SIGURNOST RAČUNALNIH MREŽA

Dr. sc. Marijan Mijatović, izvan. prof.
Nezavisni Univerzitet Banja Luka
Fakultet za informatiku

Dr.sc. Marko Mijatović, izvan. prof.
Hercegovina Univerzitet Dr.Milenka Brkić
Bijakovići, Međugorje

Pregledni rad
UDK 004.7: 004.42
https://doi.org/10.59417/nir.2024.24.58

Sažetak
Računala koja povezujemo u mrežu služe da bismo izmjenjivali podatke, koji se nalaze u radnoj memoriji računala. Sam prijenos podataka može se obavljati isto tako i elektroničkim signalima, a te veze mogu biti bežične mreže, i žičane mreže. Bitovi koji šalju jedan za drugim istodobno odgovarajućom brzinom, i pretvaraju digitalni signal u analogni signal i obrnuto obavljaju moderno. Računala također mogu biti povezana i u lokalnu mrežu i u razgranatu mrežu. Svako računalo koje je spojeno na mrežu ima svoj jedinstveni broj (adresu) iz koje se može prepoznati na kojem je kontinentu, i u kojoj je državi te na koju je adresu poslužitelj povezan. Podaci se šalju u skladu s prije dogovorenim protokolom, i to u obliku paketa. Sigurnost zaštite osjetljivih podataka i dokumenata postoji već odavno u svijetu. Tokom povijesti mnogo se metoda razvijalo u pogledu zaštite podataka i sigurnosti na internetu. Metode pružanja zaštite na internetu ponekad nisu bile efikasne i nisu pružale u dovoljnoj mjeri zaštitu koja je bila potrebna. Razvojem kriptografije i tehnologije otkriveni su vrlo dobri načini kriptiranja i zaštite dokumenata. Informacijski sustavi su temelj osnovnog i modernog poslovanja. Njihova temeljna zadaća je da se baziraju na sustav mreža,te njihovo poslovanje i sigurnost. Zbog toga je izuzetno važno da se što bolje upoznamo sa sigurnosnim problemima računalnih mreža, i načinima na koji se ti problem rješavaju. Današnje se računalne mreže sve više temelje na TCP-IP protokolu, zbog jednostavnog definiranja adresa uređaja na mreži te zbog mogućnosti povezivanja na internet i korištenje njegovih mrežnih usluga. Planiranje zaštite sigurnosnih sustava temelji se na ispitivanju poznatih prijetnji te prijedloge rješenja kao rezultat kompromisa. No efikasna zaštita ne primjenjuje samo jedno rješenje, već kombinaciju puno više različitih drugih opcija zaštite i sigurnosti mreža. U ovom radu ćemo se u kratkim crtama osvrnuti na općenito sustav mreža, a isto tako i njihova sigurnost, nastanak, te njihovu podjelu.
Ključne riječi: mreže, protokoli, paketi, LAN, antivirusi, kriptografije.

UVOD

Računalne mreže su stvorene s ciljem da spajaju računala na više različitih lokacija, tako da se istovremeno mogu razmjenjivati i dijeliti podatke tj. (komunicirati). U početku je većina podataka koji su se prenosili u takvim mrežama bila u tekstualnom obliku. Danas s velikim porastom multimedijskih i mrežnih tehnologija, multimedija je postala nezaobilazan faktor same pojave na internetu.

Na tržištu su se pojavili mrežni proizvodi kao internet telefonija, Internet televizija, videokonferencije, i dr.

U budućnosti će ljudi sve više da koriste usluge kao što su učenje na daljinu(Distance Learning), te razno distribuirane simulacije koje neće tražiti da članovi jednog tima grupe budu u istoj zgradi, pa čak ni u istoj državi. Ekonomske prednosti takvog rada su očigledne.

Mrežne usluge moraju izgraditi hardversku i softversku strukturu te razne alate koji će podržavati prijenos i multimedijskih usluga računalnim mrežama, te omogućiti korisnicima što kvalitetniju i bolju komunikaciju u poslovanju.

