SVEUČILIŠTE U SPLITU

POMORSKI FAKULTET U SPLITU

JOSIP STORIĆ

SIGURNOSNE PRIJETNJE I MEHANIZMI ZAŠTITE VoIP TEHNOLOGIJE

ZAVRŠNI RAD

SPLIT, 2019.

SVEUČILIŠTE U SPLITU

POMORSKI FAKULTET U SPLITU

STUDIJ: POMORSKE ELEKTROTEHNIČKE I INFORMATIČKE TEHNOLOGIJE

SIGURNOSNE PRIJETNJE I MEHANIZMI ZAŠTITE VoIP TEHNOLOGIJE

ZAVRŠNI RAD

MENTOR:
dr. sc. Anita Gudelj

STUDENT:
Josip Storić
(MB:0171227804)

SPLIT, 2019.

SAŽETAK

Ovim radom su opisane prijetnje koje ugrožavaju sigurnost komunikacije putem VoIP tehnologije. Napadi se odvijaju ili putem zlonamjernih programa ili na neki drugi način koji napadač može upotrijebiti kako bi ostvario svoje ilegalne ciljeve. Nakon što se razradila tema sigurnosnih prijetnji opisane su mjere zaštite koje bi se trebale primijeniti kako napadači nebi ostvarili svoje ciljeve. Cilj ovog rada je ukazati na važnost sigurnosti računalnih sustava, računalnih mreža i općenito sigurnosti prilikom korištenja usluga koje se pružaju putem interneta. Sigurnost navedenih sustava je ugrožena iz razloga jer postoji nekolicina korisnika sustava čija su namjera i cilj pomoću svih raspoloživih sredstava sebi priskrbiti korist na štetu ostalih korisnika sustava.

Ključne riječi: *VoIP, sigurnosne prijetnje, napadi, mjere zaštite*

ABSTRACT

This paper describes the security threats that jeopardize the security of communications via VoIP technology. The attacks take place either through malware or in any other way that the attacker can use to achieve his or her illegal targets. After elaborating on the topic of security threats, the protection measures that should be applied in order to prevent the attackers from achieving their objectives are described. The aim of this paper is to pay attention to the security of computer systems, computer networks and general security when using the services provided over the Internet. The security of these systems is compromised because there are a number of system users whose intention and goal is to use all available resources to bring benefits to themselves at the expense of other system users.

Keywords:*VoIP, securitythreats, attacks, protection measures*

SADRŽAJ

1. UVOD

U današnje vrijeme svijet se sve više okreće digitalnoj tehnologiji, dok analogna tehnologija polako odlazi u povijest. Razlozi tome su višestruki od dizajniranja i izrade samih uređaja, principa rada istih, obrade signala i mogućnosti komuniciranja itd.

Razvojem novih tehnologija i zahvaljujući operaterima koji ih implementiraju u svoje sustave klasična telefonija sve više postaje dijelom digitalnog svijeta.

Ta nova tehnologija komuniciranja koja polako zamjenjuje klasičnu telefoniju, se zove VoIP tehnologija ili punim imenom *Voice over Internet Protocol* tehnologija. Za ovu vrstu tehnologije još se koriste nazivi kao što su: *Internet Protocol* - IP telefonija (eng. *IP telephony*), internet telefonija (eng. *Internet Telephony*), VoBB (eng. *Voice over broadband*) itd.

Kako sama kratica VoIP i kaže ova tehnologija se u načelu koristi za prijenos glasa putem Interneta u digitalnome obliku, za razliku od klasične telefonije koja je slala analogni signal putem javne telefonske mreže.

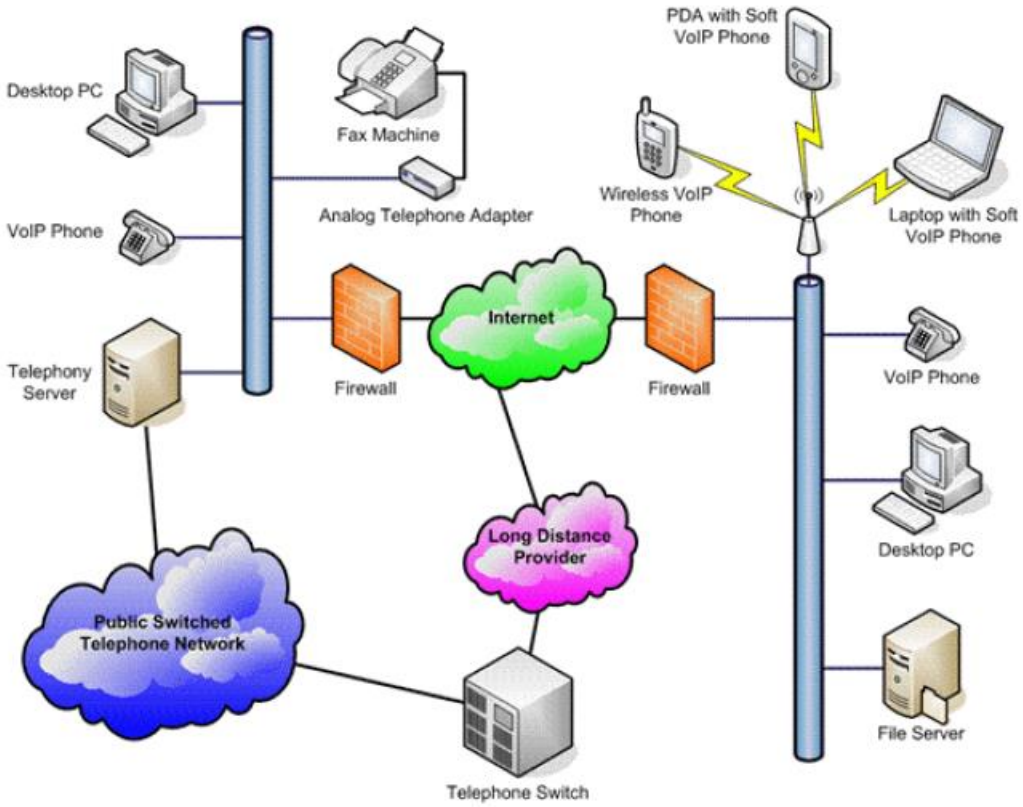
VoIP tehnologija svoje začetke ima 1995. godine kada su počela eksperimentiranja glasovnog komuniciranja putem interneta tako da se u potpunosti zaobiđe javna telefonska mreža. Za takvu vrstu komunikacije uz računalo, modem s konekcijom prema internetu, mikrofon i zvučnike bilo je potrebno imati i identičan software na oba računala koja su komunicirala između sebe. S obzirom da tada nije bilo širokopojasnog interneta velikih brzina razgovori su se tada odvijali uz poteškoće kao što je bilo kašnjenje u prijenosu signala u odnosu na izgovorene riječi, te prekidanje signala, dok danas uz velike brzine interneta praktički kako onaj koji govori slušatelj na drugoj strani ga odmah čuje uz puno veću kvalitetu zvuka nego što je to bila u početku.

Naravno kako tehnologija sve više napreduje, danas operateri nude fiksne telefonske linije putem *Digital Subscriber Loop* - DSL linije u kojoj je implementiran VoIP komunikacijski kanal, tako što se standardni telefon spaja na router koji je spojen na DSL liniju.

Za razliku od klasične telefonije gdje se analogni signal slao putem bakrenih parica, kod VoIP tehnologije šalje se digitalni signal putem Interneta (čiji se prijenos vrši ili žičanim ili bežičnim putem). Odnosno glas koji je sam po sebi analogni signal treba pretvoriti u digitalni signal, što u načelu nije problem jer taj posao zapravo kod računala odrađuju zvučne kartice te ga se potom pakira u pakete (proces koji je određen IP

protokolom) te se preko mrežnog sloja u obliku digitalnog signala (signal koji putem naponskih nivoa predstavlja logičke 0 i 1) šalje drugom korisniku s kojim se komunicira.

Javna telefonska mreža ili drukčije rečeno standardna telefonija putem bakrenih parica je također imala svoje sigurnosne prijetnje u vidu prisluškivanja ili krađe servisa, no danas kada se telefonija odvija putem interneta broj i vrsta sigurnosnih prijetnji je porasla i napadači se trude svakim danom da otkriju neku novu vrstu sigurnosne prijetnje kako bi zaobišli dostupne mjere zaštite, a sve u svrhu ispunjavanja vlastite satisfakcije počinjenjem štete ili pak u svrhu ostvarivanja vlastite koristi. Ovaj rad ukazuje na sigurnosne prijetnje u VoIP tehnologiji te na mjere zaštite koje se trebaju poduzeti da bi se te sigurnosne prijetnje izbjegle ili uklonile kako bi se izbjegle eventualne štete. Na slici 1 je prikazana upotreba VoIP tehnologije u praktičnoj primjeni.



Slika 1. Prikaz primjene VoIP tehnologije [1]

2. SIGURNOSNE PRIJETNJE KOD VOIP TEHNOLOGIJE

Da bi se moglo uopće razgovarati o mjerama zaštite VoIP tehnologije i razvijati mjere zaštite potrebno je najprije upoznati se sa svim predvidivim sigurnosnim prijetnjama i mogućim napadima u VoIP tehnologiji. U ovom poglavlju će se razraditi sigurnosne prijetnje i mogući napadi, koji sloj Internet protokola napadaju i kakvu štetu na VoIP sustavuzrokuju.

Sigurnosne prijetnje i mogući napadi na sigurnost komunikacije mogu se razmatrati na dva načina:

- sigurnosne prijetnje i napadi prema načinu djelovanja
- sigurnosne prijetnje prema vrsti ugroze tj. štete koju određeni napad može izazvati u VoIP sustavu prilikom komunikacije.

2.1. UTJECAJ NAPADA NA VoIP SUSTAV

Prvi način na koji se sigurnosne prijetnje u VoIP tehnologiji mogu razmatrati je prema posljedicama koje izazivaju pojedini napadi:

- upitna povjerljivost podataka u slučaju ako je napad izveden u svrhu neovlaštenog prikupljanja informacija ili prisluškivanje
- upitan integritet samog sustava kada se napadom na VoIP sustav nastoji omesti valjano odvijanje komunikacije
- potpuno onemogućen pristup poslužitelju usluge odnosno onemogućena komunikacija.

