CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Peer-to-peer mreže

NCERT-PUBDOC-2009-11-282

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. UVOD 4

2. ARHITEKTURA PEER-TO-PEER MREŽA 5

2.1. PODJELA PREMA NAČINU ISPISIVANJA PODATAKA 6

2.1.1. Centralizirane (hibridne) peer-to-peer mreže 6

2.1.2. Decentralizirane peer-to-peer mreže 7

2.2. PODJELA PREMA NAČINU SPAJANJA SUDIONIKA 7

2.2.1. Strukturirane peer-to-peer mreže 7

2.2.2. Nestrukturirane peer-to-peer mreže 8

3. PREDNOSTI I NEDOSTACI 9

4. PRIMJENE 11

4.1. PEER-TO-PEER MREŽE ZA DIJELJENJE PODATAKA 11

4.2. PEER-TO-PEER MREŽE ZA ISTRAŽIVANJA I ZNANSTVENE INFORMACIJE 12

4.3. PEER-TO-PEER MREŽE ZA MULTIMEDIJU 12

4.4. GLASOVNA I PISMENA KOMUNIKACIJA (VOIP) 12

4.5. STATISTIKE KORIŠTENJA PEER-TO-PEER MREŽA 13

5. SIGURNOSNI PROBLEMI PEER-TO-PEER MREŽA 14

5.1. SPYWARE PROGRAMI 14

5.2. VIRUSI I CRVI 15

5.3. NAPADAČI 15

5.4. KRAĐA I UNIŠTAVANJE PODATAKA 16

5.5. POVJERLJIVOST PODATAKA 16

5.6. AUTENTIKACIJA 16

5.7. NEDOZVOLJENI SADRŽAJI I RODITELJSKA ZAŠTITA 16

5.8. ŠPIJUNAŽA 17

6. SIGURNO KORIŠTENJE PEER-TO-PEER MREŽA 17

7. ZAKLJUČAK 18

8. REFERENCE 19

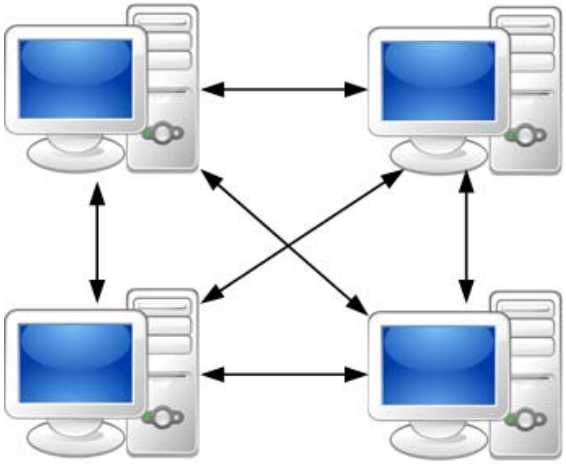
1. Uvod

Peer-to-peer mreže, poznate i pod skraćenicom P2P, vrlo su popularan način razmjene podataka i informacija među korisnicima. Razmjena se temelji na međusobnom povjerenju sudionika, što može stvoriti probleme i štetu ukoliko su u pitanju zlonamjerni sudionici. Promet ostvaren *peer-to-peer* mrežama (procjenjuje se na više od 1.3 petabyte podataka) u posljednjih 5 godina premašio je promet ostvaren pregledavanjem web stranica i drugim aktivnostima. Broj sudionika na *peer-to-peer* mrežama svakodnevno raste, međutim rastom broja korisnika pružaju se i veće mogućnosti za zlonamjerna djelovanja. Kao i pri pregledavanju Internet sadržaja, kod *peer-to-peer* mreža je također vrlo visok rizik zaraze zlonamjernim programima poput virusa, crva ili spyware-a. Također, postoji opasnost od krađe i uništavanja podataka radi stjecanja materijalne koristi, te sadržaja koji nisu primjereni za djecu i maloljetnike. *Peer-to-peer* mreže se osim za razmjenu podataka i/ili informacija koriste i za glasovnu ili pismenu komunikaciju. Komunikacija u stvarnom vremenu putem *peer-to-peer* mreža također postaje vrlo popularna.

U ovom dokumentu su opisane osnovne strukture *peer-to-peer* mreža, te njihove prednosti i nedostaci. Također, navedene su primjene peer-to-peer mreža te sigurnosni problemi koji se javljaju pri korištenju. Kako bi se korisnicima pokazalo kako je moguće sigurno koristiti *peer-to-peer* programe navedene su preporuke kojih se valja pridržavati.

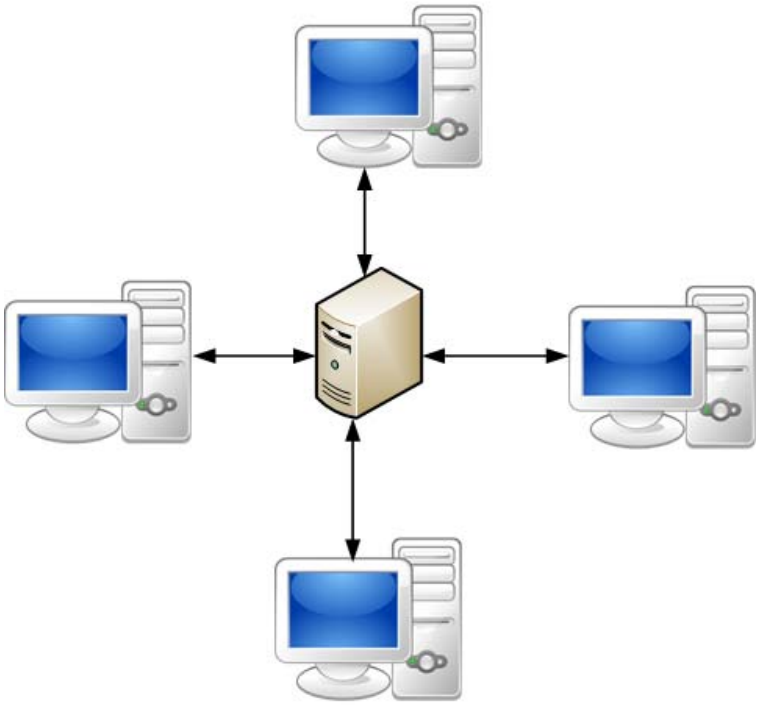
2. Arhitektura peer-to-peer mreža

Distribuirana arhitektura *peer-to-peer* mreža se sastoji od sudionika koji dijele dio svojih resursa (kao što su primjerice tvrdi disk ili memorija) koje je moguće iskoristiti međusobnim povezivanjem. Ti su mrežni resursi dostupni drugim sudionicima mreže bez potrebe za središnjim upravljačkim jedinicama kao što su poslužitelji (*eng. Server*) ili domaćini (*eng. Host*). Sudionici mreže su ravnopravni, tj. svi sudionici posjeduju jednaka prava uzimanja i davanja resursa. U nastavku je prikazana načelna shema *peer-to-peer* mreže.



Slika 1. Shema *peer-to-peer* mreže
Izvor: Wikipedia

Kod mreža s poslužiteljima sudionik može samo uzimati, a poslužitelj davati resurse. Arhitektura *peer-to-peer* mreža je jednostavnija od mreža s poslužiteljima (ali one mogu podnijeti velika opterećenja u radu).



