Sigurnost primjene telekomunikacijskih mreža

Deak, Ema

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Ema Deak

SIGURNOST PRIMJENE TELEKOMUNIKACIJSKIH MREŽA

ZAVRŠNI RAD

Zagreb, 2015.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

SIGURNOST PRIMJENE TELEKOMUNIKACIJSKIH MREŽA

SECURITY OF TELECOMMUNICATIONS NETWORKS

Mentor: Ivan Forenbacher, dipl. ing.

Studentica: Ema Deak, 0135229527

Zagreb, rujan 2015.

SIGURNOST PRIMJENE TELEKOMUNIKACIJSKIH MREŽA

SAŽETAK

Veliki broj telekomunikacijskih usluga, uključujući *Voice over IP* (VoIP) i *Short Message Service* (SMS), dostupno je korisniku kontinuirano ako postoji odgovarajuća razina pokrivenosti mrežom. Arhitektura telekomunikacijske mreže i dostupne telekomunikacijske usluge su ranjive i podložne raznim zlonamjernim napadima, poput *Denial of Service* (DoS), *phishing* i presretanje poziva. Zbog toga, spomenute usluge zahtijevaju stalnu zaštitu od zlonamjernih napada. Cilj ovog rada je razraditi važnost primjene sigurnosnih mehanizama, zaštite informacija i podataka, i sigurnosnog programa na temelju potencijalnih mrežnih napada. Rezultati sugeriraju da je zaštitu moguće provesti na nekolika načina, pomoću raznih sigurnosnih mehanizama kao što je *cyber* zaštita, fizička zaštitu, kriptografija i vatrozid. Na temelju rezultata, pružen je i pregled osnovnih budućih sigurnosnih smjernica i preporuka kao pomoć u anticipiranju ranjivosti i napada koji proizlaze dolaskom novih tehnologija.

KLJUČNE RIJEČI: sigurnost; arhitektura mreže; zaštita; usluge; buduće smjernice; sigurnosne preporuke

SECURITY OF TELECOMMUNICATIONS NETWORKS

SUMMARY

A large number of telecommunication services, including Voice over IP (VoIP) and Short Message Service (SMS) are available and accessible to user continuously if there is an appropriate level of network coverage. The telecommunication network architecture and enabled telecommunication services are vulnerable and susceptible to a wide variety of malicious attacks, such as Denial of Service (DoS), phishing and call interception. As a result, these services requireconstant protection from malicious attacks.The focus of present paper is to discuss the importance of applying security mechanisms, protecting information and data, and creating security program based on potential network attacks. Results suggest that protection can be implemented with diverse security mechanisms, including cyber protection, physical protection, cryptography, and firewall. Based on the results, an overview on main future directions and security recommendations is provided to help prevent vulnerabilities and attacks emerging with new technologies.

KEY WORDS: security; network architecture; protection; services; future directions; security recommendations

SADRŽAJ

1. Uvod 1

2. Osnove sigurnosti u telekomunikacijama 3

2.1. Važnost primjene sigurnosnih mehanizama 3

2.2. Aktivnosti korisnika 4

2.3. Zaštita informacija kroz temeljne zahtjeve 5

2.4. Napadi i izrada sigurnosnog programa 6

3. Arhitektura telekomunikacijskih mreža i usluge 9

3.1. Povijest mobilnih mreža 9

3.2. Mobilne mreže za prijenos govora 11

3.2.1. Komponente mreže za prijenos govora 12

3.2.2. Prekapčanje 13

3.2.3. VoIP usluga 13

3.3. Mobilne mreže za prijenos podataka 14

3.3.1. Komponente mreže za prijenos podataka 14

3.3.2. SMS usluga 16

3.4. SS7 signalizacijska mreža 16

3.4.1. Arhitektura 16

3.4.2. Protokolni složaj 17

4. Sigurnosne prijetnje i ranjivosti telekomunikacijskih mreža 19

4.1. Prijetnje i ranjivosti u VoIP-u 20

4.2. Prijetnje i ranjivosti u SMS-u 23

4.3. Prijetnje i ranjivosti u SS7 mreži 25

5. Zaštita telekomunikacijskih mreža 28

5.1. Cyber (web) i fizička zaštita 28

5.2. Kriptografija 29

5.2.1. Simetrična kriptografija 31

5.2.2. Asimetrična kriptografija 31

5.3. Mehanizmi zaštite 32

5.3.1. Autentikacija zasnovana na korisničkom imenu i lozinci 32

5.3.2. Autentikacija zasnovana na simetričnoj kriptografiji 33
5.3.3. Autentikacija zasnovana na asimetričnoj kriptografiji 33
5.3.4. Digitalni potpis 33
5.3.5. Message digest 34
5.4. Vatrozidi 34
6. Buduće smjernice i sigurnosne preporuke 37
6.1. Buduće smjernice 37
6.2. Sigurnosne preporuke 38
6.2.1. Sigurnosna politika 38
6.2.2. Analiza rizika 39
6.2.3. Alati 40
6.2.4. Kontrola korisničkog pristupa 41
7. Zaključak 42
Literatura 43
Popis kratica 45
Popis slika 48
Popis tablica 49
Popis grafikona 50

1. Uvod

Sigurnost u telekomunikacijskim mrežama pojam je s kojim se svakodnevno susreće veliki broj korisnika, koji koriste sve više informacija na sve više načina. Prijenos informacija vrši se otvorenim i nesigurnim komunikacijskim kanalom, kojeg je nemoguće fizički zaštititi pa se sigurnost takvog sustava može lako narušiti. Zbog navedenih činjenica, sigurnost i zaštita nad telekomunikacijskim mrežama postaju važni pojmovi kako bi se omogućio pouzdan prijenos informacija.

Naslov završnog rada je *Sigurnost primjene telekomunikacijskih mreža*, a cilj je detaljno opisati i objasniti pojam sigurnosti u telekomunikacijskim mrežama s obzirom na to da mnogi korisnici obraćaju malu ili gotovo nikakvu pozornost na sigurnost i zaštitu prilikom razmjene informacija. Završni rad sastoji se od sedam cjelina kako slijedi:

1. Uvod
2. Osnove sigurnosti u telekomunikacijama
3. Arhitektura telekomunikacijskih mreža i usluge
4. Sigurnosne prijetnje i ranjivosti telekomunikacijskih mreža
5. Zaštita telekomunikacijskih mreža
6. Buduće smjernice i sigurnosne preporuke
7. Zaključak

Poglavlje *Osnove sigurnosti u telekomunikacijama* obuhvatit će važnost primjene sigurnosnih mehanizama, najčešće aktivnosti korisnika, temeljne sigurnosne zahtjeve, kada dolazi do napada na mrežu i kako bi trebao izgledati sigurnosni program.

Treće poglavlje odnosi se na arhitekturu telekomunikacijskih mreža, gdje će se nakon povijesnog pregleda analizirati mreža za prijenos govora, mreža za prijenos podataka i SS7 (Signalling System No. 7) signalizacijska mreža. Usluge koje će također biti spomenute u istom poglavlju odnose se na VoIP (Voice over IP) i SMS (Short Message Service) uslugu.

Poglavlje *Sigurnosne prijetnje i ranjivosti* nadovezat će se na prethodno poglavlje pri čemu će se opisati prijetnje i ranjivosti VoIP i SMS usluge, te SS7 mreže.

Peta cjelina obuhvaća načine zaštite telekomunikacijskih mreža, odnosno cyber i fizičku zaštitu, kriptografiju, mehanizme zaštite i vatrozide.

U šestom poglavlju budućim smjernicama opisat će se u kojim dijelovima telekomunikacijske mreže je potrebno provesti mehanizme zaštite, a pod preporukama će se analizirati sigurnosna politika, analiza rizika, alati i kontrola pristupa.

Kao temeljno polazište upotrebljena je knjiga *Security for Telecommunications Networks*, autora Traynor, McDaniel i La Porta, uz koju su se koristili i Internet izvori: članci, knjige i autorizirana predavanja.

2. Osnove sigurnosti u telekomunikacijama

Informacija je važno sredstvo komuniciranja. U poslovnim aktivnostima, informacija često predstavlja jedan od najvažnijih segmenata kojeg tvrtka posjeduje i koji pomaže u uspješnosti pojedine tvrtke u usporedbi s drugim tvrtkama. Podaci se svrstavaju u različite kategorije kako bi se kontrolirao pristup informacijama na različite načine, ovisno o samoj važnosti, osjetljivosti na krađu i zlouporabu te druge čimbenike.

Stalni porast telekomunikacijskih mreža u svijetu i njihova integracija s ostalim mrežnim tehnologijama kao što je Internet, dovodi do općenitog povećanja međusobnog povezivanja. Tradicionalne i moderne mrežne usluge dostupne su gotovo svakom korisniku, pa tako i Internet koji također omogućuje globalne mrežne usluge kao što su: web pregledavanje, e-mail, daljinsko umrežavanje, video-konferencija, e-commerce, multicast distribucija sadržaja, prijenos govora putem IP-a (Internet Protocol), itd. Isto tako, važno je naglasiti popularnost bežičnih mreža s obzirom na to da poboljšane verzije 2G (druga generacija), a samim time 3G (treća generacija) i 4G (četvrta generacija) mobilnih komunikacijskih sustava podržavaju mobilne/bežične Internet usluge. Osim usluga za prijenos govornih informacija, mobilne mreže podržavaju gotovo sve druge usluge bazirane na Internetu.

2.1. Važnost primjene sigurnosnih mehanizama

Sigurnost u telekomunikacijskim mrežama najčešće se odnosi na problem zaštićenog prijenosa podataka samom mrežom i identifikaciju entiteta odnosno korisnika koji sudjeluju u razmjeni podataka [9]. Sustav kojim se prenose informacije je prije svega ranjiv. Ranjivošću se smatra sigurnosna slabost i nedostaci. Telekomunikacijska mreža kao sustav ne vodi računa o sigurnosti, već je potrebno uvesti brojne mehanizme i načine kako bi se osigurali i zaštitili podaci. U prošlosti su napadi na mrežu bili mnogo rjeđi nego što je to danas, iz razloga jer se gotovo svaka nova tehnologija temelji na IP-u.

Danas, svaka tvrtka želi unaprijediti poslovanje s klijentima, dobavljačima i poslovnim partnerima u cilju širenja i mogućnosti povećanja prihoda. Web stranice predstavljaju idealno rješenje za povezivanje tvrtke s potencijalnim korisnicima. Sigurnost predstavlja važan parametar jer daje uvid u situaciju koja se odvija na mreži, a samim time i u ono što se događa u poduzeću. Slaba sigurnost pokazuje brojne nedostatke jer poduzeća nisu svjesna protoka informacija na njihovoj infrastrukturi. Kontrola informacija predstavlja prednost jer

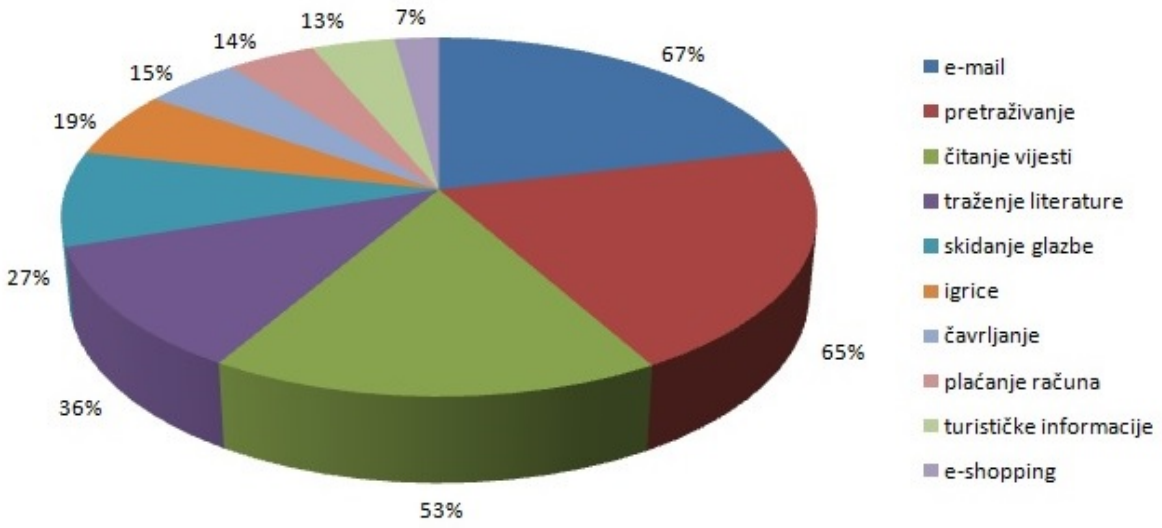
se tako olakšavaju nove poslovne mogućnosti i poslovni procesi zahtijevaju manje resursa kad se prijenos informacija obavlja učinkovito i sigurno.

Moderne sigurnosne preporuke nastoje smanjiti troškove, poput onih koji proizlaze iz gubitka podataka ili opreme. Gubitak podataka zbog nepravilnog rukovanja, zlouporabe ili greške može uzrokovati velike troškove, kao što i virusi, zastoj web stranice ili uskraćivanje usluge dovode do nemogućnosti kupovanja od strane korisnika i nemogućnosti obavljanja posla od strane tvrtke. Ako određeni sigurnosni incident dospije u javnost, može ugroziti ugled tvrtke isto kao i gubitak klijenata. Ciljevi napada su često krađa financijskih podataka ili intelektualnog vlasništva. Gubitak usluga ili „curenje“ podataka dovodi do novčanih gubitaka, povećanja naknade, smanjenje cijene dionica i sl. Jak sigurnosni sustav smanjuje gubitak podataka i povećava dostupnost usluga i povjerljivost.

Mobilni komunikacijski sustavi koji omogućuju obavljanje poziva, nastoje na što efikasniji način spriječiti mogućnost podvale i prevare korisnika, a samim time i operatera koji pružaju razne usluge. Isto tako je vrlo važno održati zadovoljavajuću kvalitetu usluge, bez da je pritom narušena sigurnost. Protivnik je svaki entitet koji pokušava narušiti kvalitetu i sigurnost, upoznat je s ponašanjem sustava i sposoban je definirati na kojem dijelu mrežnog resursa je najmanja pouzdanost. Dakle, za sustav se može reći da je siguran samo ako je sposoban spriječiti protivnika da učini štetu tijekom prijenosa različitih vrsta informacija putem komunikacijskog kanala. Naravno, u praksi je nemoguće zaštititi se od svih mogućih protivnika, tzv. sveprisutnih protivnika koji mogu spriječiti sustav da pravilno izvodi sve potrebne radnje za prijenos informacija. Prema tome, sigurnost se temelji na racionalnom projektiranju telekomunikacijske mreže i predviđanju kako će se potencijalni protivnik ponašati, odnosno koje su moguće prijetnje koje on nastoji ostvariti [3].

2.2. Aktivnosti korisnika

Korisnicima su omogućene brojne usluge i pogodnosti u kojima dolazi do razmjene informacija. Graf 1 prikazuje najčešće aktivnosti korisnika. Najveći broj korisnika služi se komunikacijskim kanalom kako bi razmijenili e-mail poruke i pretraživali Internet. Također veliki broj populacije čita vijesti ili traži literaturu. Zanimljiva činjenica je mali postotak korisnika koji obavlja e-shopping i e-bankarstvo. Razlog tome zasigurno leži u sigurnosti, odnosno transakcijama koje zahtijevaju pristup bankovnom računu. Većina korisnika nema povjerenje u ovakav način korištenja pojedinih usluga.



