BGP: Analiza i simulacija napada otimanjem prefiksa

Dunja Majstorović

***Sadržaj* — Protokol graničnog mrežnog prolaza, BGP (*Border Gateway Protocol*), je ruting protokol, koji definiše pravila komunikacije i omogućava međusobno povezivanje svih nezavisnih računarskih mreža u okviru Interneta. U ovom radu je najpre dat pregled osnovnih BGP pojmova i poznatih mana vezanih za bezbednost protokola. Zatim su predstavljene tri najrasprostranjenije nadogradnje, razvijene da odgovore na bezbednosne izazove: S-BGP, IVR i SoBGP. Funkcionalnost i karakteristike BGP nadogradnji su testirane korišćenjem programa GNS3 u okviru koga je u *backbone* mreži simuliran napad otimanjem prefiksa u različitim okolnostima: bez zaštite (sa osnovnom konfiguracijom), nakon primene filter liste, i na kraju, uz manipulaciju osnovnih BGP atributa. Pored simulacije i rezultata, u radu je data detaljna analiza predloženih rešenja.**

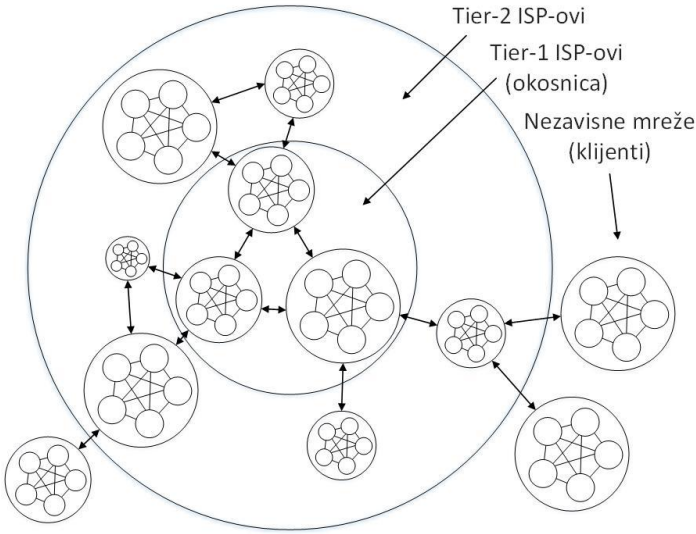
***Ključne reči* — Bezbednosni izazovi, BGP, mehanizmi zaštite.**

I. UVOD

INTERNET je, sa milionima povezanih računara, komunikacionih linkova i mrežnih uređaja, milijardama korisnika koji se povezuju putem prenosivih računara, tableta i pametnih telefona, kao i nizom novih povezanih uređaja (senzora, veb kamera, igračkih konzola, okvira za slike, pa čak i kućnih aparata) najveći inženjerski sistem koji je čovečanstvo ikada kreiralo. Internet mreža se u poslednjoj dekadi razvila u veoma složenu, hijerarhijski organizovanu strukturu. Današnji internet – mreža svih mreža – sastoji se od sedamnaest posrednika internet usluga (eng. *Internet Service Provider* – ISP) 'prvog reda' (okosnica mreže) i stotina hiljada posrednika 'nižih redova' (pridruženi sistemi). Neke od kompanija koje spadaju u provajdere prvog, najvišeg nivoa su AT&T, Sprint, NTT, Verizon i France Telecom, a takođe se

Dunja Majstorović, Računarski fakultet, Knez Mihailova 6/VI, 11000 Beograd (e-mail: majstorovic.dunja.rs@ieee.org)

referenciraju i kao „tier-1“ provajderi. Sa njima se povezuju ISP-ovi nižeg reda – pristupni i regionalni posrednici, koji dalje distribuiraju usluge krajnjim korisnicima. Ovi odnosi su prikazani na sl. 1.



Slika 1: Odnosi između posrednika za internet usluge

Iza svake od opisanih veza mora postojati i protokol, koji definiše pravila komunikacije. U računarskim mrežama postoji na hiljade protokola, pri čemu svaki od njih ima svoje mesto i svrhu u čitavom sistemu. U ovom radu bavimo se protokolom graničnog mrežnog prolaza (eng. *Border Gateway Protocol* – BGP), čiji je zadatak da logički poveže mreže različitih servis provajdera, kompanija, univerziteta i drugih entiteta. Svaka od tih mreža se može posmatrati kao nezavistan sistem, koji unutrašnju komunikaciju obavlja prema sopstvenim pravilima. Zapravo, termin koji se koristi u BGP-u je ‘autonomni sistem – AS’, i on opisuje skup rutera pod jedinstvenom administracijom, koji za međusobnu komunikaciju koriste neki od IGP (*Interior Gateway Protocol*) protokola i metrike pomoću kojih se određuje način rutiranja paketa unutar tog sistema. Dok je izbor IGP protokola u potpunosti slobodan, eksterni protokol je standardizovan – ukoliko jedan AS želi da se poveže sa drugima, mora koristiti protokol koji koriste svi ostali.

BGP je objavljen još 1989. godine, a danas je *de facto* standard koji svaka mreža koja želi da se poveže sa internetom mora da koristi. Kao protokol

rutiranja među autonomnim sistemima, BGP omogućava:

1. Pribavljanje informacija o dostupnosti podmreža od susednih autonomnih sistema,
2. Prenošenje tih informacija o dostupnosti do svih rutera unutar autonomnog sistema,
3. Određivanje 'dobrih' ruta do podmreža na osnovu informacija o dostupnosti i lokalnih pravila.

Što je najvažnije, BGP pruža svakoj podmreži mogućnost da objavi svoje postojanje drugima. U suprotnom, svaka mreža bi ostala izolovana – sama i nepoznata ostalima na internetu [1]. Iz svega navedenog, jasno je da BGP ima esencijalnu ulogu u postojanju i funkcionisanju Internet mreže a samim tim i za veliki broj komapnija koje svoje poslovanje sele u 'oblak', zbog miliona korisnika raznih digitalnih usluga, hiljada aplikacija, e-uprave i mnogih drugih. Gubitak konekcije bi mnogima napravio veliku finansijsku štetu pa danas inženjeri i administratori primenjuju različite tehnike kako bi osigurali neometano funkcionisanje BGP protokola. Postavljanje redudantnih uređaja, rezervnih linkova, redovno ažuriranje softvera i podešavanja mrežne opreme, samo su neke od tehnika i akcija koje se danas koriste. Međutim, uprkos svemu tome, opasnost od zlonamernih napada je konstantno prisutna, a BGP, iako je nastao kao odgovor na stariji protokol, sadrži različite nedostatke, koji, zloupotrebljeni, mogu dovesti do nestabilnosti globalne mreže. Ti nedostaci su u prethodnim godinama detaljno analizirani, i predložena su mnoga rešenja i objavljene razne studije. Nažalost, ni jedno od rešenja nije široko prihvaćeno, tj. nije standardizovano, već je odluka o načinima zaštite mreže i protokola ostavljena pojedinačnim sistemima. Drugim rečima, ne postoji zvanična definicija 'bezbednosnih uslova' pod kojima se jedan AS povezuje na Internet mrežu. Ovo je, naravno, mnogo puta iskorišćeno u hakerskim napadima, a neki od njih su dokumentovani u daljem tekstu.

Motivacija za ovaj rad leži u činjenici da BGP, iako predstavlja izuzetno važnu komponentu interneta, poseduje mane koje se relativno lako mogu zloupotrebiti, pri čemu naneta šteta može potencijalno biti ogromna, i to u više formi: finansijski, otkrivanjem poverljivih podataka, prekidom poslovanja (u slučaju prekida veze), pružanjem lažnih informacija (kroz lažno predstavljanje) i na mnoge druge načine. U ovom radu najpre su objašnjene osnove BGP protokola i osnovnih termina, zatim je data sumarizacija osnovnih problema – mana samog protokola i nekih poznatijih rešenja. Na samom kraju su opisani detalji simulacije u mrežnom simulatoru GNS3, parametri prema kojima su vršene analize, a zatim i rezultati tih analiza.

