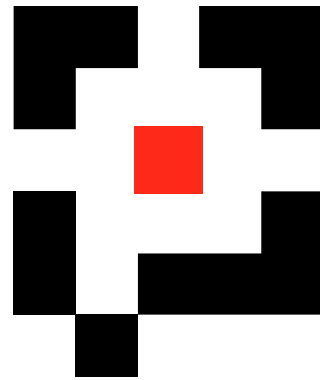


I
N
D
I
A
N
A

U
N
I
V
E
R
S
I
T
Y

Presentation by ANML
May 2003



pervasive **technology** labs

AT INDIANA UNIVERSITY

Internet Relay Chat (IRC)

About the Presenter

- Mark Meiss
- Academic Background:
 - B.S. Mathematics, B.S. Computer Science
 - Ph.D. student in Department of Computer Science
- Research interests:
 - High-performance file transfer protocols
 - Network management
 - Embedded programming languages
 - Sensor networks



About the Presenter

- Professional Experience:
 - Over 10 years in software development
 - With IU IT Services since 1997
 - Worked with Bloomington NOC
 - First employee of ANML
 - Developed Animated Traffic Map, Router Proxy, etc.



What is IRC?

- Internet Relay Chat
 - Developed in 1988 by Jarkko Oikarinen
 - Designed as a worldwide forum for public and private discussions
 - Immediately and widely successful
 - Formally defined in RFC 1459 (1993)
 - Updated in 2000 in RFCs 2810-2813



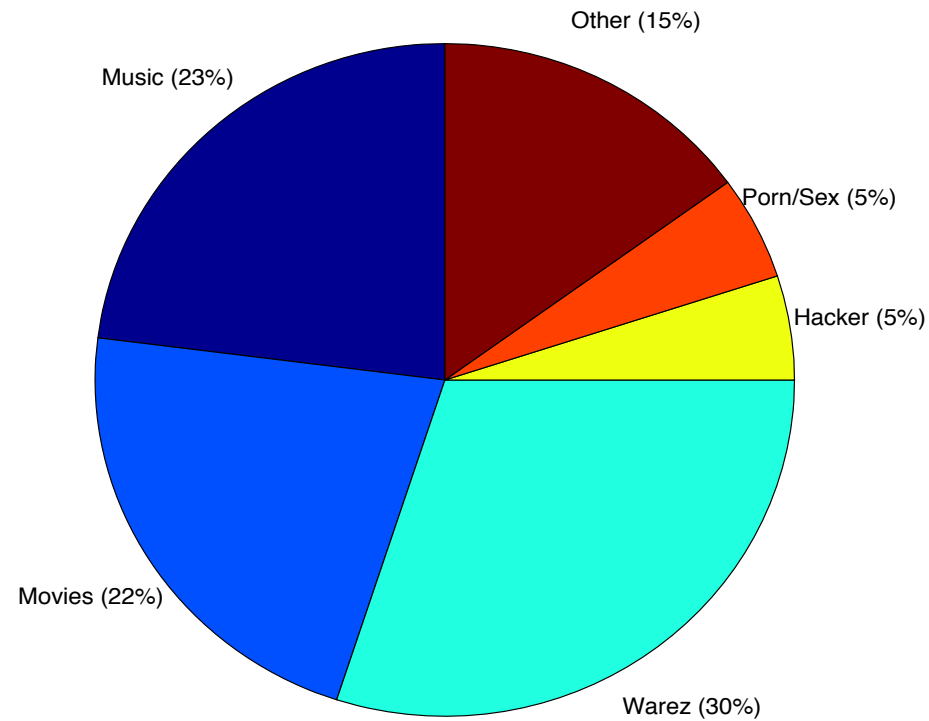
How Popular is IRC?

- Strong analogy to Usenet
 - Used by declining proportion of network users
 - Users are younger and more technically savvy than average
 - Requires at least minimal technical ability to use
 - Total amount of traffic is growing



