SIGURNOST SIP PROTOKOLA
SIP PROTOCOL SECURITY

Adis Medić, InfoSys d.o.o.
Kolodvorska bb, Bosanska Krupa, Bosna i Hercegovina
+387-37-476-505; adismedic@hotmail.com
Adis Golubović, Golubovići br. 88, Velika Kladuša, Bosna i Hercegovina
+387-61-239-535; golub_a@hotmail.com

Sažetak: *U posljednje vrijeme dolazi do ubrzanog razvoja računarskih i komunikacijskih tehnologija, a samim tim dolazi i do razvoja IP telefonije. Stručnjaci u području telekomunikacija su predvidjeli da će ovaj vid komunikacije biti prijetnja klasičnom načinu komuniciranja, pod prijetnjom mislimo na samu kvalitetu zvuka, manje cijene komuniciranja, kao i po velikom broju drugih mogućnosti koje pruža ovakav vid komunikacije. Većina današnjih VoIP telefona podržava SIP protokol. Osim operatora na tržištu se pojavilo mnoštvo sistem integratora koji nude svoja rješenja za PBX (Private Branch Exchange) sisteme, koja su u većini slučajeva bazirana na Asterisk platformi kao što je FreePBX, te većina njih po osnovnim postavkama nemaju uključene sigurnosne postavke, te taj zadatak pada na administratore da spriječe eventualne neželjene posljedice. U ovome radu ćemo se pozabaviti sa mogućim napadima koji se dešavaju kod SIP protokola na njegovom signalnom i transportnom nivou kao i rješenjima za sprječavanje takvih napada.*

Abstract: *Lately comes to the rapid development of computer and communication technologies and therefore also comes to the IP telephony development. Telecomunication expertshave predicted that this form of communication will be a direct threat to the classical way of communication. Threat is considered in a way of sound quality, lower price for communication, as well as many other features that provide this kind of communication. SIP protocol is supported by most of today's VoIP phones. In addition to the operator on the market appeared a multitude of system integrators which offer their solutions for PBX (Private Branch Exchange) systems, which are int he most cases based on the Asterisk platform as FreePBX and most of them do not have the basic settings, security settings and the administrators have to prevent any unwanted conquesences. In this paper authors will deal with possible attacks that could occur in the SIP protocol on its signal and the transport level and solutions for preventing such situations.*

1. UVOD

U današnje vrijeme skoro 90% poziva izvršava se preko stare PSTN (*Public Switched Telephoned Network*) tehnologije koja posjeduje osnovnu karekteristiku da jedan poziv rezervira vezu između dva korisnika i da tu vezu više nitko ne može koristiti i kada se linija prekine veza se oslobodi za druge korisnike [1]. Kod prijenosa zvuka preko internet protokola nemamo problema sa ograničenjem broja korisnika koji koriste istu liniju za razgovor, ali u svakom slučaju imamo veći problema sa sigurnošću prometa nego kod klasične telefonije, o kojem će biti riječi nešto kasnije. SIP protokol je u zadnjih nekoliko godina privukao dosta pažnje, te je prihvaćen kao signalizacijski protokol za pružanje multimedijskih usluga u 3G sistemima [2]. SIP je jedan od predvodnika revolucije u internet tehnologiji. Kada govorima o SIP protokolu i njegovoj implementaciji, ona je vrlo jednostavna. Temelji se na dobro razrađenom HTTP (*HyperText Transfer Protocol*) protokolu, te slično njemu posjeduje tekstualnu reprezentaciju poruka. Ova činjenica ga čini vrlo jednostavnim za otklanjanje pogrešaka kao i za analizu ispravnosti rada kod njegovog razvoja. Zbog njegovih karakteristika kao što su jednostavna implementacija i jednostavno otklanjanje pogreški, SIP protokol čine vrlo ranijim prilikom sigurnosnih napada. Ovaj rad ima za cilj da obradi sljedeće cjeline:

- izvrši pregled opasnosti po sigurnost, karakterističnih za VoIP (*Voice over Internet Protocol*), SIP protokol, SIP protokol na signalnom nivou te SIP protokol na transportnom nivou,
- definirat ćemo osnovne obrambene mehanizme kod navedenih sigurnosnih napada i
- predložiti praktične preporuke za sigurnu realizaciju. [3]

2. KATEGORIZACIJA NAPADA

Napade koji se dešavaju na VoIP sistem možemo podijeliti u nekoliko skupina, koje ovise o korištenim sredstvima kao i o očekivanim napadima. Prema postavljenim kriterijima imamo nekoliko vrsta napada kao što su: DoS *(Denial of Service)* napadi, prisluškivanje, krađa poziva i dr. Sve ove napade objasnit ćemo u sljedećim poglavljima rada.