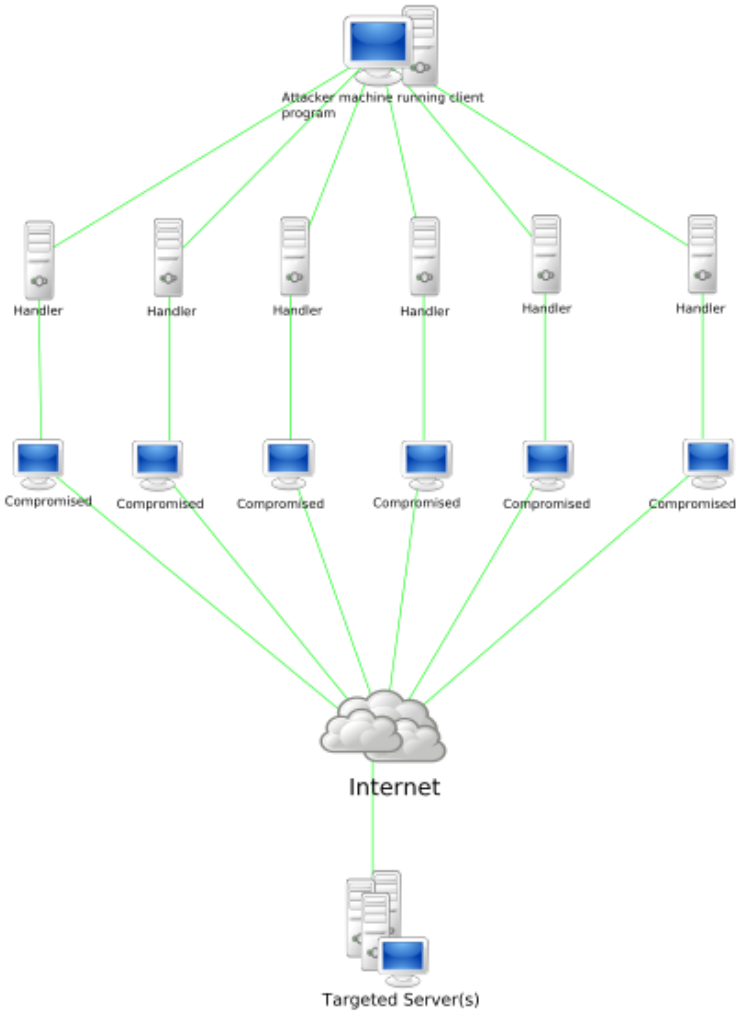
2.2. PODJELA SIGURNOSNIH PRIJETNJI PREMA NAČINU DJELOVANJA

Napadi se prema načinu djelovanja dijele na aktivne i pasivne napade.

Pasivni napadi su oni koji ne mijenjaju podatke niti ugrožavaju protok podataka i njihovu cjelovitost već se s ovom vrstom napada nastoji doći do informacija koje se izmjenjuju pri komunikaciji. To se ostvaruje presretanjem sadržaja poruke ili analizom prometa podataka gdje se analizom algoritma komunikacije detektira vrsta komunikacije i u slučaju da u njoj postoji informacija od interesa za napadače oni prisvajaju tu informaciju. Ono što je najopasnije kod pasivnih napada je to što korisnici koji trpe napad

to ne osjete u vidu usporenosti rada sustava ili lošeg prijenosa podataka ili bilo kakve anomalije u radu sustava pa često niti ne posumnjaju da su meta napada.

Aktivni napadi su za razliku od pasivnih napada destruktivniji, jer cilj nije samo presretanje i prisvajanje informacije nego se ovim napadima u krajnjoj mjeri želi postići onesposobljavanje cijelog VoIP sustava. To podrazumijeva modifikaciju ili izmjenu toka podataka, generiranjem lažnog toka informacija itd. Radi toga se aktivni napadi mogu i lakše detektirati jer se odražavaju na radu VoIP sustava i odvijanju same komunikacije.U aktivne napade pripadaju: *Denial of Service* - DoS i *Distributed Denial of Service* - DDoS napadi (otkaz servisa i distribuirani otkaz servisa), neovlašten pristup, krađa servisa, napad na protokole (ova vrsta napada je detaljnije obrađena u nastavku rada). Slika 2 prikazuje dijagram DDoS napada.



Slika 2. Prikaz dijagrama DDoS napada [7]

DoS napad djeluje na način da napadač „zatrpa“ servis velikim brojem posebno konstruiranih zahtjeva sve dok se servis tj. poslužitelj usluge ne zaguši od prevelikog broja zahtjeva ili pak toliko uspori da korisnicima bude onemogućen pristup tome servisu.

DDoS napad je u stvari prethodno opisani DoS napad samo je DDoS puno učinkovitiji. DoS napad se obično obavlja s jednog računala pa ne može poslati toliko veliki broj zahtjeva prema servisu koliko to može napraviti grupa većeg broja računala kao DDoS napadu i upravo iz tog razloga i jeste veća učinkovitost DDoS napada. Ovoj vrsti napada pripadaju *flooding* napadi, a po imenu ovog napada (eng. *Flood* – poplava) se može pretpostaviti da se radi o napadu gdje na napadnuti servis pristiže više zahtjeva nego ih on može obraditi pa dolazi do „poplave“ koja prouzrokuje štetu u vidu nemogućnosti pristupa napadnutom servisu.

Sljedeći oblik aktivnog napada je neovlašteni pristup. Sam naziv ovog napada govori o čemu se radi, a mogućnosti nastanka štete od ovog napada su višestruke. Do ovog napada dolazi ukoliko je netko ušao u sustav korisnika ili njegov korisnički račun, ili je pak presreo podatke koji sadrže takve informacije. Pristupom u korisnički račun korisnika napadač ima otvorenu mogućnost počinjenja štete na način da promjenom određenih parametara onemogući korisniku pristup svome korisničkom računu te da korisniku načini financijsku štetu korištenjem njegovog korisničkog računa za obavljanje daljnjih ilegalnih radnji. Danas postoje računalni programi koji omogućuju međunarodne i međukontinentalne pozive po puno pristupačnijim cijenama nego što to nude lokalni pružatelji komunikacijskih usluga, i ako napadači dođu do podataka za pristup korisničkim računima za spomenute računalne programe, mogu načiniti velike financijske probleme korisnicima. Ovakav način napada je dosta čest i redovna promjena lozinke pogotovo nakon što korisnik sustava posumnja da je njegov korisnički račun „probijen“ je osnovni korak u zaštiti od ovakvih napada, jer ako je napadač došao do podataka za pristup korisničkom računu ne znači da će ih odmah iskoristiti, a ako se u međuvremenu lozinka promjeni informacija koju napadač ima je zastarjela i ti podatci do kojih je došao mu neće biti od koristi.

Također, neovlaštenim pristupom u same servise, odnosno servere poslužitelja usluge, napadači mogu učiniti štetu u obliku da sruše cijeli sustav poslužitelja usluge. Međutim, poslužitelji konstantno rade na vlastitoj zaštiti sustava te su ovakvi napadi rijetki, a ako se dogode oni utječu na veliki broj korisnika u pogledu pristupa serverima poslužitelja odnosno uslugama koje taj poslužitelj pruža.

2.3. VRSTE SIGURNOSNIH PRIJETNJI NA SLOJEVE IP PROTOKOLA KOD VoIP TEHNOLOGIJE

Sigurnosne prijetnje se događaju na svim razinama IP protokola putem kojeg se odvija VoIP komunikacija. Grupiranje prijetnji prema razinama IP protokola i vrsti napada prikazano je u tablicama 1-4, a u narednim podpoglavljima svaka od njih je pojedinačno opisana.

Na mrežnom ili fizičkom sloju sigurnosne prijetnje mogu uzrokovati napade poput *Media Acces Control*, MAC spoofinga ili *Address Resolution Protocol* - ARP flood (Tablica 1).

Tablica 1.Vrste napada na mrežnom sučelju [5]

Sloj IP protokola	Vrsta napada	Povjerljivost	Integritet / Cjelovitost	Dostupnost
Mrežno sučelje (Fizički i podatkovni sloj)	Fizički napad	*		*
	ARP cache	*	*	*
	ARP flood			*
	MAC spoofing	*	*	*

Drugi sloj IP protokola koji je podložan sigurnosnim prijetnjama je Internet ili IP sloj. Tu se nalaze napadi poput IP spoofinga, promijenjenih paketa itd. (Tablica 2).

Tablica 2. Vrste napada uzrokovanih sigurnosnim prijetnjama na Internet sloju [5]

Sloj IP protokola	Vrsta napada	Povjerljivost	Integritet / Cjelovitost	Dostupnost
Internet sloj	IP spoofing		*	*
	Promijenjeni paketi	*	*	*
	IP frag	*	*	*
	Jolt			*

Sljedeći sloj koji je podložan sigurnosnim prijetnjama je transportni sloj. Osnovni protokoli ovog sloja su *Transmission Control Protocol* - TCP i *User Datagram Protocol* - UDP protokoli, pa su oni ujedno i najranjiviji (Tablica 3).

Tablica 3. Vrste napada na transportnom sloju [5]

Sloj IP protokola	Vrsta napada	Povjerljivost	Integritet / Cjelovitost	Dostupnost
Transportni sloj	TCP / UDP flood			*
	TCP / UDP replay	*	*	

Posljednji sloj TCP / IP protokola je aplikacijski sloj, a on je ujedno i najranjiviji od svih slojeva i kod njega imamo najviše prijetnji za sigurnost sustava. Jedan od razloga je i taj što na aplikacijski sloj direktno djeluju i korisnici sustava. Aplikacijski sloj predstavlja aplikacije koje korisnik koristi za VoIP komunikaciju točnije mete sigurnosnih prijetnji su u većem slučaju protokoli aplikacijskog sloja koje koriste aplikacije. Vrste napada u ovom sloju su navedene u tablici 4.

Tablica 4. Vrste napada na aplikacijskom sloju [5]

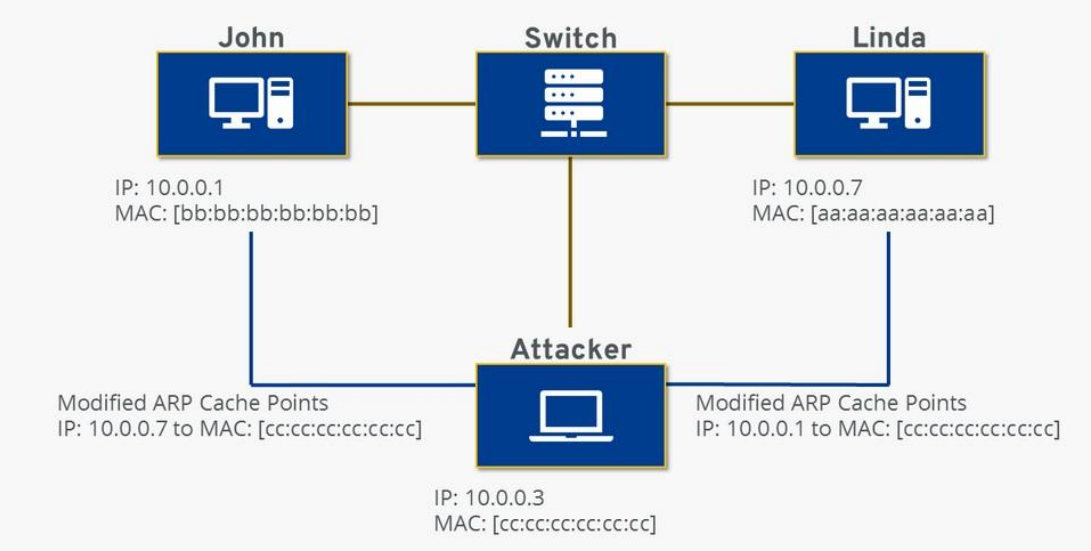
Sloj IP protokola	Vrsta napada	Povjerljivost	Integritet / Cjelovitost	Dostupnost
Aplikacijski sloj	TFTP server insertion		*	
	DHCP server insertion		*	
	DHCP starvation			*
	ICMP flood			*
	Registration Hijacking	*	*	*
	MGCP Hijack	*	*	*
	Message modification	*	*	
	Spoof via header	*	*	*
	Cancel / bye method			*
	Redirect method	*		*
	RTP flooding			*
	RTP tampering	*	*	*
	Encryption	*	*	*
	Default configuration	*	*	*
	Unnecessary services	*	*	*
	Buffer overflow	*	*	*
	DNS Availability			*

