INSTANT MESSAGING
White paper

Nina Marević

Lipanj 2006.

Sadržaj:

1. Uvod

Instant Mesaging je oblik komunikacije koji je zabilježio najbrži porast u korištenju zahvaljujući svojoj specifičnosti – omogućava komunikaciju u realnom vremenu, što ga čini prikladnijim od e-maila, (korisnik je trenutno obavješten o poruci i može jednostavno i brzo na nju odgovoriti), a opet manje je nametljiv i manje ometa od telefona (nije potrebno odgovoriti iste sekunda, nema zvonjave ako se ne javi odmah).

Ipak ima i svoje nedostatke – a to je nezaštićenost od virusa, crva, spyware-a i ostalog štetnog software-a.

U ovom dokumentu će biti iznesene prednosti i mane korištenja sustava za slanje poruka u realnom vremenu, te dan pregled najčešće korištenih protokola i najpopularnijeg software-a za IM.

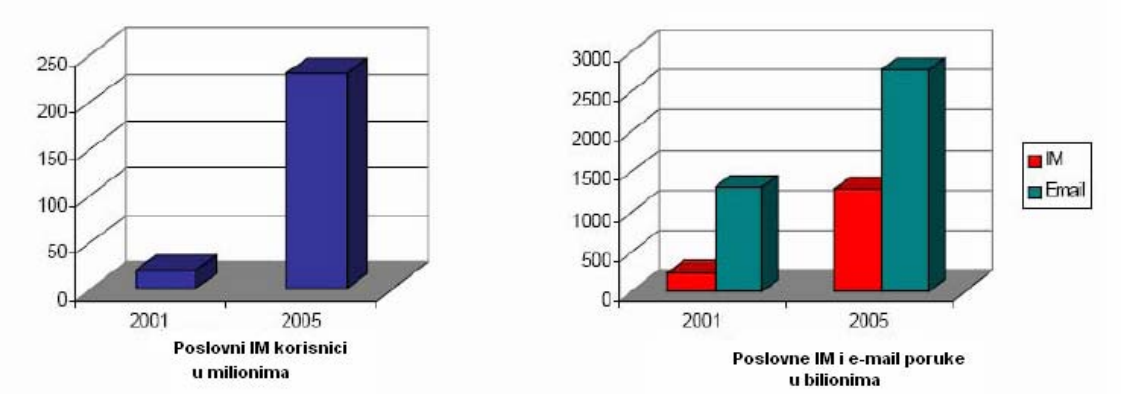
2. Što je to Instant Messaging?

Instant messaging je elektronički oblik komunikacije koji omogućuje da korisnici jedan drugome ili grupno šalju poruke u realnom vremenu, preko standardnog IP protokola.
Upotreba instant messaging-a enormno brzo raste, procjenjuje se da ima više od 300 miliona korisnika.

Tvrtke poput AOL-a, MSN-a i Yahoo!-a prijavljuju više od bilion poslanih poruka dnevno i procjenjuju da će učestalost uporabe IM-a uskoro prerasti učestalost uporabe e-maila.

Iako se inicijalno koristio za neformalno komuniciranje i to uglavnom među mlađom populacijom, instant messaging nalazi svoje mjesto i u poslovnom svijetu.

Osnovna razlika u odnosu na obični „chat" je omogućena komunikacija „jedan na jedan" između dva korisnika u IM mreži, ili eventualno više onih koje sam korisnik odabere. To ga čini puno privatnijim i diskretnijim od klasičnog „chata".
Tipično u mreži svako korisnik ima korisničko ime i kontakt listu korisnika s kojima najčešće komunicira.



Slika 2. Uporaba IM-a

3. Instant Messaging arhitektura

Postoje dvije osnovne arhitekture: arhitektura korisnik – korisnik i arhitektura korisnik – server.

U **korisnik – korisnik** arhitekturi određenog korisnika možemo zamisliti kao čvor, a svakog na njegovoj kontakt listi kao granu orijentiranu prema van. IM možemo predstaviti kao neuravnoteženi graf čiji čvorovi kako vrijeme prolazi nastaju i nestaju. Također po nekoj logici možemo pretpostaviti da će onaj čvor koji ima veću kontakt listu imati veću vjerojatnost da s vremenom nakupi sve više čvorova (kontakata) te da sam bude dodan na njihovu kontakt listu.

