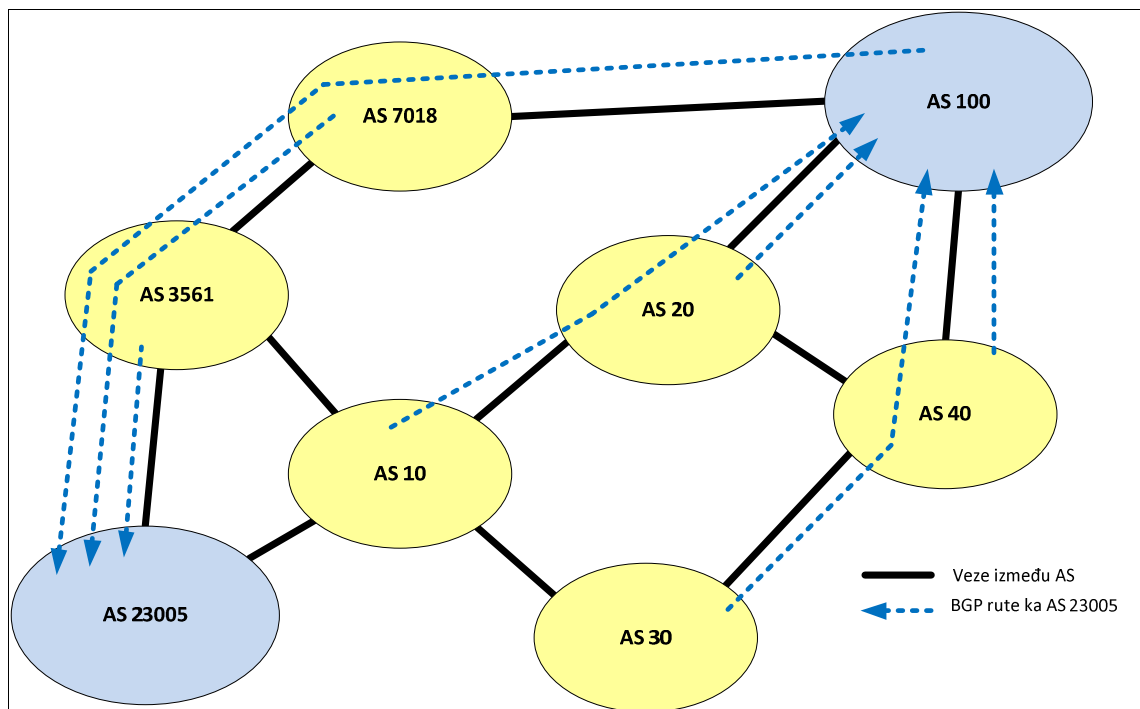
Kao što je bio slučaj sa incidentom sa Pakistan Telekom-om, otimanja IP adresa koje se već koriste se brzo rešavaju jer se brzo primećuje nedostupnost željene destinacije. Imajući ovo u vidu, saobraćaj namenjen AS23005 bi došavši do AS100 bivao predat sledećem AS i odmah zatim ponovo vraćen AS100 (jer svi susedni AS njega posmatraju kao najbolju rutu ka AS23005), tako da praktično ne bi bilo koristi od preusmerenja. Takođe, ovakvo ponašanje bi u relativno kratkom roku bilo otkriveno i sprečeno.

Da bi rešili ove probleme, Pilosov i Kapela su primenili metodu koja se u redovnoj praksi koristi za kontrolu povratnog saobraćaja, *AS_PATH prepending*²⁵ (pripajanje na AS_PATH). Ovom metodom se utiče na to kako rute koje se oglašavaju izgledaju ostatku Interneta, izmenom njihovog sadržaja. Analizom *traceroute* i sopstvenih BGP tabela odabrano je nekoliko rutera (AS7018) kao povratna putanja za saobraćaj ka AS23005, ka kojima su poslate rute sa namerno izmenjenim AS_PATH atributom, usled čega jedino oni nisu videli AS100 kao najpovoljniji put do AS23005, već su pravilno rutirali saobraćaj:

```
route-map hijacked permit 7018
match ip address prefix-list jacked
set as-path prepend 7018 3561 23005
```

Konačno, posle oglašavanja rute 10.10.220.0/24 ka susednim AS i postavljanja statičke rute ka AS7018, saobraćaj je preko AS100 uspešno stizao do AS23005:

```
ip route 10.10.220.0 255.255.255.0 4.3.2.1
```



Slika 7.2.2 Izmenjeni tranzit ka AS23005

²⁵ <http://www.networkengineerdigest.com/2010/12/22/bgp-as-path-prepend/>

Kao dodatnu meru, Pilosov i Kapela su čak vršili izmenu TTL polja u IP zaglavljljima paketa podataka koji su bili u tranzitu ka AS23005, čime su svoju mrežu i aktivnost učinili nevidljivom.

Pre izmene:

```

2 12.87.94.9 [AS 7018] 4 msec 4 msec 8 msec
3 tbr1.cgil.ip.att.net (12.122.99.38) [AS 7018] 4 msec 8 msec 4 msec
4 ggr2.cgil.ip.att.net (12.123.6.29) [AS 7018] 8 msec 4 msec 8 msec
5 192.205.35.42 [AS 7018] 4 msec 8 msec 4 msec
6 cr2-loopback.chd.savvis.net (208.172.2.71) [AS 3561] 24 msec 16 msec 28 msec
7 cr2-pos-0-0-5-0.NewYork.savvis.net (204.70.192.110) [AS 3561] 28 msec 28 msec 28 msec
8 204.70.196.70 [AS 3561] 28 msec 32 msec 32 msec
9 208.175.194.10 [AS 3561] 28 msec 32 msec 32 msec
10 colo-69-31-40-107.pilosoft.com (69.31.40.107) [AS 26627] 32 msec 28 msec 28 msec
11 tge2-3-103.ar1.nyc3.us.nlayer.net (69.31.95.97) [AS 4436] 32 msec 32 msec 32 msec
12 * * * (missing from trace, 198.32.160.134 - exchange point)
13 tge1-2-fr4.ord.llnw.net (69.28.171.193) [AS 22822] 32 msec 32 msec 40 msec
14 ve6.fr3.ord.llnw.net (69.28.172.41) [AS 22822] 36 msec 32 msec 40 msec
15 tge1-3-fr4.sjc.llnw.net (69.28.171.66) [AS 22822] 84 msec 84 msec 84 msec
16 ve5.fr3.sjc.llnw.net (69.28.171.209) [AS 22822] 96 msec 96 msec 80 msec
17 tge1-1-fr4.lax.llnw.net (69.28.171.117) [AS 22822] 88 msec 92 msec 92 msec
18 tge2-4-fr3.las.llnw.net (69.28.172.85) [AS 22822] 96 msec 96 msec 100 msec
19 switch.ge3-1-fr3.las.llnw.net (208.111.176.2) [AS 22822] 84 msec 88 msec 88 msec
20 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 84 msec 88 msec 88 msec
21 66.209.64.85 [AS 23005] 88 msec 88 msec 88 msec
22 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 88 msec 88 msec 88 msec
23 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 88 msec 84 msec 84 msec

```

Posle svih izmena:

```

2 12.87.94.9 [AS 7018] 8 msec 8 msec 4 msec
3 tbr1.cgil.ip.att.net (12.122.99.38) [AS 7018] 4 msec 8 msec 8 msec
4 ggr2.cgil.ip.att.net (12.123.6.29) [AS 7018] 4 msec 8 msec 4 msec
5 192.205.35.42 [AS 7018] 8 msec 4 msec 8 msec
6 cr2-loopback.chd.savvis.net (208.172.2.71) [AS 3561] 16 msec 12 msec *
7 cr2-pos-0-0-5-0.NewYork.savvis.net (204.70.192.110) [AS 3561] 28 msec 32 msec 32 msec
8 204.70.196.70 [AS 3561] 28 msec 32 msec 32 msec
9 208.175.194.10 [AS 3561] 32 msec 32 msec 32 msec
10 gig5-1.esw03.las.switchcommgroup.com (66.209.64.186) [AS 23005] 88 msec 88 msec 84 msec
11 66.209.64.85 [AS 23005] 88 msec 88 msec 88 msec
12 gig0-2.esw07.las.switchcommgroup.com (66.209.64.178) [AS 23005] 84 msec 84 msec 88 msec
13 acs-wireless.demarc.switchcommgroup.com (66.209.64.70) [AS 23005] 88 msec 88 msec 88 msec

```

Po rečima Kapele: “Svi su do sada pretpostavljali da nešto morate poremetiti da bi otmica bila uspešna. Ono što smo utvrdili je da ništa ne moramo da poremetimo. A ako je sve na svom mestu, ko će bilo šta primetiti?”