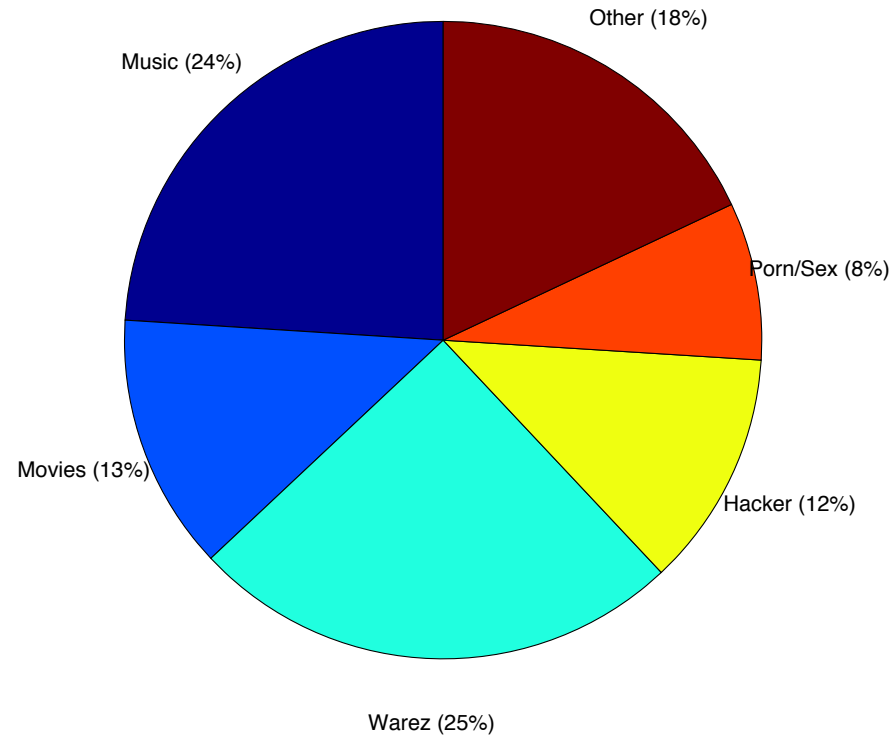
What is IRC Used For?

Top EFNet Channels (English)

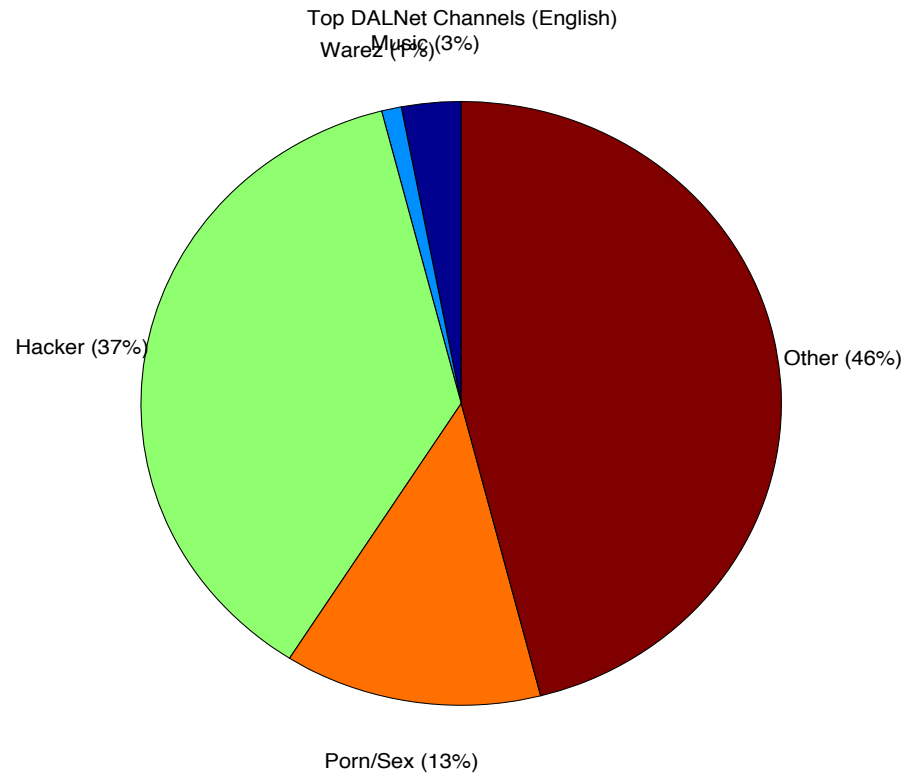


What is IRC Used For?

Top UnderNet Channels (English)



What is IRC Used For?



What is IRC Used For?

- #1 use is piracy (MP3s, Movies, Music Videos, Adult Films, Video Games, etc.)
- #2 use is communication among “Black Hats”
- (priority #6,107 is general chat with other people)



Terminology

- Channel an individual IRC forum
- Operator a channel administrator
- Handle a user's IRC username
- DCC protocol for peer-to-peer file transfer through IRC
- Ident protocol for simple and unreliable authentication



The IRC Network

- There is no “main IRC network”
 - Original network has split into hundreds of smaller networks
 - Each IRC network is independent of the others
- Most popular/notorious networks are AlterNet, DALNet, EFNet, IRCNet, UnderNet



IRC Network Structure

- Client/server architecture
- Servers are statically connected in a spanning tree
 - No redundant server connections are permitted
 - Traffic is generally not encrypted
- All chat communication is broadcast
- Clients can perform peer-to-peer file transfers



IRC Network Splits

- Because of the lack of redundant connections, IRC networks are vulnerable to “network splits”
- If a server link is broken, we now have two IRC networks
- This can allow malicious users to get operator privileges in channels, subvert bans, or enter private channels



IRC Network Splits

- IRC “warfare” is continuous and eternal
 - Most large IRC networks are under attack almost 24/7
 - Many DoS attacks are directed at IRC for revenge or to cause splits in the network
- Network administrators don’t like to host IRC
 - IRC servers are gone from most American universities
 - Majority of servers are European