2.3.1. Vrste napada na mrežnom sučelju (fizički i podatkovni sloj)

Kao prva vrsta napada na mrežnom sučelju je fizički napad. To je napad na fizički sloj IP protokola odnosno na samu infrastrukturu koja sačinjava jedan VoIP sustav. Fizičkim napadom kako je i naznačeno u tablici 1 ugrožava se povjerljivost i dostupnost komunikacije putem VoIP sustava. Povjerljivost jer netko tko ima fizički pristup samom sustavu s lakoćom se može ubaciti u komunikaciju i na taj način prisluškivati razgovor između dva korisnika sustava, a dostupnost je ugrožena samim time ako netko ima nesmetan pristup sustavu i ima potrebno znanje o ovoj vrsti tehnologije može izmjenom parametara potpuno onemogućiti rad kompletnog sustava.

Nakon fizičkog napada slijede dva napada na ARP komunikacijski protokol koji služi za dobivanje fizičke adrese na lokalnoj mreži iz poznate mrežne adrese. ARP *cache poisoning* ili ARP *spoofing* je tehnika kojom napadač šalje poruku s krivotvorenom ARP porukom u lokalnu mrežu s ciljem da svoju MAC adresu spoji s IP adresom nekog uređaja u mreži naprimjer zadanog *gatewaya*. Na taj način napadač postiže da se svi podatci koji bi trebali ići na zadani *gateway* zapravo šalju napadaču te je napadač preuzeo potpunu kontrolu nad tim sustavom. Ako napadač uspije s ovom prijetnjom on ima mogućnost presretanja informacija, ali isto tako ima kontrolu nad protokom svih podatkovnih paketa koji prolaze kroz taj sustav kao i mogućnost da zaustavi sav promet u sustavu.

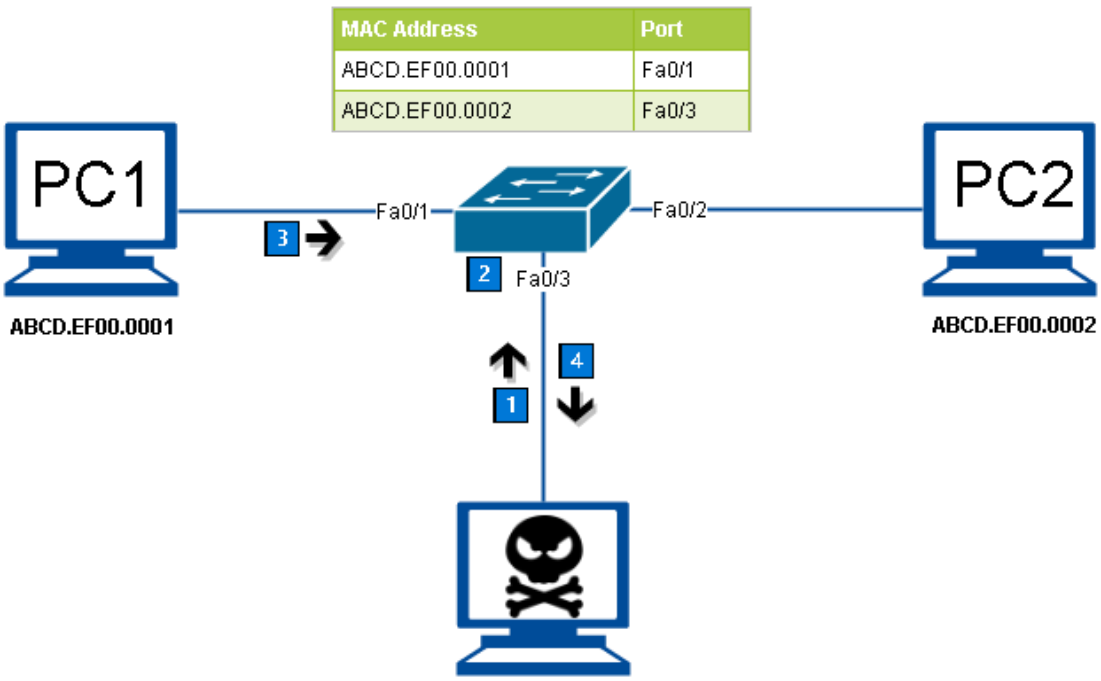
Primjer izvođenja jedne ovakvog napada prikazan je na slici 3. Iz svega gore navedenog slijedi da ovaj napad narušava povjerljivost i integritet te dostupnost samog VoIP sustava.



Slika 3. Primjer ARP *spoofing* napada [8]

ARP *flood* je pak vrsta napada s ciljem da onemogući pristup sustavu, odnosno onemogućiti komunikaciju i to na način da zaraženi sustav šalje ARP odgovore svim sustavima u mreži što rezultira pogrešnim unosom u ARP *cache*. Kao rezultat tih pogrešnih unosa dobije se nemogućnost rješavanja IP i MAC adrese od strane zaraženog sustava stoga podatci nemogu doći na točno odredište, odnosno takav zaraženi sustav ne može ostvariti komunikaciju s nijednim drugim sustavom u mreži te mu je na taj način onemogućen pristup.

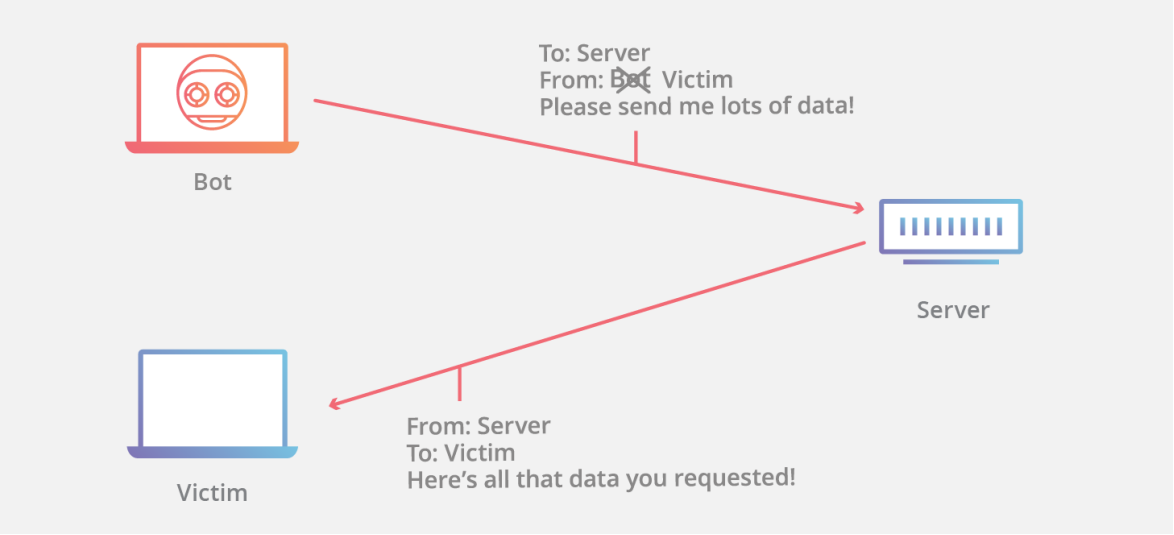
MAC *spoofing* napad je sličan ARP *spoofing* napadu samo što ovdje napadač nastoji zamijeniti originalnu MAC adresu određenog uređaja. S obzirom da je ta adresa u samim uređajima tvornički tvrdo kodirana nju nije moguće mijenjati međutim određeni upravljački programi dozvoljavaju promjenu MAC adrese i to je mjesto gdje napadač napada. Naime napadač nakon što detektira MAC adresu napadnutog uređaja podešava svoj uređaj na tu istu adresui šalje poruku prema mrežnom preklopniku koji u tablici MAC adresa postavlja napadačev uređaj na port napadnutog uređaja, a napadnuti uređaj na neki drugi port. Nakon toga kada na mrežni preklopnik dođe podatak koji treba biti dostavljen napadnutom uređaju on će prema tablici biti dostavljen napadaču (slika 4). Iz ovog razloga ova vrsta napada isto kao ARP *spoofing* ugrožava povjerljivost komunikacije, odnosno ugrožen je integritet i dostupnost samog sustava s kojim se obavlja komunikacija.



Slika 4. Primjer MAC *spoofing* napada [9]

2.3.2. Vrste napada na internet sloju

IP *spoofing* ili lažiranje IP adrese je vrsta napada u kojoj napadač IP paketima mijenja polazišnu adresu. Šta bi to značilo najbolje pokazuje slika 5. Naime napadač šalje IP paket s krivotvorenom polaznom IP adresom koja odgovara IP adresi napadnutog uređaja. U primjeru sa slike naredba koja se zahtjeva od servera je da pošalje što više podataka pošiljatelju, koji u ovom slučaju više nije napadač nego napadnuti uređaj jer krivotvorenjem njegove polazne IP adrese server podrazumijeva da mu je IP paket poslao napadnuti uređaj. Nadalje server odgovara na zahtjev koji je došao od napadača te šalje maksimalno podataka koliko može prema napadnutom uređaju. S obzirom da su serveri računala s velikom računalnom moći oni pošalju toliko podataka da ih napadnuti uređaj ne može obraditi, te dolazi do usporenog rada napadnutog uređaja ili pak do potpunog prekida rada. S obzirom da je ovom vrstom napada djelomično ili potpuno onemogućen pristup sustavu tj. odvijanju komunikacije može se utvrditi kako je i naznačeno u tablici dva da je ovim napadom ugrožen integritet i dostupnost sustava, odnosno usluge.



Slika 5. Primjer IP *spoofing* napada [10]

Još jedna u nizu napada na internet sloju je napad promjenom IP paketa. Napad se odvija tako da napadač promijeni IP paket koji se šalje napadnutom uređaju. Kada napadnuti uređaj zaprimi jedan takav neispravan paket i počne ga obrađivati dolazi do nepravilnog rada uređaja ili pak do potpunog prestanka rada. S obzirom na takav ishod vidljivo je da ova vrsta napada isto kao i IP *spoofing* onemogućuje normalnu komunikaciju ili pak komunikacija se uopće ne može uspostaviti.

