

Understanding Instant Messaging Protocol.

A case study: Windows Live Messenger

Ing. Antonio Grillo



grillo@disp.uniroma2.it

Ing. Alessandro Lentini



lentini@disp.uniroma2.it

DISP Università di Roma “Tor Vergata”



1. Introduzione

1. Caratteristiche
2. Evoluzione
3. Dimensione
4. Rischi di privacy
5. Rischi di security

2. MSNP

1. Introduzione
2. Sessione di esempio
3. SSO
4. P2P

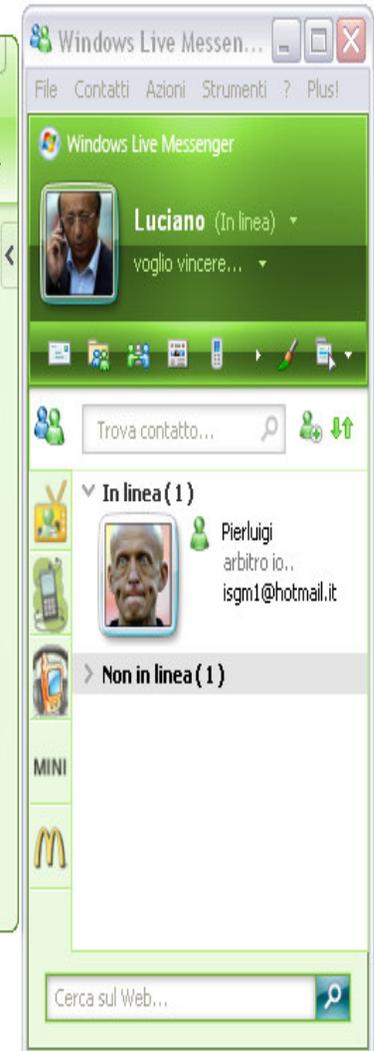
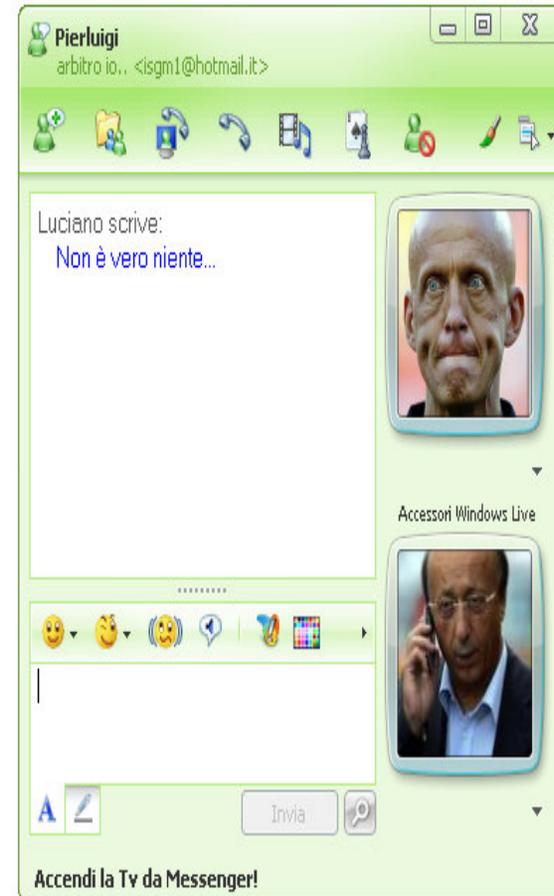
3. Virtual Parent

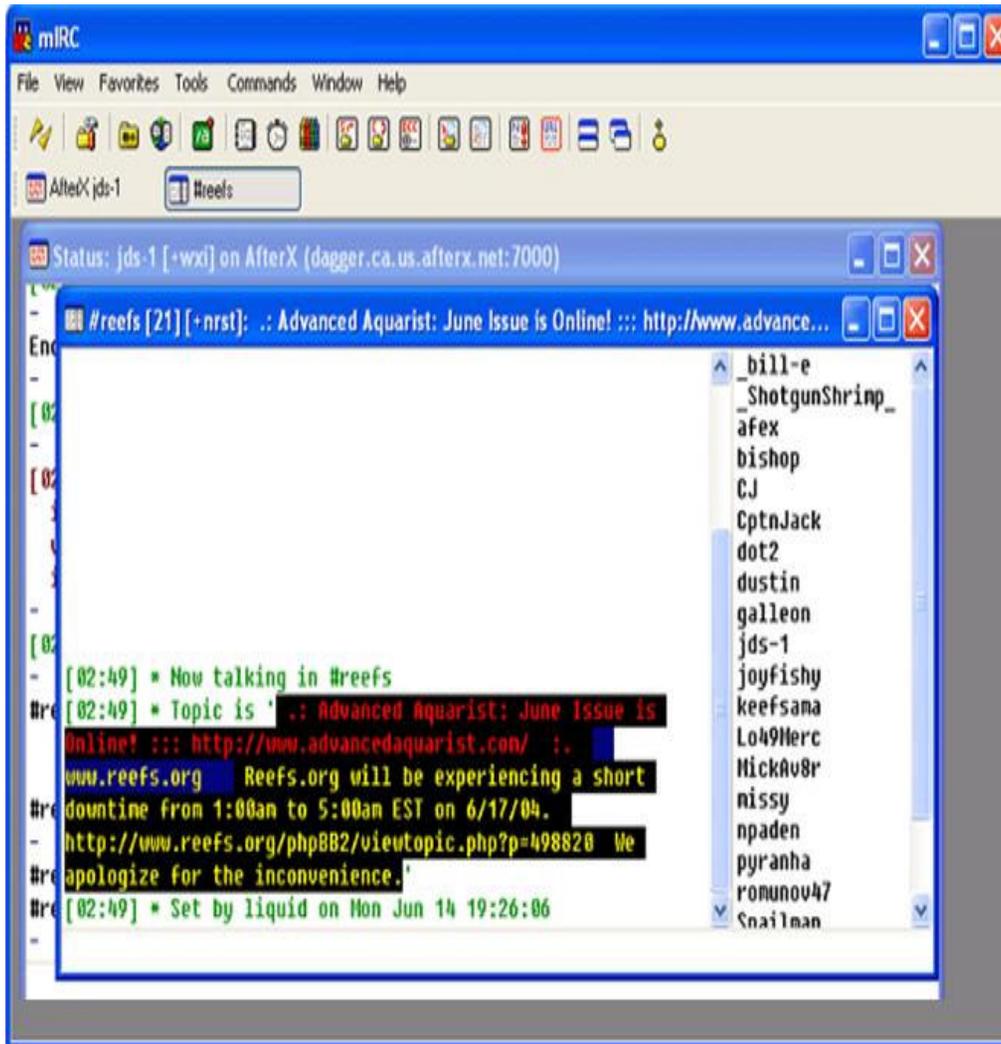
4. Conclusioni
5. Riferimenti bibliografici e sitografici
6. Varie – Q&A

Caratteristiche

Instant Messaging

- ✓ 1-to-1 chat
- ✓ Contatti personali contenuti in una rubrica archiviata on-line.
- ✓ Una finestra di conversazione per contatto.
- ✓ Funzionalità multimediali: invio audio, video, condivisione cartelle
- ✓ Nickname legati ad un indirizzo mail.

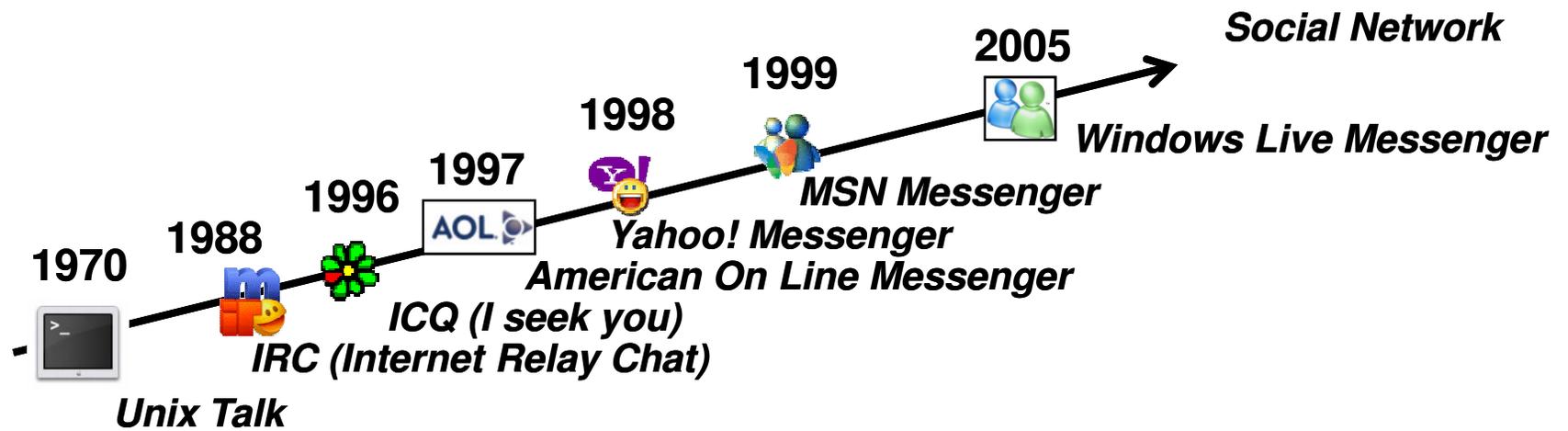




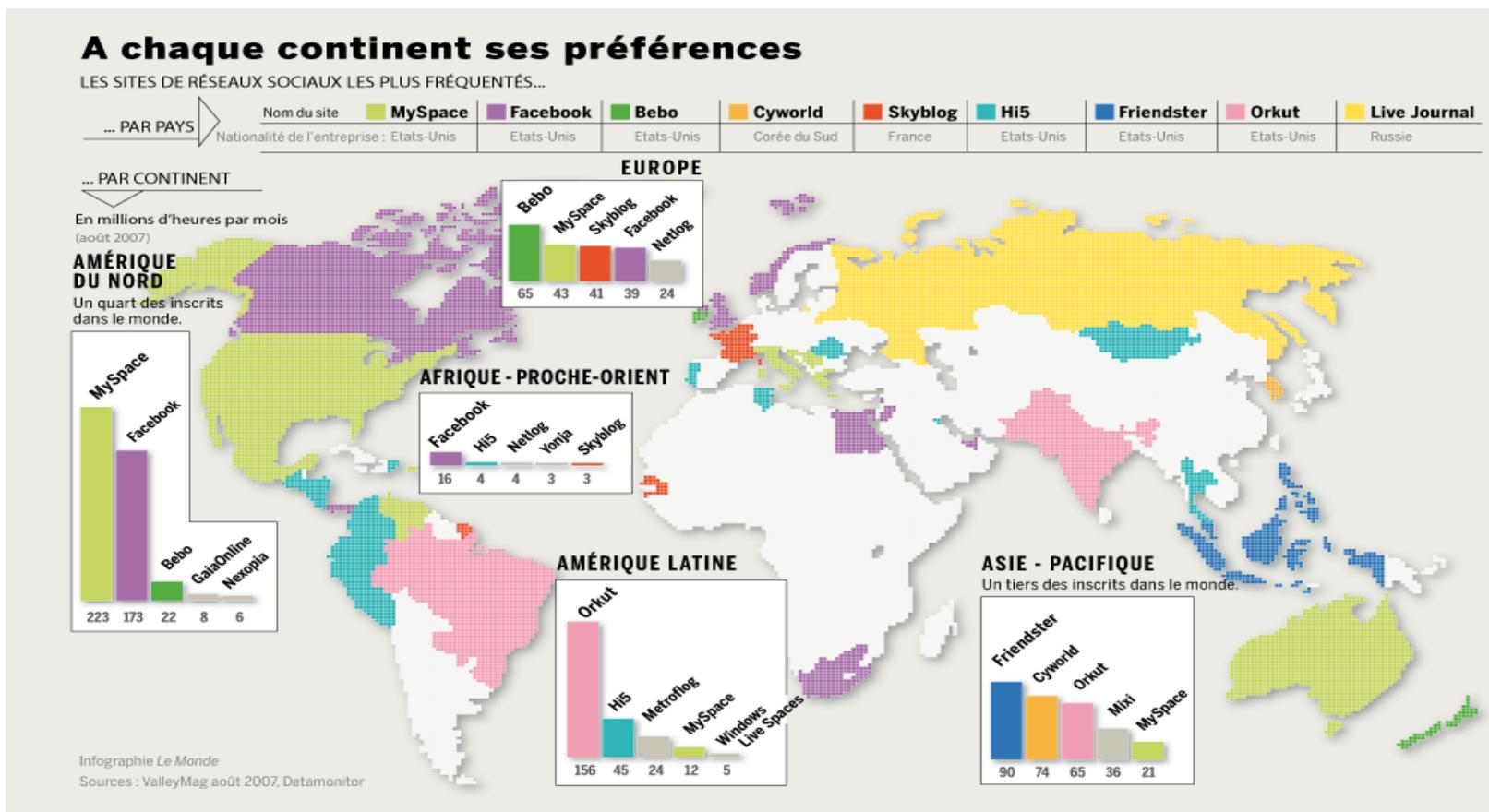
Chat group.

- ✓ n-to-n chat
- ✓ Contatti personali non esistono. (canale o stanza)
- ✓ Una finestra di conversazione per canale
- ✓ Funzionalità multimediali ridotte o assenti.
- ✓ Nickname non sono legati ad un indirizzo mail → maggiore anonimato

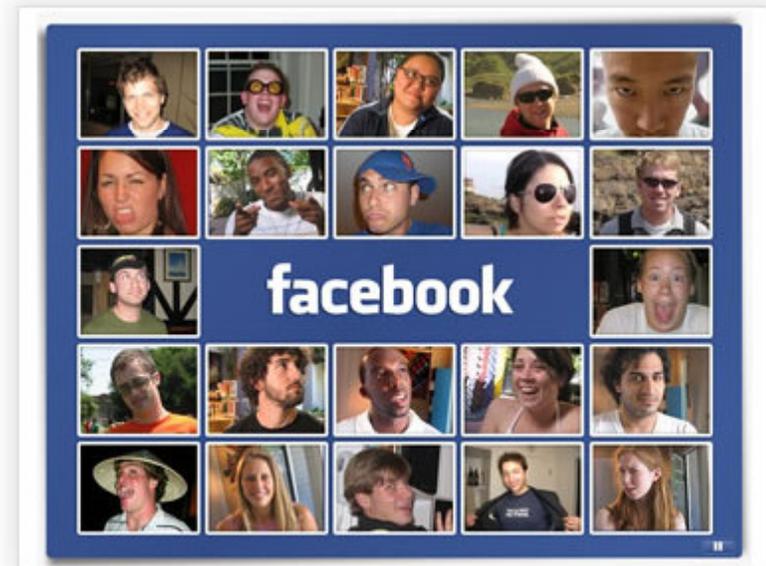
Evoluzione



Dimensione



Fonte: **Le Monde**
DIMANCHE 4 - LUNDI 5 SEPTEMBRE 2005 PASCALIE HERRERO



Dimensione

- **USA:** più del 55% dei giovani utenti americani on-line fra i 12 e i 17 anni ha creato profili personali ed ha utilizzato siti di SN quali MySpace o Facebook;
- **UK:** il 46% degli utenti minorenni di SN dichiara di comunicare le proprie informazioni personali a coloro che incontrano on line e il 40% pretende di riceverli.
- **Spagna:** la maggioranza degli adolescenti spagnoli dichiarano di preferire l'IM per comunicare con i propri amici per conversazioni più informali e di intrattenimento; per le comunicazioni più serie e formali continuano a preferire l'uso del cellulare.

