*XXIV Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2006**, Beograd, 12. i 13. decembar 2006.*

ZAŠTITA PROTOKOLA RUTIRANJA U INTERNETU

Mirjana Stojanović, Slavica Boštjančič
Institut Mihajlo Pupin, Beograd

Sadržaj: *U ovom radu je prikazan pregled mogućih napada na infrastrukturu rutiranja u Internetu i mehanizama zaštite unicast protokola rutiranja. Preventivni mehanizmi zaštite obuhvataju različite tehnike digitalnog potpisa za zaštitu integriteta i utvrđivanje autentičnosti kontrolnih poruka, kao i obeležavanje kontrolnih poruka rednim brojevima ili vremenskim pečatima, radi zaštite od promene redosleda ili replikacije. Reaktivni mehanizmi zaštite obuhvataju sisteme za detekciju napada i otkrivanje identiteta napadača. Naglasak u radu je na opisu mehanizama koji se koriste za zaštitu tri najrasprostranjenija protokola rutiranja u današnjem Internetu: OSPF (Open Shortest Path First), RIP (Routing Information Protocol) i BGP (Border Gateway Protocol).*

Ključne reči: *Internet, Preventivni mehanizmi, Reaktivni mehanizmi, Rutiranje, Zaštita*

1. Uvod

Značajan napredak ostvaren, poslednjih godina, u oblasti zaštite informacija u mrežama sa tehnologijom Internet protokola (IP) zasniva se na dve glavne komponente: zaštita podataka i kontrola prava pristupa mreži [1]. Skup IPsec (*IP security*) protokola [2] obezbeđuje kriptografske zaštitne mehanizme za IP pakete i servise zaštite kao što su poverljivost, integritet, utvrđivanje autentičnosti i zaštita od replikacije. Zaštita informacija podrazumeva bezbednu i pouzdanu infrastrukturu mreže (rutere, servere, gejtveje, linkove). Međutim, sama infrastruktura mreže može biti ugrožena napadima iz spoljnog okruženja ili unutrašnjim napadima. Spoljašnji napadač se obično "maskira" u neki element mreže i distribuira konstruisane, zakašnjene ili netačne kontrolne informacije. Unutrašnje napade vrše elementi mreže koji su sami napadnuti, što je znatno teže detektovati od spoljnih napada. Sistematizacija napada na infrastrukturu globalnog Interneta, predložena u [3], obuhvata četiri osnovne kategorije: (1) napadi na DNS (*Domain Name System*) servere; (2) zlonamerna modifikacija tabela rutiranja; (3) pogrešna obrada paketa u čvorovima i (4) odbijanje servisa (DoS – *Denial of Service*). Osim toga, implementacija arhitektura i mehanizama kvaliteta servisa značajno povećava opasnost od ugrožavanja bezbednosti infrastrukture IP mreže [4].

Predmet ovog rada je zaštita protokola rutiranja u Internetu. Rutiranje u Internetu zasniva se na distribuiranom sistemu, koji se sastoji od velikog broja rutera grupisanih u administrativne domene. Problem zaštite rutiranja je veoma aktuelan, s obzirom da originalne specifikacije postojećih protokola rutiranja nisu uzele u obzir

aspekte zaštite. U radu je prikazan pregled mogućih napada na infrastrukturu rutiranja u Internetu, kao i preventivnih i reaktivnih mehanizama zaštite tri najrasprostranjenija protokola rutiranja u današnjem Internetu: OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*) i BGP (*Border Gateway Protocol*).

2. Unicast protokoli rutiranja u Internetu

Za rutiranje u Internetu je usvojena tradicionalna podela na rutiranje unutar jednog administrativnog domena (*intra-domain*) i rutiranje između različitih domena (*inter-domain*). U zavisnosti od broja izvora i odredišta, algoritmi rutiranja mogu obuhvatati: rutiranje "tačka – tačka" (*unicast*), "tačka – više tačaka" (*multicast*) i "više tačaka – više tačaka" (*many-to-many*).

Dva najrasprostranjenija tipa *unicast* protokola rutiranja u Internetu su: (1) protokoli koji se zasnivaju na razmeni informacija o stanju linkova – LS (*Link State*) i (2) protokoli koji se zasnivaju na razmeni vektora rastojanja – DV (*Distance Vector*).

