

Departman za postdiplomske studije

Studijski program

Savremene informacione tehnologije

Organizacija velikog informacionog sistema

i kako ga zaštititi

Mentor:

Prof. dr. Mladen Veinović

Kandidat:

Tamara Velanac

br. indeksa: 410219/2012

Beograd, 2014. godina

S A D R Ź A J

1. Metodologija.....	1
1.1 Uvodne napomene i obrazloženje rada	1
1.2 Predmet istraživanja.....	1
1.3 Ciljevi i zadaci istraživanja	2
1.4 Istraživačke hipoteze.....	2
1.4.1 Opšta hipoteza	2
1.4.2 Metod istraživanja	2
2. Istorijat računarskih mreža [7].....	3
3. Zašto pravimo mreže [10]	11
3.1 Podela računarskih mreža [6]	11
3.1.1 Površina koju mreža pokriva	11
3.1.1.1 Local Area Network (LAN).....	11
3.1.1.2 Personal Area Networks (PAN)	12
3.1.1.3 House Area Network (HAN).....	13
3.1.1.4 Metropolitan Area Networks (MAN)	13
3.1.1.5 Wide Area Network (WAN)	13
3.1.1.5.1 Enterprise Private Network (EPN).....	15
3.1.1.5.2 Virtual Private Network (VPN)	15
3.1.1.6 Global Area Networks (GAN)	16
3.1.2 Prema odnosu nodova u mreži	16
3.1.2.1 Peer – to – Peer (P2P)	16
3.1.2.2 Client – Server.....	17
3.1.3 Prema mrežnoj topologiji.....	18
3.1.3.1 Point-to-Point	18
3.1.3.2 Bus (Magistrala)	19
3.1.3.3 Star.....	20
3.1.3.4 Ring (Prsten).....	21
3.1.3.5 Mesh.....	22
3.1.3.6 Tree	24
3.1.3.7 Hybrids.....	25
3.1.4 Prema načinu povezivanja.....	26
3.1.4.1 Žične [16].....	26

3.1.4.2 Bežične [22]	30
3.1.5 Prema kapacitetu prenosa podataka.....	32
3.1.5.1 Mreže osnovnog opsega	32
3.1.5.2 Mreže širokopojasnog opsega.....	33
3.1.6 Prema logičkom i fizičkom rasporedu čvorova.....	33
3.1.7 Prema specifičnim funkcijama	33
3.1.7.1 Storage Area Networks (SAN)	33
3.1.7.2 Server farms [38]	33
3.1.7.3 Process control networks.....	34
3.1.7.4 Value added network.....	34
3.1.7.5 SOHO network.....	34
3.1.7.6 Wireless Community Network	34
3.1.7.7 XML Appliance Network.....	34
4. Da li računari stvarno razgovaraju ?.....	34
4.1 Šta u stvari ovo omogućava ?.....	34
4.2 OSI model [25] [26] [27] [3] [9] [5].....	35
4.2.1 Fizički sloj (<i>Physical layer</i>)	36
4.2.2 Sloj veze (<i>Data Link Layer</i>).....	36
4.2.3 Mrežni sloj (<i>Network Layer</i>)	36
4.2.4 Transportni sloj (<i>Transport Layer</i>).....	36
4.2.5 Sloj sesije (<i>Session Layer</i>)	37
4.2.6 Sloj prezentacije (<i>Presentation Layer</i>)	37
4.2.7 Aplikativni sloj (<i>Application Layer</i>).....	37
4.3 Enkapsulacija podataka.....	37
4.4 Protokoli [3] [4].....	38
4.4.1 TCP/IP [27] [29] [30] [9].....	39
4.4.1.1 TCP/IP Stack [32] [29] [30] [9].....	40
4.4.1.1.1 TCP Protocol.....	40
4.4.1.1.2 IP Protocol.....	42
4.4.1.1.2.1 IPv4.....	43
4.4.1.1.2.2 IPv6.....	45
4.4.1.1.2.3 Razlike između IPv4 i IPv6.....	46
4.4.2 UDP Protocol	47
4.4.3 DHCP (Dynamic Host configuration Protocol)	48

4.4.4	DNS (Domain Name System)	49
4.4.5	HTTP (Hypertext Transfer Protocol).....	49
4.4.6	FTP (File Transfer Protocol)	50
4.4.7	SMTP (Simple Mail Transfer Protocol)	51
4.4.7.1	Proces.....	51
5.	Zaštita mreže [1].....	52
5.1	Digitalni potpis i Enkripcija [2] [8]	56
5.2	Digitalni potpis [2] [8]	61
5.3	Digitalni sertifikat [2] [8]	61
5.4	Kerberos Key Exchange [2] [8].....	62
5.5	E-mail.....	63
5.6	Sigurnost operativnog sistema.....	65
5.6.1	Antivirus [1]	67
5.7	Dostupnost [35] [36]	69
5.8	Habovi (Hubs), Svičevi (Network Switches) i Ruteri (Routers).....	72
5.8.1	Hub.....	72
5.8.2	Switch	72
5.8.3	Router.....	74
5.9	Firewall	75
5.9.1	Vrste Firewall-a	77
5.9.1.1	Packet Filtering Firewall.....	77
5.9.1.2	Stateful Inspection Firewall	77
5.9.1.3	Applicaton-Level Gateway	78
5.9.1.4	Circuit-Level Gateway.....	78
5.10	DMZ (Demilitarized Zone)	79
5.10.1	Intrusion Detection i Intrusion Prevention Sistemi	80
6.	Maliciozan softver [3] [2]	81
6.1	Kratka istorija računarskih virusa [5] [6].....	82
6.2	Vrste malicioznog softvera.....	85
6.2.1	Virusi.....	85
6.2.1.1	Tipovi Virusa	86
6.2.1.2	Struktura virusa	87
6.2.2	Worms (Crv)	88

6.2.3	Logic bombs	89
6.2.4	Trojan Horses	89
6.2.5	Mobile code.....	90
6.2.6	Spyware [7]	90
6.2.7	Rootkit [8]	91
6.2.8	Mobile malware	92
6.3	Druge vrste pretnji	92
6.3.1	Honey pots.....	92
6.3.2	Social engineering [9]	94
6.3.2.1	Način zaštite.....	96
7.	Metode napada.....	96
7.1	Brute Force and Dictionary	96
7.2	Denial of Service	97
7.3	Spoofing	100
7.4	Man-in-the-Middle.....	100
7.5	Sniffer napadi	101
7.6	Spamming napadi	102
7.7	Crackers [18]	102
8.	Cyber kriminal [11] [12] [17]	103
9.	Šta kaže zakon ? [1] [11] [17]	105
10.	Susret sa opasnim virusom	108
10.1	O Conficker virusu [15] [14] [13] [19] [20].....	108
10.1.1	Način zaraze i simptomi.....	109
11.	Zaključak	110
12.	Literatura.....	111

1. Metodologija

1.1 Uvodne napomene i obrazloženje rada

U ovom istraživačkom radu se obrađuju pojam i vrste velikih računarskih mreža, pojam, vrste i načini rada malicioznih kodova i ostalih pretnji po velike mrežne strukture, kao i napadi koji se tom prilikom izvode.

Razvoj računarskih sistema donosi konstante promene i unapređenje rada. Način njihovog povezivanja, kako unutar njih samih, tako i između sebe određuje se na osnovu sadržaja i servisa koje će ta mreža pružati. Zbog toga ne sme biti grešaka prilikom određivanja arhitekture sistema, a pogotovo ne sme biti sigurnosnih propusta. Savremeni poslovni svet se kompletno okrenuo digitalizaciji i oslanjanju na mašine kako bi unapredio svoje poslovanje, a samim tim i povećao svoj kapital. Time se ubrzavaju i umnožavaju usluge koje pružaju svojim korisnicima. Međutim, podatke koje ove firme i organizacije koriste za svoj razvoj i napredovanje potrebno je zaštititi od raznih spoljašnjih i unutrašnjih malicioznih uticaja.

Ovaj rad će predstaviti vrste mreža, tehnologije povezivanja, kao i način zaštite savremenih mreža, vrste malicioznih kodova, vrste napada i moguće načine odbrane.

1.2 Predmet istraživanja

Ovaj rad se bavi nastankom i vrstama mreža, kao i tehnologijama koje se koriste kako bi mreže radile što brže i sigurnije. Obrađuje metode povezivanja uređaja i protokole kojima se to čini, pojedine servise, kao i načinom prilaza fajlovima. Objašnjava kako se mreže mogu zaštititi, odnosno hardverska i softverska rešenja zaštite. Takođe, baviće se nastankom malicioznih kodova, njihovim razvojem, kao i napadima koji se odigravaju implementacijom ovih virusa. Obrađivaće način odbrane od napadača za pojedinačne maliciozne kodove, načine kako umanjiti šanse da se mreža zarazi, ali i zakonske norme koje se odnose na *cyber* kriminal, kako u svetu, tako i kod nas. U poslednjem delu govori se o ličnom iskustvu autora ovog teksta sa jednim od najznačajnijih virusa u istoriji *IT* industrije.

1.3 Ciljevi i zadaci istraživanja

Naučni cilj ovog rada jeste sistematizacija znanja iz oblasti podele računarskih mreža, vrste i načina komunikacije između uređaja, protokoli koji se koriste za komunikaciju, zaštita mreže od unutrašnjih i spoljašnjih napadača, hardver preko kojeg se vrši komunikacija, kao i o pametnoj podeli mreže kako bi se što bolje zaštitila kompletna infrastruktura, zatim znanja iz oblasti posvećenoj malicioznim kodovima, vrstama i načinima njihovog rada, napadima koji se tom prilikom odigravaju, metodama otkrivanja, kao i rezultatima njihovog delovanja.

Takođe, cilj je i predstavljanje najnovijih rešenja iz domena računarskih mreža, njihova primena u praksi, kao i predstavljanje rezultata koje su ova rešenja postigla.

1.4 Istraživačke hipoteze

1.4.1 Opšta hipoteza

Od pojave računara javila se potreba za deljenjem resursa, pa se iz tog razloga pojavljuju i prve mreže. Kako se povećavao broj servisa, tako je rasla i kompleksnost mrežnih okruženja. Dostupnost i brzina razmene podataka je od krucijalnog značaja za dobru i kvalitetnu uslugu, kakvu žele vlasnici firmi i organizacija koje na ovaj način organizuju svoje poslovanje. Zbog toga je neophodno dobro poznavanje vrsta i načina rada mreža, kako bi se odabralo najbolje rešenje za kompaniju ili organizaciju.

1.4.2 Metod istraživanja

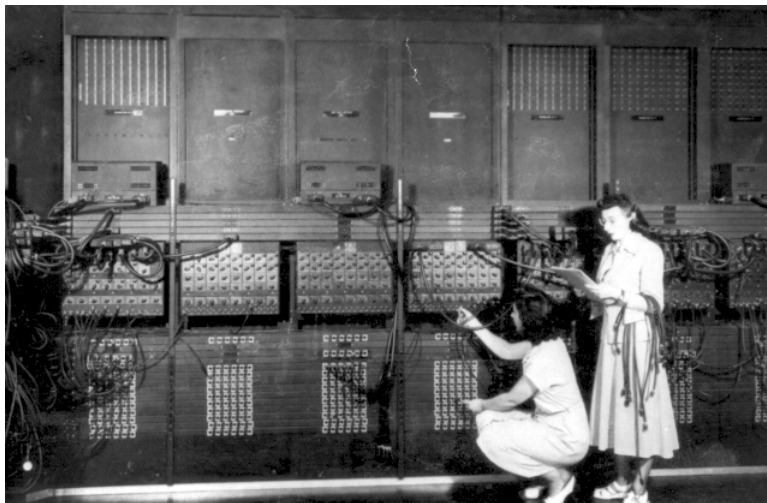
Ovo istraživanje imalo je multimetodijski karakter i sastojalo se od analize svih dostupnih izvora - naučnih radova, naučne literature i izvora sa Interneta. Analizirana su izlaganja mnogih priznatih stručnjaka iz ove oblasti, kako bi se izdvojile najbitnije činjenice koje su izložene u ovom radu. Vršena je pretraga najnovijih informacijama iz oblasti koje rad pokriva. Ovaj rad obuhvata i izlaganje sopstvenog mišljenja i preporuka, zasnovanih na iskustvu u radu na velikim računarskim mrežama.

2. Istorijat računarskih mreža [7]

Danas se računarske mreže podrazumevaju kao i telefonske. Do ekspanzije Interneta telefonska mreža je bila najveća mreža na svetu, ali se ona nije mogla računati kao računarska mreža, iako su se računari mogli povezati putem modema. Takvo povezivanje je iziskivalo i velike telefonske račune, pogotovo ako je bilo potrebno uspostaviti međugradske pozive. To nije bilo umrežavanje kakvo imamo danas.

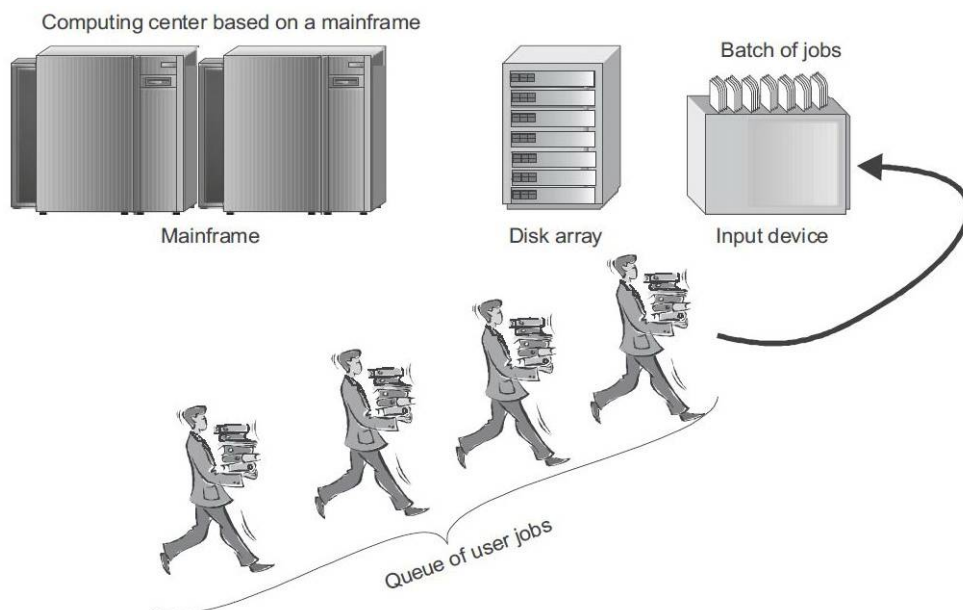
Uticaj kompjuterskih mreža na druge tipove telekomunikacionih mreža rezultiralo je približavanju i spajanju više srodnih mreža u jednu, a koji je proces započeo mnogo pre pojave Interneta. Digitalni prenos glasa u telefonskim mrežama je bio jedan od prvih primera. Noviji primeri su razvoj novih servisa u kompjuterskim mrežama koji su ranije bili vezani isključivo za telefonske, radio i TV mreže.

Umrežavanje u računarske mreže kakvo poznajemo danas razvija se još od 50tih godina prošlog veka. Ti računari su bili veoma veliki, bučni i jako skupi i zauzimali su površine celih zgrada.



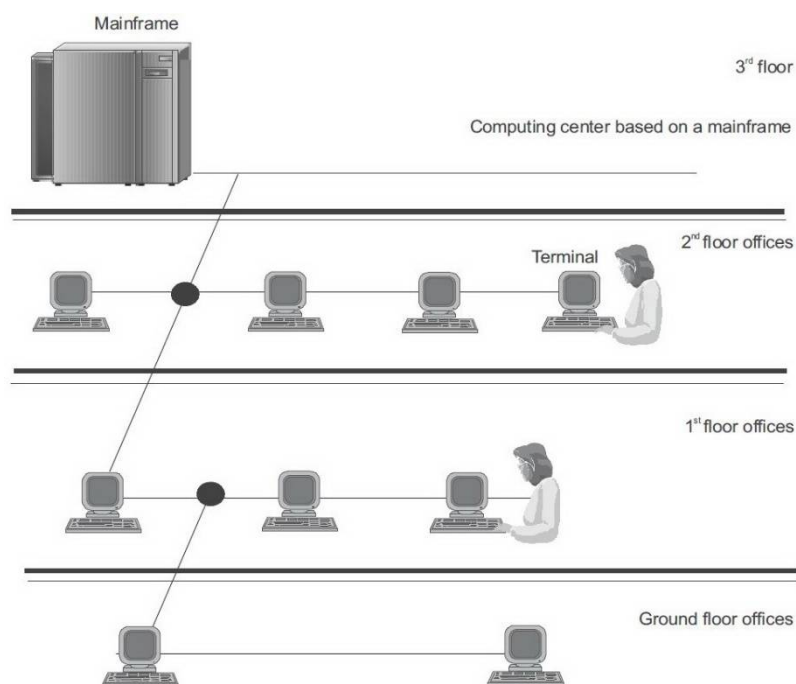
Slika br. 1 – Eniac, prvi elektronski kompjuter (1946 godina) [12]

Prvi sistemi bili su *Batch-processing* sistemi, koji su se zasnivali na *mainframe*-ovima i koji su bili veoma pouzdani. Radili su po sistemu bušenih kartica koji su sadržali određene podatke i kodove programa. Operatori sistema su te kartice ubacivali u kompjuter i rezultati bi bili gotovi tek sledećeg dana. Tako da ukoliko bi kartica sadržala grešku došlo bi do odlaganja od 24 časova.



Slika br.2 – Centralizovan sistem baziran na mainframe [7]

U prvoj dekadi druge polovine XXog veka procesori su postali jeftiniji pa se mogla obratiti pažnja i na udobnost krajnjih korisnika. Tada se javljaju prvi multiterminalni sistemi. Svaki korisnik je imao svoj terminal sa kojeg je mogao da komunicira sa računarom. Odzivno vreme je bilo dovoljno kratko kako se ne bi primećivalo da računar opslužuje više korisnika u isto vreme. Iz ovih sistema su se razvile prve LAN mreže.



Slika br.3 – Multiterminalni sistemi [7]

U isto vreme AT&T je razvio prvi komercijalni modem pod nazivom *Dataphone*, koji je konvertovao digitalne kompjuterske podatke u analogni signal kako bi bilo moguće preneti ga preko međugradskih linija. Razvoj modema predstavlja bitnu prekretnicu ka formiranju prvih WAN mreža.



Slika br.4 – Dataphone [11]

Razvojem Multiterminalnih sistema terminali su se preselili iz kompjuterskih centara na stolove korisnika. Iako je kompletna obrada podataka ostala i dalje centralizovana, funkcije kao što su *input* i *output* podataka je postale distribuirane. Krajnji korisnici su doživljavali rad na terminalima na isti način kao što današnji korisnici vide korišćenje računaru u savremenim mrežama. Korisnici su imali pristup deljenim fajlovima i perifernim uređajima.

Interesantno je da su se prve pojavile WAN (*Wide Area Networks*) mreže. One su se sastojale od povezanih računara koji su se nalazili u drugim gradovima, pa čak i državama.

Sve je počelo kao rešenje za problem omogućavanja pristupa terminalom udaljenom računaru preko telefonske linije, korišćenjem modema. Tada se razvijaju veze ne samo između terminala i računara, već i između samih računara. Računari su bili u stanju da razmenjuju podatke automatski, što predstavlja suštinu svake računarske mreže. Prvi servisi koji su bili implementirani u takve mreže bili su razmena podataka, sinhronizacija baza, *e-mail* itd. Mnoge ideje koje su tada razvijene i predstavljene predstavljaju osnovu modernih kompjuterskih mreža:

- Višeslojna arhitektura komunikacionih protokola
- *Packet-switching* tehnologija
- Rutiranje paketa u heterogenim mrežama

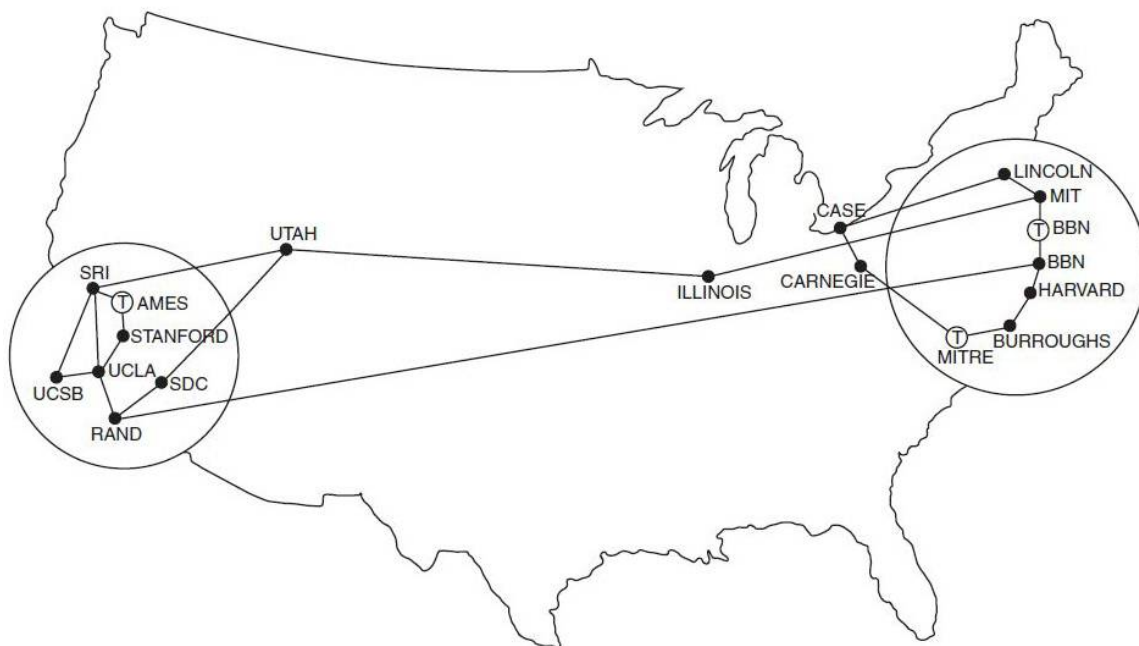
Iako su WAN mreže nasledile mnoge karakteristike starijih mreža, kao što su telefonske mreže, najinovativnija karakteristika je bila je odustajanje od principa prebacivanja kola, koji je korišćen u telefonskim mrežama dugi niz godina. Kola sa konstantom brzinom tokom cele sesije nisu mogla biti korišćena za periode intenzivne razmene podataka koja se dešavaju kod računara, sa pratećim dugim pauzama. Ubrzo se pokazalo da su mreže zasnovane na principu prebacivanja paketa (*Packet-switching*) mnogo efikasnije za intenzivnu razmenu podataka.

Kod *Packet switching* principa podaci se dele u male fragmente, tzv. pakete, gde se adresa domaćina (*host*) nalazi u zaglavlju paketa (*packet header*), a što omogućava svakom paketu da putuje kroz mrežu samostalno.

Pošto je izgradnja visoko kvalitetnih komunikacionih veza bila jako skupa, prve WAN mreže su koristile raspoložive komunikacione veze, prvobitno razvijene u druge svrhe, kao što su telefonske linije. Pošto je transmisija bila veoma spora, mogućnosti ovakvih mreža bile su limitirane. Ovakve veze imale su jednu jako značajnu manu, a to su veliki broj poremećaja koji su se javljali u ovim signalima, pa su i mrežni protokoli koji su tada korišćeni imali komplikovane procedure za kontrolu podataka.

Bitna godina za razvoj modernih računarskih mreža je 1969, kada je Ministarstvo odbrane Sjedinjenih Američkih Država objedinilo računare Ministarstva i istraživačke centre u jednu mrežu. Ova mreža je dobila ime ARPANET i predstavlja početnu tačku u razvitku prve i najrasprostranjenije WAN mreže poznate kao Internet.

Advanced Research Projects Agency (ARPA), koja je bila deo Ministarstva, krenula je sa pronalaženjem kompanija i univerziteta koji bi pomogli u razvijanju komunikacionog sistema koji bi izdržao neprijateljske napade. Primarni cilj je bio omogućavanje vojnim postrojenjima širom zemlje da komuniciraju čak iako je značajan deo komunikacionog sistema uništen. Međutim, već u početku se pokazalo da ova mreža može imati i dodatne benefite.

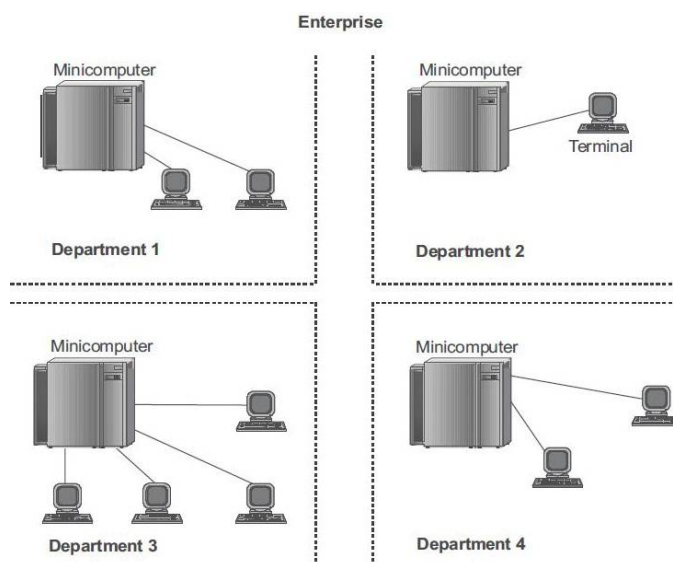


Slika br.5 – Mapa ARPANET-a [13]

ARPANET je spojio kompjutere raznih tipova, sa različitim operativnim sistemima, na kojima su bili implementirani zajednički komunikacioni protokoli. Ovakvi operativni sistemi se smatraju prvim pravim mrežnim operativnim sistemima. Oni su omogućavali samostalnu organizaciju skladištenja podataka. Dozvoljavala je i da procesiranje podataka bude distribuirano između više računara.

Razvoj WAN-a je zavisio od razvoja telefonskih mreža, te je u to vreme predstavljena glasovna transmisija u digitalnom formatu, a što je rezultiralo pojavom digitalnih kanala velikih brzina. Ovi kanali su dozvoljavali prenošenje desetina istovremenih konverzacija. Razvijena je specijalna tehnologija transmisionih mreža, poznatijih kao *backbones*, koje nisu služile krajnjim korisnicima, već predstavljale osnovu na kojoj su se zasnivali visoko-brzinski “*point-to-point*” digitalni kanali. Ovi kanali su povezivali opremu drugih mreža koje su bile na usluzi krajnjim korisnicima. Na početku ovakve mreže su korišćene u organizaciji telefonskih kompanija. Postepeno su ove kompanije iznajmljivale deo tih digitalnih kanala drugim kompanijama koje su ih koristile za organizaciju sopstvenih WAN i telefonskih mreža. Nasuprot početnih brzina od nekoliko stotina kilobita po sekundi (Kbps), današnje brzine se mere gigabitima po sekundi (Gbps), pa čak i terabitima po sekundi (Tbps).

Sledeća dekada donosi LSI (*Large-scale Integration*) kola, kao logičan nastavak razvoja SSI (*Small-scale Integration*) i MSI (*Medium-scale Integration*). SSI je sadržao tek nekoliko tranzistora, ali predstavlja osnovu za razvoj programa putovanja u svemir. NASA-in program *Apollo* je zasnovan na lakim digitalnim kompjuterima za sistem navođenja, te je i to uticalo na brži razvoj ove nove tehnologije, te 70tih godina prošlog veka donosi LSI kola, koja su sadržala desetine hiljada tranzistora po čipu. Najznačajnije karakteristike LSI kola bile su relativno niska cena proizvodnje i napredne mogućnosti. To je dovelo do razvoja mini računara koji su postali ozbiljan takmac *mainframe* računarima. Od tada male kompanije stiču mogućnost posedovanja kompjutera, a što ranije nije bio slučaj. Ovi računari mogli su da obave mnoge poslove koji su olakšavali poslovanje jedne firme. Međutim, računari unutar iste organizacije i dalje su poslovali nezavisno.



Slika br.6 – Primer primene mini računara [7]

Tokom vremena pojavila se potreba za razmenom podataka među korisnicima u organizacionoj jedinici, pa i sa korisnicima na udaljenim lokacijama, te se pojavljuju prve LAN (*Local Area Network*) mreže.

Na samom početku razvoja LAN-a korišćene su nestandardne mrežne tehnologije, a što znači da su korišćene razne aplikacije i vrste računarskih komponenti, kao što su drajveri, mrežni adapteri, kablovi i konektori, kao i razne vrste transmisije podataka. Sve ovo je onemogućavalo efikasno povezivanje računara i razmenu

podataka, jer su povezivanja bila moguća samo između specifičnih tipova i modela računara. Sredinom 80tih godina pojavljuju se prvi standardi. Prvi put se javljaju standardizovane konekcije kao što su *Ethernet*, *Arcnet* i *Token Ring*.

Stvaranje mreža je sada postalo mnogo jednostavnije. Dovoljno je bilo uzeti standardni kabl i mrežni adapter prilagođen npr. *Ethernet*-u, i povezati računar na mrežu. Mnoge inovacije su predstavljene koje su olakšavale razmenu podataka u odnosu na WAN mreže. Npr., korisnici nisu morali da pamte komplikovane identifikatore ili deljene resurse. Kod LAN mreža, sistem je nudio listu dostupnih resursa koji je bio prilagođen korisnicima. Još jedna prednost je bila mogućnost da prilikom uspostave veze ka udaljenom resursu korisnik prilazi na isti način kako bi prišao lokalnom izvoru.

Sve ove inovacije bilo je moguće primeniti kod LAN mreža sa razloga što su za te mreže korišćeni visoko kvalitetni kablovi. Čak i prve generacije mrežnih adaptera dostizali su brzinu do 10 Mbps. Pošto LAN pokriva manje geografske površine cena ovakve mreže bila je podnošljiva. Čak i danas, osnovne razlike između LAN i WAN mreža jesu velika brzina prenosa podataka, manji geografski raspon i najbitnije – nije potrebna zakupljena telekomunikaciona linija. Iz tih razloga ekonomizacija protoka nije bila primarna briga u razvoju LAN protokola, a što je bila značajna stavka kod prvih WAN tehnologija.

Tokom vremena *Ethernet* tehnologija se izdvojila prvenstveno zbog velikih brzina (*Ethernet* – 10 Mbps, *Fast Ethernet* – 100 Mbps i *Gigabit Ethernet* – 1,000 Mbps), ali i malih troškova. Veliki raspon transmisionih brzina omogućavao je racionalizaciju prilikom izgradnje LAN mreže odabirom specifične *Ethernet* tehnologije koja je najbolje odgovarala firmi.

Početkom komercijalne upotrebe Interneta i razvijanjem *World Wide Web* (*WWW*), razlika između LAN i WAN mreža se smanjila. WAN mreže su počele da se koriste za povezivanje izolovanih LAN mreža, a što je rezultiralo interakcijom odgovarajućih tehnologija. Približavanje tehnologija metoda transmisije podataka se zasnivalo na platformi digitalnog prenosa podataka kroz optičke komunikacione linije. Ovakav prenos podataka koristio je skoro sve LAN tehnologije namenjene brzom

razmeni podataka, ali na razdaljinama većim od 100 m. Isti medijum je korišćen kao osnova za savremene *backbone* transmisionne mreže koje omogućavaju digitalne kanale za konekciju WAN opreme, a što je promenilo niz WAN protokola. Time je omogućeno da pojedine usluge, kao što je glasovni saobraćaj, izbiju u prvi plan. Nastale su nove tehnologije – *Frame Relay* i *Asynchronous Transfer Mode (ATM)*. U ovakvim mrežama mogućnost pojave korumpiranih paketa je toliko mala da se takvi paketi jednostavno odbace, a da to ne utiče na brzinu protoka.

Dominacija Internet protokola (IP) je doprinela približavanju mreža. Danas se ovaj protokol koristi u svim LAN i WAN tehnologijama. On omogućava stvaranje tzv. *Internetwork* mreža. To je opšte prihvaćen tehnički izraz koji se odnosi na niz mreža povezanih ruterima i drugim uređajima i preko kojeg *Internetwork* funkcioniše kao jedinstvena mreža.

Sve ovo je omogućilo stvaranje servisa koji su donosili velike količine multimedijalnih informacija u realnom vremenu (glas, slika, video). Najznačajniji primer je *World Wide Web (WWW)*, glavni informacioni servis na Internetu. Široke mogućnosti ovih servisa prevazišle su slične servise koje je omogućavao LAN, pa je ova tehnologija primenjena u razvoju LAN mreža, pa su se pojavile Intranet mreže.

Postoji još jedna vrsta mreža koja je nastala približavanjem LAN i WAN tehnologija pod imenom *Metropolitan Area Networks (MAN)*. Teorijski, ova mreža zauzima poziciju između LAN i WAN mreža. One su namenjene za pružanje servisa u velikim gradovima. Njih karakteriše korišćenje optičkih komunikacionih kanala i *backbone* brzina od preko 155 Mbps. Lepeza usluga je veoma široka, od video konferencija do integrisanih glasovnih i tekstualnih transmisija.