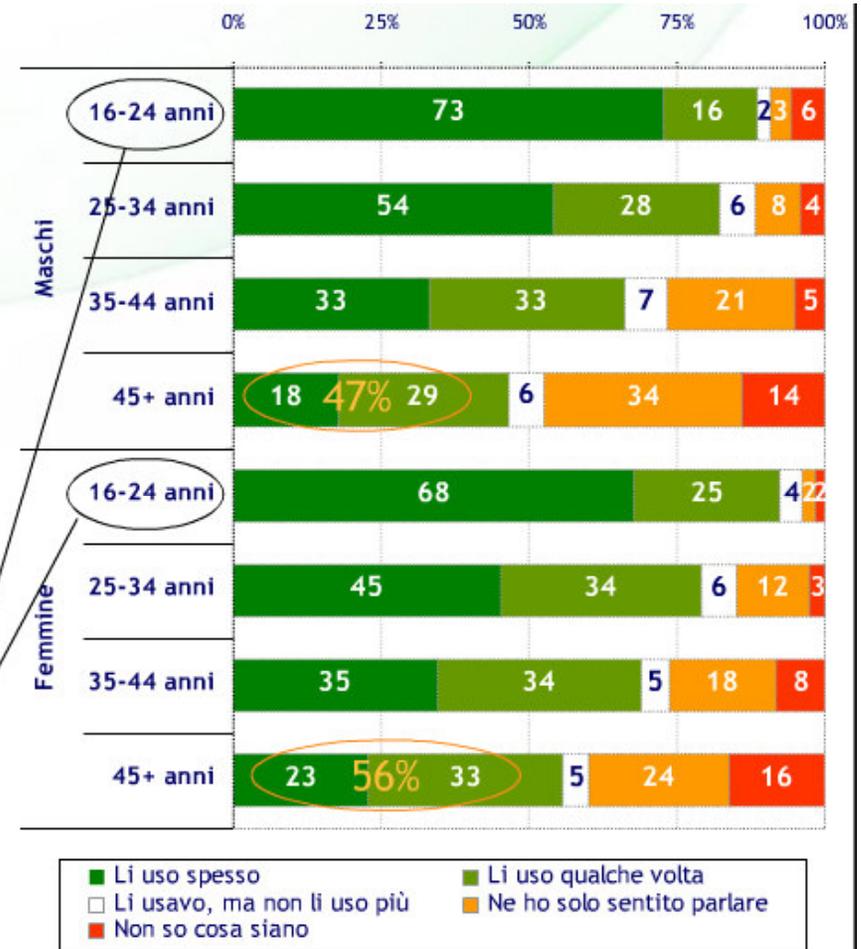
Solo la metà dei genitori afferma di avere consapevolezza che i propri figli usano abitualmente siti di SN per comunicare con amici abituali e per fare nuove "virtuali" conoscenze

La percentuale di genitori che osserva e controlla le informazioni che i propri figli scambiano attraverso software di IM è quasi nulla.



I maschi 16-24 sono i maggiori utilizzatori abituali, le loro coetanee sono le più numerose includendo anche l'uso sporadico

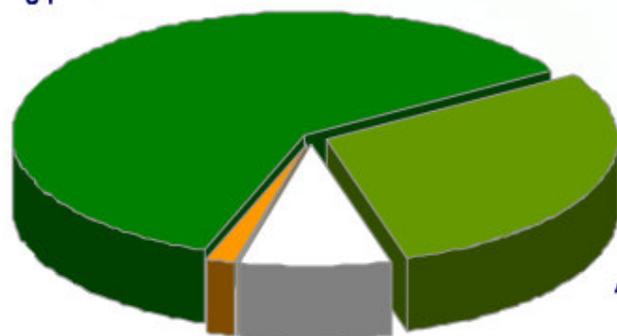
Maschi	Femmine
89%	93%



[4] Indagine NextPlora per  Microsoft, maggio 2008.

Dimensione

Tutti i giorni o quasi
61

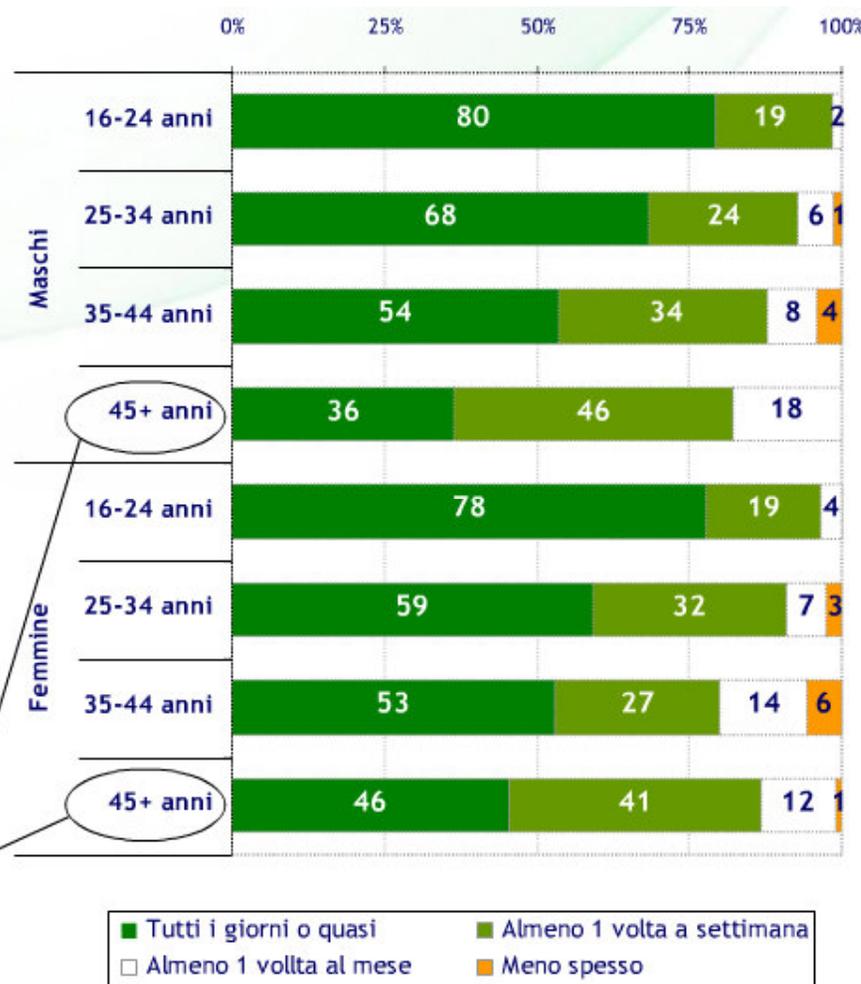


Meno spesso
2

Almeno 1 volta al mese
8

Almeno 1 volta a settimana
30

Solo oltre i 45 anni si passa da un ricorso quotidiano o quasi ad una fruizione a carattere settimanale
 Le donne 45+ più attive dei loro coetanei



[4] Indagine NextPlora per  Microsoft, maggio 2008.

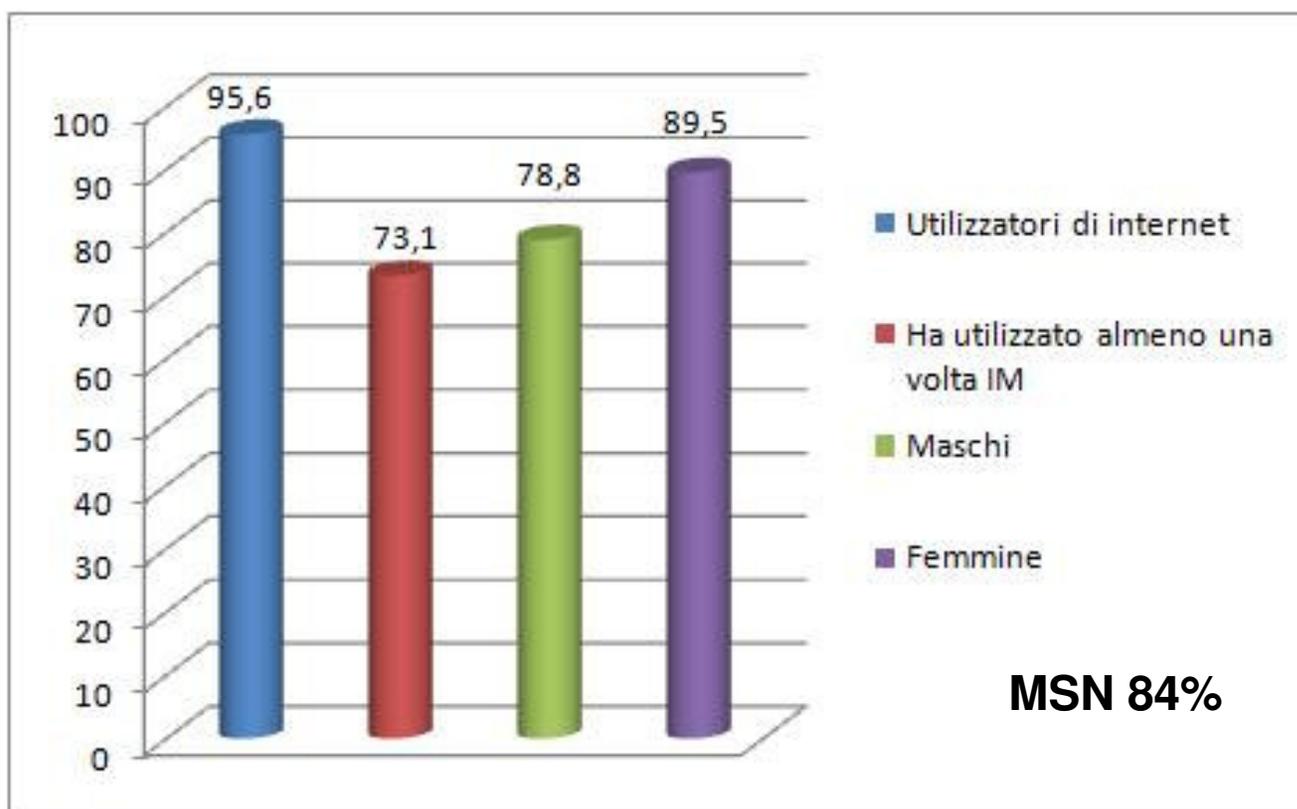
Dimensione

Indagine NextPlora per  Microsoft, maggio 2008.

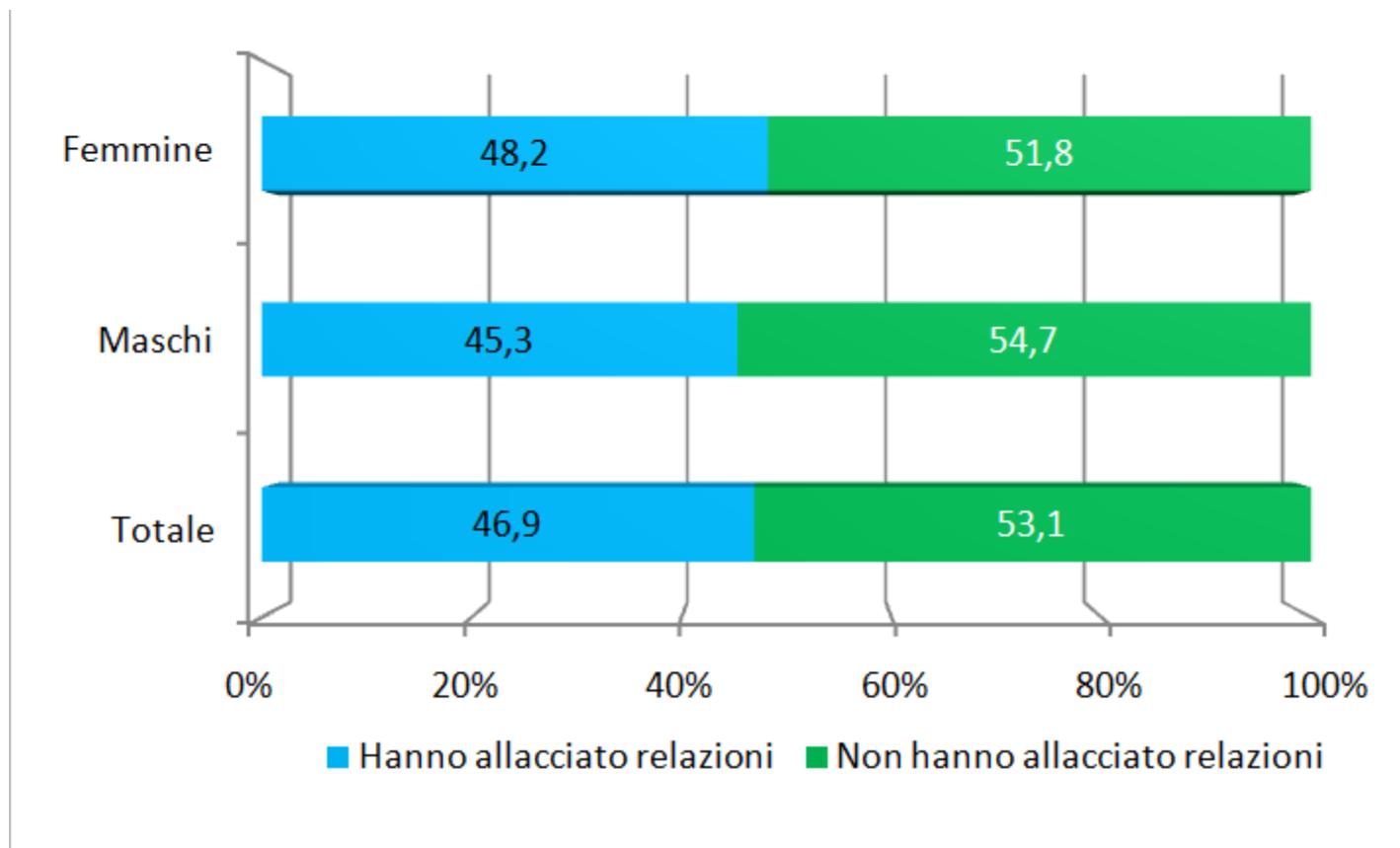
- I maschi della fascia 16-24 anni sono gli utilizzatori più abituali, le coetanee sono le più numerose includendo anche l'uso sporadico.
- Più dell'80% si connette tutti i giorni.
- Il tempo di connessione medio si aggira intorno alle 4 ore.
- Il 71% degli utilizzatori preferisce MSN Messenger come client
- Le funzionalità più utilizzate dell'IM sono:
 - Scambiare messaggi con altre persone 94%
 - Condividere file 62%
 - Condividere foto 50%