U **korisnik - server** arhitekturi server upravlja komunikacijom i podržan je od davatelja usluge (Microsoft, npr.). Server nije odgovoran samo za prenošenje poruka korisniku kome su poslane, nego i za provjeravanje identiteta korisnika, i za verifikaciju njegovog online statusa.

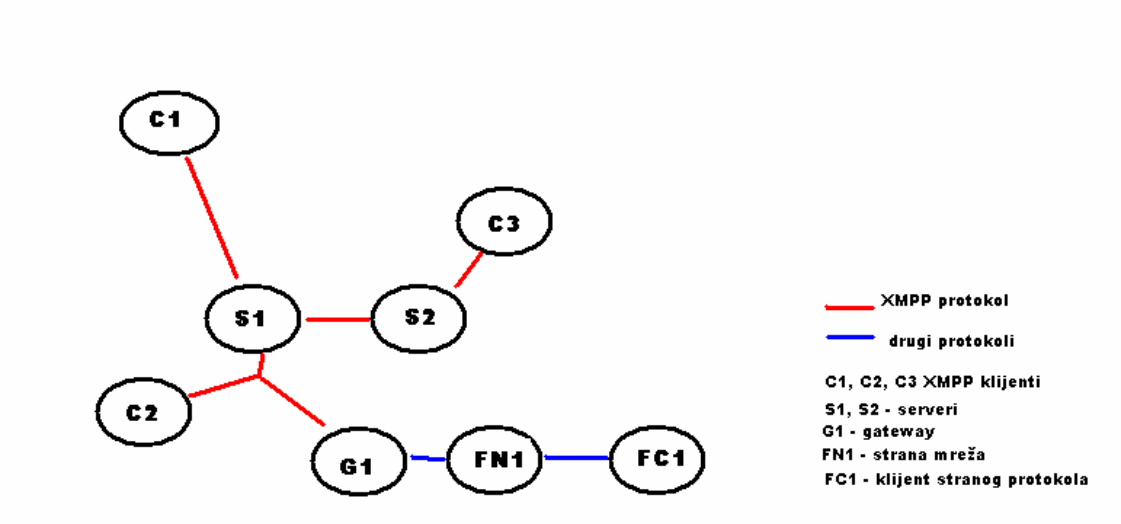
4. Pregled IM protokola

4.1. Jabber

1998. ga je pokrenuo Jeremie Miller želeći sve IM klijente skupiti pod jedno i ponuditi im koristan software jednostavan za uporabu.
Jabber je fleksibilna, višenamjenska i „višeprotokolna“ komunikacijska platforma zasnovana na XML-u.

Zasniva sa na arhitekturi e-mail sistema, tako da za razliku od AOL-a ili MSN-a koji imaju jedan centralni server, **Jabber ima mnogo servera na mnogo lokacija.**
Ovo je velika prednost, jer znatno povećava pouzdanost – naime ako se jedan od servera iz bilo kojeg razloga sruši, jednostavno je prebaciti se na drugi server.

Komunikacija se odvija na principu korisnik - server. Korisnik pristupa serveru preko TCP-a, ali i server s drugim serverom razgovara također preko TCP-a.
Dakle korisnik može komunicirati s drugim korisnikom na istom ali i na drugom serveru, jer serveri mogu komunicirati međusobno.



Slika 2. Jabber mreža

Server predstavlja „inteligentni“ sloj, čija je glavna zadaća da usmjerava podatke od i prema logiranim korisnicima i drugim serverima. Pošto je zasnovan na korisnik – server, a ne korisnik – korisnik arhitekturi, sve poruke od jednog korisnika drugom najprije moraju proći kroz server.

Glavna funkcija **Gatewaya** je da prevodi XMPP u protokole koji se koriste u ostalim sustavima za dopisivanje. Npr. postoje gateway-i prema e-mailu (SMTP), Internet Relay Chat-u (IRC), Short Message Service-u (SMS), te drugim sustavima za slanje poruka u realnom vremenu poput Yahoo i MSN Messenger-a.
To je velika prednost Jabber-a – omogućava sve protokole u jednom preglednom i za korištenje jednostavnom paketu.