Moderno doba donosi niz univerzalnih mreža pod nazivom *Multiservice networks*. One donose servise i za kompjuterske i za komunikacione mreže i spaja ih u jedinstvenu mrežu. Za sada Internet se može pohvaliti da je jedina prava globalna multi servisna mreža. Multi servisne mreže nove generacije ne mogu biti rezultat razvoja samo jedne tehnologije. Mogu postojati samo kao rezultat procesa približavanja, koji uzima najbolje karakteristike iz svake tehnologije i ujedinjuje ih u nove kombinacije koje donose novi kvalitet.

3. Zašto pravimo mreže[10]

Definicija:. „Računarska mreža je zbirka računara i drugog hardvera, povezanih komunikacijskim kanalima, a koji omogućavaju deljenje resursa i informacija, gde bar jedan proces u jednom uređaju je u stanju da prima\šalje podatke ka\iz bar jednog procesa koji potiče iz udaljenog uređaja, tada se kaže da su ta dva uređaja u mreži.“

Razlozi povezivanja računara u mreže:

1. Zajedničko korišćenje hardvera
2. Zajedničko korišćenje podataka
3. Zajednički rad korisnika na nekim poslovima
4. Razmena podataka među korisnicima
5. Komunikacija među korisnicima
6. Zaštita podataka i njihova redudansa
7. Lakša administracija

3.1 Podela računarskih mreža [6]

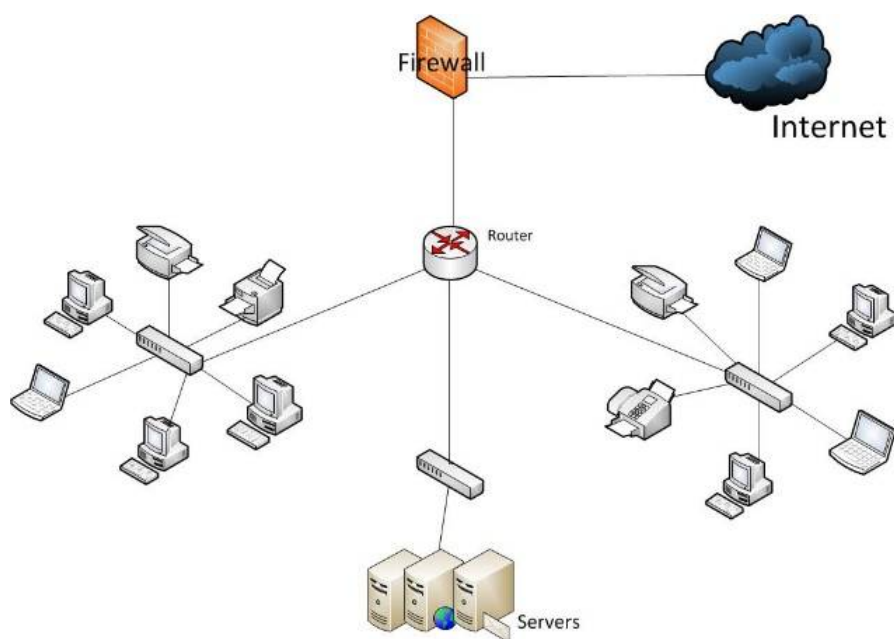
Računarske mreže se mogu podeliti po nekoliko osnova:

3.1.1 Površina koju mreža pokriva

3.1.1.1 Local Area Network (LAN)

Služe za povezivanje mrežnih uređaja na relativno kratkom rastojanju. Može se prostirati kroz jednu ili više zgrada koji su u blizini. Svaki kompjuter ili uređaj u mreži naziva se *node*. Svi povezani uređaji moraju da razumeju *network layer* - treći sloj OSI modela, da bi mogli da komuniciraju preko različitih *subnet*-ova.

Glavne karakteristike LAN-a su velike brzine prenosa podataka, manje geografske površine, nije potrebna telekomunikaciona linija i jeftinije su od *Wide Area Networks* (WAN) i *Metropolitan Aren Networks* (MAN). Najčešće koriste *Ethernet* i *WiFi* (*Wireless*) tehnologije povezivanja.



Slika br.7 – LAN mreža

Podvrste LAN mreža su:

3.1.1.2 Personal Area Networks (PAN)

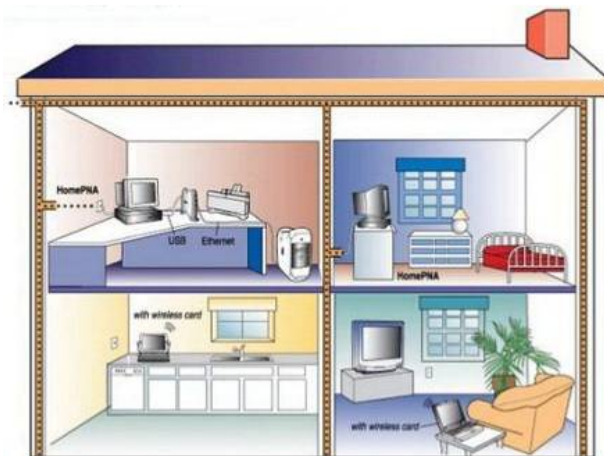
PAN mreže su kompjuterske mreže koje povezuju računare i razne uređaje, a koje su usmerene ka potrebama jedne osobe. Primer ovakve mreže je povezanost računara, štampača, faks mašine, mobilnog telefona, skenera itd. Ovakva vrsta mreže se tipično prostire na površini od 10ak metara. Mogu koristiti mrežno ili bežično povezivanje.



Slika br.8 – PAN mreža

3.1.1.3 House Area Network (HAN)

Ova mreža se koristi stambenim jedinicama i služi za komunikaciju između digitalnih uređaja koji se najčešće nalaze u domovima, obično manji broj računara i eksternih uređaja, kao što su printeri, skeneri, tableti, mobilni telefoni itd.



Slika br.9 – HAN mreža [14]

3.1.1.4 Metropolitan Area Networks (MAN)

MAN mreže su mreže sa velikom brzinom prenosa podataka u gradskim područjima. To su mreže koje pokrivaju površinu jednog grada. Negativna strana ovih mreža može biti cena, problemi sa sigurnošću mreže i podataka, sporija konekcija usled velikog broja računara.

Podvrsta ovih mreža je *Campus Area Networks (CAN)*. Mreže ove vrste predstavljaju povezane LAN mreže na ograničenoj geografskoj površini, a koje služe za potrebe Univerziteta. Povezuju razne zgrade unutar samog Univerziteta.

3.1.1.5 Wide Area Network (WAN)

To su mreže koje pokrivaju velika geografska područja, kao što su gradovi, zemlje, a mogu se prostirati i preko kontinenata. Koriste komunikacione kanale koji kombinuju mnogo tipova kao što su telefonske linije, kablovi i vazdušne talase. WAN najčešće funkcioniše na 3 nivoa OSI modela: *physical layer*, *data link layer* i *network layer*.

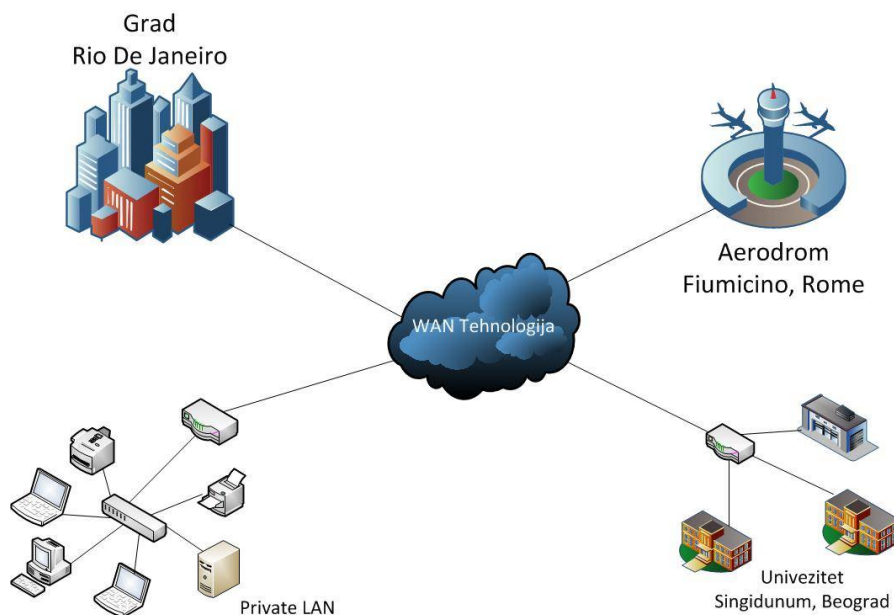
Sastoje se od uređaja i računara koji se nalaze na većim udaljenostima, pa zbog kombinacije više tipova komunikacionih kanala smanjen je propusni opseg ovih mreža

u odnosu na LAN. Internet se može smatrati WAN mrežom. Međutim, razvojem tehnologija ova činjenica se mora uzeti s rezervom.

WAN treba posmatrati kao mrežnu tehnologiju koja se koristi za prenos podataka između više LAN, MAN i drugih mrežnih arhitektura, ali na velikim udaljenostima, kako bi korisnici i računari mogli da komuniciraju između sebe. Ove linije mogu biti veoma skupe. Da bi se umanjili troškovi, prilikom organizacije WAN mreže mogu se koristiti *circuit switching* ili *packet switching* metode.

Circuit switching je način implementacije telekomunikacione mreže u kojoj dva mrežna noda uspostavljaju namenski komunikacioni kanal kroz mrežu pre nego što mogu da komuniciraju. Nod predstavlja tačku u komunikaciji, fizički aktivni elektronski uređaj povezan na mrežu, koji je sposoban da šalje, prima i preusmerava informacije preko komunikacionog kanala.

Packet switching predstavlja digitalni mrežni komunikacioni metod koji grupiše sve podatke koji se prenose, bez obzira na tip ili strukturu u blokove odgovarajuće veličine, koji se nazivaju paketi.



Slika br. 10 – WAN mreža

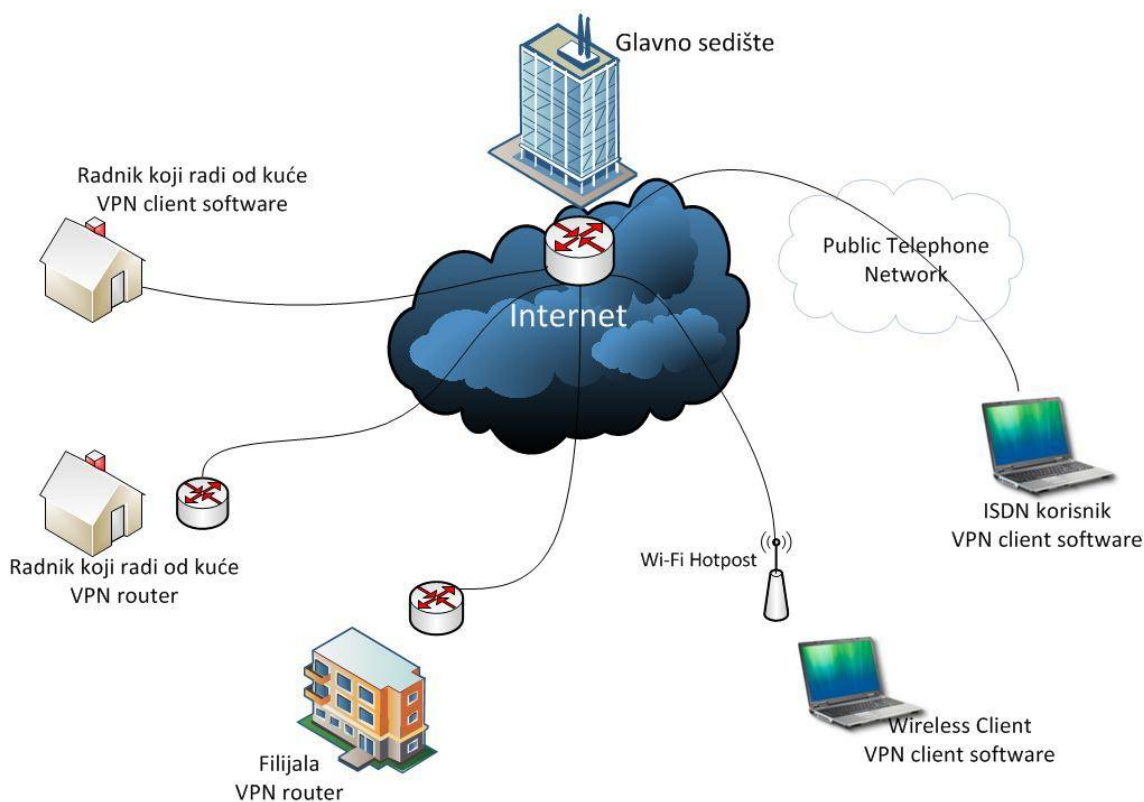
Podvrste WAN mreža su:

3.1.1.5.1 Enterprise Private Network (EPN)

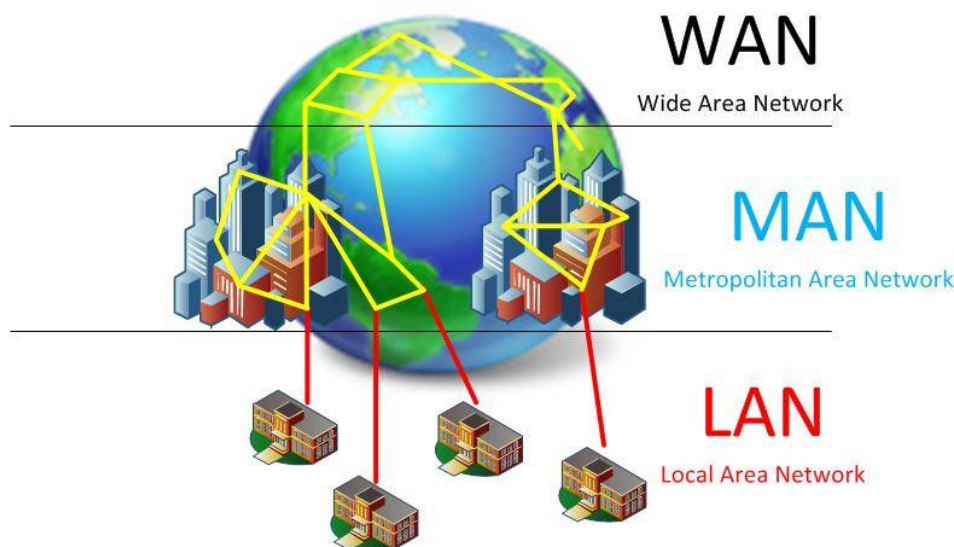
Ove vrste mreža su izgrađene od strane firme za potrebe konekcije između raznih delova kompanije, kao što su glavno sedište firme, filijale, prodavnice itd, u cilju deljenja kompjuterskih resursa.

3.1.1.5.2 Virtual Private Network (VPN)

Virtual Private Networks su kompjuterske mreže u kojima pojedine veze umesto žičnim putem su rešene bežičnom konekcijom. U tom slučaju konekcija se vrši kroz zaštićeni VPN tunel kroz veću mrežu, najčešće Internet. Kako ne bi došlo do upada u ovu vrstu konekcije od strane neovlašćenih lica ova veza mora biti zaštićena npr. autentifikacijom, enkripcijom ili upotrebom *pre-shared key*.



Slika br 11 – VPN mreža



Slika br. 12 – Odnos LAN, MAN i WAN mreža

3.1.1.6 Global Area Networks (GAN)

Mreže ove vrste pokrivaju velike geografske površine, kao što su teritorije više država. Površina koju može da prekriva je neograničena. Ovaj termin se često koristi za Internet.

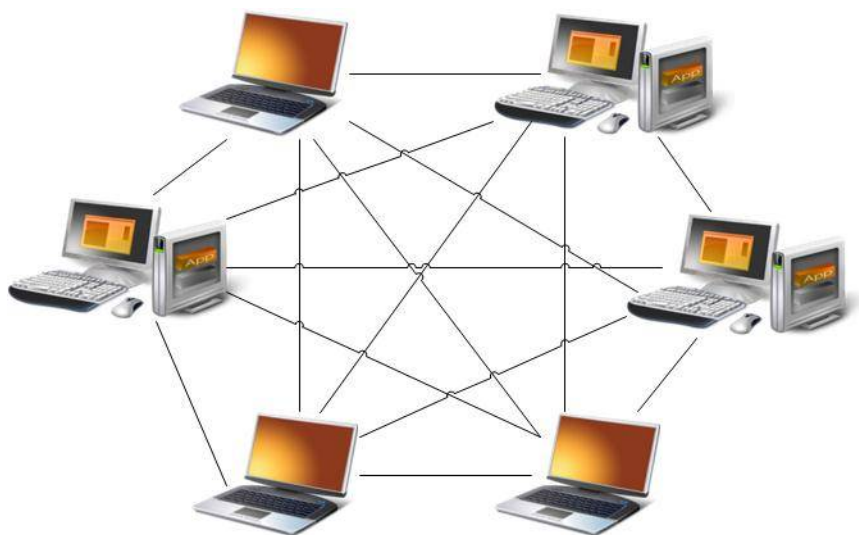
3.1.2 Prema odnosu nodova u mreži

3.1.2.1 Peer – to – Peer (P2P)

Ovakva vrsta mreže nema podele na servere i računare, dakle nema specifičnih rola. Svi računari su ravnopravni, svaki može da funkcioniše i kao klijent i kao server. Npr. na jednom računaru može biti povezan štampač, a koji deli sa celom mrežom. Ili na jednom računaru može biti određen prostor za skladištenje podataka i svim računarima je dozvoljeno da tamo spuštaju svoje podatke. U obe ove situacije imamo hostove koji i troše i koriste mrežne resurse. Glavna korist *peer-to-peer* mreže je lako postavljanje i mala cena jer nema serverskog hardvera i softvera. Ukoliko jedan od nodova ne funkcioniše ispravno, cela mreža neće biti ugrožena ili oštećena. Činjenicom da ne postoji centralizovan server koji ukoliko prestane sa radom prestaje sa radom cela mreža gubi se jedina tačka prestanka rada sistema (*single point of failure*). Pozitivna i negativna strana ovih mreža može biti to što nije potreban sistem administrator za njeno održavanje. Sa jedne strane, ova mreža se lako postavlja i radi, a sa druge strane nastaju problemi oko sigurnosti, jer je svaki korisnik ponaosob zadužen za kontrolu svojih

podataka i resursa. Takođe, korisnik može nenamerno skinuti sa Interneta virusom zaražen fajl, te se dalje taj fajl distribuira kroz mrežu, a sve zbog manjka administratora koji bi odredio koji fajlovi se mogu distribuirati. Negativne strane su i loša skalabilnost. Što ove mreže postaju veće teže je njima upravljati, a sve zbog manjka centralizovane kontrole. Obično se koriste u organizacijama koje imaju mali broj računara, najviše 10 i nazivamo ih *workgroup*. Problem za ovakve mreže predstavlja i *backup* podataka, njihov povraćaj i dostupnost. To čini P2P mreže izuzetno ranjivima.

U današnje vreme ovakve mreže se najviše koriste za razmenu fajlova, najčešće zaštićene sadržine koja nije dozvoljena za slobodnu skidanje i distribuciju. Pošto u ovim mrežama nema administratora, praktično nema kontrole nad deljenim sadržajem, te je svaki korisnik odgovoran pojedinačno. Takve mreže su npr. Gnutella, G2, eDonkey, FastTrack, te popularni Mininova, isoHunt, The Pirate Bay itd.

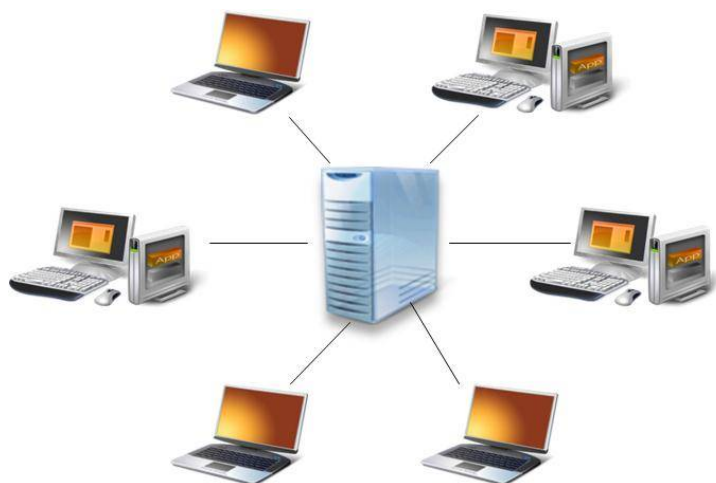


Slika br. 13 – *Peer-to-Peer* mreža

3.1.2.2 Client – Server

U *Client – Server* mreži postoji jasna raspodela uloga na servere i klijente (hostove). Server je taj koji obezbeđuje mrežne resurse, a klijenti su ti koji te resurse koriste. U slučaju P2P mreža svi članovi mreže imaju slične ili iste operativne sisteme, dok kod *client-server* mreže serveri imaju optimizovane operativne sisteme koji su osmišljeni da obezbeđuju mrežne resurse i nisu dizajnirani za zadatke namenjene isključivo klijentima. Prednost ove mreže jeste da je veoma skalabilna, a što znači da je lako proširiti je dodavanjem još klijenata i servera. Ove mreže je i lakše administrirati

zato što je servis centralizovan. *Backup* je takođe lakše raditi, pošto je moguće preusmeriti podatke korisnika na centralizovano mesto, tako da umesto da se *backup* izvršava na svakoj radnoj stanici pojedinačno, radiće se samo na centralizovanoj lokaciji. Takođe je mnogo lakše pronaći problem ukoliko se pojavi u ovakvoj vrsti mreža, pošto se svi servisi odvijaju na serverima. Negativna strana ovih mreža može biti cena licenci za veliki broj radnih stanica, kao i za servere koji su skuplji od operativnih sistema namenjenih za računare. Dodatne troškove predstavljaju i specifična softverska rešenja koja su instalirana na tim serverima kako bi pružali određene servise. Ta specifična softverska rešenja su: *mail*, aplikativni serveri, *file*, printerski serveri, *backup*, *domain controllers*, TMG serveri itd.



Slike br. 14 – *Client – Server* mreža

3.1.3 Prema mrežnoj topologiji

3.1.3.1 Point-to-Point

Ovo je najjednostavnija vrsta mrežne topologije i sastoji se od veze između dve krajnje tačke.

Postoje dve varijante ove topologije:

➤ *Permanent*

To je stalna veza između dve krajnje tačke u mreži.

➤ *Switched*

To je osnovni model klasične telefonske veze i radi na principu prekida konekcije kada ona više nije potrebna.

3.1.3.2 *Bus* (Magistrala)

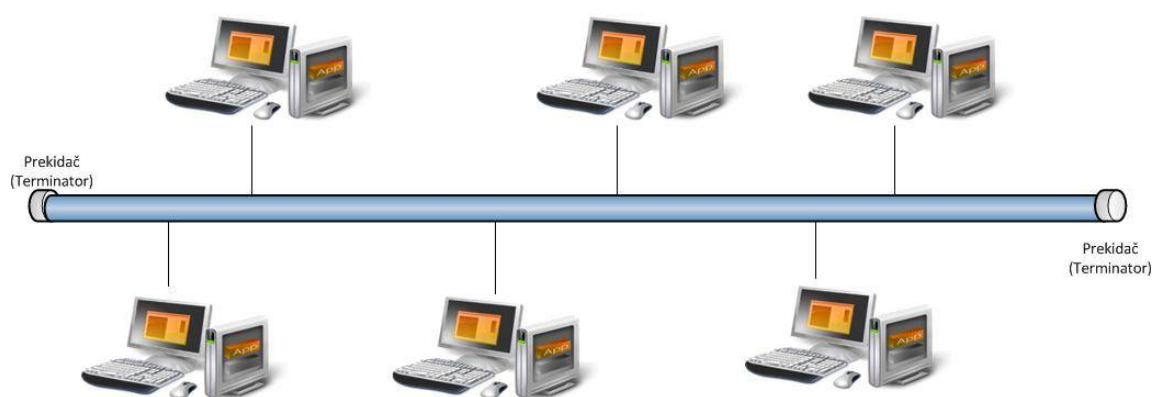
Ova vrsta mrežne topologije je najjednostavnija. Svi čvorovi, i računari i serveri, su povezani jednim kablom koji se naziva *bus* ili *magistrala*, pomoću svojih interfejs konektora. Ova centralna *magistrala* je *backbone* (kičma) mreže i svi uređaji komuniciraju kroz nju.

Signal sa izvora se emituje (*broadcast*) i on putuje do svih računara koji su povezani na *bus* kabl. Iako se signal emituje prema svim radnim stanicama, samo onaj računar čija MAC ili IP adresa odgovara onom u zaglavlju emitovanih paketa može signal i da primi. Ukoliko ne odgovaraju računar odbacuje signal. Uređaj koji se naziva prekidač (*terminator*) se postavlja na krajevima kabla da bi sprečio povraćaj ili skakanje signala. To znači da kada signal dođe do kraja kabla, on kreće (skače) nazad kroz kabl neprekidno sa kraja na kraj kabla i to se zove *ringing*. Da bi se to sprečilo na krajevima kabla se stavljaju prekidači koji upijaju signal i sprečavaju takvo ponašanje.



Slika br. 15 – Primer prekidača [15]

Prednosti ovakve mrežne topologije je što se lako uspostavlja i proširuje ukoliko je potrebno i cena koštanja je veoma mala. Najviše se koristi za male mreže. Negativne strane su ograničenje u dužini kabla i broja nodova koji se mogu povezati, zatim ukoliko kabl ima nekih problema, a što nije redak slučaj, onda cela mreža ima prekid u radu, obavezna je upotreba prekidača, vrlo teško se detektuju problemi, cena održavanja može vremenom porasti, efikasnost ove mreže se smanjuje kako se povećava broj uređaja koji se povezuju, ova topologija nije pogodna za mreže sa velikim saobraćajem i sigurnost u mreži je na niskom nivou jer svi računari primaju signal od izvora.

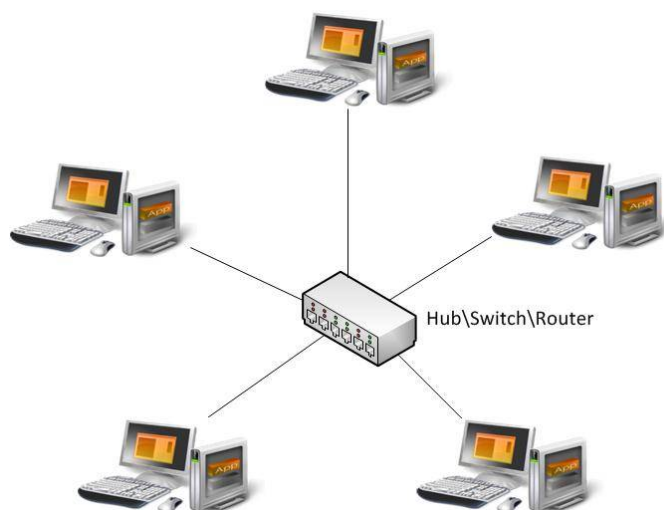


Slika br. 16 – Bus topologija

3.1.3.3 Star

Kada su mrežni uređaji privezani za centralni uređaj koji može biti *hub*, *router* ili *switch*, onda se takva topologija naziva *Star* (zvezdasta) topologija. Računari su povezani na centralni uređaj *point-to-point* konekcijom, tako da su povezani i indirektno između sebe. Svi podaci prolaze kroz centralni uređaj pre nego što stignu na određenu destinaciju. Uređaj se ponaša kao raskrsnica koja povezuje različite nodove, a u isto vreme kontroliše celu mrežu. U zavisnosti za šta se ovaj uređaj koristi može se ponašati i kao ripiter ili pojačivač signala. On takođe komunicira i sa drugim uređajima u drugim mrežama. U ovakvim mrežama koristi se *Unshielded Twisted Pair (UTP)* kabl da bi se povezali računari za centralni uređaj.

Prednosti *Star* topologije je u mnogo boljim performansama koje pruža u odnosu na *Bus* topologiju, ali ipak zavisi od kapaciteta centralnog uređaja, signal se ne prenosi ka svim računarima, već samo ka adresiranom nodu. Lako se konektuju novi računari ili uređaji bez negativnog uticaja na ostatak mreže, centralizovano upravljanje omogućava lakše nadgledanje rada mreže. Otkaz jednog noda u mreži ne utiče na rad ostatka mreže. U isto vreme je veoma lako utvrditi koji računar ili uređaj ima problem. Negativne strane su apsolutna zavisnost od centralnog uređaja, te ukoliko se desi da uređaj prestane sa radom, to znači da ne radi cela mreža. Upotreba dodatnog uređaja (*hub*, *switch* ili *router*) povećava cenu mreže i određuje performanse mreže u odnosu na svoj kapacitet.



Slika br. 17 – Star topologija

3.1.3.4 Ring (Prsten)

Ring topologija predstavlja vrstu mreže gde su svi nodovi povezani jedni za druge tako da veza čini zatvoren krug. Svaki računar je povezan sa svoja dva suseda i komunicira samo sa njima. Podaci putuju u krug po mreži u jednom smeru. Slanje i primanje podataka se odvija uz pomoć *TOKEN*-a.

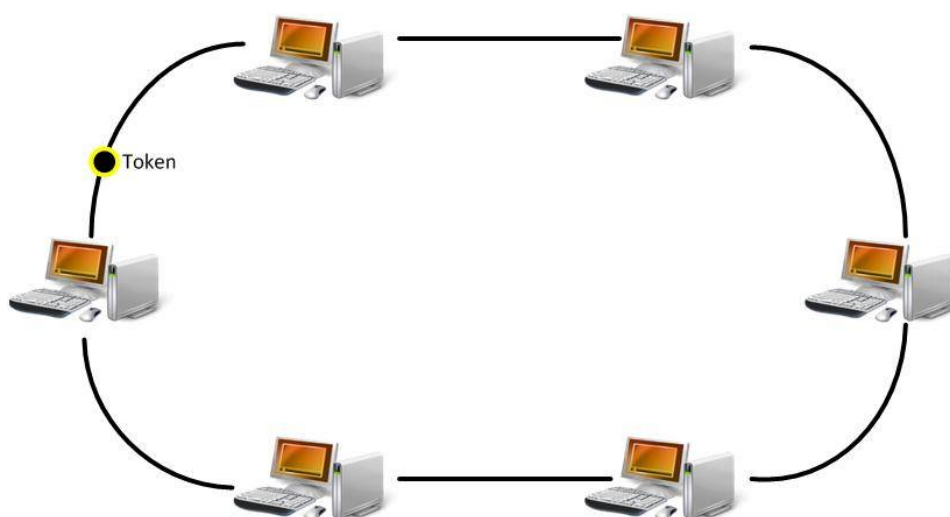
Token Ring tehnologija je protokol koji se nalazi na *DataLink* nivou OSI modela. Koristi specijalni okvir od 3 bajta koji se naziva Token i koji putuje u krug po *Ring* topologiji. Onaj nod koji ga poseduje ima dozvolu da vrši transmisije. Standardizovan je protokolom IEEE 802.5.

Kako Token radi:

- Prazni okviri konstantno cirkulišu kroz Prsten
- Kada računar ima poruku koju želi da pošalje on ubacuje token u prazan okvir, ubacuje poruku, kao i identifikator destinacije. Ubacivanje tokena u okvir znači promenu 0 u 1 u delu koji pripada tokenu
- Okvir proverava sve računare koji mu se nađu na putu. Kada naiđe na računar koji se identifikuje kao primalac, on kopira poruku i vraća vrednost u tokenu na 0

- Okvir se vraća pošiljaocu koji proverava vrednost u tokenu. Ukoliko je vrednost 0 to znači da je poruka primljena i kopirana i tada pošiljalac briše poruku iz okvira.
- Okvir tada nastavlja put kao prazan

Prednosti ovakve topologije je dobra organizacija, svaki nod može poslati poruku kada primi prazan okvir, a što smanjuje mogućnost kolizije. Nema potrebe za serverom koji bi kontrolisao konektivnost među radnim stanicama, te ukoliko se dodaju novi nodovi u mrežu to ne utiče na performanse mreže. Svaki računar ima podjednak pristup resursima. Mane mreže su: svaki paket mora da dođe do svih računara na svom putu ka odredištu, ako jedan računar je u problemu to će se osetiti kroz celu mrežu. Mreža je veoma zavisna o kabl kojima je povezana, a i mrežne karte koje se koriste kod ove topologije su znatno skuplje od *Ethernet* kartica.



Slika br. 18 – Ring topologija

3.1.3.5 Mesh

Mesh mreža jeste konekcija svakog noda u mreži jedan sa drugim. Svaki nod prima i šalje signale od i ka drugim nodovima. Ova vrsta mreže je veoma skupa pošto ima mnogo redundantnih konekcija. Redundantnost je osobina da postoji alternativna veza koja se automatski aktivira u slučaju otkaza primarne veze, te se tako omogućava neprekidan rad mreže.