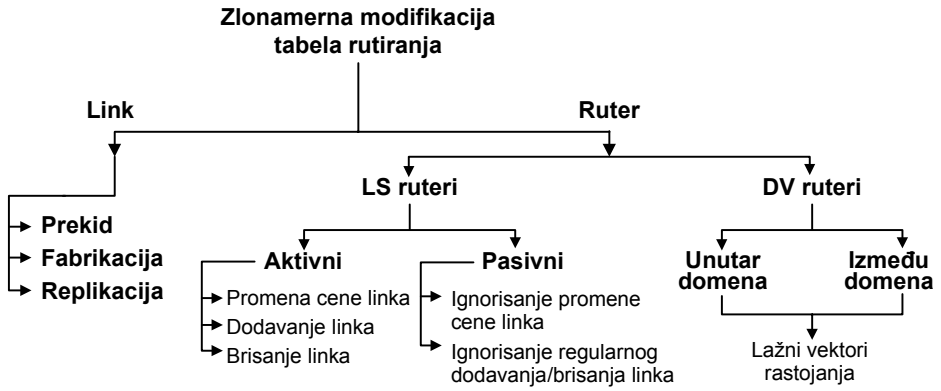
Najpoznatiji predstavnik **LS protokola** je OSPF, koji se primenjuje za rutiranje unutar jednog administrativnog domena. LS protokoli podrazumevaju centralizovano rutiranje saobraćaja u kome svaki čvor periodično šalje svim čvorovima u mreži kontrolne poruke sa informacijama o stanju svojih linkova. U OSPF se ovaj tip poruka naziva LSA (*Link State Advertisement*), a procedura prosleđivanja LSA je "plavljenje" (*flooding*). Kada primi informacije o stanju mrežnih linkova, svaki čvor formira logičko stablo sa najkraćim putanjama do svakog odredišta. Izračunavanje putanja se najčešće obavlja pomoću algoritma Dijkstra.

U **DV protokolima**, rutiranje saobraćaja je decentralizovano, tj. čvorovi nemaju informaciju o topologiji mreže. Svaki čvor prepoznaje samo susedne čvorove sa kojima razmenjuje kontrolne poruke (DV) i ažurira tabele sa rastojanjima ka svakom odredištu, preko svakog susednog čvora. Izračunavanje putanja se najčešće vrši pomoću distribuiranog algoritma Bellman-Ford, a izbor putanje se obavlja na osnovu kriterijuma najkraćeg rastojanja. Najpoznatiji predstavnici DV protokola su: RIP za rutiranje u domenu i BGP za rutiranje između domena. U BGP protokolu, informacija o rutiranju sadrži podatak o svim domenima kroz koje prolazi putanja, tj. vektor putanje, zbog čega se BGP u literaturi označava i kao ***path vector*** protokol.

3. Napadi na infrastrukturu rutiranja u Internetu

Zlonamerna modifikacija tabela rutiranja ("trovanje" – *poisoning*) vrši se unošenjem lažnih informacija u kontrolne pakete koje razmenjuju ruteri, na osnovu kojih se obavlja ažuriranje tabela rutiranja. Posledice takvih napada mogu biti: degradacija kvaliteta servisa usled rutiranja po putanjama koje nisu optimalne, zagušenje segmenta mreže koje se ne može otkloniti tradicionalnim mehanizmima kontrole zagušenja, kreiranje veštačkih particija koje su izolovane od ostatka mreže, formiranje petlji, DoS usled koncentracije ogromnih količina saobraćaja ka pojedinim serverima, neovlašćeno otkrivanje sadržaja informacija usled prolaza kroz deo mreže koji nije predviđen za prenos te klase ili tipa saobraćaja i dr.

Napadi na tabele rutiranja mogu se najopštije klasifikovati na (1) napade na linkove i (2) napade na rutere, kao što je prikazano na slici 1 [3].



Slika 1. *Klasifikacija napada na tabele rutiranja* [3]

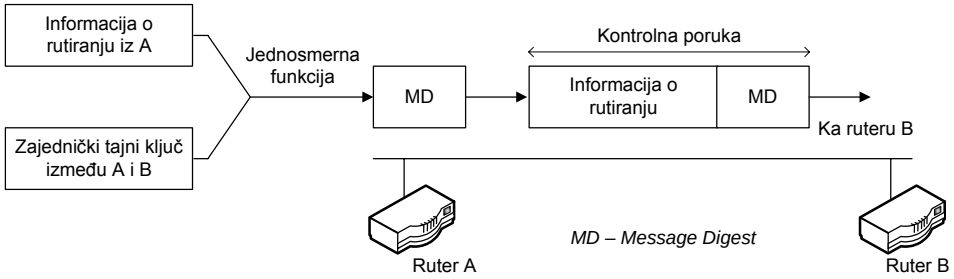
Napadi na linkove dešavaju se kada napadač ima pristup jednom ili više linkova u mreži. U tom slučaju, on može da prekine tok kontrolnih poruka sa informacijama o rutiranju, da modifikuje postojeće odnosno da generiše lažne kontrolne poruke (fabrikacija) ili da vrši replikaciju ranije poslatih kontrolnih poruka.