IP *fragmentation* napad također ima veze sa slanjem IP paketa. U TCP/IP protokolu postoji jedan dio koji je zadužen da pakete koji su preveliki za slanje pomoću fragmentacije razbije na više manjih paketa pogodnih za slanje. Prijemna strana radi defragmentaciju i ponovno kreira početni IP paket. Napadači za napad koriste upravo taj proces fragmentacije te se fragmentacija ne odvije na način kako bi trebala. Kada takvi nepravilno fragmentirani paketi dođu kod primatelja prilikom defragmentacije dolazi do nepravilnog rada prijemnog uređaja ili pak potpunog prestanka rada jer takva obrada neispravnih paketa iziskuje od prijemnog uređaja preveliki napor i on se jednostavno sruši. To naravno dovodi kao i u prethodna dva napada do djelomične ili potpune ne mogućnosti korištenja sustava odnosno komunikacija nije moguća.

Jolt napad je sličan IP *fragmentation* napadu, samo ovdje napadač ne napada fragmentaciju paketa kojima se vrši komunikacija, nego napadač sam šalje *Internet Control Message Protocol* - ICMP paket. Paket je tako fragmentiran da kada dođe do napadnutog uređaja i ovaj ga pokuša sastaviti i obraditi to od napadnutog uređaja zahtjeva veće resurse nego što ih on ima te dolazi do „zamrzavanja“ rada napadnutog uređaja te se takav uređaj ne može dalje koristiti prije nego se ponovno pokrene.

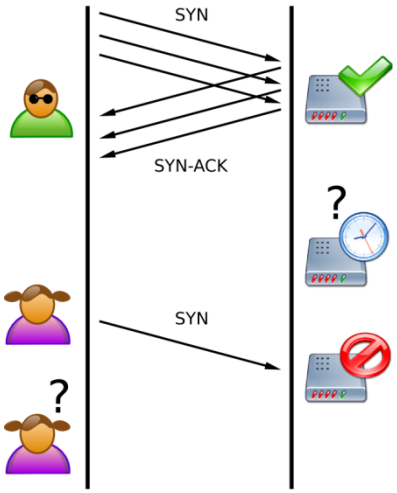
Na kraju se može zaključiti da su sve sigurnosne prijetnje na internet sloju, zapravo napadi DoS tipa. Jer kako je prethodno i napisano krajnji ishod svih ovih sigurnosnih prijetnji je nemogućnost pristupa dali sustavu, ili poslužitelju usluge ili je pak sam uređaj koji želi inicirati komunikaciju bio meta ovih prijetnji pa je došlo do njegovog prekida rada.

2.3.3. Vrste napada na transportnom sloju

Na transportnom sloju su moguće dvije vrste napada i oba ugrožavaju protokole ovog sloja: TCP i UDP. U slučaju VoIP tehnologije meta napada su češće UDP protokoli jer se u VoIP tehnologiji radi svojih karakteristika više koriste UDP protokoli i to najviše radi toga što su u VoIP-u od velike važnosti brzina i efikasnost prijenosa podataka.

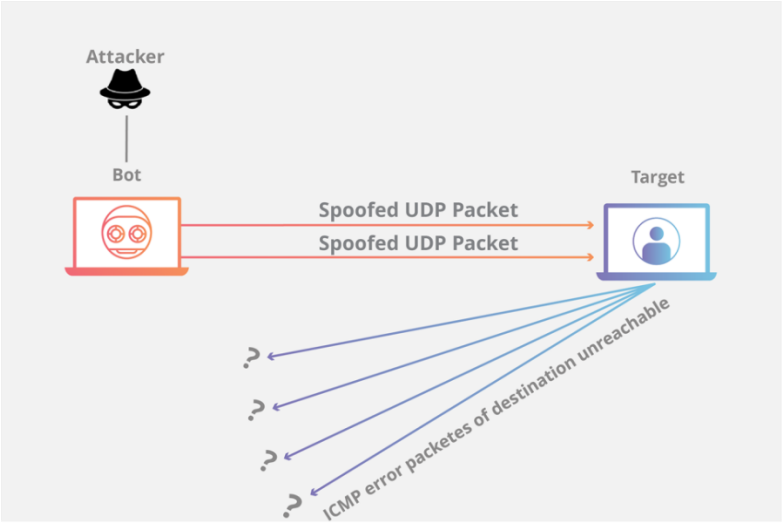
Prvi napad se zove TCP/UDP *flood*. S obzirom da se radi o *flooding* napadu zna se da je u pitanju DoS tip napada, odnosno, s ovom prijetnjom se onemogućuje pristup ili servisu ili je pak onemogućena komunikacija od strane napadnutog uređaja. TCP *flood* napad koristi proceduru uspostave veze prilikom korištenja TCP protokola. Procedura je da klijent šalje serveru poruku sinkronizacije, server odgovara s porukom da je zaprimio poruku sinkronizacije, a potom klijent ponovno odgovara serveru da je primio poruku

potvrde i veza je uspostavljena. Ova procedura je poznata kao trostruko rukovanje. Napadač napada u onom trenu kada klijent treba odgovoriti serveru s potvrdnom porukom, ali je klijent ne šalje, a server neko vrijeme stoji i čeka odgovor koji mu klijent neće poslati. Konstantnim ponavljanjem ove procedure server je stalno u stanju čekanja potvrdnog odgovora od klijenta pa drugi klijenti ne mogu ostvariti vezu sa serverom. Ukoliko je napadnuti server od nekog poslužitelja VoIP telefonije korisnici te usluge neće se moći spojiti na server koji im pruža tu uslugu.



Slika 6. Primjer TCP *flooding* napad [11]

UDP *flood* napad se temelji na principu da primjenjuje procedure koje poslužitelj poduzima kada zaprimi UDP paket na jedan od njegovih portova. Procedura koju poslužitelj obavlja je da prvo provjeri je li neka od pokrenutih aplikacija koristi port na koji je došao UDP paket, ako pak nijedna aplikacija ne koristi taj port poslužitelj šalje ICMP paket kojim obavještava pošiljatelja da nije moguće pristupiti određenoj lokaciji. Napadač zloupotrebljava ovu proceduru na način da šalje više „lažnih“ UDP paketa na više portova poslužitelja. Ti UDP paketi u sebi ne sadrže prave IP adrese napadača što je normalno jer bi se svi odgovori od poslužitelja vratili njemu, a i lako bi ga se lociralo, nego sadrže krive IP adrese na koje poslužitelj odgovara s ICMP paketima. Kako poslužitelj zaprima puno UDP paketa isto tako i odgovara s puno ICMP paketa na krive IP adrese. Ta velika količina podataka koju poslužitelj obrađuje dovodi do ne dostupnosti poslužitelja što je i slikovito prikazano na slici 7.



Slika 7. Primjer UDP *flooding* napad [12]

Drugi napad koji pogađa transportni sloj je TCP/UDP *replay* napad. *Replay* napadi su vrsta napada koja se još i naziva čovjek u sredini. Radi na principu da napadač detektira prijenos podataka, presreće ih te ih prosljeđuje dalje na odredište. Ovim napadom nije ugrožena dostupnost komunikacije, što više napadaču je u interesu da se komunikacija odvija kako bi mogao presresti podatke te na taj način doći do povjerljivih informacija. Snimljenim podatcima koje šalje klijent serveru napadač može uspostaviti ponovnu vezu sa serverom pomoću tih snimljenih podataka, a da klijent toga nije i svjestan. Iz ovog razloga ovom sigurnosnom prijetnjom je ponajprije ugrožena povjerljivost komunikacije, a potom i integritet samog sustava. Napadom na TCP / UDP protokol napadač presreće TCP / UDP pakete te ih prosljeđuje dalje ponovnim slanjem, a sebi prisvaja korisne informacije.

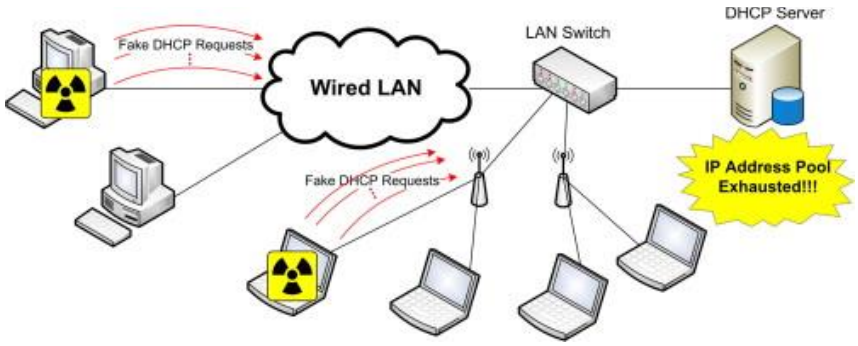
2.3.4. Vrste napada na aplikacijskom sloju

Najviše napada pogađa aplikacijski sloj iz razloga jer na ovom sloju napadač ima više mogućnosti tj. meta koje može napasti. Iz tablice 4 je vidljivo da većina napada onemogućuje pristup servisu.

Dynamic Host Configuration Protocol - DHCP server *insertion* sigurnosna prijetnja kod VoIP telefonije se događa u trenutku kada DHCP server odgovara IP telefonu, koji je prethodno zatražio odgovor od DHCP servera, odgovorom s podatkovnim poljima. U tom trenutku napadač djeluje na način da u podatkovna polja „ubaci“ lažne informacije koje na koncu rezultiraju „čovjekom u sredini“ napadom, te napadač daljnjim napadima može prisvojiti mogućnost ponovnog pokretanja IP telefona koji je meta napada, sve to bez znanja korisnika IP telefona.

Kod *Trivial File Transfer Protocol* - TFTP server *insertion* sigurnosne prijetnje napadač se ubacuje u komunikaciju između IP telefona i TFTP servera. Kako većina IP telefona prilikom uključenja od TFTP servera preuzima vlastitu konfiguracijsku datoteku, te datoteke ponekad mogu sadržavati lozinke kojima se može izravno pristupiti IP telefonu i vršiti njegovu konfiguraciju ili pak lozinke kojima se pristupa nekim drugim uslugama. Napadač koji se je „ubacio“ u komunikaciju između IP telefona i TFTP servera cijelo vrijeme „njuška“ podatke koji se izmjenjuju na ovoj relaciji. Kada napadač otkrije datoteku s navedenim lozinkama on sebi prisvaja tu datoteku i pomoću prisvojenih informacija ima mogućnost da se spaja na napadnute IP telefone mijenja njihovu konfiguraciju odnosno može u potpunosti kontrolirati IP telefon. Ovo je također „čovjek u sredini“ napad kojim napadač narušava integritet sustava.