2.1. DoS i DDoS napadi

Napadi koji su vezani za uskraćivanje servisa (eng. *Denial of Service – DoS*) zasnovani su na okupiranju računarskih mreža s nepotrebnim podacima ili na rušenju pojedinih komponenti mreže [4]. Ovi napadi predstavljaju pokušaj da se ozbiljno naruši ili potpuno uništi operativnost sistema. DoS napadi se više javljaju i mnogo lakše ih je primijeniti kod VoIP okruženja nego kod klasični PSTN sistema. Posebna vrsta ovih napada su DDoS *(Distributed Denial-of-serice)* napadi. DDoS napadi su napadi koji se javljaju sa više lokacija a usmjereni su prema jednom serveru ili lokaciji sve u cilju da bi se narušila operativnost sistema [4]. Također ovaj napad djeluje na prekidanje usluge ili na samu kvalitetu usluge QoS (Quality of Service) koju pruža određeni servis

2.2. Prisluškivanje

Kao što i sam pojam kaže, prisluškivanje predstavlja presretanje i čitanje poruka, zvukova i drugih podataka. Kada govorimo o ovome napadu u VoIP okruženju prvenstveno se misli na prisluškivanje poziva tj. na same razgovore između korisnika. Svrha ovakvih napada ogleda se u otkrivanju povjerljiv informacija kao što je: otkrivanje broja računa, PIN koda, faks poruke, poslovne informacije itd.

2.3. Man in the Middle

Ovu vrstu napada karakterizira ubacivanje napadača u komunikacijski kanal u svrhu prikupljanja povjerljivih komunikacijskih paketa. Kada se komunikacijski paketi prikupe, vrši se ponovno slanje prvobitnom primaocu ali sa izmijenjenim sadržajem poruke. Ova vrsta napada se koristi kao posredna metoda pri drugim napadima. Kao protumjere za ovakve napade potrebno je zaštititi fizičke pristupe mreži te implementirati enkripciju s nekom od raspoloživih metoda.[4]

2.4. Krađa poziva

Kao i u klasičnoj vrsti telefonije, ovaj napad se definira kao preuzimanje uloge jednog subjekta u pozivu. Krađom poziva napadač može doći do informacija potrebnih za stjecanje kontrole nad tuđim IP telefonom, te preusmjeriti promet na drugu lokaciju. Zamislimo da legalni korisnik nije svjestan napada, tada može doći do otkrivanja jako povjerljivih informacija a da legitimni korisnik nije ni svjestan. VoIP pozivi se mogu na jednostavan način skupljati i dekodirati ukoliko napadač ima fizički pristup lokalnoj računalnoj mreži preko koje VoIP paketi putuju.[4]

2.5. Spoofing poziva

Spoofing poziva je vrlo sličan napadu krađa poziva. Ova vrsta napada se ogleda u lažnom predstavljanju koristeći posebne metode za izmjenu komunikacijskih paketa. U 2009 godini je otkriveno oko 60 sigurnosnih propusta u VoIP produktima, je u 2006 taj broj iznosio 20[5]. Dakle, spoofing podrazumijeva kreiranje lažne ili krivotvorene verzije nečega, poput web lokacije ili adrese elektroničke pošte. Korisnik se prijavljuje sa svojim korisničkim imenom i lozinkom koje tako dolaze u ruke kriminalaca, a oni ih zlorabe za pristup stvarnoj web lokaciji, posebice opasno za korisnike usluga e-bankarstva.[6]

2.6. SPIT

Iako se nekima čini da je zatrpavanje IP telefona neželjenim SPAM porukama i informacijama samo neugodna nuspojava konekcije na Internet, većina korisnika gubi korisno vrijeme na čišćenje telefona od istih te tijekom tog vremena nisu u mogućnosti ispunjavati svoje poslovne zadatke [4]. SPIT skraćenica nastala je od fraze „*Spam over Internet Telephony*“ i označava širenje neželjenih poruka (odnosno poziva) putem telefonskog sistema. Najčešće se koristi za masivni marketing. Postoje naravno i druge taksonomije VoIP sigurnosti, ali svaka dodatna podjela redovito je sastavnica navedenih tehnika.

