SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Tomislav Šoštarić

SIGURNOST I ZAŠTITA RAČUNALNIH MREŽA

ZAVRŠNI RAD

U Zagrebu, rujan 2016.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 26. svibnja 2015.

Zavod: Zavod za informacijsko komunikacijski promet
Predmet: Računalne mreže

ZAVRŠNI ZADATAK br. 2275

Prvostupnik: **Tomislav Šoštarić (0035164004)**
Studij: Promet
Smjer: Informacijsko – komunikacijski promet

Zadatak: **Sigurnost i zaštita računalnih mreža**

Opis zadatka:

Opisati metode napada na računalne sustave te odgovarajuće mehanizme zadatka.

Zadatak uručen pristupniku: 25. ožujka 2015.

Mentor: Predsjednik povjerenstva za završni ispit

_____ _____

prof. dr. sc. Zvonko Kavran

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

SIGURNOST I ZAŠTITA RAČUNALNIH MREŽA (COMPUTER NETWORK SECURITY)

ZAVRŠNI RAD

Mentor: prof. dr.sc. Zvonko Kavran

Kandidat: Tomislav Šoštarić

Datum obrane: 13. rujna 2016.

Sažetak

Računalna je mreža sustav koji povezuje različite ili slične uređaje u jednu cjelinu. Upravljanje mrežom podrazumijeva pravilnu konfiguraciju, povezivanje i nadzor elemenata mreže. Održavanje računalnih mreža složen je i zahtjevan posao jer računalo povezano na računalnu mrežu nije više izolirani sustav, nego je podložno interakciji drugih sustava. Današnje se računalne mreže sve više temelje na TCP/IP skupu protokola zbog jednostavnog definiranja adresa uređaja na mreži te zbog mogućnosti povezivanja na Internet i korištenje njegovih mrežnih usluga. Planiranje zaštite sustava temelji se na ispitivanju poznatih prijetnji te prijedloga rješenja kao rezultat kompromisa. Malware je zajednički naziv za softver koji je izrađen specifično sa svrhom infiltracije ili oštećenja računalnog sustava. Vrste malwarea su spyware, adware, trojanci, crvi i virusi. Mnogi sigurnosni mehanizmi, kao što su antivirusni programi, sigurnosni protokoli mreža računala, kontrola pristupa, kriptiranje i vodeni žigovi mogu se upotrijebiti za zaštitu dokumenata. No efikasna zaštita ne primjenjuje samo jedno rješenje, već kombinaciju u ovom radu spomenutih metoda zaštite.

Ključne riječi: Računalna mreža, zaštita sustava, malware, antivirusi, sigurnosni protokoli

Summary

Computer network is a system that connects different or similar devices into a single unit. Network management includes proper configuration, connectivity and control of network elements. Computer networks maintenance is a complex and demanding job as a computer connected to a computer network is no longer an isolated system, but subject to the interaction of other systems. Today's computer networks are increasingly based on the TCP / IP set of protocols because of simplier definition of the device network address and because of the possibility of connecting to the Internet to use its online services. Planning protection system is based on examination of all known threats and proposed solutions as a result of a compromise. Malware is the common name for all software that was created specifically for the purpose of infiltration or damaging computer systems. The types of malware are Spyware, Adware, Trojans, Worms and Viruses. Many security mechanisms, such as Antivirus programs, computer networks security protocols, access control, encryption and watermarks can be used to protect documents. Effective protection does not mean applying only one solution, but a combination of different methods of protection.

Keywords; Computer network, system protection, malware, antivirus, security protocols

SADRŽAJ

1. UVOD

Računalna je mreža sustav koji povezuje različite ili slične uređaje u jednu cjelinu. U telekomunikacijskom i podatkovnom smislu, mreža povezuje uređaje za obradu podataka i komunikacijske uređaje, bilo na međudržavnom planu, unutar pojedine zemlje, grada, u industrijskom postrojenju, poslovnim zgradama ili u malom uredu.

Potreba za umrežavanjem posljedica je stalnog porasta razmjene podataka (pisama, poruka, memoranduma, poslovne statistike, izvještaja, baza podataka i sl.) među zaposlenima. Izračunato je da se oko 60 % radnog vremena koristi za komunikaciju ili razmjenu podataka; u današnje vrijeme količina tako razmijenjenih informacija dosiže i do 35 otipkanih stranica po osobi dnevno. Za uštedu su vremena napravljeni razni uređaji namijenjeni komunikaciji i razmjeni podataka (teleks, telefaks, osobna računala, pisači, višefunkcijski terminali), a sada ih sve treba povezati u računalnu mrežu da bismo svi zajedno dijelili mogućnosti koje nam ti uređaji pružaju.

Upravljanje mrežom podrazumijeva pravilnu konfiguraciju, povezivanje i nadzor elemenata mreže: računala (osobnih i poslužitelja) i komunikacijske opreme (zvjezdišta, pojačala, premosnika, prospojnika, poveznika). Uz sklopovsku osnovicu, upravljanje mrežom obuhvaća instalaciju, konfiguriranje i održavanje programske podrške (sistemske i aplikacijske), te brigu o korisnicima mreže i njihovim podacima. Cilj upravljanja i održavanja jest pouzdana, modularna i sigurna računalna mreža. Upravljanje i održavanje računalne mreže obavlja administrator mreže.

Prednost koju korisnicima pruža povezivanje u računalnu mrežu jest otvorenost prema drugim računalima i drugim mrežama, te mogućnost pristupa informacijama bez obzira na fizičku razdvojenost. Računalnoj opremi moguće je pristupiti s brojnih i udaljenih lokacija koje najčešće uopće nisu pod nadzorom vlasnika ili administratora računala. Iz tog je razloga puno zahtjevnija i ozbiljnija zadaća zaštiti umreženi, nego izolirani, nepovezani sustav. Osnovni ciljevi zaštite sustava jesu osigurati konzistentnost i funkcionalnost sustava, te integritet i pouzdanost podataka. Mjere zaštite sustava često uvode dodatne restrikcije, što može utjecati na smanjivanje dostupnosti ili kvalitete usluga. Razina zaštite sustava najčešće je kompromis potreba korisnika za zaštitom vlastitih podataka i slobode pristupa uslugama sustava.

Planiranje zaštite sustava temelji se na ispitivanju poznatih prijetnji, te prijedloga rješenja kao rezultat kompromisa. Sustav se štiti od aktivnosti nedobronamjernih osoba koji mogu, ali ne moraju biti ovlašteni korisnici resursa lokalne mreže, kao i od nedovoljno upućenih ili neobrazovanih korisnika čije pogreške mogu na bilo koji način ugroziti rad sustava. Potrebno je zaštiti mrežnu opremu, poslužitelje, radne stanice i podatke korisnika. Bitna činjenica u planiranju zaštite sustava jest temeljnost mrežnih usluga na modelu klijent – poslužitelj.

Svrha ovog rada je objasniti da sigurnost mreže znači osigurati konzistentnost i funkcionalnost sustava, te integritet i pouzdanost podataka, a zaštita mreže znači zaštitu od aktivnosti nedobronamjernih osoba koji mogu, ali ne moraju biti ovlašteni korisnici resursa lokalne mreže, kao i od nedovoljno upućenih ili neobrazovanih korisnika čije pogreške mogu na bilo koji način ugroziti rad sustava. Cilj ovog rada je u koracima objasniti mrežnu arhitekturu interneta te organizaciju lokalne mreže, a onda identificirati prijetnje računalnim mrežama da bi se moglo naposljetku navesti načine osiguranja i zaštite računalnih mreža.

Naslov rada je Sigurnost i zaštita računalnih mreža, a struktura je u pet poglavlja:

1. Uvod
2. Analiza zahtjeva rada računalne mreže
3. Prijetnje računalnim mrežama
4. Načini osiguranja računalne mreže
5. Zaključak.

Prvo poglavlje je uvod u rad. U drugom poglavlju su opisana mrežna arhitektura interneta i organizacijska struktura lokalne mreže kao elementi mreže, a upravljanje mrežom podrazumijeva pravilnu konfiguraciju, povezivanje i nadzor elemenata mreže. Treće poglavlje obuhvaća modeliranje prijetnji, inženjersku tehniku koja se koristi za identificiranje prijetnji, napada, ranjivosti i odgovarajućih protumjera u kontekstu promatrane aplikacije. Također, u trećem poglavlju su nabrojeni zloćudni softveri - računalni programi koji se pokreću na računalnom sustavu bez stvarnog korisnikovog pristanka i imaju neku vrstu nepoželjnog učinka, kao što je oštećenje programa i podataka koji se nalaze na sustavu, širenje na druga računala, krađa podataka itd. Četvrto poglavlje govori o načinima osiguranja računalnih mreža kao što su antivirusni programi, sigurnosni protokoli mreža računala (npr. IPSec), kontrola pristupa, kriptiranje, i vodeni žigovi te o trendovima u području zaštite zbog sve većeg značaja mobilnih komunikacija. Peto poglavlje je zaključak.

2. ANALIZA ZAHTJEVA RADA RAČUNALNE MREŽE

Računalna mreža služi povezivanju računala i drugih hardverskih uređaja preko komunikacijskih kanala da bi se korisnicima olakšala komunikacija i razmjena resursa. Računalna mreža je skupina dva ili više međusobno povezanih računala koji dijele neke resurse (podatke, sklopovlje, programe).[1] Računala se smatraju povezanima ako mogu razmjenjivati informacije. Krajnjim korisnicima priključak na mrežu pruža ove mogućnosti[2]:

a) dijeljenje datoteka
b) dijeljenje hardverskih resursa, poput skenera i pisača
c) korištenje brojnih usluga poput e-pošte, videokonferencije, istovremenih poruka, World Wide Weba, društvenih mreža itd.
d) lakši pristup i održavanje informacija među umreženim korisnicima itd.

Postoje različite mogućnosti za povezivanje na mrežu, dvije su osnovne skupine tehnologija uspostavljanja telekomunikacijskih veza: materijalne ili ožičene veze i bežične telekomunikacijske veze.[3] U slučaju povezivanja preko kabela najpoznatije su varijante povezivanja preko klasične telefonske linije i analognih modema te preko digitalne telefonije i kabelskog interneta, a u slučaju bežičnog povezivanja najpoznatija je varijanta povezivanja preko elektromagnetskih valova, koja je najširu primjenu našla u uspostavi lokalnih računalnih mreža bez žica (WLAN). Za bežično povezivanje moguće je koristiti se i mobilnim uređajima različitih generacija (2G, 3G, 4G ili LTE).

2.1. Upravljanje i održavanje računalnih mreža

Upravljanje mrežom podrazumijeva pravilnu konfiguraciju, povezivanje i nadzor elemenata mreže. Upravljanje mrežom u užem smislu odnosi se na upravljanje komunikacijskim mrežama. U širem smislu predstavlja sveobuhvatno upravljanje mrežama, krajnjim sistemima koji su spojeni na mreže i procesima i aplikacijama koji se izvode na

[1] Wikipedia, Računalne mreže, dostupno online: https://hr.wikipedia.org/wiki/Ra%C4%8Dunalne_mre%C5%BEe (preuzeto 29.08.2016.)
[2] Ćukušić, M., Jadrić, M. (2015) Priručnik za polaznike © 2015 Srce, Sveučilište u Zagrebu, Sveučilišni računski centar, Zagreb, str. 47
[3] Ibid.

sistemima te brigu o korisnicima mreže i njihovim podacima.[4] Upravljanje i održavanje računalne mreže obavlja administrator mreže.

Mrežna komunikacijska oprema koja radi na nižim razinama komunikacijskog modela uglavnom ne zahtjeva konfiguriranje niti upravljanje, već funkcionalna postaje spajanjem u mrežu. Jedna od definicija navodi da aktivnu mrežnu opremu sačinjavaju svi elektronički uređaji koji prihvaćaju i distribuiraju promet unutar računalnih mreža (imaju memoriju i procesor), dok pasivnu mrežnu opremu sačinjava žični sustav (bakar i optika) koji služi za povezivanje aktivne opreme.[5] Pasivna oprema se sastoji od kablova, konektora, razvodnog panela (patch panel, switching panel, punch-down panel), komunikacijskih ormara i sustava za napajanje električnom energijom (vodovi, sklopke i naponske letve, sustav za hlađenje)

Uređaji na mreži međusobno se razlikuju po svojim jednoznačno definiranim adresama, bez obzira na veličinu i zemljopisnu rasprostranjenost mreže kojoj pripadaju. Kod TCP/IP skupa protokola na kojem je zasnovana danas jedina svjetska računalna mreža Internet, adresiranje uređaja povezanih na mrežu (računala, prospojnika, usmjernika i poveznika) realizira se primjenom brojčanih IP adresa i naziva, između kojih postoji jednoznačno preslikavanje.

Upravljanje i održavanje na višim razinama komunikacijskog modela stoga se svodi na pravilnu konfiguraciju poslužničkih i korisničkih programa za odgovarajuće mrežne usluge, te njihov sukladan rad s instaliranim operacijskim sustavom. Mrežne usluge na računalnim mrežama većinom su zasnovane na modelu klijent – poslužitelj. Pojam poslužitelj može se odnositi na program instaliran na računalu koji ispunjava zahtjeve upućene od strane korisnika, drugih računala ili uređaja, na specijalizirani hardverski uređaj koji obavlja iste te funkcije ili na računalo na kojem su instalirani poslužiteljski programi i koje se ne koristi za rad u klasičnom smislu.[6] Poslužitelj je ključni dio računarskog koncepta klijent – poslužitelj. Prema ovom konceptu posao koji se obavlja na računalnom sistemu raspoređuje se na poslužitelja koji pruža usluge, podatke ili resurse i klijent koji te usluge, podatke ili resurse zahtijeva. Ova arhitektura zahtijeva da između klijenta i poslužitelja postoji veza. Klijent je

[4] Randić M. (2010) Upravljanje mrežom i uslugama, Fakultet elektrotehnike i računarstva, Zagreb, dostupno online: https://www.fer.unizg.hr/_download/repository/UMU_Skripta.pdf (preuzeto 29.08.2016.)
[5] Pralas, T. (2004) Računalne mreže – pasivna i aktivna oprema, Sys portal, Carnet, dostupno online: https://sysportal.carnet.hr/node/374 (preuzeto 30.08.2016.)
[6] Wikipedia, Poslužitelj, dostupno online: http://www.vidipedija.com/index.php?title=Poslu%C5%BEitelj (preuzeto 30.08.2016.)

program i/ili računalo koje mora biti u stanju postaviti zahtjev za podacima poslužitelju koji ih posjeduje, prihvatiti odgovor poslužitelja i primljene podatke prikazati na zaslonu korisniku.

