HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosni aspekti VoIP tehnologije

CCERT-PUBDOC-2006-03-151

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

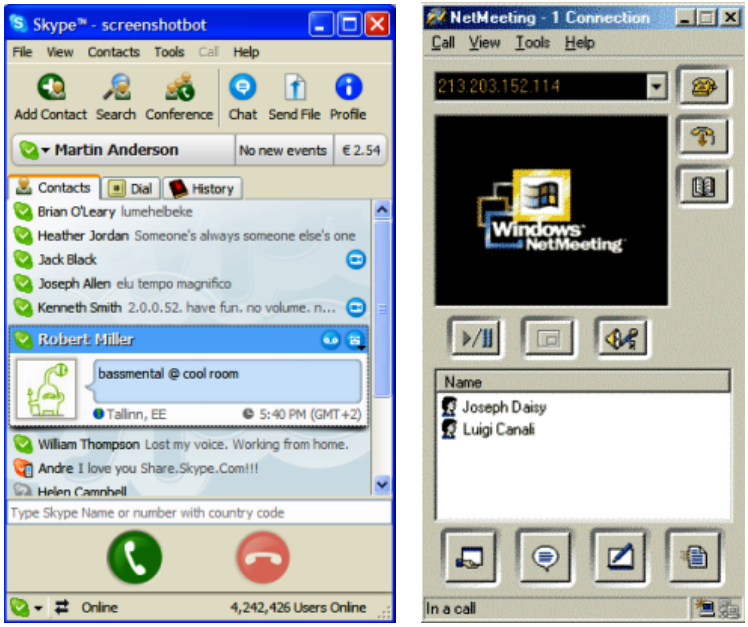
CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

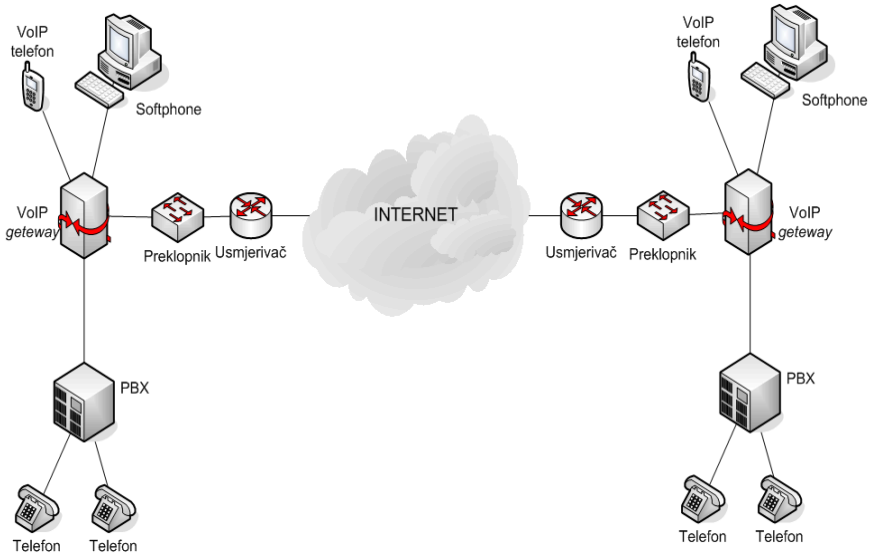
VoIP (eng. *Voice over Internet Protocol*) je proces digitaliziranja i slanja glasovnih podataka preko Interneta i drugih podatkovnih mreža. Korištenjem VoIP tehnologije, organizacije više ne moraju koristiti samo tradicionalnu telefonsku mrežu, što rezultira smanjivanjem troškova telefoniranja i većom fleksibilnosti rada. Nažalost, kao i sve nove tehnologije tako i uvođenje VoIP donosi nove sigurnosne rizike i sigurnosne ranjivosti u postojeće mreže.
Ovaj dokument opisuje osnove rada VoIP tehnologije, VoIP komponente i najčešće korištene protokole za VoIP komunikaciju. Također, opisani su sigurnosni zahtjevi koji su postavljeni pred VoIP, moguće prijetnje za VoIP mreže te preporuke za povećavanje sigurnosti VoIP mreža.



Slika 1: Primjeri najčešćih VoIP aplikacija: Skype i Microsoft NetMeeting

2. VoIP tehnologija

IP telefonija je proces prijenosa glasa preko paketno preklapanih IP mreža nasuprot prijenosu zasnovanom na javnim telefonskim mrežama. Digitaliziranje zvuka u mrežne pakete te njihov prijenos preko Interneta i drugih podatkovnih mreža (intranet i sl.) naziva se VoIP protokolom.
VoIP omogućava obavljanje telefonskog razgovora upotrebom postojećih mrežnih konekcija te predstavlja zamjenu za standardnu telefoniju, kako u lokalnom i međugradskom prometu, tako i u međunarodnom. Velika prednost VoIP tehnologije je i mogućnost pozivanja mobilnih i fiksnih pretplatnika te ostvarivanje međunarodnih poziva po izuzetno povoljnim cijenama. Na slici Slika 2 vidljiva je tipična VoIP arhitektura.



Slika 2: Tipična VoIP arhitektura

Svojom implementacijom VoIP uvodi uz brojne pogodnosti i brojne sigurnosne izazove za mrežne administratore. Nažalost, mnogi od alata koji se koriste za sigurnost računalnih mreža, prvenstveno vatrozidi (eng. *firewalls*), NAT (eng. *Network Adress Translation*) te razne vrste enkripcija ne rade na ispravan način u VoIP mrežama.
VoIP mreže imaju veliku raznovrsnost oblika i formi. Danas je skoro svako računalo sposobno za korištenje VoIP tehnologije. Windows operacijski sustavi posjeduju NetMeeting i Windows Messenger programe koji dolaze kao dio osnovne instalacije, dok za Linux platforme prostoje brojne VoIP aplikacije.