Napadi na rutere pripadaju kategoriji unutrašnjih napada, jer ih vrše ruteri koji su i sami napadnuti (tzv. kompromitovani ruteri). Vrste napada u ovom slučaju zavise od tipa protokola rutiranja. Napadi na LS rutere mogu biti aktivni, kada kompromitovani ruter menja cenu linka, dodaje nepostojeći link ili briše regularan link, ili pasivni, kada kompromitovani ruter ignoriše regularne promene stanja linkova. U napadima na DV rutere, kompromitovani ruter formira lažne vektore rastojanja i šalje ih susednim ruterima, koji prihvataju ove podatke, pošto nema načina da utvrde autentičnost porekla vektora rastojanja. U oba slučaja (LS i DV protokoli) veoma je teško sprečiti napade ako je ruter izložen tzv. Vizantijskim greškama (*Byzantine faults*), kada se on ne ponaša dosledno u interakcijama sa drugim ruterima u mreži.

4. Preventivni mehanizmi zaštite

Preventivni mehanizmi zaštite LS i DV protokola obuhvataju: (1) tehnike digitalnog potpisa za zaštitu integriteta i utvrđivanje autentičnosti kontrolnih poruka i (2) obeležavanje kontrolnih poruka rednim brojevima ili vremenskim pečatima, radi zaštite od promene redosleda ili replikacije.

Koncept PKI (*Public Key Infrastructure*) zasniva se na primeni javnih kriptografskih ključeva, koje distribuira "treća strana" od poverenja (*trusted entity*). U tom slučaju, svaki ruter poseduje par kriptografskih ključeva – privatni i javni. Ruter koji generiše kontrolnu poruku potpisuje tu poruku svojim privatnim ključem, a ostali ruteri mogu da verifikuju potpis pomoću javnog ključa. Koncept PKI je asimetričan po svojoj prirodi, jer ne predviđa uspostavljanje zaštitnih asocijacija između parova rutera i time omogućava izvoru distribuciju zaštićenih kontrolnih informacija i kada nisu poznati svi prijemnici. Veličina kontrolnih poruka se povećava za veličinu digitalnog potpisa (tipično 128–1024 bita). Definišu se metodi distribuiranja sertifikovanih (overenih) informacija o svakom ruteru i javnim ključevima.



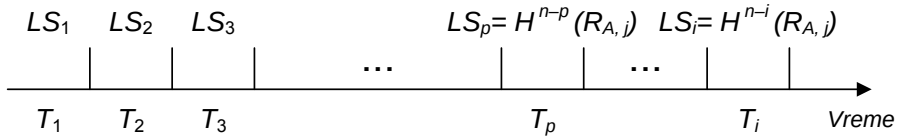
Slika 2. *MAC tehnika za zaštitu kontrolnih poruka koje razmenjuju susedni ruteri*

Koncept MAC (*Message Authentication Codes*) zasniva se na primeni simetričnih tajnih kriptografskih ključeva i koristi za zaštitu kontrolnog saobraćaja između susednih rutera, kao što je ilustrovano na slici 2. Zaštita se zasniva na primeni MD (*Message Digest*) algoritama, kao što je MD5, specificiran RFC dokumentom 1321. MD algoritam kombinuje zajednički tajni ključ i informaciju o rutiranju (proizvoljne dužine) za generisanje kratke poruke fiksne dužine (128 bita u slučaju MD5), koja se naziva MD ili "otisak prsta". Pretpostavlja se da je računski neizvodljivo generisanje takve kontrolne poruke koja bi imala unapred poznat ciljni MD, kao i da dve poruke imaju isti MD [5].

4.1 OSPF

Zaštita OSPFv2 (verzija OSPF namenjena za IPv4 mreže) digitalnim potpisima, predložena u IETF RFC dokumentu 2154 [6], zasniva se na principu priključivanja potpisa svakoj LSA poruci koja se prenosi kroz mrežu, distribuciji ključeva i sertifikovanih informacija o ruteru, kao i algoritmu za proveru autentičnosti između susednih rutera (sličnom kriptovanom MD5). Mehanizam podrazumeva: (1) primenu algoritma za formiranje digitalnog potpisa u svakom ruteru; (2) modifikaciju zaglavlja LSA dodavanjem digitalnog potpisa; (3) uvođenje novog tipa LSA (*Public Key* LSA – PKLSA) za distribuciju javnih ključeva unutar domena; (4) mehanizam za sertifikaciju ključeva i distribuciju sertifikata i (5) dodatne konfigurabilne parametre za svaki ruter (sertifikati, ključevi, tajmeri, informacija o "trećoj strani" od poverenja i dr.).