Dimensione

Indagine Doxa per  Save the children, febbraio 2008 su un campione nazionale rappresentativo di adolescenti fra i 13 e i 17 anni [5]

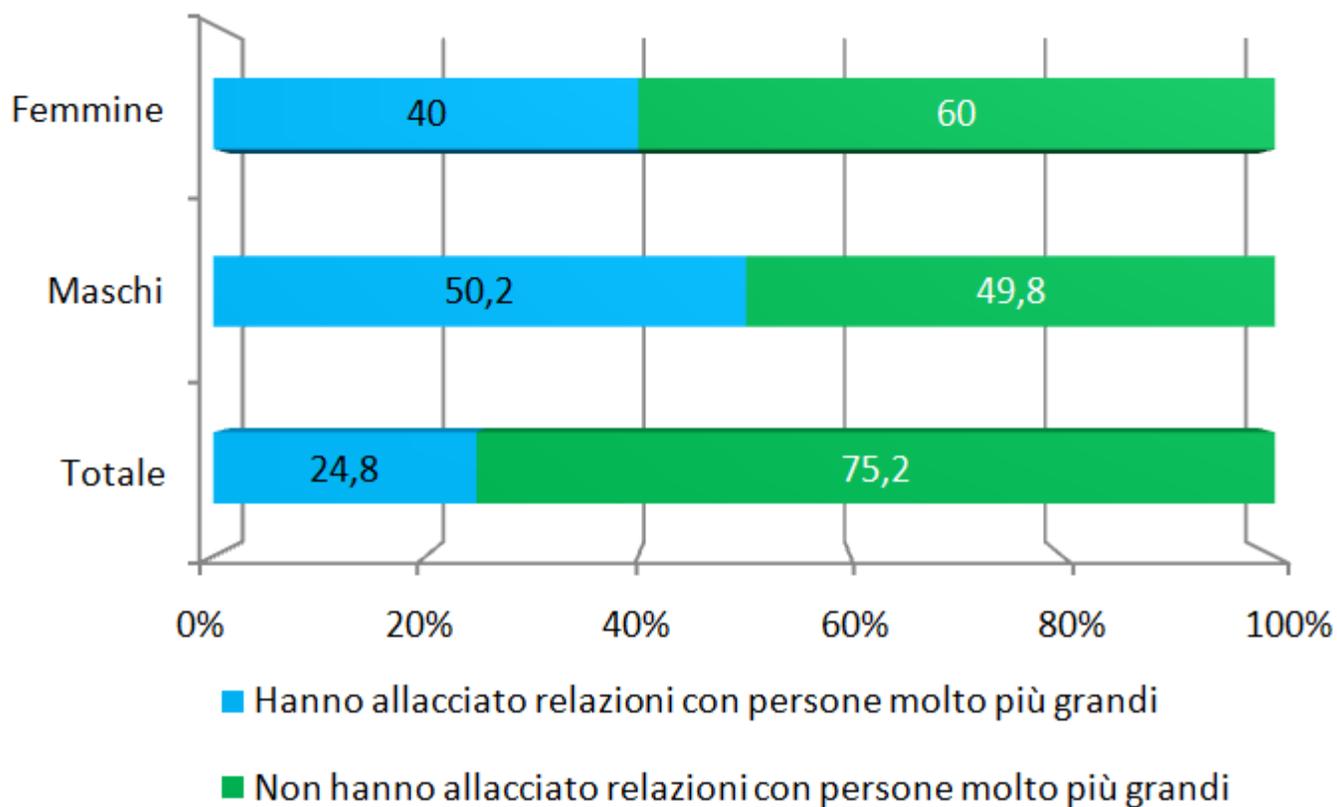


Dimensione



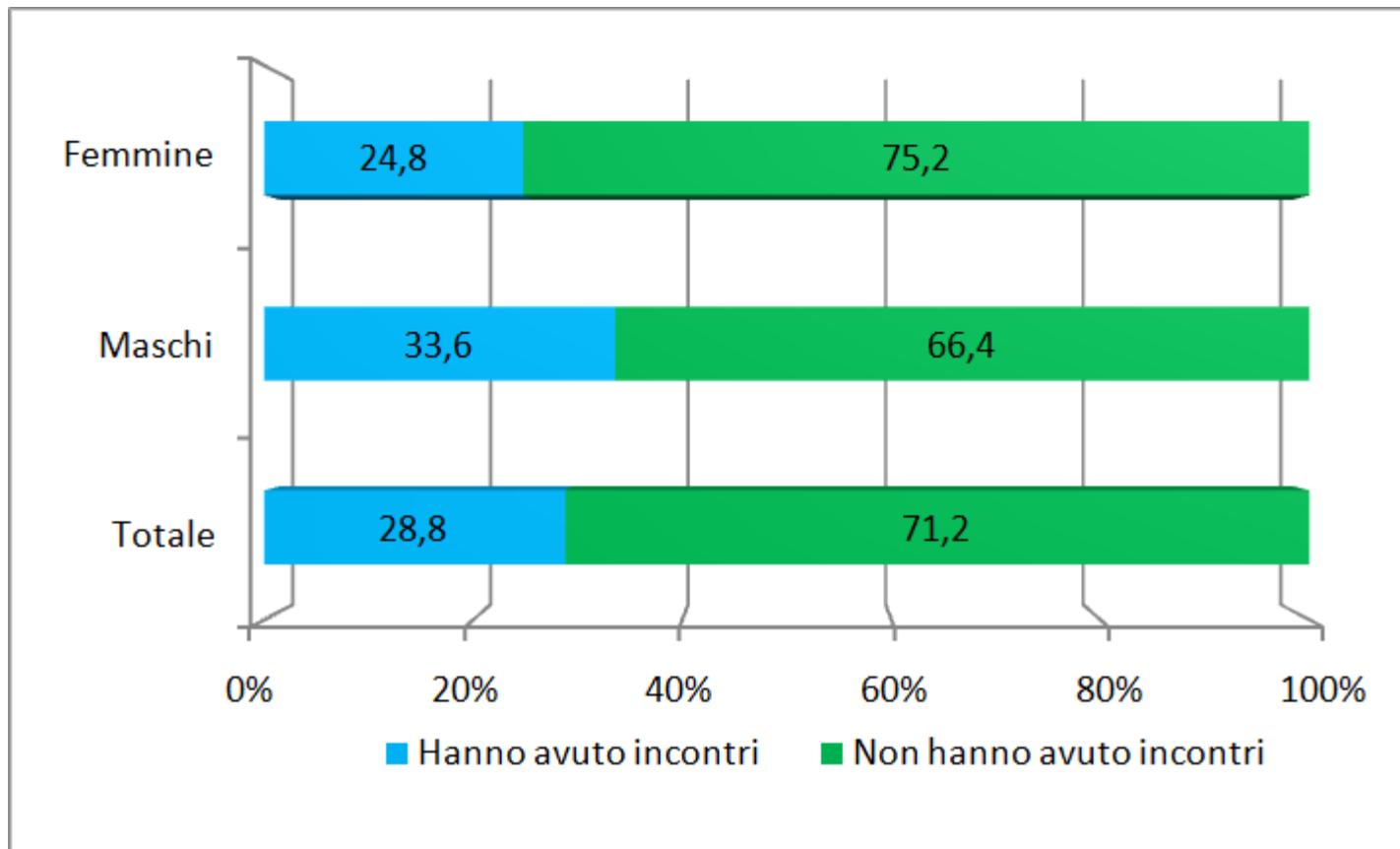
[5] Indagine Doxa per  Save the children, febbraio 2008

Dimensione



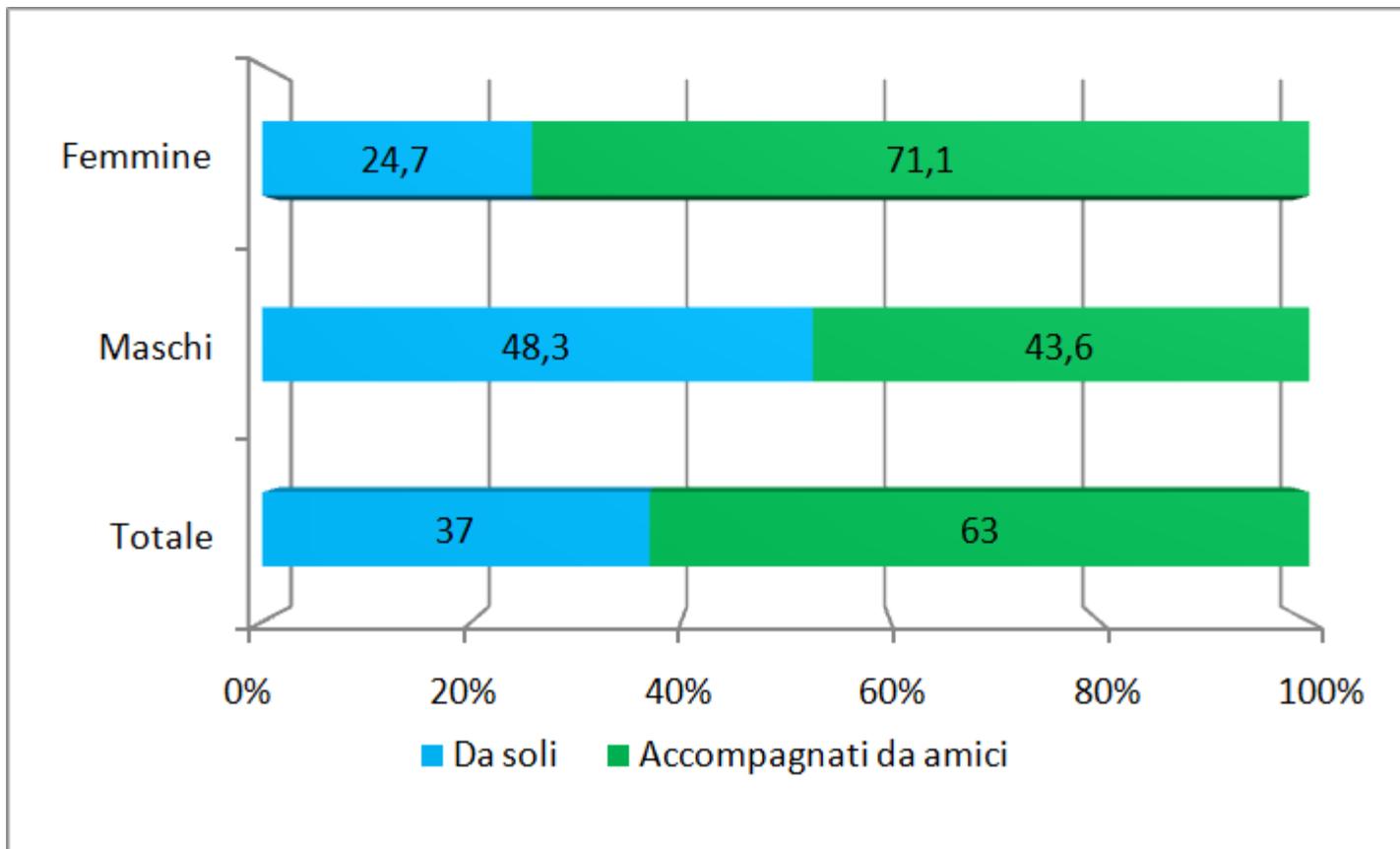
[5] Indagine Doxa per  Save the children, febbraio 2008

Dimensione



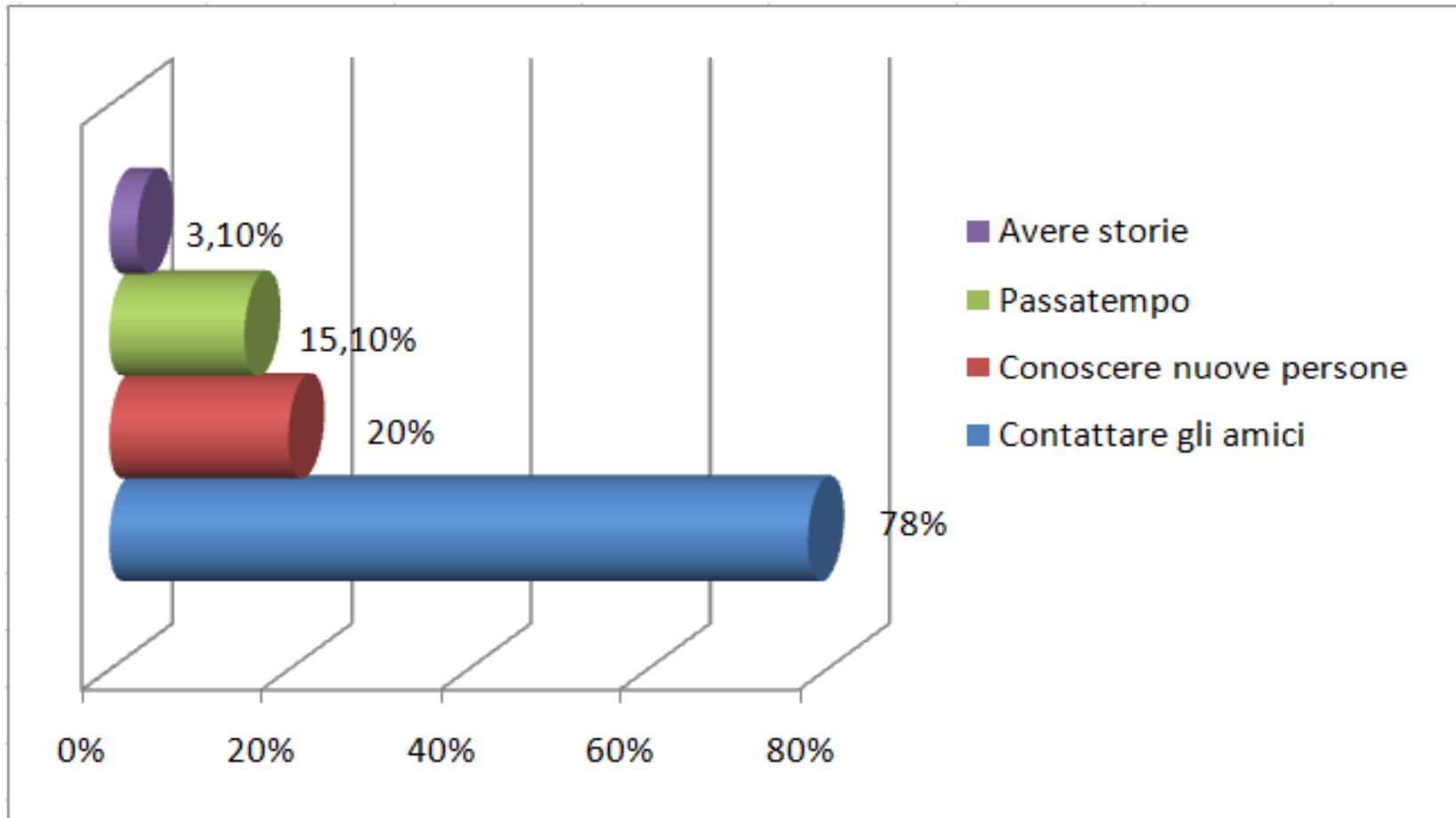
[5] Indagine Doxa per  Save the children, febbraio 2008