2.1. VoIP komponente

Iako imaju različitu tehnologiju i pristup pružanju prijenosa glasovnih usluga, neke od komponenti koje čine javnu telefonsku mrežu (eng. *Public Switched Telephone Network - PTSN*) ujedno su i dio VoIP mreža. VoIP mreže moraju omogućavati sve funkcionalnosti koje omogućavaju i javne telefonske mreže s dodatkom pružanja usluga prijenosa podataka i signala na postojeću javnu mrežu. U VoIP okolinama uvijek se mogu naći četiri glavne komponente i to su:

- MREŽNA INFRASTRUKTURA - podržava VoIP tehnologiju i može se gledati kao jedna logička glasovna mreža distribuirana preko IP okosnice koja pruža konekciju i prijenos glasovnih paketa preko mreže. Ta IP infrastruktura mora omogućiti prijenos glasovnih paketa bez ikakvih poteškoća.
- PROCESORI (KONTROLERI) POZIVA - moduli potrebni za uspostavljanje i nadziranje poziva, autorizacije korisnika, pružanja osnovnih telefonskih usluga i kontroliranje brzine prijenosa (eng. *bandwidth*) za svaki link.
- PREVODIOCI (eng. *MEDIA/SIGNALING GATEWAYS*) - potrebni su za nastajanje poziva, detekciju poziva, pretvorbu glasa iz analognog u digitalni oblik (stvaranje glasovnih

digitalnih paketa). Ujedno to su komponente koje omogućuju prelazak između različitih tehnologija (npr. prelazak između IP i ISDN tehnologija).

- KORISNIČKI VoIP TERMINALI - Potražnja za VoIP uslugama je uzrokovala široki asortiman korisničkih tzv. "*end-user*" proizvoda kao što su:
  - VoIP terminali– obično ti proizvodi imaju ekstra dodatne mogućnosti koje nadilaze obične telefone. Neki od takvih proizvoda imaju osnovne funkcionalnosti koje pružaju iste mogućnosti kao i konvencionalni telefoni.
  - Konferencijski VoIP terminali – pružaju istu vrstu usluge kao i obični konferencijski telefoni, ali pošto se komunikacija provodi preko Interneta korisniku je dozvoljeno koordiniranje tradicionalnih podatkovnih usluga (npr. što se prikazuje na monitorima na oba kraja razgovora).
  - Mobilni VoIP terminali – bežične VoIP jedinice postaju sve više i više popularne, pogotovo što organizacije već imaju ugrađene osnovne 802.11Q mrežne komponente. Bežični VoIP predstavlja veliki sigurnosni problem, pogotovo zbog naširoko poznatih nedostataka 802.11Q protokola.
- OSOBNA RAČUNALA tzv. *Soft Phone* sustavi – sa slušalicama, aplikacijom (npr. Skype, Microsoft NetMeeting) i jeftinom konekcijom na Internet, svaki PC ili radna stanica mogu biti iskorišteni kao VoIP komponenta.

3. Protokoli i standardi korišteni za VoIP

Današnji VoIP sustavi koriste jedan od dva najpopularnija protokola za uspostavu poziva, H.323 ili SIP (engl. *Sesion Initation Protocol*). Implementacija protokola za prijenos govora i slike preko IP protokola uvijek se provodi u aplikacijskom sloju referentnog OSI modela.

3.1. H.323 standard

H.323 je skup protokola specificiran od ITU udruge (engl. *International Telecomunication Union*) koji definira multimedijsku komunikaciju preko lokalnih računalnih mreža (engl. *Local Area Network* – LAN) pod pretpostavkom da nema zajamčene kvalitete usluge (engl. *Quality of Service* - QoS).
Svojstva H.323:

- standardna kompresija/dekompresija,
- povezivanje različite opreme,
- neovisnost o mreži,
- neovisnost o opremi i aplikaciji,
- podrška za konferencijsku vezu,
- nadzor mreže i
- podrška za komunikaciju s više krajnjih točaka.

Osnovne H.323 komponente:

- terminal - osnovni element svake H.323 zone. Tipičan predstavnik H.323 terminala je Microsoft-ov *NetMeeting*.
- prevodilac protokola (eng. *gateway*) - komponenta koja omogućava prelazak između različitih tehnologija, tzv. most između H.323 zone i neke druge mreže. (npr. H.323/H.320 *gateway* osigurava prelazak između IP i ISDN tehnologija).
- *gatekeeper* - komponenta koja nadgleda rad svih ostalih komponenti u H.323 zoni (može se poistovjetiti s telefonskom centralom u klasičnoj telefoniji). Njegova je uloga:
  - preslikavanje pozivanih telefonskih brojeva u IP adrese odredišnih VoIP *gateway*-a, tj. pohranjivanje plana numeracije čitave mreže i
  - zaštita mrežnih resursa odnosno kontrola broja uspostavljenih VoIP poziva kroz mrežu (čime se eliminira pojava zagušenja u mreži uslijed prevelikog istovremenog broja VoIP poziva).
- MCU (eng. *Multi-point Control Unit*) - zadužen za kontrolu *multi-point* konferencija (dvije ili više točaka "spojenih" u konferenciju). MCU sadrži *Multi-point* kontroler (MC) koji nadgleda pozive, a po potrebi ima i *Multi-point* procesor (MP) kako bi mogao upravljati medijima (prebacivanje između medija ili neki drugi proces, …).

