Presence & Instant Messaging

The Killer Application?

Introduction

- So, how many are familiar with IRC?
- How about ICQ?
- Presence: The ability to see when your friends (or whoever is on your contact list) go online
- Instant Messaging: Not quite email, not quite real-time chat.

History

- Forerunners of IM:
  - Bulletin Board Systems (popular in the 80's and early 90's, some of you may remember them?) often allowed you to chat with the System Operator or users on other nodes of the same BBS.

BBS Screenshot

History cont'd

- Forerunners of IM:
  - IRC – Internet Relay Chat
    - Invented in 1988 by a Finnish engineering student named Jarkko Oikarinen
    - We were lucky enough to find a picture of him… He's quite the computer nerd…

Jarkko's Picture

History: IRC

- Allows for real-time chat any user with an IRC client and connection to the internet.
- Uses a mixture of P2P and Client-Server computing
- IRC protocol defined in RFC 1459

History: IRC cont'd

- Users join a specific IRC server in order to start chatting
- Each server in a given network is connected to at least one other server in the same network
- To send a message to all the users in a given "chat room", the user sends a message to the server to which it is connected. The server then distributes the message to all the other servers, and the other users see the message.

History: IRC cont'd

- Peer-to-Peer (P2P): If a user wants to send a private message, can use CTCP (Client-To-Client Protocol) or DCC (Direct Client-to-Client) to avoid sending the message thru the server.
- Problems with IRC:
  - "Lag" – messages arrive late / out of sync
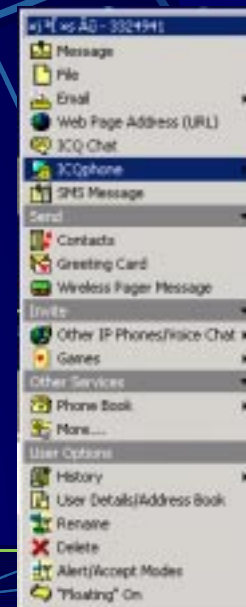 - "Net splits" – server becomes disconnected from rest of network

IRC Diagram
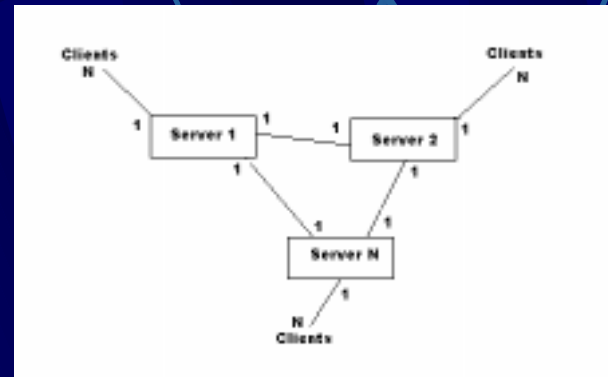
IM: What is it?

- Definition :
  - An application that enables for real time communication on line (but not necessarily).
- Advantages:
  - Less intrusive than a telephone
  - Quicker & more personal than email
  - Free!   =)
- Disadvantages:
  - It's still just plain text.
  - You get what you pay for.   =(

IM: What can you do?

IM: Clients

- Often use Both P2P and Client Server Architecture
  - AOL Instant Messenger (AIM)
  - MSN Messenger
  - Mirabilis ICQ (now owned by AOL)
  - Yahoo Instant Messenger
 - Jabber
  - and A LOT more

IM Growth

- Started in 1996 with AIM
- 50 million users worldwide in 2 ½ years
  - Internet – 5 years
  - Television – 13 years
- Approx 100 million users
- AOL controls over 85% of market
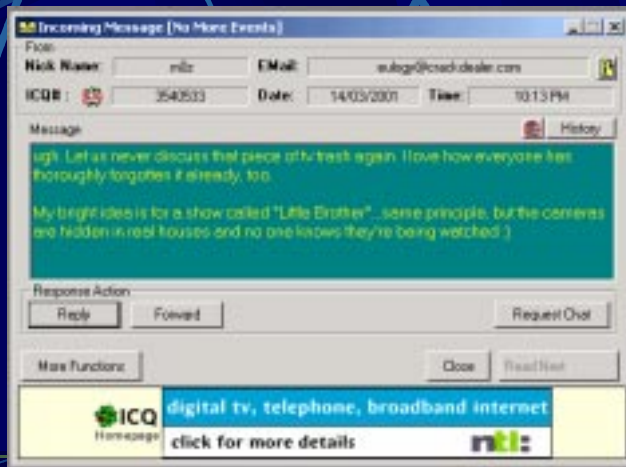- Over 100,000 downloads everyday