Korisnici također mogu odlučiti za koga će biti vidljivi, a za koga ne. Naime oni koji žele komunicirati s vama najprije moraju zatražiti vaše dopuštenje, a nastaviti pisati mogu tek kad im to odobrite.

4.2. Oscar protokol

Oscar protokol (Open System for Comunication in Realtime) je IM protokol koji se korisiti u ICQ i AOL sofrware-u za slanje poruka, specifikacija protokola je zaštićena zakonom i ulaže se veliki trud da bi se konkurencija (Jabber, Microsoft) spriječili da naprave kompatibilne sisteme za slanje poruka.
Podatci se šalju preko TCP protokola, TCP paket ima u sebi sadržan Oscar paket.

4.3. IRC

IRC (Internet Relay Chat) je oblik internet komunikacije, uglavnom je dizajniran za grupnu komunikaciju u diskusijskim forumima koji se zovu ***kanali*** , ali također podržava „jedan na jedan“ komunikaciju.
Kreirao ga je Jarkko Oikarinen 1988. inspiriran programom MUT (Multi User Talk).
IRC protokol nije zaštićen zakonom i može ga koristiti svatko tko ima server da kreira vlastitu sobu za chat.
Baš zbog toga doprinosi decentralizaciji IM servisa i zato se još uvijek koristi.
Da bi se priključio chatu na IRC-u korisnik mora definirati server (npr. oblika: server.net) i kanal (#imekanala).

4.4. MSN Protocol

MSN messenger protokol je zasnovan na ASCII kodu, decentraliziran je - svaki server u mreži može provjeriti autentičnost korisnika.
Svi serveri su u messenger.hotmail.com sub-domeni povezani preko porta 1863.
Korisnik ne može promijeniti ovaj port.

MSN lozinke su šifrirane korištenjem MD5 hash algoritma.

MSN server genrira korijen npr:
USR5MD5S 989048851.1852237230
Kojemu klijent doda string poput:
Q1P7W2E4J9R8U3S5
Što rezultira sa:
USR5MD5S 989048851.1852237230 Q1P7W2E4J9R8U3S5
Što se dalje šifrira spomenutim algoritmom da bi se dobilo nešto poput: 0212eaad0876afb8505859ca75d21a78

Očito je daje teško dobiti lozinku iz korijena i šifrirane riječi.

Poruka se šalje u HTML kodu od jednog korisnika drugom kroz centralni server. Poruka se serveru šalje preko TCP-a port 1863.

Poruke nisu šifrirane tako da treba biti svjestan da ono što se šalje preko MSN protokola može imati jako veliku publiku.

4.5. Usporedba Instant Messaging protokola:

	Autor	Prvo izdanje	Identitet u mreži
IRC	Jarkko Oikavinen	Kolovoz 1988.	Nick username@hostname
Jabber	Jeremie Miller	Svibanj 2000.	Jabber ID
MSNP	Microsoft	Srpanj 1999	e-mail adresa (.NET passport)
OSCAR	AOL		Username (usernumber)