Slika 2. Shema mreže s poslužiteljem
Izvor: Wikipedia

Peer-to-peer mrežnu arhitekturu je moguće zamisliti tako da su na istom računalu postavljeni poslužitelj i klijent, tj. svako računalo može istovremeno primati i davati resurse drugim sudionicima pripadajuće odgovarajuće mreže. Upravo to ukazuje na brzinu rada *peer-to-peer* mreža, jer svaki sudionik mreže mora poznavati mrežnu adresu drugog sudionika kako bi mu mogao pristupiti. Takav način rada značajno usporava rad samog mrežnog sustava ukoliko se radi o velikom broju sudionika.

Peer-to-peer mreže je moguće podijeliti prema:

- načinu ispisivanja podataka koji se razmjenjuju (*eng. File listing*) i
- načinu spajanja sudionika mreže (*eng. Node connection*).

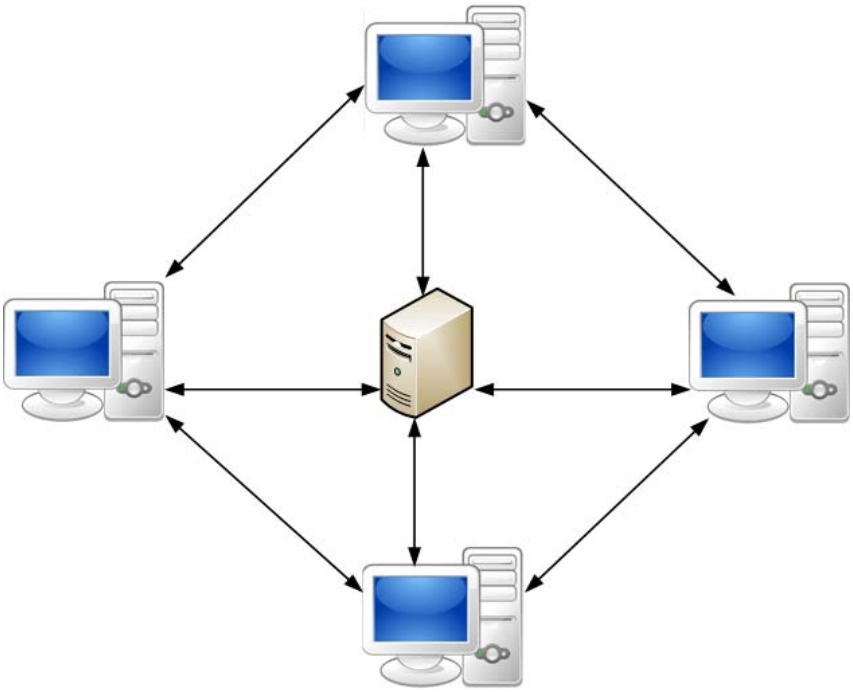
U nastavku poglavlja su detaljnije opisane navedene podjele.

2.1. Podjela prema načinu ispisivanja podataka

Način ispisivanja podataka u *peer-to-peer* mrežama od velike je važnosti jer određuje brzinu rada mreže. Ispisivanjem podataka pomoću središnjeg poslužitelja je ubrzan rad mreže jer sudionik preuzima popis traženih podataka sa poslužitelja (što nije slučaj kod decentraliziranih mreža). Kao i kod svakog mrežnog sustava, poželjna je što veća brzina prijenosa podataka, što kod *peer-to-peer* mreža često nije slučaj.

2.1.1. Centralizirane (hibridne) peer-to-peer mreže

Kod centraliziranih *peer-to-peer* mreža popis dostupnih podataka se nalazi na središnjem poslužitelju, što uvelike ubrzava rad mreže. *Peer-to-peer* mreže koje rade na ovaj način smatraju se hibridnim, zato jer sadrže poslužitelja i time odstupaju od arhitekture konvencionalnih *peer-to-peer* mreža.



Slika 3. Prikaz arhitekture centraliziranih hibridnih *peer-to-peer* mreža

Kao što je vidljivo na slici 3., kod centraliziranih *peer-to-peer* mreža svaki sudionik mreže ima izravnu vezu sa poslužiteljem, ali i ostalim sudionicima mreže. Sudionik mreže s poslužitelja preuzima popis dostupnih podataka (umjesto da popis preuzima od svakog sudionika mreže) čime se značajno ubrzava proces pretrage. Poslužitelj i kod ove vrste mreže ima samo mogućnost slanja podataka sudionicima mreže, a sudionici samo mogućnost preuzimanja od poslužitelja. Međutim kada se radi o komunikaciji među sudionicima, vrijedi već spomenuti princip *peer-to-peer* mreža - svaki sudionik mreže može uzimati i davati

resurse drugim sudionicima mreže. Većina današnjih peer-to-peer mreža se temelji na centraliziranoj arhitekturi.

2.1.2. Decentralizirane peer-to-peer mreže

Decentralizirane *peer-to-peer* mreže u svojoj arhitekturi ne sadrže središnje poslužitelje, već samo sudionike. Kod decentraliziranih *peer-to-peer* mreža svaki sudionik je povezan s mnogo drugih sudionika mreže, te od njih preuzima popis dostupnih podataka. Svaki sudionik je u mogućnosti uzimati tuđe i davati vlastite resurse drugim sudionicima komunikacije.

Kod decentraliziranih *peer-to-peer* mreža česta pojava su tzv. super-čvorovi (*eng. Super peer*) koji, ovisno o potrebi u pripadajućem mrežnom sustavu, mogu raditi kao poslužitelji i pružati popis podataka drugim sudionicima mreže. Mreže koje u sebi sadrže super-čvorove kombiniraju brzinu rada centraliziranih mreža i uravnoteženje opterećenja decentraliziranih mreža. Kombinacijom tih svojstava postignuta je optimalna brzina i učinkovitost *peer-to-peer* mreže.

2.2. Podjela prema načinu spajanja sudionika

Kao što će biti prikazano u nastavku, način spajanja sudionika također ima značajan utjecaj na rad neke *peer-to-peer* mreže. *Peer-to-peer* mreže su prema načinu spajanja sudionika podijeljene na:

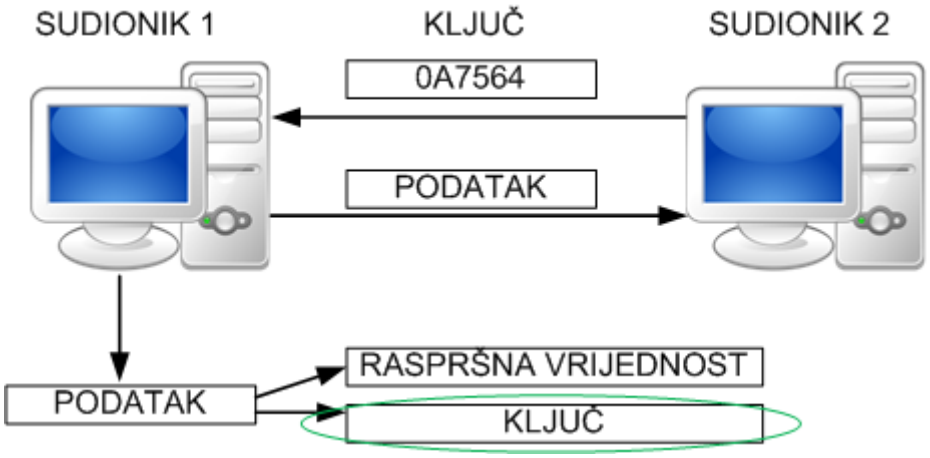
- strukturirane *peer-to-peer* mreže i
- nestrukturirane *peer-to-peer* mreže.

