Contents

[1 Analysis 2](#_Toc64805679)

[1.1 Problem Identification 2](#_Toc64805680)

[1.1.1 Problem outline 2](#_Toc64805681)

[1.1.2 Stakeholders 2](#_Toc64805682)

[1.1.3 How can the problem be solved by computational methods? 2](#_Toc64805683)

[1.1.4 Computational methods that the solution lends itself to 2](#_Toc64805684)

[1.2 Research 4](#_Toc64805685)

[1.2.1 Existing program – Discord 4](#_Toc64805686)

[1.2.2 Existing solution – Internet Relay Chat (IRC) 5](#_Toc64805687)

[1.2.3 Interview questions 7](#_Toc64805688)

[1.2.4 Interview 7](#_Toc64805689)

[1.3 Requirements 7](#_Toc64805690)

[1.3.1 Software requirements 7](#_Toc64805691)

[1.3.2 Stakeholder requirements 7](#_Toc64805692)

[1.4 Success Criteria 7](#_Toc64805693)

[2 Design 7](#_Toc64805694)

[3 Development 7](#_Toc64805695)

[4 Evaluation 7](#_Toc64805696)

[5 References 8](#_Toc64805697)

# Analysis

## Problem Identification

### Problem outline

Currently, the encryption in-transit system is widely used in instant messaging apps. This means that a user’s messages will be in plaintext in the service provider’s server, which allows the service provider to read users’ conversations breaching their privacy. These companies are then also susceptible to potential attackers accessing confidential information through this potential backdoor. Therefore, I will be making a solution to this problem of user privacy by making an end-to-end encrypted instant messaging program.

For this solution to work, the following features are required: only the endpoint users have the key for the symmetric encryption algorithm to qualify the system as end-to-end encryption; an easy-to-use GUI so that anyone can navigate and use the program; a login/sign-up system to authenticate users’ identities to the server to facilitate historic message viewing; networking capabilities in order send and receive messages from different networks with a low enough latency to be a viable ‘instant’ messaging platform.

### Stakeholders

The target audience of this program is split into two categories. Firstly, there will be privacy-conscious stakeholders who are choosing their instant messaging platform based on the security that the program provides to their information. The requirements for these stakeholders will be the following: all the communications on the program will be encrypted; the only parties that can view the plaintext messages are the endpoint users; all sensitive passwords stored on the server will be hashed. These stakeholders will make use of the program through business, gaming, or everyday communications to name a few use cases as all the needs are satisfied as part of the program’s essential features.

Secondly, there will be stakeholders who are people less familiar with computers that are looking for an easily accessible instant messaging platform. The requirements for these users will be an intuitive user interface with little to no prior setup needed for them to start using the program. They will make use of the program to keep in touch will family and friends; therefore, the program must be easy to use as to not deter them.

### How can the problem be solved by computational methods?

This problem is well suited to a computational approach as it can be solved using computational methods. This is because the process of encrypting, sending then decrypting messages over a network can be greatly abstracted for the user so that they do not need any prior technical knowledge to use the program. The solution will also have many algorithms to carry out processes without the need for complex input from the user.

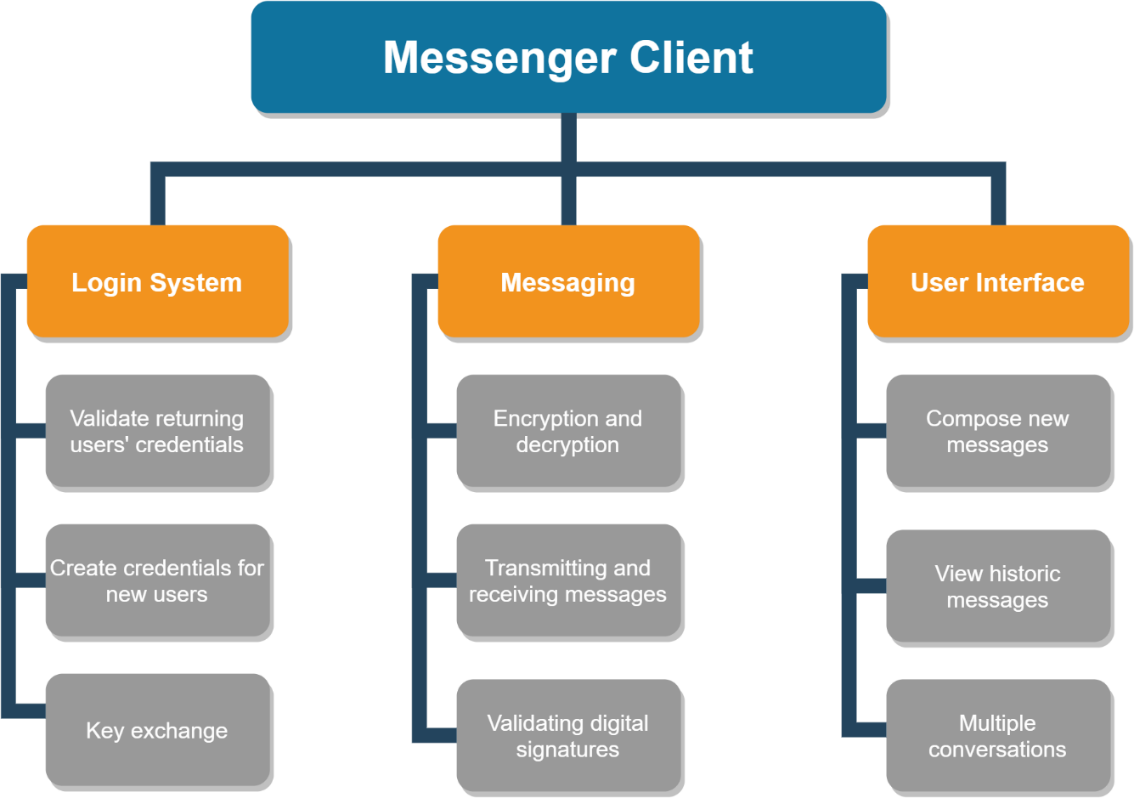
### Computational methods that the solution lends itself to