II. OSNOVE BGP PROTOKOLA

Primarna funkcija BGP sistema oglašavanja (eng. *speaking system*) je razmena informacija o dostupnosti drugih BGP mreža. Ruter koji izvršava BGP zove se BGP oglašivač (eng. *speaker*), a kada se dva ovakva rutera povežu, postaju susedi (eng. *peers*). Komunikacija između suseda se odvija preko sesije, i to koristeći TCP, koji je izabran zbog svoje usluge ispravljanja grešaka na transportnom sloju. Susedi unutar istog autonomnog sistema – interni susedi, komuniciraju preko internog BGP-a (iBGP), dok se eBGP (External Border Gateway Protocol) koristi samo između suseda iz različitih AS-ova. U daljem tekstu, kada god se referencira BGP, misli se na eksternu varijantu, tj. eBGP.

Što se tiče rutiranja, BGP ima vektorski pristup: oglašivač iz jednog AS-a oglašivaču iz susednog AS-a šalje sekvencu poruka, kojom oglašava niz destinacija. Svako oglašava one destinacije koje može da dosegne, a šalje se prefiks odredišta, zajedno sa putanjom do njega. Dodatno, ruteri mrežnog prolaza uz prefikse šalju i određene atribute. Dva najvažnija atributa su AS-PATH i NEXT-HOP, a u BGP žargonu, prefiks se zajedno sa svojim atributima naziva ‘ruta’.

- Atribut AS-PATH sadrži listu autonomnih sistema kroz koje je prošla objava za odgovarajući prefiks. Kada se prefiks prenese, tj. prođe kroz određeni AS, taj AS dodaje svoj broj (eng. AS *number* – ASN) u atribut AS-PATH. Na primer, recimo da su AS1, AS2 i AS3 redno povezani. Kada AS1 objavi mrežu 15.0.0.0 /24 koja pripada tom autonomnom sistemu, AS2 će primiti tu rutu i proslediti je dalje. Kada ona stigne do AS3, glasiće: “AS3 AS2 AS1”. Ruteri ovaj atribut koriste i za otkrivanje i sprečavanje višestrukih ponavljanja objava, a istovremeno i za sprečavanje petlji. Drugim rečima, ako neki ruter vidi da se njegov AS već nalazi u putanji, odbaciće tu objavu.
- Atribut NEXT-HOP ima malu, ali veoma važnu ulogu u ostvarivanju suštinski važne veze između protokola rutiranja unutar autonomnog sistema i protokola rutiranja među autonomnim sistemima. Konkretno, neophodan je u situacijama kada su dve mreže povezane ravnopravnim linkovima i gde postoje ruteri koji će saznati za dve različite putanje do druge mreže, sa istim AS-PATH atributima. U tom slučaju, atributi NEXT-HOP će se razlikovati, te će ruter na osnovu tih vrednosti odrediti troškove za obe putanje. Ona sa manjim troškom će biti izabrana za prosleđivanje saobraćaja.

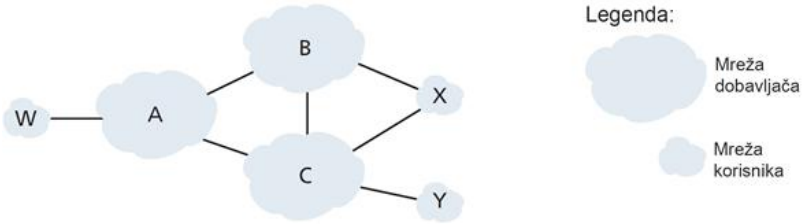
Kada ruter mrežnog prolaza primi objavu od nekog drugog rutera, on koristi svoja pravila uvoza za odlučivanje da li da odbaci ili prihvati odgovarajuću putanju i da li da postavi određene atribute kao što je prioritet metrike rutera. Ruta može biti odbačena zato što već postoji bolja, ali i zbog lokalno konfigurisane polise, koja, na primer, ne dozvoljava da saobraćaj iz lokalne mreže putuje preko nekog od autonomnih sistema iz atributa dotične putanje.

Kada ruter spozna više različitih putanja do iste destinacije, mora izabrati jednu. U tom postupku prolazi kroz sve objave koje je dobio i prihvatio, a BGP proces primenjuje svoja pravila eliminacije, koja su u potpunosti prikazana u [2], a ovde navedena u sažetom obliku:

1. Svakoj putanji je dodeljena vrednost lokalnog prioriteta, koji može da postavi odgovarajući ruter ili može da se sazna od drugog rutera u istom autonomnom sistemu. Ovo je strateška odluka i prepušta se administratoru. Algoritam bira onu putanju koja ima najveći lokalni prioritet.
2. Od preostalih ruta (sve sa jednakim vrednostima lokalnog prioriteta) bira se ruta sa najkraćim AS-PATH atributom, to jest sa najmanjim brojem skokova, gde je jedan skok razdaljina između dva različita autonomna sistema.
3. Od preostalih opcija (sve sa jednakim vrednostima lokalnog prioriteta i jednakim dužinama atributa AS-PATH) bira se putanja sa najbližim NEXT-HOP ruterom.

Na kraju, važni pojmovi vezani za politiku BGP rutiranja predstavljeni su kroz primer: na sl. 2 prikazano je šest međusobno povezanih autonomnih sistema: A, B, C, W, X i Y, pri čemu su A, B i C mreže posrednika, a W, X i Y završne, klijentske mreže. Takođe, A, B i C su međusobno ravnopravni pružaoci usluga, koji svojim korisnicima obezbeđuju sve potrebne BGP informacije. Sav saobraćaj koji ulazi u završnu mrežu mora da ima odredište u toj mreži, a sav saobraćaj koji napušta završnu mrežu mora da potiče iz nje. Jasno je da su W i Y takve mreže. X je tzv. 'višedomna' završna mreža, pošto je sa ostalima povezana preko dva različita posrednika. Međutim, kao i W i Y, X mora da bude odredište, odnosno izvor svog saobraćaja koji stiže prema mreži X ili izlazi iz nje. Takvo ponašanje se ostvaruje kontrolisanjem načina na koji se objavljuju BGP rute: u ovom slučaju, X će funkcionisati kao završna mreža, ako (svojim susedima B i C) objavi da nema putanje ni za jedno odredište osim sebe. To jest, iako X zna za putanju, na primer „XCY", kojom se stiže do mreže Y, on neće objaviti tu putanju mreži B. Pošto B ne zna da X ima putanju prema Y, B neće prosleđivati saobraćaj čije je odredište

Y (ili C) preko X. Ovaj jednostavan primer prikazuje kako se politika selektivnog objavljivanja ruta može iskoristiti za ostvarivanje odnosa korisnika i posrednika među BGP mrežama [1].



Slika 2: Jednostavan primer BGP rutiranja

Dodatno, mreže A, B i C sa sl. 2 se mogu opisati i kao 'tranzitni' autonomni sistemi. Tranzitni AS je uglavnom ISP koji se nalazi između dva druga autonomna sistema, i nije retkost da tranzitni ISP naplaćuje uslugu povezivanja dva AS-a između kojih se nalazi. Još jedan primer forsiranja oglašivača da preferira neke putanje u odnosu na druge je izmena ruta. To se postiže statičkom konfiguracijom, dodavanjem AS brojeva u putanju tako da deluje duža od alternativnih.

Još jedan pojam važan za BGP su *stub* mreže, odnosno *stub* autonomni sistemi. Oni su definisani kao mreže koje imaju samo jedan link prema spoljašnjosti, to jest, stub AS ima vezu samo sa jednim drugim autonomnim sistemom (stepen = 1), i on ne mora imati svoj, jedinstveni ASN. To su najčešće klijenti – manje i srednje mreže povezane sa svojim servis provajderom. Na sl. 2, autonomni sistemi W i Y su *stub* autonomni sistemi. Ono što izdvaja *stub* u odnosu na ostale AS-ove je nemogućnost prosleđivanja saobraćaja. Ova osobina je veoma važna za rutiranje zato što kroz takav AS ne mogu prolaziti nikakve putanje, osim one koja vodi do njega. To dalje znači da provajder ne bi trebalo da prihvata rute koje dolaze od takvih klijenata, pošto je sasvim sigurno da će one, u najmanju ruku, biti duže od pravih, a u gorem slučaju će omogućiti preusmeravanje saobraćaja zarad špijuniranja.