Veliki broj potpisanih LSA koji treba da budu generisani i provereni je značajan ograničavajući faktor u zaštiti LS protokola. Kompleksnost proračuna i dodatno saobraćajno opterećenje značajno zavise od topologije i veličine mreže, zbog čega je neophodno obezbediti efikasan i ekonomičan mehanizam digitalnog potpisa. Jedan takav mehanizam zasniva se na generisanju tzv. *hash* lanca u svakom ruteru [7]. *Hash* lanac se formira uzastopnim izvršavanjem *hash* funkcije nad slučajnom promenljivom. Osobina *hash* funkcije je da preslikava ulaz (niz bita) proizvoljne ili unapred određene dužine u izlaz konstantne dužine; *hash* funkciju je lako izračunati, ali veoma teško invertovati [5]. Ruter zatim koristi jedan element lanca po generisanom stanju linka, indeksiran vremenom ažuriranja. Ruteri koji primaju kontrolne LSA poruke primenjuju istu *hash* funkciju i trenutni vremenski pečat, a zatim vrše poređenje sa prethodno verifikovanim elementom.



Slika 3. *Korišćenje hash lanca za utvrđivanje autentičnosti ažuriranja stanja linkova* [7]

Princip korišćenja *hash* lanca za utvrđivanje autentičnosti ažuriranja stanja linkova ilustrovan je na slici 3. Pretpostavimo da ruter A selektuje slučajnu promenljivu $R_{A,j}$ za svoj link j i izračunava *hash* lanac na osnovu sledeće rekurzivne formule:

$$H^n(R_{A,j}) = H(H^{n-1}(R_{A,j})), \quad (1)$$

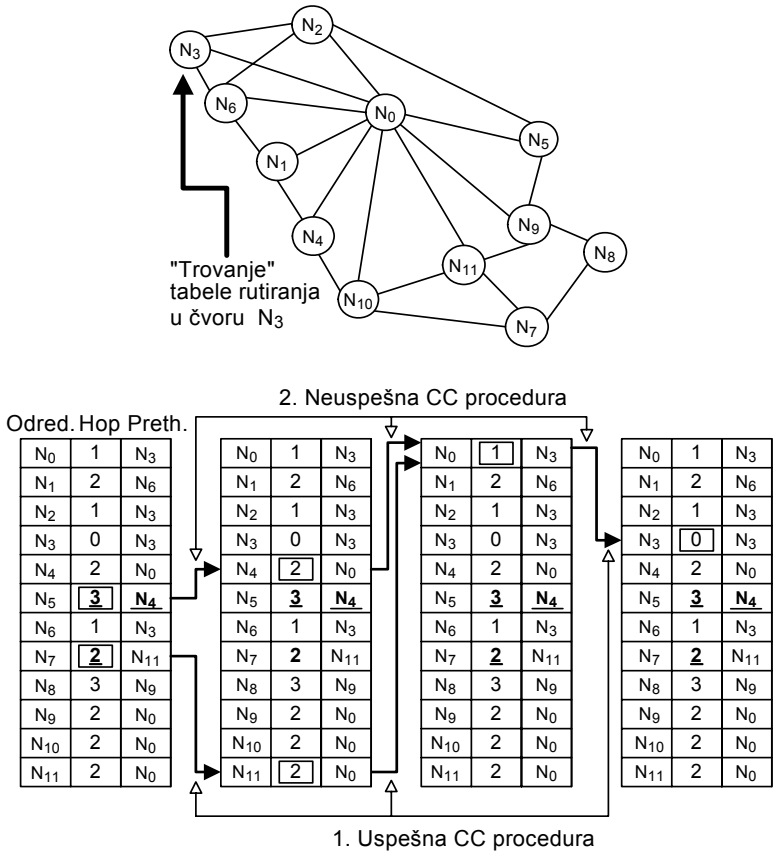
gde je H – *hash* funkcija, n – dužina *hash* lanca i $H^0(R_{A,j}) = R_{A,j}$. Ostali ruteri u mreži inicijalno primaju $H^n(R_{A,j})$. U trenutku T_i, ruter A generiše $H^{n-i}(R_{A,j})$ za utvrđivanje autentičnosti ažuriranja stanja linka (A, j). Svaki ruter koji prima LSA ima neko prethodno provereno stanje linka (A, j), na primer, $LS_p = H^{n-p}(R_{A,j})$, iz intervala T_p. Ako LSA sadrži promenu stanja linka, smatra se da je ona autentična ako je $H^i(LS_i) = H^n(R_{A,j})$. Ako LSA ne sadrži promenu stanja linka, LS_p se upoređuje sa $H^{i-p}(LS_i)$. Opisani mehanizam pretpostavlja da se informacije o stanju linkova generišu periodično i zasniva se na dobro sinhronizovanim taktovima u svim ruterima mreže. Osim toga, mehanizam predviđa korišćenje zasebnog *hash* lanca za svako stanje linka, što znači da je najefikasniji u slučajevima kada se pretpostavljaju samo dva stanja linka (UP – link u funkciji i DOWN – ispad linka). Korišćenje mere rutiranja (težinskog faktora, cene) sa više vrednosti podrazumeva generisanje zasebnog lanca za svaku vrednost, što zahteva znatno kompleksniji proračun i procesiranje kontrolnih poruka.