**Problem recognition** – The general problem is creating a program where sensitive information is not ever in plaintext whilst passing through the server. However, the more specific problems are creating a system of generating two symmetric private keys over a network connection that people monitoring the network are unable to recreate and sending and receiving the messages over that network. Once this is overcome the rest of the solution is using those keys to do the encryption/decryption and presenting the messages to the user in an intuitive form.

**Abstraction** – It is not necessary (or feasible) for the user to have hands-on control over every single process that happens when sending their messages. Therefore, abstraction will be used to hide most of the processes from the user to streamline their experience by only showing relevant detail. Some of these processes will be the following: encrypting and decrypting their message; segmenting their messages into packets; sending the packets to the server.

**Thinking ahead** – I have thought ahead by choosing C# to write the program is since I expect the backend to require a lot more focus than the frontend; the GUI capabilities in C# are much greater than Python for example (the language I am most familiar with), due to its support for WYSIWYG GUI builders in Visual Studio. I made this decision so that I can spend more time focusing on the development of the backend.

**Procedural thinking & decomposition** – The problem can be decomposed into a set of much smaller problems, using procedural thinking I will develop a solution to each of these in turn.



This set of small problems will allow me to possibly use test harnesses during development to isolate certain parts of the program during the development process. This structure will make the overall solution easier to work with and will make the entire process more efficient.

**Thinking concurrently** – Through the use of concurrent processing, I will make the server-side program more efficient by processing each user’s requests on a virtual thread. This will mean that the program can deal with requests from multiple users and the same time, which is important as if they were acted on procedurally the bandwidth of the system would be dramatically reduced leading to very high latency.

**Performance modelling** – I will make heavy use of performance modelling to ensure that the program functions efficiently. On the smaller scale, I will use performance modelling to profile my encryption algorithms to make sure that they properly balance processing time and security since for this application an algorithm that sufficiently encrypted data in a few milliseconds is vastly superior to an algorithm that more complexly encrypts data in a few minutes. On a larger scale, I will use performance modelling to ensure that my server-side program has properly utilised threads to have a suitable bandwidth to support both average and peak throughput.

## Research

### Existing program – Discord

Discord is a free instant messaging and VoIP platform created in 2015 centred around enabling communities to connect through guilds: collections of chat rooms and voice channels. In 2019 the platform saw 250 million users with a total of 25 billion messages being sent per month [1] making it one of the largest gaming-focused communications platforms available.



**Features:**

Each guild is managed by users with varying levels of permissions which can be as general or customised as desired by the guild owner. In the text channels, you can send files, links, and text with basic mark-up. In voice channels, as well as streaming audio you can also use webcams and stream your desktop. The purpose and scope of a guild very flexible as there is no predefined structure: they can be created for a small group of friends or as large official game hubs.

**Differences:**

Discord is not a privacy-focused platform and users are expected to forfeit their privacy in exchange for ease of use and versatility. Discord uses the encryption in-transit system meaning that all traffic is decrypted on the server-side; for non-audio/video data, the HTTPS protocol is used which is encrypted using TLS or SSL. It is also known that Discord inspects all user traffic whilst it passes through their server. However, the reason why is unknown.