Dimensione



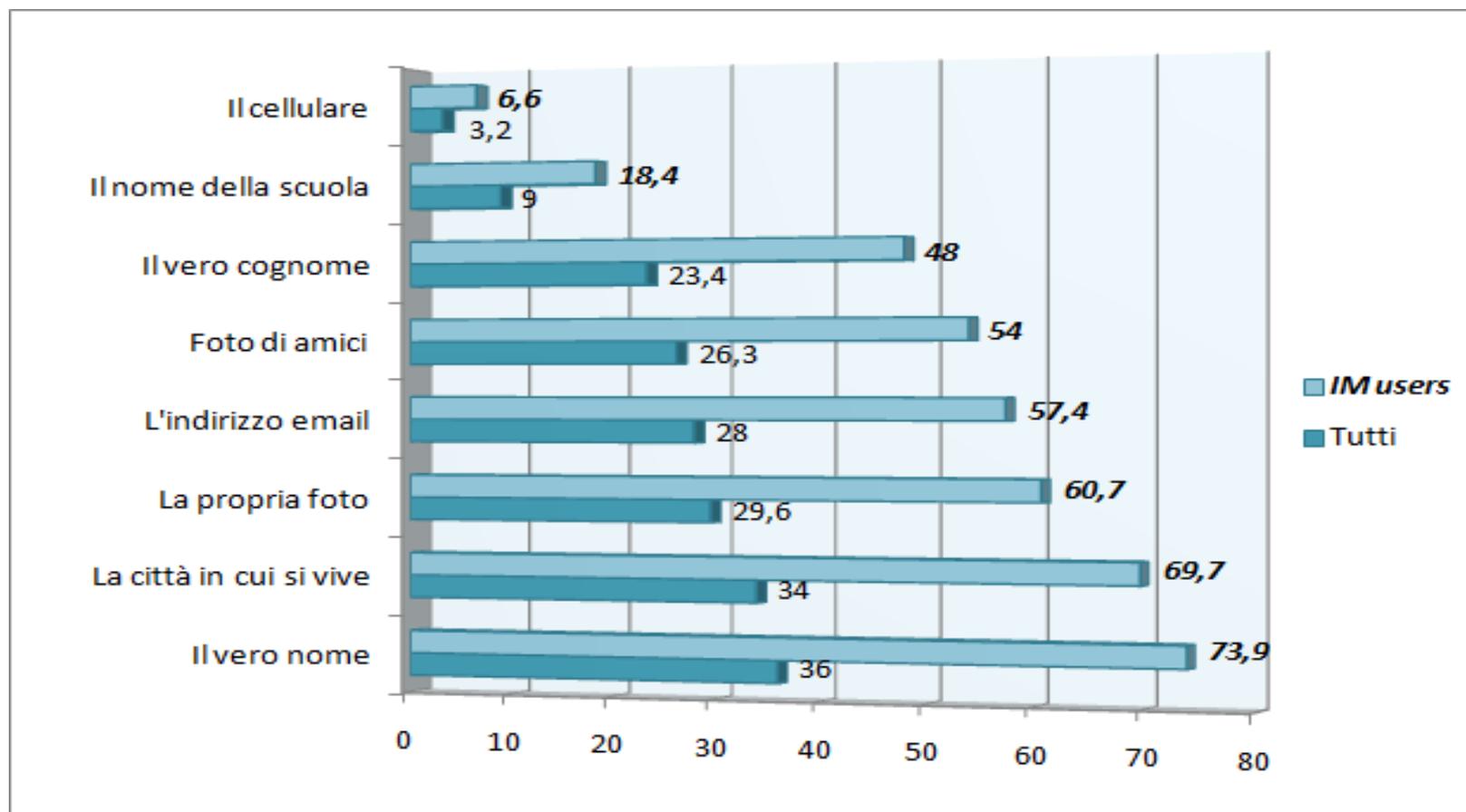
[5] Indagine Doxa per  Save the children, febbraio 2008

Dimensione



[5] Indagine Doxa per  Save the children, febbraio 2008

Dimensione



[5] Indagine Doxa per  Save the children, febbraio 2008

Rischi di privacy

La scarsa tutela della propria identità, rende gli adolescenti facilmente identificabili ed adescabili da adulti potenziali abusanti o da coetanei che possono esercitare forme di bullismo.

Il 32,8 % dei ragazzi riconosce di aver vissuto almeno una situazione spiacevole



European Network and Information Security Agency alla fine del 2007 ha presentato il primo Position Paper[7] su “Security Issues and Recommendations for Online Social Networks” che descrive 15 importanti minacce alla privacy:

- Digital Dossier
- Face Recognition
- CBIR (Content-Based Image Retrieval)

Rischi di privacy

La maggior parte di coloro che commettono crimini a sfondo sessuale su Internet sono uomini adulti che utilizzano le SN ed i programmi di IM per incontrare e sedurre giovani adolescenti, cercando di carpire informazioni riguardanti i loro interessi sul sesso [6] "Online 'Predators' and Their Victims" febbraio 2008

Grooming: l'adulto potenziale abusante “cura” (dall'inglese “grooms”) la potenziale vittima, inducendo gradualmente il bambino a superare le resistenze attraverso tecniche di manipolazione psicologica.

Contatto iniziale avviene tramite SN o IM successivamente conquistate a poco a poco le confidenze e la fiducia necessaria si passa all'incontro offline.

“Il grooming può comportare conseguenze così traumatiche sulle giovani vittime che raramente porta a confidare l'accaduto con i propri genitori o con altri adulti”

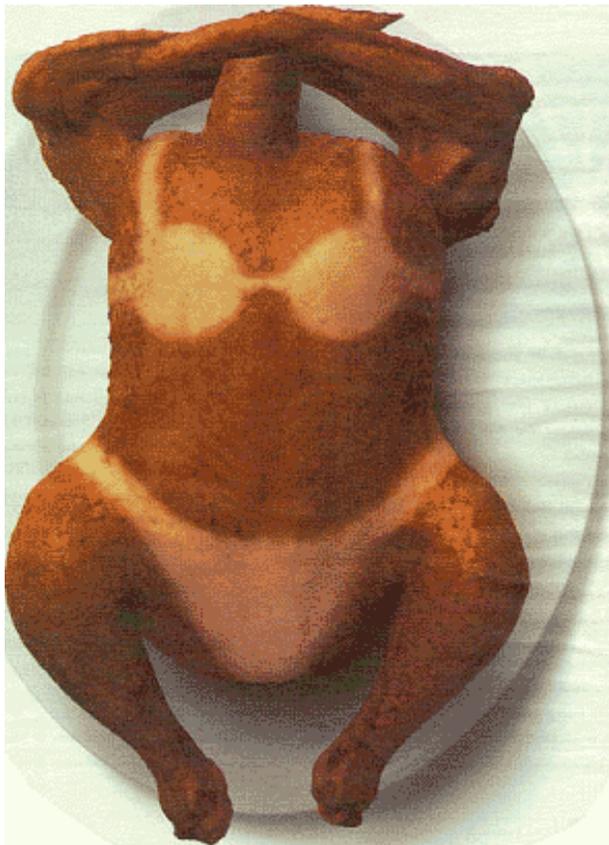
[9]“Il minore esposto alla pedo-pornografia su Internet” Save the Children 2006

Rischi di security

1. L'Instant Messaging (IM) è stato, sin dall'inizio, un vettore d'attacco per i sistemi informatici;
2. Phishing, Virus/Worm, Interruzione di servizio, Dirottamento di sessione (hijacking) sono gli attacchi più diffusi;
3. Già dal 2004, Microsoft, AOL, Yahoo, Symantec e McAfee avevano fondato l'IMlogic Threat Center, http://imlogic.com/im_threat_center/index.asp, proprio per monitorare la minaccia;
4. E.g. il 64% degli attacchi hanno colpito client MSN, alcuni tra i worm diffusi per MSN sono Bropia e Kelvir.

Rischi di security

Bropia



Si diffonde utilizzando i contatti nella rubrica di MSN

Spedisce il codice virale ai contatti appena avviano MSN e accedono alla rete.

Fa una copia sul disco locale e tiene traccia degli eventuali aggiornamenti della lista contatti.

Bropia.A installa il trojan horse Rbot

Bropia.F rilascia nei sistemi infettati anche un secondo worm chiamato Agabot.ajc.

Agabot.ajc sfrutta le stesse vulnerabilità di Slammer, Blaster (MSBlast) e Sasser per eseguire attacchi DDoS su certi servizi Microsoft.

Rischi di security

Kelvir



invia un link a tutti i contatti della rubrica di MSN

Il link punta al worm omg.pif che:

- continua a diffondersi inviandosi a tutti i contatti della rubrica MSN,

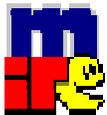
- scarica il file:

<http://home.earthlink.net/~gallery10/me.jpg>

in C:\drive come "dumprep.exe"

- esegue dumprep.exe ovvero una variante del trojan horse Rbot

Dimensione



Continua...

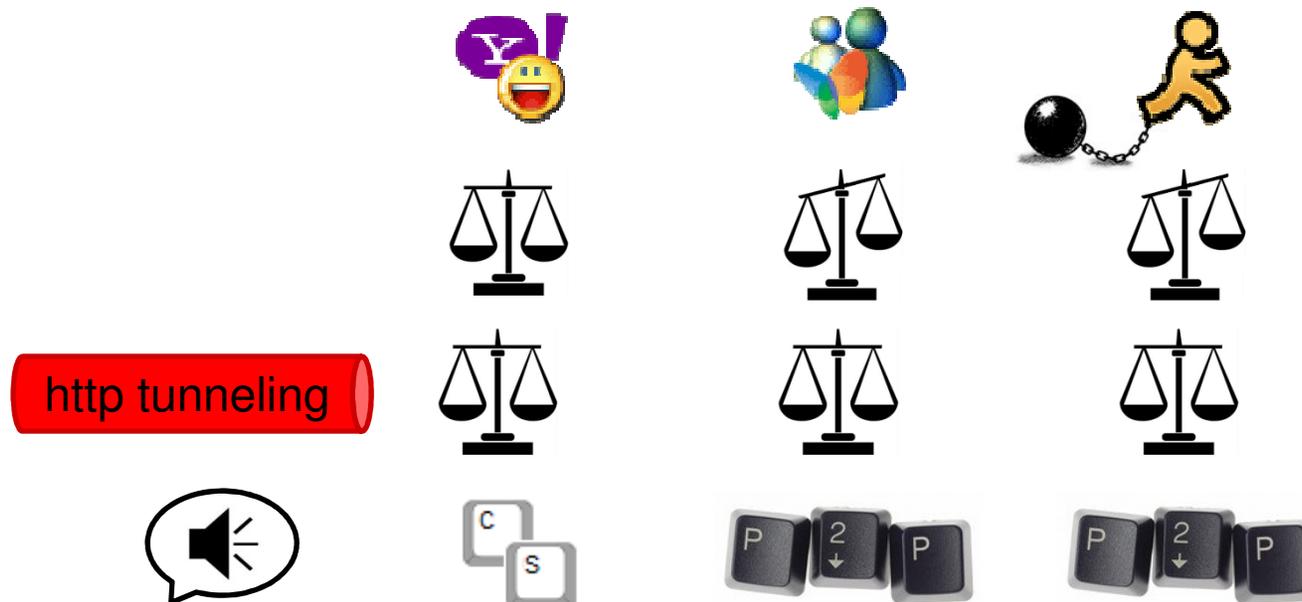
- Architettura: client – server 
- Problema: scalabilità del servizio

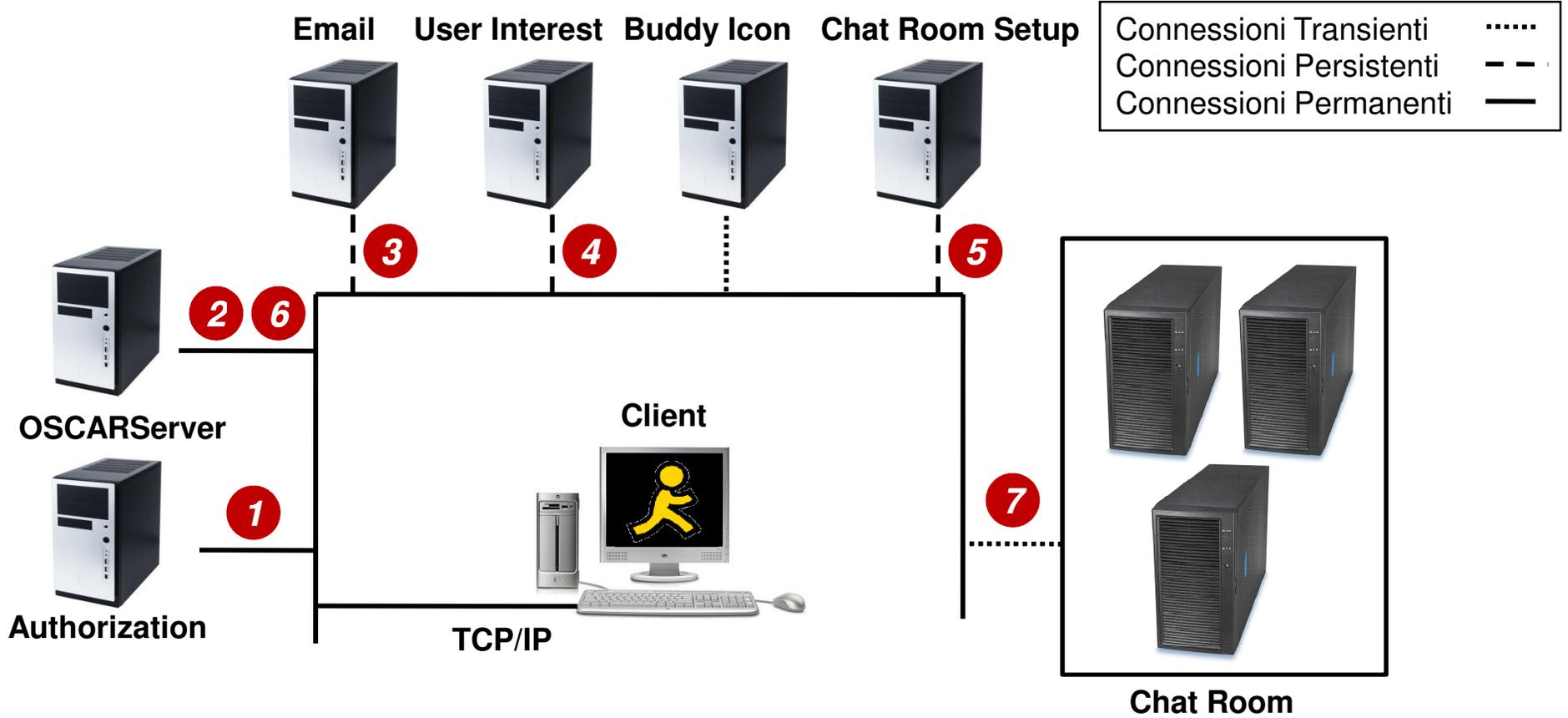


approccio simmetrico: ogni server svolge le stesse funzioni, i client non fanno distinzione sul server da contattare.