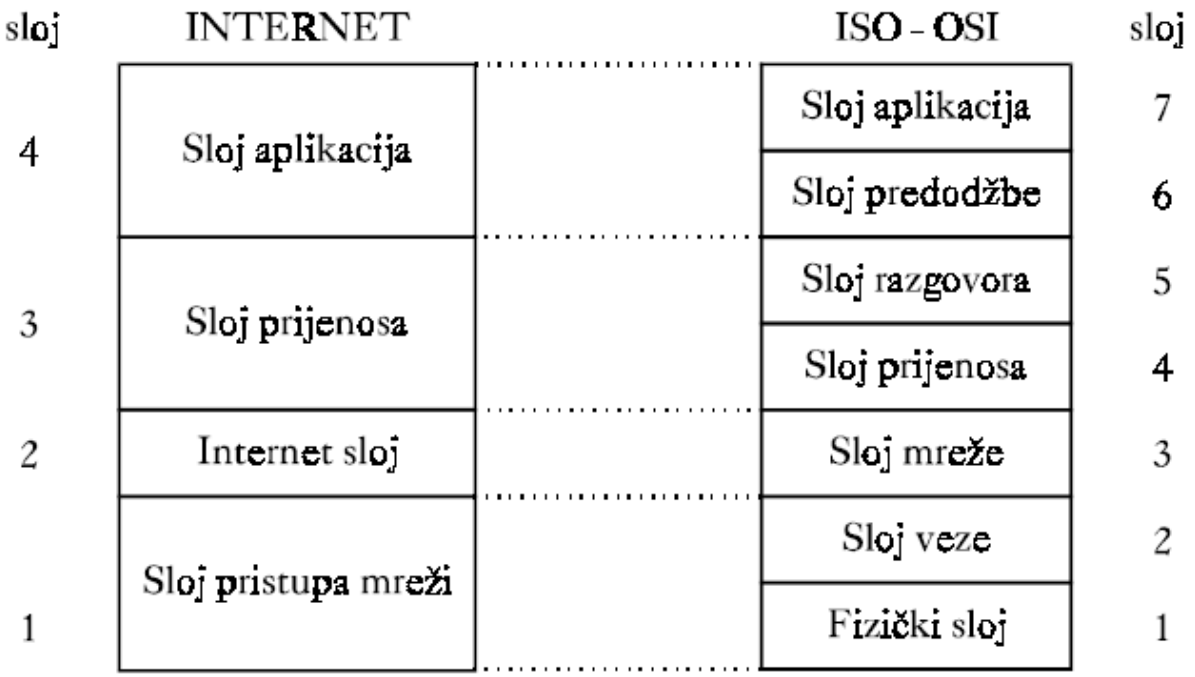
Klijent i poslužitelj komuniciraju putem protokola odgovarajuće usluge. Protokol je skup pravila koje moraju poštivati dvije strane kako bi komunikaciju uspostavile, održale određeno vrijeme potrebno za prijenos podataka i prekinule. Najpoznatije mrežne usluge na Internetu zasnovane na modelu klijent – poslužitelj s odgovarajućim protokolima su: Telnet (za pristup udaljenom računalu), FTP (File Transfer Protocol) za prijenos datoteka između dva računala, POP3 i SMTP za razmjenu elektroničke pošte, HTTP (HyperText Tranfer Protocol) za prijenos WWW stranica itd.

Održavanje računalnih mreža složen je i zahtjevan posao jer računalo povezano na računalnu mrežu nije više izolirani sustav, nego podložno interakciji drugih sustava - računala, korisnika i mreža. Posao kojeg mrežni administrator obavi na jednom računalu može utjecati na druge sustave u mreži.

2.2. Mrežna arhitektura interneta (TCP/IP)

OSI-model ili referentni model za otvoreno povezivanje sustava je najkorišteniji apstraktni opis arhitekture mreže. Opisuje komunikaciju sklopovlja, programa, software-a i protokola pri mrežnim komunikacijama. Koriste ga proizvođači pri projektiranju mreža, kao i stručnjaci pri proučavanju mreža. OSI model dijeli arhitekturu mreže u sedam logičkih razina. Postoji više rješenja realizacije lokalnih mreža za međusobnu komunikaciju korisnika na lokalnim mrežama, prijenos ili zajedničko korištenje podataka i mrežne opreme. To omogućavaju protokoli IPX Novell mreže, te Microsoftov NETBEUI, ali se sve više napuštaju zbog slabe kooperativnosti s operacijskim sustavima drugih proizvođača. Današnje se računalne mreže sve više temelje na TCP/IP skupu protokola, u prvom redu zbog jednostavnog definiranja adresa uređaja na mreži, te zbog mogućnosti povezivanja na Internet i korištenje njegovih mrežnih usluga. Njegov naziv potječe od dva najčešće korištena protokola – TCP (Transmission Control Protocol) i IP (Internet Protocol).

Za razliku od OSI modela koji ima sedam razina, TCP/IP model definira pojedine funkcije komunikacijskog modela kroz četiri razine (Slika1.).



Slika 1. - Usporedba ISO OSI i TCP/IP modela

Izvor: Ozgović, J. (2000) „5. Upravljanje i održavanje računalnih mreža“ u: Projektiranje i upravljanje računalnim mrežama – skripta

Svaka razina ne znači nužno jedan protokol, nego može biti predstavljena većim brojem protokola od kojih svaki definira i ostvaruje neku od funkcija[7]:

a) razina pristupa mreži (Network Access Layer)
b) mrežna razina (Internet Layer)
c) prijenosna razina (Transport Layer)
d) korisnička razina (Application Layer)

Kao i kod OSI modela, podaci se prosljeđuju od viših razina prema nižim kad se šalju u mrežu, a od nižih prema višim kad se primaju iz mreže. Svaka razina dodaje svoje zaglavlje na podatke koje primi od prve više razine, a koji sadrže izvornu poruku i zaglavlja prethodnih

[7] Ozgović, J. (2000) „5. Upravljanje i održavanje računalnih mreža“ u: Projektiranje i upravljanje računalnim mrežama – skripta, Fakultet elektrotehnike, strojarstva i brodogradnje, Sveučilište u Splitu, Split, str. 55

razina. Pri prihvatu podataka s mreže, svaka razina odvaja njoj upućeno zaglavlje, obrađuje primljene informacije i sukladno njima podatke prosljeđuje sljedećoj višoj razini.

Razina pristupa mreži, najniža razina TCP/IP arhitekture, obavlja funkcije prve dvije razine ISO OSI modela i odgovorna je za realizaciju komunikacije između dva uređaja u mreži. Podatke primljene od druge, mrežne razine prilagođava fizičkom mediju vodeći računa o svojstvima mrežnih uređaja. Na ovoj se razini IP paket s druge razine postavlja u okvire koji se šalju preko mreže, te se obavlja preslikavanje IP adrese uređaja na mreži u njegovu fizičku adresu. Protokoli prve razine TCP/IP modela su[8]:

- Ethernet protokol kojim je definirano povezivanje lokalnih mreža zasnovanih na različitim tipovima fizičkog medija, pri različitim brzinama prijenosa, uz četiri formata Ethernet okvira trenutno u primjeni (Ethernet II, Ethernet 802.3, Ethernet 802.4 i SNAP Ethernet).
- SLIP (Serial Line Internet Protocol), RFC 1055 - de facto standard za prijenos IP paketa preko modemskih veza koje podržavaju TCP/IP protokol
- PPP (Point to Point Protocol), RFC 1548 - standard za prijenos podataka preko modemskih veza

Mrežna razina TCP/IP modela Interneta omogućava uspostavu logičke veze između dva uređaja koja žele komunicirati. Osnovni protokol te razine je IP (Internet Protocol, RFC 791). Uređaji se prepoznaju preko 32-bitnih IP adresa koje imaju dva dijela: mrežni broj i broj računala. Mrežna razina prenosi podatke unutar TCP/IP modela, tj. prihvaća ih od razine pristupa mreži i predaje prijenosnoj razini, izdvajajući i analizirajući svoje zaglavlje. Osnovna jedinica podataka na ovoj razini jest paket. Osim IPa, među osnovne protokole mrežne razine ubrajaju se i[9]:

- ICMP (Internet Control Message Protocol, RFC 792)
- ARP (Address Resolution Protocol), RFC 826 - protokol za određivanje adresa koji IP adresu zamijeni Ethernet adresom kartice, tj. fizičkom adresom
- RARP (Reverse Address Resolution Protocol), RFC 903 - Ethernet adresu zamijeni IP adresom; primjenjuju ga računala bez čvrstih diskova za doznavanje vlastite IP adrese prilikom inicijalizacije

[8] Ozgović, J. (2000) „5. Upravljanje i održavanje računalnih mreža“ u: Projektiranje i upravljanje računalnim mrežama – skripta, Fakultet elektrotehnike, strojarstva i brodogradnje, Sveučilište u Splitu, Split, str. 55
[9] Ibid.

- DHCP (Dynamic Host Configuration Protocol), RFC 1531 - omogućava dinamičku dodjelu raspoloživih IP adresa uređajima na mreži.

Prijenosna razina osigurava prijenos paketa između bilo koje dvije krajnje točke mreže. Na ovoj razini radi se kontrola toka i kontrola pogreški. Ona predstavlja vezu između mrežne razine i aplikacijske razine. Mrežna razina iz svog zaglavlja saznaje kojem protokolu prijenosne razine mora predati podatke, a prijenosna razina na osnovu podataka u svom zaglavlju prosljeđuje podatke točno određenoj usluzi aplikacijske razine. Adresiranje na prijenosnoj razini obavljeno je brojem priključne točke (engl. port) za svaku pojedinu uslugu. Dva osnovna načina prijenosa podataka ove razine su[10]:

- Uspostavom logičkog kanala
- Bez uspostave logičkog kanala

Prijenos podataka uspostavom logičkog kanala (tzv. spojevni) - osigurava pouzdanu isporuku podataka do odredišta uz što manje gubitke i što manje pogrešaka. Primjenjuje se kod prijenosa podataka kod kojih je važno potvrditi da su pravilno isporučeni odredištu. Prijenos podataka bez uspostave logičkog kanala (tzv. bespojni) - Primjenjuje se kod prijenosa podataka koji mogu podnijeti određene gubitke (npr. video ili VoIP). Dva najznačajnija protokola prijenosne razine su[11]:

- TCP (Transmission Control Protocol), definiran RFC-om 793, spojevni protokol, uključeni su mehanizmi za detekciju i korekciju pogrešaka
- UDP (User Datagram Protocol), definiran RFC-om 768, bespojni protokol bez mehanizama za detekciju i korekciju pogrešaka.

Korisničku razinu čine programi i procesi koji svoje zahtjeve ili podatke predaju izravno protokolima prijenosne razine. TCP podržava neke od najčešće korištenih aplikacijskih protokola na Internetu, kao što su HTTP (protokol za pregled web stranica), SMTP (protokol za razmjenu elektroničke pošte), telnet i SSH (protokole za udaljeni rad na računalu) i brojne druge[12].

[10] Mujarić, E., Prijenosna razina, dostupno online: http://mreze.layer-x.com/s040000-0.html (preuzeto 29.08.2016.)
[11] Ibid.
[12] Wikipedia, TCP, dostupno online: https://hr.wikipedia.org/wiki/TCP (preuzeto 06.09.2016.)

HTTP je request/response protokol za komunikaciju između poslužitelja (servera) i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web serverom na određenom portu. SMTP (Simple Mail Transfer Protocol), protokol za prijenos elektroničke pošte, definira slanje pošte lokalnog računala bilo kojem računalu u mreži, te prijem pošte upućene računalu u lokalnoj mreži i njeno prosljeđivanje lokalnim programima za obradu pristigle pošte. Telnet je mrežni protokol unutar IP grupe protokola koji se koristi na Internetu ili u lokalnim mrežama. Namjena ovog protokola je uspostava dvosmjernog 8-bitnog komunikacijskog kanala između dva umrežena računala. Najčešće se koristi da osigura korisniku jednog računala sesiju za korištenje tzv. sučelja komandne linije na drugom računalu. Sam naziv protokola dolazi od kratice engleskog naziva TELephone NETwork iz kojeg se vidi da je protokol dizajniran s namjerom povezivanja jednog terminala na udaljeno računalo. SSH (Secure Shell) je mrežni protokol koji korisnicima omogućuje uspostavu sigurnog komunikacijskog kanala između dva računala putem nesigurne računalne mreže. SSH protokol svoj rad bazira na korištenju kombinacije simetrične i asimetrične kriptografije, metode enkripcije koja omogućuje sigurniji prijenos podataka računalnom mrežom.

Protokoli druge skupine koriste UDP. Oni često obavljaju funkcije koje se izvršavaju neovisno o aplikacijama korisnika i za koje korisnik ne mora ni znati, a potrebne su za rad mreže. Takvi su protokoli DNS, DHCP, TFTP, SNMP, RIP, VOIP itd. DNS (Domain Name Service) je hijerarhijsko raspoređeni sustav imenovanja za računala, servise ili bilo koje sredstvo spojeno na Internet ili privatnu mrežu. On povezuje različite informacije s domenskim imenima pripisanim svakom od subjekata u domeni. Ponajprije, prevodi lako pamtljiva domenska imena u numeričke IP adrese koje su potrebne za lociranje računalnih servisa i uređaja širom svijeta. Omogućujući globalno raširenu usmjeravanje prema ključnim riječima, DNS je osnovni element funkcionalnosti Interneta.

DHCP (Dynamic Host Configuration Protocol) mrežni je protokol korišten od strane mrežnih računala za dodjeljivanje IP adresa i ostalih mrežnih postavki kao što su pretpostavljeni gateway, subnet maska i IP adrese DNS servera s DHCP servera. Olakšava konfiguraciju mreže jer eliminira ručno dodavanje osnovnih postavki za jednu računalnu mrežu. DHCP server osigurava da su dodijeljene IP adrese ispravne i da u mreži nema sukoba adresa. VoIP je skraćenica od eng. složenice Voice over Internet Protocol i ime je za komunikacijsku tehnologiju koja omogućava prijenos zvučne komunikacije preko internetske

mreže. Tehnologija je postala popularna razvojem širokopojasnog interneta, jer u većini slučajeva omogućava besplatno telefoniranje s računala na računalo te jeftinije telefoniranje s računala na mobitele i fiksnu liniju.