8. Bezbednosna rešenja za BGP protokol

8.1 Bezbednosna rešenja SIDR radne grupe

Dosadašnji rad na obezbeđivanju sistema rutiranja na Internetu je dao veći broj rešenja, od kojih vredi pomenuti *Secure-BGP* (S-BGP), *Secure Origin BGP* (soBGP), *Pretty Secure BGP* (psBGP), *Internet Routing Registry* (IRR) pa čak i korišćenje AS zapisa resursa u DNS-u, potpisanog preko DNSSEC-a. Zajedničko za sva ova rešenja je da sva zahtevaju postojanje načina za verifikaciju osnovne tvrdnje prilikom oglašavanja rute: da su blok IP adresa i AS brojeva koji se koriste ispravni i da su subjekti koji ih koriste u smislu njihovog oglašavanja ovlašćeni da to rade.

IETF je 2006. godine oformio *Secure Inter-Domain Routing* (SIDR) radnu grupu²⁶ u cilju pronalaženja rešenja za ranjivosti sistema rutiranja. Mehanizmi koji su predloženi kao rešenja moraju da ispune tri glavna zadatka:

- Obezbeđivanje prava na korišćenje adresa
 - ◆ Autentifikacija blokova IP adresa i AS brojeva.
- Obezbeđivanje porekla oglašavanja rute
 - ◆ Da li su subjekti koji izvorno oglašavaju blokove IP adresa i AS brojeve ovlašćeni da to rade.
- Obezbeđivanje propagacije ruta
 - ◆ Mehanizam za proveru da li su svi AS navedeni u AS_PATH atributu BGP poruke ispravni; da li su AS parovi zaista susedni; da li niz navedenih AS brojeva predstavlja stvarnu propagacionu putanju BGP rute.

8.1.1 Digitalni sertifikati

Da bi se razumelo rešenje koje predlaže SIDR radna grupa, neophodno je razumevanje digitalnih sertifikata.

Digitalni sertifikat predstavlja elektronski dokument koji koristi digitalni potpis za povezivanje javnog kriptografskog ključa (iz para ključeva u sistemu kriptografije javnog ključa) sa informacijama o identitetu – nazivu osobe ili organizacije, adrese i slično. Sertifikatom se može verifikovati da javni ključ pripada određenom subjektu.

U uobičajenoj infrastrukturi javnih ključeva (*Public Key Infrastructure* – PKI), strana koja vrši digitalno potpisivanje je sertifikaciono telo (*Certification Authority* – CA). Potpis na sertifikatu predstavlja verifikaciju od strane potpisnika da su informacije o identitetu i javni ključ subjekta sertifikata međusobno povezane.

²⁶ <https://datatracker.ietf.org/wg/sidr/charter/>

```

Certificate:
  Data:
    Version: V3
    Serial Number: 66 8e 9e f0 e7 53 90 de fe 3e 82 af 06 4a 70 ba
    Signature Algorithm: sha1RSA
    Issuer: CN = COMODO High-Assurance Secure Server CA O = COMODO CA Limited L = Salford
           S = Greater Manchester C = GB C=ZA, ST=Western Cape, L=Cape Town,
           O=Thawte Consulting cc, OU=Certification Services Division,
           CN=Thawte Server CA/emailAddress=server-certs@thawte.com
    Valid from: 1. april 2011 2:00:00
    Valid to: 1. april 2016 1:59:59
    Subject: CN = mail.singidunum.ac.rs, OU = Comodo InstantSSL, OU = ERC,
           O = Singidunum University, STREET = Danijelova 32, L = Belgrade, S = Serbia
           PostalCode = 11000, C = RS
    Subject Public Key Info:
      Public Key Algorithm: RSA
      RSA Public Key: (2048 bit)
        30 82 01 0a 02 82 01 01 00 b7 09 7a 9d ed b4 21 38 da ab 04 65 44 7c 97 b0 fe
        dc 90 51 95 41 3c 63 61 2b d5 99 fa 7f 99 9d 50 db 4e 22 33 61 79 cb 59 d6 8c
        cb 57 87 c1 24 85 7e 20 01 56 67 87 08 19 01 fd 3a cb 88 7e e0 0f 56 eb d9 c9
        b7 a4 78 67 81 6f 6b f2 88 51 18 74 24 34 ec da 0c 41 5c e0 89 3d 7f 99 8c 20
        46 e4 de 37 2c 80 e7 e6 6a 38 89 50 a1 6d 0c dc cd 3f 00 7e 35 0e ea 7b 9f 87
        b8 0f c2 ce e8 49 23 91 db 2d c3 e0 c5 1f 68 e8 aa 76 ad 90 16 2e 76 30 f0 f9
        65 3b 64 95 dd ee 94 e9 68 06 0f f9 98 26 15 00 31 29 0a ef 6f 3a cf c5 e0 f0
        15 c9 3c a5 50 23 52 92 50 c6 98 9f b3 3e 19 53 2c 3e a1 47 e6 76 54 29 55 75
        14 32 28 a1 3c fb 17 e7 17 df b5 54 34 b1 8e 45 09 3d 57 d5 82 5b 58 67 f4 a3
        1c fb 1b ae 21 e7 1b 65 79 3a 0f 80 f5 c1 87 f6 e7 c0 14 1e 84 0b 5d 4f 37 2b
        7d 3a 79 6d 5f 02 03 01 00 01
    Thumbprint algorithm: sha1
    Thumbprint: 0a 2c 53 16 f9 2f 8e 5b 8e eb 12 3e cc 98 e8 ef a2 63 1a 86

```

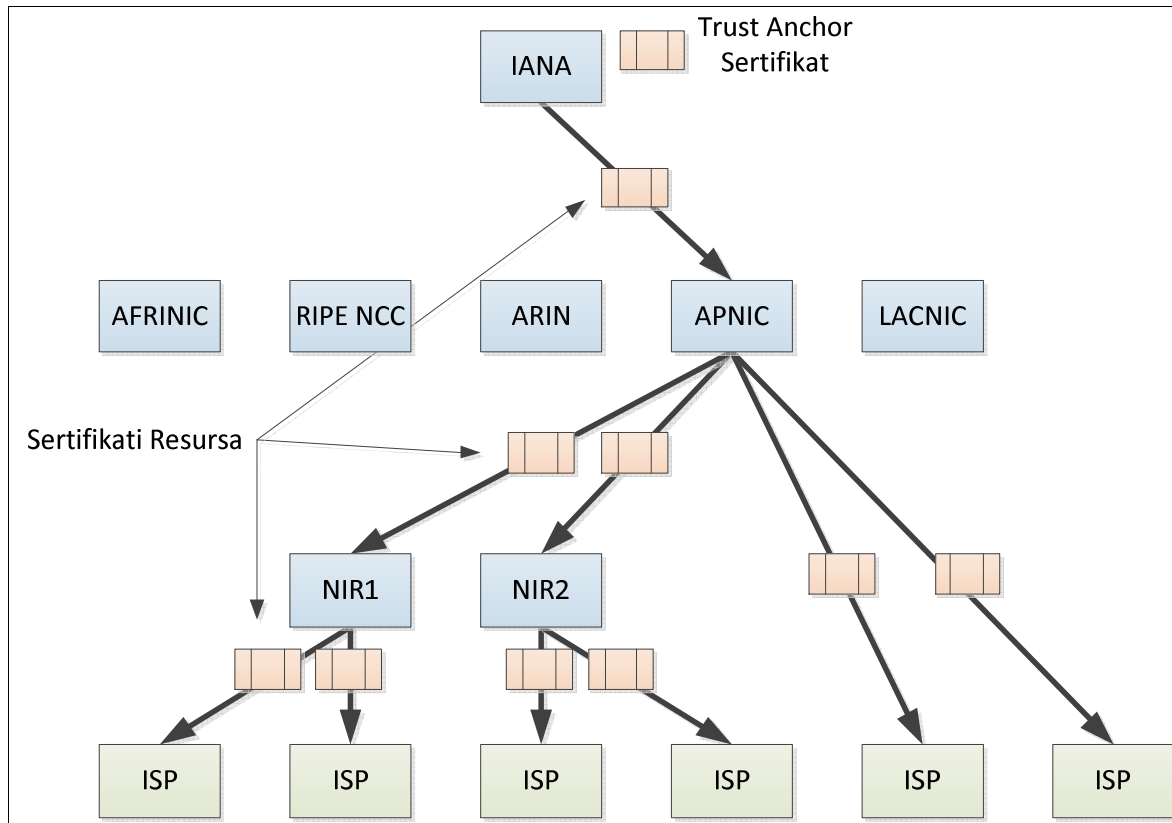
Slika 8.1.1 Digitalni sertifikat Univerziteta Singidunum

8.1.2 Obezbeđivanje prava na korišćenje adresa – RPKI

Infrastruktura javnih ključeva resursa (*Resource Public Key Infrastructure* – RPKI) je rešenje za obezbeđivanje prava na korišćenje IP adresa koje je usvojila SIDR radna grupa. Struktura rešenja je hijerarhija zasnovana na hijerarhiji administrativne dodele resursa, gde se oni raspodeljuju od strane IANA ka regionalnim Registrima, dalje ka nacionalnim i lokalnim Registrima (LIR/NIR) i konačno do krajnjih korisnika. RPKI prati ovu hijerarhiju sertifikatima koji odgovaraju trenutnoj dodeli resursa.