Verzija OSPF namenjena za IPv6 mreže – OSPFv3 koristi karakteristike IPsec koje su ugrađene u IPv6, odnosno zasniva zaštitu rutiranja na IPv6 AH (*Authentication Header*) i IPv6 ESP (*Encapsulating Security Payload*) za obezbeđivanje integriteta, utvrđivanje autentičnosti i/ili poverljivosti informacija [8].

4.2 RIP

Za zaštitu od napada na DV rutere, u [9] je predložena procedura za proveru doslednosti (CC – *Consistency Check*), koja se primenjuje u procesu ažuriranja tabela rutiranja, kao što je prikazano primerom na slici 4. Da bi se osigurala autentičnost i integritet informacija, CC procedura može se kombinovati sa tehnikama digitalnog potpisa. Procedura podrazumeva da je cena putanje određena brojem *hop*-ova do svakog odredišta (kao što je slučaj sa RIP protokolom), a tabele rutiranja proširuju se kolonom koja sadrži podatak o čvoru koji prethodi svakom odredištu. Pretpostavićemo da čvor N_3 šalje lažne vektore rastojanja svojim susedima N_2 i N_6. Pri tome, za svako odredište, on šalje podatke koji odgovaraju vrstama tabele rutiranja, u kojoj prva kolona predstavlja

adresu odredišta, druga kolona predstavlja najkraće rastojanje do odredišta, izraženo brojem *hop*-ova, a treća kolona sadrži adresu čvora koji prethodi odredištu. Kada čvorovi N_2 i N_6 prime vektor rastojanja iz čvora N_3, aktiviraju CC algoritam da provere doslednost putanje u povratnom smeru. U prvom primeru na slici 4 je zlonamerno modifikovan broj *hop*-ova do N_7, a CC algoritam otkriva nedoslednost. Međutim, u drugom primeru, napadač vešto koristi znanje o topologiji mreže i istovremeno modifikuje podatke o broju *hop*-ova i čvoru koji prethodi odredištu N_7, a CC algoritam ne uspeva da detektuje nedoslednost, jer se broj *hop*-ova u povratnom lancu regularno dekrementira od 3 do 0.

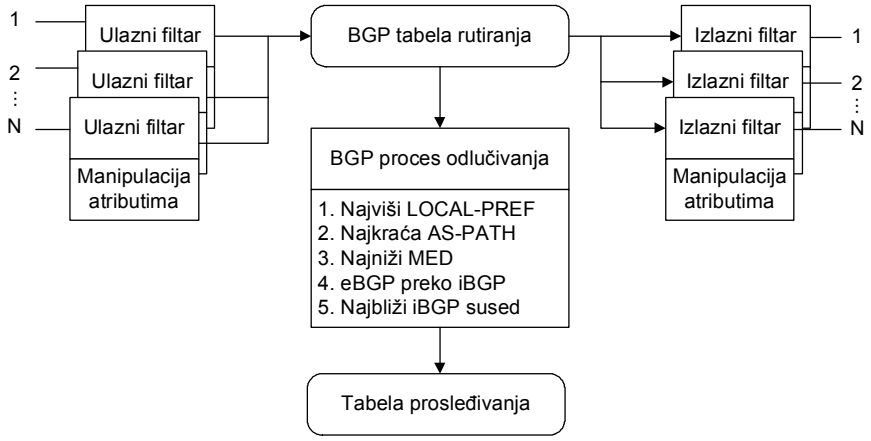


Slika 4. *Primeri provere doslednosti DV tabela rutiranja* [4]

4.3 BGP

BGPv4, specificiran IETF dokumentom RFC 1771, je de facto standardni protokol rutiranja između domena u današnjem Internetu. U BGP terminologiji, domen se naziva autonomnim sistemom (AS). U BGP protokolu, kontrolna poruka UPDATE sa

informacijom o rutiranju sadrži indikator dostupnosti odredišta, atribut putanje (*AS-path*) sa listom svih tranzitnih domena do odredišta i adresu susednog BGP rutera kome se upućuje saobraćaj do naznačenog odredišta. Informacija o rutiranju može takođe sadržati opcione atribute kao što su: lokalni prefiks – *local-pref*, diskriminator višestrukih izlaza – *multi-exit discriminator* (MED) i dr. Postoje dve varijante BGP: (1) **eBGP** za razmenu informacija o dostupnim prefiksima između BGP rutera koji pripadaju različitim domenima i (2) **iBGP** za distribuciju informacije o najboljim putanjama unutar domena.