Ova mreža može biti dizajnirana uz pomoć *flooding* ili *routing* tehnike. Kod *routing* tehnike poruka „skače“ od noda do noda dok ne stigne do željene destinacije. Da bi sve putanje bile dostupne, ova tehnika omogućava stalne veze i rekonfiguraciju oko blokiranih ili veza u prekidu, korišćenjem *self-healing* (samoisceljujuće) tehnike.

Ova vrsta topologije se najčešće koristi kod bežičnih mreža. Najpre je razvijena za potrebe vojske.

Tipovi *Mesh* topologije:

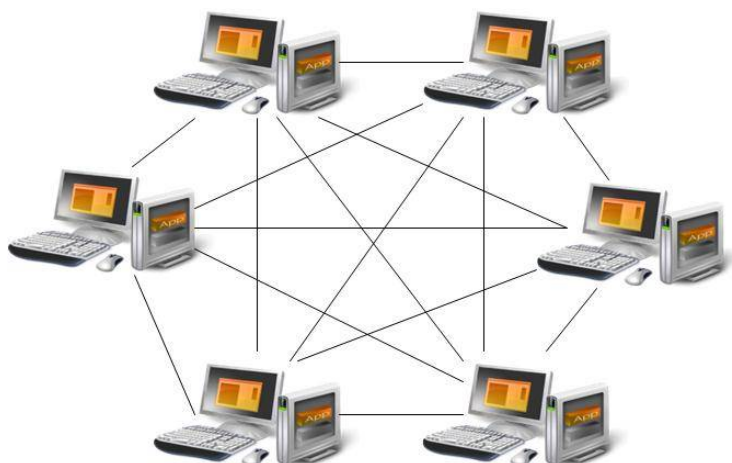
➤ *Full Mesh* topologija

Svaki nod je povezan sa svakim drugim nodom. I pored visoke cene najveća prednost ove mreže je što se saobraćaj redirektuje na druge nodove ako jedan nije dostupan. Ova vrsta topologije se uglavnom koristi za *backbone* mreže.

➤ *Partial Mesh* topologija

Praktičnija verzija *mesh* topologije donosi veze dela mreže kao što je to slučaj kod *full* verzije, dok ostatak je povezan sa jednim ili dva uređaja, tako da su svi nodovi indirektno povezani jedni sa drugima. Ova varijanta je jeftinija, ali i smanjuje redudansu.

Prednosti *Mesh* topologije su prenos podataka sa različitih uređaja istovremeno, pošto topologija može da podnese visok nivo mrežnog saobraćaja, zatim ukoliko jedan od nodova ima problema u radu uvek postoji alternativna putanja, a što ne utiče na transfer podataka, te proširenje mreže ne utiče na stabilnost i rad. Najznačajnija negativna strana je visoka cena koštanja ovakve mreže, pogotovo u odnosu na druge topologije. Tu su i teškoće prilikom postavljanja i održavanja ovakvih mreža.



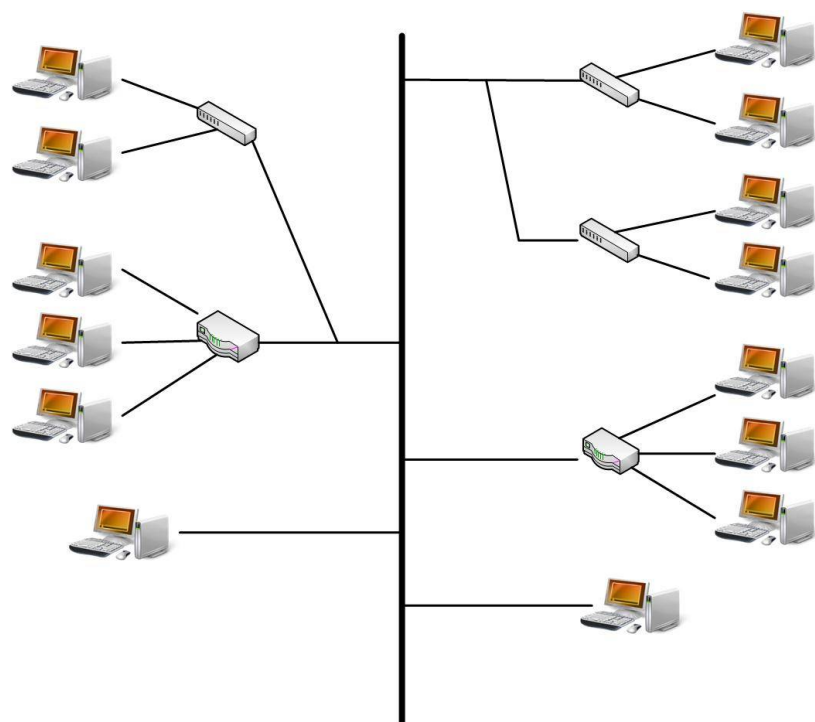
Slika br. 19 – Mesh topologija

3.1.3.6 Tree

Tree topologija objedinjuje karakteristike *Star* i *Bus* topologiju tako što je više mreža zasnovanih na *Star* topologiji povezano između sebe putem Magistrale (*Bus*). Kod nekih autora može se pronaći i naziv *Expanded Star* topologija. Kod ovih topologija najčešće se koristi *Ethernet* protokol.

Pošto je ova topologija kombinacija dve vrste topologije i koristi se u mrežama gde ni jedna ponaosob ne može biti implementirana zbog skalabilnosti to predstavlja njenu najveću prednost u odnosu na druge topologije. Ova mreža se lako proširuje, ali i administracija je lakša jer je mreža podeljena u segmente. Samim tim se lakše pronalaze i otklanjaju problemi. Svaki segment poseduje *Point-to-Point* povezanost ka centralnom uređaju (*hub*, *switch* ili *router*). Još jedna prednost je u tome što ukoliko jedan od segmenata prestane sa radom, ostatak mreže neće biti pogođeni.

Mane su oslanjanje na glavni magistralni kabl, te ako dođe do prekida segmenti neće imati između sebe konekciju. Ukoliko se vremenom poveća broj segmenata mreže teža će biti i administracija.



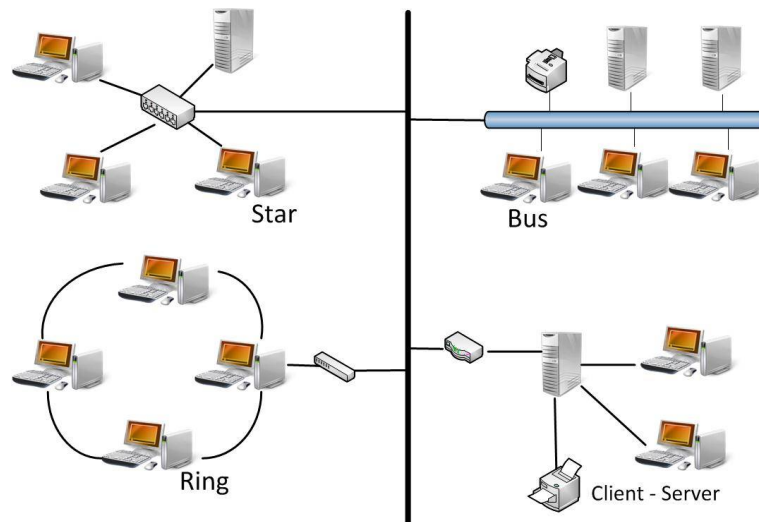
Slika br. 20 – *Tree* topologija

3.1.3.7 *Hybrids*

Hibridna topologija predstavlja mešavinu dve ili više topologija. Kombinacija se određuje na osnovu potreba organizacije za koju se mreža i pravi. Svoju primenu ovaj tip topologije našao je u WAN mrežama. Ovo se odnosi samo na povezivanje dve različite mrežne topologije, nikako iste ili slične. Najviše zastupljene kombinacije su *Star-Ring* i *Star-Bus*.

Prednosti Hibridne topologije: lakše se pronalaze problemi u mreži, te se oni mogu izolovati tako da ne utiču na rad ostatka mreže. Veoma su skalabilne, odnosno dodavanje novih nodova ne utiče negativno na rad mreže. Može se menjati i mogu se dodavati segmenti tokom vremena prema potrebama organizacije kojoj pripada. Može se napraviti tako da maksimalno iskoristi prednosti topologija koje se kombinuju.

Mane su kompleksnost dizajna, zatim uređaji koji se koriste za povezivanje mreža podižu cenu ovoj vrsti topologije, kao i veliki broj raznih drugih uređaja potrebnih za nesmetan rad mreže.



Slika br. 21 – *Hybrid* topologija

3.1.4 Prema načinu povezivanja

3.1.4.1 Žične[16]

Iako u današnje vreme bežične mreže su mnogo napredovale, akcenat je i dalje na žičnom načinu povezivanja, odnosno postojanja fizičkog kabla koji povezuje uređaje u mreži u odnosu na to koji je tip mreže, dakle jedni između drugih ili sa drugim mrežnim uređajima (*hub*, *switch*, *router*). Ovakav način organizovanja računarske mreže iziskuje značajna novčana sredstva, kao i vreme da se kablovi razvuku i uređaji povežu.

Kabl je medijum kroz koji se informacija kreće kroz mrežu. Postoji nekoliko vrsta kablova i njihov izbor zavisi od same mreže i njene organizacije, odnosno u zavisnosti od topologije, protokola koji se koriste i veličine.

Tipovi kablova:

1) *Twisted pair*

Ovo je najčešće korišćen tip žica. Podrazumeva da dve žice se, dva konduktora istog strujnog kola, uvrću kako bi ne bi dolazilo do elektromagnetnih smetnji iz spoljašnjih izvora. Nisu preterano skupi i lako je raditi sa njima. Loše strane su relativna

sporost u prenosu podataka, podložni su smetnjama iz drugih električnih izvora i lako se iskorišćavaju od strane neovlašćenih lica zarad dobijanja pristupa podacima.

Postoje dve varijante:

➤ *Unshielded Twisted Pair (UTP)*

UTP kablovi su najrasprostranjenija varijanta *Twisted pair* kablova. Kvalitet kablova može da varira od varijante za telefonske linije do kablova sa velikim brzinama. Kabl ima četiri para bakarnih žica, koji su obavijeni zaštitom, najčešće folijom. Svaki par je uvrnut različitim brojem uvrtnja po inču (2,54cm), a što pomaže u eliminaciji smetnji nastalih od susednih parova ili drugih električnih uređaja. Što je veće i čvršće uvijanje to je veća brzina transmisije, ali i veća cena po metru. Samim tim, postoje osam kategorija žica.

Kategorija	Brzina	Za šta se koristi
1	1 Mbps	Glas (Telefonska žica)
2	4 Mbps	Retko se koristi - Localtalk
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Retko se koristi – Token Ring
5	100 Mbps (2 para)	100BaseT Ethernet
	1 Gbps (4 para)	Gigabit Ethernet
5e	1 Gbps	Gigabit Ethernet
6	1/10 Gbps	Gigabit Ethernet
7	10 Gbps	ISDN, factory automation
8	40 Gbps	ISDN, factory automation

Tabela br. 1 – Kategorije i brzine WiFi

➤ *Shielded Twisted Pair (STP)*

Ukoliko je potrebno postaviti kabl na mestu gde postoje radio ili električne smetnje tada se postavlja ova vrsta kablova. Zaštita može biti postavljena na pojedinačne parove ili grupu parova. Zaštita pruža elektro-provodnu barijeru koja ublažava elektromagnetne talase izvan zaštite i obezbeđuje provodni put kojim će indukovane struje biti prosleđene i vraćene na izvor putem uzemljenja. Postoje tri vrste zaštićenih kablova:

- *Shielded Twisted Pair (STP)*
- *Screened Twisted Pair (FTP)*
- *Screened Shielded Twisted Pair (S-FTP)*

Ovi kablovi na svojim krajevima imaju konektore kojima se povezuju na interfejs računara. Najčešći konektor koji se koristi je RJ45. To je plastični konektor koji dozvoljava ubacivanje žica samo na određen način. RJ znači *Registered Jack*, a što implicira da je to standard koji je uzet iz telefonske industrije.



Slika br. 22 – Konektor RJ45

Ostale vrste konektora koji se najčešće koriste su:

- RJ11 – Za jednu telefonsku liniju
- RJ14 – Za dve telefonske linije
- RJ12 i RJ25 – Za tri telefonske linije



Slika br. 23 – Izgled UTP i STP kabla [18]

2) *Coaxial Cable* (Koaksijalni kabl)

Koaksijalni kabl ima jedan bakarni provodnik u sredini. Plastični omot obezbeđuje izolaciju između centralnog provodnika i metalne mreže koja predstavlja još jedan sloj zaštite. Ovaj štit služi za blokiranje bilo kakvog spoljnog uticaja. Inače su koaksijalni

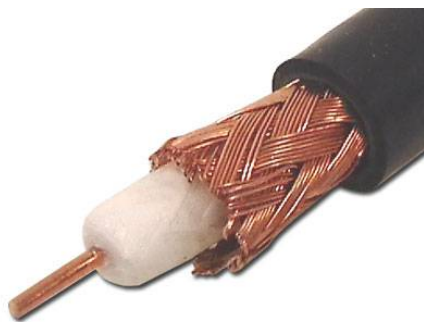
kablovi veoma otporni na smetnje, ali ih je teže postavljati. Podnose i veće dužine između mrežnih uređaja. Postoje dve vrste kablova:

➤ *Thick Coaxial 10Base2*

Ova vrsta kabla poznata je i pod imenom *Thicknet*, i poseduje oznaku 10Base5, a što je specifikacija debelih koaksijalnih kablova koji prenose *Ethernet* signal. oznaka „5“ se odnosi na maksimalnu dužinu od 500m. Debeli koaksijalni kabl ima dodatnu plastičnu zaštitu koja sprečava da vlaga dospe do bakarne žice. Zbog ovog dodatnog sloja zaštite ne savijaju se lako i teže se postavljaju.

➤ *Thin Coaxial 10Base5*

Ova vrsta kabla poznata je i pod imenom *Thinnet*. 10Base2 je specifikacija tankih koaksijalnih kablova koji prenose *Ethernet* signal. Oznaka „2“ se odnosi na maksimalnu dužinu od 200m. U praksi se pokazala kao najveća dužina 185m.



Slika br. 24 – Koaksijalni kabl [19]

Na krajevima koaksijalnih kablova nalaze se konektori pod nazivom *Bayonet-Neill-Concelman (BNC)*. Postoje razne vrste, kao što su *T-Connector*, *Barrel* i *Terminator*. Obično su obloženi visoko-provodnim metalima, srebrom ili zlatom.

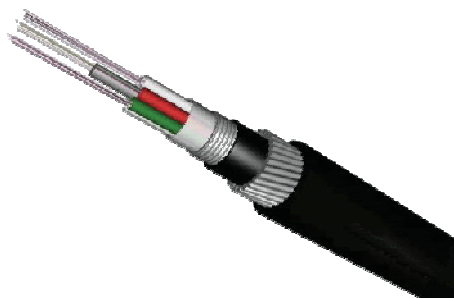


Slika br. 25 – Konektor koaksijalnog kabla [20]

3) *Fiber Optic Cable*

Optički kabl se sastoji od veoma tankog staklenog jezgra, obmotanog sa nekoliko slojeva zaštitnog materijala. On prenosi svetlost, u odnosu na elektronski signal, a čime se eliminiše problem električnih smetnji. Idealni su za okruženja sa velikom količinom elektromagnetnih smetnji. Postali su standard za povezivanje mreža između zgrada, pošto su otporni na vlagu i svetlo. Imaju sposobnost prenosa signala preko mnogo većih razdaljina u odnosu na koaksijalne ili kablove sa uvrnutim paricama. Takođe, prenose podatke mnogo većom brzinom, a što proširuje mogućnosti prilikom komunikacije, jer uključuje servise kao što su video konferencija ili interaktivni servisi. Troškovi nisu veći nego kod bakarnih kablova, ali se teže postavljaju.

Centralno jezgro je napravljeno od stakla ili plastičnih vlakana. Plastični premaz obavija centar, a kevlar ojačava kabl i sprečava lako lomljenje. Spoljna izolacija napravljena je od teflona ili PVC-a.



Slika br. 26 – Optički kabl [21]

Postoje dve osnovne vrste optičkih kablova:

- *Single mode*
- *Multimode*

Optički kablovi prenose signal brzinom svetlosti u staklu (to je sporije od varijante u vakumu) i kreće se brzinom od 180.000 do 200.000km/s, sa kašnjenjem od 5 do 5.5 mikro sekundi po kilometru. Povratno kašnjenje na 1.000km je 11 mikro sekundi.

3.1.4.2 Bežične [22]

Ono što je osnovna razlika između žičnog i bežičnog načina povezivanja jeste nepostojanje žica između izvora interneta i prijemnog tela. Zbog toga ovakav način u poslednjih par decenija postaje veoma popularan i sve više resursa se ulaže u njegov razvoj.

Popularno nazvan *WiFi*, bežični način umrežavanja dozvoljava elektronskim uređajima da razmenjuju podatke između sebe ili da se povezuju i koriste sve prednosti Interneta, a sve pomoću radio talasa.

Ono što je bitno u pogledu bežičnih mreža je razdaljina koju signal može da pokrije. Pa, stoga, imamo nekoliko vrsta bežičnih konekcija, a koje se oslanjaju na IEEE 802.11.

IEEE 802.11 predstavlja set *Media Access Control* (MAC) i fizičkog nivoa (PHY) specifikacija, a koji omogućava bežično povezivanje komunikacionih tela na 2, 4, 3.6, 5 i 60 GHz i na različitim udaljenostima.

WiFi Standard	Frekvencija	Brzina	Pokrivenost	Godina
802.11a	5.0GHz	54 Mbps	Do 120m	1999
802.11b	2.4GHz	11 Mbps	Do 140m	1999
802.11g	2.4GHz	54 Mbps	Do 140m	2003
802.11n	2.4\5GHz	300-900 Mbps	Do 250m	2009
DualBand				

Tabela br. 2 – WiFi standard

Ono što je svakako prednost ovakvog vida povezivanja jeste sloboda u kretanju, a da i dalje postoji pristup raznim resursima, naravno, dok god se uređaj nalazi u dometu odašiljača koji ga opslužuje. Uređaje koji koriste ovakav vid komunikacije nalazimo u svim segmentima života: mobilni telefoni, tableti, lap topovi, štampači, kamere, foto-aparati, konzole za igru, pa čak i automobili.

U bežično povezivanje ne spada samo povezivanje putem interneta ili interne mreže, već i *bluetooth* i *IrDa* način povezivanja.

Za jednu bežičnu mrežu potrebni su sledeći elementi:

01. *Wireless hosts* – ovaj element je isti kao i kod žičnih mreža: to je *end-system* uređaj na kojem se pokreću aplikacije. Ovaj uređaj može, a i ne mora biti mobilan.

02. *Wireless links* – hostovi se konektuju na bazne stanice ili na drugi host sa mogućnošću bežičnog komuniciranja kroz bežični komunikacioni link (*Wireless Communication Link*).

03. *Base stations* – ovo je ključan element svake bežične mrežne infrastrukture. Bazna stanica je odgovorna za primanje i slanje podataka ka i od bežičnih uređaja koji su u konekciji sa tom baznom stanicom. Pod konekcijom se podrazumeva svaki uređaj koji je unutar bežičnog komunikacionog opsega te bazne stanice i koji koristi tu baznu stanicu za konekciju ka većoj mreži.

04. *Network infrastructure* – to su veće mreže sa kojima bežični uređaj želi da komunicira.



Slika br. 27 – Izgled jedne bežične mreže [23]

3.1.5 Prema kapacitetu prenosa podataka

3.1.5.1 Mreže osnovnog opsega

To su mreže koje mogu da prenesu samo jednu poruku u isto vreme. Sporije su od mreža širokopojasnog opsega.

3.1.5.2 Mreže širokopojasnog opsega

To su mreže koje mogu da prenesu više poruka u isto vreme, a pomoću različitih frekvencija za različite poruke.

3.1.6 Prema logičkom i fizičkom rasporedu čvorova

- *Token Ring*
- *Ethernet*

3.1.7 Prema specifičnim funkcijama

3.1.7.1 Storage Area Networks (SAN)

To su specijalne, visoko-propusne mreže koje povezuju razne vrste uređaja za skladištenje podataka. Obično su deo velikih mreža u korporacijama. Tehnologija koja je trenutno najviše zastupljena u povezivanju SAN mreža sa ostatkom mreže, tako da prenos podataka bude brz i bez gubitaka paketa, je *Fibre Channel* tehnologija. Brzina prenosa podataka može dostići do 16Gbps. S obzirom da se za ovu tehnologiju koriste optička vlakna, prenos podataka je višestruko brži. Oslanja se na *FCP (Fibre Channel Protocol)*, transportni protokol, sličan TCP-u, koji prenosi SCSI komande preko FB mreže.



Slika br. 28 – Optički kabl [24]

3.1.7.2 Server farms [38]

Farme servera predstavljaju skup više servera, koje se nalaze na istom mestu, međusobno povezanih najsavremenijim načinom povezivanja, kako bi dobijeni rezultat bio mnogo veće iskorišćenje resurse nego da je to slučaj sa samo jednom mašinom.

Izuzetno su skupe, jer zahtevaju veliku količinu struje, ako i složene sisteme hlađenja. Takođe, zahtevaju i fizičku zaštitu i posebno uređen prostor.

3.1.7.3 Process control networks

3.1.7.4 Value added network

3.1.7.5 SOHO network

3.1.7.6 Wireless Community Network

3.1.7.7 XML Appliance Network

4. Da li računari stvarno razgovaraju ?

Definicija: „Mrežni protokol (*Network Protocol*) definiše pravila i konvencije, a zarad konekcije između uređaja na mreži. Protokoli za kompjuterske mreže u glavnom koriste tehniku nazvanu *Packet Switching*, koja služi za primanje i slanje poruka u formi paketa.“

4.1 Šta u stvari ovo omogućava ?

Kao što je ljudima potreban univerzalan jezik kojim mogu da se sporazumeju ma odakle dolazili, tako je i uređajima oko nas potreban jezik kojim bi se razumeli i bili u mogućnosti da razmenjuju informacije.

Kada su računarske mreže počele sa razvojem, svaki proizvođač je određivao na koji način će njegovi uređaji komunicirati unutar te mreže, te su time korisnici bili prinuđeni da koriste proizvode samo jednog proizvođača. Bilo je jasno da je potrebna određena standardizacija, kako bi velika količina hardverskih proizvoda mogla da komunicira jednobrazno.

Sredinom osme decenije prošlog veka Internacionalna organizacija za standardizaciju (*International Standards Organization - ISO*) razvila je jedan takav

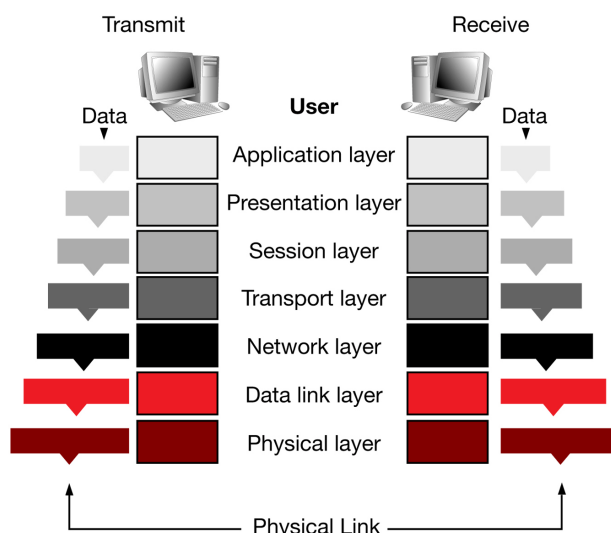
model povezivanja pod imenom *Open System Interconnection Basic Reference Model*, odnosno skraćeno OSI model. Ovaj model opisuje arhitekturu koja služi za povezivanje raznorodnih uređaja. OSI model je postao opšte prihvaćen međunarodni standard, na čijim slojevima funkcionišu određeni protokoli potrebni za komunikaciju između uređaja.

Br.sloja	Ime sloja	Najznačajniji protokoli
1	Fizički sloj (Physical Layer)	Ethernet, USB, Bluetooth, IEEE 802.11
2	Sloj veze (Data Link Layer)	PPP, ATM, Ethernet
3	Mrežni sloj (Network Layer)	IP, ARP, ICMP, IPSec, DHCP
4	Transportni sloj (Transport Layer)	TCP, UDP
5	Sloj sesije (Session Layer)	NetBIOS, PPTP
6	Sloj prezentacije (Presentation Layer)	SSL, TLS
7	Aplikativni sloj (Application Layer)	HTTP, FTP, DNS, SNMP, POP3, SMTP, Telnet

Tabela br. 3 – Primeri protokola po slojevima OSI modela

4.2 OSI model [25] [26] [27] [3] [9] [5]

OSI model je najpoznatiji i najkorišćeniji model koji oslikava mrežnu komunikaciju. Sastoji se iz sedam slojeva. Svaki sloj se bavi različitim aktivnostima na mreže. On definiše i kako će svaki sloj komunicirati sa slojem iznad i ispod sebe. Takođe, svaki sloj pruža i određene mogućnosti koji se odnose na pripremu podataka za slanje, kao i za prijem tih podataka, a u isto vreme svaki sloj je u direktnoj komunikaciji sa odgovarajućim slojem na drugom računaru.



Slika br. 29 – OSI model [28]

4.2.1 Fizički sloj (*Physical layer*)

Potpuno hardverski orijentisan i zadužen je za uspostavljanje i održavanje fizičke veze između uređaja koji komuniciraju. Njegovo zaduženje je i prenos bitova, nula i jedinica, tako da ukoliko je poslat bit sa vrednošću 1, ista ta vrednost stigne na fizički sloj odredišnog uređaja.

4.2.2 Sloj veze (Data Link Layer)

Glavni zadatak ovog sloja jeste da višim slojevima prosledi podatke u kojima nema grešaka koji mogu nastati u prenosu podataka.

4.2.3 Mrežni sloj (*Network Layer*)

Sloj mreže ima zaduženje da brine o adresiranju poruka, kao i prevođenje logičkih adresa u fizičke adrese. Brine i o određivanju putanje od izvornog uređaja do odredišnog, pa će tako izabrati putanju podataka na osnovu prioriteta, stanja mreže itd.

4.2.4 Transportni sloj (*Transport Layer*)

Ovaj sloj se stara da se paketi isporučuju bez greške, redosledom kojim su poslani, bez gubitaka ili dupliranja paketa. Na predajnom uređaju zadatak mu je da prepakuje poruke tako što dugačke deli u više paketa ili više manjih poruka pakuje u jednu celinu. Na prijemnom uređaju raspakuje paketa i ponovo sastavlja originalnu

poruku, odbacuje duplirane pakete, te ako je zahtevano vraća potvrdu da je poruka primljena. TCP i UDP protokoli određuju da li će potvrda o prijemu biti poslata.

4.2.5 Sloj sesije (*Session Layer*)

Sloj zadužen za uspostavu i održavanje sesije između uređaja koji žele da ostvare komunikaciju, a što se naziva sesija. Sesija predstavlja precizno definisan dijalog između dva uređaja. Procesira imena i adrese uređaja i druge elemente neophodne za nesmetanu komunikaciju, u šta spada i bezbednost, koja mora biti odgovarajuća na oba uređaja kako mi mogli da ostvare komunikaciju i razmenu podataka.

4.2.6 Sloj prezentacije (*Presentation Layer*)

Uloga ovog sloja jeste da odredi format koji će se koristiti za razmenu podataka, odnosno da prilagodi prosleđeni format podataka u format koji odgovara aplikativnom sloju prijemnog uređaja. Ovo je jako bitno, jer u komunikaciji mogu učestvovati uređaji različitih proizvođača i namene. Zadužen je i za kompresiju podataka kako bi se smanjio broj bitova koji se prenose.

4.2.7 Aplikativni sloj (*Application Layer*)

Ovaj sloj je najbliži krajnjem korisniku. Korisnik komunicira sa ovim slojem putem softvera kojeg koristi. Zadužen je za identifikaciju partnera u komunikaciji, stanje i prohodnost resursa i za sinhronizaciju celog procesa.

Kod pošiljaoca obrada podataka prvo kreće od Aplikativnog sloja, dok na prijemnom uređaju proces će krenuti od nazad, odnosno, prijem i otpakivanje paketa počinje od najnižeg, Fizičkog sloja.

4.3 Enkapsulacija podataka

Da bi paket uspešno stigao do odredišne destinacije mora da poseduje određene podatke kako bi slojevi OSI modela znali šta sa tim paketom da rade. Svaki sloj doda određen podatak koji je karakterističan za ulogu koju ima, i takav novonastali paket spušta na sloj ispod sebe, kako bi i ovaj dodao određeni podatak

Enkapsulacija predstavlja postupak deljenja podatka u pakete i dodavanje odgovarajućih kontrolnih zaglavlja, kako bi podatak uspešno i u celosti pristigao do odredišnog uređaja.

Na svakom od slojeva podatku se dodaje informacija koja je važna za taj sloj. Te informacije su potrebne, jer podatak na prijemnom uređaju prolazi kroz tzv. dekapulaciju, odnosno obrnuti proces.

Postoje i tri vrste emisija paketa. One šalju paket ka jednom ili više odredišta, u zavisnosti od toga šta je zahtevano od paketa. To su:

01. Unicast

To su paketi koji putuju kroz mrežu i adresirani su na određeni uređaj, tako da će taj uređaj generisati prekid procesa samo ukoliko se adresa paketa slaže sa njegovom sopstvenom adresom. Ovo je dominantan način slanja podataka, jer ne proizvodi nepotreban saobraćaj i tako opterećuje resurse, na koji način bi se smanjila efikasnost cele mreže.

02. Broadcast

Ovaj način emisije paketa znači da postoji jedan pošiljalac, a više primalaca poslatog paketa.

03. Multicast

To je mrežna tehnika koja prenosi jedan isti paket simultano grupi primalaca. Takođe može biti i grupa pošiljaoca tog paketa. U ovom slučaju primaoci primaju niz paketa samo ako to i odluče (npr. TV signal).

4.4 Protokoli [3] [4]

Protokoli su pravila i procedure koje služe za komunikaciju. Kako je prethodno prezentovano u tabeli br.3, u svakom sloju OSI modela postoje određeni protokoli koji

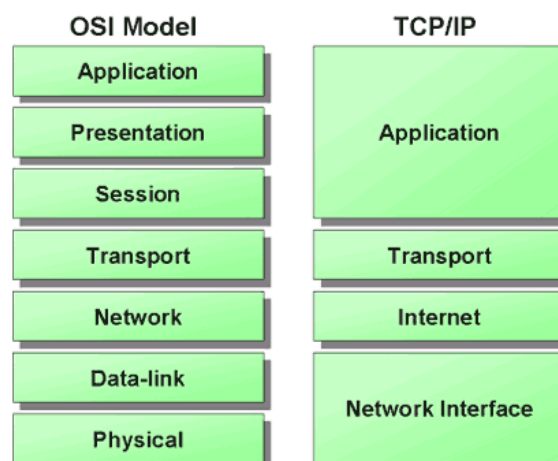
zarad uspešnog prenosa paketa obavlja određenu funkciju. Iako se većina koristi, u ovom segmentu rada biće objašnjeni najznačajniji.

4.4.1 TCP/IP [27] [29] [30] [9]

Skraćenica potekla od naziva *Transmission Control Protocol/Internet Protocol* u sebi objedinjuje dva protokola TCP i IP, dva najvažnija protokola, koja su bila prva dva protokola koji su definisali ovaj standard. Objedinjuje Transportni i Mrežni sloj. Takav zajednički rad se naziva rad u steku, odnosno nizu protokola.

Ovaj industrijski standard je napravljen za velike mreže koje se sastoje od više raznorodnih kompjuterskih sistema, koji su međusobno povezani. Može se naći u svim vidovima komunikacija, bilo da se radi o glasu, multimedijalnom sadržaju ili podacima. Projektovan je tako da određuje putanju kojom će se slati podaci. Njegova najveća prednost jeste što je to otvoren protokol, odnosno da ga ne kontroliše ni jedna kompanija. Takođe, poseduje i neke pomoćne programe za povezivanje različitih operativnih sistema.

On omogućava *end-to-end* konektivnost, precizirajući na koji način podaci trebaju biti formatizovani, adresirani, preneseni, usmereni i primljeni na svojoj destinaciji. Organizovan je logičkom, hijerarhijskom strukturom u četiri sloja, koja se koristi za sortiranje relevantnih protokola. Pošto je ovaj protokol zamišljen da bude nezavistan od načina pristupa mreži, formata paketa i medijuma, on se može koristiti za konektovanje različitih tipova mreža.



Slika br. 30 – Odnos OSI modela i TCP/IP steka [31]

TCP/IP protokol se u potpunosti ne slaže sa OSI modelom. Umesto sedam, poseduje četiri sloja:

01. Sloj mrežnog interfejsa (*Network Interface Layer*)

Ovaj sloj objedinjuje Fizički i Sloj veze OSI modela. On direktno komunicira sa mrežom. Zadužen je za spuštanje i prijem TCP/IP paketa na i sa mreže.