Mrežne usluge će se naveliko unaprijediti upotrebom računala kao komunikacijskog alata. Vjeruje se da će jednog dana multimedijske mreže zamijeniti telefone, televizore, i dr. izume koji su nekada davno u prošlosti promijenile način našeg života.

Pojavu informacijskih sustava i računalnih mreža koje su u velikoj mjeri promijenile naš život i naše aktivnosti te nas potakle na dodatno educiranje u svijetu mreža i mrežnih sustava sigurnosti, da bi što bolje zaštitili svoj dio poslovanja te samim time i ulaganje u sigurnost istih.

Šezdeset godina kasnije informacijski sustavi su prisutni u svakom dijelu ljudskog djelovanja, a današnji moderan svijet ne može zamisliti bez postojanja računalnih mreža i njihove sigurnosti.

POVJEST RAČUNALNIH MREŽA

Računalne mreže nastale su kao rezultat aplikacija napisane za velike korporacijske tvrtke. Tvrtke su uvidjele problem učinkovitosti svojih djelatnika koji su da bi na pisaču nešto napisali, morali iste prenositi na disketnim jedinicama do samog pisača. Kopirati određene vrste podataka na računalo koje je imalo priključen pisač na sebi, i tek se onda mogao ispisati određeni dokument.

Zbog jednostavnijeg i nadasve jeftinijeg poslovanja tvrtke ulagati se počelo u mrežnu tehnologiju te njihovu sigurnost radi boljeg i što sigurnijeg poslovanja. Početkom 1980-ih računalne mreže doživjele su ogromnu ekspanziju, iako su prve od tih mreža bile prilično dosta nesigurne.

Zbog naglog rasta računalnih mreža te njihove sigurnosti u jednom određenom periodu došlo je do nekompatibilnosti među mrežnim sustavima koje su financirale različite tvrtke. Rješenje tog problema je bilo LAN (Local Area Network).

Vjerovatno je najvažniji trenutak bio 1983 godine., kad je tadašnja mreža sa NCP-A (Network Control Protocol) prešla na TCP/IP (Transmission Control Protocol / Internet Protocol) noviju tehnologiju kakva se danas koristi u svijetu.

Packet- Switched tehnologija opisuje slanje određenih podataka u malim zapakiranim jedinicama podataka zvanim paket. Oni se usmjeravaju po mreži tako što koriste ciljanu ip adresu koja je sadržana u paketu. Paket koji putuje tim putem doći će do izvora odredišta, te je bitno i da svi ostali paketi stignu na odredište.

Dijeljenje podataka za slanje u pakete omogućava da se iste komunikacijske mreže dijele između većeg broja korisnika u mreži.

Svako računalo koje je spojeno na mrežu isto tako ima i svoj jedinstveni broj(adresu) iz koje se može prepoznati na kojem je dijelu svijeta, u kojoj državi i pomoću kojeg je poslužitelja povezana. Podaci se u mreži šalju u skladu s dogovorenim protokolima i to u obliku paketa.

MREŽE I NJIHOVA PODJELA

Podjela i vrste usluga koje treba osigurati informacijska mreža su sljedeće:

- U govoru i komunikaciji, u digitalnom obliku, postupkom kanala ili paketa, tekstom komunikacije, komunikacije podataka postupcima kanala i paketa u stvarnom vremenu ili s vre-

menskom zadrškom, pristup bankama i računalnim podacima uslugama te njihovom procesuiranju.

- Komunikacije slikom, videofon, telefax, višemedijske komunikacije, te daljinsko upravljanje.