2.2.1. Strukturirane peer-to-peer mreže

Strukturirane *peer-to-peer* mreže koriste algoritme koji osiguravaju da svaki sudionik može pomoću pretrage (*eng. Search*) pronaći željene podatke kod drugog sudionika mreže. Algoritmi u strukturiranim *peer-to-peer* mrežama osiguravaju najveću učinkovitost i brzinu mreže. Najuobičajenija vrsta strukturiranih *peer-to-peer* mreža su mreže koje koriste distribuirane raspršne tablice (*eng. Distributed hash table - DHT*), gdje je svaki podatak obilježen pripadajućom raspršnom funkcijom (*eng. Hash function*).

Decentralizirane strukturirane sustave čine distribuirane raspršne tablice koje sudioniku omogućuju pretragu podataka tako da mu daju ključ koji obilježava traženi podatak. Bilo koji podatak je obilježen sa dva svojstva:

- raspršnom vrijednosti i
- ključem.



Slika 4. Prikaz rada *peer-to-peer* mreže s distribuiranim raspršnim tablicama

Primjerice, Sudionik 1 koji posjeduje traženi podatak, posjeduje raspršnu vrijednost i pripadajući ključ koji obilježavaju taj podatak. Sudionik 2, koji želi preuzeti taj podatak mora

Sudioniku 1 poslati odgovarajući ključ kako bi mogao preuzeti podatak. Protokoli za provjeru uspoređuju ključ primljen od Sudionika 2, te ključ Sudionika 1. Ukoliko su ključevi jednaki, Sudionik 2 je u mogućnosti preuzeti podatak.

Više o distribuiranim raspršnim tablicama moguće je saznati na adresi:

http://en.wikipedia.org/wiki/Distributed_hash_table

2.2.2. Nestrukturirane peer-to-peer mreže

Nestrukturirane *peer-to-peer* mreže nastaju proizvoljnim međusobnim spajanjem sudionika. Kada sudionik mreže u nestrukturiranim *peer-to-peer* mrežama želi pronaći neki podatak, upit se šalje svim dostupnim sudionicima kako bi se pronašao što veći broj sudionika koji imaju isti podatak. Nedostatak nestrukturiranih mreža jest to da neki upiti nemaju rezultata. Ukoliko su u pitanju popularni podaci (oni koji se nalaze na velikom broju sudionika mreže) upit će rezultirati uspješnom pretragom, ali ukoliko se radi o rijetkim podacima, postoji velika mogućnost da sudionik neće uspjeti pronaći tražene podatke.

Slanje upita velikom broju korisnika usporava normalan rad mreže, a osim toga, kao što je ranije napomenuto, ne osigurava uspješnost pretrage.

3. Prednosti i nedostaci

Svaka mreža ima svoje prednosti i nedostatke, stoga će u ovom poglavlju biti navedene prednosti i nedostaci *peer-to-peer* mreža u odnosu na centralizirane mreže sa poslužiteljima. Veliki sustavi za dijeljenje podataka češće su izrađeni kao *peer-to-peer* mreže nego kao centralizirane mreže s poslužiteljima zbog manjih troškova ulaganja, jednostavnosti i boljeg rukovanja promjenama u opterećenju. Naravno, poslužitelji mogu podnijeti veće opterećenje od sudionika, ali ne mogu sudionicima osigurati jednake rezultate pretrage kao *peer-to-peer* mreže. U nastavku su nabrojane prednosti *peer-to-peer* mreža u odnosu na centralizirane sustave:

- *u peer-to peer mrežama se koriste jeftiniji resursi* - računala koje sudionici mreže koriste imaju manju cijenu od one koju bi vlasnik centraliziranog sustava morao platiti za nabavu nove opreme u svrhu povećanja kapaciteta sustava. U *peer-to-peer* mrežama svaki novi sudionik koji se priključi mreži koristi resurse drugih sudionika i daje na korištenje vlastite resurse ostalim sudionicima komunikacije. Ova činjenica upućuje na neograničeni potencijal *peer-to-peer* mreža kada je u pitanju broj korisnika koji mreža može podržati.
- *peer-to-peer mreže bolje rukuju promjenama u opterećenju* - iznos ostvarenog prometa u sustavu koji je priključen na Internet i dostupan velikom broju korisnika ima velike promjene u vremenu. Ovisno o vremenu mogu se uočiti vršna opterećenja sustava i minimumi opterećenja (kada sustav koristi najmanji broj korisnika). Kako bi neki centralizirani sustav mogao rukovati velikim promjenama u prometu, potrebno je pripremiti dodatne resurse koji će biti dostupni kada sustav bude potpuno opterećen. Kod peer-to-peer mreža rukovanje velikim količinama prometa ne predstavlja dodatne troškove. Ukoliko se u *peer-to-peer* mreži dogodi da su svi dostupni resursi u upotrebi, sustav jednostavno u rad ubacuje resurse dostupnih sudionika čiji resursi nisu u upotrebi. Povećanjem opterećenja u *peer-to-peer* mreži povećava se i broj uključenih sudionika koji dijele to opterećenje.
- *jednostavnost instalacije* - *peer-to-peer* sustave je lako postaviti za optimalan rad na računalu korisnika i ne zahtijevaju veliku količinu znanja o *peer-to-peer* sustavima.
- *nadzor nad dijeljenim resursima* - korisnici imaju nadzor nad resursima koje žele dijeliti sa drugim sudionicima mreže. U korisničkim postavkama moguće je odrediti koje datoteke i mape korisnik želi dijeliti sa drugima.
- *peer-to-peer arhitektura je povoljnija za male sustave koji sadrže manje od 10 računala* - za male poslovne ili privatne sustavi koji ne sadrže velik broj računala *peer-to-peer* arhitektura je povoljnija jer ne zahtijeva veliku količinu vremena uloženog za postavljanje sustava i troškovi su znatno manji nego kod postavljanja centraliziranog sustava sa poslužiteljem.
- *peer-to-peer mreže ne zahtijevaju administratora mreže* - u *peer-to-peer* mrežama nije potrebna osoba koja će nadgledati rad mreže i održavati istu.

Navedene prednosti ne dokazuju da je primjena *peer-to-peer* arhitekture u svakom slučaju bolja od primjene centralizirane arhitekture. Primjena pojedine arhitekture ponajprije ovisi o potrebama, zahtjevima i željenoj razini sigurnosti.

Iako se iz gore navedenih prednosti čini da su *peer-to-peer* mreže odličan izbor za primjenu na svakom mrežnom sustavu, iste imaju i svoje nedostatke. *Peer-to-peer* mreže nadomještaju neke nedostatke centraliziranih sustava s poslužiteljem, međutim, vrijedi i obrnuto. U nastavku su navedeni nedostaci *peer-to-peer* mrežne arhitekture:

- *sudionici mreže imaju različite interese* - većinu korisnika zanimaju različiti podaci, stoga postoji problem u komunikaciji i korištenju *peer-to-peer* mreža. Neki sudionici koriste mrežu samo za preuzimanje podataka od drugih sudionika, bez dijeljenja vlastitih podataka s drugim korisnicima (takva se pojava naziva *leeching*).
- *računalu sudionika peer-to-peer mreže je moguće pristupiti u bilo kojem trenutku* - nepovoljna okolnost *peer-to-peer* mreža i dijeljenja podataka putem ovakvih mreža jest da zlonamjerni sudionici mogu pristupiti računalu korisnika kada žele. Iskorištavanjem sigurnosnih propusta operacijskog sustava i/ili korištenih programskih paketa mogu ugroziti integritet podataka na računalu sudionika, a ponekad čak i preuzeti nadzor nad računalom.