Using IRC

- Clients are available for most platforms
 - *mIRC* most popular for Windows
 - *BitchX* most popular for Linux
 - *ircII* can run on just about anything
 - Not hard to program basic functionality
- Server usually listens on port 6667
- Most servers “authenticate” clients with *ident* protocol

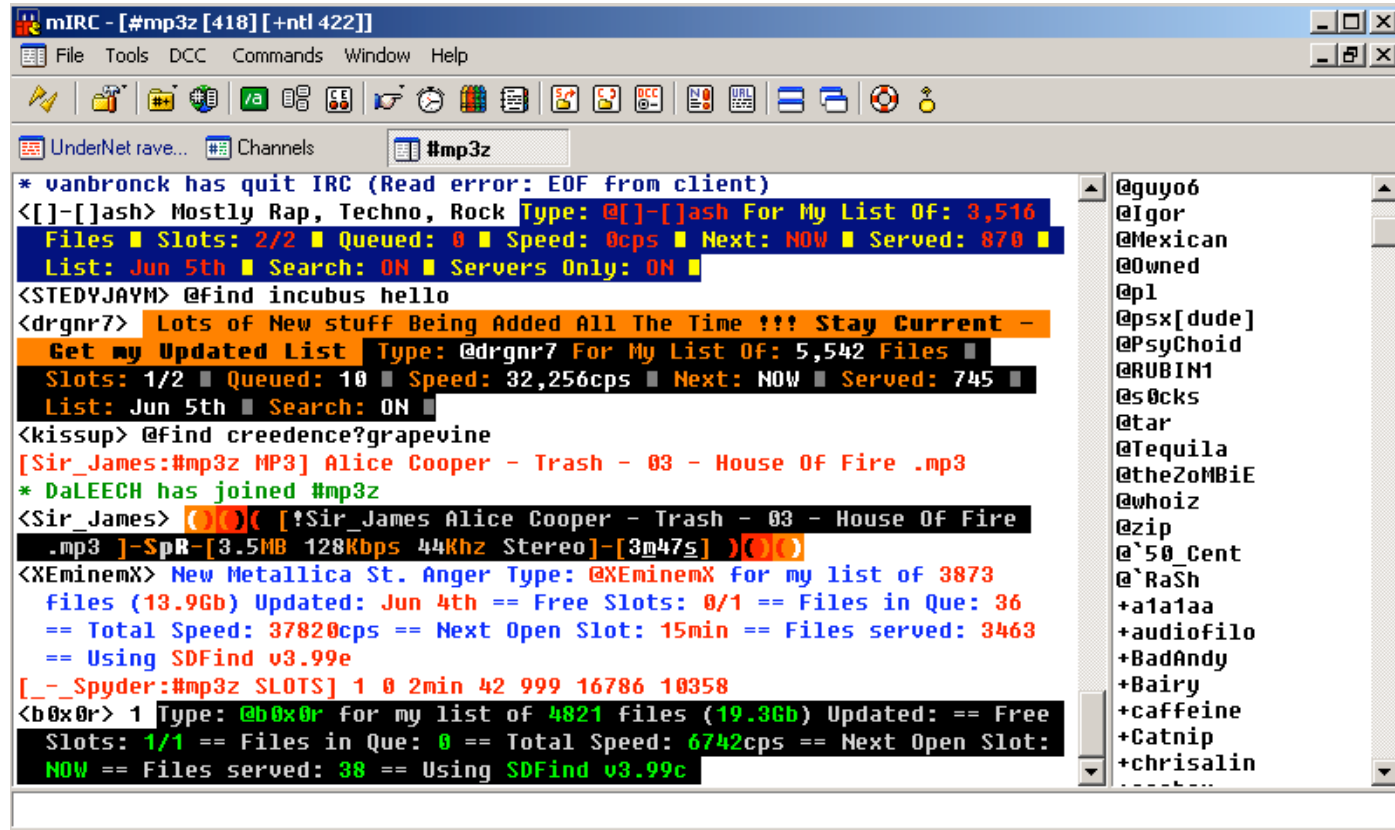


Using IRC

- Most lines of input go to the current channel
- IRC commands are prefixed with a slash:
 - /list
 - /join <channel>
 - /whois <handle>
 - /kick <handle>
 - /mode <operation>



IRC Screenshot



Private Channels and Bans

- Many channels are private and require a password or personal invitation to join
- Operators can ban users by username, IP address, domain name, etc.
- A great deal (a majority?) of IRC piracy, hacking, etc., is done openly in public channels
- Some channels operate public web servers with freely available passwords, bot locations, etc.



Role of IRC in DDoS

- Many DDoS attacks are against IRC servers themselves
- IRC is the “underground bazaar” of the Internet
- Many DDoS tools use the IRC protocol for communication and triggering