Oba protokola prijenosne razine, a time i obje skupine aplikacija korisničke razine koriste IP i/ili ICMP protokole na mrežnoj razini. Protokoli ne moraju nužno koristiti TCP ili UDP. Takav je EGP (Exterior Gateway Protocol, RFC 904) – protokol vanjskog poveznika koji definira povezivanje dva međusobno neovisna sustava s vlastitom upravom (autonomous systems).

2.2.1. Topološka struktura Interneta

Internet je svjetska računalna mreža organizirana kao skupina podmreža različitih karakteristika povezanih TCP/IP skupom protokola. Računala jedne ustanove povezana su lokalnom mrežom koja se može prostirati na jednoj ili više lokacija, projektiranom da ispunjava funcionalne i druge zahtjeve ustanove. Takva lokalna mreža ima svoje područje mrežnih adresa i naziva, koje ju jednoznačno definira u svom gradu, zemlji i svijetu, neovisna je o drugim mrežama i čini neovisni ili autonomni sustav (AS - autonomous system). Više takvih neovisnih sustava u Internet povezuju pružatelji Internet usluga (ISP - Internet Service Providers). U jednoj državi obično ima nekoliko ISPova koji mogu udruženo ili posebno ostvariti međunarodnu vezu prema Internetu posredstvom neke od međunarodnih organizacija.

Osnovnu topološku strukturu Interneta čine podmreže formirane logički (zemljopisno i/ili prema ustroju), adresno (prema veličini mreža i mrežnim klasama) te infrastrukturno (kao jedna domena prostiranja okvira s univerzalnim adresama na podatkovnoj razini).[13] Postoje mreže zasnovane na TCP/IP skupu protokola koje nisu povezane na Internet i koje ne žele biti dio Interneta, osim možda, koristiti neku od mrežnih usluga Interneta. Takve mreže mogu biti realizirane kao privatne, ili na principu intraneta. U drugom slučaju, cijela se mreža prema drugima predstavlja preko jedne IP adrese. Za takve mreže preporučljivo je koristiti neko od rezerviranih područja adresa.

[13] Ozgović, J. (2000) „5. Upravljanje i održavanje računalnih mreža“ u: Projektiranje i upravljanje računalnim mrežama – skripta, Fakultet elektrotehnike, strojarstva i brodogradnje, Sveučilište u Splitu, Split, str. 57

2.3. Organizacija lokalne mreže

Izvorna ideja mreže razvijena je prema slijedećem načelu: „Domaćin (host) korisničke programske potpore bilo je jedno glavno računalo uobičajeno nazivano Mainframe, vrlo veliko po gabaritima, koje je u osnovi imalo nekakav unix-oidni operativni sustav. S njim su komunicirale Radne postaje (RP) povezane preko prikladnog ožičenja, koje su u takvoj mreži predstavljale jedan čvor (node) mreže. Radne postaje komunicirale su s glavnim računalom na način da su preko tipkovnice host-u zadavani radni nalozi, a on je rezultate vraćao korisniku na monitor. Radne postaje nazivale su se Terminal ili WorkStation i u osnovi ih je za rad opsluživao host - poslužitelj. Način povezivanja čvorova, odnosno veze između radnih postaja i host-a određivao je tip mreže i osnovni tipovi povezivanja u mreži su: zvijezda (arcnet), sabirnica (ethernet) i prsten (token ring).[14]

2.3.1. Spajanje računala u mrežu

Uključivanje računala u mrežu zahtjeva dodatni vezni sklop, te promjenu konfiguracije programske podrške. Računalo može biti priključeno na mrežu, jedino ako posjeduje mrežnu karticu (NIC - network interface card). Mrežna kartica se ugrađuje u računalo, a ima svoju jedinstvenu MAC adresu. Na odabir mrežne kartice može, ali ne mora, utjecati postojanje i način izrade lokalne mreže. NICu treba podesiti[15]:

- prekidni broj (interrupt number)
- memorijsku adresu (I/O address)

Najčešće se to podesi automatski (pogotovo kod novih operacijskih sustava), a tamo gdje to nije tako, parametre treba odabrati na osnovu slobodnih vrijednosti. U tome mogu pomoći odgovarajući dijagnostički programi za mrežne kartice koji se isporučuju s driverima. Operacijski sustav mora imati podršku za protokol ili skup protokola na kojem se temelji mreža. Za mreže tipa Interneta, mora postojati podrška za TCP/IP skup protokola. Tim skupom protokola danas raspolaže većina operacijskih sustava. Za one koji ne raspolažu mrežnom programskom podrškom, postoje dodatni programi čijom se instalacijom

[14] Radić, D., Topologija mreže, dostupno online: http://www.informatika.buzdo.com/s420-topologija-mreze.htm (29.08.2016.)
[15] Ozgović, J. (2000) „5. Upravljanje i održavanje računalnih mreža“ u: Projektiranje i upravljanje računalnim mrežama – skripta, Fakultet elektrotehnike, strojarstva i brodogradnje, Sveučilište u Splitu, Split, str. 81

omogućava povezivanje na mrežu. Način definiranja potrebnih parametara, preko grafičkog sučelja ili upisom u tekstualne datoteke, ovisi isključivo o tipu operacijskog sustava.

Parametri koji se upisuju kod konfiguracije računala na mrežu tipa Interneta su: IP adresa, mrežna maska, adresa uređaja koji obavlja prosljeđivanje (default gateway) i DNS - FQDN te primarni DNS poslužitelj (ili više njih). Pod Windows operacijskim sustavom sve to postavlja se na jednom mjestu (Control Panel - Networks ili nešto slično), a na UNIX sustavima je to nekoliko datoteka koje treba editirati i upisati odgovarajuće vrijednosti čiji naziv i mjesto u datotečnom sustavu ovise o tipu i verziji operacijskog sustava. Spajanje računala na mrežu obavljeno je kad je računalu konfigurirana mrežna kartica i upisani odgovarajući parametri - adresa i naziv koji moraju biti jedinstveni za svako računalo, zatim spojen kabel između mrežne kartice računala i utičnice na zidu ili priključka na zvjezdištu, te kad je odgovarajući kabelski završetak na prespojnom panelu povezan s priključkom aktivne mrežne opreme.

Dodavanje bilo kojeg uređaja u lokalnu mrežu mora se dokumentirati, kako bi u svakom postojao uvid u trenutno stanje mreže, raspoložive resurse, moguće nedostatke, dakle bitno je kako za održavanje postojeće mreže tako i za planiranje i nadogradnju mreže. Također, od ogromnog je značaja u slučaju promjena u administriranju mreže, bez obzira radi li se o promjeni opreme, radnih grupa ili angažiranog osoblja. Dokumentacija o uređaju dodanom na mrežu treba sadržavati podatke kao što su: fizička lokacija utičnice gdje je uređaj spojen (oznaka prostorije), oznaka utičnice koja mora biti u paru s oznakom na prespojnom panelu, broj priključnice na mrežnoj opremi (zvjezdištu, prospojniku), dodijeljena IP adresa, te dodijeljeni FQDN naziv.

Lokalna računalna mreža (katkad se koristi i izraz područna računalna mreža, engl. *Local Area Network*, LAN) povezuje računala i druge hardverske uređaje na manjim udaljenostima (do nekoliko stotina metara), na primjer u poslovnoj zgradi, na katu zgrade, u računalnom laboratoriju ili u stanu. Implementacija tih mreža je vrlo raširena naročito stoga što korisnicima pruža pristup perifernim uređajima (skeneri, pisači), zajedničkim bazama podataka ili pristup nekim drugim mrežama. Karakteristika LAN-a je velika brzina prijenosa podataka i komunikacije.[16]

[16] Ćukušić, M., Jadrić, M. (2015) Priručnik za polaznike © 2015 Srce, Sveučilište u Zagrebu, Sveučilišni računski centar, Zagreb, str. 48

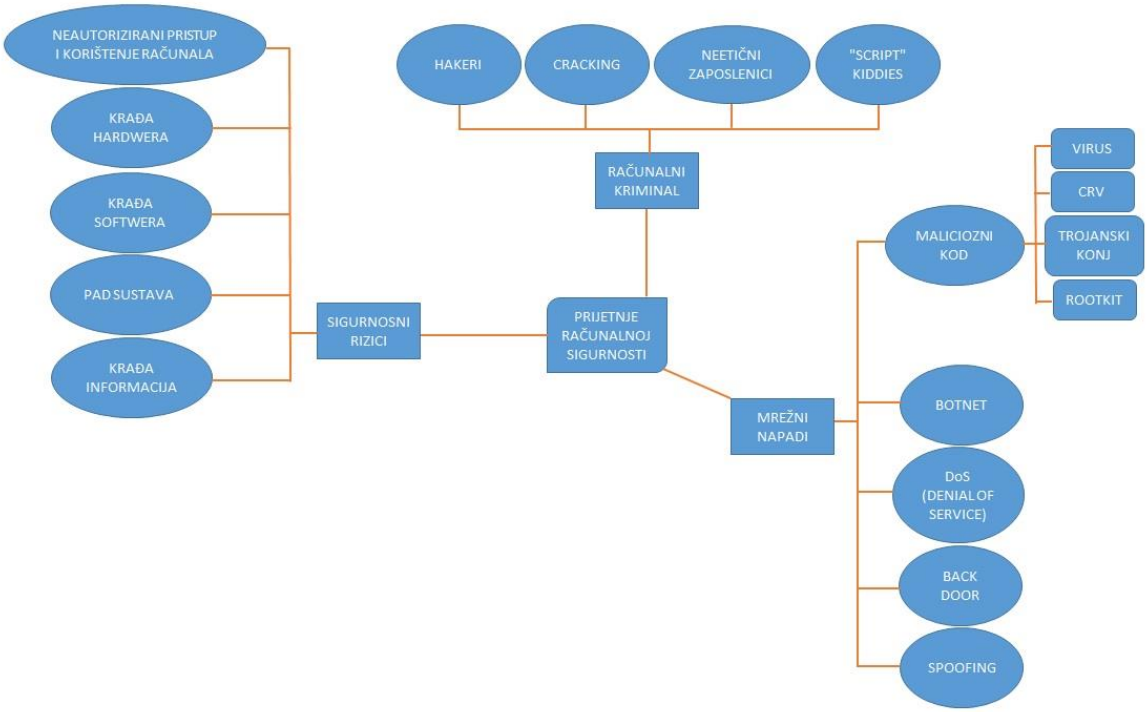
Povezivanje prostorno ili geografski udaljenih računala i drugih hardverskih uređaja krije se pod pojmom WAN (engl. *Wide Area Network*), pri čemu WAN može povezivati i različite manje mreže poput LAN-ova. Povezivanje na velikim udaljenostima najčešće se obavlja preko satelitske veze ili preko optičkih kabela, a koristi se postojeća infrastruktura LAN-ova.

Virtualna privatna mreža (engl. *Virtual Private Network*) omogućava siguran prijenos podataka preko nezaštićene javne mreže. Unutar VPN-a koriste se slična pravila kao kod lokalnih mreža, pri čemu se sigurnost prijenosa ostvaruje kombinacijom šifriranja, autentikacije i tuneliranja. Tuneliranje je tehnika prijenosa podataka namijenjenih određenoj mreži preko druge mreže, na primjer preko Interneta ili preko komunikacijske infrastrukture jednog od pružatelja internetskih usluga. Osnovna je razlika u odnosnu na privatne mreže koje se koriste vlastitim ili iznajmljenim vezama za prijenos podataka da VPN preko javne mrežne infrastrukture sigurnim kanalom spaja korisnike na različitim lokacijama.

3. PRIJETNJE RAČUNALNIM MREŽAMA

Prednost koju korisnicima pruža povezivanje u računalnu mrežu jest otvorenost prema drugim računalima i drugim mrežama te mogućnost pristupa informacijama bez obzira na fizičku razdvojenost. Računalnoj opremi moguće je pristupiti s brojnih i udaljenih lokacija koje najčešće uopće nisu pod nadzorom vlasnika ili administratora računala. Iz tog je razloga puno zahtjevnija i ozbiljnija zadaća zaštiti umreženi, nego izolirani, nepovezani sustav. Osnovni ciljevi zaštite sustava jesu osigurati konzistentnost i funkcionalnost sustava, te integritet i pouzdanost podataka. Mjere zaštite sustava često uvode dodatne restrikcije, što može utjecati na smanjivanje dostupnosti ili kvalitete usluga. Razina zaštite sustava najčešće je kompromis potreba korisnika za zaštitom vlastitih podataka i slobode pristupa uslugama sustava.

Slika 2. Prijetnje računalnoj sigurnosti



Izvor: https://www.mindomo.com/mindmap/racunalne-prijetnje-sigurnosti-71fbca5e778546c79dde1b33c0b912f0

Planiranje zaštite sustava temelji se na ispitivanju poznatih prijetnji, te prijedloga rješenja kao rezultat kompromisa. Sustav se štiti od aktivnosti nedobronamjernih osoba koji mogu, ali ne moraju biti ovlašteni korisnici resursa lokalne mreže, kao i od nedovoljno upućenih ili neobrazovanih korisnika čije pogreške mogu na bilo koji način ugroziti rad sustava (na primjer, brisanjem podataka onemogućiti rad nekog drugog korisnika na sustavu ili neke

usluge i slično). Potrebno je zaštiti mrežnu opremu, poslužitelje, radne stanice i podatke korisnika.

Bitna činjenica u planiranju zaštite sustava jest temelj mrežnih usluga na modelu klijent-poslužitelj. Poslužitelji su stalno spojeni na mrežu i pružaju usluge korisnicima na ili izvan lokalne mreže. Kako se većina podataka nalazi upravo na poslužiteljima, tako oni postaju glavna točka koju na sustavu treba štititi. Mogući ciljevi napada na sustav su[17]:

a) neovlašteni pristup podacima ili sustavu
b) promjena ili brisanje podataka
c) generiranje netočnih ili krivih podataka
d) onemogućavanje usluge (denial of service),

a postupak projektiranja zaštite sustava može se znatno olakšati ako su poznati putevi i načini na koji neki sustav može biti ugrožen. Iz tog je razloga napravljena sistematizacija mogućih prijetnji kroz nekoliko razina koje su usporedive s ISO-OSI komunikacijskim modelom, te modelom Interneta (TCP/IP).