Predviđa se korišćenje “sertifikata resursa” tj. X.509 digitalnih sertifikata koji su u skladu sa PKIX profilom²⁷, prošireni listom IP resursa (IPv4, IPv6 adrese i AS brojevi). Ovi sertifikati služe kao verifikacija da je davalac sertifikata dodelio subjektu sertifikata jedinstveno “pravo na korišćenje” pridruženih IP resursa, po obrascu dodele resursa koju sprovodi IANA i regionalni Internet Registri (RIR). Takav sertifikat omogućava trećoj strani da verifikuje tvrdjenja vezana za dodeljene resurse.

²⁷ <http://tools.ietf.org/html/rfc5280>



Slika 8.2.1 RPKI hijerarhija

U RPKI se koriste dve vrste sertifikata resursa, za različite namene.

CA (*Certification Authority*) sertifikati služe za verifikaciju vlasništva nad blokovima IP adresa i AS brojeva. Njihovo podrazumevano pouzdano polazište (*Trust Anchor*) su, zbog već postojeće hijerarhije, IANA i/ili pet postojećih RIR-a. Sertifikaciona tela koja izdaju ove sertifikate su svi entiteti kojima su ovim putem dodeljeni resursi i koji ih dalje raspodeljuju.

Za razliku od uobičajenih PKI sistema, davalac CA sertifikata može da dodeli subjektu sertifikata proizvoljno ime. Davalac sertifikata, bilo da je RIR, NIR ili ISP, nema zadatak da verifikuje zakonsko pravo subjekta da koristi određeni identitet. Stoga, dodeljivanjem imena kojim se ne označava identitet subjekta, umanjuje se mogućnost da subjekat zloupotrebi sertifikat za lažno predstavljanje, čime se umanjuje pravna odgovornost davaoca sertifikata.

Entiteti koji poseduju CA sertifikat izdaju specifične *End Entity* (EE) sertifikate. Njima se omogućava entitetu da prenese ovlašćenje za resurse koji su mu dodeljeni. EE sertifikati se izdaju po principu “jedan za jedan“, tj. privatni ključ koji se odnosi na svaki EE sertifikat se koristi za potpisivanje samo jednog objekta i svaki objekat se potpisuje samo jednim ključem. Usled ovoga, davalac sertifikata može da kontroliše ispravnost svakog prenetog ovlašćenja.

Sertifikati se objavljuju u repozitorijumima entiteta, a uz njih i registri opozvanih sertifikata (*Certificate Revocation Lists – CRLs*). Ovi registri služe za opozivanje sertifikata koji nisu istekli ali više ne važe. Kada se EE sertifikat kojim je neki objekat potpisan opozove, potpis na tom objektu se smatra nevažećim. Ovako se potpisani objekat može opozvati putem opoziva EE sertifikata kojim je potpisan.

Kako između ključa i sertifikata važi odnos “jedan za jedan”, privatni ključ koji odgovara javnom ključu u sertifikatu se koristi samo jednom i može biti uništen kada se upotrebi za potpisivanje samo jednog objekta. Ovo znatno pojednostavljuje upravljanje ključevima jer se ne mora voditi računa o zaštiti ovih ključeva u dužem vremenskom periodu.

EE sertifikat se smešta u CMS (*Cryptographic Message Syntax*)²⁸ omotač potpisanog objekta, tako da se šalje zajedno sa njim. Takođe, nije potrebno da se EE sertifikat pojavljuje u RPKI repozitorijumima osim kao deo objekta koji potpisuje.

RPKI koristi distribuirani sistem objavljivanja i svaki CA entitet objavljuje svoje „proizvode“ (pre svega EE sertifikate, CRL liste i potpisane objekte) na proizvoljnoj lokaciji (repozitorijumu). Skup svih repozitorijuma predstavlja kompletan RPKI informacioni prostor i od temeljnog je značaja za bezbednost BGP-a u ovom sistemu da kompletan RPKI informacioni prostor bude dostupan bilo kojoj trećoj strani. Takođe, potrebno je da treća strana održava lokalni keš kompletnog skupa distribuiranih repozitorijuma uz redovno sinhronizovanje lokalnih objekata sa izvornim repozitorijumima. Da bi se olakšao ovaj zadatak, na svakom repozitorijumu se koriste manifesti. Manifest je potpisani objekat koji sadrži spisak naziva (i heš vrednosti) svih objekata koji su objavljeni u tom repozitorijumu.

Glavni zadatak RPKI je da omogući proveru digitalno potpisanih informacija i time pruži trećoj strani razlog da veruje u ispravnost potpisanih tvrdnji o adresama i njihovoj upotrebi. Važno je naglasiti da RPKI ne obezbeđuje proveru ispravnosti tvrdnji o identitetu ili ulozi entiteta, već obezbeđuje samo proveru prava na korišćenje IP resursa.

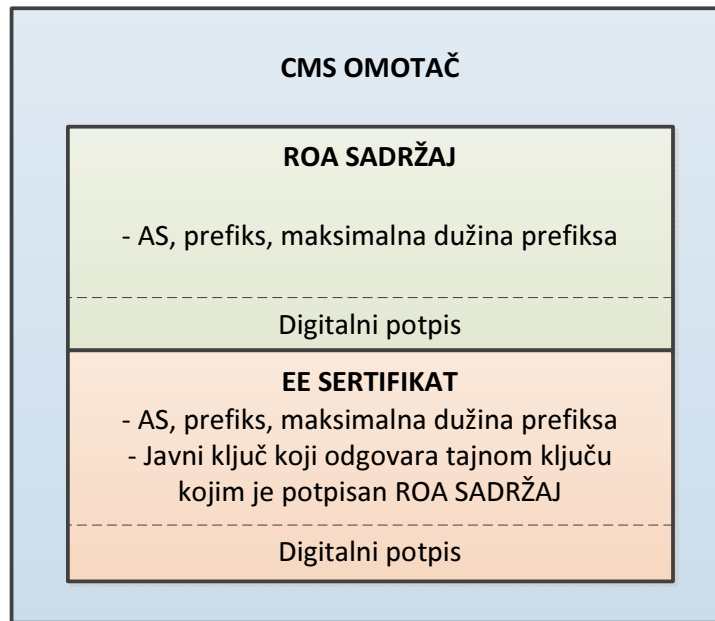
8.1.3 Obezbeđivanje porekla oglašavanja rute – ROA

SIDR radna grupa predviđa da obezbeđivanje porekla oglašavanja rute bude rešeno primenom specifičnih ovlašćenja – ROA (*Route Origination Authorization*)²⁹. ROA predstavlja ovlašćenje kojim se korisniku bloka IP adresa dozvoljava da eksplicitno i sa mogućnošću provere tvrdi da je određeni AS autorizovan da oglašava rute ka jednom ili više prefiksa. ROA se sastoji od dva dela, opšteg CMS šablona zajedničkog za sve potpisane objekte u RPKI i enkapsuliranog sadržaja specifičnog za ROA. U sadržaju ROA se nalaze AS broj, lista IP prefiksa i (opciono, za svaki pojedinačni prefiks) maksimalna dužina prefiksa koji su specifičniji (duži) a koje AS takođe može da oglašava. U okviru istog CMS formata nalazi se i EE sertifikat sa ključem koji se koristi za verifikaciju ROA i listom IP adresa koje moraju da obuhvataju IP prefikse koji su upisani u ROA.