Graf 1. Aktivnosti korisnika. Podaci od [13]

2.3. Zaštita informacija kroz temeljne zahtjeve

Prema izvoru [9] sigurnost se može preciznije definirati kroz zahtjeve koje zaštićeni oblik informacije mora zadovoljiti, a to su:

- povjerljivost prenošene informacije
- autentičnost pošiljatelja
- integritet
- raspoloživost usluge i
- neporecivost obavljene transakcije

Isti izvor kaže kako povjerljivost podrazumijeva da pohranjene i poslane informacije mogu čitati samo entiteti kojima su te informacije namijenjene. Dakle, nedopustivo je razumijevanje i čitanje informacija bilo kome osim pošiljatelju i primatelju. Pojam povjerljivosti često je upitan kada se radi o korisniku i pružatelju usluga. Naime, korisnici žele da su njihovi podaci dostupni samo onim entitetima koji za to imaju ovlasti. Pružatelji usluga također nastoje spriječiti pristup korisničkim podacima, međutim prema određenim zakonima oni trebaju dijeliti takve informacije da bi se omogućilo efikasno upravljanje mrežom.

Autentičnost pošiljatelja odnosi se na identitet pošiljatelja. Primatelj mora biti siguran da su informacije koje je primio poslao upravo onaj pošiljatelj za kojeg se očekuje da ih je

trebao poslati. Zahtjevom autentifikacije onemogućeno je uključivanje treće osobe u prijenos informacija, a u slučaju da do toga dođe, primatelj mora to otkriti. Odgovarajuće metode koriste se ovisno o aplikacijama i uslugama koje se koriste.

Integritet jamči nepromjenjivost informacije prilikom prijenosa. Informacije moraju biti poslane i primljene u izvornom obliku. Mogućnost mijenjanja informacijskog sadržaja imaju isključivo osobe koje za to posjeduju potrebne ovlasti.

Raspoloživost usluge osigurava korisnicima da mogu pristupiti informacijama kada se za to javi potreba, bez obzira na neočekivane događaje kao što su zlonamjerni napadi, nestanak struje i sl.

Neporecivost obavljene transakcije znači da sudionici koji su sudjelovali u komunikaciji ne mogu poreći da su sudjelovali u razmjeni informacija. Bitno je utvrđivanje identiteta korisnika kako bi se dokazalo da su informacije zaista poslane od osobe za koju se smatra da ih je poslala.

Prethodno spomenute zahtjeve moguće je ostvariti primjenom kriptografskih metoda. Knjiga [1] definira kriptografiju kao umijeće tajnog pisanja. U povijesti, kriptografski alati korišteni su u vojne i diplomatske svrhe, no početkom informacijskog doba, informacije i podaci počinju dobivati veliku vrijednost, te se kriptografija počinje primjenjivati na spomenute resurse. Danas postoje moderni kriptografski algoritmi koji štite informacije i podatke koje korisnici najčešće pohranjuju na tvrdi disk računala. Algoritmi koji provode kriptografiju postoje u gotovo svakom elektroničkom uređaju kao što su prijenosna računala, mobilni terminalni uređaji, resursi kabelske televizije i sl. Razvojem telekomunikacijskih mreža i uređaja, potrebno je razvijati i metode zaštite. Kriptografiju je potrebno proučavati u skladu s najnovijim dostignućima u telekomunikacijama. Vrste i način rada kriptografije bit će pobliže opisani u poglavlju Zaštita telekomunikacijske mreže.

2.4. Napadi i izrada sigurnosnog programa

Napadi se javljaju kada protivnik iskorištava ranjivost sustava [3]. U telekomunikacijskim mrežama razlikuju se dvije vrste napada: aktivni i pasivni. Kada je riječ o aktivnom napadu, protivnik mora komunicirati sa sustavom, a to može učiniti tako da šalje lažne poruke, mijenja podatke i/ili sprječava legitimne aktivnosti. Jedina prednost ovakve vrste napada je da korisnik može detektirati čudno ponašanje sustava. S druge strane, pasivni napad ne uključuje direktnu interakciju sa sustavom, već protivnici jednostavno promatraju. Takvi

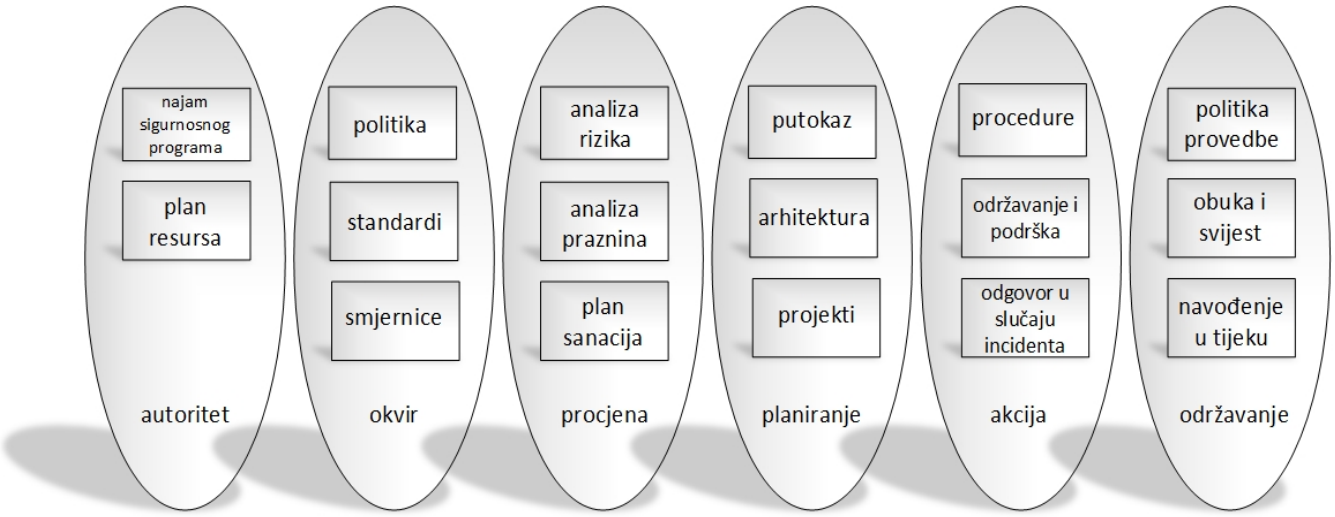
napadi uglavnom se opisuju kao prisluškivanje. Denial of Service (DoS)[1] je podvrsta aktivnog napada, a pokušava se onesposobiti ili smanjiti kvaliteta sustava. Ovakav tip napada obično se javlja na web stranicama.

Važan aspekt koji se u sigurnosti rijetko spominje je povjerenje. Procjena povjerenja jedna je od ključnih stvari za razvoj sigurnosne strategije. Osoba koja obavlja pojedine aktivnosti pod određenim uvjetima treba biti od povjerenja. Isto tako povjerenje može biti pogrešno procijenjeno pa sustav više nije otporan na ciljane napade.

Izvor [2] predlaže izgradnju sigurnosnog programa koji bi za početak trebao opisati što je potrebno i zašto, te definirati kako će se provoditi, kada i pomoću kojih metoda. Kao komponente od kojih bi se izgradio sigurnosni program navode se sljedeće:

- autoritet-sigurnosni program mora uključivati odgovarajuću razinu odgovornosti i autorizacije kako bi bio učinkovit
- okvir-sigurnosni okvir pruža pristup gradnji programa
- procjena-obuhvaća što treba biti zaštićeno, zašto i kako doći do strategije kojom bi se poboljšala sigurnost
- planiranje-definira prioritete i rokove za sigurnosne inicijative
- akcija-odnosi se na sigurnosni tim koji ostvaruje željene rezultate na temelju planova
- održavanje-zadnji stupanj sigurnosnog programa koji nakon uvođenja zahtijeva kontinuirano održavanje

[1] Više o DoS napadima na: https://www.us-cert.gov/ncas/tips/ST04-015



Slika 1. Komponente sigurnosnog programa. Podaci od [2]

Kao što je navedeno, sigurnosni program trebao bi sadržavati: autoritet, okvir, procjenu, planiranje, akciju i održavanje. Slika 1 prikazuje potkomponente sigurnosnog programa koje su karakteristične za svaku pojedinu komponentu. Ovakva struktura funkcionira u srednjim i velikim korporativnim poduzećima. Manje tvrtke mogu pojednostavniti strukturu ili kombinirati komponente ovisno o dostupnosti resursa.

3. Arhitektura telekomunikacijskih mreža i usluge

U suvremenim digitalnim komunikacijskim sustavima, mobilna komunikacija predstavlja najvažniju tehnologiju. Mobilne mreže su osjetljive na neovlašteni pristup, prisluškivanje i ostale sigurnosne probleme koje bi odgovarajući algoritmi trebali riješiti.

Mobilna mreža velikom broju korisnika predstavlja digitalnu konekciju s vanjskim svijetom. Prenosivost uređaja, razumna cijena i dobra pokrivenost značajke su koje čine mobilnu mrežu pristupačnijom u odnosu na Internet s obzirom na usluge koje pruža. Bez obzira na ograničenost usluga koje pruža mobilna mreža, jednako je važno obratiti pozornost na sigurnosne aspekte kao kada se radi o Internetu. Povezanost mobilnih mreža i Interneta, a samim time i shvaćanje sigurnosnih problema moguće je ako se dobro poznaju arhitekture spomenutih sustava.

U ovom poglavlju prikazat će se arhitektura mreže za prijenos govora, arhitektura mreže za prijenos podataka i SS7 (Signalling System No. 7) signalizacijska mreža. Kako bi se u potpunosti razumjele arhitekture spomenutih mreža, potrebno je zakoračiti u povijest mobilnih mreža, odnosno prikazati kako se došlo do današnje arhitekture mobilne mreže. Također je važno spomenuti SS7 protokol čija arhitektura je lako usporediva s Internet protokolom.

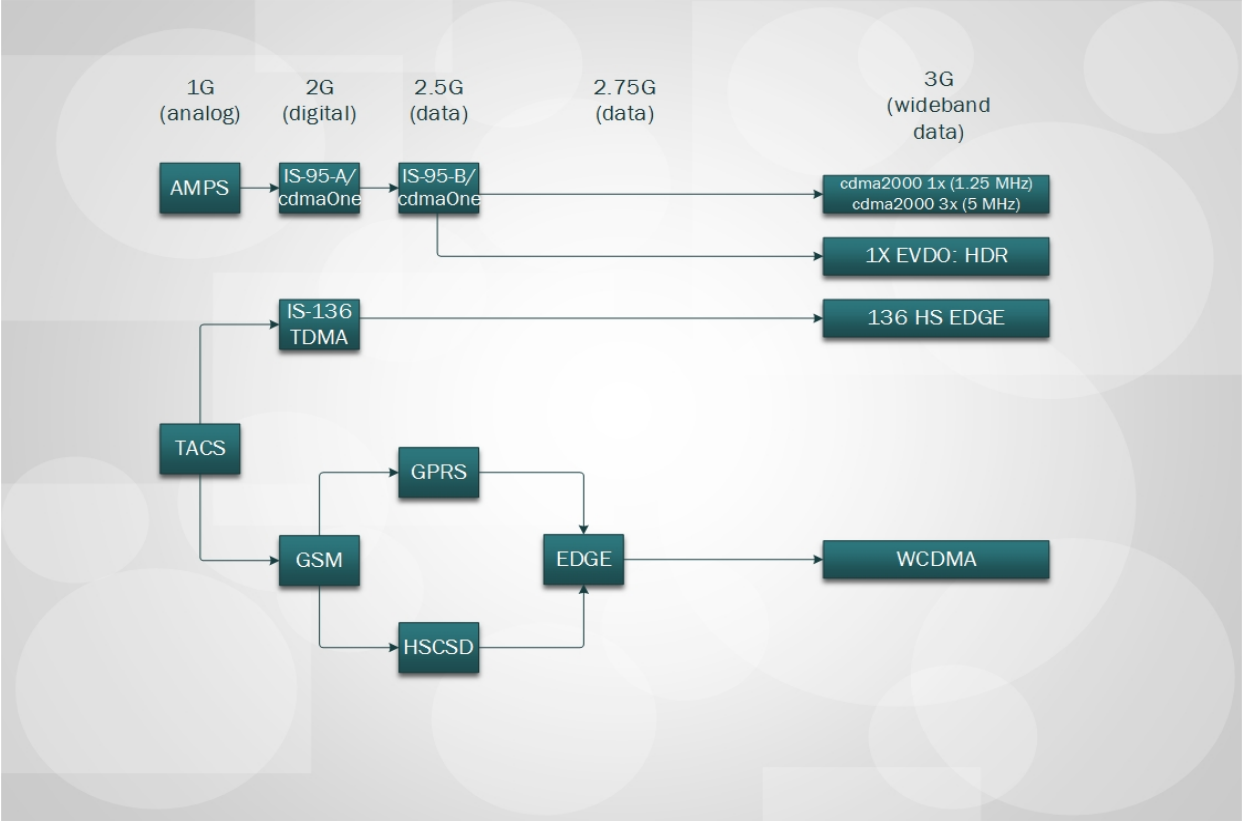
3.1. Povijest mobilnih mreža

Prvi analogni sustavi mobilne telefonije uvedeni su 1980-ih godina. AMPS (Advanced Mobile Phone System) i TACS (Total Access Communication System) sustavi omogućili su korisnicima obavljanje telefonskih razgovora [1]. Sustav je bio segmentiran pomoću FDMA (Frequency-Division Multiple Access), gdje su svakom korisniku bila dodijeljena dva frekvencijska kanala (jedan od bazne stanice prema mobilnom terminalnom uređaju i jedan od mobilnog terminalnog uređaja prema baznoj stanici) kako bi se omogućila potpuna duplex komunikacija. Ovakvi sustavi su neučinkoviti zbog ograničenog kapaciteta, no i dalje su u upotrebi diljem svijeta.

Kako bi se prevladala takva ograničenja, uvedeni su digitalni sustavi početkom 1990-ih godina i većina se još uvijek koristi. Prvi sustavi kombinirani su kao FDMA s TDMA (Time-Division Multiple Access) što znači da je svakom korisniku dodijeljen određeni vremenski okvir (slot) na korištenje za vrijeme trajanja razgovora. Kombinirajući ta dva pristupa, omogućena je ponovna upotreba iste frekvencije, a to ujedno znači dodatno povećanje

kapaciteta. Knjiga [1] kaže kako je GSM (Global System for Mobile Communications) sustav najbolji primjer TDMA pristupa, nastao je u Europi te se koristi u većem dijelu svijeta. U SAD-a se uveo sličan sustav poznat kao IS-136 standard, no početkom 2008. u potpunosti je zamijenjen GSM-om.Važan aspekt spomenutih sustava je uvođenje kontrolnih kanala koji omogućuju razmjenu većih količina informacija između mobilne mreže i mobilnih terminalnih uređaja. Time se postiže mogućnost upotrebe boljih sigurnosnih rješenja i bogatije ponude usluga kao što je SMS (Short Message Service). Paralelno s razvojem TDMA pristupa, razvio se CDMA (Code-Division Multiple Access) pristup kod kojeg je svakom korisniku dodijeljen kôd po kojem se razlikuju informacije pojedinog korisnika.