02. Internet sloj (*Internet Layer*)

U zaduženja ovog sloja spadaju adresiranje, pakovanje i rutiranje paketa na mreži. U odnosu na OSI model, Internet sloj je pandan Mrežnom sloju. On pakuje podatke u pakete koji su poznati pod nazivom *IP Datagrams*, u kojima se nalaze adrese izvora i destinacije tih paketa. Adresa može biti logička, odnosno *user friendly* adresa (npr. www.google.com) ili IP adresa (npr. 192.168.1.1). Ova informacija se koristi kako bi paketi precizno putovali preko mreža.

03. Transportni sloj (*Transport Layer*)

Preko ovog sloja vrši se izdavanje dozvola izvorišnom i prijemnom hostu da održe komunikaciju. Definiše nivo servisa i status konekcije koja se koristi kada se transportuju paketi.

04. Aplikativni sloj (*Application Layer*)

Najviši sloj ovog modela. Omogućava aplikacijama pristup servisima drugih slojeva i definiše protokole koje koriste te aplikacije da bi razmenjivale podatke.

4.4.1.1 TCP/IP Stack [32] [29] [30] [9]

Kao što je ranije navedeno, *TCP/IP Stack* se sastoji od dva protokola:

4.4.1.1.1 TCP Protocol

Ovaj protokol predstavlja jedan od osnovnih protokola modernih mreža. Omogućava prenos podataka sa proverom grešaka, odnosno garantuje da će poruka biti

isporučena. Koristi se za konekciju aplikacija (npr. pretraživača) na Internet i služi za prenos fajlova i *mail*-ova širom mreže. U ovom protokolu su kapsulirani neki od najznačajnijih protokola danas, kao što su HTTP, HTTPS, SMTP, POP3, FTP i mnogi drugi, o kojim protokolima će biti kasnije više reči.

To je set pravila koja zajedno sa *IP* protokolom šalje podatke u formi poruka između uređaja preko Interneta. Dok se *IP protokol* stara o isporuci paketa, *TCP* ima obavezu da prati pojedinačne pakete zarad efikasnog prolaska kroz mrežu (Internet). Iako cela poruka, koja se sastoji od paketa koji prolaze kroz mrežu, ima istu adresu na koju pristižu, ti paketi mogu kroz mrežu prolaziti različitim putevima. Na uređaju koji prima tu poruku TCP sklapa te pakete u poruku koja stiže kao jedan fajl. Poznat je kao protokol koji je orijentisan ka održavanju konekcije, što tačnije znači da se konekcija uspostavlja i održava dok god se sve poruke između uređaja ne razmene.

Kako TCP funkcioniše? Konekcija koja se ostvaruje preko ovog protokola, da bi bila uspešna, mora se ostvariti kroz tzv. *handshake* proces pre nego što se započne faza razmene paketa. Po završetku razmene podataka konekcija se prekida i oslobađaju se svi zauzeti resursi.

Handshake koji koristi *TCP* je *three-way handshake*. Pre nego što uređaj ostvari konekciju sa serverom, server mora da ima otvoren port preko koga će osluškivati da li neki uređaj želi da sa njim uspostavi vezu. Ovo se naziva pasivno otvoren port. Kada uređaj inicira konekciju tada port postaje aktivan. *Three-way handshake* se odigrava na sledeći način:

01. *SYN* – Aktivaciju porta inicira klijent (uređaj) koji šalje *SYN* prema serveru i šalje redni broj segmenta sa slučajno izabranim vrednošću A.
02. *SYN-ACK* – Kao odgovor server šalje *SYN-ACK*. Potvrdni broj se formira tako što se na slučajno izabranu vrednost A doda vrednost 1 ($A+1$), a broj sekvence koji server odabira za paket je takođe slučajno izabran broj B.
03. *ACK* – Klijent šalje *ACK* natrag serveru. Broj sekvence je primljena potvrдна vrednost $A+1$, dok potvrdni broj određuje tako što se na dobijeni broj sekvence doda 1 ($B+1$).

Na završetku ove razmene i klijent i server su primili potvrde o konekciji.

Za prekid konekcije koristi se četverostruki *handshake*. Kada jedna strana želi da prekine konekciju ona šalje FIN paket, a druga strana potvrđuje prijem tog paketa slanjem ACK-a.

Broj sekvence omogućava onom koji prima pakete da odbaci duple pakete, te pravilno poređa prispele pakete. Potvrda prijema paketa omogućava ponovno slanje izgubljenih paketa.

Ovaj protokol poseduje *end-to-end* kontrolu toka, kako bi se izbeglo da pošiljalac šalje pakete prebrzo. Kontrola je krucijalna u okruženju gde ima puno različitih uređaja koji komuniciraju preko različitih brzina.

Bitna odlika *TCP-a* jeste i kontrola zagušenja (*Congestion Control*). Preko svojih mehanizama ostvaruje visoke performanse i izbegava kolaps razmene paketa zbog zagušenja. Ovaj mehanizam kontroliše količinu podataka koji ulaze u mrežu i uvek drži količinu podataka na nivou nižem od onog koji bi napravio zagušenje.

Bitan činilac je i *Maximum Segment Size (MSS)*. MSS predstavlja najveću količinu podataka, predstavljenu u bajtovima, koju je TCP spreman da primi u jednom segmentu. Da bi pružio najbolje rezultate MSS treba da bude podešen na tako malo veličinu koja neće praviti IP fragmentaciju, a što bi dovelo do gubitka podataka i preteranu retransmisiju. Kako bi se to izbeglo, obe strane u komunikaciji objavljuju svoj MSS.

4.4.1.1.2 IP Protocol

IP protokol (*Internet Protocol*) je zadužen za adresiranje, a što ima za cilj da svaki uređaj koji se nađe na mreži i želi da komunicira ima jedinstvenu adresu i kao takav je jedinstven u mreži, te se na taj način omogućava da paketi stignu na pravu adresu. Takođe je zadužen i za kontrolne informacije koje omogućavaju paketima da budu rutirani prema nizu poznatih adresa. IP protokol ne sadrži nikakav mehanizam koji bi potvrdio pravilno pristizanje paketa, za to je u TCP/IP steku zadužen TCP protokol.

IP protokol ima tri funkcije:

01. Adresiranje – sastoji se iz dve funkcije: identifikacija hosta i obezbeđenje logičke lokacije servisa.
02. Rutiranje – to je određivanje putanje kojom će se paket kretati
03. Fragmentacija i sastavljanje paketa u originalan oblik.

Adresiranje pomoću IP protokola omogućava da svaki uređaj na Internetu ima svoju jedinstvenu adresu, bez obzira gde se nalaze. To znači da ni jedan uređaj neće imati adresu drugog uređaja. Adresiranje se viši po strogo određenim pravilima. Ta adresa se popularno naziva IP adresa i sastoji se od 32 bita (IPv4) ili osam grupa sa po četiri heksadecimalna broja (IPv6). Preciznije, ova adresa se generalno ne odnosi na uređaj, već na sam mrežni interfejs. Tako da ukoliko uređaj ima dva ili više mrežnih interfejsa on mora imati i dve ili više adresa, odnosno za svaki interfejs zasebno.

4.4.1.1.2.1 IPv4

Ova četvrta verzija IP protokola se koristi za najveći broj rutiranja na Internetu. Kao što je već navedeno, IPv4 protokol koristi 32bitno adresiranje, a što dovodi do limita u adresiranju.

Svaka adresa se sastoji iz dva dela. Prvi deo određuje broj namenjen mreži (*Network ID*), a drugi deo se odnosi na broj hostova koji mogu dobiti tu adresu (*Host ID*).

IP adrese se dele u pet kategorija, odnosno klasa: [33] [34]

01. Klasa A

Koristi se za mreže koje se sastoje od velikog broja uređaja. Prvih 8 bita je rezervisano za mrežu, dok ostala 24 bita predstavljaju *Host ID*. Tako se dobija 126 mreža, sa 16.777.214 hostova.

02. Klasa B

Koriste je mreže srednje veličine. Prva dva niza po 8 bitova je rezervisano za mreže, dok druga dva niza za hostove. To daje broj od 16.384 mreža sa po 65.534 hostova.

03. Klasa C

Ova klasa se najviše koristi, a koriste je male mreže. Prva tri niza bitova su za mreže, zadnji niz za hostove. Ova klasa može pružiti 2.097.152 mreže, sa po 254 hosta po mreži.

04. Klasa D

Ova klasa se ne koristi i kao ostale klase. Služi za IP *multicast* adresiranje.

05. Klasa E

Ova klasa je eksperimentalna i rezervisana za neko buduće korišćenje.

Podela se odnosi na javne adrese.

Postoje i specijalne adrese koje se ne mogu slobodno koristiti.

0.0.0.0/8	Trenutna mreža (može se koristiti samo kao izvorišna adresa)
10.0.0.0/8	Privatne mreže
100.64.0.0/10	Šerovani adresni prostor
127.0.0.0/8	<i>Loopback</i>
169.254.0.0/16	Za komunikaciju unutar mrežnog segmenta
172.16.0.0/12	Privatne mreže
192.0.0.0/24	IETF <i>Protocol Assignments</i>
192.0.2.0/24	TEST-NET-1, dokumentacija I primeri
192.88.99.0/24	IPv6 to IPv4 <i>relay</i>
192.168.0.0/16	Privatne mreže
198.18.0.0/15	Mrežni <i>benchmark</i> testovi
198.51.100.0/24	TEST-NET-2, dokumentacija I primeri
203.0.113.0/24	TEST-NET-3, dokumentacija I primeri
224.0.0.0/4	IP <i>Multicast</i> (Klasa D)

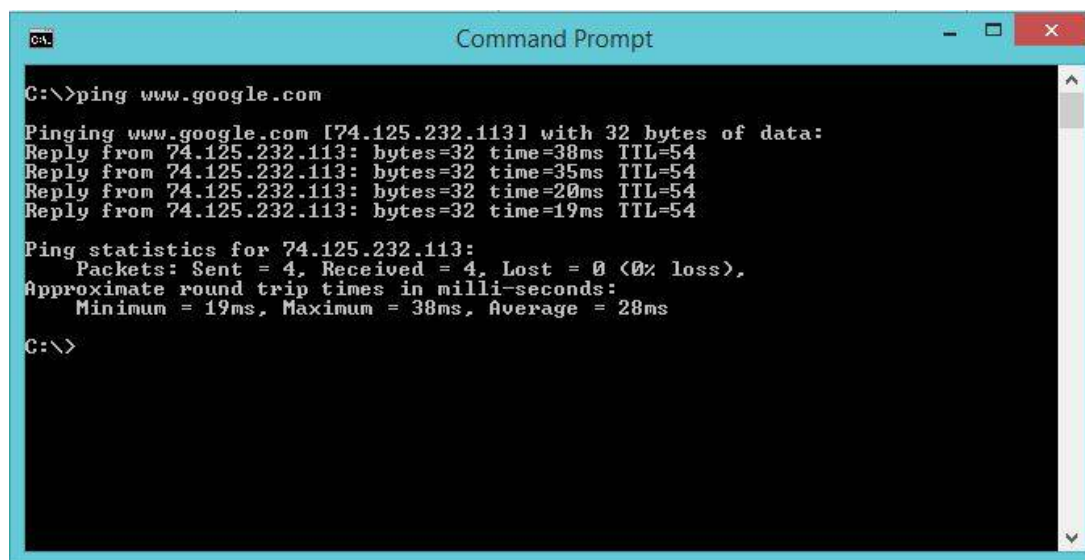
240.0.0.0/4	Rezervisan – Klasa E
255.255.255.255	<i>Broadcast</i>

Tri opsega adresa su rezervisana za privatne mreže. Privatne mreže ne mogu direktno da komuniciraju sa uređajima na javnim mrežama. To se postiže korišćenjem NAT-a (*Network Address Translation*).

4.4.1.1.2.2 IPv6

Za razliku od Ipv4 koji koristi 32bitno adresiranje, ovaj protokol koristi 128 bita. Prikazuje se kao osam grupa po četiri heksadecimalna znaka koje su odvojene dvotačkom.

Ovaj protokol je razvijen kao odgovor na sve veću potrebu za adresiranjem, a nemogućnošću Ipv4 protokola da odgovori zahtevima, iako je primarna opcija i dalje. Treba napomenuti da i adrese na Internetu koje su predstavljene na način kako bi čovek mogao lako da ih zapamti, dakle u tekstualnoj formi, takođe predstavljaju IP adrese.



```

C:\>ping www.google.com

Pinging www.google.com [74.125.232.113] with 32 bytes of data:
Reply from 74.125.232.113: bytes=32 time=38ms TTL=54
Reply from 74.125.232.113: bytes=32 time=35ms TTL=54
Reply from 74.125.232.113: bytes=32 time=20ms TTL=54
Reply from 74.125.232.113: bytes=32 time=19ms TTL=54

Ping statistics for 74.125.232.113:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 38ms, Average = 28ms

C:\>

```

Slika br. 31 – Primer razrešenja naziva u adresu

Iako se kao glavni benefit ove verzije IP protokola spominje ogroman raspon mogućih adresa, postoje još važnih promena:

- Nije potrebno više korišćenje NAT-a (*Network Address Translation*)
- Nema više kolizije sa privatnim adresama
- Bolje *multicast* rutiranje
- Jednostavniji format hedera
- Jednostavnije i efikasnije rutiranje
- Poboljšan *QoS (Quality of service)*, poznat pod nazivom „*flow labeling*“
- *Built-in* podrška za autentifikaciju i privatnost
- Fleksibilnije opcije
- Lakša administracija (*DHCP* servis postaje suvišan)

4.4.1.1.2.3 Razlike između IPv4 i IPv6

01. Adresiranje

Razlike u broju bitova koje koriste ove dve verzije su objašnjene u prethodnom tekstu.

02. Konfigurisanje adresa

Verzija 6 podržava *Stateless Address Auto Configuration (SLAAC)*. U ovom režimu nodovi mogu automatski da odrede svoju mrežnu konfiguraciju tako što će dobiti lokalnu IP adresu i na taj način odrediti uređaje koji se nalaze u neposrednoj blizini, mogu da odrede lokalni ruter, pa čak i da generišu globalnu rutabilnu adresu koristeći se prefiksom koji obezbeđuje sam ruter kroz *ICMP (Internet Control Message Protocol)* poruke. Sve ovo se odigrava bez bilo kakve interakcije sa korisnikom. Još jedna pogodnost je mogućnost verzije 6 da renumerise ove globalne adrese kroz ruter, umesto da hostove konfiguriše pojedinačno.

03. ICMP

Predstavlja ključnu komponentu za verziju 6 IP protokola. Unapređena je nizom novih ICMP poruka. *ARP (Address Resolution Protocol)* je zamenjen sa *Neighbor Discovery (ICMP tipovi 135 i 136)* i *Router Discovery (ICMP 133 i 134)*.

Fragmentacija se izvršava samo na krajnjim odredištima, a ne na usputnim ruterima kao što je bio slučaj do sada. Da paket treba fragmentirati pošiljalac se obaveštava porukom tipa 2 „*Packet Too Big*“, a pošto je originalna poruka odbačena.

04. Paketna struktura

Promenjena je struktura hedera, pa tako on sadrži samo sledeća polja:

- *Version*
 - *Traffic Class*
 - *Flow Label* – omogućava ruterima efikasniju identifikaciju paketa koji pripadaju istom toku ili konekciji.
 - *Payload Length*
 - *Next Header* - omogućava paketima i druge funkcionalnosti, kao što su fragmentacija, *IPSec* i tradicionalne transportne protokole, TCP i UDP.
 - *Hop Limit*
 - *Source Address*
 - *Destination Address*
- Sada ruteri mogu da rade efikasnije.

05. Multicast

Ova opcija omogućava slanje paketa, a da u isto vreme uređaj komunicira sa drugim uređajima na mreži. Iako je podržan i u verziji 4, u verziji 6 ima značajniju ulogu, jer ne postoji više *broadcast* adresa, pa se *multicast* koristi na razne načine u komunikaciji specifičnih grupa uređaja, kao što su *All* ili *All Routers*. U kombinaciji sa *ICMP* porukama ovim grupama omogućava *Neighbor Discovery* da funkcioniše efikasnije.

4.4.2 UDP Protocol

UDP (*User Datagram Protocol*) predstavlja vrlo jednostavan protokol, sa minimalnim servisima. Zato što nema konekcije između uređaja, ne postoji *handshake* kao kod TCP protokola. Najznačajniju karakteristiku predstavlja prenos podataka koji

nije pouzdan, a što znači da ne postoji potvrda prenosa, niti postoji garancija da će poruka uopšte stići. Takođe, moguće je da poruka kada pristigne ne bude u odgovarajućem rasporedu. UDP nema ni mehanizam za zaštitu od zagušenja, tako da pošiljalac može slati pakete intenzitetom koji mu odgovara.

4.4.3 DHCP (Dynamic Host configuration Protocol)

Ovaj jako važan protokol daje mogućnost automatske dodele IP adresa uređajima u mreži. Kao što je već navedeno, svakom uređaju je potrebna jedna takva adresa kako bi mogla da komunicira sa drugim uređajima. DHCP omogućava nadgledanje i distribuciju adresa sa jednog mesta, a najznačajnije je to što se raspodela vrši automatski, a po prethodno određenim podešavanjima. Koristi koncept „najma“ adrese na određeni vremenski period. Ovaj proces se odvija na sledeći način:

01. *Request* – klijent koji zahteva adresu šalje *broadcast* zajedno sa svojom MAC adresom. To je DHCP poruka koja ima adresu 0.0.0.0 i *subnet* masku 255.255.255.255. Status klijenta u ovoj fazi je *initialization*.

02. *Offer* – DHCP šalje poruku „*DHCP Offer*“. U poruci se nalazi adresa servera koji nudi adresu. Može ih biti i više. Te adrese su u tom momentu rezervisane, odnosno neće biti dodeljene drugom uređaju dokle god klijent ih ne odbije. Klijent je u ovoj fazi u statusu *selecting*.

03. *Selection* (ili *Acceptance*) – klijent prihvata ponudu i *broadcast*-uje svoj izbor koristeći *DHCP request* poruku koja sadrži adresu servera čija ponuda je prihvaćena. Status klijenta je *requesting*.

04. *Acknowledgement* – server potvrđuje izbor slanjem *DHCP acknowledge* poruke, kojom potvrđuje da je klijent dobio određenu adresu. Ostali DHCP serveri koji su ponudili adrese i držali ih rezervisane, sada te adrese oslobađaju, te postaju ponovo dostupne. Status klijenta u ovoj fazi je *binding*.

Kada klijent dobije adresu ona je po osnovnoj vrednosti izdata na 8 dana. Kada istekne 50% vremena klijent će pokušati da obnovi adresu slanjem *DHCPREQUEST* poruke. Ukoliko se server ne javi zadržaće postojeću adresu. Po isteku novih 50% vremena, ali ovog puta od ostatka, klijent će ponovo pokušati da kontaktira server od kojeg je dobio adresu. Kada istekne vreme klijent ponovo pokušava da dobije adresu. Ukoliko u njegovoj blizini nema servera koji bi mogli da mu izdaju novu adresu, klijent automatski dobija tzv. *APIPA* adresu, a što je skraćenica od *Automatic Private IP Addressing*. Obuhvata adrese od 169.254.0.1 do 169.254.0.254, sa *subnetmask* 255.255.0.0. APIPA servis i dalje nastavlja da proverava da li ima neki DHCP server u blizini koji bi mogao uređaju izdati adresu, i tako mu omogućiti konekciju sa ostalim uređajima u mreži. Ukoliko detektuje server, APIPA prestaje sa funkcijom i uređaj ponovo dobija automatski izdatu adresu.

4.4.4 DNS (Domain Name System)

Najčešće se koristi za prevođenje između IP adresa i domenskih imena, kao i za kontrolu isporuke *mail*-ova preko Interneta. Mnogo servisa se oslanja na pravilan rad DNS-a, tako da ukoliko ovaj servis prestane sa radom uređaji ili *web* stranice ne mogu biti locirane, kao i isporuka *mail*-ova prestaje.

To je hijerarhijski uređen sistem koji opslužuje uređaje, servise ili bilo koji drugi resurs konektovan na Internet ili u privatnoj mreži. Pridružuje razne informacije domenskom imenu koji je dodeljen uređaju. Najznačajnije, prevodi lako pamtljiva domenska imena u numeričke IP adrese koje su potrebne za lociranje uređaja ili servisa. Iz ovog razloga DNS predstavlja jedan od najvažnijih protokola.

Server na kome se nalazi ovaj servis sadrži DNS rekorde kao što su rekordi adresa (A ili AAAA), *name server* rekordi (NS), *mail exchanger* rekordi (MX) kao jedni od najznačajnijih.

4.4.5 HTTP (Hypertext Transfer Protocol)

HTTP je protokol Aplikativnog sloja, koji poseduje brzinu neophodnu za distributivne *hypermedia* informacione sisteme. Koristi se od 1990 godine i osnova je za

komunikaciju na WWW (*World Wide Web*). To je protokol za razmenu i transfer hiperteksta korišćenjem logičkih linkova, tzv. hiperlinkova.

HTTP protokol radi po sistemu zahtev\odgovor u odnosu klijent – server. Klijent šalje HTTP *request* poruku serveru, a server vraća *response* poruku klijentu. Odgovor sadrži finalnu informaciju o statusu, a takođe može sadržati i neki zahtev. Klijent može biti bilo koja aplikacija ili servis koji prima ili prikazuje *web* sadržaj.

Dizajniran je tako da dozvoljava razmenu elemenata između mreža kako bi omogućio ili poboljšao komunikaciju između klijenata i servera. Elementi su poznati pod imenom *web cache*. Najviše koristi od tih elemenata imaju Internet sajtovi sa velikim saobraćajem, pa koriste *web cache* servere koji isporučuju sadržaj kako bi poboljšali vreme odziva.

Koristi se u kombinaciji sa TCP protokolom, kako bi se osigurao siguran prenos podataka, ali i sa UDP protokolom u manjoj količini.

Resursi su identifikovani i locirani na mreži kroz *Uniform Resource Identifiers (URI)*, preciznije, preko *Uniform Resource Locators (URL)*, korišćenjem HTTP ili HTTPS koji pripadaju URI šemi.

4.4.6 FTP (File Transfer Protocol)

FTP protokol je standardni mrežni protokol koji se koristi za transfer fajlova od jednog hosta do drugog, a preko mreža zasnovanih na TCP-u. Oslanja se na klijent – server arhitekturu i koristi odvojene kontrole i data konekcije između klijenata i severa. Konekcija od strane klijenata može biti u vidu autentifikacije pomoću korisničkog imena i lozinke, ali mogu to učiniti i anonimno ako je server za to konfigurisan. Za enkripciju se oslanja na SSL/TLS, poznatiji pod imenom FTPS.

Može da radi u aktivnom ili pasivnom modu, koji određuju kako je konekcija uspostavljena. U aktivnom modu, klijent uspostavlja TCP konekciju ka serveru i šalje serveru IP adresu klijenta i odgovarajući broj porta, i čeka da server uspostavi data konekciju preko TCP-a na tu klijentsku IP adresu i broj porta. U situacijama kada je klijent iza nekog *firewall-a* i nije u mogućnosti da prihvati dolazeću TCP konekciju,

onda se može koristiti pasivni mod. U ovom modu klijent koristi kontrolisanu konekciju da bi poslao PASV komandu serveru, a onda primi IP adresu servera, kao i broj porta, koje podatke klijent onda koristi da otvori data konekciju na proizvoljnom portu prema IP adresi i portu servera koje je primio. Oba metoda su prilagođena i za IPv6.

4.4.7 SMTP (Simple Mail Transfer Protocol)

SMTP je protokol dizajniran za efikasan transfer elektronske pošte. Koristi FTP *file transfer* servis. Njegova uloga je da prenosi *mail* poruke među sistemima i osigurava notifikacije koje se odnose na dolazeću poštu.

Protokol je nezavistan i zahteva samo pouzdan *data stream* kanal. Važna odlika SMTP-a je mogućnost da transportuje *mail*-ove preko mreža, a što se obično naziva „*SMTP Mail Relaying*“. Na ovaj način, *mail* može proći kroz niz javnih i zatvorenih mreža, prolazeći kroz niz rutera i ostalih uređaja za usmerenje saobraćaja na svom putu do konačnoj odredišta.

4.4.7.1 Proces

01. *E-mail* se šalje preko *mail* klijenta (*MUA*, *Mail User Agent*) *mail* serveru (*MSA*, *Mail Submission Agent*) koristeći SMTP na TCP portu 587 ili 25, koji još uvek koriste veliki broj *mailbox* provajdera. Odatle MSA isporučuje *mail* transfer agentu (*MTA*, *Mail Transfer Agent*). Najčešće su ova dva agenta samo različite instance istog softvera, koje se pokreću sa različitim opcijama na istoj mašini.

02. Zadatak MTA je i da pronade ciljani host. Za to koristi DNS (*Domain Name System*), kako bi pronašao *Mail Exchanger Record* (*MX Record*) za domen primaoca poruke, a što čini preko dela adrese posle znaka @. Rekord koji dobije nazad sadrži ime ciljanog hosta. Zatim se MTA konektuje na Exchange server kao SMTP klijent.

03. Čim MX ciljanog hosta primi poruku, prosleđuje je *Mail Delivery* agentu (*MDA*) za lokalnu isporuku. Ovaj agent čuva poruku u odgovarajućem *mailbox* formatu.

Prijem *mail*-a može biti na jednom ili više uređaja odjednom. Kada je isporučen lokalnom mail serveru, *mail* čeka da ga preuzme autentifikovan *mail* klijent (*MUA*). *Mail* preuzima aplikacija na uređaju krajnjeg korisnika, koja se naziva *mail* klijent, a za to koristi *IMAP* (*Internet Message Access Protocol*), protokol koji u isto vreme obrađuje pristup *mail*-u i smeštanje *mail*-a, ili *POP* (*Post Office Protocol*), koji koristi tradicionalni *mailbox* file format ili sisteme kao što su Microsoft Exchange ili Lotus Notes\Domino. *Web mail* klijenti mogu koristiti bilo koji metod.

5. **Zaštita mreže [1]**

Svakodnevno do nas dolaze informacije kako je neka velika mreža kompromitovana od strane hakera. Od napada nije zaštićeno bilo čak ni Ministarstvo odbrane SAD-a, Yahoo, Amazon.com, eBay, razne firme, *web* stranice i mnogi drugi, a za koje nikada nećemo saznati, jer kriju svoje propuste u zaštiti.

Ali pogrešno je misliti da napadi dolaze samo spolja. Svakodnevno mreže se bore sa pojedincima, zaposlenim u tim firmama, koji žele da se domognu nekih poverljivih dokumenata ili nateraju svoje firme da im ponude bolje uslove. Takođe tu su i nenamerne pretnje koje donose zaposleni na svojim eksternim uređajima od svojih kuća na kojima se vrlo često nalaze fajlovi zaraženi najraznovrsnijim virusima.

Da bi se zaštitili od raznovrsnih napada kako spolja, tako i iz unutra, ljudi koji rade u velikim mrežama moraju se baviti zaštitom na svakodnevnoj osnovi, a sve zarad zaštite podataka i omogućavanja nesmetanog rada.

Svake godine milijarde dolara se troše na mrežnu zaštitu. Najvažnije za svaku mrežu jeste da odredi šta želi od zaštite koju namerava da implementira i utvrdi da li uloženi novac odgovara tim ciljevima.

Zaštita mreža je bitna iz sledećih razloga:

01. Da bi se zaštitila svojina kompanije

To je jedna od najznačajnijih stavki što se tiče zaštite mreže. Pod svojinom se podrazumeva informacije koje kompanija poseduje. One su od vitalnog značaja za rad svake firme. Pod zaštitom se podrazumeva da su te informacije nekompromitovane i dostupne 24\7.

02. Da bi se obezbedio nesmetan rad

Za profitabilne firme od izuzetne je važnosti da svoje usluge mogu pružati 24 sata, 7 dana u nedelji, 365 dana u godini. Firme koje se oslanjaju na računare i druge mrežne uređaje u svom poslovanju moraju razviti polise i procedure zaštite koje su neophodne da bi se takav tempo poslovanja postigao. Uz to, mnoge firme moraju da poštuju državne regulative. Ukoliko to ne učine na pravi način rizikuju da budu finansijski kažnjene, što donosi gubitak u poslovanju, a u mnogim slučajevima i da im na određeno vreme bude oduzeta mogućnost poslovanja, što po firmu može imati katastrofalne posledice.

03. Prednost nad konkurentima

Razvoj i održavanje sigurnosnog sistema može doneti firmi prednost nad konkurentima samom činjenicom da su informacije zaštićene i uvek dostupne. Zaštita je posebno bitna u sferi *e-commerce* i mnogobrojnih finansijskih servisa koji se danas nude preko Interneta. Upravo ta zaštita može doneti prevagu kod korisnika kada odlučuju kojoj banci će se privoleti i koristite njene *online* usluge.

Da bi komunikacija bila sigurna, ona mora posedovati sledeća svojstva:

01. Poverljivost

Poenta je da samo primalac kojem je poruka namenjena može da po prijemu poruku i razume. Da bi se to postiglo potrebna je upotreba enkripcije tako da ukoliko dođe do presretanja poruke ona ne bi mogla biti pročitana.

02. Integritet poruke

Pošiljalac poruke želi da osigura da sadržaj njegove poruke nije menjan, bilo slučajno ili usled loših namera, u toku transporta. Integritet poruke se postiže raznim tehnikama u pouzdanog prenosa poruka, kao i upotrebom raznih protokola.

03. *End-Point* autentifikacija

Cilj je da i pošiljalac i primalac poruke mogu da potvrde identitet one druge strane koja je uključena u komunikaciju, odnosno da potvrdi da je druga strana zaista ona kako se predstavlja.

04. Operativna sigurnost

S obzirom da skoro svaka organizacija poseduje mrežu koja je u komunikaciji sa javnim Internetom, te mreže se potencijalno mogu kompromitovati. Zato između unutrašnje mreže i Interneta, odnosno javne mreže, postoji tzv. *Firewall*, koji ima zadatak da kontroliše protok paketa koji izlaze i ulaze u mrežu.

Ono što treba uzeti u obzir je činjenica da je mrežna zaštita izuzetno skup projekat. On zahteva izuzetno mnogo novca, kako bi uposlilo i obučilo ljudstvo, kupio odgovarajući hardver i softver, a ponajpre nadomestilo degradiranje mreže i samih performansi koji nastaju upotrebom *firewall*-a, raznih filtera, polisa i *Intrusion Detection Systems (IDS)*. Iz svega ovoga proizilazi da cena ovakve postavke mreže nimalo nije mala, ali da je svakako jeftinije od situacije kada su podaci, odnosno sama firma kompromitovani.

Najzanimljivija stvar oko zaštite računarskih mreža jeste činjenica da najveći broj incidenata širom sveta vezanih za kompjuterski kriminal nikada nisu prijavljeni, jer bi to nanelo nesagledivu štetu.

Osnovu mrežne zaštite predstavljaju prevencija, otkrivanje problema i odgovor na taj problem.

01. Prevencija

Da bi se obezbedio određeni nivo zaštite neophodno je da se implementiraju određene mere, kako bi se sprečila eksploatacija osetljivih mesta u mreži. Ovaj korak treba da ima najznačajnije mesto prilikom planiranja šeme zaštite, jer je mnogo značajnije sprečiti eventualne napade, umesto da se isti detektuje i tek onda reaguje

kako bi se otklonile posledice. Treba napomenuti da je nemoguće organizovati tako zaštitu pa da mreža bude u potpunosti zaštićena, ali je treba organizovati tako kvalitetno da mreža ne predstavlja laku metu.

02. Otkrivanje problema

Jednom kada se postavi sistem neophodno je stalno raditi na njegovom usavršavanju, a naročito su bitne procedure koje će redovno testirati sistem i detektovati potencijalni problem ili probijanje zaštite mreže. Naravno, ukoliko se ranije otkrije problem, lakše će biti sanirati njegove posledice.

03. Odgovor na nastali problem

Takođe, neophodne su i procedure koje će odrediti korake koje je neophodno preduzeti ukoliko dođe do probijanja zaštite mreže. Najbitnije je da se znaju odgovornosti svakog člana time za svaki potez koje se preduzme u tom periodu.

Ono što predstavlja zabludu jeste mišljenje da je zaštita mreže tehnički problem. To je poslovni problem, kao i problem ljudstva. Izuzetno je komplikovan proces razvijanja i primene plana koji odgovara organizaciji da ne remeti u mnogome njen rad, ali i činjenica da je najteže naterati ljude da taj plan i prate. Treba napomenuti da zaštita mreže nikada nije išla na ruku sa komforom, pa stoga korisnici mreže predstavljaju najslabiju kariku zaštite mreže.

Da bi se napravio precizan i dobar plan zaštite potrebno je uraditi procenu rizika. Da bi se ova procena izvela, potrebno je znati i razumeti moguće pretnje i slabosti. Procena obrađuje mogućnost eksploatacije tih slabosti. Prilikom razvoja procene rizika potrebno je obratiti pažnju na sledeće stavke:

01. Identifikovanje i prioritizacija sredstava
02. Identifikovanje slabosti
03. Identifikovanje mogućih pretnji i mogućnost njihove eksploatacije
04. Identifikovanje protivmera
05. Analiza troškova i benefita
06. Razvoj sigurnosnih polisa i procedura

Postoje tri osnovna pristupa za razvoj modela sigurnosti mreže. Najčešće gotov proizvod predstavlja kombinacija sva tri pristupa:

01. Sigurnost kroz nevidljivost

U ovom modelu osnova je oslanjanje na nevidljivost, a što znači da je koncept da ako niko ne zna da mreža postoji, onda ona ne može biti ni napadnuta. Ovaj koncept nije dobar iz dva razloga. Prvi je to što ukoliko se mreža detektuje ona postaje otvorena meta, a drugi je što u današnjem biznisu skoro da i ne postoji mreža koja ne izlazi na globalnu mrežu.