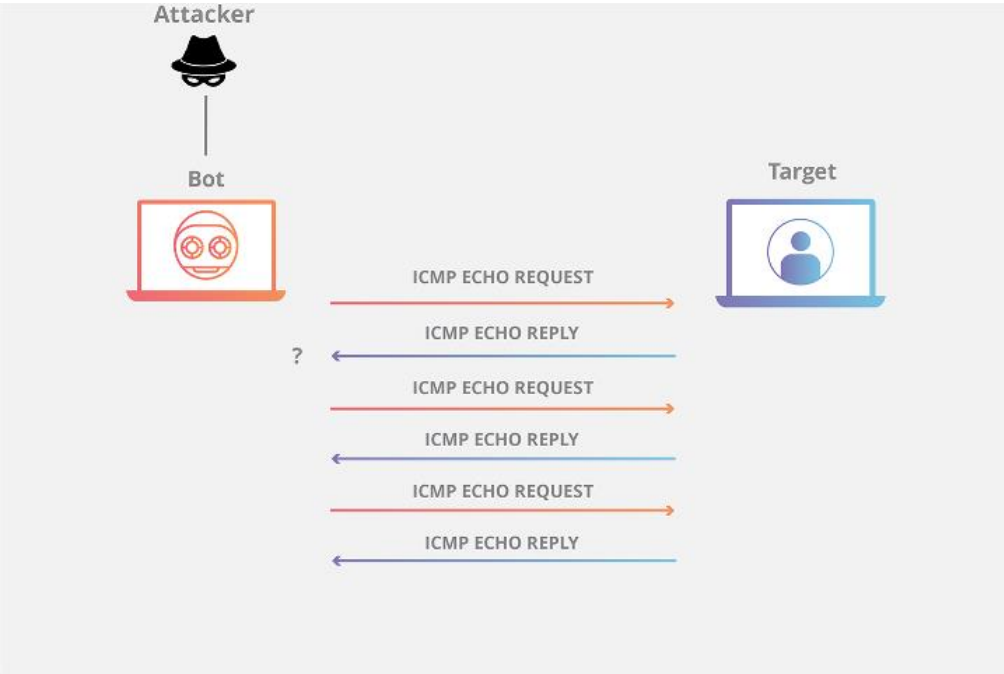
DHCP *starvation* tj. „izgladnjivanje“ je napad kojim se nastoji iz DHCP servera iscrpiti sve moguće IP adrese. Naime kako IP telefoni šalju DHCP serveru zahtjeve za dodjelom IP adrese, DHCP odgovara s podatkovnom datotekom koja sadrži tražene podatke. U normalnom radu DHCP server ima dovoljno raspoloživih IP adresa za odgovoriti svim zahtjevima, međutim kada su meta napada, napadač šalje toliko zahtjeva prema DHCP serveru da ovaj potroši sve dostupne IP adrese. Kada za vrijeme napada IP telefon nekog korisnika koji namjerava vršiti komunikaciju zatraži od DHCP servera da mu dodijeli IP adresu to neće biti moguće jer je DHCP iscrpljen. Na ovaj način je onemogućena komunikacija tj. ugrožena je dostupnost sustava, a ovaj napad spada u DoS ili čak u DDoS napade. Primjer napada je slikovito prikazan na slici 8.



Slika 8. Primjer DHCP *starvation* napada [13]

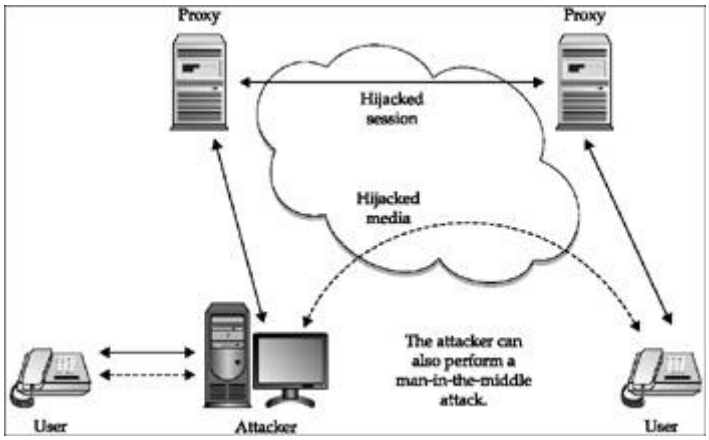
ICMP *flood* napad, kao i svi *flooding* napadi, ima za cilj onemogućiti pristup servisu, pa spada u DoS napade. Napad se izvodi tako da napadač ili preko nekih drugih

već zaraženih uređaja ili putem *bota* računalnog programa, vrste nekakvog računalnog robota s elementima umjetne inteligencije pa on za napadača odrađuje posao, šalje na napadnuti uređaj veliku količinu ICMP zahtjeva – *pingova* na koje napadnuti uređaj treba odgovoriti. Kako se radi o velikoj količini zahtjeva svi resursi napadnutog uređaja su usmjereni na odgovaranje na te zahtjeve te ne mogu odgovarati na zahtjeve drugih uređaja koji bi htjeli komunicirati s napadnutim uređajem što je i prikazano na slici 9. Na taj način je onemogućen pristup napadnutom uređaju odnosno nije moguće uspostaviti komunikaciju.



Slika 9. Primjer ICMP *flood* napad [14]

Registration Hijacking u slobodnom prijevodu otmica registracije je vrsta napada u kojoj napadač zamjenjuje stvarnu registraciju s lažnom, s čime može uzrokovati da dolazni pozivi budu preusmjereni ili napadaču ili pak na neke lažne adrese. Također otmicom registracije može se ubaciti u komunikaciju između dva korisnika i na taj način izvesti „čovjek u sredini“ napad s čim prisvaja mogućnost upravljanja komunikacijom, te može prisluškivati komunikaciju te doći do povjerljivih informacija ili pak potpuno onemogućiti komunikaciju, tako da ova sigurnosna prijetnja utječe na sve tri karakteristike sustava povjerljivost, integritet i dostupnost, a to se može vidjeti iz slike 10.



Slika 10. Primjer *Registration Hijacking* napada [15]

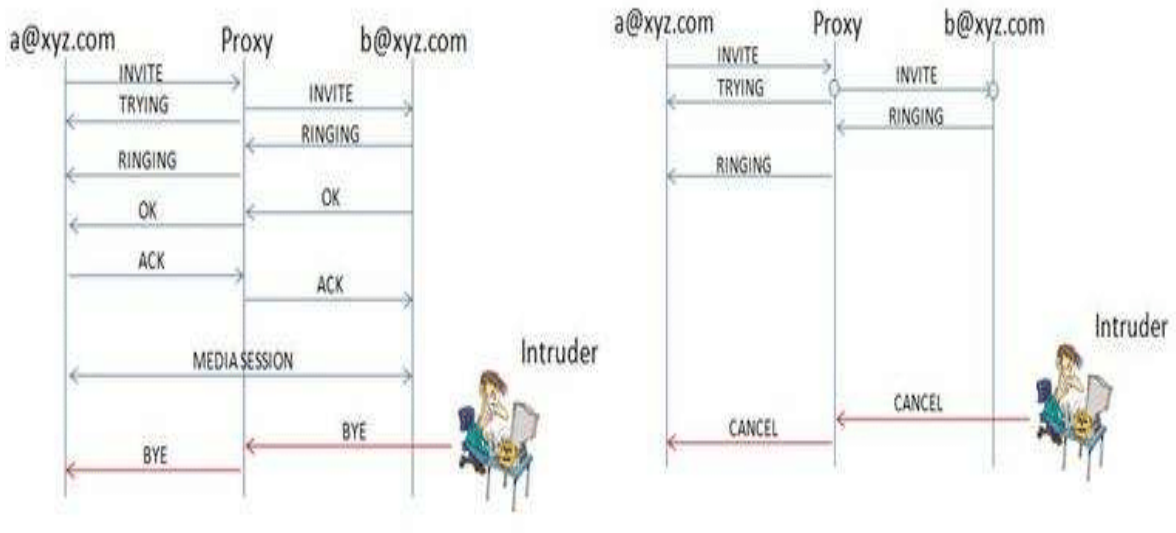
Media Gateway Control Protocol -MGCP *Hijacking* je kao i u prethodnom slučaju vrsta napada kojom se „otima“ komunikacija, samo se u ovom slučaju napada MGCP komunikacijski protokol za signalizaciju i kontrolu poziva. Ovaj protokol služi za kontrolu protoka medijskih zapisa iz mreža s IP protokolom kao što je slučaj u VoIP tehnologiji prema javnoj telefonskoj mreži PSTN. Kao i kod sigurnosne prijetnje otimanja registracije ova prijetnja ugrožava povjerljivost, integritet i dostupnost sustava, odnosno same komunikacije jer kada napadač „otme“ neku od procedura ovog protokola on zapravo ima kontrolu nad cijelim protokolom tj. odvijanjem komunikacije između IP telefona ili drugog uređaja s mogućnostima telefoniranja putem VoIP tehnologije i standardnog telefona koji se koristi u javnoj telefonskoj mreži.

Message modification ili prevedeno napad promjenom sadržaja poruke je napad kojim napadač nastoji sebi prisvojiti podatke koji se izmjenjuju tokom komunikacije. Informacije tj. podatci se šalju mrežom u obliku paketa. Svaki paket se sastoji od zaglavlja i podataka koji se šalju, a zaglavlje paketa se sastoji od više zaglavlja pojedine razine i služi tome da kada se na odredištu zaprimi paket svaki sloj protokola zna što dalje učiniti sa zaprimljenim paketom. Napadač s ovim napadom mijenja podatke u zaglavlju paketa i to najčešće adrese zaglavlja tako da paket s podatcima bude usmjeren na drugu lokaciju ili da se na odredištu ne dobiju ispravne informacije koje su poslane. Na taj način je ugrožena povjerljivost komuniciranja i integritet komuniciranja jer postoji vjerojatnost da komunikacija bude odvijana uz poteškoće.

Spoof via *header* ili *spoofing* pomoću zaglavlja je napad sličan napadu promjene sadržaja poruke jer cilj napadače je izmjena podataka u zaglavlju paketa. Za razliku od prethodnog napada ovdje napadač u zaglavlju maskira svoju adresu tako da sva komunikacija završava kod napadača, a ne na odredištu gdje bi trebala. Ovim napadom

napadač sebi prisvaja informacije koje se šalju na neko odredište, ali je ujedno i onemogućio komunikaciju jer poslana informacija nikada neće doći na odredište već kod napadača.

Cancel / *bye* napad su sigurnosne prijetnje koje se može svrstati u DoS napade iz razloga jer i jedna i druga u konačnici onemogućuju komunikaciju između dva korisnika. Kod *cancel* napada napadač se ubacuje u komunikaciju na samom početku prije nego se komunikacija počela odvijati točnije kod same uspostave poziva. Naime prije nego započne komunikacija dva uređaja trebaju uspostaviti vezu jedan od načina je trostruko rukovanje. Napadač se ubacuje u toku uspostave veze s *cancel* zahtjevom kojim se trenutno prekida nastavak uspostave poziva. Kod *bye* napada komunikacija se već odvija, a napadač se ubacuje s *bye* zahtjevom što rezultira prekidom komunikacije. Ova dva napada su slikovito prikazana na slici 11. I *cancel* i *bye* zahtjevi su normalni zahtjevi u komunikaciji jedan služi da se prekine veza nakon završetka razgovora, a drugi da se prekine uspostava poziva prije nego drugi korisnik odgovori, ali u ovom slučaju ih napadač koristi u zlonamjerne svrhe.