Nakon uspostavljanja i uvođenja govornih usluga, težište je stavljeno na razvoj mobilnih podatkovnih usluga. Proširenjem GSM standarda uz komutaciju kanala, uvodi se komutacija paketa i taj standard se naziva GPRS (General Packet Radio Service) te omogućuje brzine prijenosa podataka do 10 kbit/s. Kako bi se dodatno povećala brzina prijenosa uvodi se EDGE (Enhanced Data Rates for GSM Evolution) kod kojeg brzine sežu do 200 kbit/s. Iako su teoretski velike brzine prijenosa moguće u 2.5 i 2.75 generaciji mobilnih mreža, korisnik obično osjeti brzinu kao da je spojen sa žičanim dial-up-om. Treća generacija (3G) mobilnih mreža nastoji riješiti taj problem kroz eventualnu uporabu novog spektra i učinkovitijim tehnikama kodiranja. GSM će tako evoluirati u UMTS (Universal Mobile Telecommunications System) i koristit će WCDMA (Wideband CDMA) tehniku višestrukog pristupa. UMTS obećaje veći glasovni kapacitet i multimedijske usluge s brzinom prijenosa do nekoliko desetaka Mbit/s. Američki IS-95 sustavi također koriste uskopojasni CDMA kao dio CDMA2000 standarda. Razvoj opisanih tehnologija prikazan je slikom 2.



Slika 2. Razvoj generacija mobilnih mreža. Podaci od [1]

3.2. Mobilne mreže za prijenos govora

Mobilne mreže za prijenos govora s vremenom su napredovale u odnosu na žične telefonske mreže [1]. Takve mreže koriste vrlo inteligentne switch-eve koji su sačinjeni od iznimno pouzdanih elemenata, koji omogućuju brojne funkcije kao što su usmjeravanje i rezervacija resursa. Kako bi se izgradila mobilna telekomunikacijska mreža switchevi i pomoćni procesori kombiniraju se s dodatnim inteligentnim softverom kako bi se uspješno provela mobilnost korisnika. Upravljanje mobilnošću ima dva ključna cilja: veza preko koje se ostvaruje komunikacija mora biti uspostavljena između dviju krajnjih točaka i usluga mora biti stalno dostupna mobilnim korisnicima. Telefonski switchevi u fiksnoj telefoniji imaju pristup bazama podataka i na temelju toga procesori pružaju uslugu svojim pretplatnicima. U mobilnoj mreži korisnik mora biti lociran prije nego što se ostvari konekcija. Broj mobilnog terminalnog uređaja služi za identifikaciju samog uređaja. S obzirom na to da korisnik može primiti poziv preko raznih switcheva, ovisno o položaju, softveri i profili koji ostvaruju uslugu moraju biti na raspolaganju svim switchevima u mreži. Za postizanje ciljeva mobilne govorne mreže potrebno je objasniti nekoliko elemenata koji čine mrežu.

3.2.1. Komponente mreže za prijenos govora

HLR (Home Location Register) ili registar domaćih korisnika je centralna baza podataka koja sadrži detalje o svakom pretplatniku GSM mreže. To znači da je svaki pretplatnik mobilnog telefona autoriziran da može koristiti jezgrenu mrežu GSM mreže [10]. HLR bilježi podatke o svakoj SIM (Subscriber Identity Module) kartici koja je izdana od mobilnog operatera. Svaka SIM kartica ima jedinstven identifikator koji se naziva IMSI (International Mobile Subscriber Identity) i on predstavlja primarni ključ za svaki HLR zapis. MSISDN (Mobile Station ISDN) je također važan podatak koji se nalazi na SIM kartici, a predstavlja telefonske brojeve koji se koriste od strane mobilnih telefona kako bi mogli ostvariti poziv ili ga primiti. Postoje primarni i sekundarni MSISDN. Primarni služi kako bi se omogućili glasovni pozivi i SMS-ovi, a sekundarni se odnose na usluge fax-a i podatkovnih poziva. Svaki MSISDN je također predstavlja primarni ključ za HLR zapis. Prema izvoru [10] primjeri drugih podataka koji su spremljeni u HLR-u po jednom IMS zapisu su:

- usluge koje je korisnik zahtijevao ili su mu omogućene
- GPRS postavke da bi omogućile korisniku da pristupi usluzi prijenosa podataka paketnim modom GPRS
- trenutna lokacija korisnika
- postavke prosljeđivanja poziva koje se primjenjuju za svaki povezani MSISDN
- podaci u HLR-u su spremljeni tako dugo dok je korisnik pretplatnik određenog operatera.

VLR (Visitor Location Register) ili registar gostujućih korisnika sadrži podatke o vlastitim pretplatnicima i pretplatnicima drugih mreža. To je također baza podataka u koju se spremaju sve informacije o svim mobilnim stanicama koje se trenutno nalazi pod nadležnošću MSC-a (Mobile Switching Centre) koji ih poslužuje i omogućuje uslugu [10]. Najvažnija informacija koja se sprema je informacija o lokaciji, tj. pod kojim kontrolorom bazne stanice se trenutno nalazi. Lokacija je ujedno vrlo bitna kod uspostave poziva. MSC je zapravo komutacijsko čvorište ćelijske mreže koje je zaduženo za obavljanje osnovnih komutacijskih funkcija i ostalih specijaliziranih funkcija vezanih za pokretnu mrežu. MSC također može djelovati kao gateway prema drugim mrežama (npr. PSTN (Public Switched Telephone Network)). Kako bi se uspješno obavile određene funkcije, MSC dohvaća podatke o korisniku iz HLR-a, međutim pristup HLR-u ponekad može biti ograničen zbog različitih događaja koji se mogu pojaviti u mreži. S obzirom na to, privremene kopije korisničkih profila

smještene su upravo u VLR-u. Konfiguracija između MSC-a i VLR-a može varirati u ovisnosti o vrsti mreže.

BTS (Base Transceiver Station) ili sustav baznih stanica sastoji se od dvije komponente: MS (Mobile Station)-pokretne stanice i BS (Base Station)-bazne stanice, a osnovna zadaća je povezati mobilne terminalne uređaje s baznom stanicom. Nadalje, BTS je pod nadležnošću BSC (Base Station Controller)-kontrolora za nekoliko grupiranih baznih stanica.

3.2.2. Prekapčanje

Kako se korisnici kreću, tako mobilna stanica prelazi iz područja koje prekriva jedna bazna stanica u područje pokriveno drugom baznom stanicom. Opisani postupak naziva se prekapčanje (handoff/handover), a do njega dolazi u situacijama kada se mobilna stanica nalazi na granici ćelije i jakost signala od mobilne stanice prema baznoj je mala ili kada mobilna stanica dolazi u područje koje je pokriveno nedovoljno jakim signalom [10]. Isto tako, prekapčanje se treba razmatrati između dva sustava s obzirom na to da poziv može biti započet u ćelijskom mobilnom sustavu koji je nadziran od jednog operatera i biti nastavljen u sustavu kojeg nadzire drugi operater. Postoje dvije osnovne vrste prekapčanja:

- tvrdo prekapčanje definira se kao tip prekapčanja u kojem se postojeća veza mora prekinuti prije nego se uspostavi nova veza. Korisnik je povezan na samo jednu baznu stanicu u isto vrijeme, tj. mora se prekinuti veza s trenutno povezanom baznom stanicom prije nego što se ostvari nova veza s drugom baznom stanicom.
- meko prekapčanje zahtijeva da mobilna stanica započne komunikaciju s novom baznom stanicom bez prekida komunikacije sa starom baznom stanicom. Mobilna stanica održava komunikacijsku vezu s dvije ili više baznih stanica istovremeno.

3.2.3. VoIP usluga

Kao primjer usluge u mreži za prijenos govora opisat će se VoIP. Voice over Internet Protocol je tehnologija koja omogućuje obavljanje poziva putem širokopojasnog pristupa Internetu umjesto klasične telefonske linije [11]. Neke VoIP usluge dopuštaju uspostavu poziva samo prema onim korisnicima koji rabe istu uslugu, dok druge usluge omogućuju pozive prema bilo kojem korisniku koji posjeduje telefonski broj. To uključuje lokalne, *long distance*, mobilne i međunarodne pozive. Isto tako, neke usluge funkcioniraju samo putem specijalnih VoIP telefona, a druge koriste klasični telefon spojen na VoIP adapter.

VoIP usluge funkcioniraju tako da pretvaraju glas u digitalne signale koji se šalju Internet mrežom. Ako korisnik zove regularni telefonski broj, signal se pretvara u regularan telefonski signal prije nego dospije na odredište. VoIP dopušta uspostavu poziva direktno s računala, putem specijalnog VoIP telefona, ili klasičnog telefona koji je spojen na poseban adapter. Isto tako, bežične pristupne točke na lokacijama kao što su zračne luke, parkovi i kafići dopuštaju konekciju na Internet i pritom je moguće koristiti VoIP uslugu bežičnim putem.

Kao i sve druge telekomunikacijske usluge, tako i VoIP ima svoje prednosti i nedostatke definirane u izvoru [11]. Kao prednosti se navode sljedeće:

- neke od usluga nude značajke i pogodnosti koje nisu dostupne putem tradicionalnog telefona ili su dostupne uz dodatnu novčanu nadoknadu.
- korisnici su u mogućnosti izbjeći plaćanje i za širokopojasni pristup i za klasičnu telefonsku liniju.

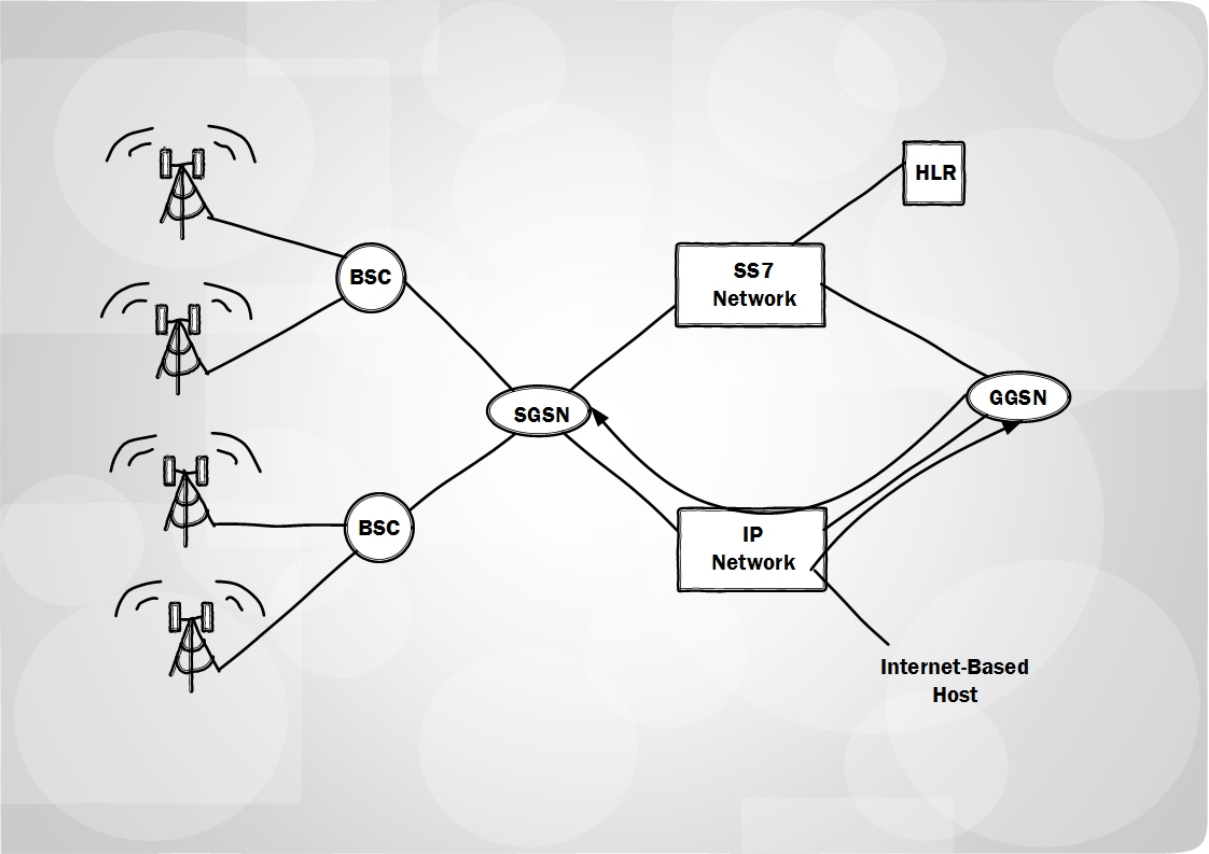
Nedostaci se mogu pojaviti uklanjanjem klasične telefonske usluge. Pojedine VoIP usluge ne rade za vrijeme nestanka struje i pružatelj usluge ne može ponuditi rezervna rješenja u tom slučaju. Problem postoji i kod izravnog spajanja s hitnim službama poput 911 broja, kao i nemogućnost korištenja imenika/oglasnika.

3.3. Mobilne mreže za prijenos podataka

Komunikacijski sustav za prijenos podataka u GSM mreži naziva se GPRS koji je implementiran tako da predstavlja nadogradnju na postojeću GSM mrežu i samu arhitekturu. Komutacija paketa ne zahtijeva nove spektre frekvencija u GSM mreži, već se zauzimaju postojeće frekvencije [1]. U postojećoj GSM mreži moguće je ostvariti komunikaciju tako da funkcije komutacije paketa ne smetaju uslugama telefonije podržane u GSM-u. Signalizacija se obavlja pomoću SS7, a HLR se koristi kako bi se provjerila autentičnost i pohranili korisnički profili.

3.3.1. Komponente mreže za prijenos podataka

Što se tiče arhitekture, novi elementi koji se uvode u odnosu na GSM su GGSN (Gateway GPRS Support Node) i SGSN (Serving GPRS Support Node) prikazani na slici 3.



Slika 3. Struktura mreže za prijenos podataka. Podaci od [1]

GGSN čvor obavlja više funkcija od jednostavnog prosljeđivanja paketa na odredište. Kao podrška brojnim mrežnim protokolima, GGSN prenosi IP i X.25 pakete do prijemnika čime su omogućene podatkovne usluge u starijim mrežama. GGSN također služi kao podrška za brojne značajke koje se ostvaruju putem telekomunikacijske mreže, pa tako primjerice QoS (Quality of Service) kvaliteta usluge na pojedinom mrežnom resursu može biti ostvarena od strane operacija koje se odvijaju u GGSN čvoru. GGSN pomaže i u sustavu naplate i terećenja s obzirom na to da zna kolika širina pojasa se koristi od strane svakog korisnika. Ipak, najvažnija funkcija GGSN čvora je adresiranje i mobilnost. Što se tiče adresiranja, GGSN radi slično kao DHCP (Dynamic Host Configuration Protocol) koji se koristi u računalnim mrežama. Nakon što je adresa dodijeljena korisniku od strane davatelja usluge, GGSN kreira listu mobilnih uređaja koju predaje SGSN-u.

Uz pomoć lokalnog registra, SGSN pohranjuje podatke o korisniku na lokalnoj razini. Slično kao u MSC-u, korisnički profili važni su u procesu prekapčanja, autentifikacije i naplate. Npr. ako određeni korisnik prima podatkovni promet, SGSN bilježi ćeliju ili sektor u kojem je korisnik lociran. Kada se korisnik kreće između baznih stanica, SGSN se ažurira. Često se

javlja problem signalizacije, odnosno potrebno ju je smanjiti. Kako bi se to postiglo, grupiraju se usluge pojedinog korisnika u snopove.

3.3.2. SMS usluga

SMS (Short Messaging Service) usluga predstavlja prijenos kratkih tekstualnih poruka s jednog mobilnog terminalnog uređaja na drugi, između fax uređaja i između IP adresa. Prema članku [12], poruke mogu sadržavati maksimalno 160 alfanumeričkih znakova, dok slike i grafičke poruke nije moguće slati.