Ispravnost ROA ovlašćenja zavisi od toga da li je potpisnik ROA zaista „ovlašćeni korisnik“ IP prefiksa koji su u njemu navedeni. Ovo se proverava preko pratećeg EE sertifikata. ROA se potpisuje privatnim ključem koji odgovara javnom ključu EE sertifikata. Da bi ROA bilo važeće, prateći EE sertifikat mora biti važeći i IP prefiksi koje sadrži moraju da bude identični sa IP prefiksima upisanim u EE sertifikat. Stoga, rok važnosti ROA predstavlja rok važnosti pripadajućeg EE sertifikata. Takođe, ROA se opozivaju jednostavnim opozivanjem pripadajućeg sertifikata.

²⁸ <http://tools.ietf.org/html/rfc6488>

²⁹ <http://tools.ietf.org/html/rfc6482>



Slika 8.3.1 Format ROA ovlašćenja

Predviđeno je izdavanje posebnog ROA, kojim se AS0 ovlašćuje određenu rutu. Kako je AS0 rezervisani AS broj, koji BGP ruteri nikada ne treba da koriste, ovo ROA ovlašćenje predstavlja „negativno“ ovlašćenje, koje služi da naznači da nijedan AS nije ovlašćen da oglašava rute za prefikse upisane u tom ROA.

Ako i kada ROA kao rešenje bude primenjeno globalno, na svakom ruteru od strane svakog AS na Internetu, prepoznavanje oglašavanja neispravne rute biće vrlo jednostavno, otkrivanjem neispravnog ili nepostojanja ROA. Međutim, u mnogo verovatnijem slučaju delimične primene ovog rešenja (ili prelaznog perioda), kada nisu sva izvorna oglašavanja ruta sa ROA ovlašćenjima, nedostatak ROA se ne može jednostavno tumačiti kao nedozvoljeno korišćenje prefiksa. Da bi se ovo prevazišlo, predviđeno je da proces provere rute može imati tri moguća rezultata³⁰.

Ako je oglašena ruta identična sa podacima sadržanim u ROA (prefiksi i AS broj), čiji EE sertifikat može biti potvrđen u RPKI („ispravan“ ROA), ta ruta se može smatrati „ispravnom“ (*valid*). U slučaju da se oglašena ruta poklapa sa rutom u ispravnom ROA, ali AS koji izvorno oglašava rutu nije isti kao AS broj naveden u ROA, i ako nema drugih ROA koji eksplicitno potvrđuju taj autonomni sistem, ruta se smatra „neispravnom“ (*invalid*). Takođe, u slučaju da je prefiks specifičniji nego što je navedeno u ispravnom ROA, i nema drugih ispravnih ROA za isti prefiks, ta ruta se smatra „neispravnom“. Na kraju, u slučaju da prefiks nije opisan ni u jednom ROA, i ne predstavlja specifičniji prefiks sadržan u nekom drugom ROA, ta ruta se smatra „nepoznatom“ (*unknown*). Ova tri moguća statusa rute se mogu posmatrati na lokalnom nivou kao kriterijum za dodelu prioriteta. Rute sa statusom „ispravna“ bi trebalo da imaju veći prioritet od onih sa statusom „nepoznata“, koje bi, opet, trebalo da imaju veći prioritet od ruta koje se smatraju „neispravnim“. Međutim, ovo je pitanje koje se tiče primene lokalne politike rutiranja i može se, na primer, definisati da sve rute sa statusom „neispravna“ budu odbačene.

³⁰ <http://tools.ietf.org/html/rfc6483>

Ono što je jedinstveno za ovde opisani sistem je način na koji se ROA koriste za potvrđivanje porekla oglašavanja rute. ROA ovlašćenja se objavljuju u RPKI repozitorijumima. Bilo koja treća strana može da koristi lokalni keš ispravnih ROA i da kreira skup filtera za potvrdu, gde svaki elemenat sadrži adresu, ograničenje dužine prefiksa i izvorni AS. Ovaj skup filtera se povezuje sa lokalnim ruterima, umesto samih ROA³¹. Ovaj deo obezbeđivanja rutiranja je potpuno modularan i ne zahteva nikakve izmene u BGP protokolu. Evropski RIPE NCC je razvio alat koji služi upravo u ove svrhe, RPKI Validator³². Njime je moguće prikupiti sva ROA ovlašćenja sa testnih repozitorijuma svih RIR-a, proveriti njihovu ispravnost, postaviti filtere i formirati listu koja se može koristiti u pomenute svrhe. Takođe, RPKI Validator može i direktno komunicirati sa ruterima koji podržavaju RPKI.

The screenshot displays the RPKI Validator web application interface. The top navigation bar includes links for Home, Trust Anchors, ROAs, Ignore Filters, Whitelist, BGP Preview, Export, and Router Sessions. The main content area is divided into two sections: 'Validated ROAs' and 'BGP Preview'.

Validated ROAs Section:

This section shows a list of validated ROAs from various sources: APNIC RPKI Root, ARIN Test Lab, AfriNIC RPKI Root, LACNIC RPKI Root, RIPE NCC RPKI Root, and ripe-pilot. The table below lists the first 10 entries.

ASN	Prefix	Maximum Length	Trust Anchor
1	61.45.250.0/23	23	APNIC RPKI Root
1	61.45.250.0/23	23	APNIC RPKI Root
42	2001:678:3::/48	48	RIPE NCC RPKI Root
42	194.0.42.0/24	24	RIPE NCC RPKI Root
42	2001:678:60::/48	48	RIPE NCC RPKI Root
42	194.0.17.0/24	24	RIPE NCC RPKI Root
174	89.207.56.0/21	21	RIPE NCC RPKI Root
174	2a00:1ed8::/32	32	RIPE NCC RPKI Root
174	91.190.168.0/21	21	RIPE NCC RPKI Root
174	2a02:798::/32	32	RIPE NCC RPKI Root

The table indicates that there are 2,128 total entries, with the first 10 shown.

BGP Preview Section:

This section provides a preview of BGP routes. The table below shows the first 10 entries.

ASN	Prefix	Validity
42	2001:678:3::/48	VALID
42	2001:678:28::/48	UNKNOWN
42	2001:678:4c::/48	UNKNOWN
42	2001:678:60::/48	VALID
42	2001:678:78::/48	UNKNOWN
43	130.199.0.0/16	UNKNOWN
43	192.12.15.0/24	UNKNOWN
43	192.153.161.0/24	UNKNOWN
43	192.203.218.0/24	UNKNOWN
43	2620:10a::/44	UNKNOWN

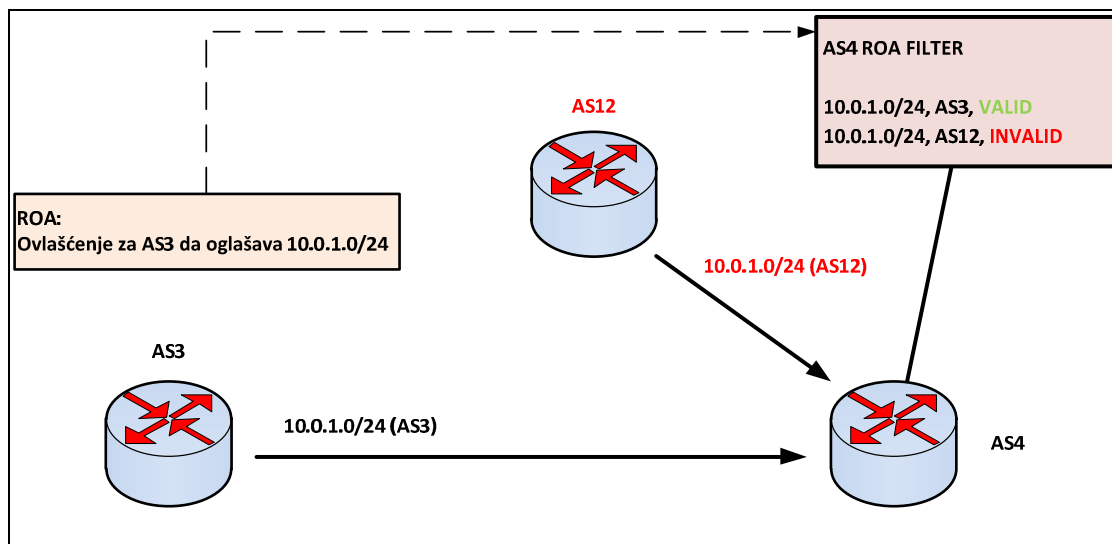
The table indicates that there are 442,028 total entries, with the first 10 shown.