3. OPĆENITE PREPORUKE ZA PODIZANJE SIGURNOSTI VoIP MREŽA

U svrhu zaštite VoIP mreže potrebno je konstantno raditi na sigurnosti. Napadi neprestano evoluiraju i administratori mreže moraju štiti, kako mrežu u globalu, tako i pojedine usluge što je i VoIP [4]. Neke od preporuka za podizanje VoIP sigurnosti mogu biti odvajanje IP adresa, pokretanje virtualnih lokalnih mreža, podizanje mrežnih barijera te šifriranje [7]. U nastavku ovog poglavlja navedeni su uobičajeni načini zaštite kojima se minimaliziraju sigurnosni rizici i prijetnje unutar VoIP mreža.

3.1. Fizička sigurnost

Promatrano s aspekta fizičke sigurnosti i konfiguriranja samih VoIP aplikacija preporučaju se sljedeće metode [4]:

- sve kritične elemente VoIP sistema trebalo bi locirati u zaštićene i sigurne lokacije odvojene od neovlaštenog pristupa,
- potrebno je izvršiti konfiguraciju VoIP telefona tako da ne prikazuju svoje mrežne konfiguracijske informacije,
- trebalo bi izbjegavati soft-phone sisteme.

3.2. Odvajanje IP adresa

Razdvajanje adresnih domena je preduvjet za primjenu daljih mjera zaštite [8]. Svaku VoIP komponentu bi trebalo postaviti na odvojene privatne mreže, koje nisu djeljive s ostalim mrežama. Da bi to bilo funkcionalno potrebno je koristiti privatne IP adrese (10.0.0.0/8, 172.16.0.0/16 i 192.168.0.0/16) za daljnje odvajanje IP telefonije od podatkovnih mreža [4]. Ako bi došlo do potrebe konekcije između ostalih podatkovnih mreža i VoIP sistema a što je u većini slučajeva, potrebno je samo

izvršiti implementaciju NAT-a. Implementacija NAT-a *(Network Address Translation)* se odvija na ključnim tačkama VoIP mreže.

3.3. Virtualni LAN

Preporuča se odvajanje VoIP-a od ostalih podatkovnih mreža korištenjem virtualnih lokalnih mreža (eng. *Virtual Local Area Networks - VLAN*) [4]. Ideja je da se izvrši logičko grupiranje korisnika, bez obzira na njihove fizičke lokacije u manje logičke cjeline, odnosno da se unutar jednog fizičkog LAN-a kreira više manjih virtulanih LAN mreža, zadržavajući svaka osobinu klasičnih LAN mreža. Grupiranje se može izvršiti na više kriterija. Npr. na osnovu MAC adresa, IP adresa, portova, itd.

3.4. Firewall

Firewall je sigurnosni internet gateway koji se koristi za sigurnosno povezivanje privatne mreže i interneta [9]. Svoju osnovnu zadaću firewall obavlja pomoću sigurnosnih pravila koja definiraju koji je promet dopušten, a koji zabranjen u skladu sa sigurnosnim pravilima neke organizacije [4]**.** Da bi se izvršilo filtriranje prometa između VoIP mreža i podatkovnih mreža najbolje je koristiti firewall. Međutim kao i svaki sistem i firewall ima svojih nedostataka. Nedostaci firewall-a se ugledaju u sljedećem: nakon definiranih pravila za filtriranjem prometa više se ne mijenjaju ili se moraju mijenjati ručno, zbog velikog broja otvorenih portova kod VoIP sistema (od 10024 do 65535) potrebno je koristiti firewall-e koji podržavaju SIP i H.323 protokole.

3.5. Enkripcija

Gdje god je moguće i gdje je izvedivo trebala bi se implementirati enkripcija VoIP prometa korištenjem VPN-ova (eng. *Virtual Private Networks*) ili bilo kojom metodom trenutno dostupnom [4]. Virtualne privatne mreže omogućavaju enkripcijske tunele te na taj način je omogućeno sigurno spajanje dvije fizički odvojene mreže.

Prilikom udaljenog spajanja na VoIP sisteme savjetuje se korištenje IPsec ili SSH *(Secure Shell)* protokola. Također se preporučuje korištenje IPsec tuneliranja umjesto IPsec transporta zbog toga što se tuneliranjem maskira odredišna i izvorišna IP adresa.