Kada korisnik pošalje poruku, ona je zaprimljena u SMSC-u (Short Message Service Center), centru koji je dužan proslijediti poruku na odgovarajući terminalni uređaj. Kako bi se taj proces realizirao, SMSC šalje zahtjev HLR-u u cilju pronalaska pretplatnika kojem je namijenjena poruka. Jednom kada HLR zaprimi zahtjev od strane SMSC-a, šalje se povratna informacija SMSC-u o statusu korisnika koji može biti:

- aktivan ili neaktivan
- gdje se korisnik nalazi

U slučaju kada je status korisnika „neaktivan“, tada SMSC zadržava poruku određeni vremenski period. Nakon što pretplatnik postane „aktivan“, HLR šalje SMS obavijest SMSC-u koji zatim pokuša dostaviti poruku. SMSC prebacuje poruku u *Short Message Delivery Point to Point* sustav posluživanja, koji identificira uređaj kojem se poruka isporučuje. SMSC dobiva potvrdu da je poruka isporučena krajnjem korisniku i poruka se označava kao „poslana“ s čime završava proces slanja poruke s jednog terminalnog uređaja na drugi.

3.4. SS7 signalizacijska mreža

Nakon shvaćanja glavnih elemenata koji sačinjavaju moderne mobilne mreže potrebno je razumjeti komunikaciju koja se odvija između njih.

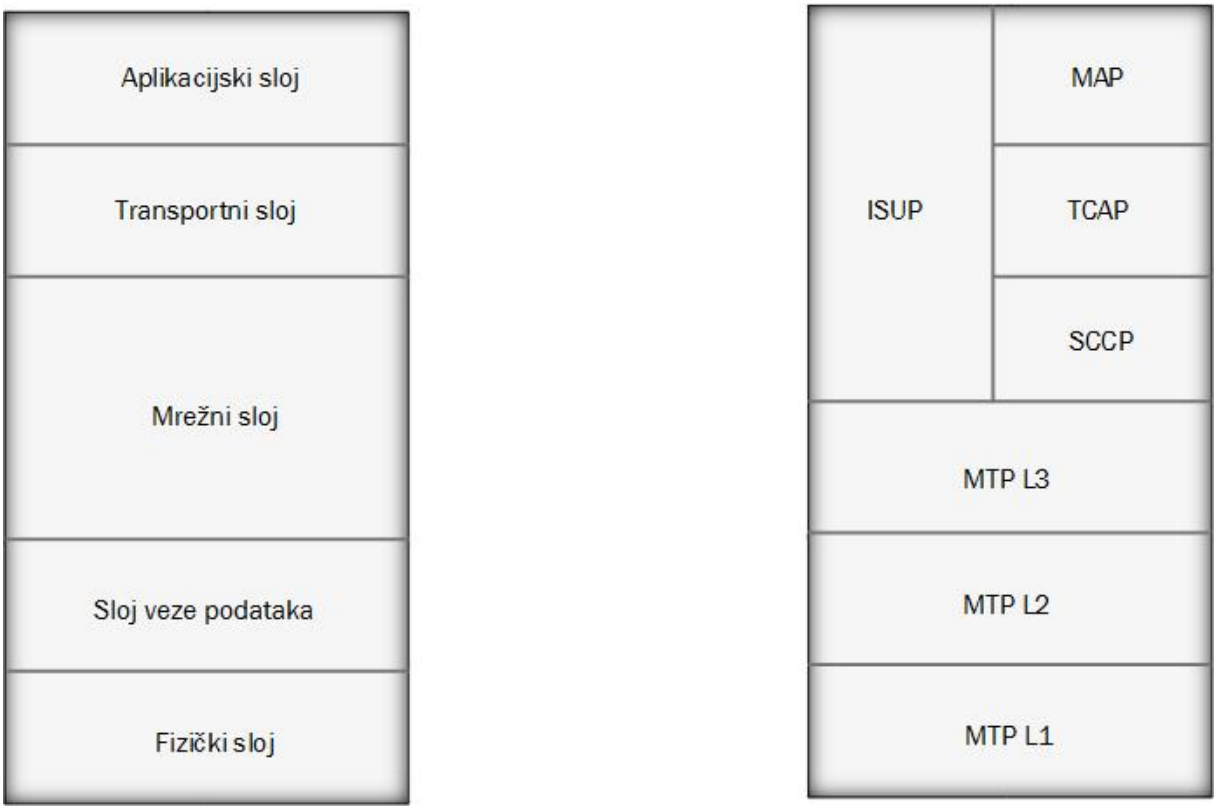
3.4.1. Arhitektura

Arhitektura signalizacijske mreže sadrži tri signalizacijske točke: SSP (Service Switching Point), STP (Signal Transfer Point) i SCP (Service Control Point) [1]. Svaka od navedenih signalizacijskih točaka identificirana je pomoću jedinstvenog point koda, slično kao što je svaki host u mreži identificiran jedinstvenom IP adresom. Signalizacijske točke su spojene signalizacijskim linkovima, obično 56 ili 64 kb/s DS0 linkom. STP su tzv. SS7 ruteri,

odnosno točke koje su zadužene za usmjeravanje signalizacijskih jedinica do odredišnih signalizacijskih točaka. SCP predstavlja bazu podataka koja je potrebna za usluge. SCP odgovara koje informacije su potrebne za obradu poziva, pristupanja bazi podataka, upravljanje i nadzor poziva.

3.4.2. Protokolni složaj

Kao što je ranije navedeno, SS7 protokol čini važan temelj signalizacije u mreži, a sastavljen je od četiri sloja na kojima se također nalaze protokoli. Slojeve je najjednostavnije raščlaniti i usporediti prema strukturi IP protokola, slika 4.



Slika 4. Usporedba IP i SS7 protokola. Podaci od [1]

MTP (Message Transfer Part) čini temelj strukture SS7 protokola, a zadužen je za pouzdanu isporuku signalizacijskih poruka uključujući i reakciju ako dođe do zastoja na linku. Kako bi se funkcionalno mogle obaviti navedene zadaće, MTP je podijeljen na tri različita dijela.

MTP1 (Message Transfer Part Level 1) odgovara fizičkom sloju strukture IP protokola [1]. Svi linkovi su dvosmjerni, a propusnost je velika kao 56 KB/s u ANSI standardnim

mrežama ili pak 64 KB/s u drugim mrežama. Moguće je kombinirati četiri fizička linka između dva čvora kako bi se kreirala agregatna stopa od 1.544 Mb/s.

Sljedeći dio MTP cjeline čini MTP2 (Message Transfer Part Level 2) koji odgovara sloju veze podataka u strukturi Interneta [1]. Komunikacije između dva direktno povezana mrežna čvora omogućene su upravo tim dijelom. Funkcionalnosti MTP2 veće su od jednostavnog adresiranja od točke do točke, i za razliku od Internet modela osigurana je pouzdana isporuka. Nadalje, MTP2 strogo nadzire stopu grešaka na svim linkovima. U slučaju da broj grešaka na linku prelazi određenu granicu, MTP2 upozorava protokole na višoj razini i konekcija je zatvorena. MTP2 nudi eksplicitne mehanizme za kontrolu toka. Ako postoji zagušenje na linku nekoliko sekundi, konekcija je zatvorena.

Posljednji dio MTP cjeline čini MTP3 (Message Transfer Part Level 3) koji je odgovoran za rutiranje paketa od izvorišta do odredišta. MTP3 također odgovara za zastoje na linkovima koje javlja MTP2. U slučaju velikih grešaka na linku ili zagušenja, MTP3 rekonfigurira rute zaobilaženjem nedostupnim susjednih čvorova kako bi se osigurala isporuka prometa.

SCCP (Signaling Connection Control Part) rješava probleme pružajući ostale funkcije koje su karakteristične za protokole mrežnog sloja. Dok se MTP3 poruke bave samo čvorovima u mreži, SCCP omogućuje specifične funkcije kako bi postalo odredište zahtjeva. U kombinaciji s tri razine MTP cjeline, SCCP tvori NSP (Network Services Part).

Za usluge kontrole, mobilnog menadžmenta i transakcijsko orijentirane protokole koristi se TCAP (Transactions Capabilities Application Part). TCAP osigurava okvir putem kojeg čvorovi u mreži mogu zatražiti vršenje udaljenih postupaka. IN (Intelligent Network) funkcije kao što su besplatni telefonski pozivi i automatsko blokiranje pokreću se pozivanjem TCAP poruke. TCAP poruke također osiguravaju transakcijske identifikatore koji su funkcionalno slični brojevima porta protokola u transportnom sloju.

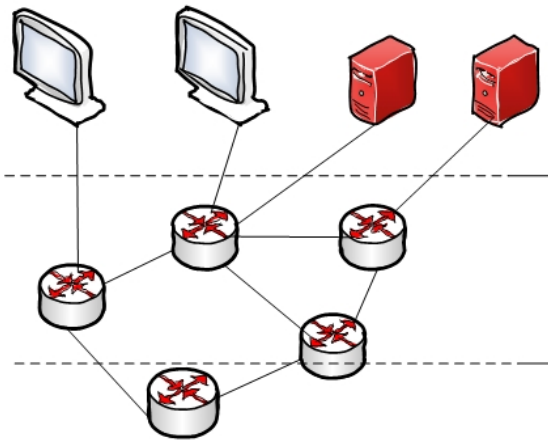
MAP (Mobile Application Part) predstavlja aplikacijski sloj u SS7 mreži [1]. Uključuje usluge poput rukovanja pozivom, tekstualne poruke i lokacijski bazirane usluge. Koristeći MAP omogućene su i neke druge usluge kao što je mobilni menadžment, korisnički profili u HLR-u i VLR-u te postupci autentifikacije.

ISUP (ISDN User Part) se koristi za kontrolu konekcije, a prenosi informacije tako da pozivi mogu biti rutirani i kako bi se obavila rezervacija resursa na putu. Može se upotrebljavati u fiksnoj i mobilnoj mreži.

4. Sigurnosne prijetnje i ranjivosti telekomunikacijskih mreža

Sigurnost telekomunikacijske mreže vrlo često je vezana uz pojam Interneta. Većina mreža mehanizme zaštite usmjerava na ranjive sustave, čija se sigurnost narušava daljinskim napadom na mrežu ili većim spomenutim DoS napadom. Telekomunikacijske tehnologije promijenile su se unatrag nekoliko godina, a samim time pojavile su se nove ranjivosti. U ovom poglavlju analizirat će se novije vrste prijetnji koje iskorištavaju ranjivost mreže i samim time vrše napad na mrežnu infrastrukturu.

Internet kao jedna otvorena mreža, često je medij pomoću kojeg se izvršavaju mnogi napadi u kojima zlonamjerni korisnici ostvaruju neovlašteni pristup krajnjim sustavima u cilju prisluškivanja, špijunaže i sl. Prijetnje obično imaju ciljani pristup podacima o krajnjim sustavima, a svrha je učiniti krajnje sustave privremeno nedostupnim. Slikom 5 prikazane su najčešće mete napada, ciljevi napada te primjeri napada u jednostavnoj mreži. Težište navedenih napada leži u podatkovnom sustavu koji u slučaju ciljanih prijetnji uskraćuje uslugu krajnjem korisniku. Napadom na taj dio mreže nastaju gubici s perspektive određenog operatera isto kao i s perspektive korisnika s obzirom na to da usluga često ne može biti isporučena. Napad na podatkovnu ravninu također može ovisiti o ruterima koji obrađuju pakete.



Meta napada	Cilj napada	Primjeri napada
Krajnji sustav	Pristup podacima i modifikacija istih	Hakiranje, phishing, špijunaža
	Denial-of-service	Denial-of-service napad putem botneta*
Kontrolni sustav	Pristup podacima i modifikacija istih	Korištenje zlonamjerne rute, DNS „trovanje" memorije
	Denial-of-service	DNS rekurzijski napad
Podatkovni sustav	Pristup podacima i modifikacija istih	Prisluškivanje, čovjek u sredini
	Denial-of-service	Iskorištavanje ranjivosti pri obradi paketa

*botnet-mreža privatnog računala koje je zaraženo putem malicioznog softvera

Slika 5. Prikaz meta, ciljeva i primjera napada. Podaci od [8]

4.1. Prijetnje i ranjivosti u VoIP-u

VoIP kao jedna od usluga koja se koristi u mrežama za prijenos govora ima jak utjecaj na globalne komunikacije s obzirom na to da omogućuje prijenos glasa, podataka i slika. Konvergencija glasa i podataka u istoj mreži donosi brojne prednosti, ali isto tako i ograničenja za korisnike. Iako VoIP ima definirane mehanizme zaštite, autori članka [5] smatraju kako postoji potreba za poboljšanjem sigurnosti. Sigurnosni propusti mogu imati negativan utjecaj na glasovnu komunikaciju i podatke u mreži.

Prijetnje koje se javljaju prilikom uspostavljanja/primanja VoIP poziva mogu se podijeliti u nekoliko skupina [5].

- Krađa usluga je sposobnost zlonamjernog korisnika da uspostavi lažni poziv. U tom slučaju napadač želi koristiti uslugu bez da plaća naknadu za istu, tako da se ova vrsta prijetnje vrši protiv davatelja usluga. Napadač koristi razne metode kako bi ostvario ono što je naumio. U većini slučajeva, neautorizirani korisnik uspostavlja pozive koristeći telefon koji se ne nadzire od strane osobe ili nekog drugog sigurnosnog sistema ili koristi telefon legitimnog korisnika.
- Maskiranje je vrsta prijetnje kada napadač nastoji prevariti udaljenog korisnika tako što ga uvjeri da zapravo priča s primateljem. Takav napad je tipičan u slučajevima kada identitet primatelja nije u potpunosti poznat sve dok informacija ne stigne do samog odredišta.
- IP podvala nastaje kada napadač unutar ili izvan mreže nastoji oponašati računalo koje je sigurno, a to može učiniti na dva načina: napadač koristi IP adresu koja se predstavlja kao povjerljiva unutar mreže, ili ovlaštenu vanjsku IP adresu s kojom je omogućen pristup na samu mrežu. Slično kao u Caller ID-u, IP podvala često se koristi za pokretanje drugih vrsta napada kao što je DoS. Napadač pomoću lažnih adresa nastoji prikriti vlastiti identitet.
- Presretanje poziva je neovlašteno praćenje glasovnih paketa ili RTCP (Real-Time Control Protocol) transmisije. Napadači mogu „uhvatiti“ pakete i dekodirati glasovne poruke dok se one šalju mrežom. Isto tako, napadač može identificirati IP i MAC adresu telefona koristeći ARP (Address Resolution Protocol) ili presresti poziv umetanjem telefona s lažnom MAC adresom pritom prikrivajući identitet. Rizik je donekle ograničen kod ove vrste napada, jer zahtijeva fizički pristup lokalnoj mreži ili

udaljeni pristup korisnika na lokalnu mrežu. Presretanje poziva u Internet mreži je teže izvesti zbog potrebe izdvajanja glasovnog od druge vrste prometa.