3.1. Modeliranje prijetnji

Modeliranje prijetnji (eng. *threat modeling*) je inženjerska tehnika koja se može koristiti za identificiranje prijetnji, napada, ranjivosti te odgovarajućih protumjera u kontekstu promatrane aplikacije. Modeliranje prijetnji pomaže kod definiranja sigurnosnih ciljeva, pronalaženja relevantnih prijetnji, ranjivosti te protumjera. To je strukturirani pristup koji je znatno učinkovitiji i jeftiniji od nasumičnog primjenjivanja sigurnosnih svojstava, bez pravog poznavanja koje prijetnje pojedino svojstvo opisuje. Uz primjenu takvog lošeg slučajnog pristupa javlja se problem kako odrediti da je sustav ili aplikacija dovoljno sigurna. Zbog svega toga, za odgovarajuću zaštitu sustava potrebno je prije svega dobro poznavati i ocijeniti

[17] Ozgović, J. (2000) „5. Upravljanje i održavanje računalnih mreža“ u: Projektiranje i upravljanje računalnim mrežama – skripta, Fakultet elektrotehnike, strojarstva i brodogradnje, Sveučilište u Splitu, Split, str. 91

prijetnje. Modeliranje prijetnji nije jednokratan proces, on je usko povezan i isprepleten s fazama dizajniranja i razvoja aplikacije ili sustava.[18]

Uz identificiranje i procjenu prijetnji usredotočenu na razumijevanju arhitekture i izvedbe aplikacije, moguće je identificirati i prijetnje te odgovarajuće protumjere počevši od prijetnji koje predstavljaju najveći rizik. Kada se koristi u ranim fazama razvoja programskog rješenja, modeliranje prijetnji je od višestruke koristi programerima.

Prvo se značenje odnosi na opis sigurnosnih problema kojima dizajneri trebaju posvetiti pažnju. Drugo značenje definira modeliranje prijetnji kao skup mogućih napada koje treba uzeti u obzir za pojedini dio programa ili računalnog sustava. Često se za jedan sustav definira više različitih modela prijetnji. Pritom svaki model opisuje uzak skup mogućih napada na koje je potrebno usmjeriti pažnju. Model prijetnji može pomoći u procjeni vjerojatnosti pojavljivanja i potencijalne štete napada kao i njihovog prioriteta te se na taj način može koristiti u smanjivanju ili iskorjenjivanju prijetnji. Odnedavno je modeliranje prijetnji postalo sastavni dio SDL (eng. Security Development Lifecycle, SDL) procesa tvrtke Microsoft.[19]

Modeliranje prijetnji zasnovano je na ideji da svaki sustav ili organizacija ima vrijedne resurse koje je potrebno zaštititi. Ti resursi imaju određene slabe točke koje određene vanjske i unutarnje prijetnje mogu iskoristiti kako bi naštetile tim resursima, no istovremeno postoje i odgovarajuće sigurnosne protumjere koje ublažavaju prijetnje.

Modeliranje prijetnji omogućuje primjenu strukturiranog pristupa sigurnosti u pronalaženju i procjeni glavnih prijetnji koje potencijalno imaju najveći utjecaj na računalni sustav ili aplikaciju. Uz identificiranje i procjenu prijetnji temeljenu na razumijevanju arhitekture i metoda razvoja aplikacije, moguće je identificirati i prijetnje te odgovarajuće protumjere u logičkom poretku, počevši od prijetnji koje predstavljaju najveći rizik. Modeliranje prijetnji osigurava dobre temelje za specifikaciju sigurnosnih zahtjeva tijekom razvoja aplikacije. Kada se koristi u ranim fazama razvoja programskog rješenja, modeliranje prijetnji na više načina koristi programerima; od ovjeravanja arhitekture aplikacije, identifikacije i procjene prijetnji, pronalaženja protumjera do penetracijskog ispitivanja temeljenog na modelu prijetnji.

[18] Centar informacijske sigurnosti (2012) Modeliranje sigurnosnih prijetnji (Threat Modeling), Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, str. 4
[19] Ibid.

Modeliranje prijetnji koristi se prilikom oblikovanja aplikacije kako bi se ostvarili sigurnosni ciljevi, zatim kao pomoć u donošenju ključnih inženjerskih odluka te kako bi se smanjio rizik sigurnosnih problema koji se javljaju s razvojem sustava.

3.1.1. Pristupi modeliranju prijetnji

Postoji više pristupa modeliranju prijetnji[20]:

- pristup usredotočen na napadača (eng. attacker-centric) započinje s napadačem te procjenjuje njegove ciljeve i načine na koje ih može ostvariti. Često se razmatra i napadačeva motivacija. Ovaj pristup započinje od napadačevih ulaznih točaka u sustav ili resursa.
- pristup usredotočen na programsko rješenje (eng. software-centric) naziva se još i pristup usredotočen na sustav (eng. system-centric), dizajn (eng. design-centric) ili arhitekturu (eng. architecture-centric). Ovaj pristup započinje od dizajna sustava i pokušava proći kroz model sustava u potrazi za napadima na svaki element modela. Upravo se ovaj pristup koristi u modeliranju prijetnji u Microsoftovom SDL-u.
- pristup usredotočen na resurs (eng. asset-centric) započinje od resursa povjerenih sustavu, poput skupa osjetljivih osobnih podataka.
- pristup usredotočen na obranu (eng. defense-centric) procjenjuje slabosti u sigurnosnom nadzoru.

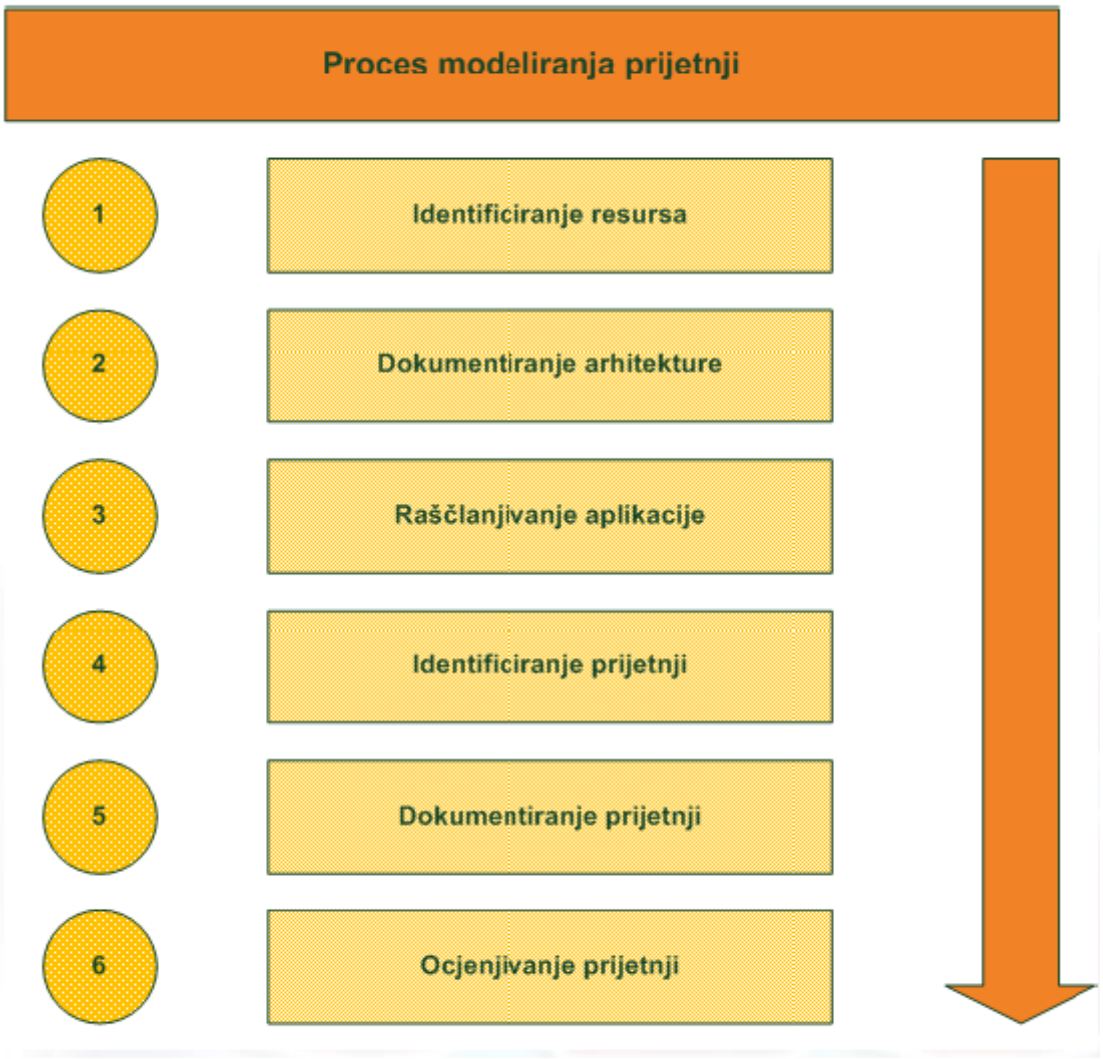
3.2. Principi modeliranja prijetnji

Modeliranje prijetnji ne bi trebao biti samo jednokratan, već iterativan proces koji započinje u ranim fazama razvoja aplikacije i nastavlja se kroz čitav životni ciklus aplikacije. Dva su glavna razloga za ovakav pristup. Za početak, nemoguće je identificirati sve postojeće prijetnje u jednom prolazu. S druge strane, proces modeliranja prijetnji potrebno je ponavljati zajedno s razvojem aplikacije zbog toga što su aplikacije rijetko statične te ih je potrebno poboljšavati i prilagođavati kako bi se prilagodile poslovnim zahtjevima.

[20] Centar informacijske sigurnosti (2012) Modeliranje sigurnosnih prijetnji (Threat Modeling), Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, str. 5

Proces modeliranja prijetnji koji se sastoji od šest faza shematski je prikazan na slici 3. i opisan u nastavku.

Slika 3. Proces modeliranja prijetnji u šest faza



Izvor: CIS

3.2.1. Identificiranje resursa

U ovom koraku obavlja se identificiranje resursa koje je potrebno zaštititi. Resursi pokrivaju širok raspon, od povjerljivih podataka do dostupnosti internetskih stranica. Među povjerljive podatke spadaju osobni podaci, podaci o intelektualnom vlasništvu, podaci o brojevima kreditnih kartica te podaci o zaporkama.

3.2.2. Dokumentiranje arhitekture

Glavni cilj ovog koraka je dokumentiranje funkcije aplikacije, njezine arhitekture i fizičkog razmještaja te tehnologija kojima je aplikacija ostvarena. Potrebno je pronaći moguće ranjivosti dizajna ili izvedbe promatrane aplikacije. U ovoj fazi potrebno je obaviti sljedeće zadatke[21]:

- identificirati funkciju aplikacije - identificirati što aplikacija radi te kako koristi ulazne resurse, što kasnije može koristiti za otkrivanje mogućih zloupotrebljavanja,
- stvoriti dijagram arhitekture - stvoriti dijagram arhitekture visoke razine koji opisuje kompoziciju i strukturu aplikacije te njezinih podsustava, kao i osobine fizičkog razmještaja. Za složenije sustave možda će biti potrebno stvaranje dodatnih dijagrama za pojedine dijelove
- identificiranje tehnologija - identificiranje različitih tehnologija koje su korištene u ostvarenju rješenja. Kasnije može biti od koristi kako bi se moglo usredotočiti na prijetnje svojstvene za pojedinu tehnologiju.

3.2.3. Raščlanjivanje aplikacije

Raščlanjivanje aplikacije podrazumijeva razbijanje aplikacije i stvaranja sigurnosnog profila za aplikaciju temeljenog na ranjivosti. Poželjno je što veće znanje o funkcioniranju aplikacije kako bi se što lakše otkrile prijetnje. Zadaci koje je potrebno obaviti u ovoj fazi su[22]:

- identificiranje granica povjerenja (eng. trust boundaries) koje okružuju svaki resurs aplikacije. Za svaki podsustav potrebno je razmotriti je li pouzdan ulazni tok podataka ili korisnički unos. U slučaju kada nije, treba razmotriti kako bi se tokovi podataka i unosi mogli autentificirati i autorizirati. Na jednak način potrebno je razmotriti pozivajući kod. Potrebno je osigurati odgovarajuću zaštitu svih ulaznih točaka u određenu granicu povjerenja kako bi se na ulaznim točkama primatelja mogla potvrditi valjanost svih podataka koji su prešli granicu.
- identificiranje protoka podataka (eng. data flow) - jednostavan pristup je započeti s najvišom razinom te zatim iterativno dekomponirati aplikaciju analizirajući protok

[21] Centar informacijske sigurnosti (2012) Modeliranje sigurnosnih prijetnji (Threat Modeling), Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, str. 6
[22] Ibid., str. 7

podataka između pojedinih podsustava. Posebno je važan protok podataka preko granica povjerenja. U tom slučaju programski kod koji prenosi podatke izvan granice povjerenja treba pretpostaviti da su podaci zlonamjerni te treba provesti temeljitu provjeru njihove valjanosti.

- identificiranje ulaznih točaka (eng. entry points) - ulazne točke u aplikaciju mogu poslužiti kao ulazne točke za napade. Dodatno, potrebno je poznavati smještaj unutarnjih ulaznih točaka te tipove ulaza koje one primaju u slučaju da napadač uspije premostiti 'prednja vrata' (eng. front door) aplikacije i napasti izravno na unutarnje ulazne točke. Za svaku ulaznu točku potrebno je odrediti 'čuvare' (eng. gatekeepers) koji osiguravaju autorizaciju i određeni stupanj provjere valjanosti.
- identificiranje privilegiranog koda (eng. privileged code) - privilegirani kod pristupa specifičnim vrstama sigurnih resursa i izvodi ostale privilegirane operacije. Privilegiranom kodu moraju biti dodijeljena odgovarajuća sigurnosna odobrenja za pristup kodu. Također, privilegirani kod mora osigurati da resursi i operacije koje on enkapsulira ne budu izloženi neprovjerenom i potencijalno zlonamjernom kodu.
- dokumentiranje sigurnosnog profila (eng. security profile) - potrebno je identificirati pristupe u dizajnu i ostvarenju aplikacije koji su korišteni za:
    - ulaznu provjeru (eng. input validation) - način na koji aplikacija filtrira, pročišćava i odbacuje ulazne podatke prije njihove daljnje obrade,
    - autentikaciju (eng. authentication) - proces u kojem korisnik dokazuje svoj identitet,
    - autorizaciju (eng. authorization) - način na koji aplikacija osigurava pristup resursima i operacijama,
    - upravljanje konfiguracijom (eng. configuration management) - načini na koje aplikacija rukuje konfiguracijom,
    - osjetljive podatke (eng. sensitive data) - način na koji se obrađuju svi podaci koji moraju biti zaštićeni,
    - upravljanje sjednicama (eng. session management) - rukovanje i zaštita međudjelovanja korisnika i web aplikacije,
    - kriptografiju (eng. cryptography) - način na koji aplikacija štiti i osigurava tajnost podataka,
    - upravljanje parametrima (eng. parameter manipulation) - način na koji aplikacija obrađuje ulazne parametre te ih štiti od mijenjanja,

- upravljanje iznimkama (eng. exception management) - što se događa prilikom neuspjelog poziva metoda u aplikaciji,
- reviziju i prijavljivanje (eng. auditing and logging) - način na koji aplikacija pohranjuje podatke o događajima vezanim uz sigurnost.