- *sigurnosne alate je potrebno postaviti na svako računalo zasebno* - za razliku od centralizirane arhitekture, u peer-to-peer mrežama svako računalo mora imati vlastitu sigurnosnu zaštitu (antivirusni alati, vatrozidi, itd.).
- *rezervne kopije podataka i informacija se moraju posebno izraditi za svako računalo u mreži* - izrada sigurnosnih kopija podataka je u ovakvim mrežama zahtjevan postupak i nije pogodan za sustav koji sadrže osjetljive i povjerljive podatke.
- *ne postoji središnja jedinica (poslužitelj) koja nadgleda i upravlja pristupom podacima* - u *peer-to-peer* sustavima nije moguće odrediti koji će sudionici imati prava sudjelovati u razmjeni podataka. Kao što je ranije naglašeno, svi sudionici mreže imaju jednaka prava, što u ovom slučaju predstavlja problem po pitanju prava pristupa podacima. U centraliziranim sustavima poslužitelj određuje koji sudionik mreže ima kakva prava, te kojim podacima je u mogućnosti pristupiti. Poslužitelj nadgleda i bilježi aktivnost sudionika na mreži, što u slučaj *peer-to-peer* mreža nije moguće izvesti jer ne postoji središnja jedinica koja bi provodila navedene radnje.
- *sudionici mreže moraju koristiti različite lozinke na različitim računalima za pristup mreži* - u centraliziranom mrežnom sustavu svaki je korisnik u mogućnosti prijaviti se na svako računalo koje je dio mreže s istom lozinkom. U centraliziranom sustavu su pri pristupu računalu određena prava korisnika, što nije slučaj kod *peer-to-peer* mreža.
- *peer-to-peer mreže imaju manju razinu sigurnosti* - iako svako računalo može imati odgovarajuću zaštitu, može se dogoditi da računalo bude ugroženo iskorištavanjem nekog sigurnosnog propusta ili da greškom nekom proizvoljnom sudioniku mreže bude odobren potpun pristup podacima.

Iako *peer-to-peer* mreže imaju određene prednosti nad centraliziranim mrežama, smatra se da je prva obveza zaštita podataka na računalu. Kad je u pitanju zaštita podataka, centralizirane mreže su naprednije od *peer-to-peer* mreža jer omogućavaju istovremenu zaštitu svih računala na mreži putem poslužitelja, te ograničavaju pristup određenim podacima i resursima.

4. Primjene

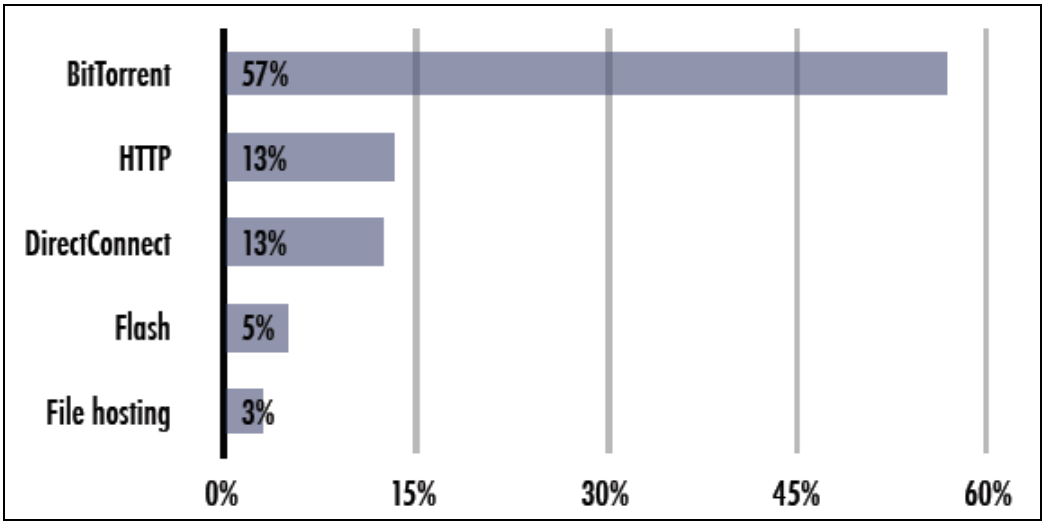
Učinkovitost *peer-to-peer* mreža je glavni razlog velike popularnosti ovakve arhitekture. Primjerice, kod preuzimanja neke datoteke s web stranice korisnik mora poslužitelju poslati zahtjev za preuzimanje. Dakle, korisnik komunicira samo s jednim poslužiteljem i preuzima datoteku samo s jednog poslužitelja. Kad su u pitanju *peer-to-peer* mreže, pri preuzimanju neke datoteke korisnik je u mogućnosti istu primati od više drugih sudionika mreže istovremeno. *Peer-to-peer* mreže se primjenjuju za:

- dijeljenje podataka,
- istraživanja i znanstvene informacije,
- pregledavanje multimedijskih sadržaja,
- glasovnu komunikaciju putem Interneta (VoIP) te
- pismenu komunikaciju putem Interneta.

4.1. Peer-to-peer mreže za dijeljenje podataka

Trenutno najpopularnija upotreba *peer-to-peer* mreža je pri dijeljenju podataka među korisnicima. Preuzimanje putem ovakvih mreža može, ali i ne mora biti brže od preuzimanja izravno sa poslužitelja. U tu svrhu razvijen je cijeli niz računalnih programa koji korisnima omogućuju preuzimanje besplatnih sadržaja od drugih korisnika. Sadržaji koje je moguće preuzeti od drugih korisnika ovakvim programima uključuju multimedijske datoteke, podatke, druge programe, itd. Međutim, preuzimanje ovakvih sadržaja nije uvijek zakonito pa je potrebno i o tome voditi računa prilikom preuzimanja sadržaja.