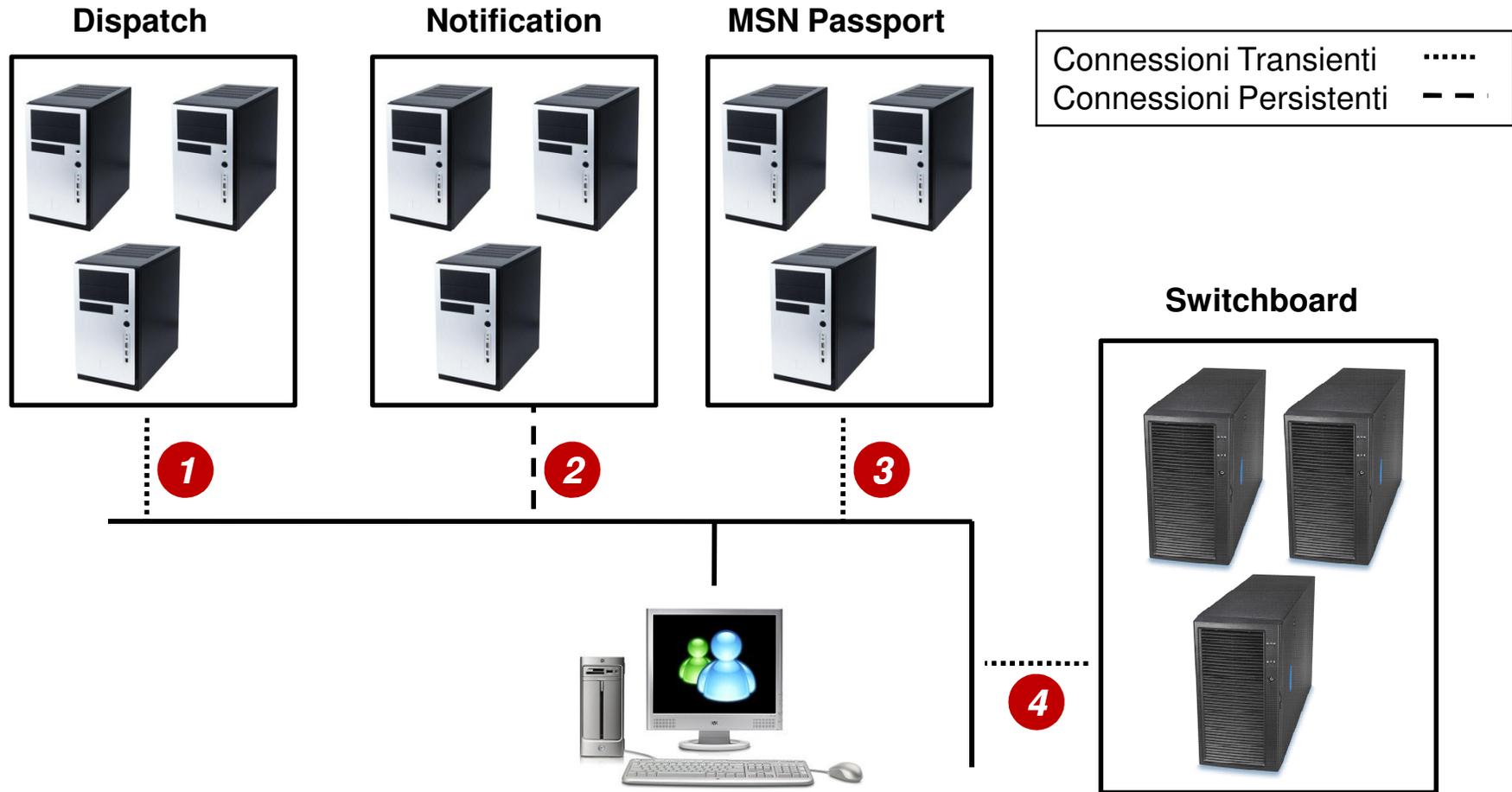


approccio asimmetrico: ogni server è dedicato a particolari attività (logging, discovery, chat room..)

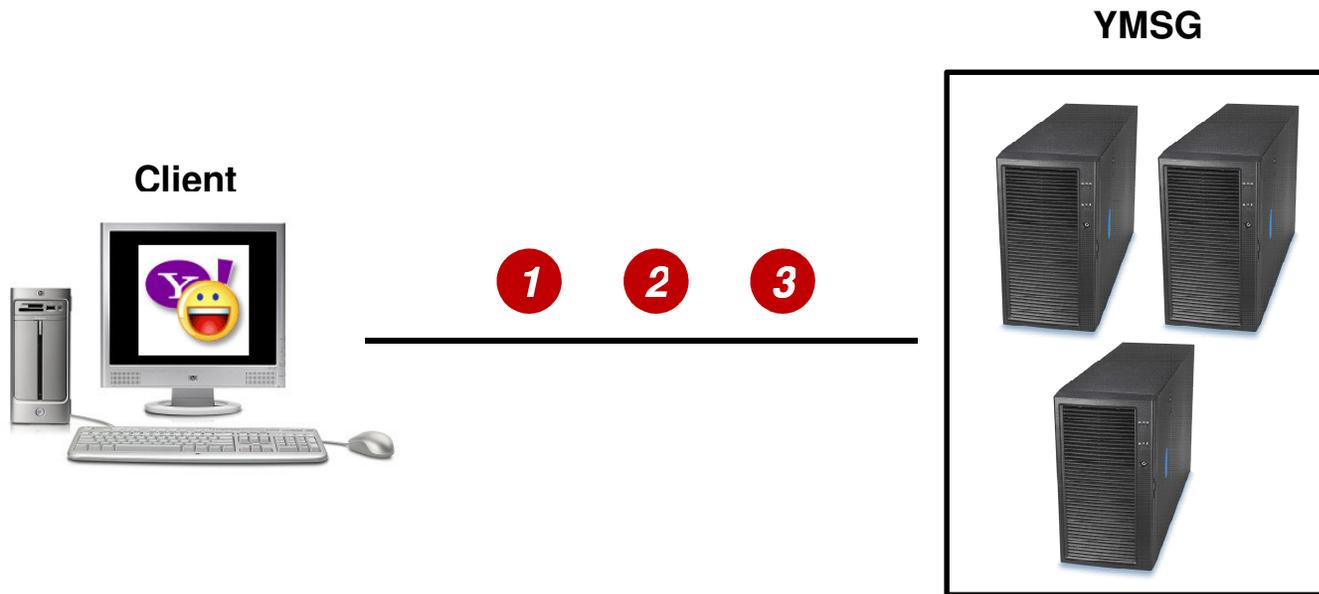




MSN/WLM 



YMSG



Cooperazione

- Esistono diverse specifiche di protocolli di pubblico dominio pensati per sistemi di instant messaging:
il **SIMPLE**, SIP per Instant Messaging e Leverage Presence,
l'**APEX**, Application Exchange,
il **PRIM**, Presence and Instant Messaging Protocol,
il **XLM-based XMPP**, Extensible Messaging and Presence Protocol, più comunemente conosciuto come **Jabber**.
- Tuttavia i più diffusi sono i protocolli usati da **Microsoft**, **Mirabilis** e le altre aziende private.
- Nelle ultime versioni di **Yahoo! Messenger with Voice**, e **Windows Live (MSN) Messenger**, hanno unito le due community e possibile comunicare fra loro.
- **Yahoo!** ha rilasciato dichiarazioni esplicite sulla propria strategia di aggiornamento e revisione continua del protocollo volta a bloccare la connessione dei client open source.

1. Introduzione
 1. Caratteristiche
 2. Evoluzione
 3. Dimensione
 4. Rischi di privacy
 5. Rischi di security
2. **MSNP**
 1. **Introduzione**
 2. **Sessione di esempio**
 3. **SSO**
 4. **P2P**
3. Virtual Parent
4. Conclusioni
5. Riferimenti bibliografici e sitografici
6. Varie – Q&A

Introduzione

MSNP è acronimo di:

- **Micro**Soft **N**etwork **P**rotocol
- **M**obile **S**tatus **N**otification **P**rotocol



Protocollo **proprietario** sviluppato da Microsoft per essere usato attraverso il .NET Messenger Service.

Le applicazioni client che lo utilizzano ufficialmente sono **WindowsLiveMessenger** e le sue precedenti versioni **MSN Messenger** e **Windows Messenger**.

Molte applicazioni client lo supportano: **Trillian** , **aMSN** , **Pidgin** 

Introduzione

Luglio 1999: MSNP1 disponibile nella prima release di MSN Messenger

Ad ogni cambiamento sostanziale del protocollo (i.e. nuovo comando, cambiamento nella sintassi) il numero di versione è stato incrementato.



a partire da **Ottobre 2003** sono stati proibiti gli accessi a .NET Messenger Service con versioni precedenti a **MSNP8**.



a partire da **Dicembre 2005** la versione **MSNP13** è stata supportata con il client WLM 8.0; il client invia una SOAP request “Client goes to ABCH (Address Book Clearing House)” per ottenere la contact list.

Introduzione

Luglio 1999: MSNP1 disponibile nella prima release di MSN Messenger



a partire da **Settembre 2006** è stata introdotta la versione **MSNP15** la quale modifica lo schema di autenticazione RPS (Relying Party Suite).



a partire da **Settembre 2007** Microsoft ha forzato gli utenti a sostituire il client MSN Messenger con il client **Windows Live Messenger 8.1** per ragioni di sicurezza.

A breve Microsoft **NON** supporterà le versioni precedenti del protocollo, molte implementazioni open source dovranno migrare alle ultime versioni **MSNP13-15**.

Le informazioni sul protocollo sono state raccolte:

- lettura del draft ufficiale IETF (link: www.ietf.org/rfc/rfc2778.txt)
- analisi dei pacchetti attraverso Wireshark (link: www.wireshark.org/)
- analisi dei client ufficiali (i.e. Windows Live Messenger, ...)
- analisi dei client opensource (i.e. aMSN, ...)
- scrittura di piccoli frammenti di codice
- siti non ufficiali

Introduzione

.NET Messenger è un “presence and instant messaging system “

(RFC 2778 02/00)



Presence: le persone con cui comunichi sono “**online**”



Notification Server (NS)



Instant messaging: i messaggi vengono recapitati in “**real time**”

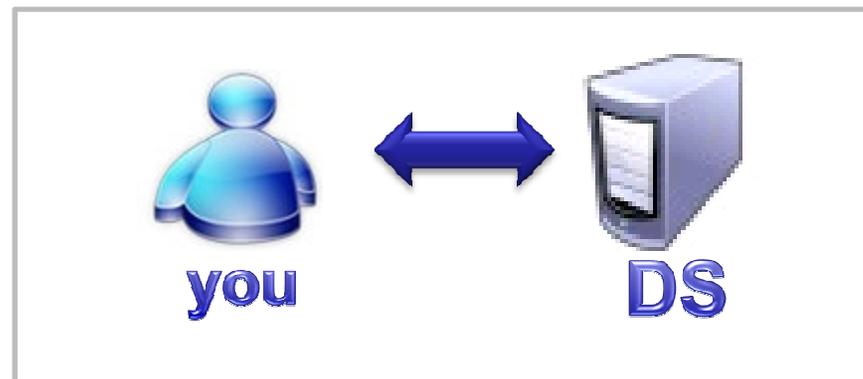


Switchboard Server (SB)

Introduzione

Dispatch Server (DS) goals:

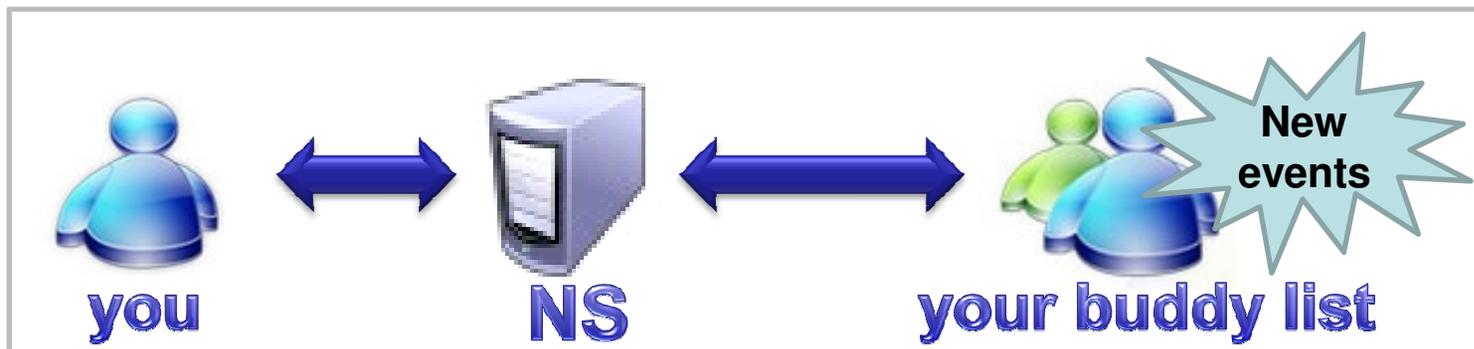
- Gestire l'accesso al .NET Messenger Service
- Negoziare le caratteristiche dell'accesso
- Autenticare l'utente



Introduzione

Notification Server (NS) goals:

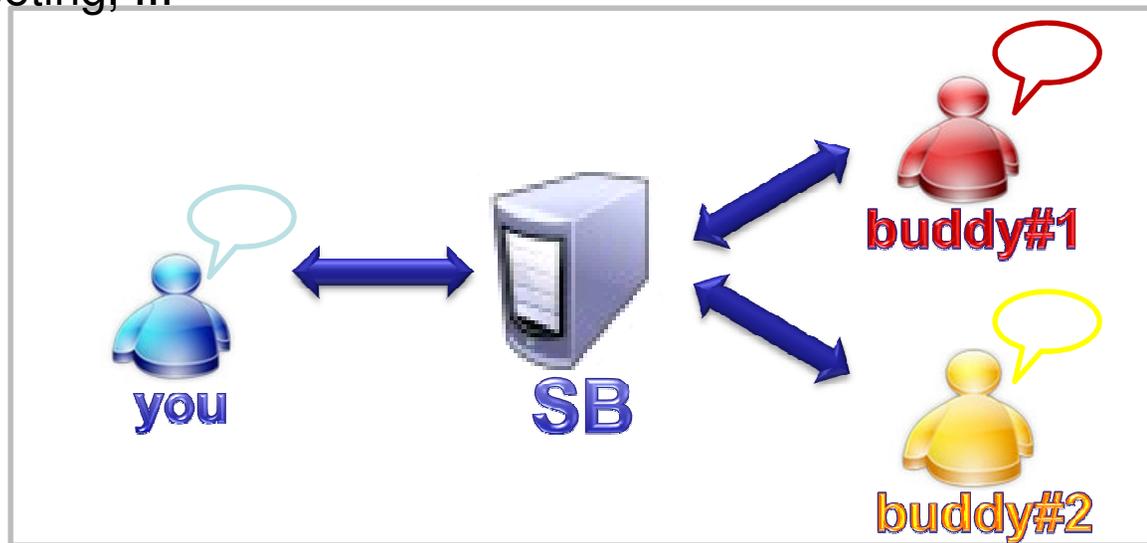
- Gestire le informazioni di “presence” (i.e. status, nickname, avatar)
- Notificare la ricezione di email nella inbox di Hotmail
- Consentire la creazione di nuove switchboard session
- Consentire il joining a switchboard session già esistenti



Introduzione

Switchboard Server (SB) goals:

- Gestisce le sessioni di instant messaging (i.e. agisce da proxy)
- Ogni partecipante ad una conversazione dispone di una connessione verso un SB condiviso
- Gestisce le fasi iniziali di alcuni servizi aggiuntivi: file transfer, NetMeeting, ...