02. Odbrana parametra

Ovaj model se oslanja na zaštitu oko mreže i ne obraća se preterano pažnja na zaštitu unutar mreže, već se oslanja na *firewall* iza koga je mreža sakrivena i koji razdvaja mrežu od javne mreže. Ovde se pretpostavlja da će to biti dovoljno da se mreža i odbrani. Model ima više mana. Osnovna je to što se ništa ne radi na zaštiti od napada iznutra. Ne treba zaboraviti, a što je ranije napomenuto, da se većina napada dešava iz same organizacije. Još jedan od problema jeste i to što spoljna zaštita u jednom trenutku će sigurno pokleknuti pred napadačima. Ukoliko se to desi mreža će ostati potpuno nebranjena.

03. Dubinska odbrana

Najkompleksnija zaštita jeste dubinska zaštita. Sastoji se od zaštite i monitoringa svakog sistema pojedinačno. Spoljna zaštita nije jedina na koju se mreža oslanja u ovom slučaju. Ovaj pristup je mnogo teže ostvariti u realnom okruženju, jer je neophodno da svi sistemi i ljudi koji rade na njihovoj zaštiti simultano budu na svom maksimumu. Koncept ove vrste zaštite jeste da ukoliko jedan od sistema bude kompromitovan, ostatak mreže može da zaštiti sebe, a u isto vreme prepozna odakle napad dolazi. Takođe, mnogo je veća zaštita od napada iznutra.

5.1 Digitalni potpis i Enkripcija [2] [8]

Za razmenu informacija preko mreža najvažniji elementi su poverljivost, pristup, autentifikacija i integritet poruke. To omogućava kriptografija, koja može biti oruđe kojim se postiže privatnost, autentifikacija identiteta koji učestvuju u komunikaciji, a i osigurava integritet razmenjenih poruka.

Kriptografija i enkripcija su u širokoj upotrebi već dugo vremena. Kada koristimo automate za podizanje novca ili plaćamo platnim karticama u suštini koristimo enkripciju.

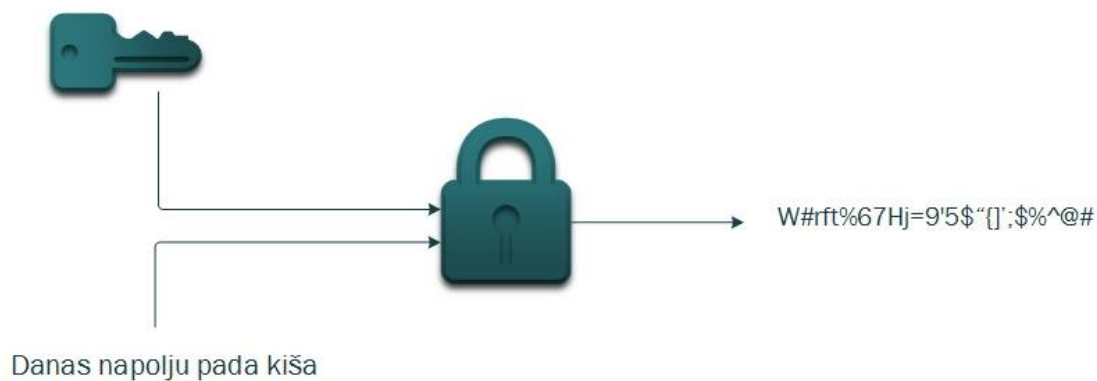
Enkripcija je proces kodiranja sadržaja koji se razmenjuje, tako da on bude nečitljiv za svakog osim onog ko poseduje „ključ“ koji je potreban da se sadržaj dekodira.

Postoji nekoliko činilaca koji određuju uspešno kodiranje, odnosno enkripciju podataka. Prvo je da mora biti reverzibilna. Sigurnost sistema treba da se oslanja na tajnost i dužinu ključa, a ne na detalje algoritma koji se koristi da bi se ostvarila enkripcija, a to znači da iako onaj koji je neovlašćeno presreo poruku i pokušava da je odgonetne možda zna način na koji je ostvarena enkripcija, ipak neće biti u stanju da dešifruje poruku. Takođe je izuzetno značajno da je algoritam korišćen za enkripciju prošao rigoroznu analizu. Algoritam ne sme da poseduje neku ozbiljnu slabost, ili neku koju je moguće eksploatirati. Algoritam koji se koristi za enkripciju poznat je pod imenom *šifra*.

Postoje dve vrste šifara:

01. *Stream* šifre

Ova vrsta šifre procesira običan tekst kako bi proizveo tok šifrata. Kroz šifru (algoritam) se propušta običan tekst kako bi se dobio šifrovani.



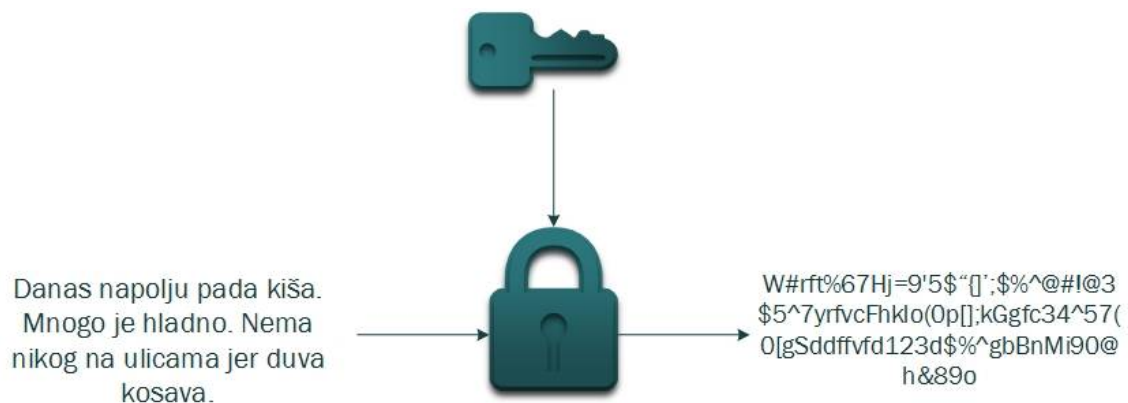
Slika br. 32 – *Stream* šifra

Ovakav način šifrovanja ima nekoliko slabosti. Najuočljivija jeste da se običan tekst reflektuje u tekstu koji je šifrovan. Šta to znači? Ukoliko šifrujemo rečenicu u kojoj se ponavlja par reči, to se primećuje i u šifrovanom tekstu, pa je razbijanje šifre olakšano. Pri tome, danas se uglavnom koristi engleski jezik kao jezik komunikacije, a on ima neka svoja pravila koja mogu da se iskoriste za razbijanje šifara. Najčešće korišćena slova u engleskom jeziku su E, T, A, I, O i N. Najmanje se koriste J, K, X, Q i Z. Najčešća kombinacija slova je „th“. Sve ovo olakšava osobi koja je iskusna u razbijanju šifara da istu razotkrije.

02. *Block* šifre

Razlika između *stream* i *block* šifre je u tome što se *block* oslanja na enkripciju i dekripciju u blokovima određene veličine, u odnosu na *stream*, gde se proces obavlja za svako slovo pojedinačno. Blok običnog teksta prolazi kroz algoritam, te se dobija blok kriptovanog teksta, idealno, skoro jednake veličine. Dobijeni blok ne sadrži neki prepoznatljiv obrazac, koji bi mogao posle da bude iskorišćen za razbijanje šifre.

Najpoznatiji algoritmi, od koji se neki i danas uspešno koriste, su *DES* (*Data Encryption Standard*), *IDEA* (*International Data Encryption Algorithm*), *RC5*, *AES* i *Blowfish*.



Slika br. 33 – *Block* šifra

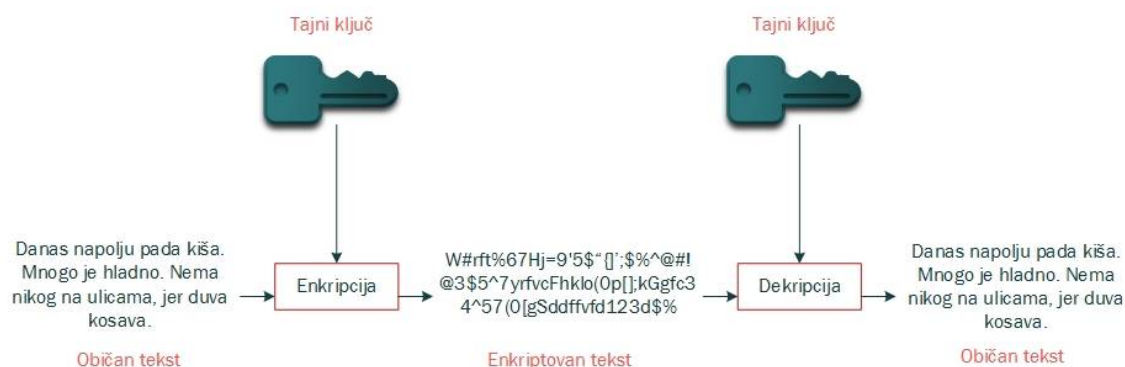
Kao što je ranije navedeno, enkripcija je proces kodiranja sadržaja poruke ili podatka, kako bi isti bio nerazumljiv za svakog osim onog ko poseduje ključ koji je neophodan da se „otključa“ poruka ili podatak.

Postoje dve vrste enkripcije:

01. *Symmetric Key Encryption*

Ova enkripcija se oslanja na privatni ključ i algoritam koji se razmenjuje između onih koji razmenjuju enkriptovan sadržaj. Isti ključ se koristi za enkripciju i dekripciju poruke. Međutim, snaga ovakve enkripcije zavisi od veličine ključa i od uspešnog\neuspešnog čuvanja da ne padne u posed neovlašćenim osobama.

Najbitnija mana ovog sistema jeste činjenica da algoritam i\ili ključ moraju da se razmene. Ukoliko se ključ razmenjuje preko neobezbeđene mreže on može vrlo lako biti kompromitovan, a što dovodi do toga da ovaj sistem nije odgovarajući za komunikaciju preko otvorenih i nezaštićenih mreža. Još jedna mana ovog sistema je i to što ne pruža mogućnost autentifikacije, kao i što ne postoji mogućnost sprečavanja opovrgavanja da je poruka poslata\primljena ili da je fajlu pristupano ili da je promenjen, a što je od izuzetnog značaj kod e-komercia (ovo se naziva *nonrepudiation*).



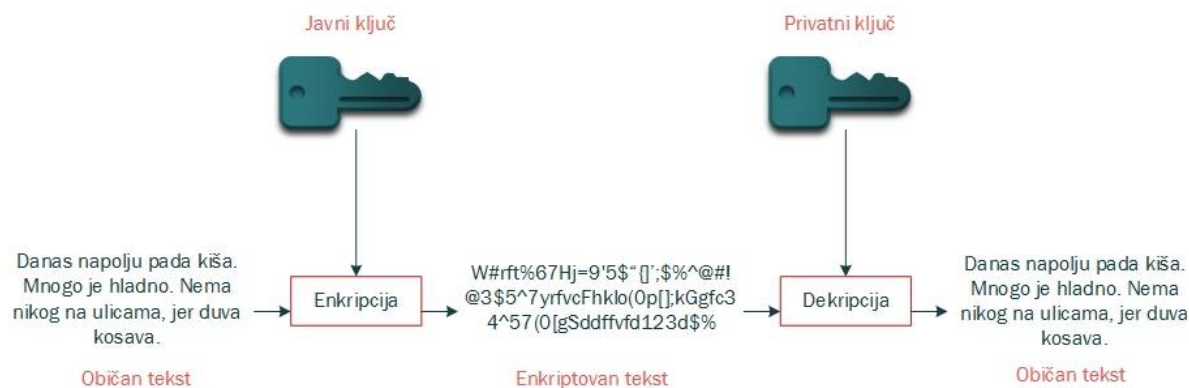
Slika br. 34 – *Symmetric Key Encryption*

02. *Asymmetric Key Encryption*

Ovaj koncept je predstavljen 1976 godine. Poznat je i pod imenom *Public Key* kriptografija. Sistem koristi dva ključa, odnosno privatni i javni ključ, koji predstavljaju odgovarajući par. Javni ključ ne otkriva privatni. Poruka se enkriptuje privatnim ključem i može se dekriptovati samo odgovarajućim javnim ključem, i obratno, ukoliko se poruka enkriptuje javnim ključem, može biti dekriptovana samo odgovarajućim privatnim ključem.

Upotrebom ovog sistema moguće je uspostaviti sigurnu komunikaciju sa bilo kim ko koristi odgovarajući softver ili uređaj. Ukoliko neko i presretne ključ nema mogućnost da dekriptuje poruku pomoću njega, jer samo odgovarajući privatni ključ može to da učini. Sigurnost je kompromitovano samo ako je privatni ključ kompromitovan.

Prednost nad krypto-sistemom sa simetričnim ključem jeste što pruža mogućnost autentifikacije i podržava digitalne sertifikate, pomoću kojih omogućava primenjivanje *nonrepudiation* (ne poricanje prijema ili izmene sadržaja poruke ili podatka).



5.2 Digitalni potpis [2] [8]

Digitalni potpis omogućava primaocu da autentifikuje identitet pošiljaoca i da potvrdi integritet poruke. Za ovaj proces je potrebno posedovanje javnog ključa pošiljaoca, jer se digitalni potpis koristi za potvrdu integriteta poruke i autentifikaciju. Pojednostavljeno, to znači da se digitalni potpis formira uz pomoć privatnog ključa pošiljaoca kako bi se hešovala (*hash* funkcija) cela poruka, od kojeg se formira *hash* vrednost. *Hash* funkcija je bilo koji algoritam koji mapira podatke proizvoljne dužine u podatke fiksne dužine. Vrednost dobijena ovom funkcijom naziva se *hash* vrednost (poznata i pod imenom *message digest*). Svaka promena u poruci ili na podatku dovelo bi do promene i *hash* vrednosti. Primalac poruke koristi javni ključ pošiljaoca kako bi potvrdio integritet poruke. Na ovaj način, istovremeno, se osigurava integritet poruke i identitet pošiljaoca.

Da bi potpisao poruku, pošiljalac dodaje digitalni potpis na kraju poruke i enkriptuje je pomoću javnog ključa primaoca. Primalac dekriptuje poruku koristeći svoj privatni ključ i potvrđuje identitet pošiljaoca i integritet poruke, tako što dekriptuje digitalni potpis pošiljaoca koristeći njegov javni ključ.

U zemljama Evropske unije, Sjedinjenim Državama, Brazilu i Indiji, digitalni potpis pravno je regulisan.

Najveća snaga digitalnog potpisa jeste u tome što je gotovo nemoguće ga falsifikovati i lako se potvrđuje. Ukoliko učesnici razmene poruka ne znaju jedno za drugo od ranije, odnosno, ne poseduju javne ključeve svojih sagovornika, mora postojati treća strana kojoj se veruje, a koja će potvrditi identitete učesnika.

5.3 Digitalni sertifikat [2] [8]

Digitalni sertifikat se koristi za potvrdu da je poruka koja je pristigla nepromenjena, kao i da verifikuje identitet pošiljaoca pomoću javnog ključa. Problem sa autentifikacijom digitalnog potpisa jeste što je potrebna potvrda da taj javni ključ zaista pripada onom ko je poslao poruku.

Sertifikat izdat od strane *CA (Certification Authority)* autoriteta, koji koristi *PKI (Public Key Infrastructure)* infrastrukturu, može da se koristi za autentifikaciju identiteta pošiljaoca prilikom prvog kontakta. Omogućava visoki nivo poverljivosti. Na ovaj način vezuje pojedinca ili entitet sa javnim ključem. Zatim digitalni sertifikat potpisuje *CA* sa privatnim ključem sertifikacionog autoriteta. Time se dobija nezavisna potvrda da je pojedinac ili entitet zaista taj za koga se izdaje. *CA* izdaje digitalni sertifikat koji garantuje identitet onog kome je izdat taj sertifikat.

5.4 Kerberos Key Exchange [2] [8]

Kerberos je mrežni protokol za autentifikaciju, koji je napravljen da obezbedi jaku autentifikaciju za server\ključent aplikacije, tako što koristi i tajni i javni ključ. Oslanja se na centralni server, tzv. *trusted server*, koji će se ponašati kao treća strana, kako bi autentifikovao korisnike i kontrolisao pristup resursima na mreži.

Nikada ne vrši transmisiju lozinke preko mreže, bez obzira da li je kriptovana ili ne. Koristi kriptografske ključeve koji se nazivaju tiketi, kako bi kontrolisao pristup mrežnim resursima. Tiketi su enkriptovane propusnice koje se izdaju korisnicima ili procesima i koji određuju nivo pristupa. Postoji šest vrsta tiketa:

- *Initial*
- *Invalid*
- *Pre-authenticated*
- *Renewable*
- *Forwardable*
- *Postdated*

Jedan od limita Kerberosa jeste da ukoliko server iz nekog razloga nije u funkciji, niko u mreži ne može da pristupi resursima, s obzirom da svaki prilaz mora biti autorizovan preko Kerberos servera. Zbog te činjenice veoma je podložan *denial-of-service* napadima, gde napadač može da zablokira rad servera tako što će slati veliki broj zahteva i tako spreći da odgovori na legitimne upite.

Napadač iz same mreže može da skenira saobraćaj i snima zahteve koji idu od i ka Kerberos serveru. Potom može kopirati te zahteve i tako zagušiti saobraćaj. Obično se ovakvi napadi, pod nazivom *replay* napadi, sprečavaju tako što se na zahtev stavlja *time stamp*.

Jedan od minusa je i ogroman saobraćaj koji se pravi, s obzirom da svaki upit ide prvo ka ovom serveru. Što veći broj servera i radnih stanica, to i veći broj zahteva upućenim Kerberos serveru. Postoji limit dokle mreža koja se oslanja na Kerberos može da raste.

5.5 E-mail

Elektronska pošta je ubedljivo najviše korišćen servis, te je stoga problematika prerasla samo puko slanje *e-mail* poruka od jednog do drugog pošiljaoca.

Postoji niz opasnosti kada je u pitanju razmena *e-mail* poruka. Ovo su samo neke od njih:

- Netačne informacije
- Prevare
- Virusi i druge vrste zlonamernog koda
- *Junk e-mail*
- Lančana pisma
- Šeme za brzo bogaćenje
- Ukraden softver
- Ukradena muzika ili video
- Plagijati
- Kriminalne aktivnosti od strane hakera
- *Online* aukcije
- *Online* kockanje
- Kupovina preko Interneta
- Igrice
- *Online* upoznavanje
- Pornografija itd.

Treba uvek imati na umu da je slanje *e-mail* poruka u principu veoma nesigurno, jer često poruka putuje kroz mnoge mreže i prolazi kroz veliki broj *mail* servera. Rezultat toga je velika mogućnost presretanja, replikacije i modifikacije. Takođe je vrlo lako lažirati identitet koji šalje *mail*.

Jedno od rešenja jest korišćenje *secure e-mail*, koji pruža:

- Neotkrivanje sadržaja poruke, a što se postiže korišćenjem enkripcije
- Integritet poruke – osigurava da poruka nije menjana na svom putu, te omogućava da se integritet poruke i potvrdi. Postiže se korišćenjem *hash* algoritma
- Potvrda o pošiljaocu – da bi se potvrda ostvarila potrebno je koristiti tehnologiju digitalnog potpisa
- Potvrda o primaocu – za ovu potvrdu je zadužena enkripcija pomoću javnog ključa

Postoji više vrsta protokola koje se koriste u *secure e-mail* tehnologiji, a najviše se koriste PGP (*Pretty Good Privacy*) i S/MIME (*Secure Multipurpose Internet Mail Extension*).

Nastao 90tih godina prošlog veka, PGP se i dalje koristi, jer poseduje niz prednosti u odnosu na druge protokole, a ponajviše jer se može koristiti na velikom broju platformi, uključujući Windows, UNIX, Macintosh itd. Zasnovan je na algoritmima koji se smatraju izuzetno sigurnim (RSA, DSS, CAST-128, IDEA, 3DES). Pri tome je i Internet standard.

Zasniva se na kriptografiji javnog ključa kako bi osigurao poverljivost. Takođe, i digitalni potpis kako bi se potvrdio identitet pošiljaoca i integritet poruke. Kao dodatak je i mogućnost enkripcije. Koristi kombinaciju simetrične i asimetrične enkripcije kako bi se ubrzao proces enkripcije.

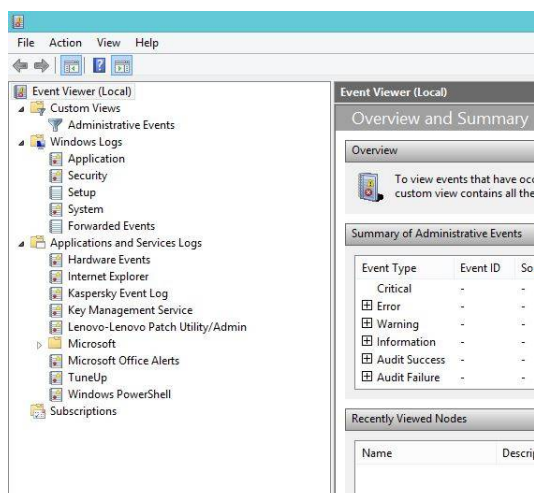
Secure MIME predstavlja nastavak originalnog *e-mail* protokol standarda koji određuje kako poruka treba da bude formatizovana kako bi mogla da bude razmenjivana između različitih sistema. Koristi RSA sistem enkripcije. Takođe predstavlja Internet standard, ali i industrijski standard koji se koristi u komercijalne svrhe. Razlika između

PGP i S/MIME je u tome što PGP koristi javni ključ za enkripciju, dok S/MIME se oslanja na digitalne sertifikate koje sadrže digitalne potpise za autentifikaciju pošiljaoca. Takođe koristi *hashing* da bi osigurao integritet poruke i kombinaciju simetričnog i asimetričnog ključa da osigura poverljivost.

5.6 Sigurnost operativnog sistema

Iako se mnoge mreže oslanjaju prvenstveno na zaštitu cele mreže, zaštita mreže počinje na nivou sistema. Da bi mreža bila pravilno zaštićena i imala visok nivo zaštite, svaki sistem mora biti pravilno zaštićen i nadgledan. Ovakav pristup zaštiti iziskuje mnogo vremena i precizne organizacije, pa je malo koja firma spremna na takva ulaganja, te se oslanja na spoljašnju zaštitu. Međutim, kako je već ranije navedeno u ovom radu, uvek postoji mogućnost da zaštita bude probijena, ali i da napad dođe iz same mreže. Ukoliko ne postoji zaštita zaposleni koji ima loše namere može doći do poverljivih informacija, uvid u plate i lične informacije o zaposlenima, ali i da ugrozi kompletnu mrežu.

Na sistemima koji su kritični za pravilan rad mreže treba omogućiti i logovanje, kao i upis svih mrežnih aktivnosti. To je jako važna stavka, jer može preventivno da ukaže na neke potencijalne probleme. Npr. veliki broj pogrešnih logovanja na mašinu može da ukaže na eventualni napad. S obzirom da osnovno mesto logova jeste na samoj mašini, potrebno je koristiti sistem koji će logove držati na jednom mestu, npr. *Microsoft System Center Operations Manager*. Na ovaj način se sprečava da se logovi brišu ili menjaju od strane zlonamernog korisnika. Logovanje je izuzetno bitno za otkrivanje kako problema na samoj mašini, tako i eventualnih sigurnosnih pretnji.



Slika br. 35 – Izgled *Event Log*-a na mašini koja radi na Windows platformi (verzija 8.1)

Sledeći korak u zaštiti jeste efikasna autentifikacija i identifikacija korisnika koji računar koristi. Za to se koristi kombinacija korisničkog imena i lozinke. Lozinka predstavlja možda i najslabiju kariku, a sve sa razloga što većina firmi ostavlja na volju korisniku da izabere lozinku koju će da koristi. Korisnici najčešće biraju previše kratke, koje je lako pogoditi, sastavljene od imena dece, supružnika, datuma rođenja, ili jednostavno niz na samoj tastaturi (npr. 123456789). Ukoliko firma odluči da sprovede rigoroznu politiku lozinke, te se odluči da obaveže korisnika da koristi kombinaciju brojeva, slova i znakova, i dalje postoji opasnost da korisnik zapiše lozinku na vidnom mestu i tako omogući zlonamernom kolegi da do te lozinke dođe. Još jedan problem jeste i razmena lozinke među korisnicima.

Firma treba da ima jaku politiku oko dužine i kompleksnosti lozinke. Preporučljivo je da bude najmanje osam karaktera dugačka, sa velikim i malim slovima, brojevima, a idealno bi bilo uključiti i specijalne znakove, ako što su @#\$%&*. Korisnicima treba precizno objasniti šta u svojim lozinkama ne treba da kombinuju, a potpuno treba da bude zabranjena kombinacija sa svojim ili korisničkim imenom. Ne sme se dozvoljavati ponavljanje lozinke kada sistem zatraži njenu promenu. Takođe, lozinka mora da ima minimalno i maksimalno vreme trajanja.

Najbolje po sistem jeste upotreba generičkih lozinke, koje se mogu napraviti jednostavno preko softvera ili sajtova na Internetu koji pružaju takve usluge. Generičke lozinke se sastoje od nasumično odabranih kombinacija slova, brojeva i specijalnih znakova. U isto vreme, odabir ovakve vrste lozinke je i jako loše po sistem, jer su korisnici skloni zapisivanju i postavljanju na vidna mesta (npr. čuveni žuti stiker zalepljen na monitor).

Izuzetno je značajno da administratori u sistemu pažljivo biraju i čuvaju svoje lozinke. Vrlo česta pojava je i da administrator koji radi paralelno na dve mreže koristi iste lozinke kako ne bi imao veliki broj lozinke da zapamti. To drastično povećava opasnost. Takođe, treba izbegavati upotrebu imena „administrator“ i „admin“ u nalozima koji pripadaju administratorima, jer to direktno upućuje koji nalog treba napasti kako bi se dobio pristup resursima.

Kada se korisnik pravilno uloguje, on pristupa ne samo resursima na svom računaru, već i mrežnim resursima. Autorizacija pristupa sistemskim resursima se kontroliše preko *Access Control List*. To je mehanizam koji brani ili dozvoljava pristup resursima. Svaki upis u ovu listu definiše prava pristupa bilo kom korisniku, odnosno da li korisnik ima pravo da čita, zapisuje, briše ili uopšte nema prava pristupa. Lista funkcioniše po sistemu eksplicitnog odbijanja. To znači da ukoliko korisnik nije na listi, automatski nema pravo pristupa. Permisije treba razlikovati i po tome da li su date za lokalni ili mrežni pristup. Takođe, mogu se dati i za korisnika pojedinačno i za grupu.

Dozvole:

01. *Read*: korisnik koji ima ovakvo pravo može jedini da pregledava sadržinu fajla ili foldera.
02. *Write*: korisnik sa ovim pravom može da menja sadržaj fajla ili foldera
03. *Execute*: ovom dozvolom korisnik je u mogućnosti da pokrene neki program unutar foldera
04. *Delete*: ovo pravo treba pažljivo dodeljivati, jer korisnik može da briše sadržaj foldera, kao i sam folder

Bitan činilac ovih prava predstavlja i uloga *Owner*. To je onaj koji je određen da to bude, bilo da ga je kreirao, bilo da je mu je to pravo dodeljeno, ili tako što je tu privilegiju preuzeo. Vlasnik fajla ima sva prava nad njim. To je posebno značajno ukoliko se želi onemogućiti osobi koji je taj fajl kreirala bilo kakav pristup. Iako bi se, npr., na samom fajlu skinula ta osoba sa liste pristupa, on bi dalje mogao da pristupa, menja, pa i obriše fajl, jer je on vlasnik. U tom slučaju je bitno da se vlasnik promeni ili da se preuzme vlasništvo. Jedino na taj način se potpuno ukida pristup tom korisniku.

5.6.1 Antivirus [1]

Pojavom virusa, računarski svet se promenio. U nekoliko zadnjih dekada predstavljaju konstantnu pretnju sistemima. Dizajnirani da načine štetu, mogu prouzrokovati krađu i uništavanje podataka, onemogućavanje normalnog rada aplikacija i operativnog sistema, pa i njegov prestanak sa radom.

Zbog visoke cene, mnoge firme se odlučuju da izbegnu ovaj trošak, te se oslanjaju isključivo na spoljnu zaštitu, ali kao što je već navedeno, najbrojniji napadi dolaze iz same mreže. Broj napada se može značajno umanjiti pravilnom politikom antivirusnog sistema.

Prvi antivirusni programi su koristili jednostavno skeniranje unutar fajla u potrazi za određenim stringom koji ukazuje na postojanje malicioznog sadržaja. Tako su današnja rešenja popularno nazvana AV skeneri. Međutim, današnji AV je daleko od pukog skenera. To mora i biti, jer nije više tako jednostavno pronaći i odstraniti virus. Međutim, zaštita i udobnost nikada nisu išli zajedno. Današnji antivirusi su izuzetno komplikovani logički softveri, pa s toga mogu i da odmognu korisniku. Poznati su problemi pojedinih poznatih AV rešenja sa VPN konekcijama.

Često se sistem administratori i ne trude preterano da upotrebe sve prednosti AV-a. Nekonfigurisani pravilno i često bez ažurirane antivirusne baze, doprineli su da pojedini virusi opstaju na mreži mnogo duže nego što je to zaista bilo neminovno. Ili, pak, da krene epidemija unutar mreže nekog virusa koji se lako otklanja, a sve zbog neažurne baze virusa.

AV rade po osnovnoj metodi zaštite:

- Detektovanje – pronalaženje već poznatih virusa
- Prevencija – monitoring pokušaja ili promene fajlova
- Heuristika – potraga za još nepoznatim virusima korišćenjem već poznatih potpisa

Na tržištu danas postoji veliki broj vendara antivirusa. Ne mogu se svi podjednako pohvaliti visokim kvalitetom. Tako da treba biti izuzetno oprezan prilikom odabira rešenja. Pogotovo se to odnosi na velika mrežna okruženja, sa šarenolikim brojem i konfiguracijama računara i servera, jer zbog toga što antivirusi nisu više samo puki skeneri i imaju veliki broj dodatnih funkcija, samim tim se povećava opterećenje procesora i memorije, što znači da u periodu kada je antivirus aktivan može doći do usporenog rada.

5.7 Dostupnost[35] [36]

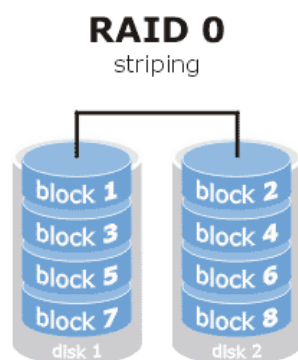
Od izuzetnog je značaja da resursi mreže budu dostupni 24\7\365, a što znači mogućnost da se pristupi podacima unutar mreže kad god je to potrebno. Jedan od metoda za postizanje ovog cilja jeste redudansa podataka. Najčešće korišćena metodaje *RAID*.

Ova tehnologija za skladištenje podataka kombinuje dva ili više HDD-ova u logičke jedinice, kako bi se postigle veće brzine i osigurala redundantnost.

Najviše se koriste:

➤ RAID 0

Podaci se dela na dva ili više diskova bez uparivanja informacija, kako bi se dobila veća brzina. Koristi se zbog povećanja performansi, kao i za formiranje velikih logičkih diskova. Mogu se upotrebiti diskovi različitih veličina pošto se oni sabiraju. Negativna strana jeste to što ukoliko podaci na jednom od diskova postanu korumpirani, velika je verovatnoća da će kompletno biti izgubljeni.

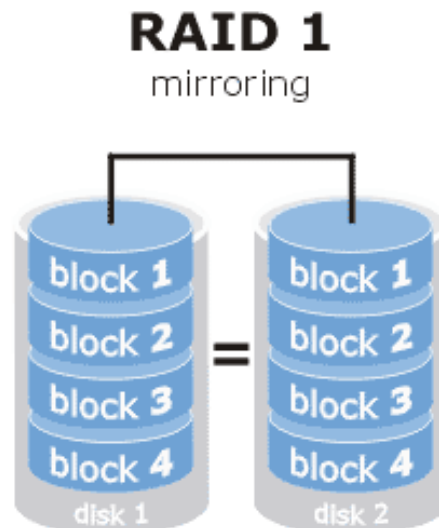


Slika br. 36 – RAID 0 [37]

➤ RAID 1

To je replikacija fizičkog HDD-a na drugi fizički disk u realnom vremenu, odnosno predstavlja njegovu identičnu kopiju. Ukoliko jedan od ova dva diska prestane sa radom, server će i dalje biti u funkciji. Potrebno je tada zameniti pokvaren disk, i uraditi *rebuild*. Posle toga ponovo ćemo imati *disk mirroring* sistem. Poznat je i kao RAID 1. Treba naglasiti da *mirroring* nije i ne sme predstavljati zamenu za backup.

