Zaštita NSIS protokola u telekomunikacionim mrežama zasnovanim na Internet tehnologiji

Dimitrije Paunović (mentori: prof dr Zoran Petrović, prof dr Miroslav Dukić, doc dr Mirjana Stojanović)

***Sadržaj* - Ovaj rad razmatra probleme zaštite NSIS (Next Steps in Signaling) protokola, koji se sastoji iz dva sloja (transportnog i signalizacionog) od kojih svaki zahteva drugačiji vid zaštite. Analizirane su bezbednosne slabosti i načini na koje bi napadač mogao da ih iskoristi, kao i mogućnosti zaštite slabih tačaka protokola od napada.**

Ključne reči – Internet, kvalitet servisa, signalizacija, zaštita

I UVOD

Razvojem Interneta pojavila se potreba za poboljšanim performansama prenosa informacija za različite nove servise. Ta potreba se ogledala u dostupnosti mreže, garantovanom protoku, varijaciji kašnjenja, gubitku paketa. Današnja internet tehnologija bazirana na best effort principu ne zadovoljava zahteve naprednih aplikacija. Da bi se prevazišla postojeća ograničenja uveden je novi skup protokola NSIS (*Next Steps In Signaling*) koji predstavlja okvirni rad za više signalizacionih aplikacija na IP baziranoj mreži [1].

U ovom radu ćemo se baviti problemom zaštite NSIS signalizacionih protokola, koja obuhvata brojne probleme, pošto NSIS teži tome da podrži veliki broj scenarija, uključuje veliki broj signalizacionih entiteta, omogućava upotrebu raznih uređaja od servera visokih performansi korporativnih mreža do mobilnih uređaja. NSIS skup protokola, takođe, podržava raznovrsne mehanizame kriptozaštite (simetrična i asimetrična kriptozaštita, različiti protokoli autentifikacije) i postojeće mrežne arhitekture, kao što su PacketCable ili 3GPP arhitekture. U radu su prvo ukratko opisana svojstva NSIS arhitekture, koja obuhvata transportni sloj i signalizacioni sloj. Zatim su analizirani mogući napadi na svaki od NSIS slojeva. Na kraju su prikazana moguća rešenja – tehnike zaštite NSIS protokola.

II. OSNOVNA SVOJSTVA NSIS PROTOKOLA

Poslednjih godina pojavio se veliki broj aplikacija koje zahtevaju signalizaciju na mrežnom sloju - uspostavljanje, održavanje i uklanjanje kontrolnog stanja u elementima mreže. Ove aplikacije zahtevaju fleksibilan i bezbedan signalizacioni protokol, koji omogućava upravljanje signalizacijom QoS (signalizacija spregnutim putanjama i signalizacija putanjama koje nisu spregnute sa tokom korisničkih podataka) i alokaciju resursa, kao i kontrolu debagovanja mreže, NAT-a i *firewall*-a.

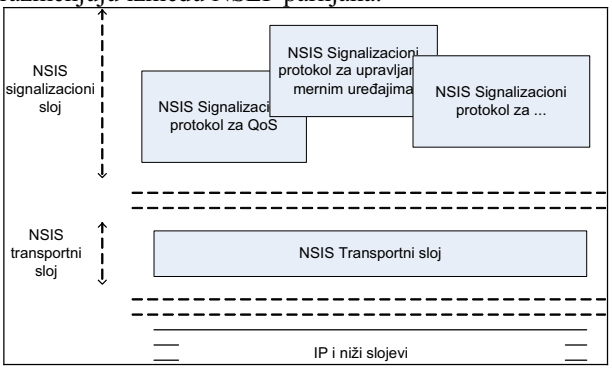
NSIS entitet (NE) je funkcija u čvoru koja implementira NSIS protokol.

Dimitrije Paunović, Elektrotehnički fakultet, Bul. Kralja Aleksandra 73, Beograd, Srbija; (tel:+381641115145 , e-mail:dishapaun@gmail.com).