Osim u fizičkom formatu za spajanje u mrežu, računalne mreže mogu se razlikovati i prema veličini:

- Lokalna mreža (Local Area Network, LAN).Jednostavna, u kojoj su dva računala povezana putem kabla.
- Kućna mreža (Home Area Network, HAN).To su računala koja su po jednom kućanstvu i prespajaju osobne elektroničke uređaje tipa mobitel, laptop, HDTV.
- Rasprostranjena računalna mreža (WIDE Area Network, WAN).To su računala koja su raširena po cijelom svijetu te povezana preko telefonskih linija satelitskih veza i radioveza.
- Metromreža(Metropolitan Area Network,MAN).Podatkovna mreža u većim gradovima na koju se povezuju velike tvrtke.

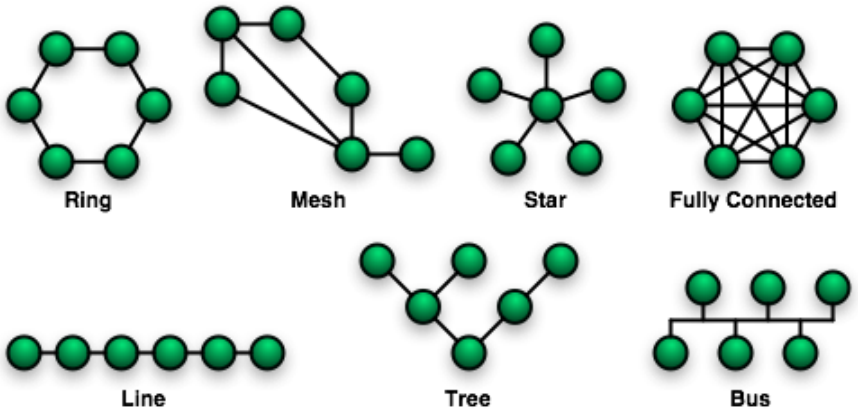
TOPOLOGIJA MREŽA

Topologija mreža je skup mreža u kojem su računalni sustavi ili mrežni uređaji povezani

jedni s drugima, međusobnih veza tj.,čvorova u mreži. Topologije se mogu definirati u fizički i logički aspekt mreža. Fizički(geografski) raspored mreža obično je manje važan od topologije koja povezuje mrežne čvorove. U većini dijagram je taj koji opisuje fizičku mrežu. Simboli na ovim dijagramima obično označavaju mrežne veze i mrežne čvorove.

Topologija također određuje način razmjene informacija unutar mreža.

- Point- to- Point;
- Bus Topology;
- Star Topology;
- Ring Topology;
- Mesh Topology;
- Tree Topology;
- Daisy Chain;
- Hybrid Topology;

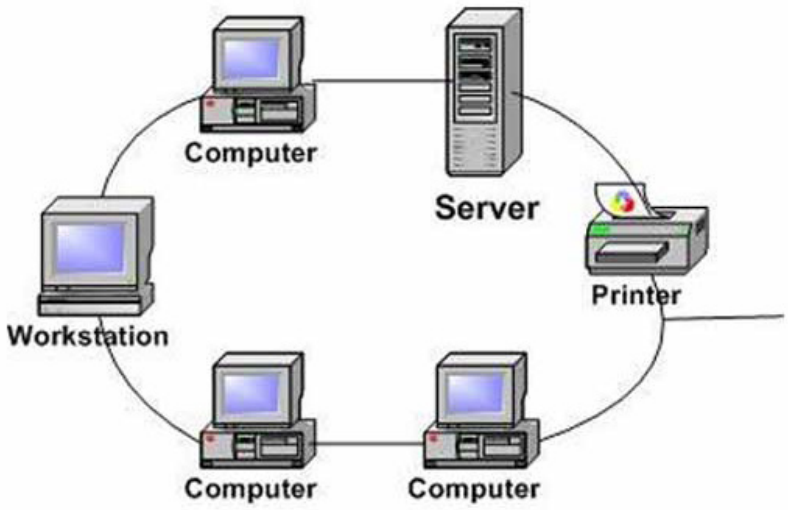


Peer to Peer – mreža od točke do točke koja sadrži dva hosta kao što su računalo, prekidač, router, i serveri koji su povezani jedan do drugoga pomoću Internet kabela. Ako su hostovi i logički povezani s ovom metodom onda mogu imati i više spojenih uređaja.