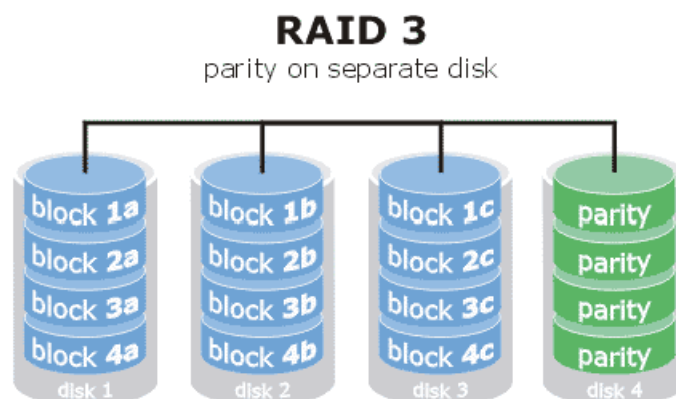
Negativna strana je drastično smanjenje prostora za skladištenje podataka. Poželjni su i odvojeni kontrolori diskova kako bi bilo moguće uraditi *hot swap*, a što znači da se može izvršiti zamena pokvarenog diska bez gašenja servera.



Slika br. 37 – RAID 1 [37]

➤ **RAID 3**

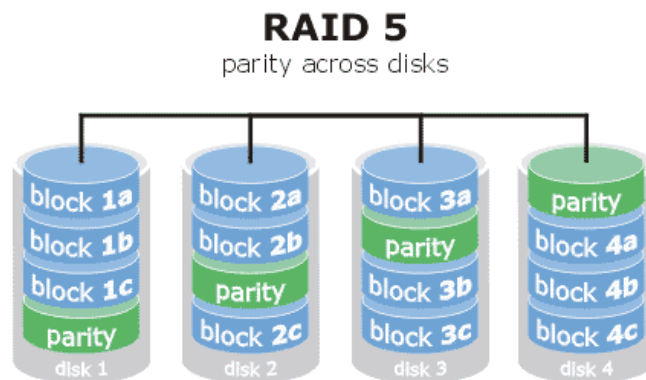
Kod ovog sistema potrebna su tri ili više diskova. Podaci se pravilno upisuju na svaki disk, s tim što sada postoji i dodatni disk na kome se smeštaju informacije o paritetu. Tako se osigurava povraćaj podataka ukoliko se jedan od diskova korumpira. Koristi se kada je potreban upis i čitanje podataka velikom brzinom i u velikoj količini. Ukoliko dođe do otkaza jednog od diskova neće se značajno usporiti rad. Zbog kompleksnosti ne koristi se često.



Slike br. 38 – RAID 3 [37]

➤ RAID 5

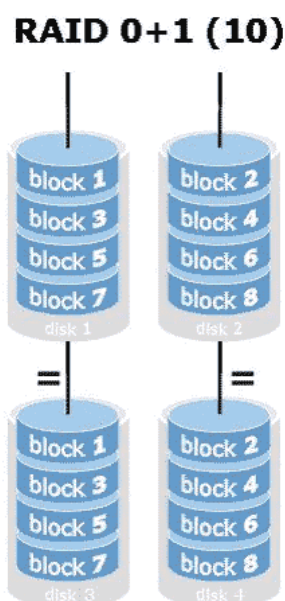
RAID 3 i RAID 5 sistemi su dosta slični. Razlika je u tome što kod RAID 5 se podaci ne upisuju paralelno na diskove. Diskovi koji sadrže informacije o paritetu ne nalaze se na jednom fizičkom disku, već na svakom od diskova uključenih u RAID 5. Potrebna su bar tri diska. Ukoliko se pokvari jedan od diskova, ovaj sistem će i dalje funkcionisati bez gubitka podataka. Može se kontrolisati i preko *software* i *hardware* disk kontrolera. Upis i čitanje podataka su veoma brzi, mada takođe se ne koriste prečesto zbog kompleksnije tehnologije. Idealno rešenje za aplikativne servere.



Slika br. 39 – RAID 5 [37]

➤ RAID 10

Predstavlja kombinaciju sistema RAID 1 i 0, te koristi njihove prednosti. A to znači da kombinuje *mirror* i *stripe* opcije. Minimum su četiri diska, od kojih dva su u *strip*-u, a dva u *mirror*-u.



Slika br. 40 – RAID 10 [37]

5.8 Hbovi (Hubs), Svičevi (Network Switches) i Ruteri (Routers)

Sve uređaje u jednoj mreži treba povezati kako bi mogli da funkcionišu zajedno. Postoji nekoliko vrsta i zavise od toga na kom nivou OSI modela funkcionišu, te kolika je njihova upravljivost.

5.8.1 Hub

Najslabiji i sa najmanje mogućnosti je *Hub*. Funkcioniše na prvom sloju OSI modela (Fizički sloj) i poznat je i pod imenom repetitor, zato što fizički povezuje uređaje. Nije upravljiv i ne može da procesuirati informacije sa drugog i trećeg nivoa OSI modela. *Hub* će uvek prosleđivati sve paketa na svaki port, uključujući i port sa kojeg paketi pristižu. Ne razlikuju tipove frejmova, te će uvek prosleđivati na sve portove *unicats*, *multicast* i *broadcast* saobraćaj. Ethernet *hub* je *half-duplex*, a što znači da uređaju mogu da primaju i šalju podatke, ali ne u isto vreme.

Ukoliko dva ili više uređaja u isto vreme vrše transmisiju doći će do kolizije. Ukoliko se to dogodi *hub* će odbaciti sve pakete i o tome obavestiti hostove. Svi uređaji će tada sačekati proizvoljni vremenski period pre nego što ponovo pošalju podatke. Ukoliko se koristi više *hub*-ova za povezivanje uređaja na mreži, treba imati na umu da oni svi spadaju u isti domen i time svi podložni koliziji. Što više uređaja i više portova, to je veća verovatnoća da će do kolizije i doći.

5.8.2 Switch

Na drugom nivou OSI modela (*Data Link sloj*) komuniciraju uređaji preko *switch*-eva. Ovi uređaji su upravljivi i mogu sadržati liste MACadrese hostova, kao i njihovih portova. *Switch* će preusmeriti paket jedino na adresu na koju je upućena, a informacije za to će pronaći u *Data Link* hederu iz samog paketa. Te liste se kreiraju dinamički, odnosno *switch* prikuplja adrese skeniranjem svih svojih portova, dakle kada jedan uređaj pošalje paket drugom *switch* će zabeležiti adresu uređaja koji šalje, dok će adresu uređaja koji prima paket zabeležiti kada sa istog uređaja krene povratna informacija.

Switch ima *full duplex* opciju, ali kao i *hub*-ovi mogu pripadati samo jednom *broadcast* domenu, pa će preusmeravati pakete ka svim portovima, osim onog koji šalje pakete. Posедуje mehanizam za izbegavanje upadanje u *loop*-a.

Switch-evi podržavaju tri metode za propuštanje paketa:

01. *Store-and-Forward* metod

Metod radi po principu kopiranja svakog kompletnog okvira (*frame*) u memoriju *switch*-a, na osnovu kojih on obračunava CRC (*Cyclic Redundancy Check*) kako bi pronašao greške. Za to koristi matematičku formulu zasnovanu na broju bitova u okviru (*frame*), kako bi utvrdio da li u primljenom okviru ima grešaka. Ukoliko pronađe grešku okvir se odbacuje. Ako grešaka nema okvir se prosleđuje na upućeni port.

02. *Store-and-Forward* metod

Ovde se u memoriju učitava kompletan okvir i proverava da li sadrži greške pre nego što se pošalje ka destinaciji. Time se obezbeđuje visok nivo mrežnog saobraćaja bez grešaka, jer se loši paketi odbace pre nego da se pošalju kroz mrežu. Ovaj metod utiče na performanse, jer se u memoriju učitava ceo podatak i proveravaju greške pre nego što se pošalje dalje, a što može da prouzrokuje veće zakašnjenje. Pogotovo se to oseća u mrežama gde ima više ovakvih uređaja, zato što se podatak proverava na svakom uređaju.

03. *Cut-Through* metod

Kod ovog metoda u memoriju se kopira samo MACadresa destinacionog uređaja, a koja se nalazi u prvim 6 bajtova okvira. *Switch* pretražuje svoje tabele, utvrđuje odgovarajući port i prosleđuje paket samo po toj putanji. Time se smanjuje kašnjenje, jer uređaj prosleđuje okvir čim pročita destinacionu adresu i odredi odgovarajući port. Treba napomenuti da se propuštaju svi paketi, i sa i bez greške, pa se pronalaženje greške ostavlja uređaju na odredištu.

04. *Fragmen-Free* metod

Poznat i kao *Runless Switching*, predstavlja hibrid *Cut-Through* i *Store-and-Forward* metoda. Radi kao i *Cut-Through*, sa izuzetkom što čuva 64 bajtova sa svakog

okvira pre slanja, jer se najviše grešaka i kolizija dešava u tih prvih 64 bajtova. Može se smatrati kompromisom između dva metoda čiji je hibrid.

Propuštanje paketa na trećem nivou OSI modela (*Network* sloj) ostvaruju uređaji pod nazivom Ruteri. Ovo je takođe *Fragment-Free* preusmeravanje paketa. Kompleksniji su od *hub*-ova i *switch*-eva.

Multilayer switching je tehnika koja kombinuje *data link* (nivo 2 OSI modela) i *network* (nivo 3 OSI modela). Da bi ovo postigao, uređaj mora da koristi *Store-and-Forward* tehniku, jer mora da primi čitav okvir pre nego što upotrebi bilo koji protokol za prosleđivanja paketa.

Čitav okvir se uvlači u memoriju i računa se CRC (*Cyclic Redundancy Check*). Tada se utvrđuje da li je paket dobar ili loš. Ako se CRC koji stoji zabeležen na paketu poklapa sa CRC-om koji je izračunao *switch*, čita se adresa destinacionog uređaja i paket se preusmerava na tačan izlazni port. Ukoliko se razlikuju okvir se odbacuje.

Najznačajnija razlika između *switch*-a i *router*-a je u tome što se sa ruterima dostigla brzina koju je nudio *switch*, pri tom je moguće i preusmeravanje paketa na trećem nivou OSI modela, što omogućava precizno usmeravanje paketa samo na određeni port.

5.8.3 Router

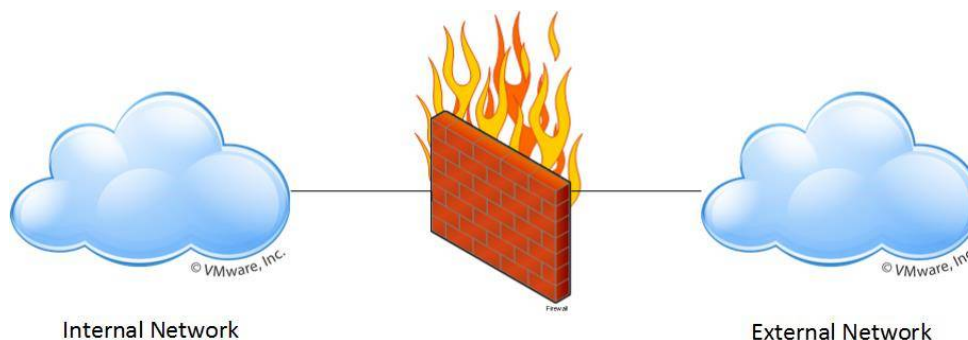
Jedna od mogućnosti koju pruža *router* jeste i to na koji način saznaje o okolnim mrežama i na taj način odlučuje najbolji put za paket. Postoje tri mogućnosti – kroz lokalno uključene/iskorišćene portove, upis statičkih ruta i dinamičkim protokolima. Da bi skupio ove informacije koristi protokole za rutiranje (*RIP*, *BGP*, *OLSR*, *OSPF*). Takođe ih koristi i za širenja informacija o mreži. Na taj način *router*-i uče o stanju mreže, a koje smeštaju zajedno sa svojim originalnim informacijama, pa tako sabrane podatke šalju drugim *router*-ima.

Kada uređaj pošalje drugom uređaju paket na njega stavlja *Ethernet* okvir i u njega stavlja IP paket. On sadrži IP adresu pošiljaoca i adresu primaoca paketa. *Router* čita te adrese, upoređuje ih sa svojim tabelama i odlučuje o putanji paketa. Koji je

sledeći korak paketa odlučuje *router* na osnovu dela IP adrese primaoca poruke. Adresa se sastoji od identifikatora mreže i identifikatora hosta. Identifikator hosta se pregleda samo kada prethodna provera pokaže da je u pitanju lokalna adresa.

Mrežni protokol koji se koristi za razrešenje IP adrese u MAC adrese je *Address Resolution Protocol (ARP)*. Uređaj kojem treba da sazna MAC adresu broadkastuje ARP zahtev preko mreže. Uređaj koji poseduje tu adresu odgovara sa MAC adresom. To se naziva ARP mapiranje (*ARP Mapping*). Čim utvrdi kojoj mreži treba proslediti paket *router* traži destinacionu MAC adresu u ARP kešu. Potom preusmerava paket kroz lokalnu mrežu u okviru koji sadrži MAC adresu lokalnog hosta, odnosno sleće *router* kojem je prosleđuje paket.

5.9 Firewall



Slika br. 41– Firewall

Firewall predstavlja kombinaciju hardvera i softvera, čija je svrha da zaštititi internu mrežu od Interneta u globalu i ima ulogu da pakete propušta i prolazi njihov prolaz. To su *Intrusion Detection Systems (IDS)* i *Intrusion Prevention Systems (IPS)*.

Pored propuštanja paketa, on omogućava kontrolu pristupa spoljnog sveta sa mrežnim resursima. *Firewall* služi da sav saobraćaj ka spolja i unutra prolazi kroz njega, kako bi ga kontrolisao prema unapred predefinisanim pravilima. To znači da će do krajnjeg korisnika proći samo saobraćaj koji je tim pravilima dozvoljen. Ta pravila se nazivaju polise. Ukoliko je *firewall* pogrešno konfigurisan predstavljaće laku metu, te će podaci i resursi vrlo lako postati kompromitovani. Pruža mogućnost NAT-a (*Network Address Translation*), kao i logovanje saobraćaja. Negativna strana jeste to što predstavlja *single point of failure*. Ukoliko *firewall* „padne“ sav saobraćaj će biti

potpuno prekinut. Mada najveći uticaj može imati na performanse mreže, jer skeniranje svakog dolaznog i odlaznog paketa zahteva vreme.

Nije dovoljno samo postaviti *firewall*. Potrebno je i redovno je nadgledati i kontrolisati logove. Mnoge firme prave krucijalne greške, jer smatraju da je to dovoljno da se mreža zaštiti, te neće obratiti pažnju na unutrašnju zaštitu, a o čemu je bilo govora ranije u ovom poglavlju.

Postoje četiri tehnike koje se koriste za kontrolu pristupa:

1. *Service control*

Određuje tip Internet servisa kojem se može pristupati, te uređaj može filtrirati na osnovu IP adrese, protokola ili broja porta. Takođe, može imati softver koji pruža *proxy*, koji ima ulogu da procesuirá svaki zahtev za određenim servisom pre nego što ga propusti.

2. *Direction control*

Određuje na koji način se određeni zahtev za servisom može inicirati i propustiti kroz „zid“.

3. *User control*

Kontroliše pristup korisnika, prvo mreži, pa onda i resursima, ukoliko ima dozvolu za ulazak spolja, kao i pregled određenog sadržaja na Internetu korisnika unutar mreže.

4. *Behavior control*

Kontrola kako se određeni servis koristi. Npr., može filtrirati *mail* poruke kako bi se eleminisao *spam*.

Kada filtrira pakete, *firewall* može to činiti na osnovu pozitivnog ili negativnog filtera. Pozitivan filter je onaj koji propušta pakete na osnovu specifičnog kriterijuma, dok negativan filter odbacuje pakete koji se poklapaju sa specifičnim kriterijumima.

5.9.1 Vrste Firewall-a

5.9.1.1 Packet Filtering Firewall

Ovaj filter primenjuje set pravila za svaki dolazni i odlazni IP paket, te u odnosu na ta pravila propušta ili odbacuje pakete. Tako je i konfigurisan, da propušta pakete u oba smera. Filtriranje se vrši na osnovu podataka koji se nalaze u paketu:

- IP adresa izvora
- IP adresa destinacionog uređaja
- *Transport-Level* adresa i izvora i odredišta (TCP, UDP)
- Polje IP protokola
- *Interface* (Kod *firewall*-a koji imaju tri ili više portova kontroliše se na

koji port paket pristiže i na koji treba da se usmeri)

Filter jeste lista pravila sa kojima se upoređuju zaglavlja paketa, IP ili TCP. Ako se sadržaj poklapa sa nekim od pravila, to pravilo određuje da li će paket biti propušten ili odbačen. Ukoliko ne postoji poklapanje, tada se primenjuju osnovna pravila: ***odbaciti*** – svi paketi bivaju odbačeni; ***propustiti*** – svi paketi se propuštaju.

Češće se koristi osnovna polisa po kojoj se svi paketi koji ne odgovaraju uslovima odbace, ali je ona značajno restriktivnija. Svaki servis se mora pojedinačno propustiti. Tada je *firewall* vidljiv korisnicima dok se polisa ne podesi kako je u skladu sa politikom firme. Druga vrsta je mnogo lakše primenjiva, ali umanjuje sigurnost, jer su svi paketi propušteni.

5.9.1.2 Stateful Inspection Firewall

Funkcioniše, takođe, na mrežnom nivou OSI modela. Filtriranje se zasniva na istom pojedinačnom skeniranju paketa, ali sa mogućnošću promene pravila propuštanja prema potrebama. To je od posebnog značaja kod servisa gde povratna informacija ne stiže istim putem (npr., *e-mail* servis).

Ovaj tip *firewall*-a prati stanje mrežnih konekcija i u svojoj memoriji čuva najznačajnije attribute svake od konekcija. Ti atributi su poznati kao stanje konekcije i mogu sadržati IP adrese, portove koji se koriste i broj senkvence paketa. Sve što kontroliše (dolazne i odlazne pakete, stanje konekcije) smešta u svoje tabele, koje se formiraju dinamički. Ovi podaci se obrađuju kako bi se buduća konekcija oslanjala ne samo na pravila koje je odredio administrator, već i na osnovu konekcija i poslatih paketa koji su već koristili istu putanju.

5.9.1.3 Application-Level Gateway

Poznat i pod imenom *Application Proxy*, predstavlja rešaj za saobraćaj na aplikativnom nivou. Korisnik se prijavljuje *gateway*-u preko aplikacije koja koristi TCP/IP (Telnet, FTP) i potrebno je da obezbedi ime hosta koji treba da se kontaktira. Kada korisnik odgovori, te unese odgovarajuće korisničko ime i lozinku, *gateway* tada kontaktira aplikaciju na krajnjoj destinaciji i pušta TCP segmente u kojima se nalaze podaci između ta dva *end-point*-a.

Ovi uređaji su znatno sigurniji od paketnog filtriranja. Umesto da procesiraju veliki broj mogućih kombinacija koje propuštaju ili zabranjuju prolaz paketa, za *gateway* je neophodno da obradi podatke od nekoliko dozvoljenih aplikacija i tako prikupi potrebne podatke.

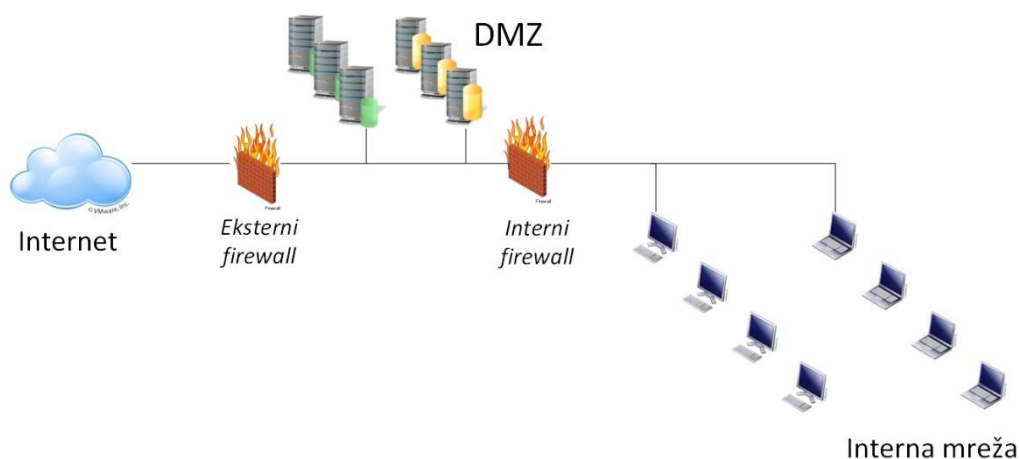
5.9.1.4 Circuit-Level Gateway

Ovaj sistem može biti samostalan ili može funkcionisati kao *gateway* na aplikativnom nivou za pojedine aplikacije. Takođe se oslanja na dve konekcije, umesto na jednu, kao i *Circuit-Level Gateway*, odnosno jednu od korisnika koji šalje pakete do sebe, i od sebe do korisnika koji prima pakete. Čim se konekcije uspostavi *gateway* propušta TCP segmente od jedne konekcije ka drugoj bez pregleda sadržaja. To će

preuzeti *security* funkcija koju poseduje. Ova funkcija će proveravati koja konekcija će biti dozvoljena.

Osim po načinu kontrole saobraćaja, *firewall*-i se mogu razlikovati i po lokaciji gde su postavljeni i po konfiguraciji.

5.10 DMZ (*Demilitarized Zone*)



Slika br. 42 – DMZ zona (*Demilitarized Zone*)

Izuzetno je bitna lokacija *firewall*-a, jer treba da predstavlja prepreku između spoljnog sveta i unutrašnje mreže. Zbog toga mora se precizno odrediti lokacija i broj „zidova“.

Najčešće korišćen je sistem gde se između dva „zida“, unutrašnjeg i spoljašnjem nalaze serveri, odnosno servisi kojima je neophodno da budu javno dostupni. Ovaj sistem se zove skraćeno DMZ, odnosno *Demilitarized Zone*. Sistemi kojima najčešće treba ovakvo okruženje su korporativni *Web* sajtovi, DNS (*Domain Name System*), ili neki *e-mail* sistem (*Microsoft Exchange*). Eksterni „zid“ obezbeđuje kontrolu pristupa i zaštitu „Demilitarizovanoj zoni“, a takođe brine o potrebi servera u toj zoni da imaju pristup spoljnjem svetu. S obzirom na određenu zaštitnu ulogu koju spoljni *firewall* ima prema unutrašnjoj mreži, unutrašnji „zid“ ima nekoliko uloga:

- Unutrašnji „zid“ poseduje čvršće filtriranje saobraćaja, kako bi zaštitio servere i radne stanice koji čine mrežu

➤ Takođe štiti i od mogućih napada i iz same DMZ zone, a mogu poticati od crva, *rootkit*-a, botova ili nekog drugog malvera koji je prodro u zonu. U isto vreme, štiti DMZ zonu od napada iz unutrašnje mreže.

➤ Može postojati više unutrašnjih „zidova“ koji imaju za zadatak da štite određene delove mreže od drugih sistema unutar nje. Npr. *firewall* može da bude postavljen između servera i radnih stanica. Takođe je praksa pokazala da je najbolje odrediti drugi mrežni interfejs u odnosu na onaj koji se koristi u unutrašnjoj mreži.

5.10.1 Intrusion Detection i Intrusion Prevention Sistemi

Da bi se detektovali mnogi napadi potrebno je dubinsko skeniranje paketa, a što znači da se pored hedera skenira i telo poruke, sami aplikativni podaci. Pošto *gateway* skenira dubinski, ali samo određene aplikacije, potreban je uređaj koji skenira i heder poruke i telo. Kada takav uređaj primeti sumnjiv paket, ili čitav niz, on ih može sprečiti da nastave putanju ka svom odredištu unutar mreže. Takođe poseduje i opciju da propusti takve pakete, ali obavesti administratora o njihovom postojanju. Tada su podaci smešteni u karantin i tek uz odobrenje administratora se propuštaju u samu mrežu. Sistemi koji imaju ovakve mogućnosti, odnosno tragaju za potencijalno opasnim sadržajem, nazivaju se *Intrusion Detection* sistemi. Sistemi koji filtriraju sumnjiv sadržaj nazivaju se *Intrusion Prevention* sistemi. O ovim sistemima se obično priča kao IDS sistemima, s obzirom da oba imaju zajedničku tačku, a to je kako detektuju štetan saobraćaj.

IDS sistemi se mogu klasifikovati na osnovu načina detekcije u dve grupe:

➤ *Signature-Based*

Poseduju bazu sa potpisima mogućih napada. Svaki potpis predstavlja set pravila koji se odnose na aktivnosti upada. To može biti i jednostavna lista karakteristika vezanih za određeni paket: port izvora i destinacije paketa, tip protokola i specifičan string ili niz bitova u samom paketa koji ukazuju da je u pitanju problematičan paket. Ovaj sistem pregleda svaki paket, upoređuje ga sa potpisima u svojoj bazi, te ako paket ili niz paketa odgovara nekom od potpisa, IDS trigeruje alarm, koji može biti smešten u log ili poslat administratoru na dalju obradu.

➤ *Anomaly-Based*

Ovaj sistem se oslanja na princip anomalije. Ukoliko primeti neobično visok broj određenih vrsta paketa, tek onda pokreće dubinsko skeniranje i proveru tih paketa. Ovakvi sistemi imaju pozitivnu stranu što se ne oslanjaju na prethodna znanja i tako propuste neki maliciozni kod, a sa druge strane je izuzetno teško na takav način razlikovati normalan saobraćaj od potencijalno opasnog. Baš iz tih razloga *Signature-Based* sistemi imaju primat.

Koriste se za skeniranje velikog opsega napada, kao npr. mapiranje mreže, skeniranje portova, skeniranje TCP steka, crvi i virusi, napada na slabosti operativnih sistema, kao i napade na same aplikacije i njihove slabosti. U mreži može postojati samo jedan IDS ili više njih. Ukoliko ih je više, obično funkcionišu tako što postoji jedan centralni IDS kome svi ostali šalju podatke. On te podatke sortira, te na osnovu njih šalje neophodne alarme. Jako je bitno pravilno odrediti koliko i na kojim mestima će se implementirati IDS sistemi. Npr., ukoliko se firma odluči za samo jedan sistem i iza njega stavi sve servere i radne stanice, onda će kompletan saobraćaj biti usmeren kroz taj jedan sistem i svaki će se dubinski skenirati, te upoređivati sa hiljadama „potpisa“ za eventualno otkrivanje malicioznog koda. Ali, ukoliko se implementiraju npr. dva sistema, s tim što je jedan zadužen za DMZ zonu koja je zaštićena samo paketnim filtriranjem, a unutrašnja mreža kompletnim dubinskim skeniranjem, tada je sistem značajno olakšan i lakši za administriranje i praćenje paketa, pošto je svaki sistem zadužen za svoj deo mreže.

6. Maliciozan softver [3] [2]

Nije jednostavno zaštititi jednu veliku mrežu. Postoji toliko tačaka i sa jedne i sa druge strane zaštitnog zida koje, ukoliko ostanu nezaštićene, mogu napraviti pravu pošast unutar mreže i koštati kompaniju veliku količinu novca.

Kompjuterski virus jeste program koji može samostalno da se umnožava i širi sa jednog računara na drugi. Barem tako kaže definicija. Ali istina nije tako jednostavna. Postoji ogroman broj raznih softverskih proizvoda koji mogu načiniti štetu. Generalno, maliciozni softver (*malicious software*) se može podeliti u dve kategorije:

01. Oni kojima su potrebni softveri domaćini

02. Oni koji su nezavisni

Maliciozni softveri koji ne mogu funkcionisati samostalno su paraziti, odnosno delovi programa koji ne mogu funkcionisati samostalno bez nekog programa kao domaćina, ili dela sistema. Najbolji primeri su virusi, logističke bombe (*logic bombs*) i *backdoors*. Samostalan je onaj koji sadrži kompletan program, podešen da se trigeriju u određenom momentu ili po izvršenoj nekoj operaciji. Primer ove vrste malvera su crvi (*worms*) i *bot* programi.

6.1 Kratka istorija računarskih virusa [5] [6]

Kao začetak ideje kompjuterskih virusa smatra se ideja naučnika Džona von Neumana (*John von Neumann*), a koja teorija se odnosila na pojam softvera koji se samostalno replicira.

1969 godine, AT&T Bell Laboratories predstavljaju svoj prvi *multi-tasking* operativni sistem. Iste godine započinje sa radom i ARPANET, koji razvija *Advanced Research Projects Agency*. To predstavlja sam početak Interneta. Od tog perioda započinje razvoj, a kasnije i ekspanzija raznih vrsta štetnih softvera. Deset godina kasnije inženjeri iz *Xerox Palo Alto* centra za istraživanje načinili su veliko otkriće pronalaskom kompjuterskog crva (*computer worm*). Ova preteča modernog kompjuterskog crva imao je za zadatak da pronalazi procesore koji miruju unutar mreže. 1983 godine pojavljuje se termin „kompjuterski virus“, kako bi se opisao program koji utiče na druge kompjuterske programe, tako što ih menja i tera ih da se kao takvi umnožavaju i dalje šire.

Godina prvog zvaničnog kompjuterskog virusa je 1986, kada se pojavljuje „*The Brain*“, pušten iz Pakistana. Dve godine kasnije pokrenut je prvi veliki napad na ARPANET mrežu. *Robert Morris* napravio je mali virus koji je zahvatio gotovo 6.000 računara na mreži i poplavio ih sa svojim kopijama. Ali prvi antivirusni softveri se pojavljuju 1991 godine, kada kompanije *Symantec* razvija svoj prvi softver za zaštitu računara od malicioznih kodova.

Značajan napad hakera odigrao se 1998 godine, kada je preko 500 računara koji su pripadali vojsci i vladi bilo napadnuto. Iako se u prvi mah sumnjalo da je napad

došao iz Iraka, ispostavilo se da su za napad bila odgovorna dva tinejdžera iz Kalifornije. Ovaj napad je pokazao kako simultani napadi mogu doneti mnogo više štete.

Jedan od najznačajnijih i razornijih virusa jeste „*Melissa*“, koji se pojavio 1999 godine. Pretpostavlja se da je bilo zaraženo više miliona računara u samo prvom danu po pojavljivanju. Cilj je da na inficiranom računaru pronađe i autoru virusa pošalje kombinacije korisničkih imena i lozinki. Međutim, novo polje u pisanju malicioznog softvera otvara virus pod imenom „*Anna Kournikova*“, s obzirom da je pisan pomoću *toolkit*-a, a koji omogućava i neiskusnom programeru da stvori svoj virus.

Jedan od najsofisticiranijih virusa koje se pojavio u novijoj istoriji jeste „*Red Code*“, koji je ozbiljno zapretio oficijalnoj *web* stranici Bele kuće. Godine 2001 kada se pojavio inficirao je desetine hiljada računara, i pri tom napravio štetu od 2 milijarde dolara. Napravljen je tako da svi inficirani računari u određeno vreme napadnu sajte Bele kuće. Međutim, napad je zaustavljen na vreme. Takođe te godine pojavljuje se „*Nimda*“ virus, podjednako opasan kao i „*Red Code*“.

Naredne godine donose dva značajna virusa. Prvi je „*Slammer*“, koji je zarazio stotine hiljada računara za manje od tri sata. Prouzrokovao je čak i kašnjenje aviona širom sveta. Drugi je „*MyDoom*“ (ili „*Novarg*“) *e-mail* virus, koji u istoriji virusa spada u jednog od najbržih na svetu, međutim, bez mnogo nanete štete. Radio je tako što je navodio korisnika da otvori datoteku u prilogu u kojem se nalazi virus koji zaražava računar i omogućava hakerima da pristupe *HDD*-u zaraženog računara. Prvobitan cilj ovog malicioznog softvera je bila firma *SCO Group*, zato što je pokrenula nekoliko sudskih procesa protiv nekoliko grupa koje su koristile *open-source* programskog jezika *Unix*.

Sredinom 2004 godine oko milion računara koji koriste *Microsoft Windows* operativne sisteme je zaraženo „*Sasser*“ virusom koji se širio velikom brzinom. Napadom su bili pogođene uspešne firme kao što je „*British Airways*“ i državne strukture (Britanska obalska garda). Razlika u odnosu na druge viruse jeste u tome što korisnik nije morao da otvori dodatak u *e-mail*-u da bi se mašina zarazila, već je virus pronalazio i iskorišćavao određene sigurnosne propuste. Nije nanosio nepopravljivu štetu računaru ili podacima, ali ga je znatno usporavao, a neki su se konstantno

resetovali. „Zasluge“ za ovaj virus pripadaju 18-ogodišnjem Nemcu, kome se pripisuje puštanje u promet još jednog virusa.