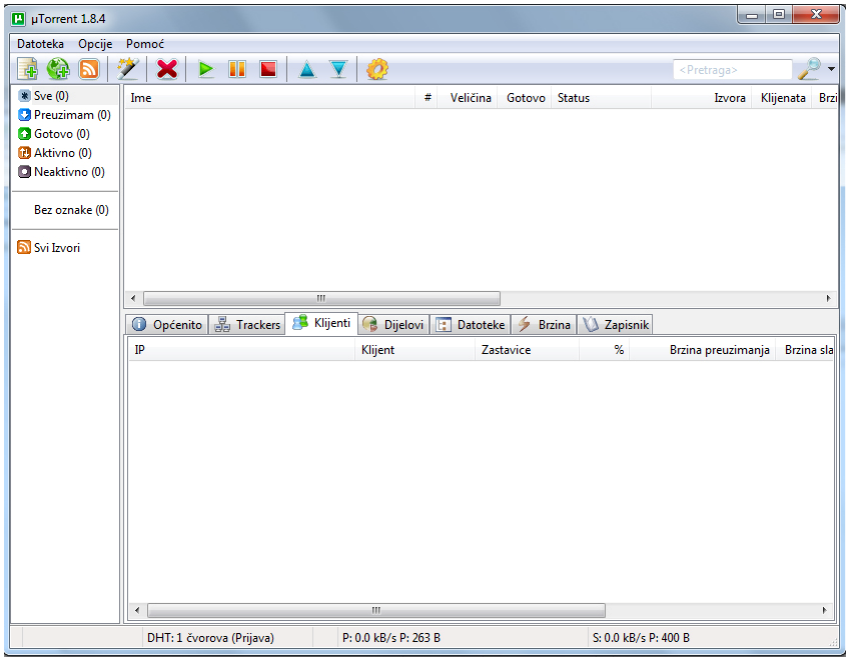
Najpopularnija mreža za dijeljenje podataka među korisnicima je *BitTorrent P2P* mreža koja se temelji na *BitTorrent* protokolu za dijeljenje velikih količina podataka. *BitTorrent P2P* mreža je vrlo popularna zbog velikog broja web stranica na kojima je moguće pronaći datoteke, ali i zbog raznovrsnosti datoteka dostupnih za preuzimanje. Također postoje i druge *peer-to-peer* mreže poput *Gnutelle* ili *Freeneta*. Prema istraživanju tvrtke Ipoque za 2008. i 2009. godinu, procijenjeno je da se putem *BitTorrent* mreže, ovisno o geografskoj lokaciji, ostvaruje 27-55% svog Internet prometa. U području istočne Europe čak 57% svog Internet prometa ostvareno je putem *BitTorrent* mreže. U nastavku su prikazani postoci prometa ostvareni korištenjem *peer-to-peer* mreža, pregledavanjem Interneta i sličnim aktivnostima.



Slika 5. Ostvareni promet u pojedinoj mreži za područje istočne Europe

Izvor: Ipoque

Putem Interneta moguće je preuzeti velik broj programa koji se temelje na *BitTorrent* protokolu za dijeljenje podataka. Jedan od takvih programa je *µTorrent,* besplatan alat za rad s *BitTorrent P2P* protokolom.



Slika 6. Prikaz grafičkog sučelja programa *µTorrent*

Podaci se preuzimaju putem *„.torrent“* datoteka koje sadrže adrese drugih sudionika mreže koji posjeduju tražene podatke. *Torrent* datoteke je moguće pronaći na Internetu putem tražilica, ali i izravnom pretragom u samom programu *µTorrent*.

4.2. Peer-to-peer mreže za istraživanja i znanstvene informacije

Istraživanja u znanstvenim područjima su mnogo učinkovitija kada su znanstvenici u mogućnosti pregledavati sadržaje koji ih zanimaju i koji bi im mogli koristiti u istraživačkom radu. Umrežavanjem i stvaranjem velikih *peer-to-peer* mreža u svrhu povezivanja interesnih skupina postignut je značajan napredak u dostupnosti materijala potrebnih za istraživački rad. Primjer takve mreže je *Sciencenet* razvijen na Institutu tehnologije u Karlsruheu.

4.3. Peer-to-peer mreže za multimediju

Osim popularnih web servisa za pregledavanje multimedijskih sadržaja, također postoje i *peer-to-peer* mreže za pregledavanje tih istih sadržaja. Takva vrsta pregledavanja zove se *peercasting,* koji se razlikuje od standardnog načina emitiranja sadržaja (*eng. Broadcasting*) putem Interneta. Razlika je u načinu dijeljenja sadržaja, tj. umjesto pregledavanja putem središnjeg poslužitelja svaki sudionik mreže koji pregledava multimedijske sadržaje ujedno i odašilje isti taj sadržaj drugim sudionicima mreže. Ovaj način pregledavanja multimedijskih sadržaja najčešće uključuje preslušavanje glazbenih zapisa, gledanje video zapisa, te gledanje televizijskih programa (ovisno o mogućnostima mreže). Primjer ovakve mreže je *P2PTV* koji sudionicima omogućuje pregledavanje multimedijskih sadržaja u stvarnom vremenu. Više o P2PTV mrežama moguće je saznati na adresi:

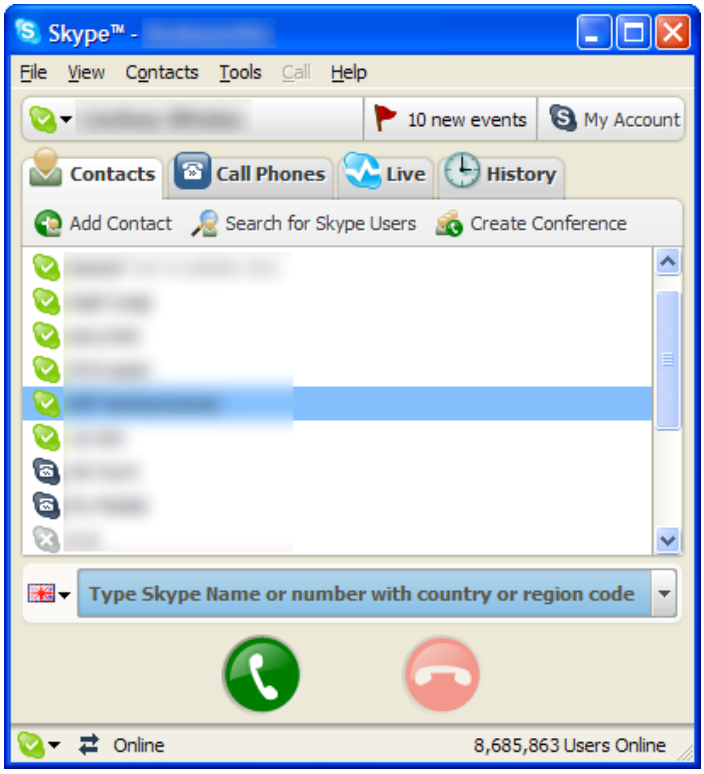
http://en.wikipedia.org/wiki/P2PTV

4.4. Glasovna i pismena komunikacija (VoIP)

VoIP (*eng. Voice over Internet Protocol*) je način komunikacije korisnika putem Interneta. Uslijed financijski nepovoljnih okolnosti razvoja programa koji će biti smješteni na poslužiteljima, razvijene su *peer-to-peer* mreže za glasovnu komunikaciju. Korisnicima su omogućeni besplatni razgovori s

računala na računalo, te povoljni razgovori ukoliko korisnik ostvaruje poziv sa računala na fiksnu ili mobilnu liniju.

Jedan od besplatnih *peer-to-peer VoIP* programa je popularni program *Skype* koji korisnicima omogućuje glasovne i video pozive, dopisivanje i razmjenu podataka putem *Skype peer-to-peer* mreže.



Slika 7. Prikaz korisničkog sučelja *VoIP* programa *Skype*

4.5. Statistike korištenja peer-to-peer mreža

U ovom poglavlju prikazane su statistike korištenja *peer-to-peer* mreža prikazane u izvješću „*Internet Study 2008/2009*“ tvrtke Ipoque. Statistički podaci navedeni u nastavku pružaju najbolji uvid u popularnost *peer-to-peer* mreža. Izvještaj tvrtke Ipoque je izrađen na temelju podataka koje su ustupili ponuđači Internet usluga i sveučilišta diljem svijeta.

U sljedećoj tablici su navedene najčešće korištene *peer-to-peer* mreže razvrstane prema zemljopisnim područjima.