Provedbom navedene identifikacije stvara se sigurnosni profil aplikacije.

3.2.4. Identificiranje prijetnji

Ovaj korak sastoji se od identificiranja prijetnji koje mogu utjecati na sustav i ugroziti resurse. Za klasificiranje prijetnji mogu se koristiti dva temelja pristupa[23]:

a) STRIDE - pristup temeljen na cilju kod kojega se razmatraju ciljevi napadača,
b) kategorizirani popisi prijetnji - kod ovog pristupa započinje se od popisa učestalih prijetnji svrstanih u mrežnu, domaćinsku i aplikacijsku kategoriju.

STRIDE je klasifikacijska shema za karakteriziranje poznatih prijetnji prema vrsti iskorištavanja za koju se koriste ili prema motivaciji napadača. STRIDE je akronim sastavljen od prvih slova svake od šest kategorija prijetnji:

- pretvaranje identiteta (eng. Spoofing identity) - pokušaj pristupa sustavu pomoću lažnog identiteta. To je ključan rizik za aplikacije koje imaju mnogo korisnika, a osiguravaju jedan kontekst izvođenja na aplikacijskoj razini i razini baze podataka.
- uplitanje (eng. Tampering) - neovlaštena promjena podataka. Postoji mogućnost da korisnici promijene primljene podatke te ih tako izmijenjene vrate natrag. Aplikacija ne bi smjela korisniku slati podatke koji se mogu dobiti samo unutar nje same. Isto tako, aplikacija bi trebala pažljivo provjeriti podatke primljene od korisnika te provjeriti njihovu valjanost i primjenjivost prije njihovog korištenja ili pohranjivanja.
- odbijanje (eng. Repudiation) - korisnik može osporiti transakcije s nedovoljnim revizijama i pohranama aktivnosti. Stoga je potrebno razmotriti zahtijeva li aplikacija neodbijajuće nadzore poput zapisa o web pristupu ili zapisa o pristupu i korištenju sustava (eng. audit trail).
- povreda informacija (eng. Information disclosure) - neželjeno čitanje privatnih podataka. Aplikacija mora uključivati strogi nadzor kako bi spriječila mijenjanje i zlouporabu

[23] Centar informacijske sigurnosti (2012) Modeliranje sigurnosnih prijetnji (Threat Modeling), Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, str. 8

korisničkog ID-a (eng. identifier), posebice ako koristi jedan kontekst za izvođenje cijele aplikacije. Jednako tako, valja imati na umu da internetski preglednici mogu biti izvori 'curenja' informacija, stoga je potrebno količinu informacija pohranjenu web preglednikom svesti na najmanju moguću.

- uskraćivanje usluge (eng. Denial of Service) - djelovanje onemogućavanjem usluge. Kako bi se pokušalo izbjeći ovu vrstu napada potrebno je korištenje skupih resursa omogućiti isključivo autentificiranim i autoriziranim korisnicima, a onemogućiti anonimnim korisnicima. Za aplikacije za koje ovo nije moguće postići, potrebno je svaki njezin aspekt najviše pojednostaviti kako bi se spriječili jednostavniji DoS napadi.
- podizanje prava (eng. Elevation of privilege) - korisnik s manjim pravima preuzima identitet privilegiranijeg korisnika. Potrebno je sve akcije ograditi pomoću autorizacijske matrice, kako bi se osiguralo da samo korisnik s dopuštenim pravima može pristupiti privilegiranoj funkcionalnosti.

Kod kategoriziranja popisa prijetnji potrebno je obaviti sljedeća tri zadatka[24]:

1. identificirati mrežne prijetnje (eng. network threats) - zadatak za mrežne dizajnere i administratore. Najznačajnije mrežne prijetnje koje treba razmotriti u fazi dizajna uključuju:
    a. korištenje sigurnosnih mehanizama koji se oslanjaju na IP (eng. Internet Protocol) adresu pošiljatelja (relativno je jednostavno poslati IP pakete s lažnom IP adresom izvora),
    b. prosljeđivanje identifikatora sjednice ili kolačića (eng. cookies) preko nešifriranih mrežnih kanala (što može dovesti do krađe IP sjednice),
    c. prosljeđivanje tekstualnih akreditacijskih uvjerenja ili ostalih osjetljivih podataka preko nešifriranog komunikacijskog kanala (što može omogućiti napadaču da nadzire mrežu, dobije podatke o logiranju i ostale osjetljive podatke).
2. identificirati domaćinske prijetnje (eng. host threats) - koristi se pristup podjele konfiguracije u odvojene kategorije. Glavne ranjivosti koje ovdje treba uzeti u obzir su:

[24] Centar informacijske sigurnosti (2012) Modeliranje sigurnosnih prijetnji (Threat Modeling), Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, str. 9

a. održavanje 'nezakrpanih' (eng. unpatched) poslužitelja koji mogu biti izloženi zlonamjernim programima,
b. korištenje vrata (eng. ports), protokola i usluga koje nisu nužne,
c. dozvoljavanje anonimnog neovlaštenog pristupa,
d. korištenje slabe politike zaporki i računa.

3. identificirati aplikacijske prijetnje (eng. application threats) - razmatraju se svi aspekti sigurnosnog profila aplikacije. Naglasak je na aplikacijskim prijetnjama, prijetnjama svojstvenim za pojedine tehnologije i prijetnjama koda. Neke od glavnih ranjivosti koje ovdje treba razmotriti su:
    a. korištenje slabe provjere valjanosti ulaznih podataka, koja vodi do više vrsta napada (XSS napad, napad umetanjem SQL koda, napad prepunjenjem spremnika),
    b. prijenos autentikacijskih uvjerenja ili kolačića preko nekriptiranih mrežnih poveznica, što može dovesti do hvatanja podataka ili krađe sjednice,
    c. korištenje slabe politike zaporki i računa što može dovesti do neovlaštenih pristupa,
    d. pohranjivanje konfiguracijskih tajni u otvorenom, nešifriranom tekstu,
    e. korištenje nesigurnog rukovanja iznimkama, koje može dovesti DoS napada te otkrivanja detalja o sustavu koji mogu biti korisni napadaču,
    f. korištenje slabe i nedovoljnog šifriranja te nedovoljna zaštita kriptirajućih ključeva.

3.2.5. Dokumentiranje prijetnji

Najbitniji atributi su opis prijetnje te meta prijetnje. Atribut napadačke tehnike može naglasiti iskorištene ranjivosti, dok je atribut protumjere nužan za adresiranje prijetnji. Atribut rizik se u ovoj fazi ostavlja prazan te se popunjava u završnoj fazi procesa modeliranja prijetnji.

3.2.6. Ocjenjivanje prijetnji

Do ovog koraka procesa sastavljena je lista prijetnji za promatranu aplikaciju. U završnom koraku ovog procesa prijetnje se ocjenjuju na temelju rizika kojeg uzrokuju. Na ovaj način dobivena je lista prijetnji u kojoj se na vrhu nalaze prijetnje koje sa sobom donose najviše

rizika. S druge strane su prijetnje čija je vjerojatnost pojavljivanja vrlo mala i koje ne mogu prouzročiti veliku štetu, mogu zanemariti.

Osnovna formula prema kojoj je moguće izračunati rizik kojeg uzrokuje pojedina prijetnja je[25]:

Rizik = Vjerojatnost pojavljivanja * Potencijalna šteta,

što dobro oslikava posljedice na sustav u slučaju pojave napada. Jedna od skala koje se mogu koristiti za vjerojatnost pojavljivanja i potencijalnu štetu je takozvana skala 110. Pri čemu za vjerojatnost pojavljivanja 1 označava prijetnju koja je najmanje vjerojatna, dok 10 označava gotovo izvjesno pojavljivanje. Analogno tome, potencijalna šteta 1 označava najmanju štetu, dok 10 označava katastrofu. Korištenjem ovog pristupa rizik uzrokovan prijetnjom s malom vjerojatnošću pojavljivanja, ali s velikom potencijalnom štetom jednak je riziku kojeg uzrokuje prijetnja ograničenog potencijala, ali uz veliku vjerojatnost pojavljivanja. Ovaj pristup rezultira skalom 1100, odnosno, skalom s rasponom od 1 do 100 koji se može podijeliti u tri područja: visok, srednji i nizak rizik. Na temelju dobivene podjele jasno je koje prijetnje je potrebno najprije riješiti, dok se prijetnje s niskim rizikom mogu i zanemariti.

DREAD je klasifikacijska shema za kvantificiranje, usporedbu i određivanje prioriteta rizika prisutnog u svakoj promatranoj prijetnji. Razvijen je i široko korišten u tvrtki Microsoft. DREAD je akronim dobiven od prvih slova svake od kategorija[26]:

1. potencijalna šteta (eng. Damage potential) - kolika je šteta ako su iskorištene ranjivosti,
2. reproduktivnost (eng. Reproducibility) - koliko je jednostavno proizvesti napad,
3. iskoristivost (eng. Exploitability) - koliko je jednostavno iskoristiti pojedinu prijetnju,
4. zahvaćeni korisnici (eng. Affected users) - gruba procjena koliki postotak korisnika je zahvaćen pojedinom prijetnjom,
5. mogućnost otkrivanja (eng. Discoverability) - koliko je jednostavno otkriti ranjivosti.

[25] Centar informacijske sigurnosti (2012) Modeliranje sigurnosnih prijetnji (Threat Modeling), Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, str. 11
[26] Ibid.

Svaka od navedenih kategorija ocjenjuje se skalom od 1 do 3 te se u konačnici dobiva skala s rasponom od 5 do 15. Dobivenu skalu moguće je podijeliti na visoke (od 12 do 15), srednje (od 8 do 11) i niske rizike (od 5 do 7).

3.3. Zloćudni softveri

Zloćudni softver, štetni softver ili malware je pojam koji označava softver koji radi štetu korisniku. Radi se o računalnim programima koji se pokreću na računalnom sustavu bez stvarnog korisnikovog pristanka i imaju neku vrstu nepoželjnog učinka, kao što je oštećenje programa i podataka koji se nalaze na sustavu, širenje na druga računala, krađa podataka, masovno slanje neželjene elektroničke pošte (spama), sudjelovanje u napadima na druga računala putem mreže, i drugo.[27] Vrste malwarea su spyware, adware, trojanci, crvi i virusi.

3.3.1. Virusi

Računalni virus je računalni program koji svojom reprodukcijom može zaraziti računala na način da bez dopuštenja ili znanja samog korisnika računala kopira samog sebe u datotečni sustav ili memoriju ciljanog računalnog sustava.[28] Jednom pokrenut računalni virus će potražiti druge datoteke na računalu koje će nastojati inficirati, s krajnjim ciljem da se na neki način proširi na druga računala – primjerice slanjem inficirane datoteke u privitku elektroničke poruke. Pod inficiranjem datoteka podrazumijeva se postupak u kojem virus nastoji uklopiti vlastiti programski kod unutar neke legitimne datoteke na disku. Virus se pokreće učitavanjem inficirane datoteke u memoriju računala, npr. prilikom pokretanja programa ili otvaranja dokumenta. Osim legitimnog sadržaja, neprimjetno će se pokrenuti i sam virus. Pored umnažanja i širenja, gotovo svaki virus u nekom trenutku uzrokovat će događaj s više ili manje štetnim posljedicama na inficiranom računalu. Moć virusa može sezati od bezazlenog ispisivanja poruke na zaslonu računala, preko brisanja datoteka i kompromitiranja podataka na računalu, pa sve do npr. generiranja masovnog mrežnog prometa i onesposobljavanja računalne mreže. „Prvi virus koji se pojavio izvan računala na kojem je stvoren je „Elk Cloner“, a napisao ga je 1982. godine Rich Skrenta. Širio se putem diskete i nije izazivao štetu, već je bio zamišljen kao šala. Prvi virus na osobnom računalu bio

[27] Zloćudni software, dostupno online https://hr.wikipedia.org/wiki/Zlo%C4%87udni_softver (preuzeto 29.07.2016.)
[28] O virusima (2010) dostupno online http://www.cert.hr/malver/virusi (preuzeto 29.07.2016.)

je virus boot sectora imenom „Brain“, napisala su ga braća Basit i Amjad Farooq Alvi iz Lahorea u Pakistanu 1986. godine kako bi spriječili ilegalnu distribuciju vlastitog softvera. Sve većim korištenjem osobnih računala u uredima i kućanstvima, a potom razvojem Interneta stvorena je velika baza korisnika - kako potencijalnih žrtava, tako i napadača. Nakon toga virusi doživljavaju procvat. Do širenja virusa dolazi prenošenjem i pokretanjem inficiranih datoteka na drugim računalima. Mogućnosti su razne: inficirane datoteke put do drugih računala mogu naći pohranom na prijenosne medije (CD, DVD, USB stick, zip, disketa...), preko dijeljenih direktorija u lokalnoj mreži, putem Weba, elektroničke pošte, sustava za razmjenu datoteka (peer-to-peer) i slično.“[29]

3.3.2. Crvi

Poput virusa, i crvi imaju sposobnost samoumnažanja, no za širenje im nisu potrebni drugi izvršni programi i dokumenti, već se šire sami. Najčešće su dizajnirani tako da iskorištavaju nedostatke u sigurnosti pri prijenosu podataka pa koriste resurse mreže kako bi napravili kopije koje potom šalju mrežom bez ikakve intervencije. Pri tome potpuno blokiraju ostali promet, djeluju na cjelokupnu mrežu (za razliku od virusa koji većinom djeluju samo na jedno računalo). Crve po običaju povezujemo s napadima na poslovne mreže, iako je zlonamjerni podatkovni promet velik problem i za mreže davatelja internetskih usluga zbog neplaniranih troškova za održavanje mreže i podršku korisnicima.