Example Session

Time	Source	Destination	Protocol	Info	
6.350010	160.80.97.42	207.46.28.93	MSNMS	VER 325 MSNP15 MSNP14 MSNP13 CVR0	DS
6.586659	207.46.28.93	160.80.97.42	MSNMS	VER 325 MSNP15	
6.586690	160.80.97.42	207.46.28.93	MSNMS	CVR 326 0x0410 winnt 5.1 i386 MSNMSGR 8.5.1302 msmsgs isgm2@hotmail.it	
6.827677	207.46.28.93	160.80.97.42	MSNMS	CVR 326 8.1.0178 8.1.0178 8.1.0178 http://msgruser.dlservice.microsoft.c	
6.827702	207.46.28.93	160.80.97.42	MSNMS	XFR 327 NS 207.46.106.36:1863 U D	
7.063351	160.80.97.42	207.46.106.36	MSNMS	VER 328 MSNP15 MSNP14 MSNP13 CVR0	NS
7.310508	207.46.106.36	160.80.97.42	MSNMS	VER 328 MSNP15	
7.310539	160.80.97.42	207.46.106.36	MSNMS	CVR 329 0x0410 winnt 5.1 i386 MSNMSGR 8.5.1302 msmsgs isgm2@hotmail.it	
7.549458	207.46.106.36	160.80.97.42	MSNMS	CVR 329 8.1.0178 8.1.0178 8.1.0178 http://msgruser.dlservice.microsoft.c	
7.550242	207.46.106.36	160.80.97.42	MSNMS	GCF 0 6944	
7.550484	207.46.106.36	160.80.97.42	MSNMS	value="Zm90b1wuzXh1" /> <imtext value="ZmFudGFzbwFclnppcA==" />	
7.787270	207.46.106.36	160.80.97.42	MSNMS	OFwuzXh1" /> <imtext value="bmv3X3llyXJzX2xldHRlc19mbGFzaFwuzXh1" />	
7.787396	207.46.106.36	160.80.97.42	MSNMS	/> <imtext value="Ym95Yw1hZ3Vjdq==" /> <imtext value="dHV0dXNr"	
7.787496	207.46.106.36	160.80.97.42	MSNMS	> <imtext value="Z3NkZGFZMjQ1ODcyMTRnc2RcLmV4ZQ==" /> <imtext	
8.531298	160.80.97.42	207.46.106.36	MSNMS	USR 331 SSO S t=EwBgAswbAQAUsl/VcBU2SH7mwyy3ByswZ71CRDGA07gvMZepT3Zoc+/ 8.901516 207.46.106.36 160.80.97.42 MSNMS USR 331 OK isgm2@hotmail.it 1 0	
8.901547	207.46.106.36	160.80.97.42	MSNMS	SBS 0 null	
8.901877	207.46.106.36	160.80.97.42	MSNMS	MSG Hotmail Hotmail 1236	
8.927283	160.80.97.42	207.46.106.36	MSNMS	BLP 332 BL	
9.161514	207.46.106.36	160.80.97.42	MSNMS	BLP 332 BL	
9.161551	160.80.97.42	207.46.106.36	MSNMS	ADL 333 102	
9.396901	207.46.106.36	160.80.97.42	MSNMS	PRP 334 MFN Gianluigi	
9.397215	207.46.106.36	160.80.97.42	MSNMS	BLP 337 BL	
9.397246	207.46.106.36	160.80.97.42	MSNMS	ADL 333 OK	
9.397584	207.46.106.36	160.80.97.42	MSNMS	CHG 335 NLN 2253176876 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20	
9.422382	207.46.106.36	160.80.97.42	MSNMS	MSG Hotmail Hotmail 289	
9.577027	207.46.106.36	160.80.97.42	MSNMS	UUX 336 0	
9.712837	207.46.106.36	160.80.97.42	MSNMS	ILN 335 NLN alessandro.lentini@hotmail.it 1 CyPHeR 2254295084 %3Cmsnobj%	
9.712856	207.46.106.36	160.80.97.42	MSNMS	UBX alessandro.lentini@hotmail.it 1 135	
10.25909	160.80.97.42	207.46.106.36	MSNMS	CHG 338 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20	
10.49527	207.46.106.36	160.80.97.42	MSNMS	CHG 338 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20	
10.65237	160.80.97.42	207.46.106.36	MSNMS	CHG 339 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20	
10.88763	207.46.106.36	160.80.97.42	MSNMS	CHG 339 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20	
15.02091	160.80.97.42	207.46.106.36	MSNMS	UUX 340 146	

 VER 325 MSNP15 MSNP14 MSNP13 CVR0

 VER 325 MSNP15

 CVR 326 [...]

 USR 327 SSO I isgm2@hotmail.it

 CVR 326 [...]

 XFR 327 NS 207.46.106.36:1863 U D

Legenda

 : Outgoing

 : Incoming

➔ VER 325 MSNP15 MSNP14 MSNP13 CVR0

➤ VER 325 0x0410 winnt 5.1 i386 MSNMSGR 8.5.1302 msmsgs

➔ CVR 326 isgm2@hotmail.it

➔ USR 327 SSO I isgm2@hotmail.it

➤ CVR 326 [...]

➤ XFR 327 NS 207.46.106.36:1863 U D

Legenda

➔ : Outgoing

➤ : Incoming

	VER 325 MSNP15 MSNP14 MSNP13 CVR0	
	VER 325	8.1.0178 8.1.0178 8.1.0178
	CVR 326	http://msgruser.dlservice.microsoft.com/download/5/6/4/5646481F-33EF-4B08-AF00-4904F7677B89/
	USR 327	IT/Install_WLMessenger.exe
	CVR 326	http://get.live.com/it
	XFR 327 NS 207.46.106.36:1863 U D	

Legenda

-  : Outgoing
-  : Incoming

Time	Source	Destination	Protocol	Info
6.350010	160.80.97.42	207.46.28.93	MSNMS	VER 325 MSNP15 MSNP14 MSNP13 CVR0
6.586659	207.46.28.93	160.80.97.42	MSNMS	VER 325 MSNP15
6.586690	160.80.97.42	207.46.28.93	MSNMS	CVR 326 0x0410 winnt 5.1 i386 MSNMSGR 8.5.1302 msmsgs isgm2@hotmail.it
6.827677	207.46.28.93	160.80.97.42	MSNMS	CVR 326 8.1.0178 8.1.0178 8.1.0178 http://msgruser.dlservice.microsoft.c
6.827702	207.46.28.93	160.80.97.42	MSNMS	XFR 327 NS 207.46.106.36:1863 U D
7.063351	160.80.97.42	207.46.106.36	MSNMS	VER 328 MSNP15 MSNP14 MSNP13 CVR0
7.310508	207.46.106.36	160.80.97.42	MSNMS	VER 328 MSNP15
7.310539	160.80.97.42	207.46.106.36	MSNMS	CVR 329 0x0410 winnt 5.1 i386 MSNMSGR 8.5.1302 msmsgs isgm2@hotmail.it
7.549458	207.46.106.36	160.80.97.42	MSNMS	CVR 329 8.1.0178 8.1.0178 8.1.0178 http://msgruser.dlservice.microsoft.c
7.550242	207.46.106.36	160.80.97.42	MSNMS	GCF 0 6944
7.550484	207.46.106.36	160.80.97.42	MSNMS	value="zm90b1wuzxh1" /> <imtext value="zmFudGFzbwFclnppcA==" />
7.787270	207.46.106.36	160.80.97.42	MSNMS	OFwuzxh1" /> <imtext value="bmv3X3llyXJzX2xlDHRlc19mbGFzaFwuzxh1" />
7.787396	207.46.106.36	160.80.97.42	MSNMS	/> <imtext value="ym95Yw1hz3Vjdq==" /> <imtext value="dhv0dxnr
7.787496	207.46.106.36	160.80.97.42	MSNMS	> <imtext value="Z3NkZGFZMjQ1ODcyMTRnc2RcLmV4ZQ==" /> <imtext
8.531298	160.80.97.42	207.46.106.36	MSNMS	USR 331 SSO S t=EwBgAswbAQAus1/VcBU2SH7mwyy3ByswZ71CRDGAA07gVMZePt3Zoc+/
8.901516	207.46.106.36	160.80.97.42	MSNMS	USR 331 OK isgm2@hotmail.it 1 0
8.901547	207.46.106.36	160.80.97.42	MSNMS	SBS 0 null
8.901877	207.46.106.36	160.80.97.42	MSNMS	MSG Hotmail Hotmail 1236
8.927283	160.80.97.42	207.46.106.36	MSNMS	BLP 332 BL
9.161514	207.46.106.36	160.80.97.42	MSNMS	BLP 332 BL
9.161551	160.80.97.42	207.46.106.36	MSNMS	ADL 333 102
9.396901	207.46.106.36	160.80.97.42	MSNMS	PRP 334 MFN Gianluigi
9.397215	207.46.106.36	160.80.97.42	MSNMS	BLP 337 BL
9.397246	207.46.106.36	160.80.97.42	MSNMS	ADL 333 OK
9.397584	207.46.106.36	160.80.97.42	MSNMS	CHG 335 NLN 2253176876 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
9.422382	207.46.106.36	160.80.97.42	MSNMS	MSG Hotmail Hotmail 289
9.577027	207.46.106.36	160.80.97.42	MSNMS	UUX 336 0
9.712837	207.46.106.36	160.80.97.42	MSNMS	ILN 335 NLN alessandro.lentini@hotmail.it 1 CyPHER 2254295084 %3Cmsnobj%
9.712856	207.46.106.36	160.80.97.42	MSNMS	UBX alessandro.lentini@hotmail.it 1 135
10.25909	160.80.97.42	207.46.106.36	MSNMS	CHG 338 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
10.49527	207.46.106.36	160.80.97.42	MSNMS	CHG 338 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
10.65237	160.80.97.42	207.46.106.36	MSNMS	CHG 339 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
10.88763	207.46.106.36	160.80.97.42	MSNMS	CHG 339 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
15.02091	160.80.97.42	207.46.106.36	MSNMS	UUX 340 146

NS

 VER 328 MSNP15 MSNP14 MSNP13 CVR0

 VER 328 MSNP15

 CVR 329 [...]

 USR 330 SSO I isgm2@hotmail.it

 CVR 329 [...]

 USR 330 SSO S MBI_KEY_OLD [...]

 USR 331 SSO S t=[...]&p=[...]

 USR 331 OK isgm2@hotmail.it 1 0

Time	Source	Destination	Protocol	Info
6.350010	160.80.97.42	207.46.28.93	MSNMS	VER 325 MSNP15 MSNP14 MSNP13 CVR0
6.586659	207.46.28.93	160.80.97.42	MSNMS	VER 325 MSNP15
6.586690	160.80.97.42	207.46.28.93	MSNMS	CVR 326 0x0410 winnt 5.1 i386 MSNMSGR 8.5.1302 msmsgs isgm2@hotmail.it
6.827677	207.46.28.93	160.80.97.42	MSNMS	CVR 326 8.1.0178 8.1.0178 8.1.0178 http://msgruser.dlservice.microsoft.c
6.827702	207.46.28.93	160.80.97.42	MSNMS	XFR 327 NS 207.46.106.36:1863 U D
7.063351	160.80.97.42	207.46.106.36	MSNMS	VER 328 MSNP15 MSNP14 MSNP13 CVR0
7.310508	207.46.106.36	160.80.97.42	MSNMS	VER 328 MSNP15
7.310539	160.80.97.42	207.46.106.36	MSNMS	CVR 329 0x0410 winnt 5.1 i386 MSNMSGR 8.5.1302 msmsgs isgm2@hotmail.it
7.549458	207.46.106.36	160.80.97.42	MSNMS	CVR 329 8.1.0178 8.1.0178 8.1.0178 http://msgruser.dlservice.microsoft.c
7.550242	207.46.106.36	160.80.97.42	MSNMS	GCF 0 6944
7.550484	207.46.106.36	160.80.97.42	MSNMS	value="zm90b1wuzxh1" /> <imtext value="zmFudGFzbwFclnppcA==" />
7.787270	207.46.106.36	160.80.97.42	MSNMS	OFwuzxh1" /> <imtext value="bmv3X3llyXJzX2xldHRlc19mbGFzaFwuzxh1" />
7.787396	207.46.106.36	160.80.97.42	MSNMS	/> <imtext value="ym95Yw1hz3VjdQ==" /> <imtext value="dhV0dXNR
7.787496	207.46.106.36	160.80.97.42	MSNMS	> <imtext value="z3NkZGFZMjQ1ODcyMTRnc2RcLmV4ZQ==" /> <imtext
8.531298	160.80.97.42	207.46.106.36	MSNMS	USR 331 SSO s t=EwBgAswbaQAUS1/VcBU2SH7mwyy3ByswZ71CRDGAAO7gvmZePt3Zoc+/
8.901516	207.46.106.36	160.80.97.42	MSNMS	USR 331 OK isgm2@hotmail.it 1 0
8.901547	207.46.106.36	160.80.97.42	MSNMS	SBS 0 null
8.901877	207.46.106.36	160.80.97.42	MSNMS	MSG Hotmail Hotmail 1236
8.927283	160.80.97.42	207.46.106.36	MSNMS	BLP 332 BL
9.161514	207.46.106.36	160.80.97.42	MSNMS	BLP 332 BL
9.161551	160.80.97.42	207.46.106.36	MSNMS	ADL 333 102
9.396901	207.46.106.36	160.80.97.42	MSNMS	PRP 334 MFN Gianluigi
9.397215	207.46.106.36	160.80.97.42	MSNMS	BLP 337 BL
9.397246	207.46.106.36	160.80.97.42	MSNMS	ADL 333 OK
9.397584	207.46.106.36	160.80.97.42	MSNMS	CHG 335 NLN 2253176876 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
9.422382	207.46.106.36	160.80.97.42	MSNMS	MSG Hotmail Hotmail 289
9.577027	207.46.106.36	160.80.97.42	MSNMS	UUX 336 0
9.712837	207.46.106.36	160.80.97.42	MSNMS	ILN 335 NLN alessandro.lentini@hotmail.it 1 cyPHER 2254295084 %3Cmsnobj%
9.712856	207.46.106.36	160.80.97.42	MSNMS	UBX alessandro.lentini@hotmail.it 1 135
10.25909	160.80.97.42	207.46.106.36	MSNMS	CHG 338 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
10.49527	207.46.106.36	160.80.97.42	MSNMS	CHG 338 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
10.65237	160.80.97.42	207.46.106.36	MSNMS	CHG 339 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
10.88763	207.46.106.36	160.80.97.42	MSNMS	CHG 339 NLN 2254290988 %3Cmsnobj%20Creator%3D%22isgm2%40hotmail.it%22%20
15.02091	160.80.97.42	207.46.106.36	MSNMS	UUX 340 146

NS

← MSG Hotmail Hotmail 1236 [...]