NSIS entiteti koji komuniciraju međusobno imaju ravnopravan odnos. Svaki entitet može da čuva podatke o svojim „parnjacima“ (*peers*). Jedan čvor, NI (*NSIS Initiator*), inicira signaliziranje, tranzitni čvorovi na putanji (NF, *NSIS Forwarders*), presreću i prosleđuju signalizacione poruke, dok NR (*NSIS Responder*) okončava signalizaciju. Na putanji nije obavezno da svi ruteri budu NSIS-svesni, niti da svi NSIS čvorovi podržavaju sve signalizacione aplikacije. U nastavku su opisani osnovni principi dizajna NSIS protokola.

Razdvajanje transporta signalizacione poruke od signalizacionih aplikacija podrazumeva podelu NSIS arhitekture na dva sloja (Sl. 1):

- Sloj transporta signalizacije na kome se definiše NTLP (*NSIS Transport Layer Protocol*), koji je odgovoran za prenos signalizacionih poruka i nezavisan od bilo koje signalizacione aplikacije. NTLP se tipično realizuje u formi generalnog transportnog protokola za signalizaciju u Internetu – GIST (*General Internet Signaling Protocol*), koji koristi standardne nekonektivne i konektivne transportne protokole i mehanizme zaštite.
- Sloj signalizacione aplikacije koji sadrži NSIS protokole signalizacionog sloja (NSLPs – *NSIS Signaling Layer Protocols*), od kojih svaki podržava specifičnu funkcionalnost potrebnu signalizacionoj aplikaciji, uključujući formate i pravila o obradi poruka koje se razmenjuju između NSLP parnjaka.



Sl 1. Komponente NSIS protokola

Druga bitna odluka pri dizajniranju protokola se odnosi na **odvajanje otkrivanja NSIS parnjaka od transportnog mehanizma signalizacionih poruka** transportnog sloja. NSIS rešava tu dilemu uvođenjem komponente otkrivanja u GIST koji se može osloniti na opciju alarmiranja IP rutera ili koristiti neki drugi pristup kao što su tabele rutiranja.

U NSIS-u je tok podataka definisan kao jednosmerna sekvenca paketa između istih krajnjih tačaka koji prate jedinstvenu putanju kroz mrežu. Oni se identifikuju pomoću identifikatora toka. Pored identifikatora toka, NSIS uvodi **identifikator sesije**, slučajni šifrovani broj, koji sa određenom verovatnoćom, jedinstveno identifikuje signalizacionu sesiju i stanje, nezavisno od identifikatora toka. Sesija može označiti poseban tok, ali u scenarijima kao

što su mobilnost, *multi-homing*, tunelovanje i prelaz IPv4/IPv6 signalizacione aplikacije mogu kreirati složenije odnose tok/sesija.

NSIS signalizacija se može primeniti u različitim delovima Interneta i može biti pokrenuta na različiti načine. Ovo je neophodno da bi se omogućilo da signalizacija bude inicirana i završena u različitim delovima mreže, tj. u krajnjim hostovima, na granicama domena i unutrašnjim ruterima. NSIS protokol na ovaj način **podržava različite vrste signalizacije**, uključujući signalizaciju „tačka-tačka“ gde se razmena vrši između krajnjih hostova, signalizaciju „ivica-ivica“ gde granični čvorovi domena mogu da komuniciraju direktno i signalizaciju „tačka-ivica“, kao što je host-mreža scenario signalizacije.

III Problemi zaštite NSIS protokola

Pošto je NSIS skup protokola podeljen na dva sloja, rešenje zaštite mora da ponudi zaštitu oba sloja [2]. Mora se dati odgovor na pretnje koje pogađaju sve signalizacione protokole i, takođe, posvetiti posebna pažnja na pretnje specifične za NSIS skup protokola.