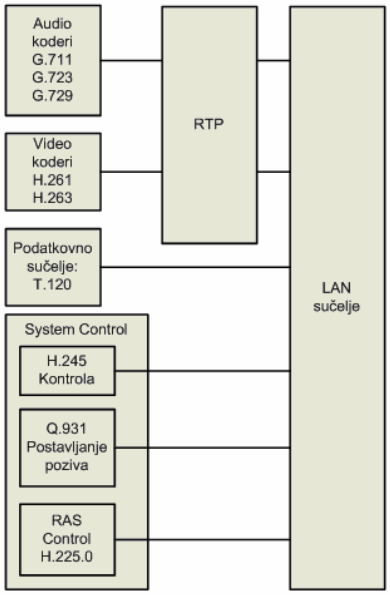
Standard je na ovom području nužan, prije svega radi osiguravanja kompatibilnosti opreme različitih proizvođača, ali i zbog kompleksnosti problema. H.323 kao najkompleksniji ali i najpotpuniji standard za video konferencije obuhvaća široko područje ovog multidisciplinarnog problema.
Kategorije koje standard obrađuje:

- transport govora i slike u realnom vremenu,
- transport tekstualnih poruka,
- kontrola kvalitete veze,
- kompresija govora i slike,
- uspostava veze, autorizacija i registracija te
- definiranje međudjelovanja mreža.

Protokoli koje specificira H.323:

- audio koderi,
- video koderi,
- H.225 *Registration, Admission and Status* (RAS) – regulira prijavu, pristup i status, a koristi se za komunikaciju terminala i H.323 *gatekeeper*-a,
- H.225 *Call Signaling* - obavlja signalizaciju kod uspostave veze kroz kontrolni kanal. Signalizacija ovog tipa odvija se između krajnjih točaka tj. H.323 terminala,
- H.245 *Control Signaling* - poruke po H.245 također se razmjenjuju između krajnjih točaka (otvaranje logičkih kanala, itd…),
- *Real-time Transport Protocol* (RTP) definiran RFC dokumentima RFC1889 i RFC3550 - transportni protokol za prijenos informacija u stvarnom vremenu, a najviše služi za prijenos slike i zvuka. Može se, među ostalim, koristiti i za interaktivne usluge kao što je, npr., Internet telefonija. Svaka informacija koja se šalje ovim protokolom sastoji se od podatkovnog i kontrolnog dijela. Kontrolni dio se sastoji od podataka koji služe za vremensku sinhronizaciju, sigurnost, identifikaciju sadržaja i detekciju gubitaka u prijenosu.
- *Real-time Control Protocol* (RTCP) definiran RFC dokumentom RFC3605 - pruža podršku za konferencije u realnom vremenu za grupe bilo koje veličine. Ova podrška uključuje identifikaciju i autorizaciju sugovornika, podršku za prijenos slike i zvuka, a u najnovijim verzijama i *real-time* prepoznavanje glasa i prevođenje na druge jezike (za sada radi samo za nekoliko najvećih europskih jezika na engleski i zahtijeva jako brzu vezu - minimalno DSL). Također pruža mogućnost stalnog nadgledanja kvalitete usluge voditelju konferencije, a i svim sudionicima (ukoliko imaju dozvolu).

Na slici Slika 3 može se vidjeti kako međusobno funkcioniraju protokoli koji rade zajedno u sklopu H.323 standarda.



Slika 3: Dijelovi H.323 standarda

U literaturi se često griješi nazivajući H.323 protokolom pošto je on zapravo ITU standard koji se poziva na više drugih standarda.

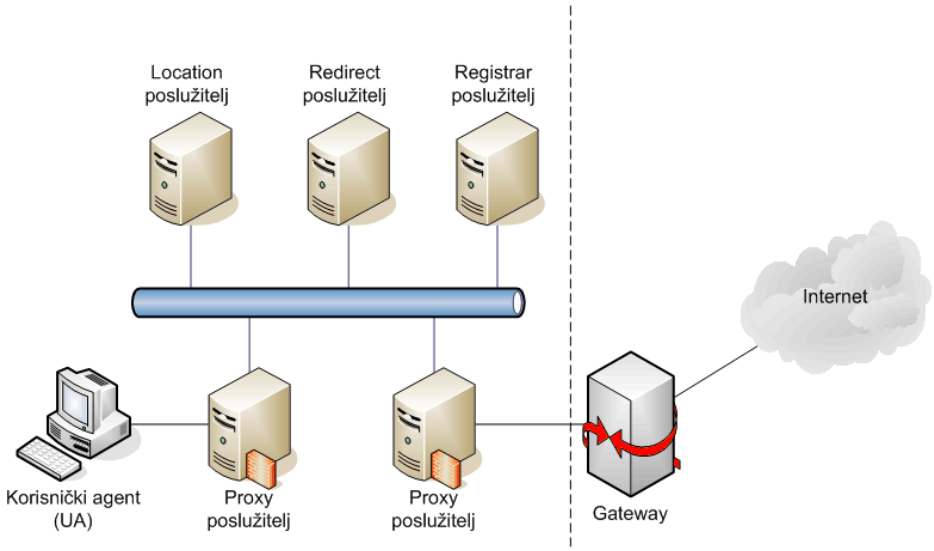
3.2. SIP protokol

SIP (eng. *Session Initation Protocol*) je protokol specificiran od IETF (*Internet Engineering Task Force*) udruge. Namjena mu je uspostava, održavanje, modificiranje i raskid multimedijskih sesija. Sudionici u sesijama mogu biti ljudi ili računalni mehanizmi (računalni poslužitelji koji služe npr. slanju određenog podatka korisniku na koji se on prethodno pretplatio).
SIP poziv koristi se za kreiranje sesije i definiranje njenih parametara. Ovi parametri omogućavaju sudionicima prilagođavanje tipu medija koji se u toj sesiji koristi. Mobilnost korisnika podržana je kroz posredne (eng. *proxy*) i preusmjerivačke (eng. *redirect*) poslužitelje, preusmjeravanjem poziva na trenutnu lokaciju korisnika. Korisnici mogu na jednostavan način registrirati svoje nove lokacije, koje se bilježe na SIP poslužiteljima.
Protokol je koncipiran neovisno o transportnom mediju pa se može jednostavno implementirati na bilo kojoj vrsti mreže. Ipak isključivo se koristi na IP protokolu, a u transportnom sloju može koristiti ravnopravno TCP (eng. *Transmission Control Protocol*) i UDP (eng. *User Datagram Protocol*) protokole premda češće koristi UDP radi njegovih prednosti kod transporta. Nedostatak TCP protokola je to što zahtjeva potvrdu o primitku paketa dok UDP to ne zahtjeva i time omogućava razgovor u stvarnom vremenu.
SIP u svom radu koristi različite protokole:

- RSVP (eng. *Resource reSerVation Protocol*) koji se koristi za rezervaciju mrežnih resursa i pomaže za ostvarivanje određenog nivoa kvalitete usluge
- RTP (eng. *Real Time Protocol*) / RTCP (eng. *Real Time Control Protocol*) / RTSP (*Real Time Streaming Protocol*) – protokoli aplikacijskog nivoa koji služe za slanje podataka u realnom vremenu,
- SAP (eng. *Session Announcement Protocol*) - protokol za objavljivanje multimedijalnih sesija te
- SDP (eng. *Session Description Protocol*) – protokol za opis multimedijalnih sesija.

Implementacija SIP protokola je jednostavna. Temelji se na dobro razrađenom HTTP protokolu te slično njemu posjeduje tekstualnu reprezentaciju poruka. Ova činjenica ga čini jednostavnim za otklanjanje pogrešaka kao i za analizu ispravnosti rada kod razvoja.
Svaki SIP sustav se sastoji od dva osnovna dijela :

- korisnički agent (eng. *User Agent – UA*) – sustav koji radi za korisnika kao kombinacija poslužitelja i klijenta. UA se nalazi u krajnjim točkama i on se uvijek dijeli na dva segmenta:
  - korisnički agent klijent (eng. *User Agent Client – UAC*) - odgovoran za generiranje zahtijeva i
  - korisnički agent poslužitelj (eng. *User Agent Server – UAS*) - zadužen odgovarati na zahtjeve.
- mrežni poslužitelj (SIP poslužitelj) - ovi poslužitelji nisu neophodni za uspostavu veze između dva terminala, međutim oni nude dodatnu funkcionalnost i u stvarnim mrežama se uvijek koriste. Navedeni poslužitelji obuhvaćaju funkcionalnost *gatekeeper*-a koji se koriste u H.323 standardu. Ovakva razdioba poslužiteljskih funkcija na više cjelina nije mana nego prednost SIP standarda. Time je postignuta preglednost i olakšana parcijalna implementacija standarda. Vrste SIP poslužitelja:
  - Posredni (eng. *proxy*) poslužitelj - najvažnija funkcija *proxy* poslužitelja je pronalaženja korisnika i prevođenje adresa. Tijekom svog rada *proxy* poslužitelj može generirati zahtjeve drugim poslužiteljima ili klijentima.
  - Identifikacijski (eng. *registrar*) poslužitelj - prihvaća identifikacijske zahtjeve i najčešće se postavlja skupa s *redirect* ili *proxy* poslužiteljem.
  - Preusmjerivački (eng. *redirect*) poslužitelj - prihvaća zahtjeve i na njih odgovara s 0 ili više mogućih adresa za uspostavljanje veze. Za razliku od *proxy* poslužitelja on ne može poslati zahtjev niti kao korisnički agent klijent uspostaviti vezu.
  - Locirajući (eng. *location*) poslužitelj - služi za pronalaženje trenutne korisnikove lokacije (IP adrese).



Slika 4: Osnovne komponente SIP-a

SIP je, kao i H.323, definiran kroz mrežne komponente i njihovu funkcionalnost. Oba protokola se danas koriste i većina proizvođača u svoju opremu ugrađuje podršku kako za H.323 tako i za SIP. Također se dosta radi i na razvoju međudjelovanja ovih standarda, s idejom omogućavanja komunikacije između dva terminala koji podržavaju samo H.323 ili SIP.

4. Zahtjevi postavljeni pred VoIP tehnologiju

Kako bi se VoIP mogao funkcionalno koristiti u svakodnevnom životu, potrebno je zadovoljiti određene preduvjete. Neki od glavnih zahtjeva koji se stavljaju pred VoIP tehnologiju su:

- KVALITETA USLUGE PRIJENOSA GLASA

Prijenos glasa ima specifične zahtjeve u vezi s kvalitetom prijenosa preko transportne mreže. Iako ne zauzima veliki dio prijenosnog pojasa, prijenos glasa zahtijeva što manje i konstantnije iznose kašnjenja paketa. Osim nepredvidive naravi Interneta, problem mogu predstavljati i zagušenja na pristupnim vezama prema Internetu. Dva su načina prevladavanja ovog problema – povećanje pristupne brzine i implementacija QoS (eng. *Quality of Service*) mehanizama. Prvi način je efikasan, ali i dosta skup, jer bi nakon svakog zagušenja trebalo povećavati pristupnu brzinu, a zagušenja se lako dostižu ako se ne kontrolira pristup prema Internetu. U svakom slučaju, značajno poboljšanje i praktičniji VoIP sustav dobio bi se primjenom stalnih veza na Internet.

Kritični parametri za kvalitetan prijenos glasa su :

- kašnjenje - između krajnjih točaka u jednom smjeru ne bi smjelo biti veće od 100 ms – 200 ms, i
- varijacija kašnjenja - razlike u vremenima kašnjenja pojedinih paketa ne bi smjele biti veće od nekoliko desetaka milisekundi.