III. PREGLED NEDOSTATAKA BORDER GATEWAY PROTOKOLA

Kada su slabe tačke nekog protokola toliko poznate kao što je slučaj kod BGP-a, one predstavljaju otvorena vrata za napade na taj protokol, a u ovom slučaju, i na Internet. Najpre, BGP je ranjiv na 'standardne' napade na koje su osetljivi i drugi mrežni protokoli, kao što su prisluškivanje, ponovno slanje,

umetanje lažnih poruka, brisanje i modifikacija poruka u transportu, čovek u sredini (eng. *Man-in-the-middle*), prekid servisa (eng. *Denial of service*, DoS) itd. U zavisnosti od protokola, ovi napadi mogu imati različite posledice, ali se i usmeravaju na različite funkcionalnosti. Kod BGP-a, izdvajaju se tri načina komunikacije koja mogu biti zloupotrebljena:

1. Kontrolne poruke koje se razmenjuju pri uspostavljanju sesije,
2. Ažuriranja o dostupnosti, i
3. Poruke o greškama u okviru sesije [3].

Ovi, skoro generički napadi, ne predstavljaju pretnju samo BGP protokolu, već i mnogim drugim protokolima, pa se zato u ovom radu ne obrađuju detaljno. Ovde je izdvojen jedan napad specifičan za BGP, a to je krađa prefiksa.

Ispravno funkcionisanje BGP protokola se zasniva na uzajamnom poverenju između učesnika – u sam protokol nisu ugrađeni nikakvi mehanizmi za autentifikaciju ili validaciju putanja koje se propagiraju kroz sistem. Kao rezultat, bilo koji AS može oglasiti loše putanje, što dovodi do preusmeravanja saobraćaja.

Krađa, odnosno otimanje prefiksa (eng. *prefix hijacking*) je napad koji se sprovodi tako što neki AS prisvoji tuđi adresni opseg i počne da ga objavljuje. Neki ruteri će, u zavisnosti od topološke pozicije, preferirati putanju koju objavljuje zlonamerni AS, ukoliko je ta putanja kraća u odnosu na pravu, tačnu putanju. U osnovi, postoje dva načina za izvođenje ovog napada: (1) napadač objavljuje prefiks koji ne poseduje i (2) ISP se ilegalno ubacuje u putanju što dovodi do preusmerenja saobraćaja. Razlika između ova dva je u tome što se, kod prvog tipa, saobraćaj šalje napadaču umesto pravoj destinaciji, što znači da paketi namenjeni legitimnom vlasniku prefiksa nikada neće doći do njega. Sa druge strane, posledica drugog tipa napda može imati dva lica: napdač može odlučiti da obriše sve pakete koji dođu do njega, ali ih može i proslediti pravom odredištu, što se uklapa u definiciju ‘Man-in-the-middle’ napada [4], [5].

Postoje mnogobrojni, dobro dokumentovani primeri krađe prefiksa – bilo da su takve akcije bile slučajne, ili namerne. Primer nenamernog napada ‘otimanjem’ prefiksa dokumentovan je u [6]. Ovaj napad se dogodio 2012. godine, kada je Indonezijski provajder ‘Moratel’, po svemu sudeći, slučajno, objavio pogrešnu putanju. PCCW, Moratelov nad-provajder je, kao što je često slučaj, imao poverenja u rute koje je Moratel objavljivao, te se putanja proširila veoma brzo. Ovome je prethodio još jedan sličan događaj – kada je Ministarstvo telekomunikacija Pakistana naredilo državnoj kompaniji ‘Pakistan Telekom’ da cenzuriše sajt Youtube zbog spornog video snimka. Međutim, zaposleni su otišli još jedan korak dalje. Umesto da učine Youtube

nedostupnim za korisnike iz svoje zemlje, sajt je postao nevidljiv za ceo svet. Napad je sproveden upravo zloupotrebom osobina BGP protokola [7].

IV. PREGLED NAJPOZNATIJIH REŠENJA I NADOGRADNJI ZA BGP

U poslednjih desetak godina objavljen je veliki broj najrazličitijih rešenja za detekciju i sprečavanje napada na BGP protokol. Uprkos tome, veoma mali procenat autonomnih sistema, tj. 'BGP korisnika', primenjuje zaštitne mere koje predlaže stručna javnost. Delimičan razlog je optimistički stav servis provajdera koji smatraju da su ovi napadi retki, a zatim i da bi cena štete bila manja od cene implementacije bezbednosnih unapređenja.

A. Secure BGP (S-BGP)

Secure BGP je obimno rešenje za uklanjanje nedostataka vezanih za bezbednost, koje se bazira na nadogradnji samog protokola, kao i postojeće hijerarhije rutiranja na Internetu. Centralni element S-BGP-a je upotreba infrastrukture javnih ključeva (PKI – *Public Key Infrastructure*). PKI je, u suštini, kriptografska tehnologija u kojoj se koristi par ključeva, gde je jedan, javni ključ, dostupan svima, a drugi je tajni, privatni ključ. PKI predstavlja sistem kojim se obezbeđuje pravljenje ključeva, sertifikata i objavljivanja relevantnih javnih informacija. Korišćenjem ove infrastrukture obezbeđuju se poverljivost, integritet i dostupnost. Kod Secure BGP protokola je predviđeno korišćenje dva PKI sistema. Prvi je namenjen za delegaciju adresnog prostora i AS brojeva, to jest za autentikaciju entiteta koji koristi određeni prefiks. Drugi PKI upravlja dodelom AS brojeva i vezom između suseda koristeći tri sertifikata, gde svaki sertifikat potvrđuje neku povezanost:

- Jedan sertifikat potvrđuje vezu između ASN-a i javnog ključa organizacije;
- Drugi potvrđuje vezu između AS broja i javnog ključa sertifikata;
- Treći potvrđuje vezu između AS broja i ruting informacija: ime domena (DNS name), ID, javni kjuč.

Još jedan deo infrastrukture javnih ključeva su 'atestacije'. To su potpisane 'izjave' o dodeli prefiksa ili o identitetu. Potpisuje ih ili BGP oglašivač ili neko drugo autoritativno telo koristeći privatni ključ. Atestacija se zatim prenosi kao atribut u UPDATE poruci, koju primaoci validiraju koristeći PKI, čime se dokazuje autentičnost pristiglih informacija. S-BGP, kao i ostali mehanizmi zaštite, treba da obezbede:

- Autentifikaciju izvora
- Validaciju putanje, i

- Integritet skoka.

Autentifikacija izvora i validacija putanje se rešavaju uz pomoć atestacija. Identitet izvora potvrđuje atestacija koju je izvor i izdao, dok se za validaciju rute primalac oslanja na atestacije svakog AS-a iz putanje ponaosob. Dakle, prema S-BGP standardu, svaki AS koji doda sebe u putanju, takođe treba da se ubaci i u atestaciju, i da je potpiše. Na ovaj način, kad god BGP oglašavač primi putanju, može da validira svaki AS koji se nalazi u njoj. Na kraju, S-BGP problem integriteta skoka rešava korišćenjem IPsec protokola. Kada dva suseda komuniciraju preko IPsec-a, zagarantovani su im integritet, autentifikacija i šifrovanje na mrežnom sloju [3].

B. Servis za validaciju među-domenskih ruta (IRV Service)

Za razliku od S-BGP-a, rad IRV (*Interdomain Route Validation*) mehanizma ne zavisi od ruting protokola. IRV koristi eksternu, nezavisnu validaciju, što znači da jedan izolovan AS može slobodno koristiti IRV, čak i bez znanja drugih. Svaki AS koji je implementirao IRV ima svoj IRV server čiji je zadatak da proveri korektnost informacija pristiglih iz drugog autonomnog sistema. Na primer, pretpostavimo da AS X primi UPDATE poruku od AS Y. Oglašivač iz X će proslediti pristiglu poruku svom lokalnom IRV serveru, koji zatim kontaktira IRV server iz AS Y radi provere.