A. Opšte pretnje

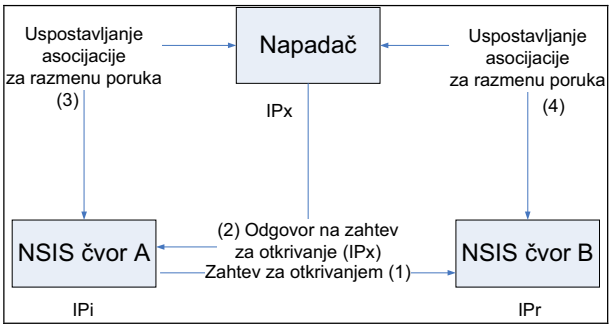
U ovom delu razmatramo pretnje koje su generalno primenjive na signalizacione protokole. Posmatraćemo dva odvojena slučaja kada može doći do napada jer se zaštita protokola najčeše odvija u dva koraka. U prvom koraku se vrši autentifikacija i uspostavljanje ključeva što dovodi do stvaranja zaštitne asocijacije, dok drugi korak podrazumeva zaštitu poruka (proveru porekla, integriteta podataka, zaštite od ponavljanja itd.), pri čemu se koristi već uspostavljena zaštitna asocijacija.

Man-in-the-middle **napadi** podrazumevaju sigurnosne pretnje koje postoje kada: (1) parnjaci nisu u zaštitnoj asocijaciji; (2) ne koriste zaštitne mehanizme i (3) kada je zaštitna asocijacija već uspostavljena.

Napadi tokom uspostavljanja zaštitne asocijacije. Tokom uspostavljanja zaštitne asocijacije, napadač može da prevari Inicijatora signalizacije, predstavljajući se kao entitet kojeg on treba da autentifikuje. Inicijator autentifikuje *man-in-the-middle* napadača, koji je tada u mogućnosti da modifikuje signalizacione poruke da bi izveo DoS napad ili da koristi usluge koje će biti naplaćene Inicijatoru. Napadač, takođe, može da uništi Inicijatorove NSIS signalizacione poruke i da sam ubaci poruke parnjaku. Kao rezultat ovoga, Inicijator pogrešno veruje da razgovara sa pravom mrežom, a u stvari je spojen sa napadačem. Da bi ovaj napad bio uspešan moraju biti ispunjeni sledeći uslovi: nedostajuća autentifikacija, unilateralna autentifikacija i slaba autentifikacija [3].

Razmatranje *man-in-the-middle* napada završavamo sa **napadom tokom faze otkrivanja**. Ovaj napad je moguć jer je verovatno da NSIS čvorovi nisu svesni topologije mreže. Napadač može da ubacuje besmislene poruke, primoravajući inicijatora poruke za otkrivanje da počne uspostavljanje asocijacije za slanje poruka sa napadačem ili sa NSIS čvorom koji nije na putanji. *Man-in-the-middle* napadač može preusmeriti asocijaciju ka drugom legitimnom NSIS čvoru. Odgovarajući mehanizmi zaštite mogu otkriti zlonamerni NSIS čvor, ali ne i legitimni NSIS čvor koji ne predstavlja sledeći NSIS čvor duž putanje bez poznavanja mrežne topologije.

Na Sl. 2 prikazan je tipičan primer napada prilikom otkrivanja mrežne topologije. Napadač može da prisluškuje početnu poslatu poruku za otkrivanje i vraća odgovor na poruku za otkrivanje sa svojom IP adresom predstavljajući se kao sledeći NSIS-svestan čvor na putanji.



Sl. 2 Napad prilikom otkrivanja mrežne topologije

Tada se uspostavlja asocijacija za razmenu poruka sa napadačem, koji zatim uspostavlja asocijaciju za razmenu poruka sa narednim NSIS čvorom i prosleđuje signalizacionu poruku. Napadač može promeniti odgovor na poruku za otkrivanje primoravajući NSIS čvor da uspostavi asocijaciju za razmenu poruka sa drugim NSIS čvorom koji se ne nalazi na putanji.

Napadač može presretati i prikupljati signalizacione poruke da bi ih kasnije **maliciozno ponavljao** sa ciljem da izvede *man-in-the-middle* napad, DoS ili krađu servisa. Problemi mogu da nastanu čak i kada postoji zaštita od ponavljanja, ali napadač mora da uništi NSIS-svestan čvor izazivajući time gubitak informacija o stanju (redni brojevi, zaštitna asocijacija, itd.) i da nakon toga počne sa ponavljanjem starih poruka koristeći nedostatke procesa resinhronizacije. Takođe, napadač može izvršiti **izmenu signalizacionih poruka** sa ciljem da izazove neočekivano ponašanje mreže kao i da izazove veliku potrošnju resursa što će dovesti do odbacivanja ostalih legitimnih zahteva.