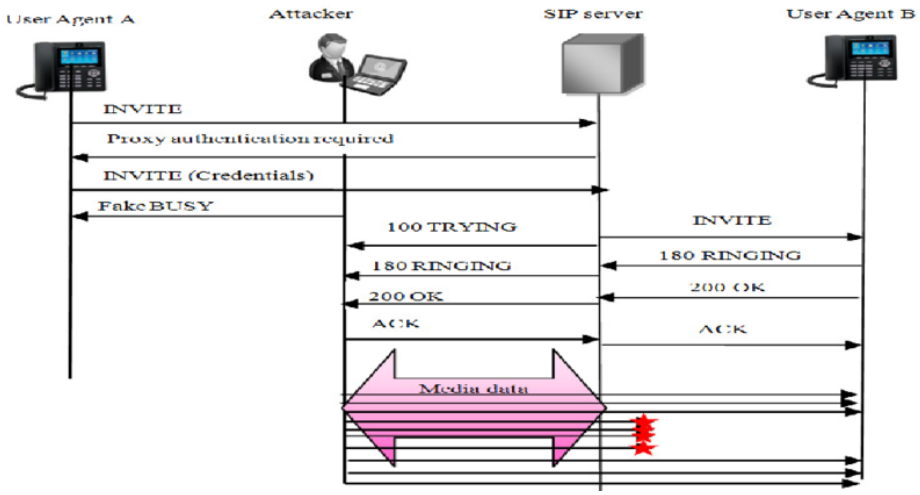


Slika 11. Primjeri BYE I CANCEL napadi [16]

Redirect metoda odnosno napad preusmjeravanjem je sigurnosna prijetnja u kojoj napadač preusmjerava komunikaciju u drugom smjeru. Kod web adresa to bi značilo kada se pokuša pristupiti određenoj web lokaciji uslijed napada budete preusmjereni na neku drugu web lokaciju koja nerijetko ako se radi o računalnom napadu bude zaražena s još nekoliko prijetnji ili nekamo drugo. U svakom slučaju vas preusmjeri na neku stranicu

kojoj niste željeli pristupiti. U VoIP tehnologiji bi to značilo da kada netko želi uspostaviti komunikaciju s drugim korisnikom napadač se ubacuje i preusmjeruje poziv recimo na nepostojeći broj te vam na taj način onemogućuje korištenje usluge ili se pak ubaci kao „čovjek u sredini“ preusmjeravanjem poziva preko sebe te na taj način prisluškuje tijek komunikacije.

Real-time Transport Protocol - RTP *flooding* napad je po svom načinu djelovanja DoS tip napada. Na slici 12 je prikazan primjer ovog napada.



Slika 12. Primjer RTP *flooding* napada [17]

Kao što se vidi iz slike 12 napadač napadom napravi „poplavu“ medijskih podataka koje korisnik na prijemnoj strani ne može obraditi jer se radi o velikoj količini podataka. No prije nego je korisnika na prijemnoj strani „poplavio“ velikom količinom podataka napadač se ubacuje na strani pošiljatelja na način da prilikom procesa uspostave veze pošiljatelju pošalje lažni odgovor da je primatelj zauzet s čim se prekida uspostava veze između pošiljatelja i primatelja, a napadač nastavlja s uspostavom veze s primateljem koja na kraju završava s uspješnim povezivanjem te napadač započne svoj napad na primatelja. Na ovaj način je potpuno onemogućena komunikacija između dva korisnika.

RTP *tampering* je vrsta napada kojim se, nakon što se napadač ubacio u komunikaciju između dva korisnika te osigurao potpunu kontrolu nad komunikacijom naravno bez znanja korisnika, mijenja medijski dio podataka odnosno umjesto izrečenoga govora jednog od korisnika on ubacuje medijski zapis koji je prethodno snimljen tako da osoba koja sluša ne dobije odgovor koji mu je uputio onaj koji odgovara. Na ovaj način s obzirom da napadač ima mogućnost upravljanja razgovorom on ne samo da narušava povjerljivost razgovora nego isti može potpuno onemogućiti.

Encryption napad ili drukčije rečeno kriptografski napad je sigurnosna prijetnja kojom napadač nastoji zaobići sigurnost kriptografskog sustava. Povjerljivi razgovori se obavljaju zaštićivanjem poziva s nekom vrstom enkripcije upravo kako se nebi netko nepoželjan lako ubacio u razgovor i prisluškivao isti. Napadač pomoću postupka kriptoanalize nastoji pronaći slabosti u enkripciji i na taj način se ubaciti u razgovor tj. preuzeti kontrolu nad komunikacijom.

Deafult configuration, prevedeno zadana konfiguracija zapravo nije naziv sigurnosne prijetnje nego meta iste. Naime svi uređaji pa tako i *router* koji se koristi u računalnoj mreži ima svoju zadanu ili kako se drukčije kaže početnu konfiguraciju koje uključuju i lozinku za pristup samom *routeru* radi njegove konfiguracije te lozinku za *wifi* itd. U koliko napadač dođe do tih zadanih postavki određenog uređaja on s lakoćom mijenja postavke samog uređaja i na taj način preuzima kontrolu nad uređajem odnosno u slučaju *routera* kontrolu nad mrežom u kojoj se taj *router* nalazi. Kada napadač to postigne on ima otvorene sve mogućnosti ometanja komunikacije i na koncu i onemogućiti uspostavu komunikacije.

Meta sljedećeg napada su nepotrebne usluge (eng. *unnecessary services*). S obzirom da se u VoIP komunikaciji koriste i računala kao jedan od uređaja za komunikaciju ona su ovim napadom najviše pogođena. Naime usluge koje su meta ovog napada su zapravo programi koji slušaju i reagiraju na mrežni promet. Što je više tih usluga aktivno to napadač ima više mogućnosti za napad, odnosno može „provaliti“ u računalo i preuzeti kontrolu nad njim. Iz tog razloga je potrebno ugasiti sve nepotrebne usluge kako bi se smanjila mogućnost uspješnog napada na računalo te se izgubio nadzor nad njim ili pak da napadač prisluškuje vaš razgovor.

Prekoračenje međuspremnika (eng. *Buffer overflow*) je anomalija kod koje program dok zapisuje podatke u međuspremnik prelazi granice mogućnosti međuspremnika te se podatci prepisuju u susjedna memorijska mjesta. Napadači iskorištavaju upravo ovu anomaliju za svoje napade na određeni uređaj. Napadači naime u tom trenutku ubacuju dodatne zlonamjerne podatke koji mogu sadržavati kod koji će napadnutom programu dati nove upute kojima će program dozvoliti napadaču neovlašten pristup kojim napadač preuzima kontrolu nad napadnutim uređajem, odnosno nad daljnjim radom napadnutog uređaja.

Napad na sustav se može izvesti i napadom na dostupnost *Domain Name System* - DNS-a (eng. DNS *Availability*). Ovdje spadaju sve sigurnosne prijetnje na DNS koji ugrožavaju njegovu dostupnost, odnosno sustava koji se nalazi iza određene domene. Kako

je DNS sustav najlakše rečeno sustav koji prevodi lako pamtljiva imena web lokacija u određenu IP adresu, što je potrebno jer komunikacija na internetu se vrši pomoću IP adresa, napad na takav sustav bi značio nedostupnost svih web lokacija za koje bi DNS trebao odrediti IP adresu. Praktično bi to značilo ako korisnik želi posjetiti web lokaciju skype.com, a nema pristup DNS-u njegovo računalo neće znati na koju IP adresu se treba spojiti i korisniku navedena web lokacija neće biti dostupna, a s obzirom da je u primjeru navedena stranica jednog od poslužitelja VoIP usluge korisniku će biti onemogućena komunikacija putem VoIP tehnologije.

3. MJERE ZAŠTITE KOD VOIP TEHNOLOGIJE

Sada kada se zna koje su to sigurnosne prijetnje koje ugrožavaju siguran rad sustava u VoIP tehnologiji, može se razmatrati koje su to protumjere tim prijetnjama, koje mjere zaštite treba poduzeti da do navedenih napada nebi došlo ili točnije ukoliko dođe do napada da napadač radi dobro odrađene zaštite odustane od svojeg nauma. Prvi korak koji je potrebno učiniti je poduzeti sve mjere u pogledu osnovne zaštite koja zahtjeva od korisnika da u nekakvim vremenskim intervalima odradi određene radnje kako bi digao razinu sigurnosti svoga VoIP sustava. Većinu tih radnji može odraditi korisnik s nekakvim osnovnim poznavanjem računalnih i mrežnih sustava, bez potrebe intervencije stručnjaka.

Nakon osnovne zaštite trebaju se poduzeti mjere zaštite prema specifičnom tipu napada. Kako svaki napad za cilj ima ugrozu jednog, dva ili sva tri parametra sigurnosti u VoIP tehnologiji (povjerljivost, integritet i dostupnost) tako su i nastale mjere zaštite koje štite sustave VoIP tehnologije u pogledu ta tri parametra, odnosno mjere zaštite koje osiguravaju privatnost komunikacije, mjere zaštite koje zadržavaju integritet sustava za komunikaciju te mjere zaštite koje su zadužene da sustavi i usluge za komunikaciju budu uvijek dostupni. Kod ovih dodatnih mjera zaštite korisnici sustava obično trebaju pomoć stručnjaka koji će implementirati te dodatne mjere zaštite i to u pogledu konfiguriranja sustava na način da pruža veću sigurnost od sustava koji je recimo konfiguriran nekakvim početnim postavkama.

3.1. OSNOVNA ZAŠTITA VOIP SUSTAVA

Osnovna zaštita sustava VoIP tehnologije zahtjeva angažman od strane samog korisnika. Pod korisnikom se ne smatra samo pojedinca koji se koristi uslugama koje pruža VoIP tehnologija, već i na organizacije koje u svom radu koriste VoIP tehnologiju za obavljanje komunikacije kako unutar organizacije tako i prema vani. Organizacije se sve češće okreću ugrađivanju VoIP sustava u svoje poslovanje jer im ono u prvom redu osigurava uštede u djelu naknada za telekomunikacijske usluge, a s druge strane jedan takav VoIP sustav za komunikaciju koji poslužuje više korisnika zahtjeva i nekakve dodatne uređaje npr. usmjerivače koji moraju biti i fizički zaštićeni.