Transakcija upita (eng. *query*) vrši se, kad god je to moguće, koristeći siguran transportni standard, kao na primer IPsec, TLS ili SSL. Ovim se obezbeđuju integritet skoka i autentičnost, pošto dva suseda proveravaju jedan drugog. Međutim, iako je validacija bitna, jasno je da ne mora baš svaka UPDATE poruka da se proverava. Zato IRV ne propisuje specifičan algoritam koji će izdvajati sumnjive poruke, već svaka mreža može da koristi drugačiji. Što se tiče autentifikacije porekla objava, IRV server može proveriti izvorni AS tako što će poslati upit organizacijama koje delegiraju ASN-ove i adresne opsege. Potvrde susednih IRV servera takođe mogu da potkrepe tvrdnju da je određeni AS validan.

Na kraju, pomoću IRV-a je moguće validirati i čitavu putanju, jednostavno, iterativnom validacijom svakog AS-a u putanji. Smatra se da je ruta prošla test ako svaki AS vrati potvrdu. Sa druge strane, treba imati na umu optrećenje koje će ovakva operacija dodati mrežnim resursima, zbog čega se predlaže da se slanje i analiza upita realizuje uz pomoć eksternog resursa.

C. SoBGP (Secure Origin BGP)

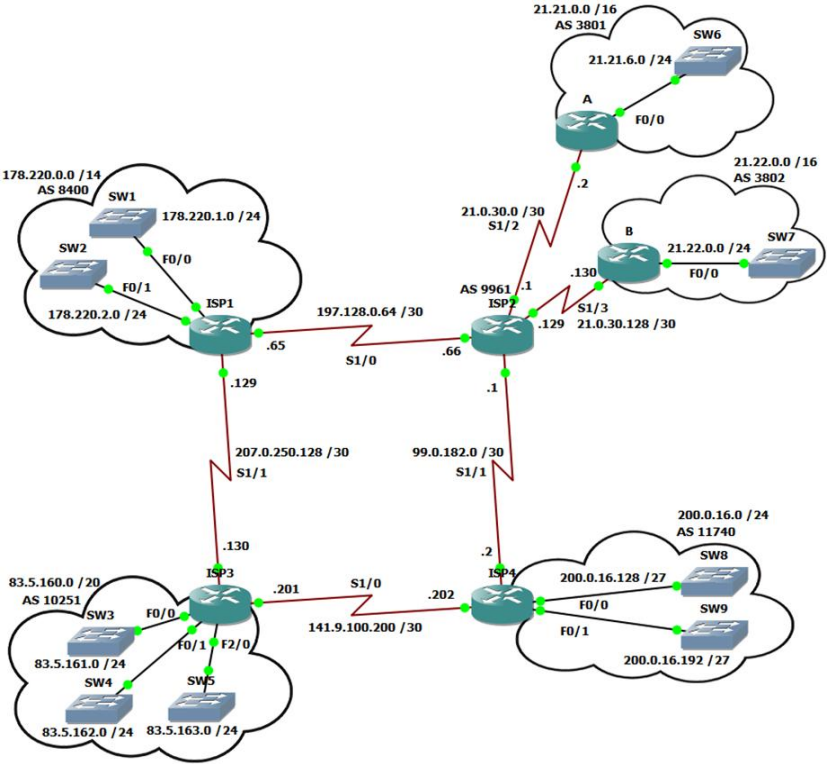
SoBGP je, u suštini, predlog ekstenzije za originalni protokol. Promene su uglavnom manja bezbednosna poboljšanja, od kojih je primarni mehanizam

zaštite implementacija novog tipa SECURITY poruke. Naime, BGP oglašivači koriste ovu poruku za razmenu sertifikata i atestacija, a sadržaj potpisuje pošiljalac, što omogućava primaocu da validira javni ključ, polise, podatke o rutiranju. U suštini, svi bezbednosni podaci vezani za soBGP prenose se unutar SECURITY poruke, među kojima su u protokolu definisana tri tipa sertifikata i atestacija: (1) entitet, (2) polise i (3) autorizacija. Uloga sertifikata entiteta je verifikacija postojanja specifičnog 'objekta' unutar ruting sistema. To, na primer, može biti izvor određene poruke ili ruter naveden u putanji. Drugi po redu, sertifikat polise, čuva podatke o nekom autonomnom sistemu i služi da dokaže njegovu autentičnost. Poslednji, sertifikat autorizacije, predstavlja dozvolu jednog AS-a da oglašava određenu adresu, ili adresni opseg. Sertifikat autorizacije takođe služi i kao alat za autentifikaciju izvora.

Što se tiče validacije putanje, ona je omogućena verifikacijom AS-ova i pravljenjem baze ruta, koja se popunjava tako što svaki oglašivač objavi AS sa kojim je povezan, i to preko „Attached AS" polja u sertifikatu polise. Ovo polje služi za identifikaciju tranzitnih i drugih mreža. Na osnovu tih informacija, oglašivači mogu da popune bazu svih mogućih putanja do određenog prefiksa. Takođe, u toku popunjavanja baze, mogu se slati upiti kako bi se saznalo da li je dotična putanja legalna. Osim toga, informacije o poreklu, kao i o sledećem, drugom skoku, takođe mogu biti verifikovane, pošto se validacija putanje vrši rekurzivno, proveravajući redom da li je svaki oglašivač na putanji zapravo povezan sa izvornim AS-om. Međutim, ovom proverom se potvrđuje legitimitet putanje, ali ne i da je paket zaista tim putem stigao do odredišta. Ono što nedostaje unutar soBGP standarda je provera integriteta skoka, ali i autori priznaju da je implementacija sigurnijeg protokola za komunikaciju, kao što je na primer IPsec, preko potrebna u BGP sesijama.

V. SIMULACIJA

U ovom poglavlju nalaze se detalji o simulaciji i eksperimentima izvedenim u mrežnom simulatoru GNS3. Na sl. 3 je prikazana šema, na kojoj su date IP adrese i brojevi autonomnih sistema. Na početku simulacije, svi ruteri su standardno konfigurisani – interfejsima su dodeljene IP adrese iz adresnih opsega naznačenim na slici, na svakom ruteru je pokrenut BGP i objavljene su odgovarajuće mreže. Na ruterima ISP1, ISP3, ISP4, A i B su objavljene agregatne adrese, takođe označene na šemi. Svičevi nisu konfigurisani – oni predstavljaju krajnje mreže.



Slika 3: Šema mreže u GNS3

Pretpostavka je da su svi ISP ruteri međusobno ravnopravni, a da su A i B klijenti od ISP2. Svaki sledeći segment u daljem tekstu opisuje po jedan eksperiment, a cilj je da se pokaže kako različita podešavanja BGP procesa utiču na sposobnost rutera da se odbrane od napada na ovaj protokol. Konkretno, simuliran je napad otimanjem prefiksa, najpre na mreži u kojoj spikeri imaju samo osnovnu konfiguraciju – dovoljnu za redovan rad BGP-a, ali kao što se pokazalo, nedovoljnu za odbranu od ilegalnog oglašavanja tuđih podmreža. Zatim je isti napad simuliran u mrežama u kojima su pokrenuti mehanizmi za odbranu, gde su ti mehanizmi već ugrađeni u Cisco IOS, i predstavljaju osnovni vid zaštite, preporučen od strane raznih internet udruženja. U svakom eksperimentu odgovoreno je na tri pitanja:

a) Od ukupno 6 autonomnih sistema u šemi, koliko je zaraženo, to jest, koliko autonomnih sistema je prihvatilo pogrešnu informaciju?

b) Koliko autonomnih sistema je lažnu informaciju prosledilo dalje, od ukupno 4 koji nisu *stub*?
c) Na koliko oglašivača (BGP rutera) je konfigurisana data metoda zaštite?