- Poricanje razgovora događa se kada dva korisnika obavljaju razgovor, a kasnije jedan od njih poriče da se razgovor dogodio.
- Napad preusmjeravanjem obavlja se kada napadač zamijeni e-mail adresu korisnika s IP adresom koja preusmjerava poziv k napadaču. U tom slučaju, poziv koji se obavlja putem VoIP-a neće stići do krajnjeg korisnika. Mehanizmi koji se koriste za pokretanje ovakve vrste napada, slični su onima koji se koriste za presretanje poziva.
- DoS napadi nastoje spriječiti legitimnog korisnika da pristupi uslugama mreže. Najčešće je poslužitelj preplavljen zahtjevima, odnosno nastoji ga se opteretiti. DoS napad može biti pokrenut prema IP telefonima kako bi se pokušala prekinuti komunikacija.
- Neovlašteno pristupanje signalnom protokolu događa se kada napadač prati i „hvata“ pakete. Tako korisnik može uspostaviti VoIP poziv bez korištenje VoIP telefona. Korisnik također može obaviti poziv koji će ga na kraju skupo koštati, vjerujući da je nastao od strane nekog drugog korisnika.
- Napadi na *soft* telefone pojavljuju se iz razloga jer se oni nalaze u VLAN-u (Virtual Local Area Network) za koji je potreban otvoren pristup kako bi se obavila kontrola poziva, uspostavili pozivi na IP telefone i ostavile glasovne poruke. VoIP sustavi imaju mogućnost rukovanja velikim brojem poziva koji se odvijaju putem IP telefona ili soft telefona. Za razliku od tradicionalnih telefona koji su fiksni, IP telefoni koriste npr. Ethernet priključak i dodjeljuje im se IP adresa. To možda predstavlja određenu prednost, no također su mete sigurnosnih napada. Svi ti napadi odnose se i na konferencijske pozive, a treba se uzeti u obzir da se ponegdje koriste i usluge govorne pošte.

Ranjivosti VoIP-a ne obuhvaćaju samo nedostatke unutar same aplikacije, već i ranjivosti operativnih sustava, aplikacija i protokola o kojima VoIP ovisi [5]. Složenost VoIP-a stvara veliki broj ranjivosti koje utječu na tri područja informacijske sigurnosti: povjerljivost, integritet i dostupnost. Obično se ranjivosti analiziraju na temelju slojeva TCP/IP modela, iako ranjivosti mogu postojati i izvan slojeva spomenutog modela.

Tablica 1. Vrste napada na VoIP uslugu. Podaci od [5]

Sloj	Vrsta napada	Povjerljivost	Integritet	Dostupnost
Mrežni	Fizički napad	X		X
	ARP memorija	X	X	X
	MAC podvala	X	X	X
Internet	IP podvala			
	Uređaj	X	X	X
	Preusmjeravanje putem IP-a	X	X	X
	IP frag	X	X	X
Transportni	TCP/UDP preplavljivanje			X
	TCP/UDP ponavljanje	X	X	
Aplikacijski	TFTP umetanje poslužitelja		X	
	DHCP umetanje poslužitelja		X	
	ICMP preplavljivanje			X
	SIP			
	Registracija	X	X	X
	Hakiranje			
	MGCP hakiranje	X	X	X
	Izmjena poruke	X	X	
	RTP umetanje			
	Otkazivanje napada			X
	Metode preusmjeravanja	X		X
	RTP			
	SDP preusmjeravanje			X
	RTP koristan teret			X
	RTP petljanje	X	X	X
	Enkripcija	X	X	X
	Zadana konfiguracija	X	X	X
	Nasljedna mreža	X	X	X
	DNS dostupnost			X

Tablicom 1 prikazane su ranjivosti, odnosno vrste prijetnji koje često utječu na više od jednog područja informacijske sigurnosti, a to su već spomenuta povjerljivost, integritet i dostupnost. U nastavku su opisane kratice koje nisu prethodno spomenute u radu, a odnose se na vrste napada u VoIP usluzi, spomenute u tablici 1:

- TCP/UDP (Transmission Control Protocol/User Datagram Protocol)-konekcija i slanje podataka od jednog hosta prema drugom
- TFTP (Trivial File Transfer Protocol)-koristi se za prijenos datoteka korištenjem UDP-a
- DHCP (Dynamic Host Configuration Protocol)-dodjeljuje IP adrese i mrežne postavke
- ICMP (Internet Control Message Protocol)-šalje kontrolne poruke o greškama
- SIP (Session Initiation Protocol)-upravlja multimedijskim porukama koje koriste IP
- MGCP (Media Gateway Control Protocol)-služi za kontrolu media gateway-a baziranog na IP-u povezanog na PSTN
- SDP (Socket Direct Protocol)-omogućuje pristup visokim performansama mreže
- DNS (Domain Name System)-sustav ili sredstvo spojeno na Internet ili privatnu mrežu

Izvor [5] smatra da je najbolji pristup sigurnosti kod VoIP-a vršiti enkripciju glasovnog prometa i koristiti VPN (Virtual Private Network) kako bi se razdvojio VoIP od podatkovnog prometa s ciljem povećanja sigurnosti i učinkovitosti. Sigurnost također može biti implementirana pomoću filtriranja i/ili firewall-a koji kontrolira glasovni i podatkovni promet.

4.2. Prijetnje i ranjivosti u SMS-u

SMS je za veliki broj korisnika dominantno sredstvo komunikacije koje često zamjenjuje glasovnu komunikaciju. Putem SMS-a omogućena je diskretna interakcija između mobilnih pretplatnika kratkim porukama. Usluga SMS-a kratko vrijeme je bila popularna, međutim prema knjizi [1] broji više korisnika u bazi od popularnog Interneta. Iako usluga sadrži niz prednosti kako iz perspektive korisnika, tako i iz perspektive davatelja usluge, uvođenje SMS-a u mobilne mreže stvara značajne sigurnosne probleme.

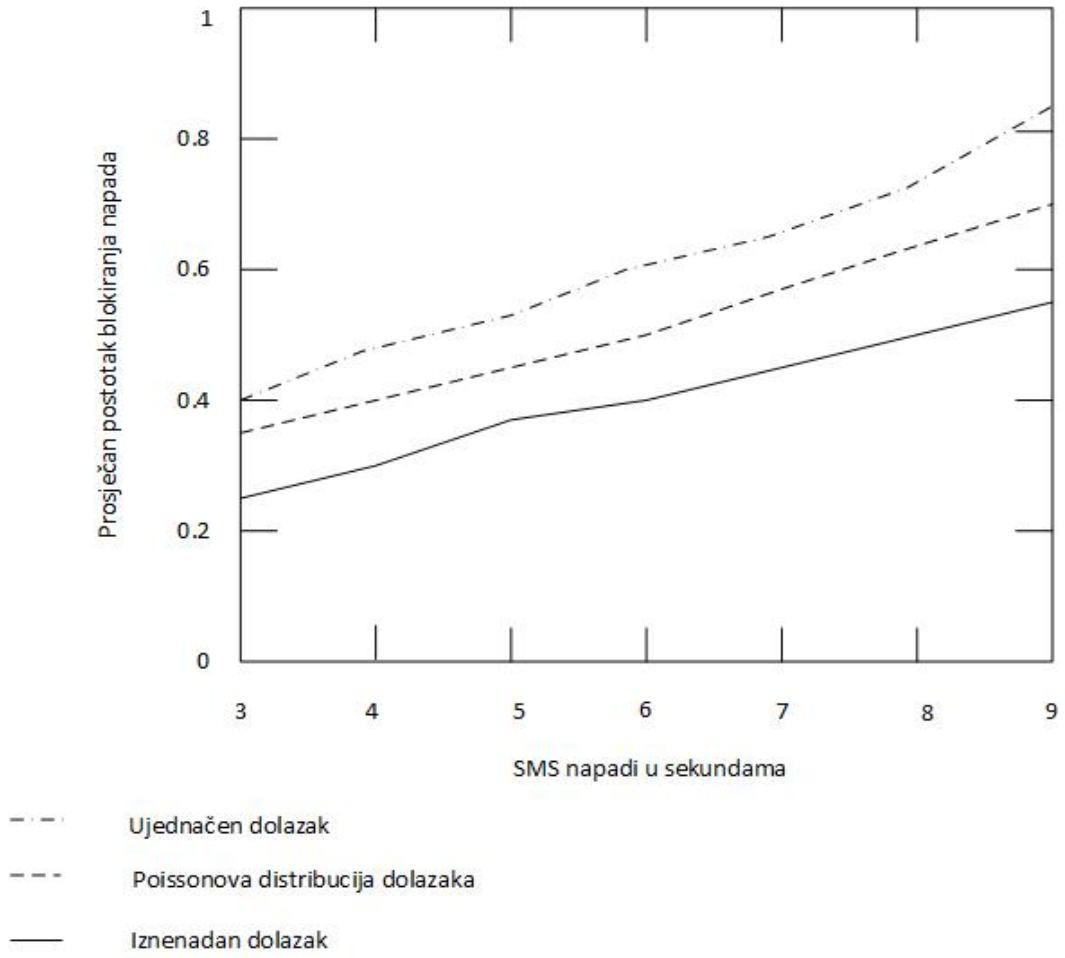
Napadi na SMS uslugu događaju se prvenstveno s ciljem da napadač ostvari nekakvu zaradu. Izvor [6] navodi razloge koji su doprinijeli sve većim prijetnjama SMS usluzi:

- Mobilne mreže postaju sve brže, javljaju se otvoreni pristupi Internetu i aplikacijskim portalima. Zatvorenost mreže postaje stvar prošlosti, dostupnost 3G mreži i Internetu dio je korisničke svakodnevice.
- Korisnici rabe sve više aplikacija na svojim mobilnim terminalnim uređajima. Uređaji postaju sve snažniji i imaju sposobnost pružiti korisniku širok spektar aplikacija, a napadači su u stanju postaviti malware unutar aplikacije na vrlo jednostavan način.
- Kanal koji rabi SMS usluga smatra se „čistim“ i sigurnim. Korisnici imaju visoku razinu povjerenja u SMS i ne ustručavaju se izmjenjivati povjerljive informacije, pristupati financijskim i sličnim aplikacijama putem mobilnog terminalnog uređaja.
- Neograničenost poruka u pojedinim tarifnim paketima također zvuči primamljivo za pretplatnike.
- SMS je nadmašio e-mail kao vrstu komunikacije diljem svijeta iz razloga jer je dostupan na gotovo svakom uređaju, te se smatra kao učinkovitija i manje napadačka usluga u odnosu na glasovnu komunikaciju.

S obzirom na spomenute razloge zbog kojih je SMS sve više nestabilan s perspektive sigurnosti, napadi su podijeljeni u sljedeće skupine:

- SMS spam poruke su najosnovniji oblik napada pri čemu se šalju neželjene poruke pretplatniku tipa masovnog oglašavanja. Vrlo često takav SMS sadrži tekst kojim se korisnik nagovara na daljnje slanje iste poruke svojim kontaktima u zamjenu za određeni novčani iznos na korisnički račun.
- Prevara s posebnom naplatom znači slanje neželjenih poruka kojima se pretplatnik navodi na pozivanje određenog broja ili se prijavljuje za neku vrstu pretplate koja se naplaćuje.
- Phishing napadom korisnika se traži da nazove određeni broj pri čemu se izdvajaju povjerljivi podaci koji će biti iskorišteni u najčešće zlonamjerne svrhe.
- Slanje neželjenih poruka poslanih pretplatniku od strane davatelja usluga u marketinške svrhe također se smatra napadom poznatijim pod nazivom VASP napad.
- Mobilni malware koji se širi preko poruka je zlonamjerni softver koji je dizajniran s ciljem da filtrira mobilni uređaj bez pristanka vlasnika. To obično uključuje slanje linkova i preuzimanje određenih datoteka koje su zlonamjerne. Malware-i uključuju viruse, crve i trojanske konje.

Kako bi se pobliže objasnio ciljani SMS napad, potrebno je vizualizirati takav događaj. Grafom 2 prikazan je odnos SMS napada u sekundama i prosječan postotak blokiranja napada. Ako poziv ili SMS stigne kada su svi kanali zauzeti, zahtjev je blokiran. Graf prikazuje učinkovitost napada kada poruke dolaze ujednačeno, Poissonovom distribucijom i iznenada. Najučinkovitiji napad je kad dolaze ujednačeno, ali s obzirom na to kako se postotak blokiranja napada povećava, takav napad će se teško ostvariti. Najmanje učinkovit napad je kada poruke stižu iznenada, ali su veće šanse da se napad ostvari u usporedbi s prethodno spomenutim ujednačen dolaskom poruka.



Graf 2. Prosječan postotak blokiranja napada. Podaci od [1]

4.3. Prijetnje i ranjivosti u SS7 mreži

Svaka telekomunikacijska kompanija posjeduje svoju vlastitu SS7 mrežu. Mreža može biti u tradicionalnoj SS7 izvedbi, preko IP-a ili se SS7 signalizacijske točke mogu primijeniti putem LAN-a tvrtke preko IP-a sve dok svaki mrežni entitet sadrži IP adresu [7]. Intranet tvrtke obično je spojen putem firewall-a na javni Internet. Slično kao i kod Interneta, ranjivost SS7 signalizacijske mreže raste brojem i kompleksnošću sučelja koja se nalazi

između različitih SS7 entiteta. Razvijenije usluge kao što je npr. preusmjeravanje poziva obilježava unutarnja ranjivost, što bi značilo da napada ima mogućnost izmijeniti SCP-e kojima će se vršiti preusmjeravanje poziva. Ranjivost se dodatno povećava povezanošću SS7 mreže i Interneta. Veliki dio komponenata od kojih je sastavljen Internet za svoj rad koristi iznajmljene telefonske linije, a SS7 sustav je umrežen putem internetskih tehnologija i Interneta samog. S obzirom na spomenutu činjenice, ranjivosti SS7 mreže mogu utjecati na Internet isto kao što i ranjivosti Interneta mogu utjecati na SS7 mrežu.

Za razliku od Interneta koji je relativno otvorena mreža na koju se može spojiti putem običnog desktop računala, SS7 mreža je veća privatna mreža koja zahtijeva specijalnu i skupu opremu. Npr. dok Ethernet zahtijeva samo fizičku konekciju na Internet, MTP kod SS7 mreže zahtijeva konfiguraciju između konektiranih signalizacijskih točaka. Isto tako, signalizacijske točke ne mogu biti jednostavno uključene u mrežu. S obzirom na to da je SS7 mreža obično konstruirana za zatvorenu telekomunikacijsku tvrtku, za razliku od Interneta, potrebno je provesti određene autentifikacijske procedure.

Napadi u SS7 mreži događaju se prvenstveno zbog spomenutih ranjivosti same mreže. Ciljevi napada su elementi mrežne arhitekture: SSP, STP i SCP, a vrste napada su: modifikacija, preusmjeravanje, prekid i lažno predstavljanje [7].

SSP čvorovi SS7 mrežu i predstavljaju točke pristupa za zlonamjerni napad. Velika većina napada iskorištava slabe autentifikacijske mehanizme u SS7 mreži. Kao primjer se može uzeti ISDN koji je dizajniran da poveže rubne dijelove SS7 mreže s krajnjim korisnicima, pri čemu se promet direktno ostvaruje kroz SS7 mrežu. Zlonamjerni korisnik ISDN usluge može modificirati ili izmisliti nepostojeću ISUP poruku. SSP je također ciljana meta za špijuniranje određenih korisnika, s obzirom na to da promet svakog korisnika ide putem odgovarajućeg SSP-a. Napadač isto tako može prekinuti protok informacija koje su namijenjene krajnjem korisniku tako da doda svoje odredište na originalno odredište koje se nalazi u zaglavlju poruke koja se šalje mrežom. Kao i ostali mrežni elementi, SSP također ima maksimalni radni kapacitet. Preopterećenost na linku između SSP-a i STP-a može ometati rad SSP čvora, i pri tome uskratiti uslugu određenom dijelu korisnika.

Članak [7] kaže kako STP vrši rutiranje i sve poruke moraju proći kroz STP. Napadač koji ima uvid u STP može vidjeti sav promet koji se odvija od i prema odgovarajućim SSP-ima. Sofisticiraniji napad uključuje udaljen pristup STP-u i kreira se lažni STP koji filtrira i preusmjerava promet. Isto tako, moguće je prisluškivanje određenih razgovora. Kao i svi

ruteri u mreži, tako i STP može biti prometno preopterećen. DoS napad moguće je izvršiti ako su SCP baze podataka modificirane za preusmjeravanje velikog broja poziva na telefonski broj koji se nalazi na određenom SSP-u. Napadač ostvaruje svoju namjeru tako da preusmjeri sve poruke na lažni STP, te zatim vrati i prenatrpa originalni STP.