Bus topology – u ovom slučaju topologije svi uređaji dijele jednu komunikacijsku liniju. Ovom metodom može se doći i do problema, dok više hostova istovremeno šalju podatke. Problem mreže koja koristi ovu metodu može biti taj da u slučaju prekida kabla na bilo kojem dijelu dolazi do prekida rada čitavog mrežnog sustava.

Star Topology – svi hostovi u ovoj topologiji su spojeni na jedan centralni uređaj, poznatiji kao HUB ili Switch, koristeći konekciju od točke do točke. Problem kod ovakvih mreža je taj što ako dođe do kvara HUB-a, čitava mreža može da padne dolje.Prednost je što nije toliko skupa i bilo koji dodatni uređaj se može povezati samo s jednim kablom

Ring Topology – u ovoj topologiji svaka host mašina je povezana sa točno dvije druge mašine, stvarajući tako kružnu mrežnu strukturu. Kada jedan domaćin pokuša da komunicira ili pak pošalje poruku hostu koji nije u njegovoj blizini, podaci putuju kroz sve srednje hostove. U slučaju kvara bilo kojeg hosta, dolazi do prekida mreže.



Mesh Topology – u ovoj topologiji host je spojen sa jednim ili više hostova. Povezani su od točke do točke te ona dolazi u dva tipa:

Full mesh pruža najpouzdaniju mrežnu strukturu među svim topologijama. Za svaki novi host su potrebne N 8N-1)/2 veze.

Partially mesh nisu svi domaćini povezani od jedne do druge točke. Hostovi se međusobno povezuju na neki svoj proizvoljan način. Ova topologija postoji kada treba da pruži pouzdanu vezu samo određenim hostovima.

Tree Topology je poznat kao hijerarhijska topologija je najčešći oblik koji se trenutno koristi. Ona prikazuje proširenu zvjezdastu topologiju te nasljeđuje i svojstva magistralne topologije. Ovakav sustav mreža podijeljen je u više slojeva, uglavnom su to tri sloja. Najniži sloj na koji su priključena računala. Srednji sloj poznat kao distribuirani sloj, koji djeluje kao posrednik između donjeg i gornjeg sloja. Najviši sloj je poznat kao jezgroviti sloj i središnja je točka mreže, korijen stabla pod kojim se čvorovi granjanju.

Daisy Chain ova topologija priključuje sve hostove linearlno. Slična je zvjezdastoj topologiji. Svaka karika u topologiji lanaca predstavlja jednu točku neuspjeha. Svaki kvar veze razdvaja mrežu na dva segmenta, i svaki posrednički domaćin radi kao relej za svoje neposredne hostove.

Hybrid Topology za ovu mrežnu strukturu čiji dizajn sadrži više od jedne topologije kaže se da je hibridna topologija. Ona nasljeđuje zasluge, ali i nedostatke svih ugrađenih topologija.

TIPOVI MREŽNIH MEDIJA

Mediji za prijenos koji se nazivaju ujedno i fizičkim medijima koriste se za povezivanje računalskih uređaja u mreži koji se sastoje:

1. električne kablove (ETHERNET, Home PNA, mrežna komunikacija).
2. Optičke kablove (fiber- optička komunikacija)
3. Radio talasi (bežična komunikacija).

U OSI modelu oni su definirani na slojevima 1 i 2, fizičkoj sloju i sloju veze podataka. Široko usvojena obitelj prijenosnih medija koja se koristi u LAN tehnologiji poznata je kao ETHERNET kabel. Prijenos podataka vrši se preko bakarnih i optičkih kablova. Standardne bežične LAN mreže koriste ujedno i radiotalase te druge frenkvencije kao mediji za prijenos istih. Komunikacija električnom linijom koristi mrežni kabel za prijenos podataka.