Protokol mora da zadovolji određeni skup mehanizama zaštite i pridruženih parametara. Teško je zadovoljiti ove, često suprotstavljene zahteve, samo jednim bezbednosnim mehanizmom ili fiksnim skupom bezbednosnih parametara. **Nebezbedna razmena parametara ili protokol za uspostavljanje zaštitne asocijacije** mogu pomoći napadaču da izvede napad tako što će primorati korisnike da izaberu slabije zaštićene mehanizme od onih koji su bili ranije uzajamno zahtevani. Na ovaj način, bez vezivanja pravih strana za proces ugovaranja parametara i njihove zaštite, sigurnost NSIS svodi se na najslabiji ponuđeni način zaštite, a prednosti definisanja konfiguracionih parametara i protokola ugovaranja su izgubljene.

B. Pretnje specifične za NSIS protokol

U ovom poglavlju su razmatrane tipične pretnje specifične za NSIS protokol .

Plavljenje kao vid pretnje na NSIS protokole nastaje usled procesiranja opcije RAO (*Router Alert Option*), kao forsiranja NTLP/NSLP na složeniju obradu.

- **Procesiranje RAO opcije** zahteva da ruter presreće IP pakete, što može voditi do dodatnog kašnjenja legitimnih paketa i odbacivanja nekog od njih. Ruter koji je preplavljen

besmislenim porukama zahteva resurse pre nego što odluči da ove poruke treba da odbaci. Ako je protokol baziran na presretanju isporučenja poruka, ova pretnja se ne može potpuno eliminisati, ali dizajn protokola bi trebalo da pokuša da ograniči potrebnu obradu.

- Neka polja u zaglavlju protokola mogu dozvoliti napadaču da **natera NTLP čvor na složeniju obradu**. Dodatno je moguća interferencija sa kontrolom protoka ili procedurom kontrole zagušenja. Takođe je moguće naterati NTLP čvor da vrši odgovarajuće proračune ili razmenu signalizacionih poruka ubacivanjem „okidača" događaja (*trigger events*) koji su nezaštićeni.
- Napadač može imati koristi od **forsiranja NSLP-a na složeniju obradu** plavljenjem čvora porukama koje se moraju sačuvati (npr. zbog fragmentiranja) pre nego što se izvrši provera njihove tačnosti. Opterećenje procesora i memorije može da onemogući funkcionisanje NSIS entiteta. Ako signalizaciona poruka sadrži digitalni potpis, tada je potrebna dodatna obrada da bi se izvršila kriptografska verifikacija. Napadač lako može kreirati sekvencu slučajnih bitova umesto digitalnog potpisa i time naterati NSIS čvor na zahtevnu obradu što može dovesti do njegovog otkaza.

Ako je napadač u mogućnosti da prisluškuje signalizacione poruke može na osnovu prikupljenih poruka da izvrši **analizu saobraćaja** ili ih može kasnije iskoristiti za napade ponavljanjem signalizacionih poruka. Onaj koji prisluškuje može saznati QoS parametre, modele komunikacije, pravila za prolazak *firewall*-a, politiku o informacijama, identifikatore aplikacija, identitete korisnika, objekte autorizacije, konfiguraciju mreže, informacije o performansama itd.

Krađa identiteta koja se odnosi na NSIS može nastati u tri oblika: (1) tokom uspostavljanja zaštitne asocijacije zbog slabe zaštite mehanizma autentifikacije; (2) napadač može promeniti identifikator toka koji se nalazi u signalizacionoj poruci i (3) moguće je izvršiti krađu saobraćaja kroz mrežu.

Nezaštićene autorizacione informacije mogu se pojaviti u slučaju korišćenja autorizacionog žetona (*token*). Vraćajući nezaštićeni *token* krajnjem hostu, napadaču se može omogućiti krađa resursa. Problem vlasništva nad sesijom/rezervacijom može se posmatrati i kao problem autorizacije. U korporativnim mrežama autorizacija je povezana sa članstvom korisnika u određenim klasama ili grupama korisnika.