SCP baze podataka sadrže osjetljive informacije koje su vrlo ranjive po pitanju sigurnosti. Za primjer se može uzeti CMSDBs (Call Management Services Databases) baza podataka koja obrađuje besplatne pozive. Besplatni brojevi zapravo su instalirani u postojeći telefonski broj, a naplata se vrši odvojeno. U ovom slučaju napadač prevarom mijenja telefonski broj odredišta u neki drugi broj, pri čemu se poremeti stvarna naplata troškova za pozive prema odredišnom broju. Napadač može čak promijeniti iznos naplate i PIN (Personal Identification Number). SCP baze podataka su također ranjive na DoS napad. Baza podataka može biti izbrisana pri čemu se narušava isporuka usluge u mreži.

5. Zaštita telekomunikacijskih mreža

Zaštita telekomunikacijskih mreža odnosi se na brojne sigurnosne mehanizme kojima se nastoji zaštititi sustav i spriječiti nelegitimnog korisnika da pristupi osjetljivim podacima i informacijama. U ovoj cjelini opisat će se cyber i fizička zaštita, kriptografija, mehanizmi zaštite i vatrozidi.

5.1. Cyber (web) i fizička zaštita

Cyber zaštita štiti informacije tako da se koriste kombinacije nula i jedinica protiv prijetnji koje mogu nastupiti kao drugačija kombinacija nula i jedinica. Tako napad može rezultirati neautoriziranim promjenama i neautoriziranim korištenjem informacija. Virus se navodi kao primjer cyber prijetnje, koja se može spriječiti antivirusnim softverom kao vrstom zaštite. Uloga fizičke zaštite je zaštititi fizički oblik informacije, a to se može ostvariti na dva različita načina. Prvi cilj obuhvaća zaštitu čitave strukture fizičke podrške kako bi bilo moguće održavanje i čuvanje podataka. U strukturu fizičke podrške prema knjizi [3] spadaju:

- hardware, u općenitom smislu-medij za čuvanje, obradu i transmisiju podataka
- okolina telekomunikacijskog sustava-električna energija, komunikacijske usluge, zgrade, ekološka kontrola
- osoblje i informacije koje osoblje posjeduje za pokretanje sustava

Kako bi se uspješno zaštitila informacijska imovina, potrebno je zaštititi sve navedene resurse. Promatrajući fizičku zaštitu sa širokog aspekta, može se reći da ona obuhvaća tri podvrste zaštite: zaštitu okoline, osoblja i administracije.

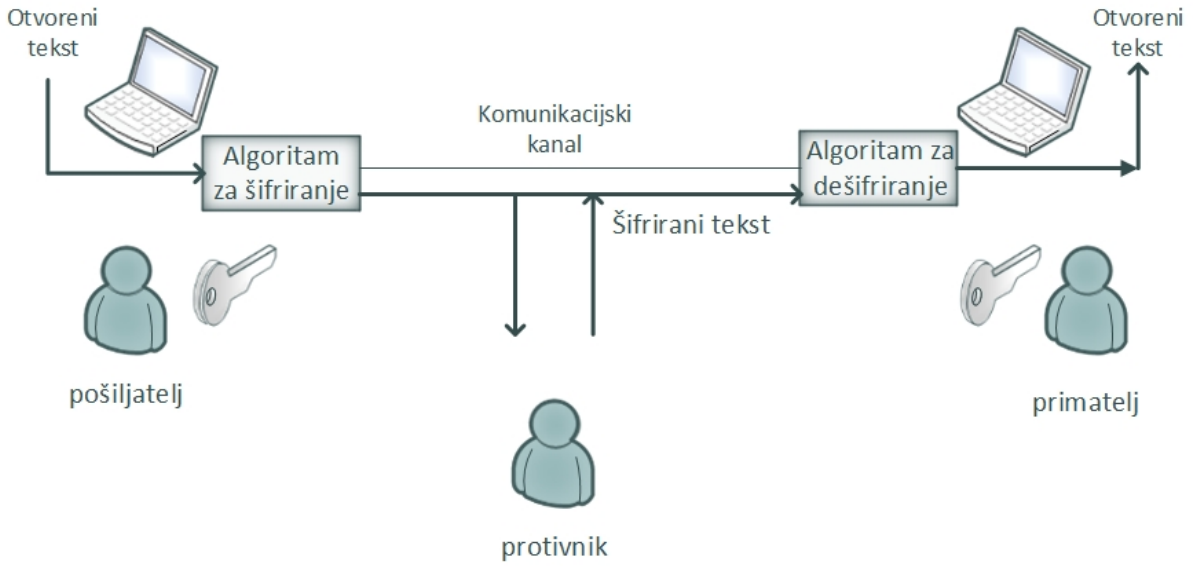
Drugi cilj fizičke zaštite je spriječiti zloupotrebu informacija. Zloupotreba može biti slučajna i namjerna, a pojavljuje se kao vandalizam, krađa, krađa tako da se kopiraju podaci i krađa usluga. Navedeni ciljevi fizičke zaštite mogu biti provedeni tako da se kombiniraju odgovarajuću uređaji i politika. Odgovarajućom praksom i ponašanjem ne može se nadomjestiti skupa sigurnosna oprema, međutim nepravilnim rukovanjem svaka oprema postaje beskorisna. Izvor [3] smatra da fizička zaštita prethodi cyber zaštiti kako si lakše predočili sigurnosni mehanizmi. Npr. obrana protiv neautorizirane modifikacije podataka nastale cyber napadom je pohraniti datoteke na CD-ROM. S druge strane, pohranom podataka na taj način ne garantira se da disk neće biti uništen od strane zlonamjernog napadača. Preventivne mjere koje se mogu poduzeti su backup podataka na udaljenoj lokaciji, ali ako napadač ucjeni zaposlenika tvrtke, svaka povjerljiva informacija postaje

ugrožena. Tradicionalna fizička zaštita obično se provodi u slučaju lopovluka i požara. Danas, mnoga virtualna poduzeća smatraju zastarjelim klasične načine fizičke zaštite . Primjerice, u slučaju da zaposlenik ostavi povjerljive informacije u uredu do kojeg je dostupan pristup napadaču, postoje šanse da te iste informacije dospiju u ruke konkurentnog poduzeća što nadalje povlači za sobom krađu ideja, noviteta i sl. Fizička zaštita telekomunikacijske mreže s vremenom je od jednog jednostavnijeg oblika izrasla u moderan i relativno kompleksan fenomen.

Cyber i fizička zaštita međusobno se nadopunjuju i preklapaju [3]. Tamo gdje završava kontrola fizičke zaštite od strane organizacije, započinje filtriranje paketa. Kada su pojačane obrane od cyber napada, fizička ranjivost postaje meta napada i obrnuto.

5.2. Kriptografija

Kriptografija je način zaštite informacija i podataka koji se šalju telekomunikacijskom mrežom, a obuhvaća metode koje pretvaraju izvorni oblik informacije u neprepoznatljiv oblik, odnosno formu koja je poznata samo pošiljatelju i primatelju [9]. Kriptografske metode obuhvaćaju sve aspekte sigurnog komuniciranja, pa tako i autentikaciju i digitalne potpise. Uz kriptografiju provodi se i kriptoanaliza koja omogućuje otkrivanje sadržaja kriptirane poruke. Za razliku od kriptografije, kriptoanaliza ne zahtijeva poznavanje ključa pomoću kojeg pošiljatelj i primatelj mogu dešifrirati poruke. Zadatak kriptografije je omogućiti pošiljatelju i primatelju komunikaciju putem nezaštićenog komunikacijskog kanala tako da zlonamjerni protivnik ne može „pročitati“ njihove poruke. Poruka koja se šalje nesigurnim komunikacijskim kanalom zove se otvoreni tekst, a može biti u različitom obliku (numerički podaci, tekst na materinjem jeziku, tekst na stranom jeziku i sl.). Šifriranje je postupak kojim pošiljatelj transformira otvoreni tekst koristeći ključ koji je poznat pošiljatelju i primatelju [9]. Otvoreni tekst nakon opisanog postupka naziva se šifrat koji se šalje komunikacijskim kanalom do odredišta, prikazano slikom 6. U slučaju pokušaja napada, odnosno prisluškivanja, napadač je u mogućnosti doznati sadržaj šifrata, ali ne može odgonetnuti otvoreni tekst. Za razliku od napadača, primatelj posjeduje odgovarajući, unaprijed dogovoreni ključ pomoću kojeg određuje otvoreni tekst.



Slika 6. Postupak šifriranja. Podaci od [9]

Izvor [9] definira kriptografski algoritam ili šifru kao matematičku funkciju koja se koristi za šifriranje i dešifriranje. Argumente koje sadrži kriptografski algoritam su ključ i otvoreni tekst. Ključevi mogu poprimiti različite vrijednosti koje čine prostor ključeva. Kriptografske sustave moguće je klasificirati s obzirom na [9]:

- tip operacija koje se koriste pri šifriranju-supstitucijske i transpozicijske šifre pomoću kojih se svaki dio otvorenog teksta transformira u neki drugi element. Primjer supstitucije je pretvaranje riječi „informacija“ u „hdertckso“, a primjer transpozicije je „informacija“ u „forcijamain“. Moguće je kombinirati obje navedene metode.
- način na koji se obrađuje otvoreni tekst-blokovne šifre kod kojih se obrađuje jedan po jedan blok elementa određenog otvorenog teksta i pritom koristi jedan ključ, te protočne šifre kod kojih se također obrađuje jedan po jedan blok elementa, ali uz niz ključeva.
- broj ključeva koji se koristi-kod simetrične kriptografije koristi se jedan, tajni ključ za šifriranje i dešifriranje, dok se kod asimetrične kriptografije koristi javni ključ za šifriranje i tajni ključ za dešifriranje.

5.2.1. Simetrična kriptografija

Simetrična kriptografija smatra se najstarijom vrstom kriptografije, naziva se i kriptografija tajnog ključa jer se informacije kriptiraju jednim te istim ključem (tajnim ključem) i istim algoritmom. Algoritam je definiran na sljedeći način [1]:

$$E(k, m) = c \qquad D(k, c) = m$$

ili

$$D(k, E(k, m)) = m$$

pri čemu je *E* enkripcijska funkcija kojom se podatak mijenja tako da postane nečitljiv osobama koje ne posjeduju odgovarajući ključ, *D* dekripcijska funkcija (postupak obrnut od enkripcije), *m* predstavlja izvorni tekst, *c* je šifrirani tekst i *k* je tajni ključ. U literaturama se opisani algoritam često spominje kao šifrat. Sigurnost simetričnih algoritama ovisi o sigurnosti njega samog kao i o dužini ključa. Ono što čini algoritam sigurnim jer prilično otežano otkrivanje sadržaja poruke bez poznavanja tajnog ključa. U praksi se pretpostavlja da protivnik ima pristup kriptografskom algoritmu, ali ne i njegovom ključu.

Vrste algoritama u simetričnoj kriptografiji su već spomenuti i objašnjeni algoritmi: protočni i blokovni. Najpoznatiji simetrični algoritam je DES (Data Encryption Standard) koji se aktivno koristio do 2000. godine kada ga je zamijenio AES (Advanced Encryption Standard) koji radi s ključevima dužine 128, 192 i 256 bita [9]. Dužina ključa ujedno je i razlog zamjene jer je kod DES algoritma iznosila 56 bita. IDEA (International Data Encryption Algorithm) algoritam je vrsta čije je operacije lako implementirati na računalu pri čemu se pokazao vrlo učinkovitim u praksi. Dužina ključa iznosi 128 bita, a mnogi mrežni stručnjaci smatraju ga jednim od najsigurnijih simetričnih algoritama koji su danas u upotrebi.

5.2.2. Asimetrična kriptografija

Asimetrična kriptografija ili kriptografija javnog ključa funkcionira na temelju algoritma koji kreira dva ključa, javni i tajni. Oba ključa koriste se za enkripciju podataka. Sistem radi tako da bilo koji podatak enkriptiran javnim ključem može biti dekriptiran samo pomoću tajnog ključa i svaki podataka enkriptiran privatnim ključem može biti dekriptiran samo javnim ključem [9]. U praksi, vlasnik javnog i tajnog ključa može slobodno podijeliti javni ključ, međutim tajni ključ mora ostati povjerljiv. Svaki korisnik koji se želi obratiti drugom korisniku mora saznati samo javni ključ, izvršiti enkripciju koristeći taj ključ i isporučiti šifrirani tekst korisniku kojem je namijenjen. Samo primatelj posjeduje tajni ključ i

samo on može otkriti originalni, jasni tekst. Najpoznatiji asimetrični algoritam je RSA čija kratica predstavlja tri znanstvenika koji su algoritam predstavili javnosti (Rivest, Shamir i Adlerman).

5.3. Mehanizmi zaštite

Pod pojmom mehanizmi zaštite podrazumijeva se autentikacija i integritet. Autentikacijom se nastoji utvrditi identitet korisnika koji sudjeluju u razmjeni informacija, odnosno vrši se provjera jesu li sudionici zaista osobe za koje se smatra da jesu. U telekomunikacijskim sustavima, autentikacija najčešće vrši provjeru identiteta korisnika, ali može obavljati i provjeru identiteta računala, aplikacija i usluga. Postupci identifikacije obavljaju se na temelju triju informacija: nešto što korisnik zna (lozinka ili identifikacijski broj), nešto što osoba ima (sigurnosna značka) i nečeg što osoba jest (otisci prstiju) [9]. Postoje tri vrste autentikacije koje će biti detaljnije opisane u odlomcima koji slijede, a to su: autentikacija zasnovana na korisničkom imenu i lozinci, autentikacija zasnovana na simetričnoj kriptografiji i autentikacija zasnovana na asimetričnoj kriptografiji. Isto tako, autentikacija može biti jednostrana pri čemu se provjerava identitet samo jednog korisnika, obično pošiljatelja i obostrana gdje se provjeravaju obje strane koje ostvaruju komunikaciju.

Integritet podataka jamči sigurnost da su podaci stigli na odredište u onom obliku u kojem su poslani, tj. da nisu mijenjani ili uništeni za vrijeme prijenosa komunikacijskim kanalom. Digitalni potpis osigurava cjelovitost i izvornost podataka, a jednostavnom provjerom lako je utvrditi jesu li podaci mijenjani.

5.3.1. Autentikacija zasnovana na korisničkom imenu i lozinci

Autentikacija zasnovana na korisničkom imenu i lozinci obuhvaća tri podvrste koje će se opisati, a to su: statička lozinka, hash lozinka i lozinka za jednokratnu primjenu [9].

Telekomunikacijski sustavi za autentikaciju statičkom lozinkom koriste postojane lozinke ili se lozinke rijetko mijenjaju. Scenarij koji se često javlja u mreži je taj da se lozinka komunikacijskim kanalom prenosi u izvornom obliku, bez da se prethodno kriptira. Sigurniji način prijenosa uveden je kasnije i njime se lozinka nastoji kodirati prema Base64 formatu. Lozinka se u tom slučaju ne prenosi u izvornom obliku, ali se vrlo lako i jednostavno može pretvoriti ponovo u originalni oblik. S obzirom na slabe zaštitne mehanizme, statičke lozinke su vrlo nepouzdano sredstvo zaštite po pitanju sigurnosti [9].