Slika 8.3.2 RIPE NCC RPKI Validator

³¹ <http://tools.ietf.org/html/draft-ietf-sidr-rpki-rtr-26>

³² <http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources>

Sam proces obezbeđivanja porekla oglašavanja rute počinje sa nosiocem prava na adrese, koji generiše parove kriptografskih ključeva i zahteva sertifikaciju svog adresnog prostora od entiteta koji mu je dodelio te adrese. Kada dođe u posed CA sertifikata, nosioc prava je u mogućnosti da generiše EE sertifikat i ROA koji daju ovlašćenje naznačenom AS da oglašava rute za adresni prefiks iz njegovog adresnog prostora. Iz razloga što je svako ROA ovlašćenje vezano samo za jedan EE sertifikat, IP prefiksi koji su upisani u tom ROA moraju biti dodeljeni od strane istog izvora, tj. ne mogu se kombinovati ovlašćenja iz različitih izvora. Ukoliko postoje dodele prefiksa iz različitih izvora, moraju se izdavati višestruka ROA ovlašćenja.



Slika 8.3.3 Filter na osnovu ROA

8.1.4 Obezbeđivanje propagacije ruta – BGPsec

U AS_Path atributu nalazi se lista autonomnih sistema preko kojih se stiže do odredišta navedenog u NLRI BGP Update poruke. Ovu listu dopunjuju svi ruteri kroz koju poruka prođe, dodajući sopstveni broj ispred već navedenih, formirajući niz AS brojeva. Stoga, u svakom momentu u kome se Update poruka kreće kroz Internet, AS_Path predstavlja ispravan tranzitni redosled od lokalnog AS do AS koji je izvorno oglosio rutu. Ovaj atribut je neophodan radi otkrivanja i sprečavanja petlji u rutiranju i služi BGP algoritmu za odabir najpovoljnije rute.

Međutim, postoji bezbednosni problem vezan za ispravnost podataka navedenih u AS_Path atributu. Iskusni napadač može da manipuliše AS_Path atributom i da spreči AS da prihvati rutu dodavajući na listu njegov AS broj³³, ili može, kao što su Pilosov i Kapela pokazali, da učini sopstveni AS povoljnijim za odabir kao najbolje rute, preusmeravajući saobraćaj i efektivno vršeći *man-in-the-middle* napad. RPKI ne pruža skoro nikakvu mogućnost zaštite u ovom slučaju, jer su svi IP prefiksi izvorno oglašeni od strane AS kojima su zaista i dodeljeni, tako da je što se tiče podataka iz RPKI u ovom slučaju sve ispravno.

³³ Uobičajeni filter na BGP ruterima. Ukoliko se u ruti koja se dobije od strane eBGP čvora susednog AS nalazi broj lokalnog AS, poruka se odbacuje.

Da bi se rešio ovaj problem, SIDR radna grupa je predvidela uvođenje posebnog proširenja za proveru ispravnosti ovog atributa – BGPsec (*BGP Security Extensions*)³⁴. Postavljeni zadatak je da svaki ruter može pouzdano da utvrdi da BGP protokol zaista funkcioniše ispravno i da sadržaj AS_Path atributa *BGP Update* poruke predstavlja stvarnu propagacionu putanju između autonomnih sistema, od tačke njenog nastanka do lokalnog AS.

Pitanja na koje predloženo rešenje u svakom trenutku mora da pruži odgovor su:

- Da li su svi AS brojevi u AS_Path atributu ispravni?
- Da li svi uzastopni parovi autonomnih sistema predstavljaju zaista susedni AS (gde oba AS iz tog para mogu da potvrde da su susedni)?
- Najvažnije, da li niz AS brojeva predstavlja stvarnu propagacionu putanju BGP *Update* poruke?

BGPsec proširuje RPKI sistem dodavanjem još jednog sertifikata, EE sertifikata BGP rutera, kojim se AS broj vezuje za javni ključ, čiji se pripadajući tajni ključ nalazi na jednom ili više BGP rutera u okviru tog AS. Ovaj tajni ključ se koristi za potpisivanje BGP *Update* poruka od strane samih BGP rutera, a „u ime“ lokalnog autonomnog sistema. Ovo omogućava da se utvrdi da li je BGP *Update* poruka zaista potpisana od strane BGP rutera koji pripada navedenom AS.

BGPsec predviđa uvođenje novog opcionog, neprenosivog atributa BGPSEC_Path_Signatures. On se sastoji od niza potpisa, po jedan za svaki AS kroz koji BGP *Update* poruka prodje. Novi potpis u ovom atributu se dodaje svaki put kada se *Update* poruka šalje susednom AS i BGPSEC_Path_Signatures potpuno zamenjuje AS_Path atribut.

Proces obezbeđivanja počinje od izvornog BGP rutera koji oglašava novu rutu. Ovaj ruter dodaje BGP *Update* poruci BGPSEC_Path_Signatures atribut u koji unosi svoj digitalni potpis. Ovaj potpis štiti NLRI polje, AS broj izvornog AS (sopstveni) i AS broj rutera kome se šalje *Update* poruka. Ovde je važno napomenuti da, za razliku od uobičajene prakse, BGPsec ne dozvoljava višestruka odredišta sa istim skupom atributa, tj. moguće je koristiti samo jedan prefiks u NLRI. Kada BGP ruter primi BGPsec *Update* poruku i namerava da propagira rutu koja je u njoj upisana, on dodaje sopstveni potpis u BGPSEC_Path_Signatures atribut. Ovaj potpis štiti sve što je zaštićeno prethodnim potpisom uz dodatak AS broja čvora kome se šalje *Update* poruka.

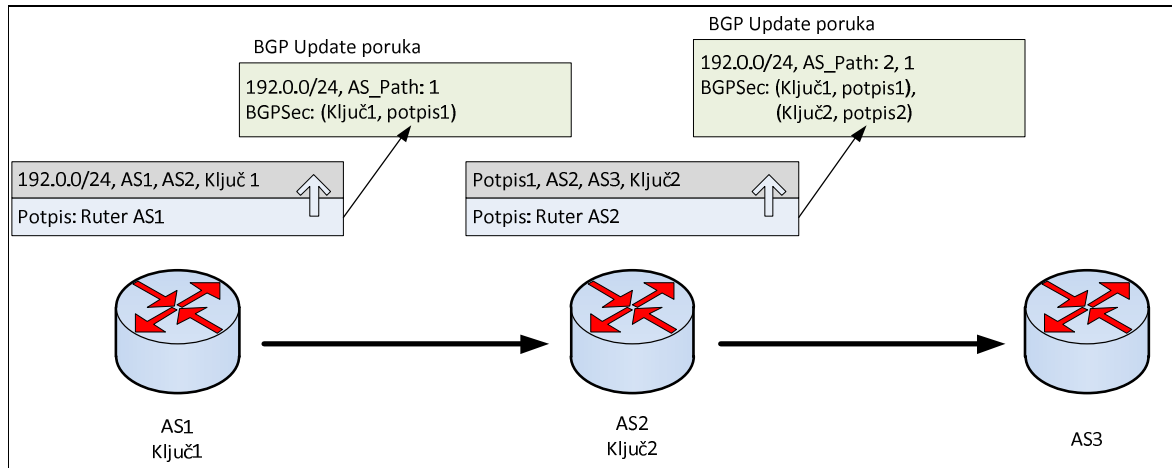
Na primer, AS1 izvorno oglašava rutu 192.0.2/24 i šalje je AS2, koja je prosleđuje ka AS3. Kada ruta stigne do AS3, sadržaće sledeće podatke:

- NLRI: 192.0.0/24
- AS_Path: 3.2.1
- BGPSEC_Path_Signatures atribut sa 2 potpisa:
 - Potpis od AS1 koji pokriva: 192.0.0/24, AS1 i AS2
 - Potpis od AS2 koji pokriva: Sve što je pokrio potpis AS1, AS3

Kada BGP ruter u AS3 primi BGPsec *Update* poruku, njena ispravnost se potvrđuje proverom potpisa. Prvo se proverava potpis za izvorni AS, AS1. Potpis se proverava korišćenjem javnog ključa iz EE sertifikata BGP rutera AS1. Ovaj postupak se ponavlja za potpis AS2.