Četiri godine kasnije pojavljuje se virus pod imenom „*Conficker*“, koji se smatra jednim od najvećih virusa u kratkoj istoriji malicioznih softvera. Procenjeno je da je ovaj

virus zarazio između 9 i 15 miliona servera širom sveta, uključujući i mornaricu Francuske, Ministarstvo odbrane Britanije i policiju Norveške. Posle njegovog prvog izdanja pojavilo se još pet verzija ovog virusa. Stručnjaci ne mogu da se usaglasе da li te verzije predstavljaju modifikovani originalni virus ili pak pokušaj da se virus „ubije“. Ono što je sigurno jeste da je ovaj virus pisan ciljano i da nikada nećemo saznati tačno ko je sve i koliko oštećen.

Pojavom „*Stuxnet*“ virusa prvi put se pojavio virus ciljano pravljen da korumpira industrijsku opremu. Napravljen je da traži *Siemens*-ove softvere namenjene industriji, a sve kroz propuste *Microsoft Windows* operativnih sistema. Prvi put je korišćena i *PCL (Programmable Logic Controller)* koji služi za prikrivanje samo postojanje virusa, kao i njegov razvoj i napredovanje. Par meseci kasnije firma *Symantec* je objavila podatak da je 60% zaraženih mašina ovim virusom iz Irana. Iako je *Siemens* kasnije objavio kako nije bilo oštećenja kod korisnika njegovih proizvoda, to međutim nije tačno. Država Iran je koristila *Siemens*-ovu opremu za svoj nuklearni program. Kompanija *Kaspersky Lab* objavljuje i da je ovaj virus toliko napredan da nije moguće ostvariti ovakve napade bez podrške struktura na vlasti, jer jedino jedna država može da ima neophodne resurse. Renomirane novine „*The New York Times*“ 01.06.2012 godine je objavio članak u kome se tvrdilo da je u proizvodnji i distribuciji „*Stuxnet*“ virusa učestovale tajne službe Sjedinjenih država i Izraela, a pod nazivom „*Operation Olympic Games*“.

Ova godina nam donosi *OpenSSL* „*Heartbleed*“ koji je uzburkao IT javnost. Eksploatiše propuste u *open-source* kriptobiblioteci, *OpenSSL*, a što omogućava napadaču da izlista sadržaj memorije na serveru ili klijentu. Na taj način može doći do SSL privatnog ključa. Veliki problem predstavlja činjenica da ovaj virus nije otkriven pošto se pojavio, čak su istraživanja utvrdila da je ovaj propust postojao od marta 2012 godine. Iako je u aprilu ove godine izašla nova verzija *OpenSSL*-a, takođe je imala isti propust, koji je dozvoljavao oslobađanje i do 64 kilobita iz memorije po jednom

heartbeat-u. Radi tako što šalje nepravilan *heartbeat* serveru kako bi inicirao odgovor memorije servera. Pošto ne postoji provera, *OpenSSL* neće proveriti da li je *heartbeat* ispravan ili ne.

Kako brzo napreduje razvoj malvera pokazuje statistika da se pojavljivao:

01. 1994 godine jedan virus svakih sat vremena
02. 2006 godine jedan virus svaki minut
03. 2012 godine jedan virus svake sekunde
04. 2014 godine *Kaspersky Lab* je objavio informaciju da se dnevno obrađuje 300.000 semplova

6.2 Vrste malicioznog softvera

Iako je za maliciozne softvere u širokoj upotrebi naziv „virusi“, to nije posve tačno. U grupu malicioznih softvera spadaju i crvi (*worms*), Trojanci, *logic bombs*, *backdoor*, *downloaders* itd.

Najznačajniji predstavnici biće obrađeni u ovom radu.

6.2.1 Virusi

Kompjuterski virusi su programi koji imaju posebne funkcionalnosti i tendenciju da se samostalno kopiraju i šire na druge računare, a sve bez znanja korisnika računara.

Ova definicija nije potpuno tačna. U današnje vreme virusi se sastoje od setova kodiranih instrukcija, koje su dizajnirane tako da se prikače na objekat koji je sposoban da bude nosilac tih kodova, kako bi se aktivirali bez znanja korisnika. Taj objekat može biti *e-mail*, program, dokument, DVD, pa čak i obična SMS tekstualna poruka, kao i svaki medijum koji je sposoban da prenosi podatke.

Da bi postali aktivni, virusima je potrebno aktiviranje bilo njegovog *host*-a, bilo njega samog od strane korisnika ili neke programirane situacije (određen datum i vreme i sl.) kako bi započeo svoj zadatak. Ukoliko je potrebna akcija od strane korisnika, to je obično neka uobičajena za korisnika radnja, te tako korisnik nije ni svestan da je upravo tog momenta započeo „infekciju“ svog računara.

Ono što definiše neki maliciozni softver kao virus jeste njegova potreba da se razmnožava. U nekim slučajevima, kada je virus dizajniran da npr. obriše sve podatke sa računara, obično se ograničava mogućnost širenja, jer virus koristi resurse operativnog sistema na kojem se nalazi.

6.2.1.1 Tipovi Virusa

Postoji veliki broj virusa, te će se ovaj rad baviti samo najznačajnijim vrstama.

01. *File infectors*

Njegova uloga jeste da zarazi objekat, odnosno fajl. U ovu grupu spadaju i virusi koji su dizajnirani da zaraze operativne sisteme.

02. *Boot-Sector infectors*

Cilj ovog virusa jeste da se „prilepi“ ili zameni *master boot record*, *system boot record* ili druge rekorde, povezane sa podizanjem (*boot*-ovanjem) operativnog sistema. Pošto prvi blok na fizičkom disku sadrži značajne informacije, potrebne operativnom sistemu da se uspešno podigne, *boot-sector infector* nastoji da izmesti te podatke u drugi neupotrebljeni sektor, a sebe prekopira u fizički prvi sektor. Primeri ovakvih vrsta su *Brain*, *Stoned* i *Michelangelo*.

03. *System infectors*

Ovaj termin se obično koristi za viruse čije je isključiva namena inficiranje operativnih sistema ili *boot* sektora, tako da se virus startuje prilikom podizanja sistema i koji tako preuzima kontrolu nad njim ili nekim njegovim funkcijama. Druga vrsta koja potpada pod ovaj termin su virusi koji menjaju druge strukture sistema (npr *registry*), kako bi bili prvi pokrenuti na računaru koji im je domaćin.

04. *E-Mail virus*

Kao što mu i ime kaže, ovi virusi koriste *e-mail* sistem da bi se širio, te je stoga takav virus svestan funkcionalnosti ovakvih sistema. Obično ciljaju određeni *e-mail* sistem, kupe adrese iz različitih izvora i mogu kopirati se na svaki poslati *e-mail* ili mogu generisati *e-mail* poruke koje sadrže kopiju virusa kao dodatak (*attachment*). Sofisticiranije verzije mogu skenirati mrežni saobraćaj i pridodati se legitimnoj poruci koja kroz tu mrežu putuje. Često se može sresti ocena da ovakav maliciozni softver pripada grupaciji *worms*, jer često im nije potreban program na ciljanom računaru kao *host*. Ovi virusi su svojom pojavom načinili krupan zaokret u dotadašnjem načinu širenja zaraze. Do tada, virusima su bili potrebni meseci da bi se proširili, ali su takođe i dugo vremena ostajali na sistemima. Dok pojavom *e-mail* virusa došla je i mogućnost širenja širom sveta i to u toku nekoliko sati.

05. *Multipartite*

Ovaj izraz je korišćen za viruse koji mogu da zaraze i programske fajlove i *boot sector*. Sada se koristi za one viruse koji imaju sposobnost da zaraze više od jednog tipa objekta ili koji može da se reprodukuje na više načina.

06. *Macro Virus*

Makro virus koristi delove aplikacija koji se oslanjaju na makroe, kao što je npr. *Microsoft Word* aplikacija. On pokušava da zarazi fajlove i ostane u aplikaciji tako što pokušava da inficira konfiguracioni template (*Normal.dot*). Pošto se oslanja na aplikaciju, česta je pojava da ovaj virus može napasti i *Windows* i *Macintosh* operative sisteme.

6.2.1.2 Struktura virusa

Kod analize kompjuterskih virusa treba obratiti pažnju na tri komponente:

01. Mehanizam infekcije ili replikacije
02. Okidač
03. Rezultat

Jedini deo strukture koji je zaista neophodan jeste mehanizam infekcije. Ovaj kod omogućava virusu da se reprodukuje i sastoji se od nekoliko funkcija.

Prva funkcija je da je sposoban da traži objekat koji može da zarazi. Pretraživanje može biti aktivno, ili pasivno, kao što je to slučaj sa *macro* virusima. Druga funkcija je sama infekcija. Ovo podrazumeva upisivanje potpuno nove sekcije koda u *boot* sektor, dodavanje koda ciljanoj aplikaciji, dodavanje *macro* koda u *Microsoft Word Normal.dot* fajl, slanje dodatka (*attachment*) na određene *e-mail* adrese, kao i mnoge druge operacije. Funkcija sadrži i neke pod funkcije, kao što su prebacivanje osnovnog *boot* sektora na novu lokaciju ili dodavanje *jump* koda u ciljanu aplikaciju, a koji kod vrši usmeravanje ka virusnom kodu. Može biti promena u sistemskim fajlovima, da bi osigurao svoje pokretanje svaki put kada se uključi računar. Takođe, svaki virus poseduje i niz koraka koji će se uslediti posle njegovog aktiviranja, kako ne bi bio detektovan.

Okidač predstavlja drugu veoma važnu komponentu virusa. To može biti određeni datum, vreme, operacija, broj infekcija i slično.

I na kraju rezultat je razlog zašto jedan virus i postoji. To može biti bilo šta. Od obične poruke koja se konstantno pojavljuje i ne nanosi nikakvu drugu štetu računaru, do formatiranja čitavog diska i brisanja svih podataka na njemu ili otuđenje tuđe svojine (novac, informacije itd).

6.2.2 Worms (Crvi)

Crvi predstavljaju ogromnu pretnju mrežama. Podjednako mogu biti razorni kao i drugi maliciozni kodovi, ali najveću pretnju predstavlja mogućnost crva da se „razmnožava“ bez intervencije korisnika.

Jedan od najpoznatijih pojavio se 2001 godine pod nazivom „*Code Red*“, o kome je već bilo reči. Ovaj crv je iskorišćavao propust u *Microsoft IIS-u* (*Internet Information Server*), i imao je tri nivoa aktivnosti. Prvi nivo predstavljalo je nasumično prikupljanje IP adresa i testiranje da li ove mašine na sebi imaju *IIS*, te da li imaju slabosti koje je moguće iskoristiti. Drugi nivo činila je promena normalnog teksta na lokalnom *web* serveru sa tekstem „*Welcome to http://www.worm.com! Hacked By Chinese !*“, a treći nivo je postavljao logičku bombu (*logic bomb*) koja je imala za

zadatak da pokrene *Denial of Service (DoS)* napad prema adresi 198.137.240.91, koja je u to vreme pripadala *web* serveru na kojem se nalazila stranica Bele kuće. Međutim, Bela kuća je na vreme saznala za ovaj potencijalni napad, te je rešenje pronađeno u promeni adrese sajta.

Kao što je ranije navedeno, crvi mogu da se samo-repliciraju, kao i da šalju te kopije na druge računare širom mreže. Na novom računaru crv će nastaviti tu aktivnost, kao i aktivnosti za koje je napravljen. Da bi se replicirao, crv koristi nekoliko metoda:

01. Elektronska pošta – crv šalje svoju kopiju ka drugom sistemu, te će se isti kod aktivirati kada se elektronska poruka primi ili pročita, ili pokrene prilog u toj pošti.

02. Mogućnost daljinskog izvršenja – crv pokreće i izvršava svoju kopiju na drugom sistemu, bilo direktnom naredbom, bilo eksploatacijom propusta u nekom određenom softveru ili operativnom sistemu.

03. Mogućnost udaljenost logovanja – crv se može ulogovati kao korisnik i tada, koristeći određeni niz komandi, kopira sebe sa jednog sistema na drugi, gde se izvršava.

6.2.3 Logic bombs

Logičke bombe jesu najstariji tip malicioznog koda, koji se ubacuje u neki legalan softver, a koje su podešene da se aktiviraju kada se ispune neki zadati uslovi, npr. određeni dan u godini ili pokretanje određene aplikacije od strane korisnika. Jednom kada se pokrene logička bomba može da promeni ili izbriše podatke, može izazvati zastoj u radu mašine i slične probleme.

6.2.4 Trojan Horses

Ovaj maliciozni kod dobio je ime po Trojanskom konju iz Grčke mitologije i to je program ili komandna procedura koje izgleda legitimno, ali sadrži sakriven kod koji, kada se aktivira, izvršava neželjene ili štetne funkcije. Trojanski konj se najčešće koristi kako bi se indirektno trigerovale funkcionalnosti koje inače neautorizovani korisnik ne može da uradi direktno.

Mogu se koristiti za neovlašćeni pristup podacima, te i za samo uništavanje podataka. Trojanski konj se može podeliti u tri najčešća oblika:

01. Nastavlja da izvršava originalnu funkciju programa, kao i sakrivenu funkciju koju aktivira maliciozni kod
02. Nastavlja da izvršava originalnu funkciju programa, ali modifikovanu (npr. prikupljanje lozinki)
03. Izvršava malicioznu funkciju koja u potpunosti menja originalni program.

6.2.5 Mobile code

Pod pojmom *Mobile code* svrstavaju se programi koji se mogu biti aktivirani na raznim vrstama platformi. Ovi maliciozni kodovi se transmituju sa udaljenog sistema na lokalni, gde se izvršava bez eksplicitne naredbe od strane korisnika. Obično predstavlja platformu za transport neke druge vrste malicioznog koda, ili eksploatiše propuste, kao što su neautorizovan pristup korporativnim podacima. *Mobile code* najčešće se koristi u kombinaciji sa *Java*, *ActiveX*, *Java* i *WBScript*.

6.2.6 Spyware [7]

Spyware predstavlja softver koji služi neautorizovanom licu kako bi prikupio informacije o licima ili organizacijama, a bez njihovog znanja i pristanka.

Najčešće se klasifikuju u četiri tipa:

01. *System monitors*
02. *Trojanci*
03. *Adware*
04. *Tracking cookie*

Najčešće se koristi za praćenje korisnika na internetu, kako bi se sakupile informacije o njegovom kretanju i navikama, da bi korisnik dobijao reklame (*pop-up*

ads) u skladu sa njegovim interesovanjima. Ukoliko se iskoristi u maliciozne svrhe, obično je sakriven od korisnika i teško ga je otkriti. Jedan od primera jeste *Keylogger*, tip malicioznog koda, koji, kada se instaliran na sistem, sakuplja sve otkucane znakove na tom računaru, pa se na taj način može doći do svih kombinacija korisničkog imena i lozinke za korisnike koji taj računar upotrebljavaju. Može otežavati rad na računaru, kao i da menja osnovne postavke računara ili *Web* pretraživača.

Ova vrsta malicioznog koda se ne širi kroz mrežu na isti način kao npr. virus ili crv, jer u osnovi ne pokušava da se prebaci na udaljeni sistem, već *spyware* se instalira, može se reći i prevarom, od strane korisnika ili iskorišćenjem nekog propusta u samom sistemu. Neke verzije dolaze već upakovane u željeni softver.

6.2.7 Rootkit [8]

Ovaj softver je dizajniran da sakrije postojanje određenih procesa ili programa od klasičnih metoda detekcije, a sa ciljem da omogući kontinuiran pristup računaru. Instalacija može biti automatska ili može biti instaliran od strane napadača kada pribavi pristupne privilegije. Cilj je upravo taj administratorski prilaz, kako bi napadač bio u mogućnosti da menja, briše i upisuje podatke na računar. To se posebno odnosi na antivirusni softver koji može pronaći ovu pretnju, pa sama činjenica da napadač ima administratorski pristup sistemu znači da taj softver može isključiti ili ga promeniti na takav način da ne vidi kao pretnju pomenuti maliciozni softver.

Pošto ga je izuzetno teško otkriti, potrebna je temeljna analiza zaraženog operativnog sistema: skeniranje raznim alatima, metodama koji se odnose na analizu ponašanja operativnog sistema i/ili *memory dump* analizu. Često jedino rešenje ovog problema jeste reinstalacija operativnog sistema ukoliko se *rootkit* „zavuč“ u *Kernel*. Postoje i verzije *rootkit*-a nazvane *firmware*, čije odstranjivanje često zahteva čak i promenu računarske opreme.

Postoji pet vrsta *rootkit*-a:

01. *User mode*
02. *Kernel mode*
03. *Bootkits*

04. *Hypervisor level*

05. *Firmware and Hardware*

Ne postoji precizan način zaštite od ovih napada, ali svakako se mogu otežati napadi tako što će se redovno primenjivati sigurnosne zakrpe, kontrola privilegija korisnika, kao i jaka antivirusna zaštita.

6.2.8 Mobile malware

Široko je rasprostranjeno mišljenje da ne postoje virusi pravljeni specifično za *Androdi*, *Windows* i *IOS* platforme, a što je apsolutno pogrešno. Na ove operative sisteme treba gledati kao na operative sisteme koji se koriste na računarima. U razmaku od 2004 do 2010 godine pojavilo se 1.160 malvera za mobilne uređaje, a samo u 2011 godini 6.193 vrste, od toga u decembru te godine čak 2.137. Sledeća godina donosi otkrivenih 46.000 malvera namenjenih mobilnim uređajima. Za sada je rekorder 2013 godina sa otkrivenih 143.211 novih vrsta malvera (statistika vlasništvo *Kaspersky Lab*)

6.3 Druge vrste pretnji

Za prosečnog korisnika napadi i zaštita počinju i završavaju se unutar operativnog sistema računara kojeg koristi. Ali za velike korporacije to je samo deo problema zaštite celog sistema.

Kako bi zaštitile svoje mreže, firme koriste razne vrste zaštite, softverske i hardverske. Međutim, ni to nekad nije dovoljno.

6.3.1 Honey pots

Firme koje ozbiljno razmišljaju o svojoj zaštiti koriste i ovu tehniku. U suštini, to je sistem koji je dizajniran tako da navuče napadače da pokušaju da probiju zaštitu baš na tom mestu, kako bi se skupili podaci o napadačima, tehnike i alati koje koriste,

ali i informacije o najnovijim virusima, crvima i drugom malveru. Mogu se postavljati iz dva razloga, kao zaštita od napada ili za skupljanje podataka.

U *security* svetu ova tehnika je poznata kao „zamka“. Njena svrha je da detektuje, odbije napadača, ali nekad i da se uspostavi konekcija sa napadačima, odnosno skuplja informacije o njima, načinu rada, alatima koje koriste, novim tehnikama napada i kodovima koji se koriste. To je najčešće strogo kontrolisana grupa računara koji služe kao zamka, često predstavljeni i kao slaba tačka i kao mesto gde se nalaze neki značajni podaci. Takođe, pomažu u ranom otkrivanju novih napada.

S obzirom da se ovi računari koriste da privuku napadače, od izuzetne je važnosti da se organizuju tako da ne postoji nikakva interakcija sa značajnim sadržajem na mreži. Primarnu rolu određuje način na koji je zamka postavljena. Klasifikacija se zasniva na količini interakcije koja se ostvaruje sa napadačem. Postoje dve kategorije: sa niskom i visokom nivou komunikacije. Takođe postoji kategorizacija i da li su okrenuti ka produkciji ili ka istraživanju.

Kako bi privukao napadače, *Honey pots* bi trebalo postaviti do *firewall*-a ili *bridge*-a, te je potrebno u njega staviti servere koji su po bilo kojoj osnovi ranjivi. U praksi se najčešće koriste stariji operativni sistemi raznih vrsta i sa različitim propustima. Takođe se u praksi primenjuje i arhitektura pod imenom *Honey Nets*. To je jednostavan dizajn mreže koji se sastoji više od jednog *honey pot*-a. S obzirom da mreže ne predstavljaju produkciono okruženje, svaki kontakt sa njima predstavlja ponašanje koje se može klasifikovati kao maliciozno. Često se ovi mamci postavljaju među produkcijske servere, kako bi što vernije izgledali pred napadačima. Kako bi dobro obavili svoj posao mamci, *honey pots* moraju se postaviti tako kao da se pretpostavlja da će napadač prvo krenuti ka lakšim ciljevima. To predstavlja *Low interaction*, s obzirom na specifičnu funkciju.

Postoje tri glavna pitanja u vezi legalnosti ovakvog načina sakupljanja podataka:

01. Klopka

Po definiciji, klopka može predstavljati prevaru da se natera neko da učini nešto što normalno ne bi. Međutim, *Honey Pots* ne vara nikog da čini dela protivna zakonu,

jer kada napadač otkrije propust u nekoj mreži, on eksploataciju tog propusta čini po sopstvenoj volji i na sopstvenu odgovornost. Napadač je u samom startu učinio protiv zakonito delo dok je tražio slabe tačke sistema kako bi ih eksploatisao.

02. Privatnost

Zakoni u pojedinim zemljama mogu limitirati pravo da se prikupe podaci o napadaču, iako taj napadač „upada“ u *Honey Pot* unutar okruženja koje je tuđe vlasništvo. Međutim, zakoni, pogotovo u SAD, nisu u potpunosti precizni kada je u pitanju privatnost i ova vrsta zamke za napadače.

03. Odgovornost

U ovom slučaju, kada se kaže odgovornost, misli se na mogućnost tužbe ukoliko se *Honey Pot* upotrebi kako bi se nekom naštetilo, npr. ukoliko se prikupljeni podaci iskoriste kako bi se oštetilo treće lice

Većina profesionalaca širom sveta se slaže u oceni da ovaj način borbe protiv napadač ne treba da predstavlja legalno pitanje. Bar ne toliko komplikovano kakvo je sada. Ono što je sigurno jeste, da mreža koja se odluči i za ovakav način obračuna sa napadačima, to treba da učini izuzetno precizno kako ne bi ugrozili produkcijske servere i kompanijske podatke, pa je stoga potrebna edukacija, kako o samom sistemu, tako i o legalnim pitanjima.

6.3.2 Social engineering [9]

Kada se kaže socijalni inženjering u kontekstu bezbednosti, misli se na manipulaciju ljudima koji rade u određenim firmama, zanimljivim napadačima. Njima se manipuliše kako bi bez svoje volje odali neke poverljive informacije.

Postoje razne tehnike koje se najčešće koriste:

01. *Pretexting*

Ovo je tehnika gde se smišlja određeni scenario kako bi žrtva socijalnog inženjeringa bila u situaciji koja bi olakšala odavanje određenih informacija, a koje ne bi otkrio u svakodnevnim situacijama. Najbolji primer jeste zakonska odredba koja zabranjuje radnicima pušenje unutar svojih kancelarijama, te su radnici obavezni da svoj porok upražnjavaju obično ispred zgrada u kojima rade. Tada sreću druge radnike, pa je napadaču lako da se infiltrira i započne priču sa radnicima. Pošto će se vraćati svakog dana, napadač će vremenom biti prepoznat kao jedan od njih, te je vrlo moguće za domišljatog govornika da izvuče informacije koje su mu potrebne.

02. *Phishing*

Phishing je tehnika koja se koristi kada je potrebno priviti privatne informacije. Npr, napadač šalje *e-mail* sadržine koja bi mogla da odgovara legalnom pismu nekog biznisa poznatog žrtvi napada. U tom slučaju, u *e-mail*-u postoji link, često čak i ka *web* stranici koja može izgledati kao legitimna stranica nekog biznisa. Često se traži broj kreditne kartice, adresa kuće ili radnog mesta, dakle sve što bi napadaču moglo da pomogne kako bi izvukao ciljane informacije. Sa ovom tehnikom je povezan i *phone phishing*. Često ova tehnika je povezana sa *phishing* tehnikom. Žrtva se poziva telefonom, pozivalac se ne retko poziva na *e-mail* koji je prethodno poslat.

03. *Baiting*

Ova tehnika je posebno zanimljiva, jer se oslanja na radoznalost, pa čak i pohlepu žrtve. Napadač snima određeni sadržaj na *USB flash* ili *DVD*, ostavi ga na lokaciji na kojoj će lako biti pronađen, npr. kupatilo, lift i slično, i sve što je potrebno jeste da sačeka da žrtva upotrebi uređaj. Ukoliko mašina nema AV ili neku drugu zaštitu, a uključena je opcija *autorun*, to je siguran način da napadač dođe do željenih informacija.

04. *Quid pro quo*

Ova tehnika je vrlo prosta. Napadač poziva nasumično brojeve telefona određene firme predstavljajući se kao radnik tehničke službe, sve dok ne naiđe na radnika te firme koji zaista ima neki legitiman problem. Radnik, zahvalan što će mu neko otkloniti problem, otkriva sve relevantne podatke napadaču, pri tom dajući mu i mogućnost implementacije nekog alata koji mu pomaže u prikupljanju podataka.

05. *Tailgating*

Ukoliko je napadaču potreban pristup zaštićenoj eriji unutar firme, može jednostavno da prati radnika koji ima pristup ovom delu. Računajući na kulturu ljudi, napadač će sačekati da mu radnik pridrži vrata kako bi ušao zajedno sa njim. Kolegijalno neće upitati napadača koji se predstavlja kao kolega, zašto ne poseduje digitalnu legitimaciju koja mu dozvoljava ulazak u zaštićen deo, ili će prihvatiti objašnjenje da je istu zaboravio, jer svi smo jednom u karijeri koristili slične izgovore.

6.3.2.1 Način zaštite

- Neophodno je obučiti radnike koji rade sa poverljivim podacima na koji način moraju da se odnose prema istima
- Obuka radnika kako bi prepoznali socijalni inženjering
- Postavljanje sigurnosnih protokola, polisa i procedura prilikom korišćenja osetljivih informacija

7. **Metode napada**

Kao što je ranije objašnjeno, napadač želi da ostvari nedozvoljenu kontrolu ili pristup kako bi ostvario pristup podacima, kako bi ih menjao, uništavao ili prisvajao. Načini na koji napadač to čini su različiti. Iako postoje jednostavni napadi, gde je napadaču dovoljna samo *IP* adresa i poznavanje osnovnih hakerskih tulova i skripti, ali i kompleksni, gde je napadaču potrebno široko znanje iz oblasti operativnih sistema, tehnika programiranja, zaštite samog *OS*-a i okruženja, ipak se ti napadi mogu svrstati u nekoliko grupa:

7.1 *Brute Force and Dictionary*

Često se ove dve vrste napada svrstavaju u jednu grupu, jer se odnose na kompromitovanje istog entiteta, a to je lozinka. *Brute Force Attacks* imaju za cilj otkrivanje korisničke lozinke na taj način što se isprobavaju sve moguće kombinacije slova, brojeva i simbola. Povećanjem brzina računara uz određeni vremenski period mogu se bez problema otkriti i kompleksne lozinke. Međutim, što veća dužina lozinke,

kompleksnija kombinacija slova, brojeva i znakova, odnosno u lozinki ne postoje prepoznatljivi šabloni, to je duži vremenski period potreban napadaču da lozinku i otkrije. Jedno je sigurno, ukoliko nije ograničen vremenom, napadač pomoću ove vrste napada može otkriti bilo koju lozinku.

Dictionary attack je pokušaj otkrivanja lozinke korišćenjem svih lozinki sa predefinisanih listi poznatih ili očekivanih lozinki. Iako ovaj način može zvučati čak i laički, on se zasniva na poznavanju ljudske prirode, jer čovek je sklon korišćenju poznatih imena, datuma rođenja i slično prilikom odabira lozinke.

Zaštita od *brute force* i *dictionary* napada zahteva stroga pravila, odnosno strogu sigurnosnu politiku. Najosnovnije, fizički pristup mreži mora biti kontrolisan. Zatim, potreban je strog nadzor i servera koji je zadužen za autentifikaciju, odnosno, pojedinačno treba odobravati pristup ovom serveru. Ukoliko se otkrije sumljiv pristup ovom serveru treba odmah izvršiti proveru. Ukoliko se ne može utvrditi da je pristup izvršilo lice kome je to dozvoljeno treba podrazumevati da su sve lozinke kompromitovane. Treba forsirati politiku jake lozinke. Što je lozinka duža i kompleksnije duže će vremena trebati da se ona otkrije, a ukoliko je postoji i vremensko ograničenje, a što je poželjno, onda napadač često neće ni postići da u određenom vremenskom periodu otkrije lozinku. Po istraživanjima, lozinka stara više od 30 dana može se smatrati kompromitovanom. Nikad se ne bi trebalo oslanjati samo na jednu vrstu autentifikacije. Trebalo bi da postoji barem barem dva načina prilikom prilaska mreži, jer su lozinke veoma slab mehanizam zaštite ukoliko se samo one koriste. Tada predstavljaju samo trenutnu prepreku za napadače.

7.2 Denial of Service

Po jednoj od definicija, *DoS* napadi su oni koji sprečavaju sistem da procesira ili odgovori na saobraćaj koji zaista potiče iz mreže kojoj mašina pripada. Najčešće je to prenos velikog broja paketa ka serveru koji ne može da ih sve i procesira, te na taj način se sprečava obrada legitiman saobraćaj. To se naziva *flooding*. Takođe, napad može imati fokus na eksploataciji poznatih propusta ili slabih tačaka operativnog sistema, servisa ili neke od aplikacije. Ovaj oblik često dovodi do pada sistema ili zauzeća procesorskog vremena od 100%. Pored toga *DoS* može prouzrokovati i

konstatno resetovanje sistema, korupciju podataka, a može i da sprečava pokretanje određenih servisa.

Postoji nekoliko vrsta ove vrste napada. Prva koja se pojavila bila je pojedinačno plavljenje hosta nizom paketa. Ovakvu vrstu je lako zaustaviti jednostavnom blokadom dolazećeg saobraćaja sa izvorišne IP adrese. Sledeća vrsta jeste *Distributed Denial of Service (DDoS)*. Napadač kompromituje nekih nekoliko sistema koje koristi za dalje napade. Kompromitovani sistemi se najčešće nazivaju *slaves* ili *zombies*. Rezultat su napadi na jednog hosta sa više izvora. *DDoS* se može zaustaviti blokiranjem kompromitovanih sistema, a što može izazvati dosta problema. Samom blokadom kompromitovanih sistema se blokira i legitiman saobraćaj, jer su ovi izvori i sami žrtve napada, a ne originalni izvori zaraze. Ovaj tip se može nazvati i distributivnim zbog velikog broja sistema koji učestvuju.

Zadnje otkrivena vrsta napada nosi naziv *Distributed Reflective Denial of Service (DRDoS)*, a koja koristi normalne mehanizme za rad svake mreže, kao što je DNS ili *router update* protokoli. Funkcioniše tako što šalje veliki broj *update* ili kontrolnih paketa, kao i paketa sesija, ka raznovrsnim Internet servisnim serverima ili ruterima na kojima se javlja adresa žrtve koja se cilja. Obično su ti serveri ili ruteri deo *backbone*-a. Rezultat je poplava (*flood*) *update* paketa, potrdnih odgovora za započinjanje sesija ili grešaka koje vraća žrtva ovog napada. Širina ovakvog napada može biti tolika da obuhvati čak i sisteme koji se nalaze iznad gađanih resursa, samo zbog ogromne količine saobraćaja koji se u tim trenucima odvija. Ovakva vrsta napada naziva se *reflective* napad, jer visokopropusni *backbone* sistemi reflektuju napad ka ciljanoj žrtvi. Ovakve napade je gotovo nemoguće zaustaviti, jer počiva na legitimnom saobraćaju. Ukoliko bi se sprečio priliv paketa iz ovih najznačajnijih izvora na Internetu, žrtva (korisnik) bi bio uskraćen za veliki deo Interneta.

Sledeći u nizu su *SYN flood* napadi. Oni razbijaju standardni *TCP/IP handshake (three-way)* koji se koristi prilikom inicijacije sesije. Na početku razmene informacija klijent šalje *SYN* paket ka serveru koji odgovara sa odgovarajućim *SYN/ACK* povratnim paketom. Po prijemu ovog paketa, klijent odgovara sa *ACK* paketom, koji šalje nazad ka serveru. Po završetku ove razmene uspostavlja se sesija koja se koristi za prenos podataka do momenta prekida sesije. *SYN flood* se događa kada je veliki broj *SYN*

paketa šalje ka serveru, ali pošiljalac tih paketa ne odgovori na serverske *SYN/ACK* pakete sa finalnim *ACK* paketima. Uz to, ti *SYN* paketi obično imaju lažne izvorišne adrese, tako da *SYN/ACK* odgovor je poslat negde drugde, a ne i originalnom pošiljaocu paketa. Za to vreme server ceka odgovore od klijenta držeći sesije otvorene. Ovakav sever lako postaje preopterećen zbog tih otvorenih sesija, a što može izazvati pravilan prestanak rada servera. Prestanak rada može značiti od nemogućnosti odgovora na legitimne zahteve pa do pada sistema servera.

Teško je zaštititi se od ovakvih napada. Jedna od protivmera može biti povećanje broja mogućih konekcija na serveru. Međutim, to nije tako jednostavno, jer ova mora povlači i povećanje hardverskih resursa za taj server, kao što su memorija, brži procesor itd. Efikasniji način je smanjenje vremena odziva za krajnji *ACK* paket. Opet, ovaj način može onemogućiti ostvarenje konekcije za mašine koje se konektuju preko sporijih linija.