Napomena: ruter sa koga je izvršen napad se takođe računa kao zaraženi ruter. *Stub* mreže (A i B) nemaju kome da proslede lažnu informaciju, pa se stoga drugo (b) pitanje ne odnosi na njih.

Cilj je analizirati odgovore na ova pitanja, međusobno ih uporediti, i na kraju, odrediti efikasnost primenjenog rešenja za svaki pojedinačni eksperiment. Mnoge nadogradnje BGP-a se oslanjaju na masovnu primenu – da bi postigle željen rezultat, neophodno je da veliki broj autonomnih sistema prihvati i implementira predložene promene. Pošto izmene nisu uvek jednostavne, a često nose i dodatne troškove, ni jedno od postojećih rešenja trenutno nije globalno pristuno, a nije realno očekivati da će se to dogoditi u skorijoj budućnosti. Zato je važno proceniti uspešnost pojedinačnih mehanizama u situaciji koja nije idealizovana, već bliža stvarnosti. Što se tiče veličine simulirane okosnice, ona se nikako ne može porediti sa veličinom interneta, ali takve strukture svakako postoje, i one su, kao i drugi autonomni sistemi, takođe podložne napadima spomenutim u ovom radu.

A. *Prvi scenario: napad otimanjem prefiksa na nezaštićenu mrežu*

U ovom, prvom eksperimentu, ukazuje se na posledice napada otimanjem prefiksa na mrežu u kojoj nije implementiran nikakav mehanizam zaštite. Najpre je, na ruteru ISP4, objavljena, ili, po BGP žargonu, 'oteta' mreža povezana na ruter A, ali sa smanjenom maskom: 21.21.0.0 /16. Neposredno nakon ove izmene, izlaz komande `show ip bgp` je na ruteru ISP4 promenjen. Ispod je istaknuta linija koja nas interesuje, pre izdavanja komande u prvom koraku, i posle.

Pre:

```
   Network       Next Hop      Metric LocPrf Weight Path
*> 21.21.0.0/16  141.9.100.201                   0 10251 8400 9961 3801 i
```

Posle:

```
   Network       Next Hop      Metric LocPrf Weight Path
*> 21.21.0.0/16  0.0.0.0            0         32768  i
```

Rezultat je isti i na ISP3, koji u BGP tabeli čuva obe putanje, ali je ruta preko ISP4 označena ne samo kao validna, već i kao najbolja (*>), pa je stoga urpavo ona smeštena u ruting tabelu.

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 21.21.0.0/16     141.9.100.202            0             0 11740 i
*                   207.0.250.129                          0 8400 9961 3801 i
```

Na ruteru ISP2, koji je najbliži ugroženoj mreži, stanje ostaje isto. U sledećem koraku, na ruteru ISP4 objavljen je specifičniji prefiks. To jest, umesto 21.21.0.0/16, u BGP je oglašena mreža 21.21.6.0/24. Sada je dovoljno posmatrati samo ruter ISP2. Pošto se pojavila putanja do manje podmreže unutar opsega 21.21.0.0/16, svi ruteri će je prihvatiti. Izlaz komande `show ip bgp` na ruteru ISP2 je sada:

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 21.21.0.0/16     21.0.30.2                0             0 3801 i
*  21.21.6.0/24     197.128.0.65                           0 8400 10251 11740 i
*>                  99.0.182.2               0             0 11740 i
```

Zaključak za prvi deo eksperimenta (21.21.0.0 /16)

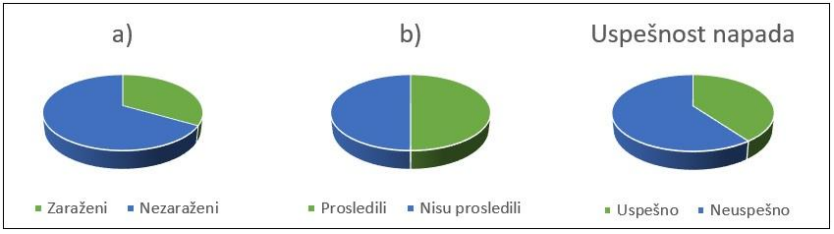
a) Od ukupno 6 autonomnih sistema u šemi, kod 4 BGP rutera je pogrešna informacija smeštena u BGP tabelu, ali je lažna putanja izabrana kao bolja samo 2 puta. Dakle, **2/6**.

b) Od ukupno 4 autonomna sistema koji su lažnu rutu mogli da proslede drugim mrežama (pošto su A i B *stub*), 2 AS-a su to i učinila. To su ISP3 i ISP4, koji su pogrešnu rutu i prihvatili. ISP3 ju je poslao prema ISP1, a ISP4 prema ISP3 i ISP2. Dakle, **2/4**.

c) Ni na jednom od ukupno 6 rutera nije pokrenut nikakav mehanizam zaštite. Dakle, **0/6**.

Napomena: Od dve stub mreže, ni jedna nije zaražena, pošto ISP2, na koji su povezane, takođe nije prihvatio pogrešnu informaciju.

Uspešnost napada merimo tako što sabiramo rezultate pod a) i b). U ovom eksperimentu, napad je bio delimično uspešan, a konačan rezultat je 4/10, to jest, 40%. Ovo je za svaki eksperiment prikazano grafički.



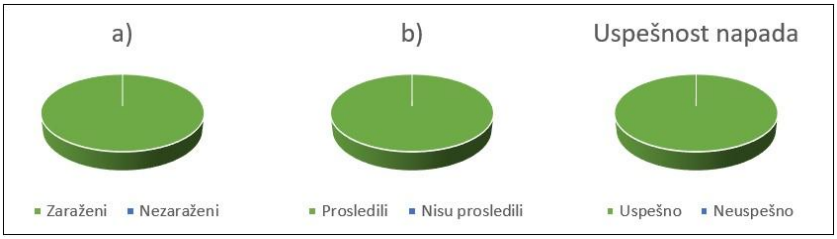
Zaključak za drugi deo eksperimenta (21.21.6.0 /24)

a) Od ukupno 6 BGP rutera u šemi, svi su prihvatili pogrešnu putanju, pa čak i A, na koji je napadnuta mreža direktno povezana. Međutim,

ona je označena kao ‘potisnuta’ (eng. *suppressed*), i jedino ruter A može da pinguje pravu adresu 21.21.6.1. Ipak, pošto je BGP proces na A prihvatio lažnu putanju, smatra se da je i on zaražen, te je rezultat **6/6**.

b) Od 4 posmatrana rutera, svi su lažnu putanju prosledili susedima. Dakle, **4/4**.

c) Ni na jednom od ukupno 6 rutera nije pokrenut nikakav mehanizam zaštite. Dakle, **0/6**.



B. Drugi scenario: Prefix-List filter

Najosnovnija moguća zaštita BGP-a je filtriranje. U ovom scenariju, primenjen je takozvani Prefix-List filter. Njime je moguće zabraniti prihvatanje objava od specificiranih suseda, ukoliko te objave nose sumnjive podatke. Na primer, pošto su mreže A i B klijenti provajdera ISP2, bilo bi čudno da neki drugi provajder objavi putanju do A ili B. Upravo to je učinjeno u prethodnom scenariju, ali je ISP2 prihvatio nove rute, zato što nije bila podešena nikakva zaštita. Ovde se, prema standardima „najboljih praksi“ (eng. *best practices*), uvodi lista „Klijenti“ koja će sprečiti problem iz prethodnog scenarija.