Tablica 1. Usporedba IM protokola

5. Pregled software-a za instant messaging

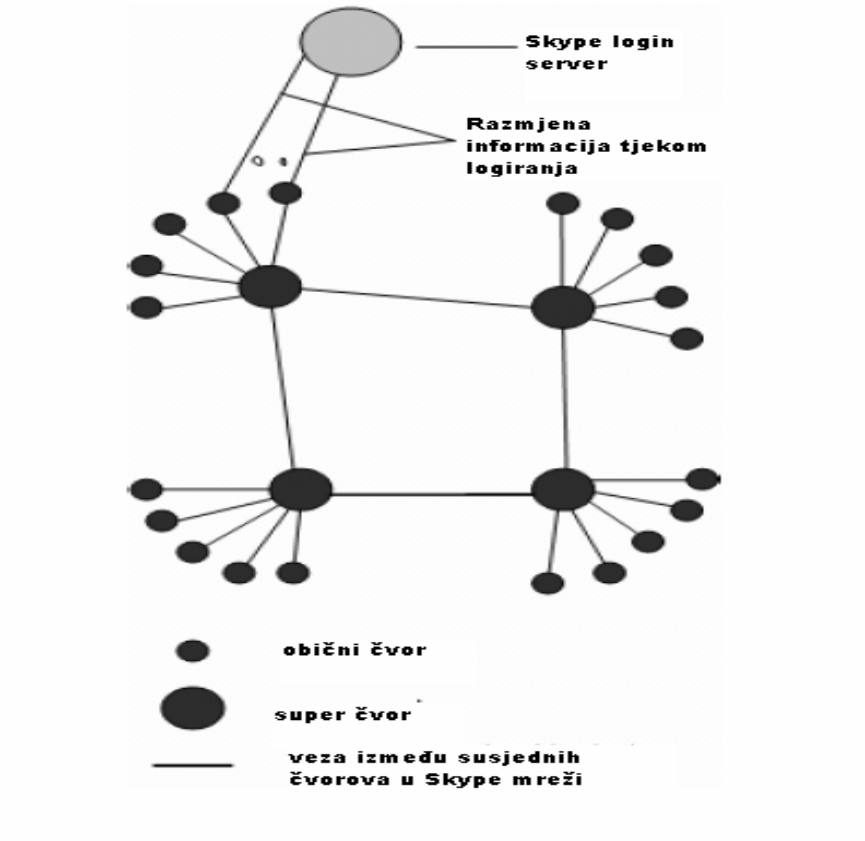
5.1. SKYPE

Skype mreža je prekrivajuća mreža (mreža nastala preko druge mreže, kao i većina ostalih - jer nastaju preko interneta).

Pokrenuli su je Niklas Zennström i Janus Friis.
Skype funkcionira na modelu korisnik – korisnik.
Skypov kod je "close source" i protokol je zaštićen zakonom.

Ima dvije vrste čvorova: obična računala povezana u mrežu, te „super čvorove", na rubnim točkama Skype mreže.
Svaki čvor s javnom IP adresom, odgovarajućom procesnom moći i memorijom može postati super čvor. Koji će to biti automatski odabire Skype sistem. Postoji oko 20 000 super čvorova preko kojih se povezuju milioni korisnika.

Obično računalo može s priključiti na super čvor i registrirati se na Skype login server.
Iako sam nije Skype čvor, Skype login server je važan dio mreže.
Server obavlja logiranje, provjeru identiteta, te pazi da svako ime u Skype mreži bude jedinstveno. U njemu su sačuvana korisnička imena i lozinke.
Osim login servera ne postoji drugi centralni server u Skype mreži.



Slika 3. Skype mreža

Svaki Skype klijent mora izgraditi i osvježavati tablicu dostupnih čvorova. Ta se tablica zove Host Cache (HC) i u sebi sadrzi IP adrese i brojeve postova super čvorova. Tablice su pohranjene u „windows registry" svakog od čvorova

Osim instant messangera Skype ima i druge brojne mogućnosti: moguće je razgovati s PC-a na PC, primiti poziv s fiksnog telefona, zvati fiksni telefon, ostavljati govornu poštu, ostvariti videopoziv, slati SMS za 0.05 eura...

5.2. MSN Messenger

MSN messenger je namjenjen Windowsima i zamišljen za svakodnevnu, „kućnu“, neprofesionalnu uporabu.
Ima razne zanimljive mogućnosti poput dodavanja emocija, sličica i sličnog, ukratko, ostavlja puno prostora za izražavanje.

Glavna namjena softvera je za slanje poruka, ali ima i druge mogućnosti kao mogućnost poziva, web kamera (videokonferencija, prijenos dokumenata, igre…)

Kad je prvi put objavljen(verzija 1.0.0863 je objavljena u srpnju 1999.), omogućavao je pristup America Online's AIM mreži, ali su im konstantno pokušavali blokirati pristup pa su na kraju maknuli tu mogućnost.
Sad softwer dozvoljava pristup NET Messenger servisu, i to uz kreiran „Microsoft Passport Network” korisnički račun.

Koristi MSNP (Mobile Status Notification Protocol) preko TCP-a da se priključi u .NET Messenger servis – sevis na portu 1863 od messenger.hotmail.com.