Nedostatak procedure za priznavanje (*non-repudiation*) predstavlja problem kod signalizacije za QoS koja često uključuje tri strane: korisnika, mrežu koja nudi rezervaciju QoS (provajder usluge) i treću stranu koja garantuje da strana koja obezbeđuje rezervaciju dobija odgovarajuću finansijsku nadoknadu. U ovom kontekstu, *non-repudiation* se odnosi na problem gde ili korisnik ili servis provajder kasnije poriču postojanje nekih parametara QoS rezervacije prema trećoj strani od poverenja. Problemi koji nastaju zbog nepriznavanja iskazuju se kako iz aspekta provajdera servisa, tako i iz aspekta korisnika servisa.

Elementi mreže u okviru domena imaju različite nivoe poverenja u odnosu na krajnje NSIS entitete, a napadaču je cilj da uspostavi **zlonameran NSIS entitet**. Podrazumeva se da su krajnji NSIS entiteti odgovorni za kriptografsku zaštitu (autentifikaciju, zaštitu integriteta i zaštitu od ponavljanja, autorizaciju i tarifiranje) dolaznih signalinzacionih poruka koje stižu iz drugih domena. Na ovaj način se sprečava pojava nezaštićenih signalizacionih poruka u okviru jednog domena. Ako napadač nekako uspe da preuzme ivični ruter kompromitovana je bezbednost cele mreže. Kompromitovani *firewall* može oštetiti druge *firewall*-ove promenom pravila.

Da bi napad uspeo mora postojati NSIS-svestan čvor na putanji na kojeg je uspešno izveden napad ili napadač mora preuzeti neki drugi NSIS čvor i učiniti da on postane sledeći NSIS parnjak.

Odbijanje servisa (DoS) može dovesti do otkaza na NSIS čvoru.

Neki signalizacioni protokoli uspostavljaju stanja (npr. stanje rutiranja) i izvode neke akcije (npr. pronalaženje resursa) na brojnim NSIS čvorovima bez zahteva za autorizacijom (ili čak ni autentifikacijom) bazirane na jednoj poruci. Napadač može koristiti ovu činjenicu da prilikom **pronalaženja putanje** prenosi veliki broj signalizacionih poruka, alocira stanja u čvorovima duž putanje i da izazove potrošnju resursa.

Proces otkrivanja parnjaka je ranjiv u odnosu na mnoge napade jer ga je teško zaštiti. Napadač može koristiti mehanizme otkrivanja da ubedi entitet da pošalje signalizacionu informaciju drugom entitetu koji nije na putanji podataka ili da izazove neuspeh procesa otkrivanja. U prvom slučaju može izgledati da je signalizacioni protokol nastavio korektno sa izvršavanjem, izuzev što su pravila uspostavljena u pogrešne *firewall*-e ili da je QoS rezervacija resursa izvršena u pogrešnim NSIS entitetima. Za krajnji host ovo znači grešku u protokolu iz nepoznatih razloga.

Napadač bi mogao da iskoristi NSIS poruke da **preslika topologiju mreže**, dok u nekim organizacijama ili preduzećima postoji želja da se ne otkriva interna struktura mreže. Poruke za otkrivanje, praćenje rute, dijagnostičke poruke i upiti mogu pomoći napadaču kao dodatak u beleženju putanje i objekata na njoj. S druge strane, potreba da se ne otkrije topologija mreže može biti u konfliktu sa drugim zahtevima da se obezbedi automatsko otkrivanje NSIS-svesnih čvorova ili omogući upotreba dijagnostičkih sredstava.

IV. MOGUĆA REŠENJA ZAŠTITE NSIS PROTOKOLA

Kako je NSIS protokol podeljen u dva sloja, predložena bezbednosna rešenja moraju da ponude zaštitu za NTLP i postojeće NSLP-ove. Na osnovu prethodne analize, sledeća pitanja su od vitalnog značaja za zaštitu NSIS protokola [4]: (1) Mogućnost vršenja autentifikacije i razmene ključeva između susednih NSIS parnjaka; (2) Uspostavljanje zaštitne asocijacije da bi se obezbedio integritet, poverljivost i zaštita od ponavljanja za signalizacione poruke koje se razmenjuju između susednih parnjaka; (3) Zaštita od DoS-a; (4) Osnovna zaštita za mehanizme otkrivanja; (5) Autorizacija NTLP signalizacionih čvorova; (6) Fleksibilna autorizacija na NSLP sloju uključujući i rad sa postojećom AAA infrastrukturom.