→ BLP 332 BL

← BLP 332 BL

→ ADL 333 102 [...]

→ CHG 335 [...]

→ UUX 336 108 [...]

← PRP 334 MFN Gianluigi

← BLP 337 BL

← ADL 333 OK

```
← MSG Ho MIME-Version: 1.0 Age:
→ BLP 332 Content-Type: text/x- BDayPre:
← BLP 332 msmsgsprofile; charset=UTF-8 Birthday:
→ ADL 333 LoginTime: 1222176356 Wallet:
← PRP 334 EmailEnabled: 1 Flags: 1073742915
→ CHG 333 MemberIdHigh: 393216 sid: 72652
→ UUX 336 MemberIdLow: -1619998182 MSPAuth:[...]
← BLP 337 lang_preference: 1040 ClientIP: 160.80.97.42
→ UUX 336 preferredEmail: ClientPort: 53516
← BLP 337 country: IT ABCHMigrated: 1
→ UUX 336 PostalCode: Nickname: mario
← BLP 337 Gender: MPOPEEnabled: 0
→ UUX 336 Kid: 0
← BLP 337 BL
← ADL 333 OK
```

← MSG Hotmail Hotmail 1236 [...]

→ BLP 332 RI

← BLP 332 <ml l="1"><d n="hotmail.it">
<c n="alessandro.lentini" l="3"t="1"/>

→ ADL 333 <c n="isgm1" l="3" t="1"/>
</d></ml>

→ CHG 335 [...]

→ UUX 336 108 [...]

← PRP 334 MFN Gianluigi

← BLP 337 BL

← ADL 333 OK

```
← MSG Hotmail Hotmail 1236 [...]  
→ BLP 332 BL  
← BLP 332 BL  
→ ADL 333 NLN 2253176876 <msnobj Creator="isgm2@hotmail.it"  
Size="26039" Location="0"  
Friendly="ZwBpAGEAbgBsAHUAaQBnAGkAAAA="/>  
→ CHG 333  
→ UUX 336 <Data>  
<PSM>gianluigi 16 sept parent...</PSM>  
← PRP 334 <CurrentMedia></CurrentMedia>  
<MachineGuid></MachineGuid>  
← BLP 337 </Data>  
← ADL 333 OK
```

 CHG 335 [...]

 MSG Hotmail Hotmail 289 [...]

 UUX 336 0

 ILN 335 [...]

 UBX alessandro.lentini@hotmail.it 1 135 [...]

 CHG 338 NLN 2254290988 [...]

 CHG 338 NLN 2254290988 [...]

 UUX 340 146 [...]

 UUX 340 0

```
← CHG 338 NLN 2253176876  
← MSG Ho <msnobj Creator="isgm2@hotmail.it" Type="3"  
← UUX 336 SHA1D="TqCChd+11EW90gaOVgVQYP9J3C8=" Size="26039" Location="0"  
← UUX 336 Friendly="ZwBpAGEAbgBsAHUAaQBnAGkAAAA="/>  
← ILN 335 [...]  
← UBX alessandro.lentini@hotmail.it 1 135 [...]  
→ CHG 338 NLN 2254290988 [...]  
← CHG 338 NLN 2254290988 [...]  
→ UUX 340 146 [...]  
← UUX 340 0
```

← CHG 335 [...]

← MSG Ho

← UUX 336

← ILN 335

← UBX ale

→ CHG 33

← CHG 338 NLN 2254290988 [...]

→ UUX 340 146 [...]

← UUX 340 0

MIME-Version: 1.0
Content-Type: text/x-msmsgsinitialmdatnotification;
charset=UTF-8
Mail-Data:
<MD><E><l>0</l><IU>0</IU><O>0</O><OU>0</OU></E><
Q><QTM>409600</QTM><QNM>204800</QNM></Q></MD>
Inbox-URL: /cgi-bin/HoTMaiL
Folders-URL: /cgi-bin/folders
Post-URL: http://www.hotmail.com

← CHG 335 [...]

← MSG Ho NLN alessandro.lentini@hotmail.it 1 CyPHeR 2254295084
<msnobj Creator="alessandro.lentini@hotmail.it" Type="3"

← UUX 336 SHA1D="023fKuaVelpWcjMgpYMQaYizMu0=" Size="24646"
Location="0"

← ILN 335 Friendly="MQAwADAAXwAyADMANwA3AAAA"/>

← UBX alessandro.lentini@hotmail.it 1 135 [...]

→ CHG 338 NLN 2254290988 [...]

← CHG 338 NLN 2254290988 [...]

→ UUX 340 146 [...]

← UUX 340 0

Autenticazione unica o identificazione unica: consente mediante una sola autenticazione l'accesso ad un insieme di risorse a cui è abilitato. SSO soggetto ad attacco di tipo dizionario su password (cfr. [1])

Obiettivi:

- semplificare la gestione delle password;
- semplificare la gestione degli accessi ai vari servizi;
- semplificare la definizione e la gestione delle politiche di sicurezza.

Architettura:

- **Centralizzata:** un unico database globale e centralizzato di tutti gli utenti, approccio destinato a piccole comunità di utenti (e.g. azienda);
- **Federativa:** differenti gestori federati gestiscono i dati di uno stesso utente, l'accesso ad uno dei sistemi federati garantisce automaticamente l'accesso a tutti gli altri (e.g. viaggiatore cliente di un albergo e compagnia di volo federate);
- **Cooperativa:** ciascun utente dipende per ciascun servizio da uno solo dei gestori cooperanti. Come per l'approccio federativo ogni gestore può realizzare la propria policy di sicurezza.

Protocollo:

- **SSL/TLS**(certificati X.509) oppure **Kerberos5** (SPNEGO)

Il protocollo P2P è utilizzato per il trasferimento di contenuti multimediali: immagini personali (i.e. display picture), emoticon personalizzate (i.e. custom emoticon),...

Il protocollo P2P è realizzato in modo da essere indipendente dal “trasporto”.

Ci sono tre tipi di “trasporto”:

- Switchboard
- Direct Connection
- Traversal Using Relay NAT (TURN)

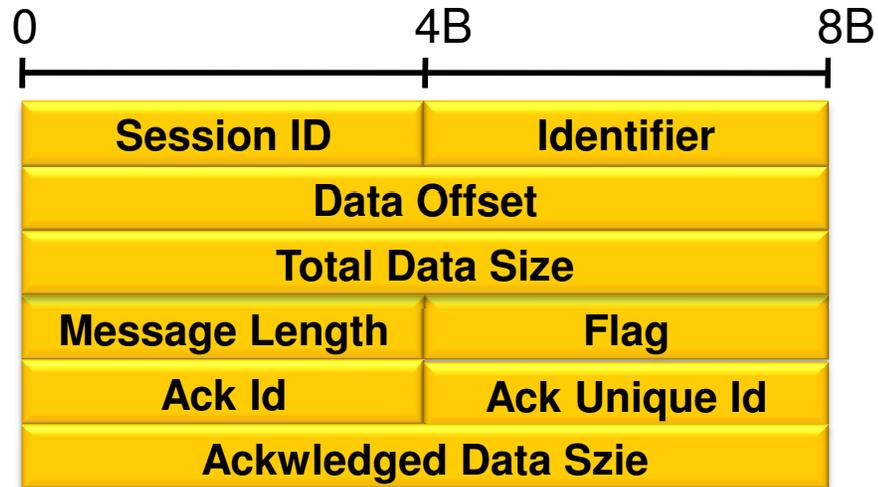


Messaggio P2P:



Binary Header:

Little Endian



Binary Footer:

Big Endian



MSNSLP: protocollo introdotto per lo scambio di dati P2P, basato su un insieme ristretto del protocollo SIP (Session Initiation Protocol, RFC2543) .

MSNSLP usa solo i metodi **INVITE**, **BYE** ed **ACK**

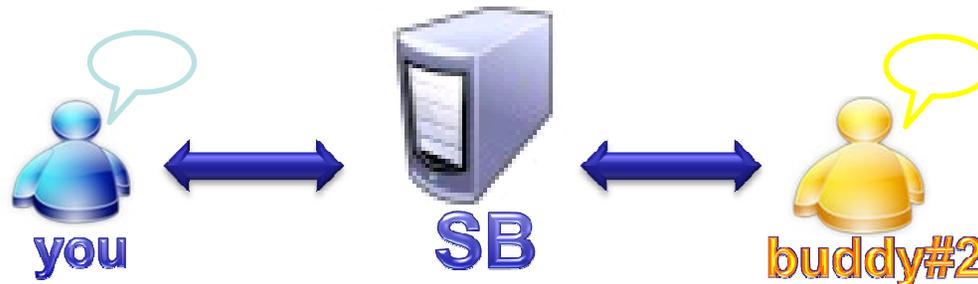
MSNSLP Message: start line\r\n
message-header-1: header value 1\r\n
message-header-2: header value 2\r\n
...
message-header-n: header value n\r\n
\r\n
message body of zero or more bytes
NUL (\0)

Inizialmente i messaggi P2P erano veicolati sullo stesso Switchboard Server utilizzato per la conversazione all'interno di messaggi MSG particolari:

```
MSG 1 D 143
MIME-Version: 1.0
Content-Type: application/x-msnmsggrp2p
P2P-Dest: buddy1@hotmail.com

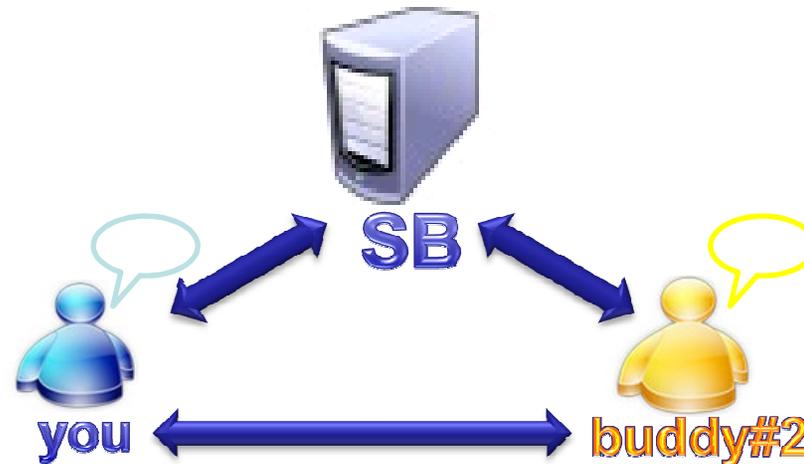
[52 bytes binary data]
```

È possibile sperimentare la migrazione verso uno Switchboard Server differente. Il contenuto da trasferire deve essere inviato in chunk da 1202 bytes.



Il protocollo P2P su Direct Connection prevede una negoziazione basata su messaggi MSNSLP di tipo INVITE al fine di stabilire una connessione diretta.

Il contenuto da trasferire deve essere inviato in chunk da 1202 bytes.



Il protocollo **P2P su TURN** consente a chi si trova dietro ad un **NAT** o ad un **Firewall** di ricevere comunque dati in ingresso mediante connessioni **TCP/UDP su porte non *well-known***.

Permette la comunicazione tra un **host locale** ed un **peer esterno**.

É un semplice protocollo **client-server** che provvede ad un meccanismo di **mutua autenticazione** tra client e server prima della fase di domande e risposte.

Il **client TURN** fornisce al server il proprio indirizzo di trasporto privato e chiede al server il suo indirizzo pubblico.

Il **server TURN** memorizza l'indirizzo di trasporto privato del client e risponde con il proprio indirizzo pubblico.

Il **server TURN** fa poi in modo che tutti i pacchetti inviati da peer esterni verso l'indirizzo pubblico del client siano in realtà diretti verso se stesso. Quando riceve questi pacchetti (UDP o TCP), il server li inoltra verso il client.

Quando il **client TURN** invia pacchetti verso il peer, il server li riceve e li inoltra. Il server TURN lavora quindi da relay per il traffico.

Il protocollo TURN risulta essere **molto pesante** sia in termini di **carico elaborativo** per il server che lo supporta che in termini di **traffico**.

1. Introduzione
 1. Caratteristiche
 2. Evoluzione
 3. Dimensione
 4. Rischi di privacy
 5. Rischi di security
2. MSNP
 1. Introduzione
 2. Sessione di esempio
 3. SSO
 4. P2P
3. **Virtual Parent**
4. Conclusioni
5. Riferimenti bibliografici e sitografici
6. Varie – Q&A

<http://www.virtualparent.eu>

Supporta il genitore nell'attività di controllo su IM, fornendogli uno strumento sw di registrazione/consultazione:

- **semplice** per un genitore con minima familiarità con la tecnologia IM/MSN;
- identifica automaticamente potenziali situazioni **sospette**;
- **reattivo**:
 - Lascia al minore la possibilità di agire liberamente,
 - Registra ed analizza tali attività le analizza,
 - Propone i risultati al genitore.