Navedeni parametri mogu se provjeriti `ping` naredbom koja daje kružno (dvosmjerno) kašnjenje između krajnjih točaka, a približno kašnjenje u jednom smjeru iznosi polovinu od kružnog kašnjenja.

QoS se može implementirati na rubnim uređajima za pristup Internetu i u idealnim uvjetima bilo bi poželjno da se implementira na svim lokacijama. To može biti vatrozid, usmjerivač ili prevodilac protokola (eng. *gateway*). Kako su usmjerivači u pravilu u vlasništvu davatelja Internet usluga (eng. *Internet service provider - ISP*), na njima najčešće nije moguće implementirati vlastiti QoS. Moguća je implementacija QoS programske aplikacije na *gateway* računalima ili na specijaliziranim profesionalnim uređajima koji se dodaju u mrežu spajanjem na *gateway*. Postoji mogućnost i kupovine vlastitih usmjerivača. Sva navedena rješenja su relativno skupa i složena za implementaciju. Najjednostavnije rješenje je nabavka vatrozida i VPN *gateway* uređaja s podrškom za QoS.

Navedena rješenja mogu dati dobre rezultate, ali ne u potpunosti, jer se ne može potpuno kontrolirati promet na vezi središnje lokacije prema Internetu. Naime, nije moguće izravno utjecati na količinu i ponašanje prometa koji dolazi s Interneta. Ostaje mogućnost korištenja

profesionalnih QoS uređaja, koji su dosta efikasni za TCP promet, ali imaju slabije mogućnosti utjecaja na UDP promet. Također, ostaje problem eventualnih zagušenja na Internetu.
Sama implementacija QoS-a uvelike ovisi o vrsti sklopovske ili programske opreme na kojom se primjenjuje i o aplikacijskim zahtjevima samog korisnika.
Otežavajuća okolnost za implementaciju VoIP-a je smještanje VoIP *gateway* uređaja iza vatrozida i VPN *gateway*-a, jer vatrozid unosi dodatno i relativno nepredvidivo kašnjenje, a VPN osim dodatnog kašnjenja povećava i zauzeće prijenosnog pojasa.

- DINAMIČKI VATROZIDNI NADZOR KOMUNIKACIJE (eng. *Dynamic per-call firewall control*)

VoIP sigurnosna rješenja bi trebala koristiti "više" dinamičkih razina sigurnosti kako bi zaštitili VoIP mreže uključujući:

  - dinamičko otvaranje i zatvaranje vatrozidovih portova prema pozivnoj bazi (eng. *per-call basis*),
  - dijeljenje mreže u više sigurnosnih zona (odvajanje glasovne i podatkovne mreže u zasebne pod-mreže) i
  - traženje mrežne korisničke identifikacije prema pozivnoj bazi.

- DINAMIČKI NADZOR ŠIRINE POJASA LINKA (eng. *Dynamic pe-call bandwidth control*)
  Perfomanse i kvalitete usluge prjenosa glasa su jedni od najvećih problema u uvođenju i implementiranju VoIP tehnologija. VoIP sigurnosna rješenja bi u rješavanju ovih problema trebala imati mogučnost da:
  - dodjeljuju širinu pojasa linka prema pozivnoj osnovi,
  - dodjeljuju širinu pojasa linka prema klasifikaciji poziva,
  - dodjeljuju širinu pojasa linka i usmjeravaju pozive preko višestrukih WAN (eng. *Wide Area Network*) linkova, i
  - istovremeno dodjeljuju širinu pojasa linka za usluge hitnih poziva (eng. *Emergency calls*).
- NAT PREVOĐENJE (eng. *NAT traversal*)
  Korištenje NAT tehnologije između privatnih i javnih adresa može uzrokovati konfiguracijske probleme za uspostavljanje VoIP poziva. Stoga je potrebno koristiti takva rješenja za NAT koja podržavaju VoIP protokole te dopuštaju prolazak kriptiranih signala.
- KOMPATIBILNOST PREMA SIGNALNIM PROTOKOLIMA
  VoIP sigurnosna rješenja bi trebala biti korištena u sprezi sa svim verzijama SIP i H.323 standarda. Time bi se izbjegli potencijalni problemi prilikom mijenjanja VoIP sigurnosnih komponenti kada ti protokoli evoluiraju.
- SPOSOBNOST RUKOVANJA KRIPTIRANIM VoIP PROMETOM
  Budući da idealna VoIP sigurnosna rješenja ne bi trebala ovisiti o provjeravanju vrste signala ti signali mogu biti kriptirani bilo kojim zaštitnim mehanizmom.
- PONAŠANJE U SLUČAJU PREKIDA
  U slučaju prekida uspostavljenih VoIP konekcija, u idealno konfiguriranim VoIP mrežama, automatski bi se trebao preusmjeriti VoIP promet prema redundantnim *gateway* uređajima.