4. NAPADI NA RAZINI SIGNALNOG PROTOKOLA

Postoji više napada na razini signalnog protokola. Međutim mi ćemo u ovom radu kratko objasniti neke od najvažniji. Napadi na razini signalnog protokola su sljedeći:

a) **SIP bombing** – Ovaj napad karekteriše slanje velike količine lažnih SIP poruka prema ciljnom SIP sistemu [10]. Rezultat napada u najboljem slučaju je samo smanjeni kapacitet, dok u većini slučajeva napada na krajnje uređaje (telefone), napad rezultira potpunim prestankom rada (freeze) i potreban je restart uređaja.

b) **Prekid poziva** – U ovom slučaju mogu se desiti dvije zlonamjerne radnje [10]. U prvom slučaju „SIP Cancel“ poruka, koristi se kako bi se prekinulo uspostavljanje poziva. Napad se dešava u trenutku uspostave poziva. Ovisno o načinu primjene može se koristiti za onemogućavanje primanja ili uspostavljanja poziva na točno određenom segmentu VoIP mreže. Druga vrsta napada je poruka „SIP bye“ napadač prekida postojeći poziv, postižući isti efekt.

c) SIP bazirani „Man in the Middle“ napadi - Primjenom metode MITM moguće je ostvariti dvije vrste napada. Prva vrsta sastoji se od klasičnoga MITM napada, ubacivanjem u komunikacijski kanal (bilo u svrhu prisluškivanja ili promjena komunikacije), dok se druga sastoji od korištenja MITM metoda za „krađu“ poziva , pri čemu se poziv preusmjerava na napadača.[10]

4.1. NAČINI ZAŠTITE NA RAZINI SIGNALNOG PROTOKOLA

Svi napadi koji spadaju u skupinu napada baziranih na iskorištavanju karakteristika signalnog protokola, baziraju se na modifikaciji SIP headera. Osnovni način na koji SIP headeri bivaju poslani kroz mrežu je plain text, što znači da bilo tko sa mogućnošću prisluškivanja i modifikacije prometa na mreži je potencijalni napadač, kao i naravno da je razina sigurnosti u takvoj mreži daleko ispod „best practice“ minimuma. Best practice u ovome slučaju sastoji se od snažne enkripcije i mehanizama autentifikacije [10]. Postoji nekoliko načina zaštiti na razini signalnog protokola.

a) TLS zaštita SIP signalnih poruka - Korištenje TLS (*Transport Layer Security*) zaštite uvelike povećava sigurnost SIP baziranih VoIP mreža, te efektivno onemogućuje napade bazirane na promjeni SIP kontrolnih poruka.[10] TLS zaštićena SIP komunikacija štiti od gubitka integriteta, tajnosti, te reproduciranja SIP headera korištenjem sigurnih ključeva i dvostrane idetifikacije. Budući da se za primjenu TLS-a koristi isključivo TCP (*Transmission Control Protocol*) protokol, nemoguća je primjena SIP TLS zaštite na UDP (*User Datagram Protocol*) baziranim SIP mrežama.

b) **Korištneje IPSec tunela** - Druga popularna metoda zaštite SIP prometa u VoIP mrežama je „gradnja“ virtualne mreže koja se sastoji samo od sigurnosno verificiranih elemenata, kroz primjenu IPsec sustava. [10] IPSec predstavlja vid zaštitnog kodiranja i mada naširoko implementiran u sistemima za prijenos podataka, u VoIP-u je primenljiv samo pod određenim uvjetima [8]. Prednost ove metode je što se u VPN može „zatvoriti“ cjelokupan VOIP promet (voice+signaling), te je neovisan o transportnom mehanizmu (TCP ili UDP). Najčešće korišteni protokol izmjene ključeva u VoIP IPsec mrežama je Internet Key Exchange (IKE).

5. NAPADI NA RAZINI TRANSPORTNOG PROTOKOLA

Napadi na razini transportnog protokola odnose se na napade na VoIP mreže napadajući protokole za transport glasa (RTP/RTCP) *Real-time Transport Protocol/ Real Time Transport Control Protocol*. Prilikom napada pretpostavlja se da su isti nezaštićeni enkripcijom. Logički ih dijelimo u nekoliko skupina:

Prisluškivanje - bazira se na činjenici da se glas prenosi putem transportnog protokola u jednom od standardnih enkodinga/kompresije (ulaw,alaw,gsm, itd), te da ga je jednostavno prikupiti iz same mreže i podataka u signalnom headeru.

a) **Napadi bazirani na ubacivanju RTP sistem** - ovi napadi baziraju se na ubacivanju lažnih RTP paketa u postojeći RTP stream. Rezultat je, redovito, izbacivanje napadnutog korisnika iz razgovora. Radi nastale kolizije paketa sa istim SSRC identifikatorom. Umjesto čistog kopiranja SSRC-a (odnosno paketa), napadač može kreirati pakete sa istim SSRC identifikatorom, ali i višom vrijednosti brojača paketa ili vremena. Na taj način izvodi se napad sa ubacivanjem zvuka u govorni kanal.