U početku su crvi bili napravljeni u znanstvene svrhe (Xerox PARC, 1978. godine), a služili su za pronalaženje slobodnih procesora u mreži, tj. optimizaciju distribuiranih procesa i poboljšanje učinkovitosti mreže. Posebno su zloglasni tzv. mass mailing crvi koji se šire u privitku elektroničkih poruka, a obično će se poslati na sve adrese koje pronađu u adresaru na inficiranom računalu, pri čemu često koriste ugrađeni vlastiti poslužitelj elektroničke pošte. Osim pošte, crvi redovito zlorabe razne druge mrežne komunikacijske protokole kako bi se u što kraćem vremenskom roku proširili Internetom, a postoji mogućnost da se ugrade u sustav i dopuste nekom drugom da s udaljenosti preuzme kontrolu nad računalom. „Primjerice, crv MyDoom stvoren je za otvaranje backdoor ulaza na zaraženim sustavima i korišten je za napad na Web-poslužitelje. Kao primjer "uspješnog" napada često se navodi računalni crv Sapphire, kao najbrži crv u povijesti. Sam crv sastojao se od jednog UDP paketa veličine 360 okteta (bez opasnog koda). U prvoj minuti veličina crva se udvostručavala svakih 8.5 (±1)

[29] Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 7

sekundi, a najveća brzina kojom se širio je bila 55 milijuna paketa u sekundi (postignuta nakon treće minute širenja). Zarazio je preko 75 tisuća računala, od čega 90% u prvih deset minuta. Crv je izazvao veliko zagušenje mreže, pa čak i rušenje nekih poslužitelja. Širenje crva se temeljilo na slučajnom skeniranju IP adresa, što mu je u početku omogućilo eksponencijalno širenje, da bi ga poslije usporilo. Bilo je ograničeno samo dostupnom količinom prijenosnog pojasa, što je crvu dopuštalo da se širi brzinom kojom su zaražena računala mogla odašiljati pakete u mrežu.“[30]

3.3.3. Trojanci

Trojanac (ili trojanski konj) maliciozni je računalni program koji se koristi da bi inficirao ciljani PC sistem i uzrokovao na njemu zlonamjerne aktivnosti. Obično se takvi programi koriste za krađu osobnih podataka, širenje drugih virusa ili jednostavno remećenje performansi računala. Uz to, hakeri ih mogu koristiti za dobivanje neautoriziranog daljinskog pristupa kompromitiranom računalu, inficiranje određenih datoteka i nanošenje štete samom sistemu. Čim se trojanac infiltrira u računalo, on će se početi skrivati svojoj žrtvi. Trojanci su veoma slični pravim virusima i zato ih je vrlo teško detektirati. Zbog toga bi se trebali oslanjati na renomirani anti-spyware program. U početku trojanci nisu bili napravljeni da se mogu samostalno širiti internetom. No, novije verzije u sebi imaju dodatnu komponentu koja može omogućiti njihovo umnožavanje. Aktivnost svakog trojanca ovisi o namjerama njihovog autora. Uspjeh trojanaca ovisi o postupcima žrtve. Čak i ako se trojanci repliciraju i izvršavaju sami, svaka nova žrtva mora samostalno pokrenuti trojanca. Zbog toga je opasnost koju predstavljaju drugačije prirode u odnosu na opasnost koja proizlazi iz virusa i crva i više ovisi o uspjehu socijalnog inženjeringa i metoda kojima će se korisnika potaknuti da sam sebi učini štetu pokretanjem trojanaca, nego nedostacima u sigurnosnoj zaštiti računala. Gotovo uvijek trojanci rade štetu, no mogu biti i bezopasni. Prema šteti koju uzrokuju i načinu na koji napadaju sustav, mogu se podijeliti na nekoliko kategorija[31]:

- trojanci koji omogucuju udaljeni pristup,
- trojanci koji šalju podatke,
- destruktivni trojanci koji uništavaju datoteke i resurse računala,
- proxy trojanci,

[30] Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 7

[31] Kigoulis, L. (2016) Trojanci. Kako ukloniti?, dostupno online http://virusi.hr/trojanci/ (preuzeto 16.08.2016)

- FTP trojanci,
- trojanci koji onemogućavaju rad sigurnosnih programa,
- trojanci koji omogućuju napade uskraćivanjem usluge,
- trojanci koji otvaraju određene Web-stranice.

Neki od primjera rada trojanaca su[32]:

- brisanje podataka na računalu,
- šifriranje podataka (npr. za kriptovirusna iznuđivanja, kad se od napadnutog traži npr. novac kako bi povratio podatke),
- dopuštanje pristupa iz daljine na napadnuto računalo,
- širenje ostalih malicioznih programa, npr. virusa (takav trojanac se zove dropper ili vector),
- izgradnja mreže računala-zombija (zombie) koji se koriste u napadima distribuiranog uskraćivanja usluge (DDoS) ili slanja spama,
- špijuniranje rada korisnika i slanje tih podataka napadaču (npr. spyware),
- bilježenje pritisnutih tipki na tastaturi kako bi se pohranile lozinke ili brojevi kreditnih kartica dok ih korisnik upisuje,
- instalaciju tzv. backdoor programa koji ce omogućiti spajanje napadača na napadnuto računalo,
- otvaranje i zatvaranje ladice za CD/DVD (ovo je bezazlen, ali iritantan napad),
- prikupljanje adresa elektroničke pošte za slanje spama,
- ponovno pokretanje računala (*reboot*).

Posebne vrste trojanaca su logičke i vremenske bombe. Vremenske bombe aktiviraju se u određeno vrijeme ili dan. Logičke bombe aktiviraju se kad se poklopi niz okolnosti na napadnutom računalu. Većinom se trojanci naseljavaju na računalo nakon što korisnik, ne znajući, pokrene inficirani program. Zbog toga se savjetuje da se ne otvaraju nepoznati privici elektroničkoj pošti - često su to naizgled zanimljive animacije ili slike, a zapravo zlokobni programi. Osim elektroničke pošte, trojanci se mogu širiti putem sustava za Instant Messaging (MSN, ICQ, chat), putem Weba ili FTP-a, putem CD-a i DVD-a, disketa, USB stickova i drugih medija.

[32] Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 9

3.3.4. Dialeri

Dialer je program koji pomoću modema instaliranog na računalu uspostavlja dialup pristup Internetu. Naziv dolazi od engleske riječi dial, što znači "birati broj na telefonu". Ta se veza ostvaruje biranjem unaprijed određenog telefonskog broja. Radi se o zlućudnom softveru stvorenom da zaobiđe pristup Internetu preko lokalnog internetskog davatelja usluga i ostvari vezu korištenjem međunarodne ili neke druge skupe tarife. Aktivnost dialera uzrokuje visoke telefonske račune korisnika. Većina dialera djeluje poput računalnih virusa, mijenjajući osnovne postavke u sustavu računala bez znanja korisnika. Dialer koji se već "naselio" u računalo korisnika obično se pokrene samim uključenjem računala, te nastoji ostati nezapažen u sustavu. Dialerima su podložni korisnici ISDN-a te korisnici koji putem dial-up modema pristupaju internetskim servisima. Korisnici koji koriste pristup putem ADSL-a ili lokalne mreže u pravilu nisu ugroženi, osim ako imaju funkcionalan modem ili ISDN karticu (čak i kada korisnik ne koristi modem, ako je on instaliran u računalu te povezan s telefonskim priključkom, postoji opasnost od dialera).

Većina dialera slična je virusima, ali se metode distribucije razlikuju. Dialeri se ne šire sami, nego se instaliraju, kao i drugi softver. Korisnik može "pokupiti" dialer surfajući Internetom. Dialerima su posebno izloženi korisnici koji pristupaju Web-stranicama koje sadrže pornografski materijal, ilegalni softver (npr. crackove i serijske brojeve za komercijalne programe), ili pak ilegalnu glazbu: često takva sjedišta od korisnika traže da ručno instalira posebni softver koji će mu omogućiti pristup tim sadržajima. Instalaciju dialera dakle, obavlja korisnik. Takvi dialeri uglavnom nemaju mogućnost deinstaliranja ili cjelovita deinstalacija nije moguća, pa se svaki ponovni pristup Internetu može odvijati preko skupih brojeva. Drugi način instaliranja dialera u računalni sustav je iskorištavanjem nedostataka i ranjivosti Web-preglednika (browsera). Kad korisnik posjeti rizičnu Web-stranicu ili klikne na nesigurnu oglašivačku pop-up ikonu, može se instalirati dialer, a da korisnik ne zamijeti ništa sumnjivo. Nadalje, dialeri se mogu instalirati posjetom linkovima koje je korisnik dobio putem elektroničke pošte (npr. spamom).

Računalo na kojem je pokrenut dialer spaja se na Internet preko vrlo skupih telefonskih brojeva; ako je prethodno ostvarena veza na lokalni ISP, dialer će je prekinuti i ponovno se spojiti na "svoj" ISP. Korisnik najčešće neće primijetiti taj čin. Dodatno, dialeri mogu[33]:

- otvarati potencijalno nesigurne internetske stranice s pornografskim, oglašivačkim i slicnim sadržajima,
- mijenjati osnovne postavke dial-up pristupa i mreže u sustavu računala, te ih zamijeniti novim postavkama, registrirajući se kao unaprijed određeni (default) pristupni servis, koji se uvijek koristi pri spajanju računala na Internet, a u pravilu po skupoj tarifi,
- mijenjati polazišnu stranicu preglednika (Home page) i onemogućiti korisnika da promijeni te postavke,
- kreirati brojne linkove na potencijalno nesigurne stranice, mijenjati prečace (shortcuts) na zaslonu i upućivati na sumnjive stranice, te multiplicirati odabrane stranice na pregledniku, u popisu omiljenih internetskih stranica (bookmarks).

Posljedice instalacije dialera mogu biti vrlo mučne. Dialeri su dizajnirani u komercijalne svrhe, a njihovi autori žele zaraditi novac prijevarom neupućenih i nesavjesnih korisnika. Korisnik - žrtva dialera, ne znajući što zapravo radi, gubi novac svakodnevno surfajući Internetom, a šok nastupa po primitku telefonskog računa svog davatelja internetskih usluga. Uobičajeno surfanje Internetom dialer ometa kroz vrlo spor prijenos, određene stranice ne funkcioniraju kako su korisnici naviknuti, a dohvaćanje (download) softvera, glazbe, on-line gledanje video sadržaja ili animacija, kao i pretraživanje složenih multimedijalnih stranica, gotovo je onemogućeno. S obzirom da dialeri djeluju kao i virusi, u sustavu računala može ih se naći i ukloniti pomoću učinkovitog antivirusnog programa. Napredni softver može detektirati i ukloniti dialere i s njim povezane komponente. No, u nekim slučajevima uklanjanje ipak nije moguće.

[33] Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 11

Korisnikova nepažnja i neznanje glavni su razlozi instaliranja dialera na računalo. Korisnik može djelovati preventivno[34]:

- treba biti oprezan kad se pojavi ikona za download programa, te prije pristanka obvezno procitati uvjete koje eventualno odobravate klikom na "Yes, I agree", "Accept", odnosno nekim drugim oblikom pristanka;
- važno je instalirati antidialerske programe i redovito ih ažurirat, kako bi bili u stanju prepoznati nove dialere i varijacije postojećih. Antidialerske programe besplatno nude davatelji usluga pristupa Internetu, pa im se korisnik može obratiti.

Antidialerski program djeluje tako da softverski blokira pozive. Kad aplikacija presretne zahtjev za pozivanjem nekog broja, obavještava korisnika i taj broj uspoređuje s popisom u svojoj bazi pohranjenih brojeva. Nakon toga poziv se dopušta ili zabranjuje, ovisno o postavkama antidialera i odluci korisnika. Upravo zbog toga što se svakodnevno pojavljuju popisi novih brojeva, programe treba redovito ažurirati;

- instalacijom dialer controla, program kojim se može dopustiti na koje će se brojeve računalo spojiti, a na koje neće; time se osigurava nadzor biranja broja, odnosno spajanja na Internet;
- mora koristiti legalni softver i imati potrebne licence, te redovito ažurirati operacijski sustav; također treba redovito ažurirati antivirusne programe i njihove definicije virusa;
- nipošto ne otvarati dokumente u privitku elektronićke pošte, posebice ako postoje sumnje u njegovo porijeklo;
- dobro je koristiti alternativne preglednike (npr. Firefox, Opera) koji su ipak manje podložni dialerima;
- korisnik može od svog ISP-a zatražiti zabranu odlaznih poziva prema određenim brojevima, odnosno u tom slučaju pozive ostvarivati korištenjem zaporke (PIN);
- dodatna mjera opreza je nakon korištenja Interneta fizički iskljuciti vezu modema s telefonskim priključkom.

[34] Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 11

3.3.5. Hoax

Hoax je poruka elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja. Želja osobe koja je poslala hoax je njegovo prosljeđivanje na što veći broj adresa. Pri tome ih primatelji doista i prosljeđuju Internetom jer su uvjereni da time pomažu drugima. Najčešći oblici hoaxeva su[35]:

- hoaxevi kao upozorenja o štetnim programima - hoaxevi koji obicno sadrže lažna upozorenja na nove, "jako opasne" viruse i crve, trojanske konje ili druge oblike zlonamjernog koda.
- lanci sreće i zarade - hoaxevi u kojima se primatelju za prosljedivanje hoaxa na određen broj adresa obećava novac, besplatni mobiteli, turistički aranžmani ili drugi pokloni. Lanci sreće mogu imati i prijeteći karakter. U tim slučajevima primatelja se upozorava da će ga zadesiti nesretan i neugodan događaj ako primljenu poruku ne proslijedi na što veći broj adresa.
- lažni zahtjevi za pomoć - poruke kojima se izaziva suosjećanje prema nemoćnim osobama, obicno djeci, i poziva se na pomoć daljnjim slanjem hoaxa.
- zastrašujući i prijeteći hoaxevi - poruke koje upozoravaju na potencijalne opasnosti te pokušavaju zastrašiti primatelja s ciljem da proslijedi upozorenje svojim prijateljima i poznanicima.
- lažne peticije - poruke raznih sadržaja koje pozivaju na prikupljanje "potpisa" za neku važnu stvar te prosljeđivanje poruke kako bi i drugi korisnici mogli dati podršku.
- kompromitirajući hoaxevi - hoaxevi koji narušavaju ugled određenih organizacija ili osoba. Poruka sadrži lažne ili iskrivljene navode o određenim organizacijama, tvrtkama ili osobama.
- bezazleni hoaxevi - poruke za koje primatelji uglavnom odmah shvate da su lažne, ali ih prosljeđuju zbog njihovog šaljivog sadržaja.