Tablica 1. Prikaz najčešće korištenih *peer-to-peer* mreža prema područjima

MREŽA	Južna Afrika	Južna Amerika	Istočna Europa	Sjeverna Afrika	Južna Europa	Bliski Istok	Jugozapadna Europa
Sve P2P	65,77%	65,21%	69,95%	42,51%	55,12%	44,77%	54,46%
Ares	0,29%	42,63%	0,00%	2,24%	0,16%	0,11%	1,80%
BitTorrent	48,34%	30,02%	80,83%	74,51%	48,94%	78,85%	58,20%
DirectConnect	0,01%	0,00%	17,87%	0,08%	0,00%	0,12%	0,30%
eDonkey	2,48%	25,99%	1,16%	7,70%	47,17%	15,37%	35,99%
Gnutella	18,60%	0,36%	0,14%	14,21%	1,66%	5,00%	2,75%
iMesh	13,60%	0,02%	0,00%	0,47%	0,03%	0,00%	0,14%
Thunder	14,04%	0,80%	0,00%	0,69%	1,64%	0,52%	0,62%
Druge	2,64%	0,19%	0,00%	0,10%	0,41%	0,03%	0,21%

Iz tablice je vidljiv podatak o zastupljenosti pojedine *peer-to-peer* mreže u navedenim zemljopisnim područjima. Vidljivo je da je u svim navedenim područjima najčešće korištena *peer-to-peer* mreža *BitTorrent*, najveći postotak zastupljenosti *BitTorrent* mreže od čak 80% je u istočnoj Europi, gdje spada i Hrvatska. Naime, programi za preuzimanje putem BitTorrent P2P mreže vrlo brzo i učinkovito preuzimaju velike datoteke dostupne na mreži. Upravo zbog toga, preuzimanje video zapisa, te programskih paketa je vrlo brzo. Ostala područja imaju nešto manju zastupljenost spomenute *peer-to-peer* mreže.

Pri proučavanju sadržaja prisutnog na *peer-to-peer* mrežama, otkriveno je sljedeće:

- Video zapisi su najpopularniji sadržaj prema količini i broju podataka.
- Programi su drugi najpopularniji sadržaj na *BitTorrent* mreži s trećinom ostvarenog prometa.
- Glazbene datoteke su drugi najpopularniji sadržaj na *eDonkey* (decentralizirana *peer-to-peer* mreža vrlo dobra za preuzimanje velikih datoteka) mreži.

5. Sigurnosni problemi peer-to-peer mreža

Peer-to-peer mreže, za razliku od centraliziranih mreža s poslužiteljem, nemaju primjeren nadzor. Korištenje *peer-to-peer* mreža u privatnom, a pogotovo u poslovnom okruženju predstavlja velik rizik. Tvrtke i korisnici sve više i više postaju svjesni opasnosti korištenja *peer-to-peer* mreža. Datoteke na *peer-to-peer* mreži za koje se tvrdi da su glazbeni ili video zapisi zapravo mogu sadržavati druge različite sadržaje štetne za računala korisnika. Kada korisnik postavi *peer-to-peer* program na vlastito (ili poslovno) računalo, nije moguće utvrditi hoće li preuzete datoteke nanijeti štetu računalu i podacima na njemu. Dakle, korisnik može uz željenu datoteku preuzeti viruse ili crve, te na taj način ugroziti vlastito računalo ili cijeli mrežni sustav tvrtke. Također, računala koja su sudionici *peer-to-peer* mreža često bivaju zaražena *spyware* programima koji prate aktivnost korisnika, te prikupljaju povjerljive podatke i informacije.

5.1. Spyware programi

Spyware programi su zlonamjerni programi namijenjeni praćenju aktivnosti korisnika na Internetu i prikupljanju podataka o korisniku, bez njegovog znanja i pristanka, a sve u svrhu otkrivanja prikupljenih podataka zainteresiranim stranama. Prisutnost *spyware* programa na računalima korisnika je postala zabrinjavajuća jer velik dio korisnika nije svjestan da su njihova računala zaražena nekom vrstom *spyware* programa. *Spyware* programi najčešće uzrokuju usporen rad računala, pojavu neželjenih oglasnih materijala, gubitak povjerljivih informacija, itd.

Slika 8. Štetno djelovanje *spyware* programa

Izvor: Google

Korisnici vrlo često ugrožavaju vlastita računala i podatke preuzimanjem datoteka putem *peer-to-peer* mreža. Razlog tome je taj da se *spyware* programi najčešće nalaze pohranjeni u drugim, popularnim programima i datotekama. Nakon što korisnik preuzme i pokrene datoteku ili program koji sadrži *spyware*, računalo biva zaraženo. *Peer-to-peer* mreže su vrlo popularan način za širenje *spyware* programa zbog velikog broja korisnika.

Spyware programi također mogu uzrokovati i druge vrste napada na računalo korisnika, te mogu imati sljedeće funkcije:

- zapisivanje posjećenih URL adresa,
- snimanje zaslona korisnika,
- snimanje poruka e-pošte i zapisivanje razgovora,
- zapisivanje tipki i snimanje lozinki,
- otimanje web preglednika i veze s Internetom, itd.

Više o *spyware* programima moguće je saznati u dokumentu „Spyware programi“ (CCERT-PUBDOC-2009-10-280) objavljenom na službenim stranicama CERT-a.

http://www.cert.hr/documents.php?id=395

5.2. Virusi i crvi

Peer-to-peer mreže je moguće, uslijed nedostatka primjerenog nadzora i mjera sigurnosti, iskoristiti za širenje zlonamjernih programa poput virusa i crva. Virusi i crvi se mogu na *peer-to-peer* mreži predstaviti kao korisni programi, te zavarati korisnika da ih preuzme. *Peer-to-peer* programi omogućuju korisnicima izravno dijeljenje i slanje datoteka čime se zaobilaze sigurnosni mehanizmi poput vatrozida i antivirusnih alata što im u konačnici omogućuje brzo i učinkovito širenje s računala na računalo.

- Crvi su zlonamjerni programi koji se upisuju u radnu memoriju računala u kojoj ostaju aktivni. Upravo zato jer ostaju aktivni u radnoj memoriji računala, lako se šire na druga računala i u kratkom vremenskom periodu su sposobni zaraziti velik broj računala. Virusi mogu uzrokovati druge vrste napada na računalo korisnika poput neovlaštenog udaljenog pristupa ili postavljanje drugih vrsta zlonamjernih programa na računalo korisnika.
- Virusi su zlonamjerni programi koji se zapisuju na tvrdi disk računala, te iskorištavaju sigurnosne propuste u programima ili operacijskim sustavima kako bi nanijeli štetu računalu i podacima koji se na njemu nalaze. Virusi se najčešće šire uz pomoć drugih programa ili datoteka kako korisnik ne bi zamijetio zarazu zlonamjernim programom.

Otkriveni su posebni tipovi virusa i crva napravljeni specijalno za P2P mreže. Takvi virusi i crvi mogu se mogu pojaviti u dijeljenim mapama na korisničkom računalu, te zavarati korisnika da ih pokrene. Primjeri takvih virusa i crva su *Swen, Fizzer, Lirva, Benjamin, KwBot, Bodiru*, itd. Ovi zlonamjerni programi najčešće su pronađeni na *eDonkey P2P* mreži.

5.3. Napadači

Kao što je ranije napomenuto, napadači su u mogućnosti izvesti udaljeni napad na računalo korisnika koje je prisutno u *peer-to-peer* mreži. Većina *peer-to-peer* programa drugim sudionicima mreže prikazuje IP (*eng. Internet Protocol*) adresu korisnika, što predstavlja veliku opasnost. Poznavanje IP adrese žrtve napadaču uvelike olakšava zlonamjerno djelovanje. Napadač je u mogućnosti putem *peer-to-peer* mreže, iskorištavanjem sigurnosnih propusta u korištenim programima ili operacijskom sustavu, spojiti se na računalo korisnika i izvesti udaljeni napad ili proizvoljni zlonamjerni programski kod.