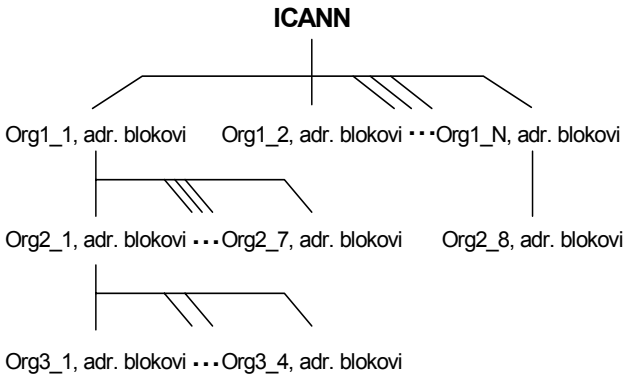
Slika 5. *Princip funkcionisanja BGP rutera*

Princip funkcionisanja BGP rutera je ilustrovan na slici 5. Administrator specificira ulazni filtar, pomoću koga se obavlja izbor prihvatljivih informacija o rutiranju od svakog susednog BGP rutera. Na primer, ruter može izabrati samo putanje koje sadrže skup domena od poverenja (*trusted domains*). Informacija o rutiranju se, zatim, memoriše u BGP tabeli rutiranja, pri čemu je moguće lokalno ažuriranje pojedinih atributa. Tabela rutiranja sadrži skup svih prihvatljivih putanja primljenih od susednih BGP rutera. U procesu odlučivanja biće izabrana najbolja putanja ka svakoj poznatoj mreži. Na osnovu sledećeg *hop*-a najbolje putanje i tabele rutiranja u domenu, BGP ruter će upisati rutu ka toj mreži u svoju tabelu prosleđivanja. Pretraživanjem tabele prosleđivanja, BGP ruter selektuje izlazni interfejs ka naznačenom odredištu za svaki primljeni IP paket. Pored toga, ruter koristi izlazne filtre za selekciju najbolje od svih prihvatljivih putanja u tabeli rutiranja i o tome obaveštava svaki susedni BGP ruter. Pri tome je dozvoljeno selektovati najviše jednu putanju za jedno odredište.

Uprkos širokoj rasprostranjenosti BGP, do danas nisu standardizovane ekstenzije ovog protokola koje obuhvataju zaštitne mehanizme. Tek se nedavno pojavila sistematična analiza osetljivosti BGP na spoljne i unutrašnje napade (RFC dokument 4272 [10] iz 2006. godine), koja obuhvata pregled "ranjivih tačaka" u samom protokolu, kao i u interakcijama BGP sa drugim protokolima kao što je TCP.

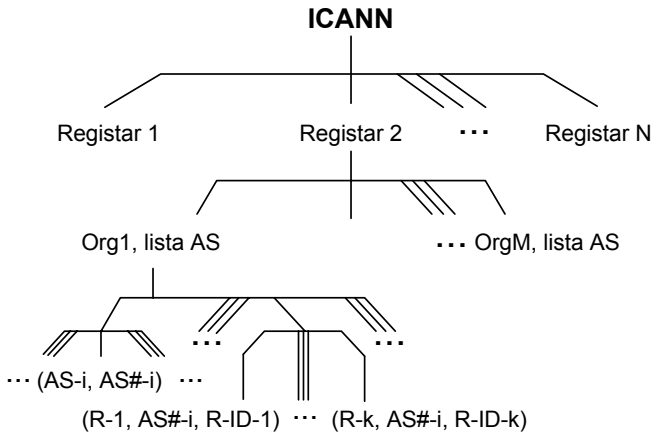
Pošto BGP u osnovi pripada klasi DV protokola, princip CC procedure, opisan u poglavlju 4.2, primenljiv je na ovaj protokol. Zahvaljujući razmeni informacija o kompletnoj putanji, BGP inherentno eliminiše problem originalne CC procedure, koji se

pojavljuje kada cena putanje nije određena brojem *hop*-ova, već izražava funkciju relevantnog parametra performanse linkova. Svaki BGP ruter identifikuje autonomne sisteme koji mu neposredno prethode, održava baze podataka sa informacijama o AS – prethodnicima i utvrđuje autentičnost putanje u povratnom smeru – polazeći od odredišta i njegovog neposrednog prethodnika, kroz celu bazu podataka, dok se celokupna putanja u potpunosti ne verifikuje ili odbaci. U ovom slučaju je neophodno da digitalni potpis obuhvati celu putanju od izvora do odredišta (a ne samo odredište i AS koji mu neposredno prethodi), kako bi se korektno verifikovale i one putanje koje sadrže samo tranzitne AS [7].