U većini slučajeva iskusni primatelji mogu razaznati je li primljena poruka hoax ili ne. Jedan od glavnih pokazatelja je rečenica: "Pošaljite ovu poruku na što veći broj adresa!" Kako se tvorci hoaxa služe stručnom terminologijom, a kredibilitet pokušavaju postići pozivanjem na poznate tvrtke, korisnici ne mogu uvijek uvidjeti da je poruka lažna. Širenjem hoaxa ne može se izazvati velika šteta. Ipak, hoaxevi često zavaravaju korisnike, narušavaju ugled

[35] Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 12

određenih organizacija ili osoba, a pri tome bespotrebno opterećuju mrežu, povećavaju troškove korištenja Interneta te zatrpavaju poštanske sandučiće osoba koje ih dobivaju. Najbolja zaštita za probleme uzrokovane raznim malware-softverom i napadima su antivirusni programi i vatrozidi.

4. NAČINI OSIGURANJA RAČUNALNE MREŽE

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. Mnogi sigurnosni mehanizmi, kao što su antivirusni programi, sigurnosni protokoli mreža računala (npr. IPSec), kontrola pristupa, kriptiranje, vodeni žigovi, mogu se upotrijebiti za zaštitu dokumenata. No efikasna zaštita ne primjenjuje samo jedno rješenje, već kombinaciju spomenutih metoda zaštite.

4.1. Antivirusna zaštita

Antivirusni programi su posebna kategorija programa čija je osnovna namjena identifikacija, neutralizacija i eliminacija virusa, crva, trojanaca 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 neosvježavanje 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. Ovakvim pristupom zaštita se proširuje i na one viruse čije definicije još nisu uvedene u baze podataka. Problem ovakvog pristupa je u tome da će često sumnjivim akcijama proglasiti i one sasvim legitimne – mnogi korisnici će se zbog toga oglušiti na situacije u kojima će stvarno biti prepoznata opasna akcija.

4.2. 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.[36]

[36] CERT, LSS (2010) Metode zaštite dokumenata, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 6

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. Neka je poruka dokument sa osjetljivim podacima koji se razmjenjuje. Ukoliko se koristi simetrični kriptosustav za dekriptiranje, primatelj treba poznavati ključ kojim je dokument kriptiran. Ključ posjeduje samo osoba koja je kriptirala dokument i primatelj jedino od nje može dobiti ključ. Prema tome, potrebno je obaviti razmjenu ključeva, odnosno pošiljatelj treba na neki način poslati ili osobno predati ključ kojim primatelj može dekriptirati dokument. Takav se ključ naziva tajnim ključem i koristi se za kriptiranje i dekriptiranje poruke, što znači da primatelj može dekriptirati dokument samo upotrebom istog ključa kojim je kriptirana. Kako bi došao do tog ključa pošiljatelj mu mora na neki način predati ključ, odnosno primatelj i pošiljatelj moraju obaviti razmjenu tajnog ključa. Najčešće korišten protokol za razmjenu tajnog ključa je Diffie-Hellmanov protokol.[37]

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. Zbog toga se obično on naziva javni ključ. Ako Ivan želi Ani poslati poruku, jednostavno će potražiti njezin javni ključ, koji će biti objavljen u nečemu sličnom telefonskom imeniku. Zatim će Ivan njezinim javnim ključem kriptirati poruku i poslati je. Kada poruka stigne, Ana ju može dekriptirati svojim privatnim ključem. Na isti način bilo tko može Ani poslati kriptiranu poruku. Velika prednost sustava je što on uklanja problem distribucije ključa. Poruku može dekriptirati samo Ana jer jedino ona posjeduje privatni ključ.

Primjer najčešće korištenog asimetričnog kriptosustava je RSA, čiji su autori Ron Rivest, Adi Shamir i Len Adleman.[38] Još neki primjeri takvih algoritama su ElGamal, NTRUEncrypt, LUC i drugi. Sigurnost kriptiranih dokumenata ovisi o tome koji se algoritam koristi za

[37] Gledec, G., Mikuc, M., Kos, M. (2008) Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 13

[38] CERT, LSS (2010) Metode zaštite dokumenata, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 6

kriptiranje te duljini kriptografskih ključeva. Napadači mogu provesti kriptoanalizu teksta kojeg žele dekriptirati.

4.3. IPSec protokol

TCP/IP je skup protokola koji je de facto prihvaćen kao standard za mrežnu komunikaciju u većini današnjih računalnih mreža.[39] 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.

Kako je već spomenuto, IPSec funkcionira unutar mrežnog sloja te osigurava tajnost, integritet, autentikaciju i neporecivost. Pošto IP protokol osigurava uslugu komunikacijskog kanala od kraja do kraja (eng. end-to-end), zaštita kanala na istoj razini korištenjem IPSec-a omogućava mu neovisnost obzirom na niže slojeve. To znači da komunikacijski uređaji na putu između dvaju entiteta ne moraju podržavati IPSec, što omogućava korištenje IPSec-a bez obzira na način implementacije fizičkog sloja (eng. physical layer) i sloja prijenosa podataka (eng. data link layer). S druge strane, ukoliko dva

[39] CERT, LSS (2004) IPSec, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 4
[40] Ibid.

krajnja entiteta podržavaju IPSec, njegova uporaba je transparentna obzirom na više slojeve protokolnog stoga. Aplikacije mogu koristiti sigurnu komunikaciju koju pruža IPSec, bez obzira na vlastitu funkcionalnost. Isto se odnosi i na protokole koji su implementirani u transportnom sloju (eng. transport layer), što znači da svi podaci koji se prenose korištenjem TCP i UDP protokola, isto kao i ICMP poruke, mogu koristiti sigurni komunikacijski kanal koji pruža IPSec.

4.4. Trendovi u području zaštite

4.4.1. GSM

GSM je najpopularniji standard za sustave mobilne telefonije u svijetu. Njegova sveprisutnost omogućuje međunarodne „roaming“ ugovore između pružatelja usluga mobilnih telefona te pruža neprekidnu uslugu upotrebe mobilnog telefona u mnogim dijelovima svijeta. GSM je ćelijska mreža, što znači da se mobilni telefoni na nju povezuju traženjem ćelija u neposrednoj blizini uređaja. Postoji pet različitih veličina GSM mreža[41]:

- makro ćelije – ćelije u kojima se nalazi antena temeljne postaje, obično je postavljena na vrh visoke zgrade ako se nalazi na području grada,
- mikro ćelije – antena se nalazi ispod prosječne visine krovova, obično se nalazi u urbanim područjima,
- piko ćelije – pokrivaju nekoliko desetaka metara, koriste se u zgradama,
- femto ćelije – koriste se u poslovnom okruženju i povezuju mrežu pružatelja usluga na Internet,
- ćelije kišobran – koriste se za pokrivanje rupa između ćelija.

Najveći radijus koji podržava GSM specifikacija u praktičnoj upotrebi je 35 kilometara. Mreža se sastoji od sljedećih komponenti[42]:

- Podsustav bazne stanice (eng. Base Station Subsystem) - temeljna stanica i njihovi upravitelji.

[41] CERT, LSS (2004) IPSec, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 4
[42] CERT, LSS (2010) Sigurnost mobilnih mreža, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 11

- Podsustav za mrežu i prebacivanje (eng. Network and Switching Subsystem) – dio mreže koji je najsličniji fiksnoj mreži.
- GPRS jezgrena mreža (eng. GPRS Core Network) – neobavezni dio koji omogućuje povezivanje na Internet temeljeno na paketima.
- Potporni sustav operacija (eng. Operations support system – OSS) – podsustav koji se koristi za održavanje mreže.

Jedna od ključnih značajki GSM mreže je SIM (eng. Subscriber Identity Module) modul. SIM je pametna kartica koja sadrži podatke o korisnikovoj pretplati i telefonski imenik. Ona omogućuje korisnicima da zadrže svoje podatke nakon promjene mobilnog uređaja. Dakle, SIM kartica je neovisna o mobilnom uređaju. Osim toga, korisnici mogu promijeniti pružatelja mobilnih usluga mijenjanjem SIM kartice i zadržavanjem istog mobilnog uređaja. Neki pružatelji usluga postavljaju blokade tako da telefon može koristiti samo SIM kartice koje su oni izdali. To se naziva zaključavanje SIM kartica i ilegalno je u nekim državama (u Hrvatskoj je dozvoljeno).

4.4.2. GPRS

GPRS je paketno orijentirana mobilna usluga za prijenos podataka dostupna korisnicima 2G i 3G komunikacijskih sustava. U 2G sustavima GPRS pruža brzine prijenosa od 56 – 114 kbit/s. 2G mreže koje podržavaju GPRS se često nazivaju 2.5G mreže. Usluga pruža umjerenu brzinu prijenosa podataka upotrebom TDMA kanala nad GSM sustavom. GPRS nadograđuje GSM usluge i omogućuje sljedeće usluge[43]:

1) stalan pristup Internetu,
2) MMS (eng. Multimedia Messaging Service),
3) PTT (eng. Push to talk) preko ćelija (Poc/PTT) – metoda komunikacije na kanalu koji podržava obostranu, ali neistovremenu (half-duplex), komunikaciju upotrebom tipke za prebacivanje s primanja poruka na slanje poruka,
4) IM (eng. Instant messaging),
5) podrška za aplikacije za pregledavanje Internet stranica namijenjene pametnim uređajima (eng. smart devices) preko protokola WAP (eng. Wireless Application Protocol) i

[43] CERT, LSS (2010) Sigurnost mobilnih mreža, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 14

6) P2P (eng. Point-to-point) spajanje na Internet.

Ako se koristi SMS preko GPRS-a moguće je postići brzinu prijenosa od oko 30 poruka u minuti. To je mnogo brže od prijenosa poruka putem GSM-a gdje je brzina prijenosa između 6 i 10 poruka u minuti. GPRS podržava sljedeće protokole:

- IP,
- PPP (eng. point-to-point protocol) – ovaj način rada često ne podržava pružatelj usluge, ali ukoliko se koristi, mobitel se spaja na modem koji je povezan na računalo te se mobitelu dodjeljuje IP adresa,
- X.25 veze – obično se koristi za aplikacije kao što su bežični terminali za plaćanje.

Kada se koristi TCP/IP, svaki telefon može imati dodijeljenu IP adresu. GPRS će spremati i prosljeđivati IP pakete telefonu tokom putovanja kroz ćelije. TCP protokol upravlja mogućim gubitkom paketa. GPRS veza se uspostavlja referencom na ime točke pristupa (eng. Access point name – APN). APN definira usluge kao što su WAP pristup, SMS, MMS te pristup elektroničkoj pošti i Internetu. Za uspostavljanje GPRS veze na bežični modem korisnik mora odrediti APN, korisničko ime i lozinku (opcionalno) te rijetko IP adresu. Sve navedeno korisniku dodjeljuje pružatelj usluge.

4.4.3. GSM/GPRS

Osnovna funkcija GSM/GPRS mreže je pružiti potporu i olakšati prijenos informacija (glasovnih i podatkovnih). Obzirom da se radi o prijenosu informacija, postoje sigurnosni rizici pa je potrebno poduzeti određene sigurnosne mjere kako bi se zaštitila komunikacija. Tipovi informacija koji se trebaju zaštititi na GSM/GPRS mreži uključuju sljedeće[44]:

1) Korisnički podaci – glasovne ili podatkovne informacije poslane ili primljene preko GSM/GPRS mreže.
2) Naplaćivanje informacija – informacije koje prikupe SGSN i GGSN koriste se za naplaćivanje usluga.
3) Informacije o pretplatniku – pohranjene su u mobilnom uređaju te u HLR-u i VLR-u.
4) Tehničke informacije o GSM/GPRS mreži – opisuju arhitekturu i konfiguraciju mreže.

[44] CERT, LSS (2010) Sigurnost mobilnih mreža, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 16

Pružatelji mobilnih usluga su odgovorni za postavljanje sigurnosti na svojoj GSM/GPRS mreži. Neki uređaji koji se koriste u mreži već imaju u sebi sigurnosne funkcionalnosti, kao što su kriptiranje podataka i autentikacija korisnika. Uz to, pružatelj usluga može dodati funkcionalnosti koje poboljšavaju sigurnost mreža. Neke od njih su vatrozidovi (eng. firewall) i VPN veze preko GPRS mreže. Standardne sigurnosne usluge koje nude GSM/GPRS mreže su anonimnost, autentikacija, zaštita slanja signala te zaštita korisničkih podataka.

GSM/GPRS mreže koriste TBMI (eng. Temporary Mobile Subscriber Identities) funkcionalnost kako bi osigurali da identitet pretplatnika ostane zaštićen na mobilnoj mreži. Identitet pretplatnika se utvrđuje u kratkom vremenskom razmaku kada se mobilni uređaj priključuje na mrežu. Kada mobilni uređaj uspostavi vezu s mrežom, mora pružiti svoj IMSI (eng. International Mobile Subscriber Identity). IMSI sadrži osobni broj pretplatnika, njegovo ime i mrežu te kod države u kojoj je ugovorio pretplatu. Kada je mreža završila s upotrebom informacija za identifikaciju pretplatnika, mobilnom uređaju se dodjeljuje TMBI. Nakon toga se održava anonimnost korisnika.

GSM/GPRS mreže koriste mehanizam „izazov-odgovor“ (eng. challenge-response) kako bi osigurali da samo autorizirani korisnici imaju pristup mreži. Za GSM glasovne usluge autentikaciju obavlja MSC, a za GPRS SGSN. SGSN dodjeljuje slučajno odabrane 128 bitne brojeve mobilnom uređaju. Mobilni uređaj upotrebom privatnog autentikacijskog ključa jedinstvenog za svakog pretplatnika (pohranjenom u SIM kartici) i GSM autentikacijskog algoritma A3 stvara 32 bitni broj kao odgovor 128 bitnom broju kojeg je poslao SGSN. SGSN prima odgovor na izazov i obavlja isti računski postupak kao i mobilni uređaj. Ako su rezultati jednaki, mobilni uređaj se uspješno autenticirao na GPRS mreži i može koristiti njezine usluge. Tokom opisane interakcije pretplatnikov privatni ključ se ne prenosi preko radio sučelja (kako bi se zaštitio). Slanje signala i korisničkih podataka preko GPRS-IP potporne mreže i preko radio veze zaštićeno je od presretanja i prisluškivanja kriptografskim algoritmima. SGSN i mobilni uređaj koriste 128 bitni broj korišten u procesu autentikacije i privatni ključ pretplatnika (također spremljen u HLR-u) te u kombinaciji sa algoritmom za stvaranje ključeva A8 stvaraju kriptografski ključ. Podaci koji seprenose između mobilnog uređaja i GPRS mreže se mogu kriptirati upotrebom algoritma GPRS-A5 (prilagođene inačice A5 algoritma koji se koristi za kriptiranje glasovne komunikacije preko GSM mreža).