U prvom koraku je kreirana, i primenjena prefix lista. Napomena: „`permit 0.0.0.0/0 le 32`“ je ekvivalentno „`permit any`“ u standardnim Access listama.

```
ISP2(config)#ip prefix-list Klijenti deny 21.0.0.0/8 ge 16 le 32
ISP2(config)#ip prefix-list Klijenti permit 0.0.0.0/0 le 32

ISP2(config)#router bgp 9961
ISP2(router-config)#neighbor 197.128.0.65 prefix-list Klijenti in
ISP2(router-config)#neighbor 99.0.182.2 prefix-list Klijenti in
```

Nakon uvođenja liste, na ruteru ISP4 je, kao u prethodnom eksperimentu, objavljena mreža 21.21.0.0/16 i on ju je odmah prihvatio. Što se tiče rutera ISP2 i ISP3, situacija je identična kao u prethodnom eksperimentu – ISP3 je

prihvatio novu rutu do 21.21.0.0/16, dok ISP2 nije. U sledećem koraku je na ISP4 objavljena specifičnija podmreža, isto kao u prethodnom eksperimentu.

Slušajući na serijskom interfejsu 1/1 rutera ISP2, interfejsu serial 1/0 na ruteru ISP3, i na serial 1/1 rutera ISP1, pomoću Wireshark-a uhvaćena je UPDATE poruka koja je nosila upravo objavljenu mrežu na ISP4. Iz sadržaja tih paketa može se zaključiti da je ISP3 prihvatio putanju preko AS 11740 (što se vidi u Path Attributes, AS_PATH).

Na ISP3, mreža sa manjim prefiksom (podmreža 21.22.0.0/24) se, prema BGP tabeli, nalazi u AS 11740, dok za podmrežu 21.22.0.0/16 postoji putanja sve do AS 3801:

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 21.22.0.0/24     141.9.100.202            0             0 11740 i
*  21.22.0.0/16     141.9.100.202                          0 11740 9961 3802 i
```

Stavke u tabeli rutiranja su takođe kontradiktorne:

```
B       21.22.0.0/24 [20/0] via 141.9.100.202, 00:20:53
B       21.22.0.0/16 [20/0] via 207.0.250.129, 01:15:42
```

Pravo stanje pokazuje izlaz traceroute-a, pošto paket namenjen adresi 21.22.0.1 stiže samo do Loopback interfejsa na ruteru ISP4:

```
ISP3#traceroute 21.22.0.1

Type escape sequence to abort.
Tracing the route to 21.22.0.1

  1 141.9.100.202 60 msec 52 msec 56 msec
```

BGP i ruting tabela su slične i na ISP1, to jest, za prefiks 21.22.0.0/24 je prihvaćena loša putanja. Preostaje još da se vidi da li je prefix lista konfigurisana na ISP2 urodila plodom, bar na ISP2. Pre ilegalne objave mreže na ISP4, na ruteru ISP2 je pokrenut *debugging* za UPDATE poruke BGP-a. Izlaz je dat ispod.

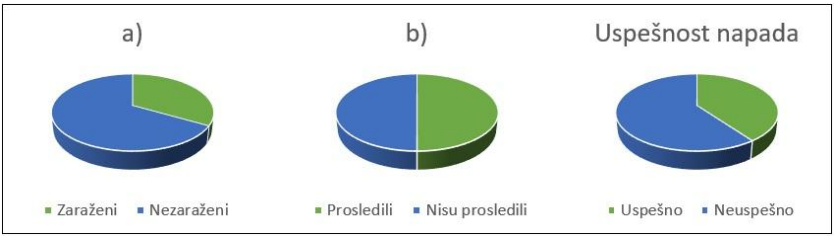
```
ISP2#debug ip bgp updates
BGP updates debugging is on for address family: IPv4 Unicast
ISP2#
*Aug 22 17:56:40.315: BGP(0): 99.0.182.2 rcvd UPDATE w/ attr: nexthop
99.0.182.2, origin i, metric 0, path 11740
*Aug 22 17:56:40.319: BGP(0): 99.0.182.2 rcvd 21.22.0.0/24 -- DENIED due
to: distribute/prefix-list;
*Aug 22 17:56:40.343: BGP(0): 197.128.0.65 rcvd UPDATE w/ attr: nexthop
197.128.0.65, origin i, path 8400 10251 11740
*Aug 22 17:56:40.347: BGP(0): 197.128.0.65 rcvd 21.22.0.0/24 -- DENIED due
to: distribute/prefix-list;
```

Iz prethodnih redova može se zaključiti sledeće: i ISP1 i ISP4 su poslali UPDATE poruku sa putanjom do mreže 21.22.0.0/24 preko AS 11740

(ISP4). Oba puta, objava je odbijena zbog prefix liste „Klijenti“. Ovaj put je zato, za razliku od prethodnog scenarija, tabela na ruteru ISP2 ostala nepromenjena, i sada jedino ruteri ISP2 i B mogu uspešno da komuniciraju sa ruterom A.

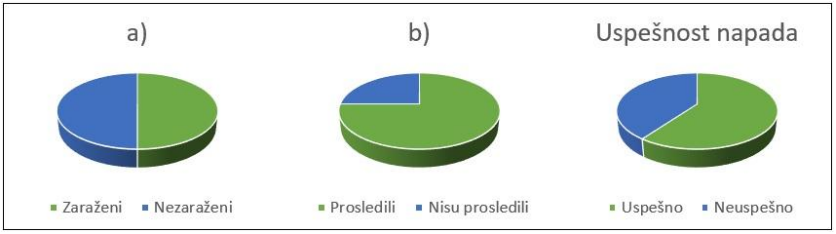
Zaključak za prvi deo eksperimenta (21.21.0.0 /16)

a) Od ukupno 6 autonomnih sistema u šemi, zaraženi su samo ISP3 i ISP4, dakle, **2/6**.
b) Od ukupno 4 rutera koja posmatramo, oba zaražena rutera su lažnu putanju prosledila dalje. Dakle, **2/4**.
c) Od ukupno 6 rutera, samo na jednom je kreirana lista, dakle, **1/6**.



Zaključak za drugi deo eksperimenta (21.21.6.0 /24)

a) Od ukupno 6 autonomnih sistema u šemi, zaraženi su ISP1, ISP3 i ISP4, dakle, **3/6**.
b) Od tri zaražena rutera, svaki je lažnu putanju prosledio dalje. Dakle, **3/4**.
c) Od ukupno 6 rutera, samo na jednom je kreirana lista, dakle, **1/6**.



C. Treći scenario: Weight atribut

Atribut ‘težina’ (eng. *weight*) u putanji se može konfigurisati tako da spiker favorizuje jednu rutu u odnosu na druge, to jest, da daje prednost putanjama koje dobije od specifičnog suseda. U [2] je dat algoritam prema kome BGP

donosi odluku o izboru najbolje rute, a prvi parametar je upravo težina. Što je vrednost ovog atributa veća, to će putanja biti povoljnija – rute za koje se saznalo od nekog suseda (preko eBGP-a) će imati težinu 0, dok će rute koje su unete statički ili redistribuirane iz nekog IGP-a, po standardnom podešavanju, imati težinu 32768. Specifična težina se može podesiti ili direktno u BGP konfiguracionom režimu i vezati za određenog suseda, ili se sa tim susedom može povezati preko *route* mape, uz pomoć pristupne liste. U ovom scenariju, pretpostavićemo da je ISP2 manji provajder koji je direktno povezan sa ISP1 i ISP4, gde je prvi pouzdaniji. Ovakva konfiguracija se može primeniti i u slučaju da je poznata pretnja povezana sa ISP4, to jest, ukoliko je primećeno da su raniji napadi dolazili iz tog pravca. Za putanje koje oglasi ISP1 vezivaće se težina 500, a za putanje koje oglasi ISP4 vezivaće se težina 300:

