Msn Messenger Protocol

You have been using MSN for quite some time wondering how it works. Well You need not look any further. This article will not just tell you how MSN works but will also tell you how to make your own version of MSN messenger. You can download a sample application from here MSN Clone .Let's get ready to rumble!!!!

We can split up the working of MSN messenger into 2 phases

- Authentication Phase
- Instant Messaging Phase

The Authentication Phase involves logging into the MSN messenger server and also (friends) list retrieval in this case.

The Instant Messaging Phase involves sending/accepting requests for an Instant Messaging session and also sending/receiving messages.

The MSN messenger protocol is an ASCII based protocol. In other words the commands are in pure English !!!.The first phase involves connecting to an MSN messenger server .In this case we shall connect to the server 64.4.13.58 on port 1863(MSN messenger works through port 1863).

Once the connection is done we need to start the log in process. The first stage in this phase is the versioning stage. In this stage the client (in this case your app) lists/sends the versions that it can support to the server and waits for the server to respond.

VER 0 MSNP7 MSNP6 MSNP5 MSNP4 CVRO

In the MSN messenger protocol a "trial id" is sent along with every command. The trial id starts from 0 and is incremented every time the server responds successfully to the client's commands.

The server responds like this

VER 0 MSNP7 MSNP6 MSNP5 MSNP4

The Client and the server have agreed on a version in which they will communicate.

Next the client sends a request to the server asking it for the name of the security package it supports for authentication.

INF 1

Unlike Yahoo, Rediff and a few other Messengers MSN does not actually send the password as it is.It encrypts the password while sending it ensuring that your password will not be leaked out easily if somebody monitors your port.

The server responds with this

INF 1 MD5

Here MD5 is the name of the security package which the server currently supports.

Next the client sends the userid to the server

USR 2 MD5 I venky_dude@hotmail.com

Here the server does a check whether it contains all the relevant details about the user for authentication .If it does not then it sends the following reply

XFR 2 NS 64.4.13.55:1863 0

What the server says is that the client should connect to the Notification Server(NS) on 64.4.13.55 on port 1863. We close the current connection and repeat the steps while being connected to the new server i.e 64.4.13.55

- **(client) VER 3 MSNP7 MSNP6 MSNP5 MSNP4 CVRO**
- **(server) VER 3 MSNP7 MSNP6 MSNP5 MSNP4**
- **(client) INF 4**
- **(server) INF 4 MD5**
- **(client) USR 5 MD5 I venky_dude@hotmail.com**

Now the server to which we are connected to has the relevant information about the user trying to log in. The server replies this way

USR 5 MD5 S 989048851.1851137130

The string which is sent by the server is the " MD5 Hash". It is a hash generated by the server and is used in the authentication process. The client then has to send the password which is encrypted using the MD5 algorithm.In effect the client has to send the unique MD5 equivalent of the MD5 hash i.e 989048851.1851137130 in this case and the password combined .i.e. MD5 equivalent of (hash+pass). In this case it turns out to be 3b7926d277068ec49576a0c40598ff21.

USR 6 MD5 S 3b7926d277068ec49576a0c40598ff21

If the password is right then the server replies with this

USR 6 OK venky_dude@hotmail.com venkat

Here the last word is the nickname/name by which the user is known.

In the new version of the protocol (MSNP7) the server sends additional data like some general information about the user and a authentication code something similar to a cookie which can be used for various other functions.

MSG Hotmai Hotmail 362
MIME-Version: 1.0
Content-Type: text/x-msmsgspro file; charset=UT
LoginTime: 1011252477
EmailEnabled: 1
MemberIdHigh: 84736
MemberIdLow: - 1434729391
lang _preference: 103
preferredEmai l: venky_dude@hotmail.com
country: IN

```
PostalCode:
Gender: M
Kid:0
Age: 22
sid: 517
kv: 2
MSPAuth:
2AAAAAAAADU0p4uxxxJtDJozJSlUTS0i7YpwnC9PUHRv56YKxxxCTWmg$$
```

Now we are logged into the server but our status is still offline. We need to change our status to online in order to send and receive messages. The client does this in the following way

```
CHG 7 NLN
```