4.4.4. UMTS

UMTS je jedna od tehnologija treće generacije. Najuobičajeniji oblik UMTS-a koristi W-CDMA (eng. Wideband Code Division Multiple Access) kao sučelje za prijenos podataka bežičnim putem, koje također pokriva TD-CDMA (eng. Time-division Code Division Multiple Access) i TD-SCDMA (eng. Time Division Synchronous Code Division Multiple Access) pristup. CDMA (eng. Code division multiple access) je metoda za pristup kanalu kojeg koriste različite radio komunikacijske tehnologije. Jedan od osnovnih koncepata u komunikaciji prijenosom podataka je ideja da nekoliko odašiljača šalje podatke istovremeno preko jednog komunikacijskog kanala.

Nove usluge koje je uvela UMTS tehnologija zahtijevaju nove sigurnosne značajke kako bi se te usluge zaštitile. Uz to, uočeno je da postoje nedostaci kod sigurnosti GSM-koji se trebaju ispraviti (prvenstveno kod UMTS sustava). UMTS pruža uslugu međusobne autentikacije između dva UMTS pretplatnika koju omogućuje USIM. Uz to, mreža provjerava identitet pretplatnika i obratno, pretplatnik provjerava da je povezan na mrežu na koju treba biti. Osim autentikacije obavlja se i provjera besprijekornosti podataka te autentikacija izvornosti. To se obavlja sljedećim funkcionalnostima[45]:

1) Dogovor algoritma provjere integriteta – mobilna stanica i poslužujuća mreža mogu sigurno pregovarati o algoritmu koji koriste,
2) Dogovor integriteta ključa – mobitel i mreža se dogovaraju o integritetu ključa koji bi mogli koristiti.

UMTS pruža i povjerljivost korisničkog prometa:

1) algoritam kriptiranja – mobitel i postaja pregovaraju o upotrebi algoritma kriptiranja,
2) ključ kriptiranja – dogovara se i ključ kriptiranja,
3) povjerljivost podataka i korisnika – napadač ne može prisluškivati preko radio sučelja korisničke podatke, kao ni podatke koji se prenose.

UMTS primjenjuje MAPSEC. Osnovna ideja MAPSEC-a je da se MAP (eng. Mobile Application Part) poruka kriptira te da se kriptirana poruka pridružuje drugoj MAP poruci. MAP je protokol koji pruža funkcionalnost aplikacijskog sloja u GPRS i UMTS mrežama.

[45] CERT, LSS (2010) Sigurnost mobilnih mreža, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, str. 18

Istovremeno se kriptografski zbroj (eng. checksum), npr. autentikacijski kod poruke koji pokriva izvornu poruku, uključuje u novu MAP poruku. Za čitanje kriptirane poruke i upotrebu autentikacijskih kodova poruke potrebno je imati ključeve.

5. ZAKLJUČAK

TCP/IP je skup protokola koji je prihvaćen kao standard za mrežnu komunikaciju u većini današnjih računalnih mreža. Internet također koristi TCP/IP stog protokola koji se bazira na IPv4 protokolu. Jedan od glavnih nedostataka TCP/IP protokola jest nepostojanje nikakvih mehanizama kojima bi se osigurala zaštita i integritet podataka u prijenosu i izvršila autentikacija strana u komunikaciji. Sigurnost je moguće implementirati u drugim slojevima, od fizičkog do aplikacijskog sloja, a svaka od implementacija ima svoje prednosti i nedostatke te je preporučljivo koristiti kombinacije zaštita. Novije metode modeliranja prijetnji i analize rizika postaju sve pristupačnije za korištenje korisnicima koji nisu sigurnosni stručnjaci. U tome im mnogo pomažu i dostupni programski alati.

Postoji mnogo vrsta dokumenata koji su u svakodnevnoj upotrebi, a velika većina njih sadrži i osjetljive podatke. Kako ne bi dospjeli u neželjene ruke potrebno je takve dokumente zaštititi. Često se događaju gubici dokumenata zbog slučajnog ili namjernog brisanja, prepisivanja, kvarenja čvrstog diska, krađa i slično. Tvrtke koje su izgubile ili su im ukradeni važni dokumenti s osjetljivim podacima mogu izgubiti mnogo novaca i produktivnost. Prema tome, važno je pristupiti zaštiti dokumenata ozbiljno i spriječiti neovlašten pristup, izmjenu, brisanje i neprimjerenu upotrebu osjetljivih dokumenata. Razvojem kriptografije i tehnologije otkriveni su vrlo dobri načini kriptiranja i zaštite dokumenata. Nekoliko je metoda zaštite dokumenata, a one su upotreba enkripcije, upotreba zaporki, odnosno ograničavanje pristupa dokumentima, digitalno potpisivanje dokumenta, upotreba digitalnog vodenog žiga i kriptiranje cijelog diska. Antivirusni programi su posebna kategorija programa čija je osnovna zadaća antivirusnog prepoznati virus i zaštiti sustav od njegovog djelovanja. 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.

Jedan od ključnih faktora za uspjeh mobilne tehnologije je mogućnost pružanja poboljšane funkcionalnosti koja se može usporediti s fiksnim mrežama. Uz to, razvijene su napredne i dalekosežne mreže koje omogućuju korisnicima laku dostupnost podataka, brze i efikasne komunikacije te jednostavan pristup Internetu. Postojeća zaštita je dovoljno dobra za stare tehnologije, pa je s nadogradnjom sustava potrebno nadograditi i obnoviti zaštitu mobilnih sustava. Jednake sigurnosne prijetnje koje postoje u fiksnim mrežama, postoje i u bežičnim. Pružatelji usluga moraju prilagoditi sigurnosne mjere razvoju tehnologije te

spriječiti napadače od ugrožavanja dostupnosti mreže, besprijekornosti podataka i povjerljivosti informacija.

Na pitanje koji je standard bolji nema jedinstvenog odgovora kao niti na pitanje hoće li neki od njih u budućnosti preuzeti dominaciju, ili će nestati uopće potreba za tom vrstom zaštite. Svaki korisnik između ponuđenih rješenja treba odabrati ono koje mu najbolje odgovara. Kako bi ta odluka bila što kvalitetnija, prvenstveno je bitno informirati se o postojećim sigurnosnim problemima i dostupnim rješenjima.

POPIS LITERATURE

Knjige i publikacije:

1. Bača, M. Uvod u računalnu sigurnost, Zagreb, Narodne novine, 2004.
2. Centar informacijske sigurnosti, Modeliranje sigurnosnih prijetnji (Threat Modeling), Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, Zagreb, 2012.
3. CERT, LSS, IPSec, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, 2004.
4. CERT, LSS, Metode zaštite dokumenata, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, 2010.
5. CERT, LSS, Sigurnost mobilnih mreža, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, 2010
6. Ćukušić, M., Jadrić, M. Priručnik za polaznike © 2015 Srce, Sveučilište u Zagrebu, Sveučilišni računski centar, Zagreb, 2015.
7. Dragičević, D. Kompjutorski kriminalitet i informacijski sustavi. 2. izmijenjeno i dopunjeno izd. ,Zagreb, Informatorov biro sustav, 2004.
8. Feghhi, J. Digital certificates : applied internet security. Reading : Addison-Wesley, 2000.
9. Gledec, G., Mikuc, M., Kos, M. Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, 2008.
10. Hamidović, H. WLAN - bežične lokalne računalne mreže : priručnik za brzi početak. Zagreb : Info press, 2009.
11. Kunštek, Z. Računalne mreže II : priručnik. Zagreb : Algebra, 2009.
12. Minoli, D. Minoli-Cordovana's Authoritative computer & network security dictionary. Hoboken : Wiley-Interscience, cop. 2006.
13. Pastore, M. A. Security+ : studijski priručnik, ispit SY0-101 : udžbenik. Čačak ; Beograd : Kompjuter biblioteka , 2007.
14. Reid, P. Biometrics for network securitiy. Upper Saddle River : Prentice Hall PTR, cop. 2004.
15. Stallings, W. Cryptography and network security : principles and practice. Upper Saddle River : Prentice Hall : Pearson Education International, cop. 2003.
16. Stefanek, G. L. Information security best practices : 205 basic rules. Boston [etc.] : Butterworth-Heinemann, cop. 2002.

17. Strebe, M. Firewalls : zaštita od hakera : u praksi : [za administratore]. Čačak : Kompjuter biblioteka, 2003.
18. Tanenbaum, A. S. Računarske mreže : prevod četvrtog izdanja. Beograd : Mikro knjiga, 2005.
19. Turk, S. Računarske mreže. Zagreb : Školska knjiga, 1991.
20. Ozgović, J. „5. Upravljanje i održavanje računalnih mreža“ u: Projektiranje i upravljanje računalnim mrežama – skripta, Fakultet elektrotehnike, strojarstva i brodogradnje, Sveučilište u Splitu, Split, 2000.

Članci:

1. Filipović, I. New trends in networks and systems security. // KOM ... : komunikacijske tehnologije i norme u informatici. (2003) ; str. III 83-96.
2. Jušić, S. Sigurnost web aplikacija. // KOM ... : komunikacijske tehnologije i norme u informatici. (2003) ; str. III 75-82.
3. Kujundžić, A. Ispitivanje metoda sigurnosti u bežičnoj mreži temeljenih na protokolu EAP. // KOM ... : komunikacijske tehnologije i norme u informatici. (2003) ; str. III 57-74.
4. Kukec, M. Uvod u izgradnju računalne mreže za pristup internetu za male i srednje urede na sustavu otvorenog koda. // Tehnički glasnik : časopis Veleučilišta u Varaždinu : časopis s područja elektrotehnike, strojarstva, multimedije, informatike, logistike i građevinarstva. 1 (2007), 1/2 ; str. 59-62.
5. Majić, I. Provođenje analize ranjivosti računalnih mreža. // KOM ... : komunikacijske tehnologije i norme u informatici. (2007) ; str. 111-115.
6. Šikić, M. Sigurnost bežičnih WLAN-ova. // KOM ... : komunikacijske tehnologije i norme u informatici. (2003) ; str. III 41-55.
7. Šorman, M. Implementing improved WLAN security. // Proceedings Elmar ... / ... International Symposium Elmar ; edited by Mislav Grgić, Tomislav Kos, Sonja Grgić. 46 (2004) ; str. 229-234.
8. Vrdoljak, M. Sigurnost virtualnih privatnih mreža. // KOM ... : komunikacijske tehnologije i norme u informatici. (2005) ; str. 11-20.

Izvori na internetu:

1. Čagalj, M. (2006) Sigurnost u bežičnim računalnim mrežama, Fakultet elektrotehnike, strojarstva i brodogradnje, Split (30.07.2016)
   URL: http://www.fesb.hr/~mcagalj/presentations/WiFiSec_nastupno.ppt
2. Sviličić, B., Kraš, A. (2005) Zaštita privatnosti računalnog sustava, Pomorski fakultet u Rijeci (01.07.2016.)
   URL: http://hrcak.srce.hr/file/6510
3. Škundrić, S., Sok, A. (2007) Analiza računalne mreže na tehničkom fakultetu u Rijeci, Tehnički Fakultet, Rijeka (01.07.2016.)
   URL: http://hrcak.srce.hr/file/41639
4. Randić M. (2010) Upravljanje mrežom i uslugama, Fakultet elektrotehnike i računarstva, Zagreb (30.08.2016,)
   URL: https://www.fer.unizg.hr/_download/repository/UMU_Skripta.pdf
5. Pralas, T. (2004) Računalne mreže – pasivna i aktivna oprema, Sys portal, Carnet, Zagreb (30.08.2016.)
   URL: https://sysportal.carnet.hr/node/374
6. Vidipedija, Poslužitelj (30.08.2016.)
   URL: http://www.vidipedija.com/index.php?title=Poslu%C5%BEitelj (preuzeto 30.08.2016.)
7. Wikipedia, Računalne mreže (30.08.2016)
   URL: https://hr.wikipedia.org/wiki/Ra%C4%8Dunalne_mre%C5%BEe
8. Mujarić, E., Prijenosna razina (29.08.2016.)
   URL: http://mreze.layer-x.com/s040000-0.html
9. Radić, D., Topologija mreže (29.08.2016.)
   URL: http://www.informatika.buzdo.com/s420-topologija-mreze.htm
10. Wikipedia, Zloćudni software (29.07.2016.)
    URL: https://hr.wikipedia.org/wiki/Zlo%C4%87udni_softver
11. CERT, O virusima (2010) (29.07.2016.)
    URL: http://www.cert.hr/malver/virusi
12. Kigoulis, L. (2016) Trojanci. Kako ukloniti? (16.08.2016)
    URL: http://virusi.hr/trojanci/
13. Wikipedia, TCP (06.09.2016.)
    URL: https://hr.wikipedia.org/wiki/TCP

POPIS SLIKA

METAPODACI

Naslov rada: SIGURNOST I ZAŠTITA RAČUNALNIH MREŽA

Autor: TOMISLAV ŠOŠTARIĆ

Mentor: PROF. DR. SC. ZVONKO KAVRAN

Naslov na drugom jeziku (engleski):

SECURITY OF COMPUTER NETWORKS

Povjerenstvo za obranu:

- PROF. DR. SC. DRAGAN PERAKOVIĆ, predsjednik
- PROF. DR. SC. ZVONKO KAVRAN, mentor
- DR. SC. IVAN GRGUREVIĆ, član
- PROF. DR. SC. ŠTEFICA MRVELJ, zamjena

Ustanova koja je dodijelila akademski stupanj: FAKULTET PROMETNIH ZNANOSTI SVEUČILIŠTA U ZAGREBU

Zavod: ZAVOD ZA INFORMACIJSKO KOMUNIKACIJSKI PROMET

Vrsta studija: PREDDIPLOMSKI

Naziv studijskog programa: INFORMACIJE I KOMUNIKACIJE

Stupanj: SVEUČILIŠNI PRVOSTUPNIK

Akademski naziv: SVEUČILIŠNI PRVOSTUPNIK INŽENJER PROMETA

Datum obrane završnog rada: 13. rujna 2016.

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem da je ZAVRŠNI RAD
(*vrsta rada*)
isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom SIGURNOST I ZAŠTITA RAČUNALNIH MREŽA, na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu,_____ _____
(*potpis*)