```
ISP2(config)#router bgp 9961
ISP2(config-router)#neighbor 99.0.182.2 weight 300
ISP2(config-router)#neighbor 197.128.0.65 weight 500
```

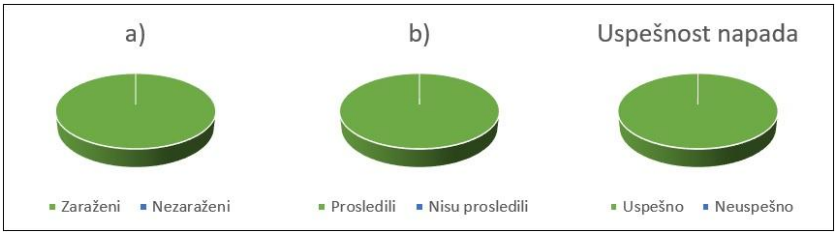
U sledećem koraku, na ISP4 objavljujemo mrežu 21.21.0.0 /16 i posmatramo posledice. Prema izlazu komande `show ip bgp`, pogrešnu putanju su prihvatili ISP1, ISP2, ISP3, kao i ruteri A i B. Interesantno je primetiti da je dodavanje weight atributa ovde imalo kontra efekat, zato što ostale putanje po standardnom podešavanju imaju težinu 0, pa je težina ruta iz ISP4 opet bila veća od onih dobijenih od klijenata A i B. ISP2 je zatim prosledio pogrešnu informaciju svojim klijentima, i A je, kao i u prvom scenariju, ponovo prihvatio spoljnu putanju do mreže koja je direktno povezana na njega. Napad je već u prvom delu eksperimenta potpuno uspešan, ali je, kao i u prethodnim eksperimentima, objavljena manja podmreža 21.21.6.0 /24, radi poređenja na kraju. Kao što je i očekivano, ponovo su svi ruteri zaraženi.

Pošto su rezultati ovog eksperimenta izuzetno loši, razmotrimo šta bi se moglo izmeniti zarad poboljšanja. Najpre treba definisati problem, koji je očigledan: putanje koje objavljuju ruteri ISP1 i ISP4 imaju težine 500 i 300, a putanje koje objavljuju klijenti A i B imaju težinu 0. Međutim, rešenje nije trivijalno – kada bi se objavama od A i B jednostavno dodale veće težine, izbegle bi se posledice dobijene simuliranim napadom, ali se ne bi sprečio bilo koji drugi napad. Na primer, ukoliko A objavi mrežu 200.0.16.128 /27, ISP2 će prihvatiti tu rutu umesto one preko ISP4. Naravno, ovo bi se moglo izbeći upotrebom dodatne mere zaštite. Jedna mera, poznata pod nazivom „BCP38“ [8] bi u simuliranoj mreži mogla biti primenjena uz pomoć Prefiks liste ili AS-Path liste, a ukratko, njen cilj je kontrola sadržaja koji ISP klijenti šalju prema internetu. Ideja je jednostavna: ISP treba da filtrira saobraćaj tako

da zaustavi sve pakete čija se izvorna IP adresa ne nalazi u opsegu adresa koje je dotični ISP dodelio svojim klijentima.

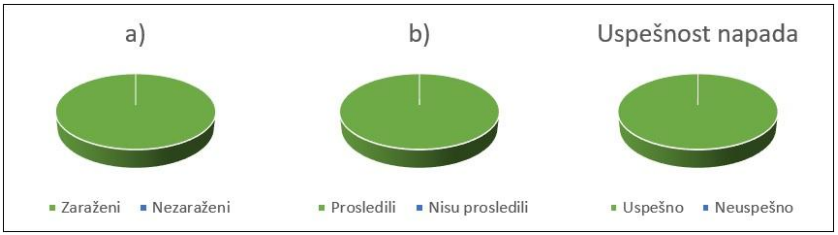
Zaključak za prvi deo eksperimenta (21.21.0.0 /16)

a) Od ukupno 6 autonomnih sistema u šemi, zaraženi su svi, dakle, **6/6**.
b) Od ukupno 4 rutera koja posmatramo, svi su lažnu putanju prosledili dalje. Dakle, **4/4**.
c) Od ukupno 6 rutera, samo na jednom smo veštački uticali na weight parametar, dakle, **1/6**.



Zaključak za drugi deo eksperimenta (21.21.6.0 /24)

a) **6/6**.
b) **4/4**.
c) **1/6**.



D. Četvrti scenario: LOCAL_PREF atribut (Local Preference)

'Local preference' je metrika koja ukazuje na prioritet rute, gde veća vrednost znači veći prioritet. Po standardnom podešavanju, svaka putanja u početku ima prioritet 100. U prvom koraku, kreirana je po jedna mapa za ISP1 i ISP4, a dodeljene vrednosti bi trebalo da repliciraju prethodni scenario, gde se preferiraju informacije koje pošalje ISP1, u odnosu na ISP4. Mape su povezane sa odgovarajućim susedima, a standardna vrednost za

LOCAL_PREF atribut će, bez ikakvog podešavanja, biti 100. To znači da će susedi A i B imati prioritet nad ISP1 i ISP4.

```
ISP2(config)#route-map LocalPref-ISP1 permit 10
ISP2(config-route-map)#set local-preference 90

ISP2(config)#route-map LocalPref-ISP4 permit 10
ISP2(config-route-map)#set local-preference 80

ISP2(config)#router bgp 9961
ISP2(config-router)#neighbor 197.128.0.65 route-map LocalPref-ISP1 in
ISP2(config-router)#neighbor 99.0.182.2 route-map LocalPref-ISP4 in
```

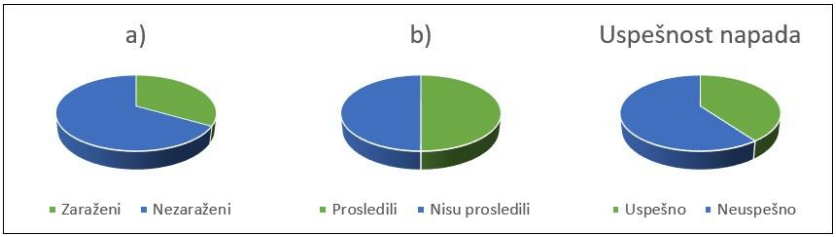
Ruter ISP4 zatim objavljuje mrežu 21.21.0.0 /16, nakon čega se u izlazu komande `show ip bgp 21.21.0.0`, vidi se da je izabrana putanja preko rutera A, zbog veće `localpref` vrednosti:

```
ISP2#show ip bgp 21.21.0.0
BGP routing table entry for 21.21.0.0/16, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to update-groups:
     1
  11740
    99.0.182.2 from 99.0.182.2 (21.21.0.1)
      Origin IGP, metric 0, localpref 80, valid, external
  3801, (aggregated by 3801 21.21.6.1)
    21.0.30.2 from 21.0.30.2 (21.21.6.1)
      Origin IGP, metric 0, localpref 100, valid, external, atomic-
      aggregate, best
```

Međutim, kada je na ruteru ISP4 objavljena mreža 21.21.6.0 /24, ISP2 je prihvatio i prosledio putanju gde se do te mreže dolazi preko AS 11740. A i B su tu informaciju takođe prihvatili kao validnu.

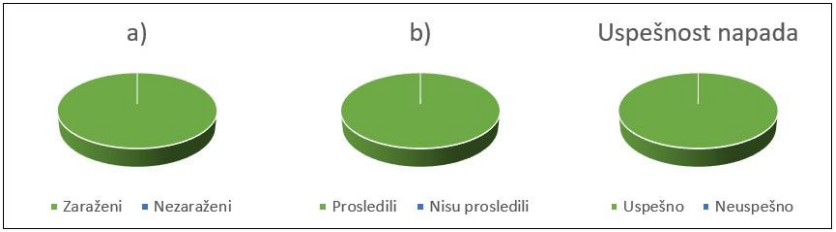
Zaključak za prvi deo eksperimenta (21.21.0.0 /16)

a) Od ukupno 6 autonomnih sistema u šemi, zaraženi su samo ISP3 i ISP4, dakle, **2/6**.
b) Od ukupno 4 rutera koja posmatramo, oba zaražena rutera su lažnu putanju prosledila dalje. Dakle, **2/4**.
c) Od ukupno 6 rutera, samo na jednom su preduzete mere, dakle, **1/6**.



Zaključak za drugi deo eksperimenta (21.21.6.0 /24)

a) Od ukupno 6 autonomnih sistema u šemi, svi su zaraženi, dakle, **6/6**.
b) Od ukupno 4 rutera koja posmatramo, svi su lažnu putanju prosledili dalje. Dakle, **4/4**.
c) Od ukupno 6 rutera, samo na jednom su preduzete mere, dakle, **1/6**.



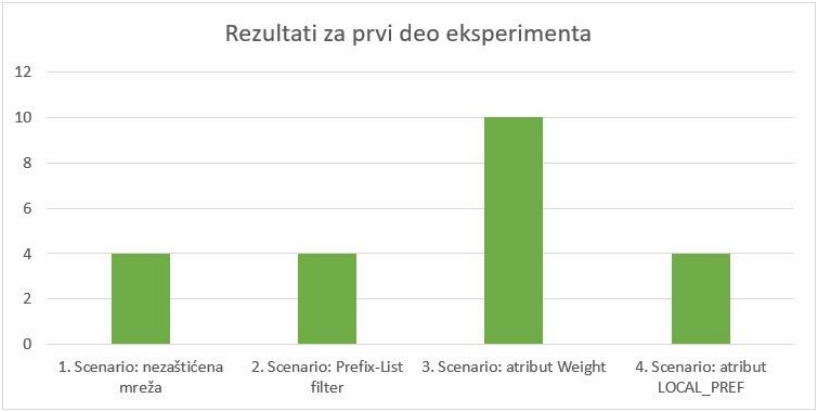
E. Ostali mehanizmi

Na kraju treba spomenuti i druge mehanizme koji bi mogli sprečiti testirani napad, a koji nisu upotrebljeni u ovoj simulaciji. Radi se o tehnikama čija je konfiguracija kompleksnija od gore prikazanih, a to su BGP 'zajednice' (eng. *communities*) i MED (*Multi Exit Discriminator*) atribut. U prethodnim poglavljima objašnjeni su poslovni odnosi i fizičke veze između različitih autonomnih sistema, kao i različita pravila kojih se ponuđači internet usluga pridržavaju. Kod BGP-a, ta pravila se uglavnom nameću filtriranjem: koriste se AS-Path, Prefix-List filtri i BGP 'zajednica' (eng. *community*). U simulaciji su napravljeni eksperimenti sa *Prefix-list* filterom, *weight* i *local preference* atributima, koji su svakako korisni, ali nisu dovoljno automatizovani, to jest, kada god se pojavi nova mreža, ona se mora ručno obraditi – uneti u listu ili označiti posebnim atributom. Ovaj proces se može ubrzati raznim skriptama i bazama za registraciju putanja, ali takve implementacije gube na efikasnosti pri povećanju mreže. BGP zajednice i manipulisanje MED atributom predstavljaju elegantnije rešenje, ali su prilagođeni većim autonomnim sistemima čiji ruteri komuniciraju uz pomoć iBGP-a, i zato nisu korišćeni u ovom radu.

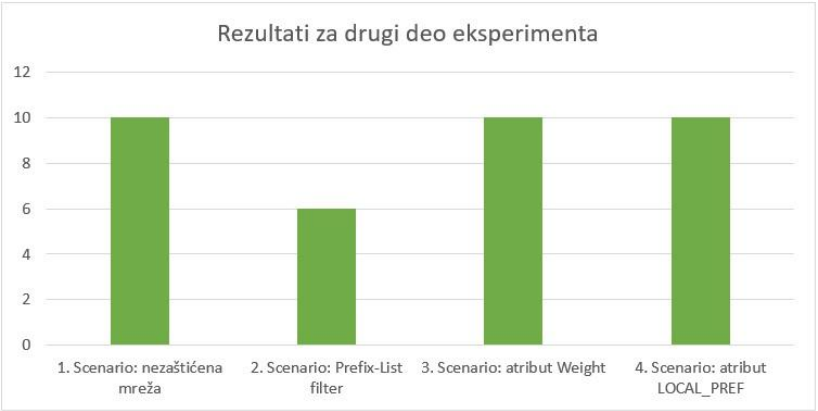
Takođe, izostavljen je još jedan tip filtera, a to je 'AS-Path Filter List', koji bi u ovoj simulaciji bio uspešan samo ukoliko su pretnje unapred poznate, što je u realnosti retko slučaj. U stvarnosti, administrator ne može da predvidi odakle će doći pretnja, a s obzirom na to da mi ovde sami simuliramo napad, takav eksperiment ne bi bio od velike koristi.

VI. ZAKLJUČAK

Na osnovu prikazanih rezultata, jasno je da ni jedna od osnovnih metoda zaštite ne može samostalno odbraniti čak ni simuliranu mrežu, koja je relativno mala. Ipak, dobijen je osnovni uvid u efikasnost primenjenih mehanizama. Slike 3 i 4 prikazuju rezultate eksperimenata. Na prvoj slici se vidi uspešnost napada objavljivanjem prefiksa sa manjom maskom (21.21.0.0 /16), a na drugoj objavljivanjem specifičnije podmreže (21.21.6.0 /24).



Slika 4: Napad objavljivanjem većeg opsega



Slika 5: Napad objavljivanjem specifičnijeg opsega

Očigledno je da je drugi deo eksperimenta u svakom scenariju imao veće posledice, kada je, pri istoj konfiguraciji i na istom uređaju, objavljen prefiks sa većom mrežnom maskom. Kao najuspešniji mehanizam pokazao se *Prefix-List* filter, koji je implementiran samo na jednom uređaju, i to po standardnim preporukama iz prakse. U tom scenariju, čak i da je napad pokušan iz drugog autonomnog sistema, rezultat bi ponovo bio bolji nego da je mreža ostala bez ikakve zaštite. Sa druge strane, pokazano je da je pri upotrebi *Weight* atributa neophodna dodatna opreznost, pošto su rezultati eksperimenta u trećem scenariju bili gori nego u prvom, gde je mreža ostavljena potpuno nezaštićena. U istom eksperimentu je spomenuta dodatna mera, poznata kao BCP38, koja bi, primenjena kao dodatak, sigurno poboljšala rezultat, ali je cilj simulacije bio pokazati uspešnost pojedinačnih osnovnih mehanizama, te se dodatna ispitivanja ostavljaju za buduće radove.

ZAHVALNICA

Zahvaljujem se profesorki Mirjani Radivojević na korisnim savetima, sugestijama i smernicama u toku izrade ovog i prethodnih radova u toku osnovnih i master studija.

LITERATURA

[1] Kurose, J., Ross, K., „Umrežavanje računara, Od vrha ka dnu“, prevod šestog izdanja, 2013
[2] Cisco, „BGP Best Path Selection Algorithm“, 2016, dostupno na http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
[3] Butler, K., Farley T., McDaniel P., „A Survey of BGP Security Issues and Solutions“, AT&T Labs Research, Proceedings of the IEEE (Volume 98, Issue 1), 2010
[4] Bono, V., „Explanation and apology”, NANOG Email, 26 April 1997
[5] Lad, M., Oliveira, R., Zhang, B., Zhang, L.: „Understanding resiliency of Internet topology against prefix hijack attacks”, IEEE/IFIP DSN Proceedings, 2007
[6] Paseka, T., „Why Google Went Offline Today and a Bit about How the Internet Works”, Cloud Flare, 2012, dostupno na https://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about/
[7] McCullagh, D., „How Pakistan knocked YouTube offline (and how to make sure it never happens again)”, CNET, 2008, dostupno na http://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/
[8] BCP38, dostupno na http://www.bcp38.info/index.php/Main_Page

ABSTRACT

Border Gateway Protocol (BGP), is the most important internet protocol. It defines the rules of communication and enables independent computer networks to connect with others and join the global network. In this paper, we

introduce some of the basic BGP concepts, as well as some of the well-known flaws. Then we discuss the three most widespread solutions, developed to fix certain secutiry challenges: S-BGP, IVR and SoBGP. In the end, we simulate prefix hijacking attack using GNS3, aimed at a backbone network. Several scenario are demonstrated: an unprotected network is first attacked, then we repeat the attack after applying a filter, and in the end, after manipulating several BGP attributes.

BGP: Prefix hijacking simulation and analysis

Dunja Majstorović