UREĐAJI I MREŽNI ČVOROVI

Pored bilo kog fizičkog prijenosa medija koji postoje, mreže sačinjavaju dodatne i osnovne sustavske blokove, kao što su Network Interface Controller (NIC), repetitori, HUB-ovi, mostovi(BRIDGE), switchevi, ruteri, modemi i drugi zaštitni zidovi(FIREWALL).

Mrežno korisničko sučelje

Network Interface Control je računalski hardver koji računalu omogućava pristup za prijenos podataka te ima mogućnost obrade mrežnih informacija na nižem nivou.

NIC može imati konektor za prihvaćanje kabla ili antenu za bežični prijenos podataka.

NIC odgovara na promet upućen Internet adresi bilo za NIC ili za samo računalo.

U Internet mrežama svaki kontroler ima svoju jedinstvenu **MAC (Media Acess Control)** adresu koja je dužine 6 okteta.**00-0a-83-B1-c0-b8,** koja se obično čuva u trajnoj memoriji kontrolera. Da bi izbjegli sukobe adresa između mrežnih uređaja, institut injžinjerstva Elektrotehnike i Elektronike (IEEE) održava i administrira jedinstvenost MAC adresa.

Repetitori i HUB-ovi

Repetitor je mrežni uređaj koji prima mrežni signal, te ga čisti od nepotrebne buke regenerira (pojačava).Signal se zatim ponovo emitira na višem nivou snage ili na drugu stranu prepreke, tako ga signal može prijeći i veće daljine bez propadanja. Kod Internet konfiguracija repetitori su potrebni za kablove koji su duži od 100 m, dok kod optičkih vlakana mogu biti udaljeni desetine, pa čak i stotine kilometara. Repetitori za više portova su poznatiji kao HUBovi, i oni rade na fizičkom sloju OSI modela.

Most(Bridge)

Mrežni most povezuje i filtrira promet između dva mrežna segmenta na sloju veze podataka. OSI modela da bi formirao jedinstvenu mrežu. Ovo razbija domen mreže ali zadržava domen emitiranja. Mrežna segmentacija razbija veliku zagušenu mrežu u skup manjih, efikasnijih mreža te postoje i tri osnovna tipa:

- **Lokalni mostovi:** povezuje LAN-ove.
- **Daljinski mostovi:** može se koristiti za stvaranje WAN između LANO-ova. Udaljeni mostovi, gdje je veza sporija od krajnjih mreža, uglavnom su zamijenjeni ruterima.
- **Bežični mostovi:** mogu se koristiti za spajanje LAN-OVA ili povezivanje udaljenih uređaja sa LAN-ovima.

Switch

Mrežni prekidač je uređaj koji upravlja protokom podataka između dijelova lokalne mreže(LAN).Za razliku od HUB-a, switch dijeli mrežni promet te ga šalje na određene lokacije, dok HUB šalje podatke na sve uređaje koji su na mreži. Koriste se za mreže srednje veličine, jer su bolji i efkasniji od HUB-a. Switch daje računalu punu brzinu mreže, dok ostala računala prikopčana na HUB dobivaju samo dio konekcije.

Ruteri

Ruter ili mrežni usmjerivač je uređaj koji služi za međusobno povezivanje računalnih mreža. On ima funkciju da za svaki paket podataka odredi točnu putanju kojom paket treba da ide i da taj isti paket proslijedi slijedećem uređaju u nizu. U lokalnim mrežama ruter se obično postavlja da bude veza između mreže i interneta, tj. podrazumijeva se kao izlaz sa mreže(GATEWAY).

Wireless access point (WAP)

WAP je mrežni hardverski uređaj koji omogućava uređaju kompatibilnosti sa WIFI mrežom da se poveže na žičanu mrežu. WAP se obično povezuje sa ruterom (putem žičane mreže) kao

samostalni uređaj, ali isto tako može biti i sastavni dio samog rutera. WAP se razlikuje od pristupne točke(HOTSPOT), koja je fizička lokacija na kojoj je dostupan WIFI pristup WAN – u.