MSN Messenger sadrži oglase i korisnici ga mogu ručno „update-ati“.

Trenutno se koristi verzija MSNP13 za MSN Messenger 7.5.

Za poslovne korisnike je osmišljen **Windows Messenger**. On je puno formalniji, ne sadrži nikakve dodatne mogućnosti, ne sadrži oglase i “update-a“ se zajedno sa windows update-om.
Iako radi i sa .NET Messenger servisom, više se bazira na uporabi Microsoft Live Communications Servera koristeći i SIP / SIMPLE protokol (Session Initiation Protocol/ Instant Messaging and Presence Leveraging Extensions).

5.3. Yahoo! messenger

Poput ostalih dosad spomenutih, Yahoo! messenger je slobodan za preuizmanje i nakon preuzimanja Yahoo ID korisnik je spreman priključiti se Yahoo! mreži i svim njenim uslugama.
Yahoo! također ima mogućnost da korisnik postavi „nevidljiv" status.
Posebnost mu je Buddy Spy, aplikacija koja omogućava da se „zaobiđe" nevidljivost, tj. da bez obzira na njihov status možete vidjeti koja je od osoba s vaše kontakt liste na vezi.

Yahoo! je najnesigurniji od svih IM platformi. Protokol ne šifrira ni korisničko ime ni lozinku, što samo logiranje čini dovoljno riskantnim.

Također je kao i MSN baziran na ASCII kodu i koristi dva porta za komunikaciju. Klijent šalje informacije kroz Yahoo! Server, port 5050 a ASCII kod kroz port 80.

U Yahoo! Paketu postoji zaglavlje koje nije u ASCII kodu, kad se korisnik logira početni paket se šalje preko HTTP-a. HTTP server odgovara cookie-em koji je valjan neko vrijeme, sve ostale usluge koriste ovaj cookie za provjeru autentičnosti
.
Instant poruke jednostavno putuju od jednog korisnika drugom preko centralnog servera u HTML obliku. Nisu šifrirane.
Šalju se serveru preko TCP-a, port 5050.

Što se tiče sigurnosti vrijedi isto ako i za MSN: ono što se šalje može imati jako veliku publiku.

5.4. ICQ

ICQ (naziv nastao igrom od „I seek you“) je 1996. razvila tvrtka Mirabilis, koju je 1998 kupio AOL.

ICQ podrzava slanje poruka, URL-ova, chat više korisnika, prijenos dokumenata, njegov sustav je toliko jak da se do danas nije uspio napraviti puno bolji, ali mana ICQ-a je neinteresantan dizajn sučelja. Zahvaljujući tom propustu su ostali IM sustavi (Yahoo, MSN) lakše pridobili mlađu populaciju.

ICQ korisnik se identificira pomoću brojeva koji se nazivaju UIN (Universal Internet Numbers), a dodjeljuju se redom. Novi korisnici dobivaju broj koji je već puno iznad 300,000,000, .
Za razliku od ostalih IM sustava, ovo je jedini podatak koji trebate za ICQ, ime i sve ostalo može se po volji mijenjati, bez ponovne registracije.

Komunikacija među korisnicima se odvija preko jednog ili više ICQ servera, preko porta 5190.
Kad se korisnik logira u ICQ mrežu njegov UIN broj i lozinka se šifriraju odgovarajućim algoritmom.

Instant poruke jednostavno putuju od jednog korisnika drugom preko centralnog servera u HTML obliku. Nisu šifrirane.Šalju se serveru preko TCP-a.