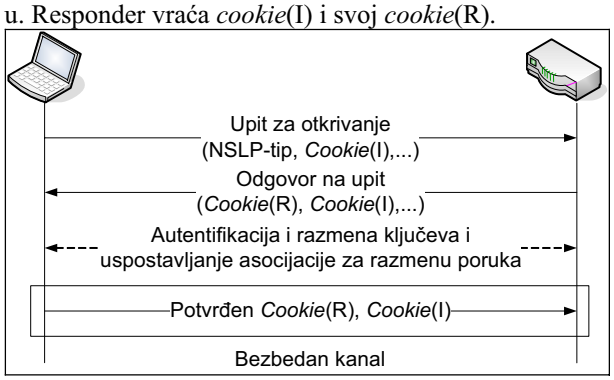
Značajna količina prisluškivanja, ponavljanja i *man-in-the-middle* napada mogu biti rešeni **efikasnom autentifikacijom i protokolom razmene ključeva na NTLP sloju**. Često je ovo operacija sa visokim troškovima i da bi se izbegla skupa kriptografska obrada (npr. za obradu digitalnih potpisa) za svaki pojedinačni objekat, poruka ili signalizaciona sesija bi trebalo da koriste uspostavljenu zaštitnu asocijaciju između

NTLP parnjaka. Kao posledicu, veliku količinu obrade možemo smanjiti korišćenjem brže simetrične kriptografske zaštite više signalizacionih sesija. Ovo je moguće podržati na NTLP sloju i razmatra se nekoliko pristupa ovom problemu.

Jedan pristup se zasniva na **TLS** (*Transport Layer Security*) koji omogućava fleksibilnu autentifikaciju i okvir za protokol razmene ključeva (*TLS Handshake Layer*) i obezbeđuje zaštitu za naknadno razmenjene aplikacione podatke preko *TLS Record Layer*-a . Drugi pristup je primena varijanti **IKE** (*Internet Key Exchange protocol*) da bi se podržala uspostava IPsec zaštitne asocijacije, kada je IPsec izabran za zaštitu signalizacionih poruka između susednih parnjaka.

Razmena poruka za otkrivanje je bezbednosno osetljiv proces i vrlo ga je tesko zaštiti potrebno je obezbediti **zaštitu za mehanizme otkrivanja**, gde se može primeniti mehanizam baziran na kratkim porukama (*cookies*).

Cookie(I) se nalazi u okviru upita za otkrivanje (Sl. 3) da bi sprečio da napadač izvede plavljenje besmislenim odgovorima čvora koji je generisao upit. Kako je *cookie*(I) slučajno izabrana vrednost, napadač ne može da proračuna valjan odziv. Čvor koji odgovara kreira *cookie*(R) koji se koristi za sprečavanje DoS napada, na isti način kao što ga koriste drugi protokoli (npr. IKE). Čvor koji generiše odziv ne sme da kreira stanje po sesiji sa odgovorom na upit za otkrivanje, jer će, u suprotnom, otvoriti put ka slabostima prema DoS-u. Responder vraća *cookie*(I) i svoj *cookie*(R).



Sl. 3 Osnovna zaštita za mehanizme otkrivanje

Na kraju, kada inicijator primi odgovor na poruku za otkrivanje, upoređuje vrednost *cookie*-ja(I) i pokreće autentifikaciju i protokol razmene ključeva sa otkrivenim čvorom pre nego što počne uspostavljanje asocijacije za slanje poruka. Da bi se sprečilo da napadač menja odgovor na poruku za otkrivanje i dodaje pogrešne podatke o sledećem NSIS čvoru na putanji, *cookie*(R) se ponavlja kada je uspostavljena zaštita kanala. Ovo omogućava čvoru koji generiše odziv da proveri da li je on stvarno učestvovao u razmeni poruka za otkrivanje.