Prva u nizu osnovnih mjera zaštita koliko god ona banalno zvučala i koliko god bi se ona treba podrazumijevati pod normalno je redovna obnova lozinki za pristup VoIP usluzi. Nažalost mnoga istraživanja su pokazala porazne rezultate po pitanju lozinki u

pogledu složenosti, učestalosti promjene, te nerijetko se o tome mogu pronaći članci u kojima se može pročitati da su lozinke koje se najčešće „probiju“ sadržaja 123456 ili slično. Korisnici se danas ne žele zamarati sa pamćenjem kompliciranih lozinki i često nisu svjesni u kakvu opasnost se dovode u pogledu da im netko preuzme kontrolu nad uslugom koju koriste, a kvalitetne lozinke su tamo gdje se traže prvi stup obrane od neovlaštenog pristupa. Iz ovog razloga promjena lozinke je navedena kao prva mjera zaštite koju korisnik treba poduzeti da bi se zaštitio, a neke standardne preporuke su da lozinka bude što duža, nekakva preporuka je da sadrži minimalno 12 znakova, te da se kombiniraju sve moguće kombinacije znakova, velika i mala slova, brojevi, interpunkcijski znakovi. Također preporuka je da se lozinke mijenjaju u određenim vremenskim periodima, i to otprilike svakih 6 mjeseci do godinu dana, ili onda kada se sumnja da je lozinka otkrivena te je netko ostvario neovlašten pristup uslugama.

Među sigurnosnim prijetnjama kao jedna od prijetnji je naveden fizički napad. Kako je za ovaj napad potrebna fizička prisutnost odnosno potrebno je imati fizički pristup uređajima koji se koriste u VoIP sustavu zaštita se ostvaruje na način da se taj pristup onemogući neovlaštenim osobama. To je najlakše odraditi na način da se sve kritične komponente VoIP sustava odvoje u posebne prostorije po mogućnosti štićene naprimjer video nadzorom u koje nemaju pristup neovlaštene osobe. Po mogućnosti trebalo bi izbjegavati takozvane *softphone* sustave koje su sačinjeni od osobnog računala, slušalica s mikrofonom i nekog programa kojim je moguća VoIP komunikacija. Sve uređaje kao što su na primjer IP telefoni bi trebalo tako podesiti da ne prikazuju svoje mrežne konfiguracijske informacije.

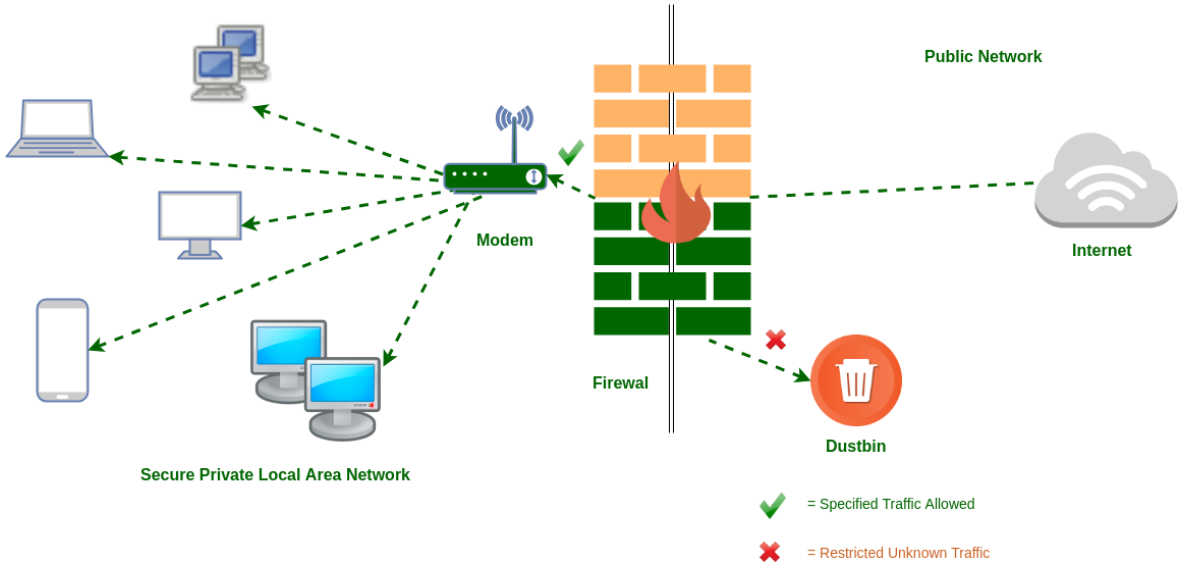
Kao mjera osnovne zaštite može se podrazumijevati i redovno održavanje operativnog sustava i programa koji je koriste za VoIP komunikaciju. To u prvom redu znači redovno instaliranje zakrpa za operativne sustave i programe koji se koriste, jer u većini slučajeva upravo te zakrpe služe da „poprave“ otkrivene nedostatke u pogledu sigurnosnih propusta.

Obavezno korištenje antivirusnih programa podrazumijeva se za one koji komunikaciju obavljaju putem osobnih računala. Također i za antivirusne programe vrijedi da ih treba redovno obnavljati tj. redovno obnavljati definicije virusa, jer kako napadači kreiraju viruse pa možda i na dnevnoj bazi tako treba i nadograđivati antivirusne programe da bi te novo otkrivene viruse mogli zaustaviti prije nego počinu štetu na računalu.

3.2. DODATNA ZAŠTITA VOIP SUSTAVA

Kako je prethodno u radu navedeno svi se napadi u VoIP tehnologiji mogu razvrstati u tri najčešća tipa napada: DoS (otkaz servisa), DDoS (distribuirani otkaz servisa), neovlašteni pristup koji se najčešće ostvaruje napadom „čovjek u sredini“ (eng. *Man in the middle attack*).

Prva mjera zaštite koja se treba koristiti od ova tri napada je postavljanje vatrozida (eng. *firewall*). Zadatak vatrozida je filtriranje mrežnog prometa kako bi se stvorio sigurniji okoliš u samoj mreži, a to obavlja na način da određenom programu koji želi pristupiti na internet to omogući ili onemogući, odnosno kontrolira sve dolazne i odlazne podatke na računalu. Kontrola se obavlja provjerom paketa koji se šalju mrežom dali određeni paketi ispunjavaju određene kriterije kao što su polazne i odredišne adrese, rabljeni protokoli, broj porta koji koriste i drugo. U koliko vatrozid utvrdi da jedan takav paket ispunjava uvjete kriterija on će taj paket pustiti na računalo ili s računala, u koliko ne ispunjava uvjete kriterija taj paket će biti zaustavljen. Na taj način vatrozid blokira neželjene upade iz vani od strane napadača. Slikoviti prikaz vatrozid zaštite se može vidjeti na slici 13.



Slika 13. Slikoviti prikaz vatrozid zaštite [18]

Vatrozid može biti izveden ili kao posebno sklopovlje ili kao programsko rješenje. Kod osobne upotrebe gdje se štiti jedno računalo najčešće se koristi programsko rješenje kao što je Microsoft Windows *Firewall* koji je ugrađen u sam operativni sustav, a pored njega među najpopularnijim su i Zone Alarm *Firewall*, *ComodoFirewall* i drugi. Kod štićenja većih računalnih sustava odnosno većih računalnih mreža kakve najčešće koriste

nekakve organizacije vatrozid zaštita je odrađena u obliku i sklopovskog i programskog rješenja.

Sljedeći način kako se može zaštititi VoIP sustav od napada je da se IP adrese VoIP uređaja odvoje od IP adresa ostalih komponenti koje se koriste u podatkovnoj mreži. To se izvodi na način da se za VoIP komponente koriste privatne IP adrese kako bi se nadalje izvršilo odvajanje IP telefonije od podatkovne mreže. Kada zbog nekih zahtjeva komunikacije dođe do potrebe mrežne konekcije između VoIP-a i podatkovne mreže potrebno je implementirati NAT (eng. *Network Address Translation*). NAT je metoda pretvaranja IP adrese koja se koristi u jednoj mreži u IP adresu koja se koristi u drugoj mreži. Konkretno u ovom slučaju služi da prevede javne IP adrese u privatne te na taj način odvoji interna računala od vanjske mreže. NAT bi trebalo ugraditi na dodirnim točkama VoIP-a i ostalih mreža. Na ovaj se način pod uvjetom da je NAT ispravno konfiguriran postiže dodatna sigurnost koja će napadaču onemogućiti skeniranje VoIP mreže u potrazi za sigurnosnim propustima.

Također jedan od čestih napada u VoIP tehnologiji je napad čovjek u sredini koji među ostalim omogućava prisluškivanje razgovora između dva ili više korisnika ovisi dali se radi o konferencijskom pozivu. Kao logična pretpostavka se nameće da bi se kao najefikasnija zaštita od prisluškivanja mogla koristiti nekakva metoda šifriranja poziva. Šifriranje nije neka novost u svijetu pogotovo u vojnoj industriji gdje se šalju jako povjerljive strateške informacije. U VoIP tehnologiji se za to koristi enkripcija i to gdje god je to moguće i izvedivo. Jedan od načina kako se to može izvesti je korištenjem *Virtual Private Network* - VPN-a. VPN je naziv za računalnu mrežu koja spaja udaljene mreže koristeći se javnim komunikacijskim mrežama kao što je Internet. VPN pruža sigurnost od napada i od prisluškivanja pomoću šifriranja i tunelskih protokola. Dobra strana VPN-a je to što kada se jednom uspješno uspostavi, ona je zaštićena od neovlaštenih pristupa dok su god enkripcijske tehnike sigurne. Da bi se netko od udaljenih korisnika mogao spojiti na lokalnu mrežu mora proći proces autentifikacije, koja mora biti dobro kriptirana kako nebi došlo do krađe podataka te iskorištavanja istih od strane napadača. Kako je rečeno za sigurnost kod VPN-a se brinu među ostalim tunelski protokoli koji služe za udaljeni nadzor i udaljeni pristup komponentama VoIP sustava, a kao preporuka često se može vidjeti je IPsec protokol.

IPsec je protokol koji se koristi u internet sloju, a on koristi dva neovisna protokola AH (eng. *Authentication Header*) protokol i ESP (eng. *Encapsulating Security Payload*) protokol. AH protokol služi za osiguranje integriteta, autentikacije i neporecivosti, dok

ESP protokol uz ovo navedeno osiguraje i tajnost podataka koji se prenose. Oba ova protokola omogućuju dva načina rada: IPsec transportni način rada i IPsec tunelski način rada. Kod enkripcije se preporuča korištenje tunelskog načina rada iz razloga jer tuneliranje maskira izvorišnu i odredišnu IP adresu.