Modem

Modemi(modulatori-demodulatori) se koriste za povezivanje mrežnih čvorova pomoću žice koji prvobitno nije projektiran za digitalni mrežni promet ili za bežično povezivanje. Modemi se obično koriste za telefonske linije, koristeći tehnologiju digitalne pretplatničke linije. Oni modeliraju digitalni signal u oblik koji je pogodan za prijenos preko komunikacijski kanala, a poslije prijenosa ga vraćaju u prvobitni oblik.

Firewall

Firewall ili zaštitni zid je mrežni uređaj za kontrolu sigurnosti i pravila pristupa nekoj mreži. Uglavnom su konfigurirani da odbijaju pristup iz nepoznatih izvora, dok istovremeno dozvoljavaju radnje iz poznatih. Igraju vitalnu ulogu u sigurnosti mreža sa stalnim porastom cyber napada.

ZAŠTITA I SIGURNOST RAČUNALNIH MREŽA

Oduvijek je postojala potreba zaštite osjetljivih podataka, a time i dokumenata koji sadrže takve podatke. Tokom povijesti razvijeno je mnogo metoda kojima su ljudi pokušavali i uspijevali očuvati tajnost važnih podataka. Mnoge metode su bile jednostavne i nisu pružale dovoljnu zaštitu. U takvim slučajevima tajnost je često bila narušena. Razvojem kriptografije i tehnologije otkriveni su vrlo dobri načini kriptiranja i zaštite dokumenata.

Kriptiranje je dobar način sprječavanja neovlaštene osobe od pregledavanja sadržaja osjetljivog dokumenta. Ali kada se dokument dekriptira tajnim ključem, ovlaštena osoba loših namjera može spremiti, kopirati, ispisati ili proslijediti dokument. Ograničavanje pristupa dokumentu nekolicini pojedinaca jedan je od pristupa zaštite dokumenta, no uvijek postoji mogućnost da jedna od osoba kojoj je povjeren pristup oda podatke.

U tom slučaju treba se pronaći osobu koja je odala informacije, što nije uvijek jednostavan zadatak. Rješenje koje osigurava zaštitu osjetljivih informacija ne može ovisiti o samo jednoj tehnologiji.

Antivirusna zaštita

Antivirusni programi su posebna kategorija programa čija je osnovna namjena identifikacija, neutralizacija i eliminacija virusa, crva, trojanca i ostalih malicioznih programa. Osnovna zadaća antivirusnog programa je prepoznati virus i zaštiti sustav od njegovog djelovanja. Ako je računalo zaraženo virusom, tada ga antivirusni program mora izolirati i ukloniti. Za prepoznavanje virusa koriste se antivirusne definicije. Naime, svaki virus karakterizira određena sekvenca okteta (znakovnih kodova), budući da je i virus u osnovi računalni program. Nakon što detektira virusnu sekvencu u nekoj datoteci, antivirusni program će:

- pokušati popraviti datoteku brišući iz nje sam virus,
- staviti datoteku u karantenu (quarantine) tako da toj datoteci više ne može pristupiti nijedan program, pa se samim tim ni virus više ne može širiti,
- izbrisati inficiranu datoteku.

Kako se virusi stalno razvijaju, bazu definicija virusa i njihovih kodova treba stalno osvježavati, uglavnom više puta dnevno. To najčešće rade sami antivirusni programi. Ako se definicije ne bi osvježavale, antivirusni program ne bi mogao prepoznavati nove viruse.

Upravo je ne osvježavanje definicija virusa glavni razlog stalnog širenja nekih odavno poznatih virusa. Kako bi nadigrali mehanizme detekcije virusa, programeri virusa često stvaraju tzv. oligomorfne, polimorfne ili metamorfne viruse. Takvi virusi mijenjaju oblik i programski kod, nastojeći ostati neopaženi u svakoj sljedećoj "inkarnaciji".