Tako primjerice, napadač može upotrijebiti računalo drugog korisnika za zlonamjerno djelovanje kako bi prikrio vlastiti identitet. Poznati su slučajevi u kojima je napadač upotrijebio računala drugih korisnika za širenje zlonamjernih programa, slanje neželjenih poruka e-pošte (*eng. spam*) ili za izvođenje udaljenih napada na druge mrežne sustave.

Više je moguće saznati u dokumentu „Računala mamci i ponašanje napadača“ (CCERT-PUBDOC-2008-09-241) objavljenom na službenim stranicama CERT-a.

5.4. Krađa i uništavanje podataka

Podaci prisutni na računalima korisnika *peer-to-peer* mreže su također u opasnosti, pogotovo kada su u pitanju mrežni sustavi tvrtki. Naime, takvi sustavi mogu sadržavati veliku količinu osjetljivih i povjerljivih podataka, te intelektualno vlasništvo. Krađom ovakvih podataka moguće je nanijeti veliku materijalnu štetu pojedincu ili tvrtki. Zlonamjerni programi postavljeni na računala korisnika mogu napadačima omogućiti pristup podacima koji se nalaze izvan dijeljenih mapa koje je odredio. Određeni virusi i crvi izrađeni samo za *peer-to-peer* mreže imaju upravo funkciju da promijene dijeljene mape, te omoguće napadačima uvid u sve podatke na računalu korisnika. Međutim, zlonamjerna djelovanja nisu uvijek usmjerena na stjecanje materijalne koristi krađom, već im je ponekad cilj i/ili uzrokovanje štete na podacima.

5.5. Povjerljivost podataka

Većina *peer-to-peer* mreža daje svim sudionicima mreže izravan pristup podacima pohranjenim na tvrdom disku računala. Korisnici su u mogućnosti odabrati koje dokumente i podatke žele dijeliti s drugim sudionicima mreže, te tako osigurati da povjerljivi podaci i informacije nisu dijeljeni na mreži. Međutim, uslijed nedostatka nadzora i mjera sigurnosti, te prikazivanjem IP adrese korisnika, napadači su u mogućnosti otkriti koji operacijski sustav računalo koristi, te pristupiti istom. Zbog mogućnosti pristupa računalu korisnika, moguć je scenarij u kojem će napadač preuzeti nadzor nad cjelokupnim računalom. Pristupanjem računalu korisnika napadač otkriva podatke i informacije koje korisnik ne želi dijeliti sa drugim sudionicima mreže, te tako narušava povjerljivost podataka pohranjenih na računalu.

5.6. Autentikacija

Razlog velike popularnosti *peer-to-peer* mreža je neograničen protok podataka među sudionicima, što ujedno predstavlja i veliki problem. Svaki sudionik *peer-to-peer* mreže je u mogućnosti pristupiti podacima dostupnim na mreži čime su, u slučaju postojanja zlonamjernog sudionika, ugroženi drugi sudionici. Nedostatak metoda za autentikaciju sudionika koji žele pristupiti dijeljenim podacima na mreži može uzrokovati velike štete. Primjerice, ukoliko se radi o povjerljivim podacima potrebno je utvrditi identitet sudionika koji želi pristupiti podacima. Autentikacija putem *peer-to-peer* mreža u ovakvim slučajevima nije moguća, stoga se ne preporuča dijeljenje osjetljivih podataka i informacija putem *peer-to-peer* mreža.

5.7. Nedozvoljeni sadržaji i roditeljska zaštita

Također, problem kod *peer-to-peer* mreža je dijeljenje nedozvoljenih sadržaja bilo da se radi o sadržajima zaštićenim autorskim pravima ili zakonom zabranjenih sadržaja. Dijeljenje sadržaja zaštićenih autorskim pravima nije moguće nadzirati u *peer-to-peer* mrežama, međutim u nekim zemljama su uspostavljene uspješne mjere koje onemogućavaju dijeljenje ovakvih sadržaja. Naime, ponuđači Internet usluga su u nekim zemljama (Japan, Australija, Nizozemska, itd.) ograničili ili potpuno zabranili dijeljenje sadržaja putem *peer-to-peer* mreža u svrhu zaštite autorskih prava umjetnika. Osim toga, primjerice u SAD-u se primjenjuju strogi zakoni kada su u pitanju autorska prava, te kršenje istih može rezultirati zakonskim mjerama. Kod zakonski zabranjenih sadržaja je nešto teže spriječiti dijeljenje, ali i ovakvi podaci također podliježu strogim zakonskim mjerama. Razlog velike popularnosti *peer-to-peer* mreža u istočnoj Europi je upravo izostanak primjerenih zakonskih okvira.

Broj djece i maloljetnika prisutnih na Internetu i *peer-to-peer* mrežama je u stalnom porastu. Uslijed izostanka primjerene zaštite na *peer-to-peer* mrežama, djeca su u mogućnosti preuzimati sadržaje koji nisu primjereni njihovoj dobi. Roditelji bi trebali nadzirati aktivnost vlastite djece i po mogućnosti zabraniti im preuzimanje neprimjerenih sadržaja koji mogu uključivati:

- pornografske sadržaje,
- sadržaje vezane uz maloljetnicima nedozvoljena sredstva (droga, alkohol, itd) i
- sadržaje u kojima se prikazuje nasilje.

Djeca i maloljetnici često nisu svjesni da posjedovanje ovakvih sadržaja, od kojih su neki zakonski zabranjeni, na računalu podliježe zakonskim mjerama.

5.8. Špijunaža

Kod programa za glasovnu ili pismenu komunikaciju koji korisnike povezuju *peer-to-peer* infrastrukturom postoji opasnost od presretanja podataka poslanih drugim sudionicima. Zlonamjerni korisnik je korištenjem zlonamjernih programa ili iskorištavanjem sigurnosnih propusta u korištenim programima u mogućnosti presretati poruke koje sudionici međusobno izmjenjuju. Osobitu opasnost predstavljaju programi za komunikaciju u kojima ne postoje algoritmi za kriptiranje podataka (*eng. Encryption*). Uporaba ovakvih programa u poslovnim mrežnim sustavima može uzrokovati otkrivanje povjerljivih podataka.

6. Sigurno korištenje peer-to-peer mreža

Navedene sigurnosne probleme *peer-to-peer* mreža nije nemoguće riješiti. *Peer-to-peer* mreže imaju svoje slabosti koje je moguće ukloniti nekim metodama. Najveći problem kod *peer-to-peer* mreža je svakako neograničen i nekontrolirani pristup sudionicima mreže, stoga su u nastavku navedeni neki sigurnosni mehanizmi koje danas neki *peer-to-peer* programi koriste:

- *tehnika tajnog ključa* (*eng. Secret Key Technique*) - ova se tehnika temelji na činjenici da dva sudionika, koji međusobno komuniciraju, dijele tajni ključ koji se koristi za razne kriptografske operacije poput šifriranja i dešifriranja poruka. Tajni je ključ potrebno razmijeniti odvojenim procesom prije početka komunikacije.
- *tehnika javnog ključa (eng. Public Key Technique)* - ovakve se tehnike temelje na asimetričnim parovima ključeva. Najčešće, jedan korisnik posjeduje samo jedan par ključeva. Jedan je ključ dostupan drugim sudionicima, dok je drugi ključ tajan. Više o PKI (*eng. Public Key Infrastructure*) infrastrukturi moguće je saznati u dokumentu „Nedostaci PKI infrastrukture“ (CCERT-PUBDOC-2009-09-255) objavljenom na službenim stranicama CERT-a.
- *tehnika parova asimetričnih ključeva (eng. Asymmetric Pair Key*) - temelji se na asimetričnom javnom ključu kojim se može uspješno šifrirati poruke, ali ne može dešifrirati poruke.