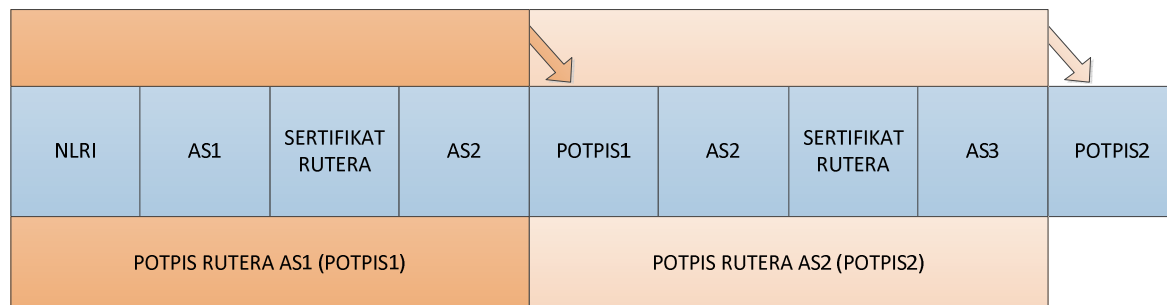
³⁴ <https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-overview>

Ukoliko se svi potpisi mogu potvrditi na ovaj način, smatra se da je *Update* poruka zaista stigla putem koji je naznačen u BGPSEC_Path_Signatures atributu.



Slika 8.4.1 Zaštita AS_Path atributa putem BGPSEC-a

Ovakvo preklapanje potpisa omogućava prijemnoj strani BGP *Update* poruke da koristi preklapajući niz digitalnih potpisa u cilju potvrđivanja (za svaki AS u BGPSEC_Path_Signatures) da je odgovarajući potpis ispravno generisan „u ime“ autonomnog sistema iz BGPSEC_Path_Signatures, i da se sledeći AS u putanji poklapa sa sledećim AS u potpisanim podacima. Takođe, ovakvo „potpisivanje unapred“ gde je obuhvaćen i AS kome se *Update* šalje sprečava *man-in-the-middle* napad u smislu preusmeravanja saobraćaja namenjenog susednom AS.



Slika 8.4.2 Preklapanje potpisa u BGPSEC-u

Korišćenje EE sertifikata uz potpisane BGP *Update* poruke uvodi još jednu promenu u pravila rutiranja. U BGP-u bez bezbednosnih proširenja oglašena ruta se smatra ispravnom sve dok se eksplicitno ne oglasi nevažećom ili dok se ne prekine BGP sesija sa čvorom koji je oglasio. U BGPSEC-u, sva oglašavanja imaju rok isteka koji se dodeljuje od strane izvornog rutera. Ovaj rok predstavlja rok isteka EE sertifikata kojim je potpisana *Update* poruka, čijim istekom ruta postaje nevažeća. Ovo znači da izvorni ruter mora periodično da ponovo ogłosi rutu i da periodično „osveži“ vreme isteka pripadajućeg digitalnog potpisa.

8.1.5 Konfigurisanje rutera za rad sa RPKI

Prvi korak u konfigurisanju rutera za rad sa RPKI je uspostavljanje komunikacije sa RPKI Validator servisom. Naveden je primer konfigurisanja CISCO RPKI rutera na IP 10.1.1.6.

```
cisco-rpki-rtr#show running-config | begin bgp

router bgp 64500
  bgp log-neighbor-changes
  bgp rpki server tcp 10.1.1.6 port 8282 refresh 600
```

Sledeći korak je definisanje politike rutiranja na osnovu „stanja ispravnosti“. U skladu sa IETF standardima³⁵, prednost imaju ispravne (*valid*) nad neispravnim (*invalid*) i ispravne i nepoznate (*unknown*) nad neispravnim. U ove svrhe se koristi *local-preference* parametar.

```
!
route-map rpki-loc-pref permit 10
  match rpki invalid
  set local-preference 90
!
route-map rpki-loc-pref permit 20
  match rpki not-found
  set local-preference 100
!
route-map rpki-loc-pref permit 30
  match rpki valid
  set local-preference 110
```

Poslednje podešavanje je primena postavljene politike rutiranja na susedne BGP čvorove, u ovom slučaju ruter na adresi 10.1.1.2.

```
cisco-rpki-rtr#show running-config | begin bgp

router bgp 64500
  bgp log-neighbor-changes
  bgp rpki server tcp 10.1.1.6 port 8282 refresh 5
  network 192.0.2.0
  neighbor 10.1.1.2 remote-as 64510
  neighbor 10.1.1.2 route-map rpki-loc-pref in
!
```

Posle podešavanja sledi provera veze sa RPKI Validator servisom.

```
cisco-rpki-rtr>show ip bgp rpki server
BGP SOVC neighbor is 10.1.1.6/8282 connected to port 8282
Flags 64, Refresh time is 300, Serial number is 4, Nonce is 9169
InQ has 0 messages, OutQ has 0 messages, formatted msg 4
Session IO flags 3, Session flags 4008
Neighbor Statistics:
  Prefixes 1391
  Connection attempts: 32
  Connection failures: 0
  Errors sent: 0
  Errors received: 0
```

³⁵ <http://tools.ietf.org/html/rfc6483>

```
cisco-rpki-rtr>show ip bgp rpki table
1030 BGP sovc network entries using 90640 bytes of memory
1113 BGP sovc record entries using 22260 bytes of memory

Network          Maxlen  Origin-AS  Source  Neighbor
24.232.0.0/16    32      10318      0       10.1.1.6/8282
31.3.8.0/21      21      5524       0       10.1.1.6/8282
31.7.8.0/21      21      8676       0       10.1.1.6/8282
...
217.198.192.0/20 20      197077     0       10.1.1.6/8282
217.199.224.0/20 24      25299      0       10.1.1.6/8282
217.224.0.0/11   11      3320       0       10.1.1.6/8282
```

Na kraju, može se proveriti kako se postavljena pravila primenjuju na rute.

```
cisco-rpki-rtr>sh ip bgp 93.175.146.0/24
BGP routing table entry for 93.175.146.0/24, version 8995350
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
64510 3333 12654, (received & used)
 10.1.1.5 from 10.1.1.2 (10.1.1.2)
   Origin IGP, localpref 110, valid, external, best
   path 51012284 RPKI State valid
```

```
cisco-rpki-rtr>sh ip bgp 93.175.147.0/24
BGP routing table entry for 93.175.147.0/24, version 8995351
Paths: (1 available, no best path)
Not advertised to any peer
Refresh Epoch 1
64510 3333 12654, (received & used)
 10.1.1.5 from 10.1.1.2 (10.1.1.2)
   Origin IGP, localpref 90, valid, external
   path 510122C8 RPKI State invalid
```

```
cisco-rpki-rtr>sh ip bgp 84.205.83.0/24
BGP routing table entry for 84.205.83.0/24, version 5427340
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
64510 3333 12654, (received & used)
 10.1.1.5 from 10.1.1.2 (10.1.1.2)
   Origin IGP, localpref 100, valid, external, best
   path 2609454C RPKI State not found
```

Za potrebe testiranja, trenutno se može koristiti javno dostupni CISCO RPKI ruter, povezan sa RIPE NCC RPKI Validatorom, na adresi **rpki-rtr.ripe.net**.

9. Budućnost rutiranja i Interneta

Rutiranje i adresiranje predstavljaju srž funkcionisanja Interneta. Oni su više od tehničko-operativnog procesa – predstavljaju važan oblik upravljanja Internetom. Infrastruktura javnih ključeva resursa, sa predloženom hijerarhijom digitalnih sertifikata, može imati dalekosežan uticaj na budućnost Interneta.

Ono što je izvesno da će se uvođenjem RPKI sigurno dogoditi je dovođenje u pitanje nezavisnosti Internet provajdera, izmena upravljačke uloge Regionalnih Internet Registara i promena odnosa između IANA i RIR-a. U najboljem slučaju, sprečiće namerno i nenamerno izazvane probleme u rutiranju i omogućiti efikasnije i fleksibilnije korišćenje adresnih resursa. U najgorem slučaju, mogla bi da u velikoj meri centralizuje moć nad Internetom, stvarajući političke težnje da se ostvari uticaj na kontrolu korisnika Interneta.

Uprkos ovome, javna svest i diskusije o RPKI su uglavnom svedene na uzak tehnički krug, od kojih je većina van vidokruga javnosti. Čak i u okviru stručne zajednice, diskusija o implikacijama RPKI na upravljanje Internetom je vrlo slaba. Razlog za ovo može biti u tome da je politika rutiranja (samim tim i RPKI) zapostavljena iz istog razloga iz koga su to i mnogi drugi aspekti upravljanja Internetom: analiza ove problematike zahteva retku kombinaciju stručnih, operativnih, institucionalnih, ekonomskih i političkih znanja vezanih za Internet. Ljudi koji razumeju tehnološke standarde i način rada retko poseduju stručnost u oblasti javne politike, institucionalnog projektovanja ili ekonomije. Sa druge strane, ljudi sa stručnošću iz oblasti ekonomije i javne politike retko poseduju razumevanje tehnologija i načina rada. Čak i za stručnjake, RPKI i kompromisi koji se njime prave u smislu šta se dobija a šta gubi, su komplikovani. Uz sve to, strane koje učestvuju u dogovaranju rešenja i pristupa problematici – kao što su Internet Registri, vojni preduzimači iz SAD, Internet provajderi, dobavljači opreme itd. nemaju interesovanje da pokreću kritičke i sveobuhvatne dijaloge o upravljačkim implikacijama njihovih postupaka. Njihov cilj je da izbegnu politiku koliko god je to moguće i da postignu dogovor koji će u najmanjoj mogućoj meri poremetiti postojeću praksu.