5.5 Pregled svojstava

	Autor	Objavljen	Tip Protokola	Zadnja verzija	Cijena	Software licenca
ICQ	Mirabilis	Studeni 1996.	Single	5	Freeware	Zakonom zaštićena
MSN	Microsoft	Srpanj 1999.	Single	7.5.0311(XP) 7.0 (2000, ME,98)	Freeware	Zakonom zaštićena
Skype	Zennström i Friis	2003.	Single	2.0.0.107 Windows 1.2.0.18 Linux 1.4.0.49 Mac	Freeware	Zakonom zaštićena
Yahoo!	Yahoo!	Lipanj 1999.	Single	7.5.0.811 Windows 2.5.3. Mac	Freeware	Zakonom zaštićena

Tablica 2. Usporedba osnovnih svojstava

	Windows	Mac	Linux	Unix
ICQ	+	+	-	-
MSN	+	-	-	-
Skype	+	+	+	+
Yahoo!	+	+	+	+

Tablica 3. Kompatibilnost s operacijskim sustavima

	Šifriranje	Prijenos podataka	Grafika (smileys)	Igre	Uređivanje okvira
ICQ	-	+	+	+	+
MSN	- (WM +)	+	+	+	+
Skype	+	+	+	-	-
Yahoo!	-	+	+	+	+

Tablica 4. Usporedba dodatnih mogućnosti

6. Opasnosti uporabe Instant Messaging-a

Kao što smo rekli, uporaba Instant messaging servisa je sve veća i veća, ali nije nadzirana niti zaštićena, ni unutar tvrtki niti kod pojedinačnih korisnika, što otvara put raznim virusima, crvima i spyware-u. Također se javlja i SPIM (spam over IM) koji je pogodan za prijenos štetnog software-a.

Crvi su takvi da se skrivaju u poruku od poznatog IM korisnika, npr. nekoga sa kontakt liste. Ciljana osoba je ohrabrena time, i najčešće otvara privitak koji je došao s porukom. Jednom kad se prihvati i otvori zaraženi software se instalira na dotično računalo i još k tome se sam direktno proslijedi svim IM korisnicima na listi kontakata napadnutog korisnika.

Zbog prirode instant messaginga svi su trenutno obaviješteni da su primili poruku, te se tako virus jako brzo širi.
Za usporedbu se daju vremena potrebna da se zarazi 500 000 korisnika sa 3 različita virusa:

Virus	Način prijenosa	Vrijeme
Code Red	TCP/IP	14 h
Slammer	e-mail	20 min
IM crv	IM	30 – 40 s

Tablica 5. Usporedba vremena potrebnih za zarazu

Najčešće opasnosti:

1. koliko god brzo raste uporaba IM-a, toliko se širi i spektar prijetnji sigurnosti sustava. Također najavljena interoperabilnost između Yahoo-a i MSN Messengera će povećati rizike. Naime što je mreža instant poruka veća i povezanija, to joj je potrebnija adekvatna zaštita u realnom vremenu.

2. Nove mogućnosti IM servisa kao npr video konferencije i slično otvaraju nove puteve sofisticiranijim napadima virusa – tvorci virusa imaju već veliko iskustvo iz e-mail-ova, a IM im je novi izazov, tako da već postoji crv koji imitira čovjekov glas, i to na više jezika.

3. Ti sofisticiraniji virusi donose i veće štete, lako prelaze iz jedne mreže u drugu, brzo se šire, uspješno zaobilaze postojeće antivirusne programe, te krajnji korisnik vjerojatno neće odmah primjetiti njihov utjecaj što ih čini još štetnijima.

4. Jedan put kad virus instalira svoj softver na računalo ono postaje nesigurno, kao i sve pohranjeno na njemu: povjerljive informacije, bakovni računi, lozinke... sve na otvorenoj meti kriminalaca.

7. Zaključak

Iz iznesenog se može zaključiti da je uporaba IM-servisa korisna, kako u privatne tako i u poslovne svrhe.

Pa ipak treba znati s čime se raspolaže, da u većini aplikacija poruke nisu šifrirane, da su lako dostupne cyber-kriminalcima i da se mogu izgubiti.
Također ne treba nasjedati na trikove autora virusa i ne otvarati sve linkove i privitke koji pristignu, čak ako su od poznatih kontakata.

Pametna uporaba Instant Messaginga može donjeti puno zadovoljstva te čak pridonjeti povećanju produktivnosti na radnom mjestu.

Literatura:

www.en.wikipedia.org
www.wisegeek.com
www.e-consultancy.com/knowledge/whitepapers

Paul Piccard – Interner security sistems

Salman A. Baset and Henning Schulzrinne -
An Analysis of the Skype Protocol

Reginald Smith - Instant Messaging as a Scale-
Free Network