ICQ: History

- ICQ stands for "I Seek You"
- Started in 1996 by Mirrabilis
  - A group of 4 Israeli students
  - High school drop outs
- Sold to AOL for $287 million in 1998
- Most features of any other client
- Interesting communication protocol

ICQ: The Interface
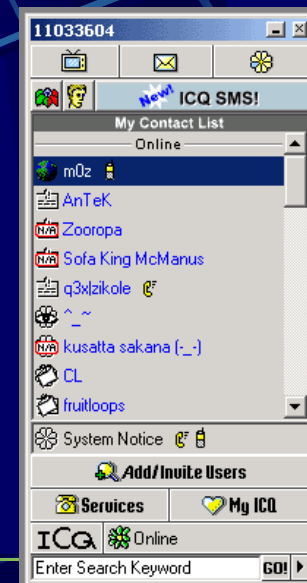
ICQ: An Instant Message

ICQ: Protocol

- 6 versions since 1996
- All versions are backward compatible
- Latest version in ICQ 2000b – much more complex than all previous versions. No one has been able to reverse engineer it.
- Identification message to server
  - IP address
  - Port (usually 4000)
  - User name & Password
  - Contact list

ICQ: Protocol cont'd

- Peer To Peer (P2P) Communication
  - TCP Connection
  - Connection left open until ICQ closed
  - File transfers
  - PC to PC talk
  - Chat
  - Online gaming

ICQ: Protocol cont'd
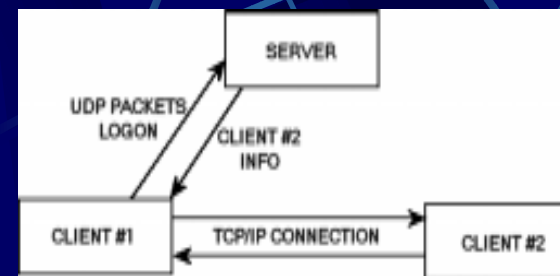
- First 2 bytes of each packet indicate version of protocol used (Major, Minor)
- For example: 02 00 means protocol v2.0
- For more info:
  - http://omega.uta.edu/~tom/ICQ/

Security Issues

- http://blacksun.box.sk/icq.html
  - Too many operations done on client-side
  - Programmers at Mirabilis generally sloppy
  - Does not authenticate connections – anyone with correct protocol is accepted.
  - If client receives unexpected data, usually crashes – usually takes Windows with it, too!

Security Issues cont'd

- ICQ protocol v2 – everything in plain text. Oldest version still in use today – and **all clients are backwards compatible**. Important security implications.
- ICQ protocol v3 – added a simple checksum to verify integrity of packets
- ICQ protocol v4 – first version to start using encryption (still only a weak XOR & a fixed (non random) key though)
- Still, can find programs that will decrypt packets up to v5 - http://acidindustries.8m.com/icqhacking.html

Interoperability Issues

- Each client uses its own protocol and network of servers – IM's biggest problem is lack of standards
- In 1999, Microsoft altered its MSN Messenger, allowing it to "talk" to AIM clients
- AOL in turn accused Microsoft of "hacking" into its system.

IM Standards

- IETF Working on a Standard - http://www.imppwg.org/
  - IMPS (Instant Messaging and Presence using SIP)
  - IMXP (Blocks Extensible Exchange Protocol) (aka APEX)
  - SIMPLE (Simple Instant Messaging Protocol)
  - PRIM (Presence & Instant Messaging)

IM Future

- IM Standard
- Cross-Client Access
  - ICQ can send SMS to my cell phone
  - ICQ - Web page interaction
    - http://www.icq.com/panels/tools-catalog.html
- Convergence - IM in your Fridge?
  - When to buy milk?
  - When is my beer cold?