Najvažnija osobina predloženog RPKI rešenja je pokušaj da se sertifikati resursa povežu sa autoritativnim izvorima internet resursa, tj. ICANN-om i RIR-ima. Po rečima jednog člana *Internet Architecture Board* (IAB) pri IETF, RPKI može biti upotrebljen da dozvoli institucijama koje kontrolišu dodelu IP adresa kontrolu nad time šta se rutira (samim tim i koje informacije su dostupne) na Internetu³⁶.

9.1 Autonomija Internet provajdera

Na Internetu kakav postoji danas, razdvojene su odgovornosti dodele adresa i odgovornosti za rutiranje. RIR-i vrše registraciju i beleže dodelu blokova adresa da bi se isti održali jedinstvenima. Iako provajderi koriste baze podataka RIR-a, oni u potpunosti kontrolišu i ovlašćuju koje rute se oglašavaju, i sami odlučuju koja oglašavanja ruta drugih provajdera

³⁶ D. McPherson, "IPv4 Exhaustion: Trading Routing Autonomy for Security." Arbor Networks blog

prihvataju ili filtriraju. Drugim rečima, autoritet koji Registri poseduju nad korišćenjem adresa je skoro u potpunosti zasnovana na spremnošću provajdera da koriste njihove baze podataka kao koordinacione alate.

RPKI sve ovo menja, jer ima potencijal da Registrima dozvoli direktan uticaj na rutiranje. Dejvid Konrad, direktor IANA u to vreme, napisao je 2009. sledeće na SIDR listi:

„Danas, uticaj Registrara na rutiranje je u suštini savetodavna – ako, na primer, korisnik adresa ne uplati nadoknadu za održavanje, najviše što RIR može da uradi je da ukloni njegov blok adresa iz *whois* baze podataka. Međutim, kako sam ja razumeo, ovo ima ograničen efekat na postojeće rutiranje. RIR bi mogao da dodeli te iste adrese nekom drugom, ali bi ovo bio dobar način za stvaranje neprijatnosti svim stranama (ne samo strani od koje su adrese oduzete). Ako bi bili postavljeni filteri ili bi ruteri proveravali autentičnost porekla preko RPKI, izgleda da bi značajno više kontrole bilo smešteno u svaki čvor u hijerarhiji, sve do root-a RPKI. Plašim se da bi ovo bilo jednostavno neprihvatljivo u političkom ili poslovnom smislu.“³⁷

Jedan od ključnih problema vezanih za upravljanje tiče se uslova pod kojim bi sertifikati bili opozivani. Na primer, kada je RIPE NCC predložio implementaciju sertifikata resursa, njegovi članovi su to odbili usled zabrinutosti vezane za trajanje ispravnosti sertifikata i vezivanjem opoziva sertifikata sa statusom članstva u RIPE. Učesnici su komentarisali da će „ljudi biti nevoljni da koriste sertifikate resursa ako imaju razloga da se boje da rutiranje može biti prekinuto usled neočekivanih okolnosti vezanih za opoziv sertifikata“³⁸. Takođe, bilo je i tvrdnji da neke Vlade vide mogućnost Registrara da opozivaju sertifikate (samim tim teorijski spečavajući rutiranje prefiksa) kao povredu nacionalnog suvereniteta.³⁹

Neke od političkih implikacija je primetio D. Mekfirson, član IAB: „Ako bi neka zemlja u čijem posedu se nalaze ključevi (*trust anchor*) zaratila sa nekom drugom i odlučila da želi da opozove sve dodeljene resurse, Internet provajderi ne bi imali nikakvu kontrolu nad ovim van svog domena rutiranja“.⁴⁰

9.2 Model poverenja i kompatibilnost

Ako RPKI ima potencijal da centralizuje moć, postavlja se pitanje gde bi ova moć mogla da bude centralizovana. Konkretno, koja organizacija ili institucija bi bila pouzdano polazište (*trust anchor*) za hijerarhiju sertifikata?

U uobičajenoj infrastrukturi javnih ključeva, sve strane veruju jednom CA, tj. i pošiljalac i primalac informacije se oslanjaju na isti CA. Ovakva centralizacija se postiže relativno lako kada se radi o jednoj organizaciji. Međutim, ovo postaje sve teže kako broj organizacija koje koriste ovo postaje veći i raznovrsniji. Kada je reč o globalnom Internetu, koji obuhvata preko 35.000 autonomnih sistema i stotine hiljada korisnika IP resursa raštrkanih preko stotina različitih jezičkih grupa i političkih sistema, centralizacija i jedinstvo oko pouzdanog polazišta može postati nerealan, pa čak i remetilački i opasan cilj.

³⁷ <http://www.ietf.org/mail-archive/web/sidr/current/msg01098.html>

³⁸ <http://www.ripe.net/ripe/maillists/archives/ca-tf/2009/msg00013.html>

³⁹ <http://www.ripe.net/ripe/maillists/archives/ca-tf/2010/msg00008.html>

⁴⁰ <http://www.ietf.org/mail-archive/web/sidr/current/msg00346.html>

Kad god se stvara centralizovan, striktno hijerarhijski model poverenja, uz njega se stvara i potencijal za centralizaciju političkog i regulatornog autoriteta nad Internetom. Scenarij sličan ovom se već odigrava sa Sistemom imenovanja domena (DNS), koji predstavlja hijerarhijski sistem imena. Sa tehničke tačke gledišta, celokupan posao administratora *root*-a je da koordinira dodelu naziva domena najvišeg nivoa (*top level domains*), da bi svi ostali jedinstveni i da ne dođe do pojave duplikata. Međutim, koncentracija moći na *root*-u stvara interesovanje od strane političkih, vojnih i poslovnih aktera. Na primer, ICANN reguliše raspodelu *top level* domena (ali i *second level* domena) na način koji se prilagođava političkim zahtevima za zaštitu postojećih zaštitnih znakova i autorskih prava, podržava kontrolu nacija nad geografskim nazivima, itd.

Pitanje upravljanja vezano za kontrolu *root*-a nije razjašnjeno ni kada su *Number resource Organization* (NRO, asocijacija RIR-a) i IAB objavili saopštenja na ovu temu 2009. i 2010. godine. U oba saopštenja se podržava „jedinstveno, autoritativno pouzdano polazište“ za RPKI, ali se takođe izražava spremnost da se dozvoli trećim stranama da samostalno odaberu pouzdano polazište, ali ništa detaljnije.^{41 42} Ovakva mogućnost izbora se može pokazati kao varljiva. Iako bi mogućnost da ISP samostalno odabere pouzdano polazište mogla dovesti do heterogenijeg ali kompatibilnog sertifikacionog sistema, isto tako je moguće da Vlade država ili ICANN/RIR sistem odluči da zahteva sertifikaciju kao preduslov za dobijanje adresnih resursa (kao predsednik, ICANN je 2012. odlučio da zahteva implementaciju DNSSEC-a za sve nove *top level* domene⁴³). Takođe, vrlo je verovatno da kada RPKI sistem dostigne kritičnu masu, fokus postane jedno, centralizovano pouzdano polazište, što bi stvorilo probleme sa kompatibilnošću za provajdere koji ne bi koristili isto polazište. Dok god je nejasno kako se u primeni RPKI rešava problem kompatibilnosti između različitih *root*-ova, bilo bi naivno smatrati da je u RPKI dozvoljen slobodan izbor pouzdanih polazišta – kao što bi bilo naivno misliti da svako ko želi da formira alternativni DNS *root* može to da uradi bez problema.

Pitanje koji tip pouzdanog polazišta bi trebalo koristiti i kako bi trebalo izbeći probleme povezane sa više ili manje centralizovanim sistemom, predstavlja globalno pitanje upravljanja Internetom od najvišeg značaja. U ovom trenutku je jasno da entiteti koji su do sada odlučivali – IETF, IAB i NRO – nisu učinili dovoljno da bi pronašli zadovoljavajuće rešenje.