Sledeća vrsta u nizu jeste *Smurf* napad. Dešava se kada tzv. *amplifying* server ili mreža se iskoriste za poplavu nekorisnim podacima. *Amplifying* server ili mreža je bilo koji sistem koji generiše višestruke pakete koji se koriste za odgovor, kao što su *ICMP ECHO* paketi ili specijalni *UDP* paketi. Ovaj napad se zasniva na obrascu slanja *broadcast* poruke kroz *subnet* ili mrežu, tako da svaki nod te mreže reprodukuje jedan ili više paketa. Napadač šalje zatraženi informacioni paket sa sakrivenom izvornom adresom žrtve ka *amplifying* sistemu, pa će svi vraćeni paketi biti poslani žrtvi. Ukoliko je navedeni sistem sposoban da proizvede potreban broj paketa koji predstavljaju odgovor, tada će sistem koji je žrtva ovog napada doživeti *DoS* napad.

Sprečavanje, kao i kod drugih vrsta, nije jednostavno. Jedna od mera jeste zabrana *broadcast*-a na svim graničnim ruterima i konfiguracija sistema da odbace *ICMP ECHO* pakete.

Za napad pod nazivom *Ping of Death* napadač koristi specijalne alata kojim šalje ogroman broj prevelikih *ping* paketa ka žrtvi. U najvećem broju slučajeva sistem zahvaćen ovim napadom može da doživi u najboljem slučaju da se zamrzava ili restartuje, a nije čest slučaj i kompletan prestanak rada sistema. Iako ova vrsta napada više liči na neke druge vrste, ipak pripada grupaciji *DoS* napada, jer često kompletan

sistem prestaje sa radom. Zaštita može biti blokiranje ping paketa koji stižu sa rutera koji se nalaze na obodu mreže, konstatno održavanje sistema primenom najnovijih zakrpa, kao i precizno kodiranje aplikacija koje su interno razvijene da spreče *buffer overflow* i izbegavanje puštanja nekog koga sa *system* ili *root* privilegijama.

7.3 Spoofing

Specifično za ovu vrstu napada jeste pretvaranje da je paket nešto što on nije, odnosno ovaj napad menja validnu izvorišnu i/ili destinacionu IP adresu i ubacuje pogrešnu. Ova tehnika se primenjuje u velikom broju napada, jer daje napadaču mogućnost da sakrije svoj identitet, gde napadač koristi ukradeno korisničko ime i lozinku, kada promeni izvorišnu adresu malicioznog paketa ili kada napadač nagađa identitet klijenta kako bi zavarao ciljani server. Zaštita mora da sadrži konstantnu primenu zakrpa za operativne sisteme, korišćenje opcije provere izvora i destinacije na ruterima, kao i upotreba *IDS* sistema koji su u stanju da detektuju i blokiraju napad.

7.4 Man-in-the-Middle

Ime ove vrste napada govori samo za sebe. Dešava se kada napadač ili neki korisnik mreže stekne poziciju između dva krajnja korisnika, odnosno u sredini njihove komunikacije.

Postoje dve vrste:

- Napad koji podrazumeva kopiranje ili *sniffing* saobraćaja između dva krajnja korisnika
- Napad gde se napadač pozicionira na liniji komunikacije između dva krajnja korisnika, a gde napadač simulira da je *proxy* uređaj/aplikacija. On je nevidljiv za krajnje korisnike i kao takav menja podatke koji se razmenjuju. Na ovakav način može skupiti razne jako bitne podatke, kao što su kombinacije korisničkih imena i lozinki sa kojima može pristupiti raznom mrežnom sadržaju, ali i da menja podatke po sopstvenom nagođenju.

Za ovakve vrste napada potrebno je veliko znanje, jer napadač često mora da menja informacije potrebne za rutiranje saobraćaja, *DNS* vrednosti, krađe i *IP* adrese ili bilo koje druge informacije kako bi se predstavio kao legitiman server iz perspektive klijenata uključenih u ovu komunikaciju.

Podvrsta jeste napad pod imenom *hijack*. Kod ovog tipa napadač je pozicioniran između klijenta i servera, prekida njihovu komunikaciju kako bi je preuzeo. Tada se napadač predstavlja klijentu kao server kako bi od njega izvukao podatke. Legitiman server nije svestan prekida u komunikaciji. Korisnik koji je cilj je svestan da je komunikacija sa serverom prestala, ali s obzirom da se komunikacija nastavlja, ne dovodi u pitanje legitimnost komunikacije.

Još jedan tip predstavlja *replay (playback)* napad, koji je sličan prethodnom tipu, pa napadač snima saobraćaj između klijenta i servera, a potom paketi koji idu od klijenta ka serveru se ponavljaju (*playback*) ka serveru sa izmenom *time stamp*-a i izvorišne *IP* adrese. U nekim slučajevima ovakav način pristupa serveru omogućava napadaču da restartuje stari komunikacioni link. Kada se sesija ponovo aktivira napadač može da skuplja podatke ili dozvoli sebi pristup nekim drugim fajlovima kojima legitiman korisnik do tada nije mogao.

Zaštita podrazumeva unapređenje identifikacije, autentifikacije i uspostavljanje sesije. Takođe važi kao i za sve ostale vrste da je potrebno redovno primenjivati sigurnosne zakrpe vezane za operativne sisteme i softvere koji se koriste. Sigurnosni sistemi, kao što su *IDS*, nisu u stanju u potpunosti da identifikuju ove napade, ali mogu ustanoviti povećanu aktivnost preko sigurnosnih komunikacionih kanala, te na takav način mogu detektovati i blokirati ponovljene napade.

7.5 Sniffer napadi

Podjednako poznati i pod imenom *snooping*, ovi napadi predstavljaju bilo koju aktivnost koja za rezultat ima prikupljanje podataka o mreži ili mrežnom saobraćaju od strane napadača. Obično je to program koji kopira sadržaj sakupljen na mreži u neki izdvojen prostor (folder), a pogotovo na podatke koji se razmenjuju na početku

komunikacije između klijenta i servera, kao što su kombinacije korisničkih imena i lozinki, ključevi i slično.

Ukoliko se dobro izvede ovu vrsta napada je teško otkriti. Da bi se zaštitila mreža potrebno je unapređenje fizičkog pristupa, aktivno pretraživanje mreže za *sniffing* potpisima (npr. odlaganje slanja, dodatni koraci (*hops*) na putanji paketa, izgubljeni paketi itd), a najbitnija je upotreba enkripcije za unutrašnji i spoljašnji saobraćaj.

7.6 Spamming napadi

Ovaj izraz se koristi kada se opisuju neželjene *e-mail* poruke, *news* grupe ili poruke koje pristužu sa raznih foruma. Obuhvata širok spektar, od običnih oglasnih *e-mail*-ova do malicioznih „poplava“ i poruka u kojima se nalazi Trojanac ili neki drugi virus, koji može da naškodi mašini. U principu to nije značajan sigurnosni problem, ali kako se povećava količina spama teže je ustanoviti koje su poruke legitimne, a koje ne. Uz to, spam oduzima najveći deo mrežnog protoka i saobraćaja, kao i samo *CPU* procesuiranje, što može da prouzrokuje usporen saobraćaj.

Kada se koristi ovakva vrsta napada, ugrožen može biti pojedinačan *mailbox* korisnika ili čitav server. Ovakav napad će prouzrokovati *DoS* problem, jer ima za cilj da popuni sav slobodan prostor u *mailbox*-u ili na serveru i time spreči legitimne poruke da budu procesuirane. Najbolja zaštita je korišćenje filtera, ali najviše korišćenje *IDS*-a (razna rešenja renomiranih proizvođača koji se bave samo *e-mail* saobraćajem), kako bi se detektovao, pratio i sprečio napad ove vrste.

7.7 Crackers [18]

U više navrata je u ovom radu napomenuto da korisnici mogu i predstavljaju najveću pretnju svake mreže. Ali posebnu pažnju treba obratiti pažnju na korisnike koje imaju drugaciju motivaciju. Za razliku od običnog korisnika, koji usled neznanja, unese preko *USB flash*-a i drugog prenosnog medija neki problematični fajl, ovi korisnici mogu se odlučiti da kompromituju mrežu zbog pohlepe, ličnog priznanja ili osećaja moći. Oni se nazivaju *Crackers*. To su najčepće radnici firme koji već imaju određeni pristup mreži, a svojim znanjem pokušavaju da ukradu značajne podatke koji su

vlasništvo firme, kompromituju sigurnost mreže, onemogućavaju rad značajnih sistema, a šta sve može dovesti do negativnog javnog mnjenja ukoliko je njihovim postupcima kompromitovan neki javni servis koji firma pruža, gubitak dela tržišta. Sve ovo može dovesti i do slabljenja ili čak zatvaranja firme.

Zaštita je slična kao kod bilo kog *DoS* napada, redovno „krpljenje“ operativnih sistema, pravilna konfiguracija, kao i *IDS* i *Honey Pots* sistemi, o kojima je bilo reči ranije u tekstu.

8. **Cyber kriminal [11] [12] 17]**

Svi alati i tehnike navedene u ovom radu predstavljaju oružje Sajber (*Cyber*) kriminalaca. Po opšte prihvaćenoj definiciji ova vrsta kriminala zloupotrebljava kompjuterske tehnologije za realizaciju bilo kog oblika tradicionalnog kriminala, kao što je krađa, utaja ili pronevere, a koji se podaci mogu koristiti u razne svrhe kako bi se pribavila protivpravna imovinska korist, a koja je pribavljena u tzv „sajber okruženju“. Pod ovim okruženjem se podrazumeva grupa međusobno povezanih računara, a koje grupe su pak povezane između sebe.

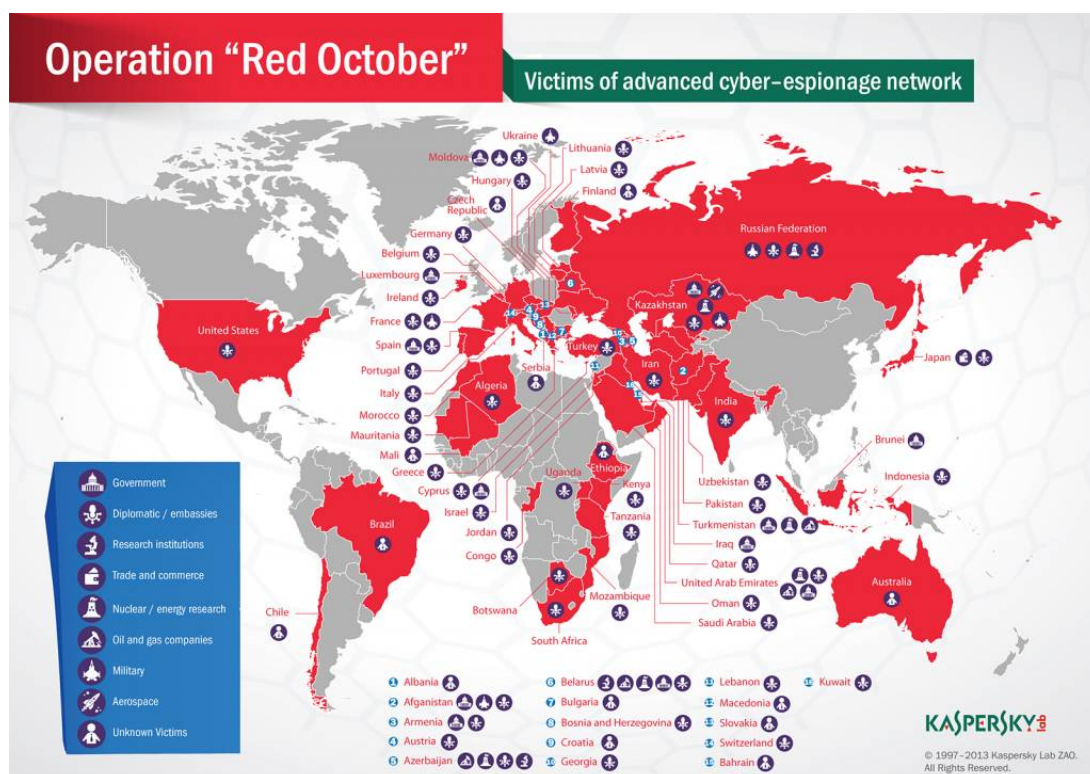
Ali nije sve tako jednostavno. Vrlo često ciljevi napada i *cyber* špijunaže vrlo bitne mreže i postrojenja u raznim zemljama, pa možemo smatrati da su ciljevi ekonomski, vojni ili politički razlozi. Zbog vrednog sadržaja koji mogu dobiti nelegalnim putem, u ovu nezakonitu igru se uključuju čak i nezavisne države preko svojih tajnih službi. Ono što je sigurno jeste činjenica da nikada nećemo saznati ko su žrtve ovih velikih napada, jer objava takvog propasta može uništiti ceo biznis.

Primer takvog napada, a koji je otkriven od strane kompanije *McAfee* u avgustu 2011 godine, jeste „*Shady RAT*“. Ceo proces trajao je pet godina, zahvaćeno je 14 zemalja i preko 72 kompanija, državnih ustanova i agencija, uključujući Olimpijske komitete u tri države. Najviše su na udaru bile Sjedinjene Američke Države sa 49 ugroženih firmi i organizacija. Ono što je interesantno da ovaj napad nije otkriven ni 2007 godine kada su napadi povećani za 260% i prošireni na 29 raznovrsnih firmi i organizacija, uključujući i spoljne saradnike *U.S defense*. Forenzička istraga je utvrdila da je u pitanju napad pod imenom *spear-phishing*, koji u sebi sadrži malver koji koristi

enkriptovane *HTML* komentare, a koji se nalaze u *Web* stranicama i koji se koriste kao kanal kroz koji se može upravljati zaraženim mašinama. [10]

Drugi primer visokotehnološke *cyber* špijunaže jeste globalni napad pod nazivom „*Red October*“. Otkriven od strane *Kaspersky Lab*-a, ovaj napad je bio aktivan od 2007 godine, pa sve do 2013 godine, kada je i otkriven. Glavni cilj je skupljanje informacija od diplomatskih i državnih agencija u zemljama širom sveta. Da bi kontrolisali zaražene sisteme, napadači su koristili više od 60 domenskih imena i posedovali više *hosting* servera u Nemačkoj i Rusiji. Najviše su zahvaćene zemlje Ruska federacija (35 zaraženih institucija), Kazahstan (21), Azerbejdžan (15), Belgija (15), Indija (14), Avganistan (10), Armenija (10) i Iran (7). Na listi su još i Ukrajina, Sjedinjene Američke Države, Grčka, Italija, Švajcarska i Ujedinjeni Arapski Emirati. [16]

Maliciozni kod je pristizao na mašine u vidu priloga u *e-mail* poruka, najverovatnije u vidu *Microsoft Excel* i *PDF* dokumenata. Pored ovih fajlova, napadači su koristili i propuste u *Java* aplikaciji. Kada bi žrtva primila zaraženi *e-mail*, otvorila prilog ili otišla na navedeni *URL*, maliciozni kod bi u mašinu infiltrirao osnovnih komponenti. Odmah potom bi dobio dodatne module, koje su omogućavale više opcija za špijuniranje. Jedan od tih modula je bio i za skidanje podataka sa mobilnih uređaja.



Slika br. 1 – Države i organizacije zaražene virusom „Red October“, (slika vlasništvo Kaspersky Lab-a) [21]

Istraživanje je pokazalo da su najviše bile ugrožene ambasade, državne agencije i ustanove, nuklearna postrojenja, istraživačke stanice, vojna postrojenja, postrojenja za vađenje i preradu nafte, kao i trgovinski centri u Japanu. Otkriven je sasvim slučajno, kada je jedna od partnera Kaspersky Lab-a zahtevao proveru nečega što je izgledalo kao napad, ali sa do tada nepoznatom načinu rada. Ova firma do danas nije objavila o kom partneru se radi. Kao što je već navedeno, većina žrtava nikada neće javno objaviti podatke o napadu, jer to šteti poslovanju. Takođe se sa sigurnošću ne zna ko stoji iza ovih napada. Po nekim informacijama ovu opasnu napast napravili su hakeri iz Kine, dok su određene module napravili Ruski hakeri. Ono što jeste sigurno je činjenica da su podaci koji su ukradeni od visokog značaja i predstavljali su državni\vojnu\poslovnu tajnu, a takve informacije se na crnom tržištu mogu prodati za vrtohlave svote novca.

9. Šta kaže zakon ? [1] [11] [17]

Svote novca stečene cyber kriminalom povećavaju se iz godine u godinu, a što izuzetno šteti ekonomijama ugroženih država, a koje pokušavaju da stanu na put ovom

novom načinu sticanja dobara na nedozvoljen način. Najznačajniji međunarodni dokument predstavlja Konvencija o *cyber* kriminalu. Donet je 2001 godine, pravosnažan je postao sredinom 2004 godine. Iako donesena od strane Saveta Evrope, ovu konvenciju potpisuju i Sjedinjene Američke Države, Kanada, Japan i Južna Afrika. Republika Srbija potpisala je Konvenciju 2005 godine, a ratifikovala ga je 2009 godine.

Sjedinjene Američke Države su mnogo ranije krenule u borbu protiv ove vrste kriminala od država Evrope, a kasnije Evropske unije. Glavni dokument jeste *The Computer Fraud and Abuse Act*, usvojen od strane Kongresa 1986 godine i koji je tokom godina imao više značajnih unapređenja. Jedan od njih je *The Identity Theft and Restitution Act*, izglasan 2008 godine. Doneo je izmenu definicija raznih vrsta kriminala, kao i dopunio novim terminima.

Srbija tek razvija zakon o *cyber* kriminalu na način koji bi ga približio svetskim zakonima i trendovima. Tako da visokotehnološki kriminal spadaju sledeća krivična dela:

01. Oštećenje računarskih podataka i programa
02. Računarska sabotaža
03. Pravljenje i unošenje računarskih virusa
04. Računarska prevara
05. Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka
06. Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži
07. Neovlašćeno korišćenje računara ili računarske opreme.

Osim ovih dela ova oblast pokriva i krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.

Opšteprihvaćeno mišljenje je da je Srbija u velikom zaostatku za ostatkom Evrope kada se govori o razvijenosti računarskog sistema. Ali po zvaničnim podacima inostranih stručbi Srbija je na trećem mestu po prevaram preko Interneta. Koliko se naša

zemlja visoko kotira govori i činjenica da tek u poslednje vreme ima zakonskih osnova da usluga *Pay-Pal* zaživi i u Srbiji. U cilju što bolje borbe Republika Srbija je osnovala Posebno tužilaštvo za visokotehnološki kriminal i doneo Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji je stupio na snagu sredinom 2005 godine. Po ovom zakonu za postupanje u predmetima kričnih dela zaduženo je Okružno javno tužilaštvo u Beogradu, a u okviru njega posebno odeljenje za borbu protiv visokotehnološkog kriminala.

Osim ovog zakona, Srbija je usvojila više propisa kako bi se Konvencija implementirala u pravni sistem. Najvažniji su:

01. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv sajber kriminala
02. Krivični zakonik
03. Zakon o odgovornosti pravnih lica za krivična dela
04. Zakonik o krivičnom postupku
05. Zakon o policiji
06. Zakon o autorskim i srodnim pravima
07. Zakon o telekomunikacijama
08. Zakon o elektronskom potpisu
09. Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine
10. Pravilnik o uslovima za pružanje internet usluga

U poslednjih nekoliko godina broj krivičnih dela u Srbiji rapidno raste, a prognoze stručnjaka da će se rast nastaviti, usled povećanja broja sistema za elektronsko plaćanje. Od izuzetnog je značaja što je Srbija potpisala Konvenciju o *cyber* kriminalu, jer je međunarodna saradnja od krucijalnog značaja, s obzirom da napadači mogu koristiti bilo koju zemlju, bilo koju mrežu, a da napadnu ciljeve u Srbiji. Odeljenje za visokotehnološki kriminal najviše je usresređeno na zaštitu dece i omladine (u skorije vreme izvršena akcija „Armagedon“, usmerena na otkrivanje krivičnog dela pedofilije) i prevencija ilegalne migracije i trgovine ljudima („Nigerijska šema“). Najveći uspesi ovog odeljenja su otkrivanje SMS prevara, kao i veliki doprinos u prekidu lanca pedofilije. Dobitnici su velikog broja priznanja.

10. Susret sa opasnim virusom

Mnogo domaćih firmi i organizacija tokom 2009 godine imalo je veliki problem sa virusom koji je dobio ime *Conficker* ili *Kido*. Između mnogih i institucije grada Beograda. Rešavanje ovog problema merilo se bukvalno u danima, sve dok *Microsoft* i *Kaspersky Lab*, čije antivirusno rešenje grad Beograd je koristio u to vreme, nisu objavili „zakrpe“ za taj problem. I pored toga, izuzetno je bilo teško osloboditi se ovog „napasnika“.

10.1 O *Conficker* virusu [15] [14] [13] [19] [20]

Conficker virus otkriven prvi put u novembru 2008 godine. Veruje se da je jedan od najrasprostranjenijih virusa u istoriji IT industrije. Po informacijama koje je početkom 2009 godine izbacila televizijska stanica *CNN*, 8 miliona računara je zaraženo početkom 2009 godine. Eksploataisao je propust *MS08-067* u *Microsoft Windows Server Service*.

Do sada je otkriveno pet varijanti ovog virusa:

01. *Conficker A* – otkriven 21. novembra 2008 godine
02. *Conficker B* – otkriven 29. decembra 2008 godine
03. *Conficker C* – otkriven 20. februara 2009 godine
04. *Conficker D* – otkriven 4. marta 2009 godine
05. *Conficker E* – otkriven 7. aprila 2009 godine

Dobio je razne pseudonime po kojima je poznat:

- Net-Worm.Win32.Kido (Kaspersky)
- Net-Worm.Win32.Kido.bt (Kaspersky)
- Net-Worm.Win32.Kido.dv (Kaspersky)
- Net-Worm.Win32.Kido.fx (Kaspersky)
- WORM_GIMMIV.A (TrendMicro)
- TSPY_GIMMIV.A (TrendMicro)
- WORM_DOWNAD.A (TrendMicro)

- Trojan.Moo (Symantec)
- W32.Downadup (Symantec)
- TrojanSpy:Win32/Gimmiv.A (Microsoft)
- TrojanSpy:Win32/Gimmiv.A.dll (Microsoft)
- W32/Conflicker.worm (McAfee)

10.1.1 Način zaraze i simptomi

Za zarazu ovaj virus koristi NetBIOS ili je pristigao u sistem preko prenosnih medija. Kada zarazi prvi računar *Kido* ima mogućnost širenja na druge sisteme preko *NetBIOS push*, *HTTP pull\push* i *P2P pull\push*.

Simptomi su blokiran rad antivirusa, ujedno korisnik nije u mogućnosti da ode na stranicu antivirusnog rešenja koji koristi, takođe mašina nije bila u mogućnosti da povuče najnovije zakrpe za operativni sistem, lokalna polisa koja se brine o zaključavanju sistema se automatski resetovala, tako da su svi administratorski nalozi bili zaključani i nije bilo mogućnosti prilaska sistemu kao administrator, pojedini servisi su bili stopirani, kao što su *Automatic Updates*, *Background Intelligent Transfer Service (BITS)*, *Windows Defender* i *Error Reporting Services*, domen kontroleri su presporo odgovarali na zahteve korisnika, a ne retko uopšte nisu odgovarali, lokalna mreža je bila zagušena, virus je pravio taskove za svoje pokretanje, te se uvlačio u *System restore* opciju na *Windows* operativnim sistemima.

Prvo rešenje došlo je od strane *Kaspersky Lab* firme, dok je *Microsoft* izbacio zakrpu za operativne sisteme par dana kasnije. Međutim, nije bilo dovoljno jednostavno primeniti ove zakrpe. Dok se otklanja problem na jednom operativnom sistemu, drugi bivaju zaraženi sa drugih sistema. Tako da je bilo neophodno izolovati deo po deo mreže i onda otklanjati nastale probleme. Gotovo kompletan proces obavljao se ručno, s obzirom da su svi administratorski nalozi u mreži bili onemogućeni. Alat koji je *Kaspersky Lab* izbacio kao prvo rešenje dobio je naziv *KidoKiller*. Bilo je neophodno izvršiti niz postupaka pre nego što je mašina bila slobodna od ovog opasnog napasnika.

Opasnost je ležala u sofisticiranom načinu adaptacije binarne enkripcije, digitalnih potpisa i naprednih *hash* algoritama koji su sprečavali da neko treći preuzme

zaražene računare. Njegova uloga je bila da obezbedi svome autoru momentalni prilaz mreži preko zaraženih računara. Korišćenjem binarnih enkripcionih metoda autori ovog virusa su se postarali da niko drugi ne može da priđe zaraženim računarima i ubaci „lek“ za nastali problem, pa su enkripcijom bili zaštićeni svi mogući izlazi i ulazi koji bi mogli da unesu „lek“. Iz tog razloga nije bilo moguće koristiti eksterne uređaje, pa se koristili stari, dobri *CD* i *DVD* diskovi, iz razloga što su podaci na njima narezani i nije ih moguće menjati, a kako je to činio virus kada se u zaražen računar ubaci eksterni uređaj.

Pojava ovog virusa je izuzetno značajna za *IT* industriju, jer je bio izuzetno inovativan u odnosu na viruse koji su do tada se pojavljivali. Profesionalno razvijen, imao je mogućnost da se širi kao *DLL*, mogao je da vrši sinhronizaciju vremena mimo *NTP* servera. Menjao je način rada i strategiju domena, napadi su bili tempirani, kačio se za procese (npr. *services.exe*), stvarao je nasumična imena fajlova koji su bili smeštani u *%system%* i *%program files%*, za svoje širenje koristio je i *autrun* opciju, ali i slabo zaštićene foldere koji su deljeni (*share*) za korišćenje kroz mrežu. Gasio je sigurnosne procese i isključivao servise, sprečavao je pristup svakom domenskom korisničkom nalogu koji je imao mogućnost da virusni proces zaustavi, te je stoga menjao *ACL* liste i uspešno je isključivao podizanje mašine u *safe* modu. Koliko je ovaj virus bio komplikovan govori činjenica da nabrojane mogućnosti nisu i jedine, te da je *Conficker* bio u mogućnost da za svoga autora odradi još niz komandi.

11. Zaključak

Digitalni svet u kome živimo rapidno raste iz dana u dan. Podaci su pristupačniji više nego ikad, usluge, plaćanje računa jednim klikom miša, kupovina preko interneta ili popularno naručivanje hrane. Ono što običan korisnik ne zna jeste da iza svakog komoditeta koji ima i koristi, stoje kompleksne, razgranate mreže i niz servisa i pravila koji omogućavaju usluge koji se koriste na dnevnom nivou.

Zastarevanje tehnologije je neminovan proces, pa već sad veliki deo gore izloženog već potpada pod taj termin, iako se i dalje koristi i koristiće se još neko vreme. Polako mreže sele svoje podatke od kojih im zavisi poslovanje u „oblak“, tako smanjujući ljudstvo i cenu koštanja održavanja svojih servisa. Ali takav premeštaj još

dugo će biti prihvatano sa nepoverenjem, jer se poverljivi i osetljivi podaci prepuštaju na brigu i staranje trećem licu.

Sa razvojem raznih tehnologija koje sačinjavaju jednu veliku i uspešnu mrežu povećava se i njena kompleksnost, ali i mogućnost prodora od strane napadača. U sledećem radu će biti govora o tome šta sve može da se desi u jednoj kompleksnoj mreži, odnosno kakvi maliciozni kodovi mogu da prodru u mrežu, te kako drugi spoljni faktorimogu uticati na rad velikih sistema.

12. Literatura

- [1] Bosworth Seymour, Kabay M.E., „*Computer Security Handbook*“, Publisher: John Wiley & Sons, INC, 4th Edition, 2002;
- [2] Casey Eoghan, „*Digital Evidence and Computer Crime*“, 3th Edition, Publisher: elsevier, 2011;
- [3] Grupa autora, „MCSE – Udžbenik za pripremu ispita – Osnove umrežavanja Plus“, Izdavač Microsoft Press, 2000;
- [4] Grupa autora, „*Information Security Management Handbook*“, Auerbach Publications, A CRC Press Company, 5th Edition, 2004;
- [5] Grupa autora, „*Windows Server 2008 – TCP/IP Fundamentals for Microsoft Windows*“, izdavač Microsoft Press, 2006 godine;
- [6] Kurose James F., Ross Keith W., „*Computer Networking*“, 6th Edition, Publisher: Pearson, 2013;
- [7] Ogletree, Terry W., Soper, Mark Edward, „*Upgrading and Repairing Networks*“, Publisher: Que, May 2006;
- [8] Olifer Natalia, Olifer Victor, „*Evolution of computer networks*“, Publisher: Wiley, November 2005;
- [9] Stallings Wiliam, „*Network Security Essentials: Applications and Standards*“, 4th Edition, Publisher: Prentice Hall, 2011;
- [10] Veinović Mladen, Jevremović Aleksandar, „Uvod u računarske mreže“, Izdavač: Univezitet Singidunum, 2008;
- [11] Grupa „*Information Security Management Handbook*“, Auerbach Publications, A CRC Press Company, 5th Edition, 2004;
- [12] Časopis „*Hakin9 Bible*“, january 2012,

Internet izvori:

- [13] <http://nszilvia.wikispaces.com/Рачунарске+мреже>
- [14] <http://www.computerhistory.org/timeline/?category=net>
- [15] <http://www.computermuseum.li/Testpage/ENIAC4.GIF>
- [16] <http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/arpanet3.gif>
- [17] http://www.att.com/Common/DSL/center/images/connected_house.gif?01AD=3cDL4VChg5zst-

dlyasb9m005ihilEzd4SYnnr0Lj7Y062MFy47ej7A&01RI=F8227F024E1263D&01NA

=

- [18] <http://www.dansdata.com/images/networking/terminator320.jpg>
- [19] <http://fcit.usf.edu/network/chap4/chap4.htm>
- [20] <http://www.sparksdirect.co.uk/image/data/zencart/lights/rj45plug.jpg>
- [21] <http://webpage.pace.edu/ms16182p/networking/utp%20and%20stp.jpg>
- [22] <http://www.computercablestore.com/images/products/No%20Manufacturer/0-RG6.jpg>
- [23] http://support.brighthouse.com/media/video/equipment/wires/Coaxial_Cable.jpg
- [24] <http://www.opticalfibercable.teracabindia.com/>
- [25] http://en.wikipedia.org/wiki/IEEE_802.11
- [26] <http://www.tutorialspoint.com/shorttutorials/wp-content/uploads/2012/12/7421-asus-wl500gp-wireless-router-connectivity.jpg>
- [27] www.quagwire.com
- [28] <http://blog.simplilearn.com/it-security-management/understanding-open-systems-interconnection-reference-model-osi>
- [29] <http://support.microsoft.com/kb/103884>
- [30] <http://technet.microsoft.com/en-us/library/cc958821.aspx>
- [31] <http://realitypod.com/wp-content/uploads/2011/08/model.gif>
- [32] http://en.wikipedia.org/wiki/Transmission_Control_Protocol
- [33] http://en.wikipedia.org/wiki/Internet_Protocol
- [34] <https://learningnetwork.cisco.com/servlet/JiveServlet/showImage/2-400741-258349/OSI-TCP-Comparison.jpg>
- [35] <http://www.tcpipguide.com/>
- [36] <http://technet.microsoft.com/en-us/library/cc940018.aspx>
- [37] http://en.wikipedia.org/wiki/IP_address
- [38] <http://en.wikipedia.org/wiki/RAID>
- [39] http://en.wikipedia.org/wiki/Standard_RAID_levels
- [40] <http://www.prepressure.com/library/technology/raid>
- [41] http://en.wikipedia.org/wiki/Server_farm
- [42] <http://www.computervirusremovalguide.com/a-brief-look-at-the-history-of-computer-viruses.php>
- [43] <http://www.infoplease.com/ipa/A0872842.html>

- [44] <http://en.wikipedia.org/wiki/Spyware>
- [45] <http://en.wikipedia.org/wiki/Rootkit>
- [46] http://en.wikipedia.org/wiki/Social_engineering_%28security%29
- [47] <http://www.darkreading.com/attacks-and-breaches/shady-rat-attack-hit-72-organizations/d/d-id/1099357?>
- [48] http://www.mup.gov.rs/cms_lat/saveti.nsf/saveti-sajber-kriminal.h
- [49] http://sr.wikipedia.org/sr/Сажбер_криминал
- [50] http://www.simc-inc.com/web/articles/k-soc/pdf/K-SOC_Advisory-Conficker_Worm.pdf
- [51] http://www.caro2009.com/presentations/igor_muttik.pdf
- [52] <http://download.nai.com/products/mcafee-avert/documents/>
- [53] <http://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/>
- [54] <http://www.begrad.vtk.jt.rs/>
- [55] http://www.morebusiness.com/running_your_business/technology/d935705243.brc
- [56] <https://technet.microsoft.com/library/security/ms08-067>
- [57] <https://technet.microsoft.com/library/security/ms08-068>
- [58] <http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2013/01/208194085.png>
- [59] <http://blog-cache3.extensis.com/wp-content/uploads/2013/08/1993-vs-2003.jpg>