Drugi način rada antivirusnog programa je nadzor ponašanja svih programa. Ako neki program pokuša zapisivati podatke u izvršni kod nekog programa, pristupati mreži ili pokušati slati podatke na neki port, antivirusni program će to signalizirati i dojaviti korisniku

Kriptiranje

Važan dio zaštite dokumenata pohranjenih na tvrdim diskovima računala, posebno prijenosnih, svakako je enkripcija. Ovim relativno jednostavnim postupkom moguće je izbjeći otkrivanje povjerljivih informacija u slučaju gubitka prijenosnog računala, kao i napade zlonamjernih korisnika koji ostvare fizički pristup računalu. Većina modernih operacijskih sustava posjeduje ugrađene mehanizme koji omogućuju kriptiranje pohranjenih podataka.

Postupak kriptiranja uključuje preoblikovanje otvorenog ili jasnog teksta u tekst nerazumljiv osobama kojima nije namijenjen. Osobe kojima je dokument namijenjen i koje ga smiju pročitati moraju posjedovati poseban ključ za pretvaranje dokumenta u jasan tekst, odnosno dekriptiranje. Postoje simetrični i asimetrični kriptosustavi.

U simetričnom kriptosustavu ključ kriptiranja ili pretvaranja dokumenta u nerazumljiv tekst jednak je ključu dekriptiranja, dok kod asimetričnog kriptosustava to nije slučaj. U komunikaciji porukama obično postoji pošiljatelj i primatelj poruke.

Asimetrični kriptosustavi zasnivaju se na određenim svojstvima brojeva koja se istražuju u teoriji brojeva. Ideju objašnjava sljedeći primjer. Ana stvara samo svoj par ključeva: jedan za kriptiranje i jedan za dekriptiranje. Ako se pretpostavi da je asimetrično kriptiranje oblik računalne enkripcije, tada je Anin ključ za kriptiranje jedan broj, a ključ za dekriptiranje neki drugi broj. Ana svoj dekripcijski ključ drži u tajnosti te se on zbog toga obično naziva privatnim ključem. Ona, međutim, svoj ključ za kriptiranje javno objavljuje tako da je on svakome dostupan.

Primjer najčešće korištenog asimetričnog kriptosustava je RSA, čiji su autori Ron Rivest, Adi Shamir i Len Adleman. Još neki primjeri takvih algoritama su ElGamal, NTRUEncrypt,

LUC i drugi. Sigurnost kriptiranih dokumenata ovisi o tome koji se algoritam koristi za kriptiranje te duljini kriptografskih ključeva. Napadači mogu provesti kriptoanalizu teksta kojeg žele dekriptirati.

IPSec protokol

TCP/IP je skup protokola koji je de facto prihvaćen kao standard za mrežnu komunikaciju u većini današnjih računalnih mreža. Internet, kao "mreža svih mreža", također koristi TCP/IP stog protokola. Trenutno se TCP/IP stog protokola bazira na IPv4 (IP protokol inačice 4) protokolu, iako već dulje vrijeme postoji i IPv6 (IP protokol inačice 6), koji bi trebao ispraviti neke inherentne nedostatke u IP protokolu i unaprijediti mrežnu komunikaciju. Jedan od

osnovnih nedostataka TCP IP stoga protokola u svom izvornom obliku jest nepostojanje nikakvih mehanizama kojima bi se osigurala zaštita i integritet podataka u prijenosu i izvršila autentikacija strana u komunikaciji.

IPSec (eng. IP Security), je skup proširenja IPv4 protokola kojim se osiguravaju osnovni sigurnosni aspekti mrežne komunikacije, a to su: tajnost, integritet, autentikacija i neporecivost.40 S tim da valja napomenuti da IPSec, osim što proširuje IPv4 koji se trenutno koristi, dolazi i kao integralni dio IPv6 protokola. Obzirom da se integrira s IP protokolom, IPSec implementira sigurnu mrežnu komunikaciju na trećem, odnosno mrežnom sloju (eng. network layer) ISO OSI toga protokola, tj. u internet sloju, ukoliko se promatra TCP/IP stog. Naravno, sigurnost je moguće implementirati i u drugim slojevima, od fizičkog do aplikacijskog sloja (SSH, SSL/TLS). Svaka od implementacija ima svoje prednosti i nedostatke.