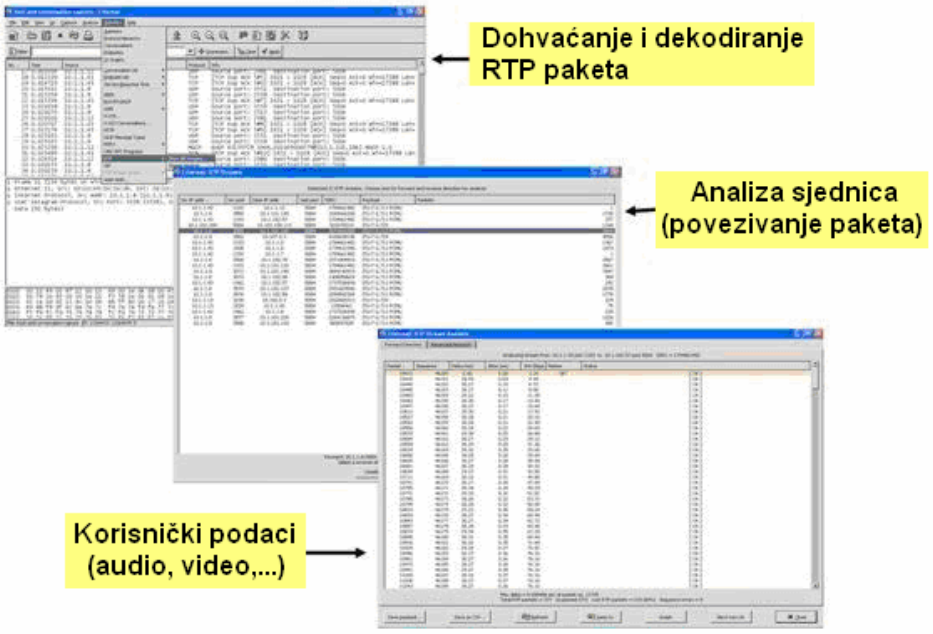
5. Prijetnje za VoIP mreže

Neki od glavnih sigurnosnih problema koji se pojavljuju u VoIP okolinama su slični ako ne i isti kao i problemi koji se tiču sigurnosti IP mreža. Danas se većina podatkovne komunikacije obavlja preko Interneta, što je moguće korištenjem IP adresiranja. VoIP isto koristi IP adresiranje za lociranje ostalih korisnika na glasovnim komunikacijskim mrežama. Stoga je IP sigurnost veoma važna stavka za osiguravanje VoIP mreža, za koje se očekuje da postane okosnica svih glasovnih komunikacija u svijetu. U prva tri poglavlja ove cjeline navedene su neke od prijetnji koje su zajedničke IP i VoIP mrežama. Prijetnje koje su karakteristične za VoIP mreže opisane su u zadnja četiri poglavlja ove cjeline.

5.1. Neovlašteno praćenje i analiza prometa

Neovlašteno praćenje i prisluškivanje mrežnog prometa (eng. *Sniffing/Eavesdropping*) može rezultirati otkrivanjem povjerljivih ili nezaštićenih korisničkih informacija, a u najgorem slučaju i krađom identiteta korisnika. Iskorištavanjem ovog propusta sofisticiranim malicioznim korisnicima

omogućeno je prikupljanje informacija o VoIP mreži koje se mogu iskoristiti za napade na druge dijelove mreže (podatkovna, nadzorna …). Svi potrebni alati za prisluškivanje, uključujući i H.323 i SIP pomoćne programe za paketno prisluškivanje mogu se naći na *open source* stranicama na Internetu. Na slici Slika 5 mogu se vidjeti koraci u procesu sakupljanja i krađe VoIP informacija korištenjem programskog paketa Ethereal.



Slika 5: Koraci krađe VoIP paketa pomoću programskog paketa Ethereal

Za rješavanje ovih napada predlaže se primjena neke od dodatnih metoda enkripcije na višim mrežnim slojevima (npr. tuneliranje prometa korištenjem virtualnih privatnih mreža).

5.2. Uskraćivanje računalnih resursa

Napadi uskraćivanja računalnih resursa (eng. *Denial of Service – DoS*) mogu biti zasnovani na okupiranju računalnih mreža s nepotrebnim podacima ili na rušenju pojedinih komponenti mreže. Ukoliko organizacija koristi tradicionalne komunikacijske kanale za razgovor (javna telefonska mreža) tada čak i u slučajevima kada je podatkovna mreža srušena, organizacija i dalje može komunicirati i obavljati telefonske razgovore. Ali ukoliko organizacija bazira svoje poslovanje na VoIP mreži, tada DoS napadi mogu biti veoma efikasni protiv tih organizacija. To je prvenstveno rezultat činjenice da DoS napadi ili prekidaju uslugu ili smanjuju kvalitetu postojeće usluge (eng. *Quality of Sevice* - QoS) za koju je nužno da bude visoka kako bi VoIP bio funkcionalan. Zbog opasnosti koju DoS napadi predstavljaju za VoIP mreže, proizvođači VoIP opreme sve češće ugrađuju u svoje proizvode različite metode zaštita od DoS napada.

5.3. Distribuirano uskraćivanje računalnih resursa

Distribuirani napadi uskraćivanja računalnih resursa (eng. *Distributed Denial of Service – DDoS*) slični su prethodno opisanim napadima uz tu razliku što se ovi napadi ne izvršavaju s jednog nego s većeg broja računala. Da bi maliciozni korisnik izvršio DDoS napad potrebno je da na određeni način utječe na veću skupinu računala. To se može izvesti ukoliko napadač preuzme kontrolu nad tim računalima. Ta računala mogu biti upravljana preko različitih virusa i trojanaca koji napadaču omogućavaju upravljanje računalima i zagušivanje mreže hrpom nepotrebnih podataka koji uzrokuju uskraćivanje resursa na napadnutom računalu ili mreži.

Za ispunjenje DDoS napada nije potrebno da napadač preuzme kontrolu nad računalima s kojih želi izvesti napad. Napadač može izvesti DDoS napad ukoliko pošalje zahtjev s lažiranom izvorišnom IP adresom na grupu računala. Tada će sva ta računala odgovoriti na te upite na ciljano računalo te time onemogućiti rad tog računala.

5.4. Presretanje poziva

Presretanje poziva (eng. *call interception*) omogućava nedozvoljeno nadgledanje i snimanje poziva te glasovnih poruka. Presretanjem i prisluškivanjem poziva unutar organizacija moguće je ukrasti tajne i povjerljive poslovne podatke. VoIP pozivi se mogu presretati tako da se preusmjere na neki posredni poslužitelj koji prema svojoj konfiguraciji nadzire VoIP pozive - tzv. „*Man in the middle*“ napad.
VoIP pozivi se mogu na jednostavan način skupljati i dekodirati ukoliko napadač ima fizički pristup lokalnoj računalnoj mreži preko koje VoIP paketi putuju. Kao protumjere za ovakve napade potrebno je zaštititi fizičke pristupe mreži te implementirati enkripciju s nekom od raspoloživih metoda.