Kao još jedna mjera zaštite VoIP sustava koristi se metoda virtualnih LAN-ova. Virtualni LAN-ovi ili virtualne lokalne mreže služe za odvajanje VoIP sustava od ostalih podatkovnih mreža. VLAN (eng. *Virtual Local Area Network*) predstavlja skupinu računala, odnosno VoIP komponenti koje sačinjavaju jednu ili više odvojenih mreža, a koje su konfigurirane tako da im je omogućena međusobna konfiguracija. Ovo je moguće zahvaljujući VLAN tehnologiji pomoću koje je moguće logičko grupiranje korisnika, neovisno o njihovoj fizičkoj lokaciji, u manje logičke cjeline. VoIP mreža se odvaja od podatkovnih mreža kako bi se spriječili DoS napadi, odnosno prisluškivanje paketa koji putuju podatkovnom mrežom. Ono što je također dobro za karakteristike VoIP sustava je to što se odvajanjem VoIP mreže u kojoj se taj sustav nalazi smanjuje natjecanje za mrežnim resursima. To bi značilo da će VoIP mreža imati dovoljno resursa da neće dolaziti do kašnjenja u prijenosu ili će se vrijeme kašnjenja značajno smanjiti, a možda najbitnija karakteristika u glasovnoj komunikaciji je ta da se razgovor odvija u realnom vremenu, a s ovom metodom se ta karakteristika nastoji što više poboljšati.

4. ZAKLJUČAK

Svakim danom napadači koji su očito vrhunski informatičari nastoje „nadmudriti“ sustave zaštite koji se primjenjuju osmišljavanjem i razvojem novih načina napada, a s druge strane se nalaze također vrhunski informatičari čiji je cilj detektirati te nove prijetnje te razviti mjere zaštite od istih. Kao što je rečeno jedni i drugi su vrhunski stručnjaci na području informatičkih znanosti neki školovani, a neki možda i samouki, ali ona bitna razlika između njih je u namjerama odnosno ciljevima u koje žele utrošiti svoje znanje i mogućnosti.

Ako se zanemari tko je i zašto je nešto napravio, i uđe se u samu srž problematike može se zaključiti da napadači ostvaruju svoje ciljeve na tri načina. Prvi način za koji se može reći da napadač ostvari svoj cilj je neopreznost korisnika koji se služe uslugama VoIP tehnologije. Svi oni koji se koriste uslugama općenito na internetu, moraju biti svjesni da postoje i oni koji ne koriste mogućnosti interneta samo u pozitivne svrhe, kao što su komunikacija, obavljanje poslova, razonodu i slično. Iz tog razloga svi korisnici bilo kakvih usluga na internetu pa tako i u VoIP tehnologiji obavezno se moraju pridržavati onih osnovnih mjera zaštite koje su navedene u ovome radu. U suprotnom napadači će iskoristiti tu opuštenost, neopreznost, u nekim slučajevima i manjak znanja, pa čak može se reći i lijenost korisnika te će uspjeti u svome naumu da dođu do njima korisnih informacija, da preuzmu kontrolu nad korisnikovim uslugama i na taj način dođu do svojih ciljeva.

Drugi način kojeg napadači koriste je manjkavost odnosno nekakve rupe u sustavima koji se koriste za komunikaciju u VoIP tehnologiji. Te manjkavosti najčešće nastaju lošom konfiguracijom uređaja koji se koriste u sustavu za komunikaciju. Ono osnovno što se treba učiniti je izvršiti konfiguraciju uređaja tako da postavke koje su podešene u uređaju nisu one početne koje dođu s uređajem, nego ih treba prilagoditi zahtjevima sustava u koji se ugrađuju i u postavkama onemogućiti dijelove sustava koji se ne koriste, a mogu biti meta napada da bi se na koncu preuzela kontrola nad cijelim sustavom. Tu se u prvom redu misli na nepotrebne servise koji mogu biti ugrađeni u neki sustav. Svaki servis tj. program kao što je rečeno sluša i reagira na mrežni promet. Upravo tu napadač napada i ulazi u komunikaciju sa servisima koji se ne koriste i preko njih ostvaruje kontrolu nad sustavom. Postavlja se jednostavno pitanje pa čemu onda da ti servisi budu aktivni i budu svojevrsni stražnji ulaz (stražnji ulaz iz razloga jer te servise

nitko ne nagleda jer se ne koriste) napadaču. Iz tog razloga preporuka je da se angažira stručnjaka koji će izvršiti pravilnu konfiguraciju uređaja u sustavu, jer ako netko tko nema dovoljno znanja za to ide na svoju ruku sam nešto pokušavati učiniti, zapravo će učiniti više štete nego koristi.

I treći način kojeg napadači koriste barem se tako da zaključiti analizom napada je taj da koriste redovne procedure pojedinih protokola. Naime načinom na koji se odvijaju *flooding* napadi, u radu ih je navedeno nekoliko kao što su TCP *flooding* napad, UDP *flooding* napad, ICMP *flooding* napad itd., do uspješno izvedenog napada dođe upravo zato jer meta napada, bilo da je to neki poslužitelj ili neki od korisnikovih uređaja, nastoji zadovoljiti procedure protokola koji je napadnut. Odnosno meta napada pokušava odgovoriti na sve pristigle zahtjeve jer je to ispravan slijed događanja. Napadači su iskoristili te „dužnosti“ mete napada na način da su se ubacili u komunikaciju i poplavili tu metu sa toliko zahtjeva da ih ovaj ne može odgovoriti i jednostavno prekine s radom. Od ovakve vrste napada se može zaštiti jedino da se nastoji doskočiti napadaču da se ne uspije ubaciti u tu komunikaciju kojom se odvijaju procedure određenog protokola. Ono što je nažalost činjenica je to da su protokoli takvi kakvi jesu i njihove procedure su takve kakve jesu i uvijek postoji mogućnost da kada se uspije spriječiti jedna vrsta napada na njih napadači će, samo je pitanje vremena, naći neki novi dio protokola koji je ranjiv i preko kojeg mogu izvršiti napad na ciljanu metu.

Iz svega navedenog na kraju se nameće konačni zaključak da je činjenica da sigurnosne prijetnje postoje i da je za njih nađeno rješenje u obliku mjera zaštite, ali ono na šta se nikad ne smije zaboraviti je da napadači nikad ne miruju, oni uvijek pokušavaju naći neku novu vrstu sigurnosne prijetnje, pa se logično tome ne smije se niti prestati tražiti nove mjere zaštite u nastojanju da se preduhitre eventualne nove sigurnosne prijetnje, a također tako treba se redovno pridržavati postojećih mjera zaštite kako nebi postali žrtva neke od već postojećih sigurnosnih prijetnji.

LITERATURA

[1] Delač, Z.: *VoIP sigurnost, rizici, zaštita*, Dictus d.o.o., Zagreb, 2010. http://www.dictus.hr/strucni-clanci/EIS2012_S4_TK-7_ZDelac.pdf

[2] Miljanović, D.: *Sigurnost VoIP-a (opasnosti, mjere, riješenja)*, 14. Telekomunikacioni forum TELFOR, Beograd, 2006. http://www.telfor.rs/telfor2006/Radovi/02_TM_07.pdf

[3] Budigere, K.: *Defending against common attacks in SIP*,Aalto University, Espoo – Finska, 2010. https://www.researchgate.net/publication/309148470_Defending_against_common_attacks_in_SIP

[4] CarnetCert i LS&S: *Sigurnosni aspekti VoIP tehnologije*, Nacionalno središte za sigurnost računalnih mreža i sustava, Zagreb, 2006. https://www.cert.hr/wp-content/uploads/2006/06/CCERT-PUBDOC-2006-03-151.pdf

[5] McGann, S.; Sicker, D.C.: An analysis of security threats and tools in SIP – based VoIP systems,University of Colorado at Boulder, SAD, https://startrinity.com/VoIP/Resources/sip371.pdf

[6] CarnetCert i LS&S: *IPsec*, Nacionalno središte za sigurnost računalnih mreža i sustava, Zagreb, 2004 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-01-58.pdf

[7] https://en.wikipedia.org/wiki/Denial-of-service_attack (pristupljeno 08.08.2019.)

[8] https://www.ionos.com/digitalguide/server/security/arp-spoofing-attacks-from-the-internal-network/ (pristupljeno 09.08.2019.)

[9] https://www.jannet.hk/en/post/mac-address-table-attack/ (pristupljeno 09.08.2019.)

[10] https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/ (pristupljeno 11.08.2019.)

[11] https://en.wikipedia.org/wiki/SYN_flood (pristupljeno 13.08.2019.)

[12] https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/ (pristupljeno 13.08.2019.)

[13] https://www.sciencedirect.com/science/article/pii/S0045790612001140 (pristupljeno 14.08.2019.)

[14] https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/ (pristupljeno 14.08.2019.)
[15] https://flylib.com/books/en/2.351.1.106/1/ (pristupljeno 17.08.2019.)
[16] https://www.researchgate.net/figure/BYE-Attack-and-Cancel-Attack_fig2_309148470 (pristupljeno 18.08.2019.)
[17] https://www.researchgate.net/figure/An-example-RTP-flooding-attack_fig1_306067949 (pristupljeno 18.08.2019.)
[18] https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/ (pristupljeno 20.08.2019.)

POPIS SLIKA

POPIS TABLICA

POPIS KRATICA

IP (eng. *Internet protocol*)	-	Internetski protokol
VoBB(eng. *Voice over broadband*)	-	Kratica za slanje glasovnih poruka putem široko pojasne mreže
VoIP (eng. *Voice over Internet Protocol*)	-	Protokol za slanje glasovnih poruka putem interneta
DSL (eng. *Digital Subscriber Loop*)	-	Digitalna pretplatnička petlja
DoS (eng. *Denial of Service*)	-	Otkaz servisa
DDoS (eng. *Distributed Denial of Service*)	-	Distribuirani otkaz servisa
ARP (eng. *Address Resolution Protocol*)	-	Komunikacijski protokol
MAC (eng. *Media Acces Control*)	-	Kontrola pristupa mediju
TCP(eng. *Transmission Control Protocol*)	-	Protokol kontrole prijenosa
UDP(eng. *User Datagram Protocol*)	-	Datagram protokol korisnika
ICMP(eng. *Internet Control Message Protocol*)	-	Protokol poruka u internetskoj kontroli
TFTP (eng. *Trivial File Transfer Protocol*)	-	Jednostavan protokol za prijenos datoteka
DHCP (eng. *Dynamic Host Configuration Protocol*)	-	Protokol za dodjeljivanje IP adresa i ostalih mrežnih postavki
MGCP (eng. *Media Gateway Control Protocol*)	-	Komunikacijski protokol za kontrolu signalizacije i upravljanja pozivima
RTP(eng. *Real-time Transport Protocol*)	-	Mrežni protokol za isporuku zvukova i videa putem IP mreže
SDP (eng. *Session Description Protocol*)	-	Protokol za opis komunikacijskih parametara strimanog medija
DNS (eng. *Domain Name System*)	-	Domenski sustav imena
NAT (eng. *Network Address Translation*)	-	Metoda pretvaranja IP adrese
VPN (eng. *Virtual Private Network*)	-	Virtualna privatna mreža
VLAN (eng. *Virtual Local Area Network*)	-	Virtualna lokalna mreža
AH (eng. *Authentication Header*)	-	Sigurnosni protokol
ESP (eng. *Encapsulating Security Payload*)	-	Sigurnosni protokol