LITERATURA

B. Đorđević, D. Pleskonjić, N. Maček, "Operativni sistemi: UNIX i Linux", Viša

elektrotehnička škola, Beograd, 2004.

Čagalj, M. (2006) Sigurnost u bežičnim računalnim mrežama, Fakultet elektrotehnike, strojarstva i brodogradnje, Split.

Darko A; Osnovna mrežna terminologija, (2010).

Eugene B; Uvod u podatkovne komunikacije.(1999).

Ilišević, S; Brzi vodič kroz kućen mreže, BUG & SysPprint, Zagreb, (2003).

Jušić, S. Sigurnost web aplikacija. Komunikacijske tehnologije i norme u informatici. (2003).

M. Bojović, "Squid proksi server", diplomski rad, Viša elektrotehnička škola, Beograd, (2005).

Milan K; i Dario C; Uvod u računalne mreže, Zagreb, (2014).

Mužić, V: Metodologija pedagoškog istraživanja, Svjetlost, Sarajevo, (1982).

M. Živković, "Algoritmi", Matematički fakultet, Beograd, (2000).

Olivier B; Umrežavanje računala: principi, protokoli i praksa. (2011).

Pralas, T. (2004) Računalne mreže – pasivna i aktivna oprema, Sys portal, Carnet, Zagreb.

Randić M. (2010) Upravljanje mrežom i uslugama, Fakultet elektrotehnike i računarstva, Zagreb.

Sinković, V. Informacijske mreže, Školska knjiga, Zagreb (1994).

Srdić, Ida, Hrpka, Branko, K; Goran, Udžbenik iz informatike, ALFA d.d., Zagreb, (2007).

Škundrić, S., Sok, A. (2007) Analiza računalne mreže na tehničkom fakultetu u Rijeci, Tehnički Fakultet, Rijeka.

Toni P;, Računalne mreže – OSI referentni model, (2008).

V. Vasiljević, P. Gavrilović, B. Krneta, M. Krstanović, N. Maček, B. Bogojević,"Priručnik za administraciju računarskih mreža", Viša elektrotehnička škola, Beograd, (2004).

COMPUTER NETWORK SECURITY

Marijan Mijatović, PhD

Summary
The computers that we connect to the network serve to exchange data that is in the computer's working memory. The data transmission itself can also be carried out using electronic signals, and these connections can be wireless networks and wired networks. Bits that send one after another at the same time at the appropriate speed, and convert a digital signal into an analog signal and vice versa perform a modem. Computers can also be connected to both a local network and an extensive network. Each computer connected to the network has its own unique number (address), by which it can be determined on which continent it is located, in which country and to which address the server is connected to. The data is sent in accordance with the previously agreed protocol in the form of a package. The security of protecting confidential data and documents has existed in the world for a long time. Throughout history, there have been many methods of data protection and Internet security. The methods of protection on the Internet were sometimes ineffective and did not provide enough protection that was needed. With the development of cryptography and technology, very good ways of encrypting and protecting documents have been discovered. Information systems are the basis of basic and modern business. Their main task is to base themselves on a Network System, as well as their business and security. Therefore, it is extremely important that we become as familiar as possible with the security problems of computer networks and ways to solve them. Modern computer networks are increasingly based on the TCP-IP protocol, thanks to the simple identification of device addresses on the network and the ability to connect to the Internet and use its network services. Security system protection planning is based on studying known threats and proposing solutions as a result of compromises. But effective protection implements not only one solution, but also a combination of many other options for network protection and security. In this article, we will briefly consider the general system of networks, as well as their security, occurrence and separation.
Keywords: networks, protocols, packets, LAN, antivirus, cryptography.