Uz navedene tehnike također se preporuča:

- *korištenje antivirusnih i antispyware alata, te vatrozida* - korištenjem navedenih alata korisnik osigurava svoje računalo i podatke na računalu od zlonamjernih programa. Također, vatrozidi sprječavaju udaljene napade, te tako onemogućuju napadačima pristup računalu, krađu ili uništavanje podataka.
- *redovito ažuriranje korištenih programa i operacijskog sustava* - u programima na računalu, ali i operacijskom sustavu moguća je pojava sigurnosnih propusta, stoga je ažuriranje istih u svrhu povećanja razine zaštite nužno.
- *zaštita podataka na računalu i izrada sigurnosnih kopija* - ukoliko korisnici žele biti prisutni na *peer-to-peer* mrežama, poželjno je da prethodno zaštite osjetljive i povjerljive podatke, uklone ih sa računala ili izrade sigurnosne kopije istih.
- *zaštita privatnosti* - u svrhu zaštite privatnosti, korisnicima se preporuča korištenje programa i sredstava za zaštitu privatnosti, te prikrivanje IP adrese (korištenjem zamjenskih - *proxy* poslužitelja, šifriranom komunikacijom među sudionicima koji razmjenjuju podatke, itd.) koja potom neće biti vidljiva drugim sudionicima na *peer-to-peer* mreži.
- *izbjegavanje sadržaja zaštićenih autorskim pravima* - kao što je ranije napomenuto, nedozvoljeno preuzimanje sadržaja zaštićenih autorskim pravima je zakonski kažnjivo, stoga se ne preporuča preuzimanje istih. Ovakvi programi najčešće sadrže i neku vrstu zlonamjernog koda integriranu u sami program.
- *nadzor djece i maloljetnika prisutnih na peer-to-peer mrežama* - kako bi se djecu zaštitilo od neželjenih sadržaja i sadržaja koji nisu primjereni njihovoj dobi, potrebno je primijeniti nadzor kada koriste *peer-to-peer* programe ili u potpunosti zabraniti njihovo korištenje.

Primjenom navedenih preporuka razina sigurnosti korisnika prisutnog na *peer-to-peer* mreži će uvelike porasti. Također, jedan od važnih dijelova zaštite od opasnosti koje prijete na *peer-to-peer* mrežama je edukacija korisnika kako bi bili svjesni mogućih posljedica neopreznog djelovanja.

7. Zaključak

Peer-to-peer mreže svakako pomažu u razvoju komunikacije i razmjeni podataka među sudionicima. Svaki sudionik je u mogućnosti pristupiti dijeljenim podacima drugog korisnika, što predstavlja moguću prijetnju za sigurnost računala korisnika i podataka koje isto sadrži. Dijeljenje podataka putem *peer-to-peer* mreža se temelji na uspostavljanju međusobnog povjerenja sudionika. Takav je koncept u današnje vrijeme, obzirom na broj zlonamjernih sudionika i programa, gotovo neprihvatljiv (jer sudionici ne mogu nikakvim kriterijem otkriti radi li se o zlonamjernom sudioniku). Najčešći problemi svakako su zaraza računala i podataka zlonamjernim programima, krađa i uništavanje podataka, te vjerojatno najveći problem - dijeljenje nedozvoljenih sadržaja i zakonom zaštićenih sadržaja. U nekim državama su uvedene zakonske mjere za sudionike *peer-to-peer* mreža koji preuzimaju zakonom zaštićene sadržaje.

Sudeći prema trenutačnoj popularnosti razmjene podataka i datoteka putem *peer-to-peer* mreža, za očekivati je da će *peer-to-peer* mreže u budućnosti još više olakšati traženje podataka putem Interneta. U razvoju je nekoliko koncepata za koje se vjeruje da će u budućnosti postati standardi u *peer-to-peer* mrežama. Naravno, riječ je o metodama raspoznavanja sudionika mreže kako bi se ograničio trenutačno neograničen pristup drugim sudionicima.

Jedna od takvih metoda je stjecanje povjerenja drugih sudionika. Dakle, na *peer-to-peer* mreži je teško procijeniti kojem sudioniku vjerovati, a kojem ne. Stoga je predložen vrlo zanimljiv koncept ocjenjivanja povjerenja u druge sudionike *peer-to-peer* mreže. Prema ovom konceptu, svaki sudionik bi se dodijelio jedinstven digitalni potpis (*eng. Digital Signature*) koji je povezan s razinom povjerenja od sudionika. Ta vrijednost bi se kretala u određenim numeričkim vrijednostima, gdje bi veća vrijednost označavala veće povjerenje, a niža manje. Zlonamjerne aktivnosti određenog sudionika bi uzrokovale snižavanje razine povjerenja u istog, te naposljetku i mjere zabrane pristupa mreži. Ovaj je koncept tek u razvoju i potrebno je mnogo rada i truda kako bi ovakav način rada *peer-to-peer* mreža bio ostvaren. Više o ovakvom i sličnim konceptima moguće je saznati na adresi:

http://www.p2ptrust.org/trust/trust.html

Također, za vjerovati je da će se u budućnosti koristiti određene vrste autentikacije sudionika na *peer-to-peer* mreži. Moguće je koristiti dvo ili više faktorsku autentikaciju. Metode autentikacije koje će biti primijenjene radi podizanja razine sigurnosti sudionika na mreži ovisiti će o kvaliteti tehnologije, te jednostavnosti izvedbe.

Peer-to-peer mreže su korisne za napredak društva u pogledu dijeljenja informacija, međutim potrebno je postaviti neke zakonske okvire kojima će se regulirati ponašanje sudionika peer-to-peer mreža kako bi se spriječilo zlonamjerno djelovanje radi nanošenja štete drugim sudionicima.

8. Reference

[1] Peer-to-peer arhitektura, http://en.wikipedia.org/wiki/Peer-to-peer, studeni 2009.

[2] Sve o peer-to-peer arhitekturi, http://www.webopedia.com/DidYouKnow/Internet/2005/peer_to_peer.asp, svibanj 2005.

[3] Prednosti i nedostaci peer-to-peer mreža, http://freedom-to-tinker.com/blog/felten/cost-tradeoffs-p2p, listopad 2005.

[4] Internet statistike, http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009, listopad 2009.

[5] Peer-to-peer mreže, http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html#TheFutureofP2PSecurity, 2003.

[6] Sigurnost peer-to-peer mreža, http://www.websense.com/docs/WhitePapers/PeertoPeer.pdf, 2009.

[7] Sigurnost peer-to-peer mreža, http://allan.friedmans.org/papers/P2Psecurity.pdf, 2009.

[8] eDonkey P2P mreža, http://en.wikipedia.org/wiki/EDonkey_network, 2009.

[9] BitTorrent P2P mreža, http://en.wikipedia.org/wiki/BitTorrent_%28protocol%29, 2009.