ABSTRACT

This thesis emphasizes on solving the security problems in IRC, by proposing the alternative security model on IRC that is implemented by four main techniques:

- Strong authentication based on cryptography (RSA algorithm 2048 bits key)
- Strong encryption (Triple DES algorithm 168 bits key)
- Use random function
- Use one way hashing function (SHA-1 algorithm 128 bits key)

After implementing these techniques, IRC will have good authentication process to verify people before establishing session between client-server, have encryption process to encrypt message before sending through the Internet, and have preventing playback messages.

The experiment shows it does not affect the performance of the chat system, so an alternative model has advantages for private communication, and for applying for use in business organization which require chatting via the public network.