5.1. Načini zaštite na razini transportnog protokola

Slično kao i napadi na razini SIP protokola, napadi na razini transportnog protokola (RTP/RTCP) napadi baziraju se na modifikaciji paketa i ubacivanju u postojeći stream. Sam protokol nema zaštitu od takvih napada. Budući da je kod ovakvih vrsta napada, vrijeme napada slabije definirano (kod SIP napada bitno je napasti u točnom trenutku uspostave poziva), npr. kada je već razgovor u tijeku, on može trajati i do nekih 15 minuta, a budući da napadamo RTP stream, imamo punih 15 minuta da ubacimo svoje pakete. Slično kao i kod SIP napada, obrana je zasnovana na enkripciji protokola i digitalnig potpisa.

U tu svrhu razvijen je SRTP protokol, koji u svojem portfoliu sadrži tajnost podataka, autentifikaciju poruka kao i zaštita od ponovnog slanja poruka za RTP i RCTP promet. SRTP protokol standardiziran je od strane IETF-a, te publiciran kao RFC3711.

6. ZAKLJUČAK

Prijenos govora preko interneta postala je sasvim normalna stvar. Velika razlika u karakteristikama je između govornog saobraćaja i saobraćaja prijenosa podataka. Kada govorimo o sigurnom načinu implementacije VoIP sistema u organizacijama ona je svakako moguća ali nije jednostavna. Svakako će svaka organizacija biti izložena pokazanim napadima a ujedno i svim onim sigurnosnim napadima koji se dešavaju i na podatkovnu mreže. Priliko sigurnog načina implementacije VoIP sistema treba imati više stvari u vidu, kao što su: kompatibilnosti, skalabilnosti, upravljivosti, interoperabilnosti, troškova i slično.

7. REFERENCE

[1] J.Šaban, „Mreže računala – SIP protokol“, Zavod za elektroniku, mikroelektroniku i inteligentne sustave, Fakultet elektrotehnike i računarstvam, Sveučelište u Zagrebu, Zagreb 2003, dostupno na: http://www.zemris.fer.hr/predmeti/mr/arhiva/2002-2003/seminari/finished/pdf/sip.pdf

[2] N.Biondić, M.Vukušić-Vasiljevski, L.Medak, V.Bolt, V.Vrlika, „Protokol za pokretanje sesije (3-34)“, Ericsson Nikola Tesla, REVIJA 18(2005) 1, dostupno na: http://www.ericsson.com/hr/etk/revija/Br_1_2005/protokol_za_pokretanje_sesije.pdf

[3] D.Miljanović, „Sigurnost VoIP-a (opasnosti, mjere i rješenja)“, 14.Telekomunikacioni forum TELEFOR Srbija, Beograd, novembar 21.-23.2006.godine, dostupno na: http://www.telfor.rs/telfor2006/Radovi/02_TM_07.pdf

[4]Sigurnosni aspekti VoIP tehnologije, dostupno na: http://datapodium.com/dokumenti/uploads/mreze/Sigurnosni_aspekti_VoIP_tehnologije.pdf

[5]Ranjivosti VoIP sistema, dostupno na: http://hacklab01.org/vijesti/41-vijesti/84-voip-ranjivosti-u-porastu.html

[6]Zaštita od krađe identiteta, dostupno na: http://www.javno.com/hr-profit/kako-se-mozete-zastititi-od-kradje-identiteta_131778

[7] D. Pleskonjić, N. Maček, M. Carić, „Sigurnost računarskih mreža“ 2005-2009.godine, dostupno na: http://www.conwex.info/draganp/SRM_Predavanje_8.pdf

[8] S. Valjarević, Z. Petrović, „Metode zaštite u VoIP sistemima“, XII Telekomunikacioni forum TELEFOR Srbija, Beograd, novembar 23.-25.2004. godine, dostupno na: http://www.telfor.rs/telfor2004/radovi/TM-2-9.PDF

[9] D. W. Chadwick „Network Firewall Technologies“ IS Institute, University of Salford, Salford, M5 4WT, England, dostupno na: http://www.itsec.gov.cn/docs/20090507145737126918.pdf

[10] M.Amarandei-Stavila, „Voice over IP security a layered approach“, Xmco Partners, dostupno na: http://www.xmcopartners.com/whitepapers/voip-security-layered-approach.pdf