5.5. Krađa identiteta

Krađom tuđeg identiteta napadač može doći do informacija potrebnih za stjecanje kontrole nad tuđim IP telefonom te preusmjeriti promet na drugu lokaciju. I ukoliko legitimni korisnik nije svjestan preusmjeravanja poziva tada on može odavati povjerljiva informacije, a da nije ni svjestan toga.

5.6. Financijska zlouporaba VoIP infrastrukture (eng. *Call Fraud*)

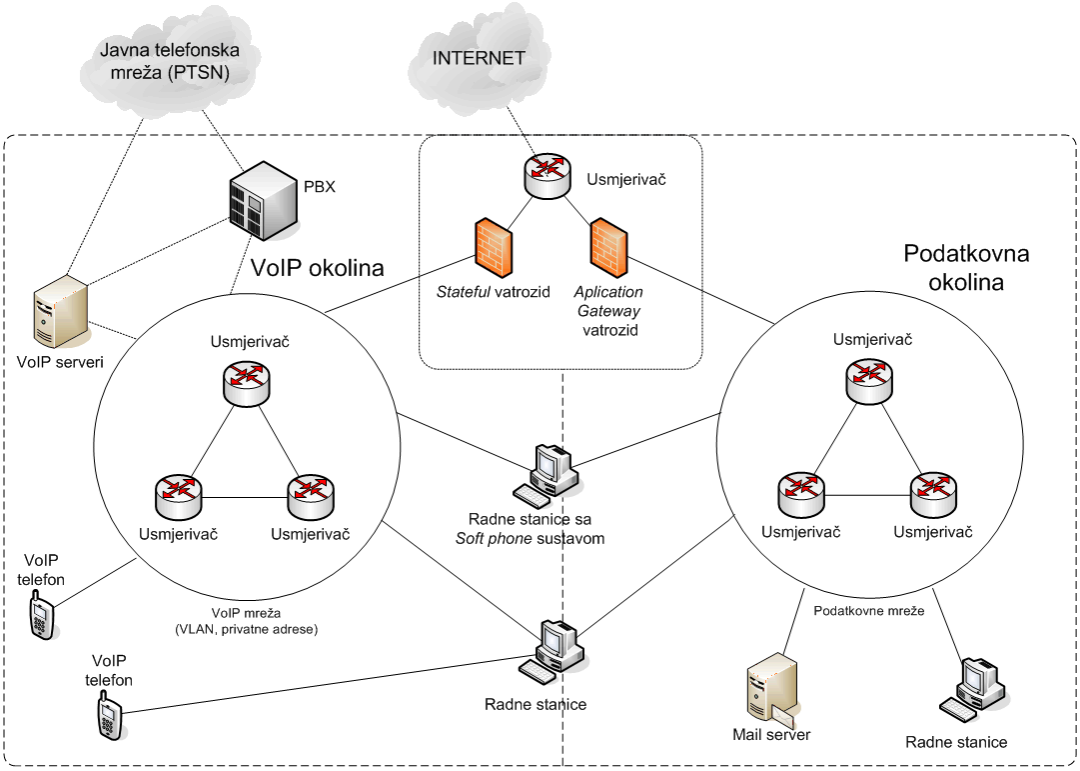
Call fraud je specifičan napad za VoIP mreže koji se sastoji od nezakonitog korištenja VoIP infrastrukture za obavljanje telefonskih poziva. Takvi telefonski pozivi izgledaju kao da su pokrenuti od legitimnih korisnika unutar napadnute mreže pa se njima i naplaćuju.

5.7. VoIP neželjena pošta (eng. *Spam over Internet Telephony - 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. Kako se sve više poslovnih korisnika odlučuje za VoIP komunikacije, VoIP neželjena pošta ima sve veću i veću tendenciju širenja i sve veću populaciju kojoj je namijenjena.

6. 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. U nastavku ovog poglavlja navedeni su uobičajeni načini zaštite kojima se minimaliziraju sigurnosni rizici i prijetnje unutar VoIP mreža. Na slici Slika 6 može se vidjeti logička shema VoIP sigurnosne arhitekture.



Slika 6: Logička shema VoIP sigurnosne arhitekture

6.1. Fizička sigurnost

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

- sve kritične VoIP mrežne i poslužiteljske komponente trebalo bi locirati u zaštićene i sigurne lokacije odvojene od neovlaštenog pristupa;
- IP telefone bi trebalo konfigurirati tako da ne prikazuju svoje mrežne konfiguracijske informacije;
- tzv. *Soft Phone* sustavi, koji provode VoIP komunikaciju pomoću običnog računala, slušalica i specijalnog programa, trebalo bi izbjegavati.

6.2. Odvajanje IP adresa

Sve VoIP komponente bi trebalo postaviti na odvojene privatne mreže, koje nisu djeljive s ostalim mrežama. U tu svrhu 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.
Kada su potrebne mrežne konekcije između VoIP i ostalih podatkovnih mreža (npr. zbog glasovne pošte) potrebno je implementirati NAT koji prevodi javne IP adrese u privatne te time interna računala odvaja od vanjske mreže. NAT bi trebalo implementirati na dodirnim točkama VoIP i ostalih mreža. Tako je pružena dodatna sigurnost od malicioznih korisnika koji neće biti u mogućnosti skeniranja VoIP mreža u potrazi za mogućim sigurnosnim propustima, osim kada NAT nije pravilno konfiguriran.