Slika 6. *Stuktura PKI za dodelu adresa* [11]

U [11] je predložena specifikacija S-BGP (*Secure* BGP) koja se zasniva na primeni dva PKI mehanizma. Prvi PKI (slika 6) se koristi za sertifikaciju vlasništva nad adresnim prostorom koji se odobrava svakoj organizaciji. Koren hijerarhijskog stabla predstavlja ICANN (*Internet Corporation for Assigned Names and Numbers*), za kojim slede organizacije ovlašćene za dodelu regionalnog adresnog prostora (ARIN – *American Registry for Internet Names*, RIPE – *Résaux IP Européens* i dr.), provajderi Internet servisa i krajnji korisnici. Drugi PKI (slika 7) koristi se za sertifikaciju identiteta autonomnih sistema i njihovih BGP rutera. I u ovom slučaju je ICANN koren stabla, drugi nivo sastoji se od DNS imena registara, treći nivo sačinjavaju organizacije – vlasnici AS-ova, iza čega sledi lista brojeva AS (AS#-i) i IP adresa njihovih BGP rutera (R-ID-k). Zahvaljujući šemi udvojenih PKI, BGP ruteri mogu da verifikuju informaciju o vlasništvu AS, identitet AS i identitet drugih BGP rutera. Sa takvom hijerahijom, na svaku poruku UPDATE primenjuju se dva tipa digitalnih potpisa: atesti adrese i atesti rute.



Slika 7. *Stuktura PKI za identifikaciju AS i BGP rutera* [11]

5. Reaktivni mehanizmi zaštite

Reaktivni mehanizmi zaštite obuhvataju sisteme za detekciju napada i otkrivanje identiteta napadača (IDS – *Intrusion Detection Systems*). Takvi mehanizmi se zasnivaju na pretpostavci da se ponašanje napadača (npr. kompromitovanog rutera) značajno razlikuje od ponašanja drugih elemenata mreže. U kontekstu napada na protokole rutiranja, od suštinskog značaja je da se precizno definiše šta je normalno ponašanje rutera, posebno u procesu pronalaženja ruta.

U [12] je predložena arhitektura centralizovanog modula za analizu napada na LS protokole rutiranja, koji detektuje napade na osnovu mogućih sekvenci alarmnih događaja. Iako su takvi sistemi korisni za identifikaciju zlonamernih aktivnosti u mreži, oni imaju dva glavna nedostatka: (1) nesposobnost da detektuju distribuirane ili koordinisane napade i (2) loša skalabilnost zbog centralizovanog procesiranja velike količine podataka.

Alternativni pristup se zasniva na inkorporaciji procedura za detekciju napadača u protokole rutiranja. U [13] je predložen SLIP (*Secure Link State Protocol*) koji se zasniva na potvrđivanju LSA poruka, pre ažuriranja tabela rutiranja. Nedostatak ovog rešenja je što podrazumeva simetričnu mrežu, u kojoj oba čvora povezana linkom moraju da budu sposobna da identifikuju promenu stanja linka.

Osnovu distribuiranih IDS [14], [15] predstavlja skup heterogenih senzora raspoređenih po infrastrukturi mreže, programiranih nizovima potpisa koji opisuju moguća zlonamerna ponašanja. Celokupan saobraćaj koji se prenosi kroz mrežu poredi se sa tim potpisima u cilju detekcije zlonamernog saobraćaja. Glavni problem distribuiranih IDS predstavlja konfigurisanje senzora u skladu sa karakteristikama konkretne mreže. Zbog prirode rutiranja, konfiguracija senzora mora da uzme u obzir topologiju mreže, pozicioniranje senzora u mreži i karakteristike konkretnog protokola rutiranja. Osim toga, pojedini napadi mogu se detektovati samo u međusobnoj komunikaciji senzora. Kao posledica, konfigurisanje potpisa koje koriste senzori može da bude dugotrajno, neefikasno i podložno greškama.