Cilj donošenja **odluke o autorizaciji na NTLP sloju** je da se osigura da samo legitimni NSIS čvorovi iniciraju komunikaciju signalizacijom. GIST entitetu može biti teško da donese smislenu odluku bez konsultacije sa NSLP-om sa osvrtom na specifičnu funkcionalnost signalizacione aplikacije. U nekim postavkama je moguće da NTLP sloj vrši osnovnu kontrolu pristupa i da dozvoli samo pojedinim čvorovima iz određenog domena da uspostave asocijaciju. Odluke o autorizaciji na NTLP sloju naročito su korisna na unutardomenskim scenarijima, kao i u okruženjima korporativnih mreža gde su parnjaci koji komuniciraju unapred konfigurisani.

Aspekti autorizacije zahtevaju posebnu pažnju i neophodno je da se omogući **fleksibilna autorizacija na NSLP sloju**. Rad sa NAT/*Firewall*-om i QoS NSLP-om pokazao je probleme koji nastaju pri autorizaciji u osnovnom obliku za sve NSLP-ove tako da će se postupci pri autorizaciji razlikovati za svaki NSLP.

Odluka o uspešnom autorizovanju QoS rezervacije može biti u vezi sa mogućnošću korisnika da plati željenu uslugu. Donošenje odluke o autorizaciji da bi se stvorila NAT veza, verovatno će zavisiti od smera saobraćaja. Za kreiranje paketskih filtera u *firewall*-u, bezbednosna pravila administrativnog domena (npr. korporativna mreža, akademska mreža, 3G mreža) će igrati značajnu ulogu. NSIS ruter neće biti u mogućnosti da sam donese odluku o autorizaciji bez konsultacije sa trećom stranom, na primer AAA infrastrukturom kojoj će potencijalno prepustiti odluku o autorizaciji.

V ZAKLJUČAK

Dizajn IETF NSIS protokola karakteriše: razdvajanje transportnih signalizacionih poruka od signalizacionih poruka aplikacija, razdvajanje otkrivanja i transporta signalizacionih poruka, uvođenje identifikatora sesije kao i podrške ka hostovima, mrežama i proksijima.

Posebna pažnja u ovom radu posvećena je mogućim napadima na NSIS signalizacioni protokol. Napadi su klasifikovani na one koji pogađaju sve signalizacione protokole i na one koji su specifični za NSIS protokol. Sagledana su moguća rešenja nekih od problema: efikasnom autorizacijom i razmenom ključeva na NTLP sloju, uvođenjem zaštite na NTLP sloju kao i fleksibilna autorizacija na NSLP sloju. Brojni problemi zaštite NSIS protokola su i dalje otvoreni, a naročito korišćenje u mobilnom okruženju zahteva dalje proučavanje i istraživanje zbog ograničenja u performansama i potrebe za optimizacijom.

LITERATURA

[1] X. Fu et al., "NSIS: A New Extensible IP Signaling Protocol Suite", *IEEE Comm. Magazine*, vol. 43, no. 10, October 2005, pp. 133-141

[2] H. Tschofenig, D. Kroeselberg, „Security Threats for Next Steps in Signaling (NSIS)“, RFC 4081, IETF, June 2005.

[3] D. Paunović, „Zaštita NSIS protokola u telekomunikacionim mrežama baziranim na internet tehnologiji“, diplomski rad, Elektrotehnički fakultet, Beograd, 2007.

[4] H. Tschofenig, X. Fu: „Securing the Next Steps in Signaling (NSIS) Protocol Suite“, *Int. Journal of Internet Protocol Technology*, Vol. 1, No. 4, 1 August 2006, pp. 271-282.

ABSTRACT

This paper considers the security threats for Next Steps in Signaling (NSIS) protocol suite, which consists of two layers (transport and signaling), each demanding different types of security. Security flaws and ways for attacker to use them are analyzed, as well as security options for weak protocol points.

SECURING NSIS PROTOCOLS IN IP-BASED NETWORKS

D. Paunović