Rutiranje i dodela i raspoređivanje IP adresa su duboko međuzavisni. Stoga, politika o IP adresama, od ICANN-a kroz regionalne Internet Registre, biće duboko zahvaćena uvođenjem RPKI. Metode i politike rutiranja imaju regulatorne implikacije kao i implikacije vezane za sprovođenje zakona – kako za one koji bi pokušali da kontrolišu Internet tako i za one koji bi pokušali da ga održe zaštićenim od proizvoljnih intervencija.

⁴¹ NRO statement on RPKI, <http://nro.net/pipermail/nro-announce/2009-July/000044.html>

⁴² IAB statement on the RPKI, <http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html>

⁴³ <http://www.dnssec-deployment.org/index.php/2012/01/new-gtlds-will-support-dnssec-from-the-start/>

Zaključak

U ovom radu su predstavljeni sistem imenovanja domena (DNS) i rutiranje na Internetu, kao i način na koji oni funkcionišu. U trenutnom stanju, ovi sistemi kao fundamentalni za rad Interneta, samim tim i Internet u celini, podložni su zloupotrebi. Opisana su bezbednosna proširenja sistema, DNSSEC i RPKI/BGPsec, koja uz pomoć kriptografije javnog ključa uvode elemente autentičnosti izvora i verifikacije integriteta. Ove promene su od velikog značaja za sveobuhvatnu bezbednost na Internetu.

U predloženom rešenju za obezbeđivanje DNS-a, DNSSEC, postoje specifični zahtevi da softver koji se koristi za DNS bude adekvatno prilagođen i pravilno podešen. Opisana je implementacija DNSSEC-a za *de facto* standard kada su u pitanju DNS serveri – BIND. Kako je ponekad i sam DNS dovoljno težak za razumevanje, edukacija o pravilnoj upotrebi DNSSEC-a mora biti visoko na listi prioriteta kada je održavanje i obezbeđivanje Interneta u pitanju.

Posebna pažnja je posvećena društveno-političkim dešavanjima koja utiču na odluke o budućnosti DNS-a a samim tim i Interneta. U svetu a naročito u SAD vlada tendencija da se bezbednost uopšte podigne na mnogo veći nivo nego što je danas, pa to sa sobom povlači reorganizaciju administrativnog sistema i donošenje zakona koji bi trebalo da učine Internet bezbednijim za sve. Međutim, postoji realna opasnost da sloboda govora, privatnost i prava krajnjih korisnika Interneta budu žrtve najavljenih mera i svaki oprez u ovom domenu itekako je opravdan.

Sistem rutiranja na Internetu, u trenutnom stanju, takođe sadrži esencijalne bezbednosne nedostatke. Opisan je predlog SIDR radne grupe, infrastruktura javnih ključeva resursa (RPKI), koja uz pomoć digitalnih sertifikata i digitalnih potpisa, tj. pomoću kriptografije javnog ključa, ima mogućnost da reši mnoge probleme sa kojima se sistem rutiranja trenutno suočava.

Međutim, u ovom trenutku postoje nedoumice vezane za primenu RPKI. Neophodna je veća diskusija o ovom sistemu kao i o njegovim implikacijama na upravljanje internetom. Tehnička ekspertiza u vidu IAB i IETF je dragocena, ali ne sme biti neporeciva. Da bi se došlo do kvalitetnog rešenja od koje će korist imati svi ali pre svega Internet zajednica, potrebno je uključiti i druge forme eksperata kao i pokrenuti što obimnije javne rasprave o svim aspektima obezbeđivanja sistema rutiranja.

„Postoji puno ljudi koji ne posmatraju bezbednost i slobodu kao robu za razmenu, koja se menja jedna za drugu ili se njima balansira, već kao elemente iste celine. Misliti da deo jedne može biti menjan za deo druge deluje pogrešno, opasno, nepravedno i neslobodno. Smatrajući da stručni rad koji nastavlja ovakvu praksu ima veliku važnost za građanske slobode (ili bezbednost) je u najboljem slučaju pogrešno a u najgorem prividno i naivno”⁴⁴

⁴⁴ <http://www.opendemocracy.net/ourkingdom/dr-michael-lister-dr-lee-jarvis/counter-terrorism-review-trading-liberty-for-security>

Određivanje najbolje budućnosti za rutiranje i DNS nije pitanje na koje se lako može dati odgovor. Faktori koji utiču na njihovo funkcionisanje su različiti, od tehničkih do političkih, i često nije lako odabrati pravo rešenje za probleme koji svakim danom postaju sve veći. Ali, u svakom slučaju, rasprave o ovoj temi su veoma važne i neophodno je da ih bude što više. Kako sve više ljudi u svetu postaje svesno značaja i praktične koristi Interneta i uključuje Internet u svoje svakodnevne živote, svaka promena koja utiče na njegov rad imaće sve veće implikacije.

Literatura

1. Albitz, P. i Liu, C. (2006) – **DNS and BIND, Fifth Edition**, O'Reilly Publishing, maj 2006.
2. Aitchinson, R. (2005) – **Pro DNS and BIND**, Apress publishing.
3. Kabelová, A. i Dostálek, L. (2006) – **DNS in Action**, Packt Publishing.
4. Mockapetris, P. et al (1987) – **RFC 1035: Domain Names – Implementation and specification**, IETF.
5. Atkins, D i Austein, R. (2004) – **RFC 3833: Threat Analysis of the Domain Name System (DNS)**, IETF.
6. Arends, R. et al (2005) – **RFC 4033: DNS Security Introduction and Requirements**, IETF.
7. Arends, R. et al (2005) – **RFC 4034: Resource Records for the DNS Security Extensions**, IETF.
8. Arends, R. (2005) – **RFC 4035: Protocol Modifications for the DNS Security Extensions**, IETF.
9. Franks, J. et al (1999) – **RFC 2617: Extension Mechanisms for DNS (EDNS0)**, Paul Vixie, IETF
10. Bono, V. (1997) –, **7007 Explanation and Apology**, Merit Network email list archives <http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html>
11. http://renesys.com/blog/pakistan_blocking_order.pdf
12. RIPE NCC (2008) – **YouTube Hijacking: A RIPE NCC RIS case study**. <http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>
13. Parks, J. (2010) – **BGP AS-Path Prepending**, <http://www.networkengineerdigest.com/2010/12/22/bgp-as-path-prepend/>
14. **Povelja Secure Inter-Domain Routing (SIDR)** radne grupe, <https://datatracker.ietf.org/wg/sidr/charter/>
15. Cooper, D. et al (2008) – **RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**, IETF. <http://tools.ietf.org/html/rfc5280>
16. Lepinski, M. et al (2012) – **RFC 6488: Signed Object Template for the Resource Public Key Infrastructure (RPKI)**, IETF. <http://tools.ietf.org/html/rfc6488>
17. Lepinski, M. et al (2012) – **RFC 6482: A Profile for Route Origin Authorizations (ROAs)**, IETF. <http://tools.ietf.org/html/rfc6482>

18. Huston, G. et al (2012) – **RFC 6483: Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)**, IETF. <http://tools.ietf.org/html/rfc6483>
19. Bush, R et al (2012) – **The RPKI/Router Protocol, draft-ietf-sidr-rpki-rtr-26**, IETF. <http://tools.ietf.org/html/draft-ietf-sidr-rpki-rtr-26>
20. RIPE NCC (2011) – **RIPE NCC RPKI Validator**. <http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources>
21. Lepinski, M. et al (2012) – **An Overview of BGPSEC, draft-ietf-sidr-bgpsec-overview-02**, IETF. <https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-overview>
22. McPherson, D. (2008) – **IPv4 Exhaustion: Trading Routing Autonomy for Security**, Arbor Networks blog. <http://ddos.arbornetworks.com/2008/03/ipv4-exhaustion-trading-routing-autonomy-for-security/>
23. Number resource Organization (2009) – **NRO statement on RPKI**. <http://nro.net/pipermail/nro-announce/2009-July/000044.html>
24. Internet Architecture Board (2010) – **IAB statement on the RPKI**, IETF. <http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html>
25. Michael, L. et al (2011) – **The Counter-Terrorism Review: Trading liberty for security**, OpenDemocracy. <http://www.opendemocracy.net/ourkingdom/dr-michael-lister-dr-lee-jarvis/counter-terrorism-review-trading-liberty-for-security>
26. <http://www.dnssec.net/>
27. <http://www.icannwatch.org/>
28. <http://www.internetgovernance.org/>
29. <http://www.isc.org/>
30. <http://www.networkdictionary.com/>
31. <http://www.root-servers.org/>
32. <http://www.securityfocus.com/>
33. <http://www.wikipedia.org/>
34. <http://bgp.potaroo.net/>