6. Zaključak

Napadi na infrastrukturu rutiranja u Internetu mogu prouzrokovati degradaciju kvaliteta servisa, zagušenje segmenata mreže, kreiranje veštačkih particija, formiranje petlji, DoS, neovlašćeno otkrivanje sadržaja informacija i dr. Preventivni mehanizmi zaštite zasnivaju se na tehnikama digitalnog potpisa i sekvenciranju kontrolnih poruka. Koncept PKI omogućava distribuciju zaštićenih kontrolnih informacija i kada nisu poznati svi ruteri – prijemnici. Generisanje i provera velikog broja potpisanih kontrolnih poruka mogu prouzrokovati kompleksne proračune u ruterima i povećano saobraćajno opterećenje, zbog čega je neophodno obezbediti efikasne algoritme digitalnog potpisa. IDS sistemi, kao osnovni reaktivni mehanizam zaštite, mogu se realizovati kao centralizovani, u sklopu sistema za nadzor i upravljanje mrežom, ili distribuirani (zasnovani na modifikacijama protokola rutiranja ili na sistemu senzora raspoređenih po infrastrukturi mreže). Sa ciljem da se verifikuje efikasnost predloženih rešenja zaštite, neophodne su detaljne studije izvodljivosti za svaki konkretan tip protokola i za mreže različitih topologija, veličine i kapaciteta linkova.

Literatura

[1] R. J. Sutton, *"Secure Communications: Applications and Management"*, John Willey & Sons, 2002.
[2] S. Kent, R. Atkinson, *"Security Architecture for the Internet Protocol"*, RFC 2401 (Standards Track), IETF, 1998.
[3] A. Chakrabarti, G. Manimaran, *"Internet Infrastructure Security"*, IEEE Network, vol. 16, no. 6, November/December 2002, pp. 13-21.
[4] M. Stojanović, V. Aćimović-Raspopović, *"Inženjering telekomunikacionog saobraćaja u multiservisnim IP mrežama"*, monografija, Saobraćajni fakultet Univerziteta u Beogradu, oktobar 2006.
[5] D. Eastlake, T. Hansen, *"US Secure Hash Algorithms (SHA and HMAC-SHA)"*, RFC 4634 (Informational), 2006.
[6] S. Murphy, B. Wellington, *"OSPF with Digital Signatures"*, RFC 2154 (Experimental), IETF, 1997.
[7] P. Papadimitratos, Z. J. Haas, *"Securing the Internet Routing Infrastructure"*, IEEE Communications Magazine, vol. 40, no. 10, October 2002, pp. 60-68.
[8] M. Gupta, N. Melam, *"Authentication/Confidentiality for OSPFv3"*, RFC 4552 (Standards Track), IETF, 2006.
[9] B. R. Smith, S. Murthy, J. J. Garcia-Luna-Aceves, *"Securing Distance Vector Routing Protocol*s", in Proceedings of the Symposium on Network Distributed Systems Security, February 1997, pp. 85-92.
[10] S. Murphy, *"BGP Security Vulnerability Analysis"*, RFC 4272 (Informational), IETF, 2006.
[11] S. Kent, C. Lynn, K. Seo, *"Secure Border Gateway Protocol (S-BGP*)", IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, April 2000, pp. 582-592.
[12] F. Wang et al. *"Intrusion Detection for Link State Routing Protocol through Integrated Network Management"*, in Proceedings of the ICCCN, 1999, pp. 694-699.
[13] A. Chakrabarti, G. Manimaran, *"A Scalable Method for Router Attack Detection and Location in Link State Routin*g", DCNL Tech. Report, October 2002.
[14] V. Mittal, G. Vigna, *"Sensor-Based Intrusion Detection for Intra-Domain Distance-Vector Routing"*, in Proceedings of the CCS, ACM, 2002, pp. 127-137.
[15] R. A. Wasniowski, *"Multisensor Agent Based Intrusion Detection"*, Transactions on Engineering, Computing and Technology V5, April 2005, pp. 110-113.

Abstract: *In this paper, we present a survey of possible threats to the Internet routing infrastructure and mechanisms for securing unicast routing protocols. Preventive security mechanisms encompass various techniques of digital signatures to provide data integrity and authentication, and sequence information (numbers or time stamps) to prevent message disordering or replication. Reactive security mechanisms refer to diverse architectures of intrusion detection systems. The emphasis in this paper is on securing the three widely deployed Internet routing protocols: OSPF (Open Shortest Path First), RIP (Routing Information Protocol) and BGP (Border Gateway Protocol).*

Keywords: *Internet, Preventive mechanisms, Reactive mechanisms, Routing, Security*

SECURITY OF THE INTERNET ROUTING PROTOCOLS
Mirjana Stojanović, Slavica Boštjančič