6.3. Virtualni LAN-ovi

Preporuča se odvajanje VoIP-a od ostalih podatkovnih mreža korištenjem virtualnih lokalnih mreža (eng. *Virtual Local Area Networks - VLAN*). Tehnologija virtualnih LAN-ova omogućuje logičko grupiranje korisnika, neovisno o njihovoj fizičkoj lokaciji, u manje logičke cjeline, tzv. virtualne lokalne računalne mreže (VLAN). Ovakvim pristupom moguće je unutar jednog fizičkog LAN-a kreirati nekoliko manjih, međusobno odvojenih virtualnih LAN-ova, od kojih svaki zadržava svojstva klasične računalne mreže. Grupiranje korisnika moguće je realizirati prema različitim kriterijima kao

što su MAC adrese mrežnih kartica, IP adrese, portovi preklopnika, itd… Svaki virtualni LAN predstavlja jednu *broadcast* domenu, a komunikaciju između pojedinih VLAN-ova moguće je kontrolirati. U preklapanim mrežama VLAN-ovi ostvaruju logičko segmentiranje i odvajanje i time dodatno povećavaju performanse i sigurnost mreže. Odvajanje VoIP mreža od ostalih podatkovnih mreža služi za umanjivanje opasnosti od DoS napada i prisluškivanje paketa iz podatkovnih mreža. Uz to, odvajanjem podatkovnih i VoIP mreža smanjuje se "natjecanje" za mrežnim resursima i samim time smanjuje se vrijeme kašnjenja za prijenosne servise. Kako je VoIP jako osjetljiv na vrijeme kašnjenja, ovakav segmentni pristup je jedan od najjeftinijih načina poboljšavanja performans postojeće mrežne infrastrukture.

6.4. Vatrozidi

Najbolji način za osiguravanje VoIP usluge jest filtriranje prometa između VoIP mreža i podatkovnih mreža korištenjem vatrozida (eng. *firewalls*). Vatrozid je sustav (programski ili sklopovski) čija je osnovna uloga filtriranje dolaznog i odlaznog mrežnog prometa organizacije. Svoju osnovnu zadaću vatrozid obavlja putem sigurnosnih pravila koja definiraju koji je promet dopušten, a koji zabranjen u skladu sa sigurnosnom politikom organizacije. Jedan od nedostataka vatozidne zaštite je taj što se nakon definicije pravila filtriranja ona više ne mijenjaju, ili se moraju mijenjati ručno. Nažalost, zbog specifičnosti VoIP-a koji za normalan rad zahtjeva korištenje velikog raspona otvorenih portova (protokol koji se koristi za prijenos VoIP podataka koristi raspon portova od 10024 do 65535 za transportiranje paketa), potrebno je koristiti vatrozide koji direktno podržavaju SIP i H.323 protokole.

6.5. 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.
Virtualne privatne mreže (tzv. enkripcijski tuneli) omogućavaju sigurno spajanje dvije fizički odvojene mreže preko Interneta bez izlaganja podataka neautoriziranim korisnicima. Nakon što je jednom uspješno uspostavljena, virtualna privatna mreža je zaštićena od neovlaštenih iskorištenja sve dok su enkripcijske tehnike sigurne. Koncept VPN-a omogućava udaljenim korisnicima na nezaštićenoj strani direktno adresiranje računala unutar lokalne mreže, što drugim korisnicima nije moguće zbog NAT-a i filtriranja paketa. Brzina kojom takva udaljena računala komuniciraju s lokalnim računalima mnogo je sporija od one koju računala u lokalnoj mreži koriste. Razlog tome je njihova fizička udaljenost i oslonjenost na brzinu Interneta, ali i procesi enkripcije podataka, filtriranja paketa na vatrozidu, i dekripcije originalnih podataka.
Kako bi udaljeni korisnici uspješno prošli fazu spajanja na lokalnu mrežu potrebno je uspješno obaviti autentifikaciju istih. Ta autentifikacija mora biti kriptirana u svrhu sprečavanja krađe podataka od strane napadača i iskorištenja istih.
Za svaki udaljeni nadzor i udaljeni pristup VoIP komponentama preporuča se korištenje *IPsec* ili SSH (eng. *Secure Shell*) protokola. Također, svugdje gdje je moguće, preporuča se korištenje *IPsec* tuneliranja umjesto IPsec transporta iz razloga što tuneliranje maskira odredišnu i izvorišnu IP adresu.

7. Zaključak

VoIP se može implementirati u organizacije na siguran način, ali ta procedura nije jednostavna. Što se više počinje koristiti VoIP u organizacijama to će one same biti više izložene opisanim napadima i sigurnosnim rizicima koji su već prisutni na podatkovnim mrežama.
Vjerojatno će proći još određeno vrijeme dok se ne usavrše standardi za VoIP sisteme i dok sama VoIP komunikacija ne postane standardna u glasovnom komuniciranju u svijetu. Dok se to ne dogodi organizacije bi trebale obraćati veliku pažnju na jedinstvene zahtjeve koje VoIP ima te nabavku pravilne opreme i programa pomoću kojih je moguće uspješnije odgovoriti na sve sigurnosne prijetnje usmjerene protiv VoIP-a.

8. Reference

[1] National Institute of Standards and Technology: Special Publication 800-58 - Security Considerations for Voice Over IP Systems, siječanj 2005.
[2] Defense Information Systems Agency: Voice over Internet Protocol (VoIP) security tehnical implementation guide, 2004
[3] RFC specifikacija SIP protokola, http://www.ietf.org/rfc/rfc2543.txt
[4] H.323 Protocols Suite, http://www.protocols.com/pbook/h323.htm
[5] Ethereal, http://www.ethereal.com/
[6] Greg S. Tucker: Voice Over Internet Protocol (VoIP) and Security, listopad 2004.