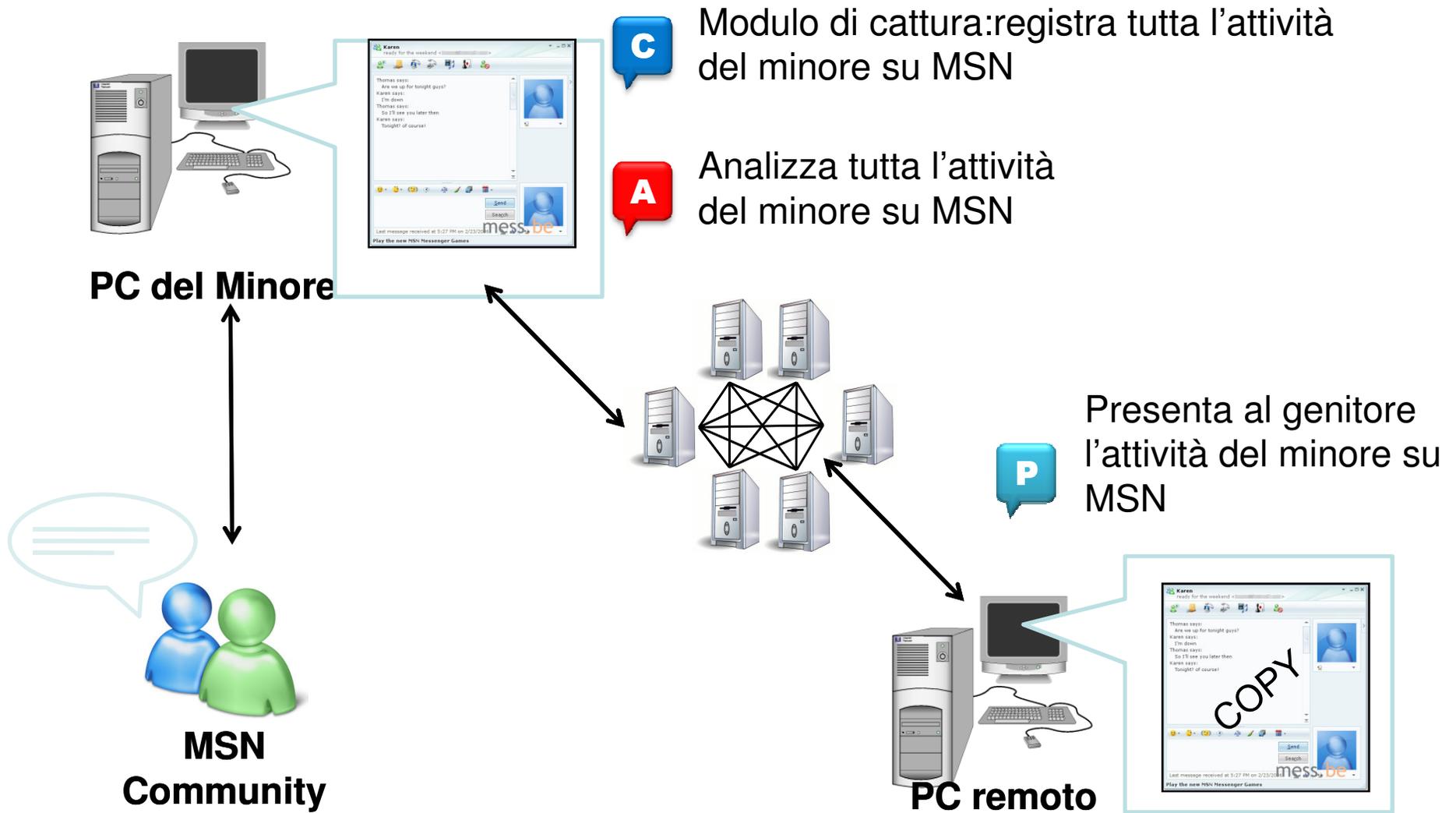
Virtual Parent

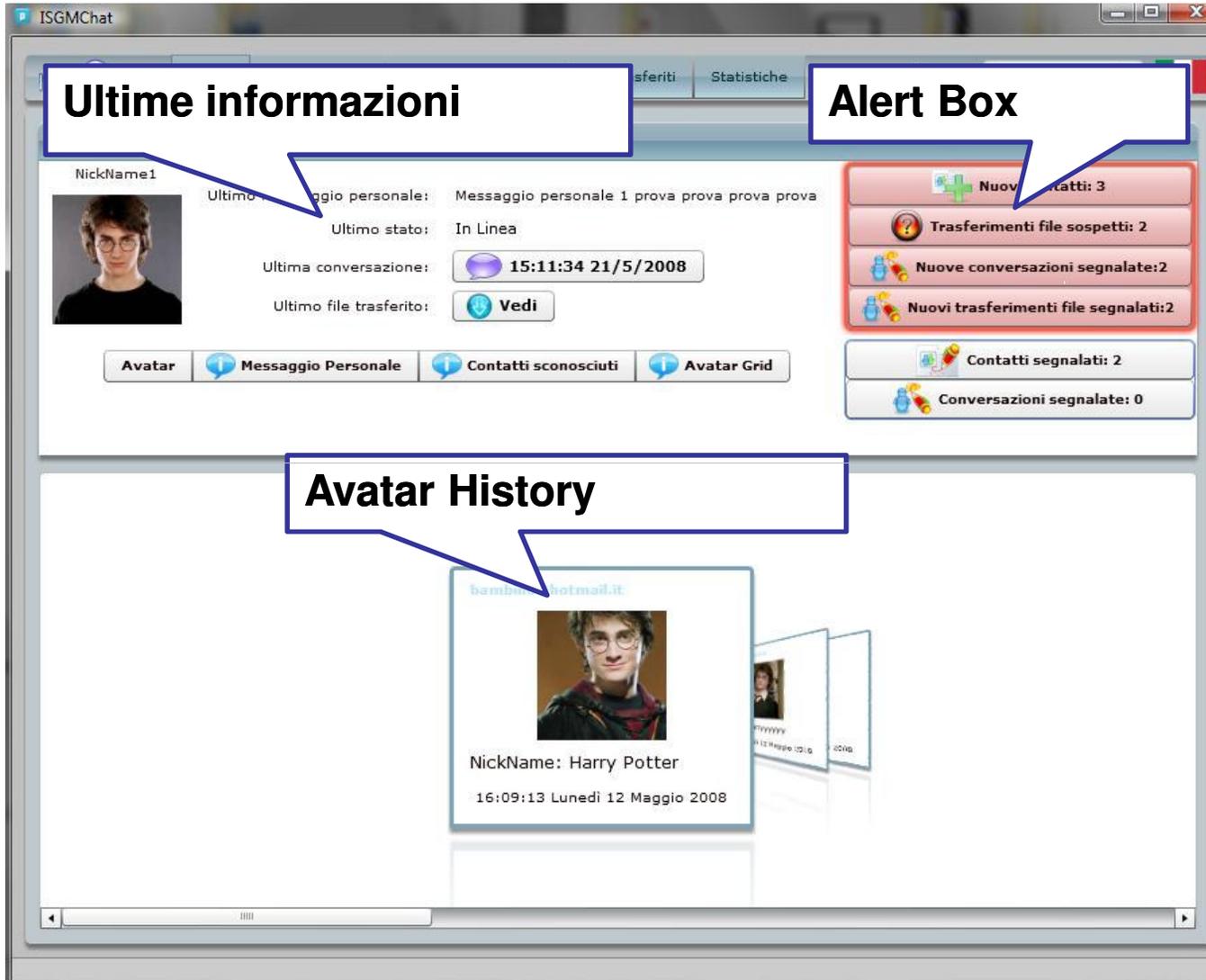
Competitori

Rank	Software	Type	IM Control	Efficacy	Vote
1	Windows Vista Parental Control	OS Module	No	80%	8
2	Optenet	Application	Yes*	62%	7.5
3	Windows Live One Care Family Safety	Application Service	Yes*	74%	7
4	K9 Web Protection	Application	No	62%	7
5	Net Nanny	Application	Yes*	58%	6.5
6	Stopalporno.net	ISP Service	No	73%	6
7	ZOT	Application	No	60%	6
8	Davide.it	ISP Service	No	58%	6
9	Norton Internet Security 2008	Application	No	44%	6
10	KEYfamily	Application	Yes*	n.d.%	5
11	Naomi	Application	No	n.d.%	4

* Blocco totale del traffico applicando regole sulla porta registrata dal protocollo

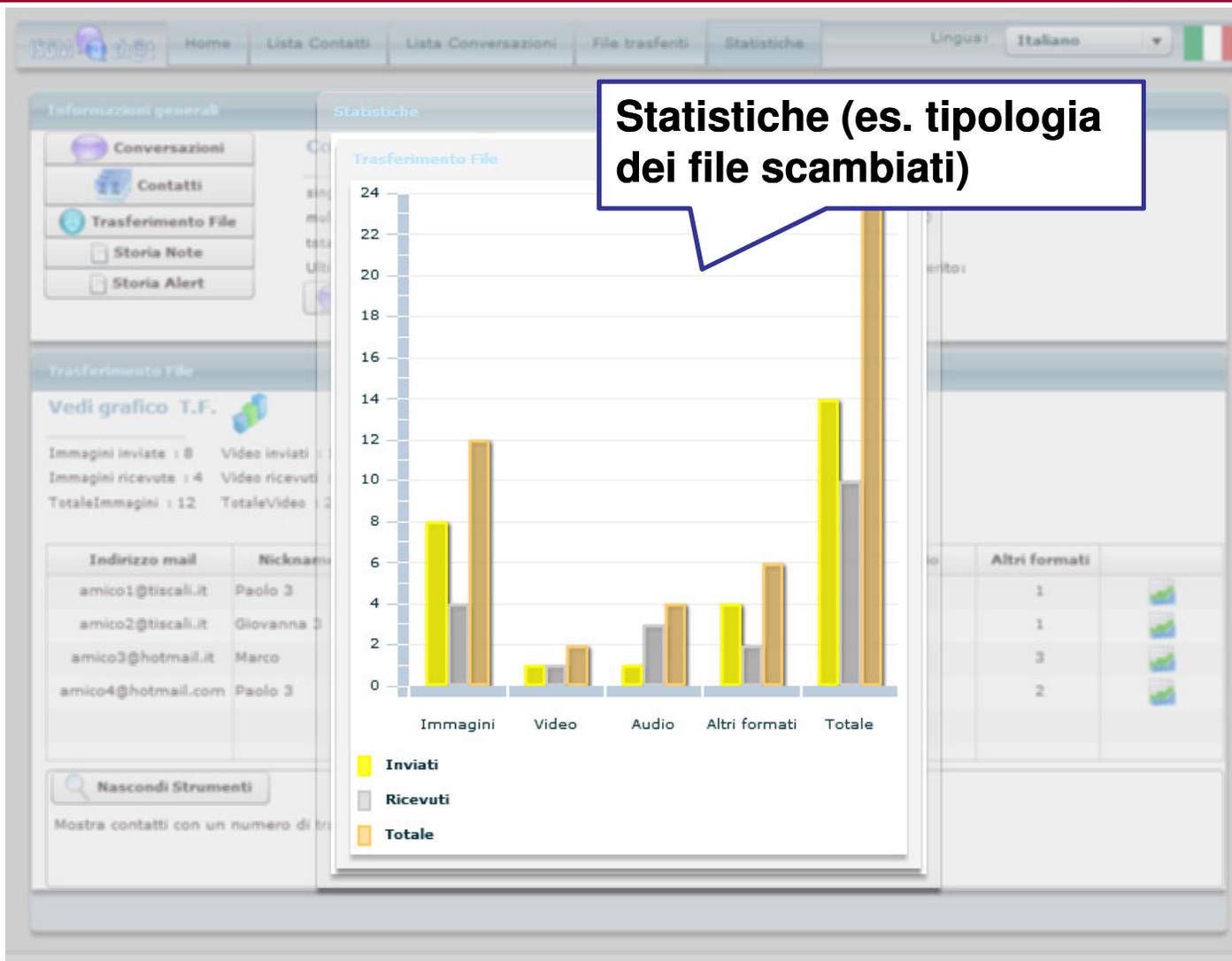
Source : www.elis.org (2008-08-12)





The screenshot shows the ISGMChat application window. It features a user profile for 'NickName1' with a profile picture and various status indicators. A callout box labeled 'Ultime informazioni' points to the profile details. To the right, an 'Alert Box' displays several notifications: 'Nuovi contatti: 3', 'Trasferimenti file sospetti: 2', 'Nuove conversazioni segnalate: 2', and 'Nuovi trasferimenti file segnalati: 2'. Below the profile, there are buttons for 'Avatar', 'Messaggio Personale', 'Contatti sconosciuti', and 'Avatar Grid'. At the bottom, an 'Avatar History' section shows a sequence of avatars, with the most recent one being 'Harry Potter' with the nickname 'Harry Potter' and a timestamp of '16:09:13 Lunedì 12 Maggio 2008'.

Virtual Parent Screenshot



1. Introduzione
 1. Caratteristiche
 2. Evoluzione
 3. Dimensione
 4. Rischi di privacy
 5. Rischi di security
2. MSNP
 1. Introduzione
 2. Sessione di esempio
 3. SSO
 4. P2P
3. Virtual Parent
4. **Conclusioni**
5. Riferimenti bibliografici e sitografici
6. Varie – Q&A

SocialNetwork ed **InstantMessaging** hanno evidenziato la “porosità” della rete, i pericoli di un tale utilizzo sono quelli relativi alla sindrome “**boiling frog**”.

Il rilascio delle **informazioni personali** (e.g. dati anagrafici, recapiti telefonici, domicilio, ...) presso siti di SN e IM non è target di alcuna soluzione tecnologica adeguata.

Esistono rari casi in cui l’applicazione di **software di nicchia** (e.g. KeyLogger, Sniffer) riservati ad utenti esperti ha consentito la rilevazione di tentativi di grooming.

In tali casi l’**impegno** richiesto per **analizzare** i risultati prodotti da strumenti realizzati per scopi differenti potrebbe far sfuggire informazioni preziose.

SocialNetwork ed InstantMessaging hanno creato, in rete, i pericoli di un tale utilizzo senza...



o
ad

Esis
Sniffa

In tali c...
realizzati...
...are i risultati prodotti da strumenti
... potrebbe far sfuggire informazioni preziose.

... grooming.

Un'alternativa all'utilizzo di tali meccanismi è l'utilizzo di **software di monitoraggio** con l'enorme svantaggio di dover agire in modalità preventiva (i.e. **BlockList**).

VirtualParent è un software di monitoraggio ma agisce in modalità che agisce in modalità **proattiva e reattiva**; consente la consultazione dei dati raccolti in “**soft real time**” da una postazione remota. Tale software si pone infatti come **strumento supplementare ma non sostitutivo** del processo educativo

<http://www.virtualparent.eu>

Tuttavia benchè sia possibile per un genitore controllare le attività del proprio figlio ai minori è riconosciuta la **libertà di corrispondenza** di cui devono essere **tutelate** la **libertà** e la **segretezza** fino a quando ciò non rappresenti un ostacolo alla tutela della **integrità fisica e morale del minore**.

1. Introduzione
 1. Caratteristiche
 2. Evoluzione
 3. Dimensione
 4. Rischi di privacy
 5. Rischi di security
2. MSNP
 1. Introduzione
 2. Sessione di esempio
 3. SSO
 4. P2P
3. Windows Live Messenger – Tracce su fs
4. Virtual Parent
5. Conclusioni
6. Riferimenti bibliografici e sitografici
7. Varie – Q&A

- [1] Jennings, Nahum, Olshefski, Saha, Yin Shae, Waters. “A study of Internet instant messaging and chat protocols”. IEEE Network, journal of August 2006
- [2] Khoshbakhtian, Darvishan, Eghtedari. “Comparative Analysis of IMP services”. ICTTA 2008, Information and Communication Technologies: From Theory to Applications.
- [4] <http://www.nextplora.it/business/news>.
- [5] Doxa “L’uso di Community, Instant Messaging e Social Network - Indagine presso gli adolescenti di 13-17 anni”, S. 8704/c - Febbraio 2008.
- [6] Wolak, Finkelhor, Mitchell “*Online Predators and their Victims, Myths, Realities, and Implications for Prevention and Treatment*”. Crimes against Children Research Center & Family Research Laboratory, University of New Hampshire
- [7] ENISA, European Network and Information Security Agency, “*Security Issues and Recommendations for Online Social Networks*”, Position Paper No.1, Oct. 2007

Per maggiori informazioni

Ing. Gianluigi Me



me@disp.uniroma2.it

DISP Università di Roma “Tor Vergata”