Hash lozinkom nastoji se načiniti sažetak lozinke i taj sažetak se šalje mrežom. U tom slučaju protivnik nije u mogućnosti otkriti izvornu lozinku je hash funkcija nije inverzna. Isto tako, mogućnost napada ne može se u potpunosti isključiti jer je moguće ponoviti sažetak lozinke. Ovakva vrsta napada može se izbjeći ako se sažetak napravi kombinacijom lozinke i podataka koji su primljeni od strane autentikacijskog sustava.

Lozinka za jednokratnu primjenu jedna je od najčešće primjenjivanih u slučaju kada autentikacija zahtijeva korisničko ime i lozinku, odnosno u sustavima gdje je potrebno osigurati visoku razinu zaštite i pouzdanosti. Kao što sam naziv kaže, lozinka se može koristiti samo jednom i samim time se isključuje mogućnost napada ponavljanjem poruke. Lozinke se generiraju na strani korisnika, a za generiranje korisnik koristi sigurnosne značke.

5.3.2. Autentikacija zasnovana na simetričnoj kriptografiji

Vrste autentikacije koje za svoj rad koriste kriptografske metode zahtijevaju poznavanje ključa koji omogućuje kriptiranje i dekriptiranje poruka koje se šalju mrežom. Autentikacija zasnovana na simetričnoj kriptografiji koristi se za jednostrano utvrđivanje autentičnosti, a mogu je provesti oba sudionika koji su prethodno razmijenili tajni simetrični ključ. Pretpostavka i je prethodna razmjena tajnog ključa za ostvarivanje simetrične kriptografije poruka.

5.3.3. Autentikacija zasnovana na asimetričnoj kriptografiji

Asimetrični kriptosustavi imaju svojstvo da se poruka koja je kriptirana tajnim ključem pošiljatelja može dekriptirati njegovim javnim ključem. Kako bi se utvrdila autentičnost, asimetrična kriptografija koristi se jednostrano i obostrano. Ovakva vrsta autentikacije često se primjenjuje u praksi jer nije potrebna prethodna razmjena simetričnih ključeva korisnika koji sudjeluju u komunikaciji.

5.3.4. Digitalni potpis

Digitalni potpis prema izvoru [9] definira se kao struktura kojom je moguće obuhvatiti tri aspekta sigurnosti: autentičnost, integritet i neporecivost poslanih podataka. Digitalnim potpisom primatelju se jamči autentičnost pošiljatelja i provjera podataka kojom se utvrđuje da isti nisu mijenjani ili uništeni. Kada jednom pošalje poruku, pošiljatelj više nije u mogućnosti poreći da je poruka potekla upravo od njega ako se koristio digitalnim potpisom. Najbliža usporedba digitalnog potpisa je s vlastoručnim potpisom ili otiskom prstiju. Digitalno

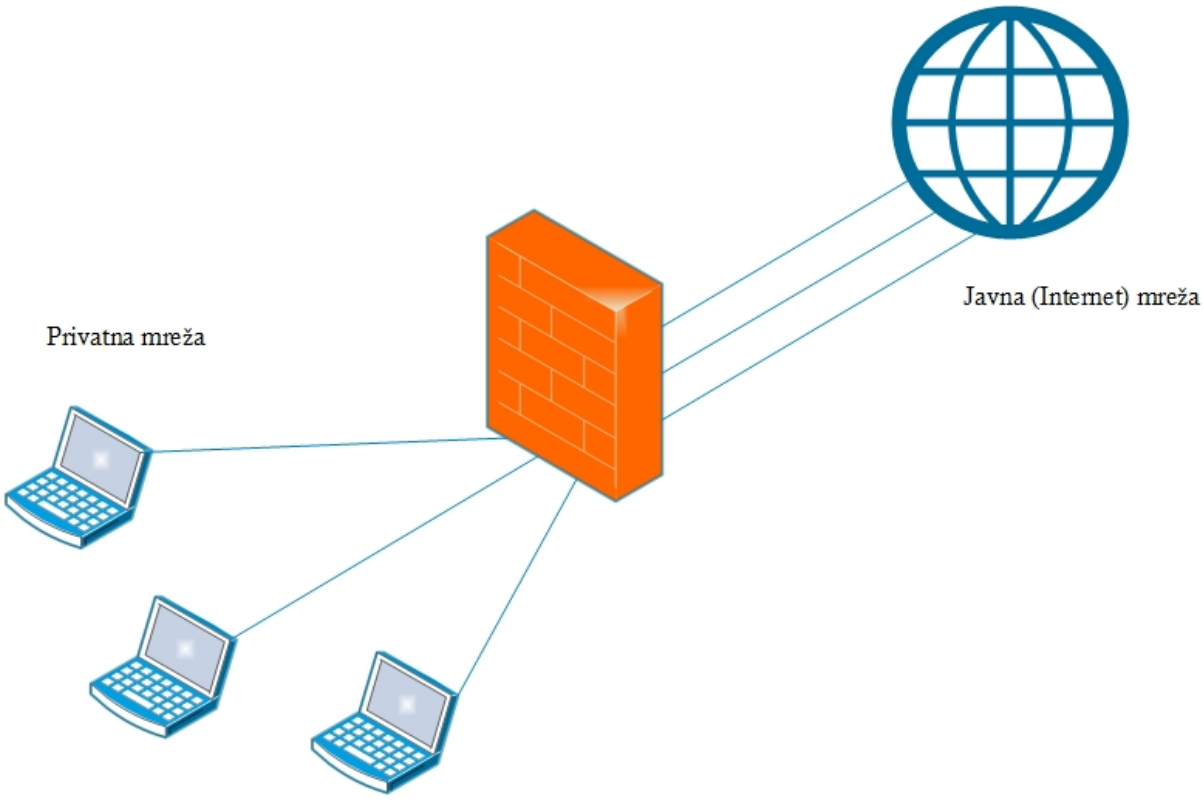
potpisivanje zahtijeva obrnuti postupak od uobičajenog kriptiranja asimetričnom kriptografijom. Naime, za kriptiranje se koristi tajni, a za dekriptiranje javni ključ.

5.3.5. Message digest

Digitalno potpisivanje koristi hash funkcije i asimetričnu kriptografiju. Podaci koji zahtijevaju digitalni potpis služe kao ulazni podaci u kriptografsku hash funkciju. Rezultat hash funkcije su podaci iste duljine i nazivaju se sažetkom poruke, a njihova duljina obično iznosi 128, 160 ili 256 bita [9]. Dobiveni sažetak kriptira se tajnim ključem pošiljatelja i skupa s izvornim podacima šalje se na odredište. Kombinacija izvorne poruke i sažetka poruke koja je kriptirana tajnim ključem pošiljatelja naziva se digitalno potpisanom porukom.

5.4. Vatrozidi

Vatrozidi su sredstva kojima se izolira jedno sigurnosno područje (npr. aplikacija, mreža) od drugog, a smješteni su na ulaznim i izlaznim točkama mreže, krajnjeg uređaja ili aplikacije. Vatrozidi pojedinog mrežnog sloja su obično postavljeni na *gateway* između mreže i Interneta ili mreže davatelja usluga. Vatrozid čine hardverske i softverske metode kontrole pristupa, a cilj je očuvati sigurnost unutar privatne mreže. Često je dopušten pristup korisnicima privatne mreže na Internet, ali pristup s Interneta na privatnu mrežu nije moguće ostvariti, prikazano na slici 7.



Slika 7. Uloga vatrozida

Skup raznih mehanizama koji čine vatrozid služe za sprječavanje prometa paketa u mreži i omogućavanje prometa paketa u mreži. kao što je već spomenuto, vatrozidi se postavljaju na granici mreže kako bi se omogućio pristup drugim mrežama. Ta stavka je vrlo bitna jer vatrozidi jednim dijelom obavljaju funkcije računala i tako računala ne troše vlastite resurse. Zaštita telekomunikacijske mreže vatrozidom podrazumijeva prolazak prometa kroz jednu kontrolnu točku, tj. stvaraju se „uska grla“ između privatne i javne mreže. Što se tiče kašnjenja u mreži uzrokovano vatrozidom, ono se može zanemariti. Izvor [9] navodi četiri osnovne funkcije vatrozida:

- paketno filtriranje kojim se odbacuju neželjeni mrežni paketi s obzirom na izvorišnu adresu računala, odredišnu adresu računala ili vrstu podataka koji se šalju mrežom.
- maskiranje mrežnih adresa obuhvaća pretvorbu mrežnih adrese privatne mreže kako bi se zaštitila tajnost mrežne konfiguracije.
- posrednu uslugu obavlja posebna aplikacija ili određeni program kojim se želi ostvariti veza između klijentskog i serverskog računala s ciljem zaštite identiteta korisnika privatne mreže.

- virtualnom privatnom mrežom kriptografski se zaštićuju podaci tako da se javna mreža predstavlja kao privatna.

Vatrozidi mogu biti smješteni na bilo kojem mrežnom sloju u protokolnom složaju, od fizičkog pa sve do aplikacijskog sloja. Vatrozidi koji su locirani na aplikacijskom sloju predstavljaju učinkovit način čišćenja ulaza od nepovjerljivih izvora podataka.

6. Buduće smjernice i sigurnosne preporuke

Najsigurnijom mrežom koja bi imala najmanje šanse da bude ugrožena s bilo kojeg sigurnosnog aspekta, smatrala bi se ona mreža koja nema direktnu vezu s vanjskim svijetom, u kontekstu ovog rada s Internetom [1]. Takva mreža u praksi gotovo da i ne postoji jer je prisutnost web-a neizostavna stavka u poslovnom svijetu. Kako bi se postigla ravnoteža između mrežne sigurnosti i potrebe korisnika, potrebno je zauzeti sigurnosni stav koji će još uvijek omogućiti pristup podacima. Iako se korisnici smatraju primarnim akterima neke poslovne organizacije, oni su također najveći potencijalni izvor „zaraze“ informacijskog podsustava. Naime, ako poslovni sustav dopušta pristup korisnicima, vrlo je teško zaustaviti zlonamjerni napad. Sigurnosni sustav trebao bi biti najjači što može i raditi u skladu s količinom prijetnji koje nastoje pristupiti mreži. Isto tako, važno je uhvatiti korak s najnovijim tehnologijama i održavati sigurnosne sustave kako bi mreža tako bila otporna na nove prijetnje koje se pojavljuju. Edukacija korisnika postaje bitan čimbenik u telekomunikacijskim tehnologijama. Gubitak službenih uređaja, korištenje istih na mjestima gdje protivnik lako može uočiti lozinke i povjerljive podatke i pristup nesigurnim bežičnim mrežama samo su neke od opasnosti koje mogu nastupiti kao posljedice ljudske nepažnje.

6.1. Buduće smjernice

Mobilne i tradicionalne telekomunikacije naveliko su bile ignorirane po pitanju sigurnosti od strane mrežnih organizacija i obrazovnih institucija. Telekomunikacijski sustavi bili su redizajnirani i obnovljeni puno više puta nego što je to slučaj s Internetom. S obzirom na to, pojedini sustavi ukazali su se kao prilika istraživačima koji su unijeli promjene velikih razmjera u područje telekomunikacijskih tehnologija. Knjiga [1] smatra da bi se sigurnosni mehanizmi trebali primijeniti u sljedećim komponentama telekomunikacijske mreže:

- SS7: Kao i kod mnogih naprednih tehnologija, skokovit razvoj IMS-a (IP Multimedia Subsystem), višemedijskog podsustava zasnovanog na Internet protokolu, ne može u potpunosti nadomjestiti sve SS7 sustave. Prema tome, dok postoji mnoštvo sigurnosnih rješenja u jezgrenom dijelu mreža koje se trenutno koriste, pojedini sustavi kao SS7 trebaju dodatnu sigurnosnu analizu.
- IMS: S obzirom na to da se IMS temelji na IP tehnologiji, sigurnosni izazovi ove mreže nešto su drugačiji nego kod Interneta. Prema tome, sustavi imaju zadatak osigurati

komunikaciju u stvarnom vremenu, a istraživačima prilično veliki izazov predstavlja ravnomjerno rasporediti promet unutar mreže.

- SS7/IMS/Internet usklađivanje: Za vrijeme razvoja IMS mreža bilo je za očekivati da će pojedini sustavi morati osigurati interoperabilnost s drugim mrežama. Implikacije koje mogu nastati ako se dovoljno ne razradi pitanje interoperabilnosti, protivnik lako može iskoristiti tako da ometa promet unutar različitih sustava.
- Mobilni terminalni uređaj: Krajnjim uređajima u telekomunikacijskoj mreži nedostaju „alati“ koji bi osigurali dobru i ispravnu interakciju s mrežom. Iako uređaj sam po sebi nije u mogućnosti suočiti se s problemima koji su mogući u mreži, ima ulogu u minimizaciji zlonamjernih napada.
- Aplikacije temeljene na mreži: Ekspanzija aplikacija svakodnevno zahtijeva analizu svakog pojedinog sigurnosnog zahtjeva od strane zajednica koje brinu o sigurnosti. Naglasak nije samo na povjerljivosti i integritetu, već i na privatnosti korisnika.
- Kontrola preopterećenja: Kako bi se rasteretili pojedini linkovi u mreži, nastoje se konstruirati „inteligentniji“ mehanizmi koji će osigurati protok prometa na najučinkovitiji način. Mehanizmi također trebaju biti sposobni ispuniti zahtjeve različitih vrsta prometa, npr. real time vs. best effort.

6.2. Sigurnosne preporuke

Sigurnosnim preporukama nastoji se spriječiti napad na mrežu, a u ovom radu opisat će se: sigurnosna politika, analiza rizika, alati i kontrola korisničkog pristupa.

6.2.1. Sigurnosna politika

Sigurnosna politika treba konstantno pratiti napredak. Mora se razvijati zajedno s tehnologijom, osobito s tehnologijama kojima je cilj potajno ući u sustav. Dobra sigurnosna politika nije uvijek samo običan dokument, već skup raznih politika koje se mogu odnositi na: adresiranje određenih područja (računalnu i mrežnu uporabu), autentikaciju, e-mail politiku, korištenje mobilne/bežične tehnologije i politika web pretraživanja. Sigurnosna politika mora biti opisana na opsežan i razumljiv način kako bi bila učinkovita. Prije uvođenja sigurnosne politike u sustav, potrebno je imati uvid u mrežu i mrežne komponente. Knjiga [4] smatra da bi prije uvođenja politike trebalo odgovoriti na nekolicinu pitanja kao što su:

- Koje vrste resursa je potrebno zaštititi (novčani podaci, informacije o kreditnoj kartici korisnika i sl.)?

- Koliki broj korisnika bi imao pristup mreži (zaposlenici, izvođači radova)?
- Treba li se pristup sustavu omogućiti samo u ključnim trenucima ili 24/7?
- Hoće li se omogućiti daljinski pristup mreži korisnicima, i ako da, koliko će ih biti?

Nadalje, potrebno je detaljno objasniti koji sigurnosni zahtjevi moraju biti ispunjeni, komunicirajući pritom s korisnicima i definirati ulogu mrežnog administratora. Sigurnosnu politiku obično kreira sigurnosni tim tako da bude što praktičnija, korisnija i održiva. Sigurnosna politika treba sadržavati planove koji će se provesti u slučaju prijetnji na sustav, kao i raspored ažuriranja opreme i softvera. Vrlo važnu ulogu imaju već spomenuti vatrozidi kojima se ne dopušta promet određenih podataka kroz mrežu. Također je bitno osvrnuti se na korisnike koji pokušavaju neovlašteno pristupiti sustavu, uzimajući pri tome datoteke ili podatke.