The server replies with friends who are online and in various states.

```
CHG 7 NLN

ILN 7 NLN btxxxe@hotmail.com nick
ILN 7 AWY wmpyxxx@msn.com mike
ILN 7 BSY tehpxxpxx@hotmail.com yeaxxx

MSG Hotmail Hotmail 223
MIME-Version: 1.0
Content-Type: text/x-msmsgsinitialemailnotification; charset=UTF-8

Inbox-Unread: 293
Folders-Unread: 0
Inbox-URL: /cgi-bin/HoTMaiL
Folders-URL: /cgi-bin/folders
Post-URL: http://www.hotmail.com
```

The next command to be sent to the server pertains to the version of the client currently being used.The client send to the server it's version number and also information about the machine like the OS and the build.

```
CVR 8 0x0409 win 4.10 i386 MSMSGS 4.5.0127 MSMSGS
```

Here 0x409 win 4.10 i386 specifies that the client is running win98 on a intel microprocessor, and MSMSGS 4.5.0127 MSMSGS here specifies the version and build no of msmsgs.exe (basically the version no of MSN messenger).

The server responds with the url to download the latest version and some other info

```
CVR 8 4.5.0127 4.5.0127 1.0.0863
http://download.microsoft.com/download/msnmessenger/install/4.5/win9
8me/en-us/mmssetup.exe http://messenger.microsoft.com
```

It is not necesarry to send the CVR command, the messenger protocol will function properly regardless of this command being sent

To get a list of people who are in our friends list we may send this command

```
LST 9 RL
```

On sending this command the server will reply by sending the reverse list .The reverse list is basically a list of users who can see you when you are online and send you a message.You could alternatively also request for the forward list by sending **LST 9 FL** .The forward list contains a list of all users whom the user has added to his/her list.

The server responds this way

```
LST 9 RL 69 1 19 venky_dude@hotmail.com venkat
LST 9 RL 69 2 19 puxxxxx@hotmail.com PUJA
LST 9 RL 69 3 19 vancxxxxx@hotmail.com ramachandran
LST 9 RL 69 4 19 moxxxxx@hotmail.com chandramouli
LST 9 RL 69 5 19 v_n_xxxxx@hotmail.com Narayanaswamy
LST 9 RL 69 6 19 dexxxxx@hotmail.com Venkatesh
LST 9 RL 69 7 19 lousydxxxxx@hotmail.com
deepika%20kalyani%20Vairam                              LST 9 RL 69
8 19 hexxxxxr@hotmail.com Hetchar%20Ramachandran
LST 9 RL 69 9 19 ambxxxxx@hotmail.com Aiyer
LST 9 RL 69 10 19 suxxx@hotmail.com Ganesh
LST 9 RL 69 11 19 deexxxxx@hotmail.com Deepak
LST 9 RL 69 12 19 anilxxxxx@hotmail.com anil
LST 9 RL 69 13 19 dixxxxx@hotmail.com <Diamond>
LST 9 RL 69 14 19 nvxxxx@hotmail.com giri
LST 9 RL 69 15 19 shxxx@hotmail.com Hari
LST 9 RL 69 16 19 radhikashuxxxxx@hotmail.com radhika
LST 9 RL 69 17 19 eskaxxxxx@hotmail.com kannan
LST 9 RL 69 18 19 shaxxxxx@hotmail.com Shankar
LST 9 RL 69 19 19 puneetagarxxxxx@hotmail.com puneet
```

*Every time a friend comes online the server(NS) sends us the following command

NLN 10NLN deaxxxx@hotmail.com Venkatesh

and when the friend goes offline the server sends us this

FLN 10 FLN deaxxxx@hotmail.com

With the MSNP7 protocol msn has introduced a new challenege authentication mechanism. The MSN server sends t a challenge key which the user has to authenticate succesfully in order for the session to continue.

CHL 0 20881396011366812350

The client has to send the md5 equivalent of this string which is formed by appending this hash with the string "Q1P7W2E4J9R8U3S5".So the final string which will be sent to the server will be the md5 equivalent of **20881396011366812350Q1P7W2E4J9R8U3S5**

i.e MD5string(20881396011366812350Q1P7W2E4J9R8U3S5)

So the client response would be something like this

QRY 18 msmsgs@msnmsgr.com 32
0212eaad0876afb8505859ca75d21a78

Here 18 is the trial id .Replace it by the appropriate trial id in your program .

The server will respond in the following way if the authentication is right

QRY 18

We have successfully logged into the MSN Messenger server. The Instant Messaging phase is next.

Instant Messaging in MSN Messenger is session based . The people in between whom the conversation is going to take place have to be in a session mode. We cannot send/receive messages unless we start a chat session with a user.

There are basically two methods in which a user can be in a chat session

- User sends a chat session request to another user
- User receives a chat session request from another user

User sends a chat session request

The client(user) sends a command to the server asking it for the address of the SwitchBoard(SB) server. All instant messaging conversation take place via the switchboard server.

XFR 9 SB

The server(SB) replies back with the ip address of the switchboard server(SB),the port on which to connect and a CKI hash. CKI is a security package and the client has to use the hash to connect to the switchboard server.

XFR 9 SB 64.4.13.88:1863 CKI 989487642.2070896604

Now we have to make another new connection this time to the switchboard server. Our previous connection to the MSN messenger server must be kept as it is. If we lose connection with that server we would log out.

After we have connected to the switchboard server(SB) we send the following command to the switchboard server.

USR 1 venky_dude@hotmail.com 989487642.2070896604

If the CKI hash sent by us is right the server(SB) responds back with this

USR 1 OK venky_dude@hotmail.com venkat

After this has been done the user has to "Call" the other user to the chat session. This is done by sending the following command.

CAL 2 deadxxx@hotmail.com

The server replies back with the a session id which it will pass on to the other user

CAL 2 RINGING 11717653

When the other user replies and is ready for a chat the server(SB) sends us this command

JOI deadlee@hotmail.com Venkatesh

This indicates that the other user has joined in the conversation and we are now ready to send and receive messages.

User receives a chat session request

When we are being invited to a chat session by a user the server(NS) send us the following message.

RNG 11742066 64.4.13.74:1863 CKI 989495494.750408580 deaxxxx@hotmail.com Venkatesh

Here the server(NS) sends us the session id ,the ip address of the SwitchBoard server to connect to,the port on which to connect to ,the CKI hash and the user trying to start a conversation with us.

Now we have to make another new connection this time to the switchboard server. Our previous connection to the MSN messenger server must be kept as it is. If we loose connection with that server we would log out.

We connect to the switchboard server and send the following command

ANS 1 venky_dude@hotmail.com 989495494.750408580 11742066

Here we send our login name ,the CKI hash that was sent to us and the session Id that was sent to us

The server responds back with

IRO 1 1 1 deaxxxx@hotmail.com Venkatesh

and

ANS 1 OK

We are now ready to send and receive messages.

Before sending/receiving messages let us see how the message is constructed.

When we are sending a message we build the header information in the following way

```
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=Microsoft%20Sans%20Serif; EF=; CO=0; CS=0;
PF=22
```

While sending a message we send it this way

```
MSG  2  N
137
                    MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=Microsoft%20Sans%20Serif; EF=; CO=0; CS=0;
PF=22

hello
```

Here 2 is the trial id which has to incremented each time we send a message. 137 is the total length of the message i.e length of the header and length of the actual message that we are sending in this case it is 'hello'.

While receiving the message it is more or less similar

Here is an example of a message received

```
MSG deaxxxx@hotmail.com Venkatesh 137
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=Microsoft%20Sans%20Serif; EF=; CO=0; CS=0;
PF=22

hello
```

When the other user is typing a message we receive the foll message

```
MSG deaxxxx@hotmail.com Venkatesh 100
MIME-Version: 1.0
Content-Type: text/x-msmsgscontrol
TypingUser: deaxxxx@hotmail.com
```

References:

You could take a look at these sites for more information

This is the original protocol published by microsoft.

http://www.tlsecurity.net/Textware/Misc/draft-movva-msn-messenger-protocol-00.txt

This is the MD5 homepage where u can find programs/codes for doing the MD5 encryption

http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html