6.2.2. Analiza rizika

Analizu rizika potrebno je definirati u slučaju pojave rizika kod raznih operacija koje se događaju u sustavu. Kod jednostavne extranet/intranet mreže prosječna zaštita vatrozidom može biti dovoljna za mala poduzeća koja ne posjeduju veliku količinu povjerljivih podataka koji mogu biti ukradeni. Međutim, takav način zaštite vatrozidom neće biti od koristi kompanijama koje posjeduju financijskim podacima i korisničkim informacijama. U tom slučaju potreban je „slojevit“ sistem, odnosno sigurna mreža koja nije konektirana na Internet. Takva mreža može se ostvariti od strane korisnika na fizičkom računalu, a podaci mogu biti premještani samo fizičkim medijem.

Sigurnosna politika koja uključuje analizu rizika treba provoditi testiranje ranjivosti sustava. Alati kojima je to moguće ostvariti su: WebInspect, Acunetix, Nessus i sl. [4]. Nadalje, postoje tvrtke koje se bave isključivo skeniranjem mreže koja sadrži dostupne priključke, vatrozide i ranjive web stranice. Najmodernijim paketom alata moguće je provesti testiranje kritičnih točaka i sustava zaštite u mreži.

Sustav revizije također je važno spomenuti kao sigurnosnu preporuku. Zadatak takvog sustava je promatrati promet paketa u mreži tijekom dana. Za vrijeme radnog vremena točno se zna koliki promet se može očekivati kroz mrežu s obzirom na dužnosti koje zaposlenici poduzeća imaju. Međutim, kada je promet izvan očekivanog, vrlo vjerojatno se nešto događa na mreži što je potrebno istražiti. Postoji mogućnost da zaposlenici preuzimaju

glazbene ili video datoteke i time povećavaju promet, ali isto tako povećanje može upućivati na protivnika koji se spojio na mrežu nelegitimnim putem.

Ako dođe do napada potrebno je realizirati prethodno definiran plan koji rješava pitanja oporavka mreže nakon napada. Potrebno je riješiti probleme rekonfiguracije mreže, procjenu štete itd. „Oporavak“ sustava složena je operacija jer se može zaustaviti rad pojedinih jedinica poduzeća na nekoliko dana, ako ne i više. U slučaju zaraze sustava virusom, slanje i primanje e-pošte onemogućeno je sve dok se zaraženi sustav ne očisti. Prema tome, potrebno je voditi računa o spomenutom planu u slučaju katastrofe kako bi bio učinkovit i zadovoljio trenutno stanje na mreži. Aktivnosti kao što su obavijesti o mogućim prijetnjama, ažuriranje softvera i aplikacija, procjena ranjivosti sustava, pojava novih aplikacija koje možda sadrže neke nepravilnosti samo su neki od zadataka koje sigurnosni plan mora riješiti.

6.2.3. Alati

Iako su alati dostupni napadačima koji žele neovlašteno ući u sustav, postoji niz alata kojima je moguće ostvariti jaku sigurnost sustava. Prije nego što se implementira sigurnosna strategija, treba znati tko će točno koristiti resurse tvrtke. Jednostavni alati protiv crva i spama nisu dovoljni s obzirom na današnji skokovit razvoj raznih softvera i programa.

Kao vodeći obrambeni alat spominje se vatrozid, opisan u prethodnom poglavlju. Knjiga [4] navodi kako je Sidewinder od strane Secure Computing-a jedan od najsigurnijih dostupnih vatrozida i do sada nikada nije bio u potpunosti hakiran. Korišten je od strane vladinih i zaštitnih agencija. Siguran sustav vatrozida podrazumijeva pet stavki: sam vatrozid, antivirusni/antispam program, virtualnu privatnu mrežu i sustav za detekciju/prevenciju.

IPS (Intrusion Prevention System) razvijeniji je odnosu na vatrozid jer automatski sprema sumnjive pakete u posebnu mapu. Također je vrlo učinkovit jer lako raspoznaje pravu prijetnju od lažne i tako propušta pakete do odredišta. Postoji više vrsta IPS-a [4]:

- IPS koji se temelji na mreži
- IPS koji se temelji na krajnjim uređajima
- IPS koji se temelji na sadržaju
- IPS koji se temelji na stopi

IPS-om je potrebno ostvariti zaštitu za aplikacije, krajnjih uređaja i pojedinih elemenata mreže. Također treba štititi od prijetnji koje iskorištavaju ranjivost u određenim aplikacijama,

kao što su VoIP, e-pošta i sl. Otkrivanje i uklanjanje crva, virusa i trojanskih konja IPS isto mora ostvariti.

UTM (Unified Threat Management) je najnoviji trend kojim se nastoji spriječiti prijetnja sustavu. Pruža različite mogućnosti kao antivirus, VPN, usluga vatrozida, antispam, kao i prevenciju upada. Najveće prednosti su jednostavnost rada i konfiguracija. S obzirom na to da se njegove sigurnosne značajke mogu brzo ažurirati, prijetnje se relativno rano otkriju.

6.2.4. Kontrola korisničkog pristupa

Tradicionalni korisnici, tj. zaposlenici predstavljaju najslabiji obrambeni mehanizam kada se radi o sigurnosti [4]. Postavlja se pitanje kako zaposlenicima omogućiti neometan rad unutar mreže dok je u procesu kontrola njihova pristupa u mreži. Naime, za to je zadužen autentikacijski sustav koji mora biti sposoban prepoznati o kojem korisniku je riječ.

Autentikacija, autorizacija i računovodstvo poduzeća vodi računa o korisničkom identitetu. U mrežnim tehnologijama, fizički dokaz poput osobne iskaznice ne može biti upotrebljen kao dokaz identiteta. U svijetu telekomunikacija, korisnik ostavlja „trag“ da je bio povezan sa sustavom putem korisničkom imena koje mu je dodijeljeno, vremenu registracije u sustav i resursima kojima ima dozvoljen pristup. Veliki broj korisnika kao jednostavan način autentikacije koriste vrlo nesigurne lozinke kao što su datum rođenja i sl. Kako bi se povećala učinkovitost sigurnosnog sustava, potrebno je provesti mnogo jači oblik autorizacije. Kao najjače sredstvo autentikacije izvor [4] navodi kombinaciju hardverskog uređaja (token, pametne kartice, biometrijski uređaji) i nečega što korisnik zna kako bi mogao izvršiti prijavu u sustav.

7. Zaključak

Završnim radom pod nazivom *Sigurnost primjene telekomunikacijskih mreža* opisane su arhitekture mreža, prijetnje i ranjivosti usluga koje se koriste u mreži te neki od načina kako najbolje zaštititi mrežu. U prošlosti telekomunikacijske tehnologije nisu zahtijevale tako opsežne i pouzdane sigurnosne mehanizme i zaštitu. Jedan od razloga je što danas gotovo svaka nova tehnologija koja se razvije funkcionira preko Internet Protokola (IP), a Internet sam po sebi predstavlja otvorenu i vrlo nesigurnu mrežu.

Analizom arhitektura pojedinih mreža, uočljivo je da one sadrže relativno veliki broj komponenata koje mogu biti metom napada i nije uvijek jednostavno primijeniti sustav sigurnosti u svaki dio mreže. Sprječavanje napada na telekomunikacijsku mrežu nije nimalo lak zadatak, i bez obzira koliko dobro sigurnosni mehanizmi rade u ovom trenutku, samo je pitanje vremena kada će protivnik razviti „alat“ kojim će se probiti do mreže. Dakle, sigurnost je potrebno razvijati iz dana u dan, u skladu s promjenama u tehnologiji, jer ako je danas sve u redu, ne znači da sutra neće doći do napada. Potrebno je ulagati u kvalitetne, višenamjenske sigurnosne sustave koje je lako instalirati i implementirati. Važno je da se brzo prilagođavaju i konfiguriraju u ovisnosti o potrebama, te da drže korak s aktualnim trendovima u telekomunikacijama.

Literatura

[1] Traynor, P., McDaniel, P., La Porta, T. Security for Telecommunications Networks. New York: Springer; 2008.

[2] Ousley, M. R. Information Security, Second Edition. USA: The McGraw-Hill Companies; 2013.

[3] Bidgoli, H. Handbook of Information Security, Volume 3. Canada: John Wiley & Sons, Inc.; 2006.

[4] Vacca, J. R. Network and System Security. Oxford: Elsevier Inc.; 2010.

[5] Hao Liu, L. Security Of VoIP Networks. 2nd International Conference on Computer Engineering and Technology; IEEE; China; 2010; V3-104-108 str.

[6] By Cloudmark. SMS Spam and Mobile Messaging Attacks Introduction, Trends and Examples; London; 2011.

[7] Moore, T., Kosloff, T., Keller, J., Manes, G., Shenoi, S. Signaling System 7 (SS7) Network Security. Center for Information Security; IEEE; USA; 2002; III-496-499 str.

[8] Chasaki, D., Wolf, T. Attacks and Defense in the Data Plane of Networks. IEEE Transactions on dependable and secure computing, vol. 9, no. 6. US; 2012; 799-810 str.

[9] Kavran, Z. Računalne mreže, autorizirana predavanja s e-Studenta. Fakultet prometnih znanosti; Zagreb; 2014.
http://e-student.fpz.hr/Predmeti/R/Racunalne_mreze/Materijali/10_Predavanje.pdf,
preuzeto 20.4.2015.

[10] Mrvelj, Š.: Tehnologija telekomunikacijskog prometa, autorizirana predavanja s e-Studenta. Fakultet prometnih znanosti; Zagreb; 2014.
http://e-student.fpz.hr/Predmeti/T/Tehnologija_telekomunikacijskog_prometa_I/Materijali/9_predavanje.pdf,
preuzeto 20.4.2015.

[11] Federal Communications Commission. Voice over Internet Protocol (VoIP), 2015.
https://www.fcc.gov/encyclopedia/voice-over-internet-protocol-voip,
preuzeto 16.5.2015.

[12] Beal, V. Short Message Service. Webopedia, 2015.
http://www.webopedia.com/TERM/S/short_message_service.html;

preuzeto 24.5.2015.

[13] Gledec, G. Sigurnost i privatnost. Fakultet elektrotehnike i računarstva; Zagreb, 2014.

www.fer.unizg.hr/_download/repository/Sigurnost-i-privatnost.pdf,

preuzeto 8.5.2015.

Popis kratica:

2G (2nd Generation) druga generacija mobilnih mreža

3G (3rd Generation) treća generacija mobilnih mreža

4G (4th Generation) četvrta generacija mobilnih mreža

AES (Advanced Encryption Standard) napredan enkripcijski standard

AMPS (Advanced Mobile Phone System) napredan sistem mobilne telefonije

ARP (Address Resolution Protocol) protokol za rješavanje adresa

BSC (Base Station Controller) kontrolor baznih stanica

BTS (Base Transceiver Station) sustav baznih stanica

CDMA (Code-Division Multiple Access) raspodjela kanala po kôdu

CMSDBs (Call Management Services Databases) baza podataka koja obrađuje besplatne brojeve

DES (Data Encryption Standard) podatkovni enkripcijski standard

DHCP (Dynamic Host Configuration Protocol) protokol koji dodjeljuje IP adrese i mrežne postavke

DNS (Domain Name System) sustav ili sredstvo spojeno na Internet ili privatnu mrežu

DoS (Denial of Service) napad kojim se nastoji onesposobiti ili narušiti kvaliteta sustava

EDGE (Enhanced Data Rates for GSM Evolution) generacija mobilnih mreža gdje brzine sežu do 200 kbit/s

FDMA (Frequency-Division Multiple Access) raspodjela kanala po frekvenciji

GGSN (Gateway GPRS Support Node) glavna komponenta GPRS mreže

GPRS (General Packet Radio Service) omogućuje prijenos podataka u GSM mreži

GSM (Global System for Mobile Communications) standard za mobilnu telefoniju

HLR (Home Location Register) registar domaćih korisnika

ICMP (Internet Control Message Protocol) protokol koji šalje kontrolne poruke o greškama

IDEA (International Data Encryption Algorithm) enkripcijski algoritam

IMS (IP Multimedia Subsystem) višemedijski podsustav zasnovan na IP-u

IMSI (International Mobile Subscriber Identity) primarni ključ za HLR zapis

IN (Intelligent Network) mrežna arhitektura specificirana od strane ITU-T

IP-a (Internet Protocol) Internet protokol

ISUP (ISDN User Part) dio SS7 mreže odgovoran za uspostavu telefonskih poziva u PSTN-u

MAP (Mobile Application Part) aplikacijski sloj SS7 mreže

MGCP (Media Gateway Control Protocol) protokol za kontrolu media gateway-a baziranog na IP-u povezanog na PSTN

MSC (Mobile Switching Centre) komutacijsko čvorište ćelijske mreže

MSISDN (Mobile Station ISDN) telefonski broj mobilnog telefona

MTP (Message Transfer Part) temelj strukture SS7 mreže

MTP1 (Message Transfer Part Level 1) fizički sloj SS7 mreže

MTP2 (Message Transfer Part Level 2) sloj veze podataka u SS7 mreži

MTP3 (Message Transfer Part Level 3) mrežni sloj u SS7 mreži

NSP (Network Services Part) cjelina MTP-a i SCCP-a u SS7 mreži

PIN (Personal Identification Number) osobni identifikacijski broj

PSTN (Public Switched Telephone Network) javna telefonska mreža

QoS (Quality of Service) kvaliteta usluge

RTCP (Real-Time Control Protocol) protokol za razmjenu informacija i podataka u stvarnom vremenu

SCCP (Signaling Connection Control Part) kontrolni dio SS7 mreže odgovoran za konekciju

SCP (Service Control Point) baza podataka SS7 mreže

SDP (Socket Direct Protocol) protokol koji omogućuje pristup visokim performansama mreže

SGSN (Serving GPRS Support Node) dio GPRS mreže koji pohranjuje podatke o korisniku

SIM (Subscriber Identity Module) kartica na koju je pohranjen IMSI

SIP (Session Initiation Protocol) protokol koji upravlja multimedijskim porukama koje koriste IP

SMS (Short Message Service) usluga kratkih tekstualnih poruka

SMSC (Short Message Service Center) centar koji prosljeđuje poruku na odgovarajući terminalni uređaj u SMS usluzi

SS7 (Signalling System No. 7) signalizacijska mreža 7

SSP (Service Switching Point) signalizacijska točka u SS7 mreži

STP (Signal Transfer Point) ruteri u SS7 mreži

TACS (Total Access Communication System) analogni sustav koji omogućuje komunikaciju

TCAP (Transactions Capabilities Application Part) obavlja transakcije u aplikacijskom dijelu SS7 mreže

TCP/UDP (Transmission Control Protocol/User Datagram Protocol) protokoli za konekciju i slanje podataka od jednog hosta prema drugom

TDMA (Time-Division Multiple Access) raspodjela kanala po vremenskim slotovima

TFTP (Trivial File Transfer Protocol) protokol koji se koristi za prijenos datoteka korištenjem UDP-a

UMTS (Universal Mobile Telecommunications System) generacija mobilne mreže nakon GSM-a

UTM (Unified Threat Management) vrsta zaštite protiv zlonamjernih napada

VLAN (Virtual Local Area Network) virtualna lokalna mreža

Popis slika:

Slika 1. Komponente sigurnosnog programa 8
Slika 2. Razvoj generacija mobilnih mreža 11
Slika 3. Struktura mreže za prijenos podataka 15
Slika 4. Usporedba IP i SS7 protokola. 17
Slika 5. Prikaz meta, ciljeva i primjera napada. 19
Slika 6. Postupak šifriranja 30
Slika 7. Uloga vatrozida 35

Popis tablica:

Tablica 1. Vrste napada na VoIP uslugu 22

#

Popis grafikona:

Graf 1. Aktivnosti korisnika 5

Graf 2. Prosječan postotak blokiranja napada. 25