**Parts I can apply to my solution:**

1. The idea of having a central area consisting of multiple ‘channels’ for different conversations or topics would potentially be worth including in my solution. This is because it would be an intuitive structure for larger chat rooms, where having a singular area for everyone to talk in would not be feasible.
2. I also think that Discord’s feature of activity statuses for each user would be a good addition to my solution. This would not be an essential feature but, if I have enough time to add it, it will improve the overall experience of the user by enabling them to see who is also online while they are using the program.

### Existing solution – Internet Relay Chat (IRC)

Internet Relay Chat is an internet protocol created in 1988 to allow group plaintext conversations with channels working on a client-server model or to individuals with private messages using the Direct Client-to-Client protocol (DCC). In February 2005, at the height of IRC the largest network – QuakeNet – saw a peak user count of almost a quarter of a million users [2]. This has dramatically reduced since then and is now at an average of 10 thousand users [3]. However, the protocol is still used by some services today as a means of lightweight communication typically attached to a larger service: The Twitch IRC network is responsible for the live chat in a Twitch stream and some games such as Tabletop Simulator, StarCraft, and Unreal Tournament use IRC for their in-game chat.



*Image via* [*WeeChat.org*](https://weechat.org/about/screenshots/)

**Networking:**

The structure of an IRC network is a spanning tree, in which clients will connect to one of the multiple servers that all share the same state [4]. This introduces the first limitation of IRC: the fact that the networks are distributed becomes extremely inefficient with large networks as all the servers need to know about all the other servers, clients and channels every time something happens. The second limitation is that if one of the server-server connections was to go down, the network would split in half and many users will appear to have disconnected in what is called a netsplit.

**Difference:**

In my solution, I will use a centralised network. This means that I will not have to constantly share state information between servers like in an IRC network so the configuration and maintenance will be easier. However, the solution will be limited with scalability as the maximum throughput of the network is limited to the bandwidth of the one machine and the only way to scale up the network is to upgrade the parts in that machine.

**Group Messaging:**

To access IRC channels, users must first install an IRC client and select the domain name for the network they want to connect to. Once connected they will have to choose a display name. This is because users do not need to register to use IRC, only supply a short identifier in the form of a nickname [5]. Finally, once they join a network’s channel, the network’s server they are connected to will relay all the messages they send to all the other users connected to the channel, and vice versa.

**Difference:**

In my solution, I will require users to register before they can use the program. This will help to prevent the nickname collisions which occurred with IRC where multiple people had/wanted the same nickname. This will ensure the all the messages are sent to the correct users and data validation can be used to make sure no two people accidentally share an identifier.

**Offline Messages:**

Some IRC networks support bouncers that enable offline messages, these are daemons on a server that act as a proxy for the client. When a client connects to a bouncer, the bouncer simply relays all the traffic to and from the server. However, in the event the client disconnects, the bouncer can store the messages that the client would have received if they were still connected. These will then be sent to the client once they reconnect. A similar implementation for offline messages is having a client run on an always-on server to which users connect to via SSH for their session. This also allows users who do not have an IRC client installed to connect.

**Part I can add to my solution:**

In my solution, I could include a way of archiving messages for users when they are not online. This could be implemented in a similar way to the bouncer where if the server detects that the client is no longer connected it will reroute the messages to a daemon. However, I will need to find a way of securely storing the user’s messages as security is a focus point of the solution.

**Typical Client User Interface:**

The layout of the UI for many IRC clients is the following: channels on the left, a nickname list on the right and the chat in the middle (this has become a common chat program layout as can be seen in Discord’s GUI in the section prior). In the past and in addition to standalone programs, Opera came with an IRC client attached to Opera Mail and there was an IRC client for Firefox called ChatZilla. This proved that IRC was a very lightweight protocol with not many needs besides a socket to run off.

**Part I can include in my solution:**

In my solution, I will also try to create a lightweight protocol that only requires a single socket as it is a requirement for my solution to create a lightweight program. I also think that sticking to the tried and tested chat program layout shown in many IRC clients will be a good inclusion into my program; since it will make using the program a lot easier for users who have used other chat programs in the past and it seems like an intuitive design for new users.

### Interview questions

### Interview

## Requirements

### Software requirements

### Stakeholder requirements

## Success Criteria

# Design

# Development

# Evaluation

# References

|  |  |
| --- | --- |
| [1] | C. Corberly, “Discord has surpassed 250 million registered users,” TechSpot, 13 May 2019. [Online]. Available: https://www.techspot.com/news/80064-discord-has-surpassed-250-million-registered-users.html. [Accessed 12 February 2021]. |
| [2] | A. Gelhausen, “IRC Networks - Top 10 in the annual comparison,” Netsplit, 2005. [Online]. Available: https://netsplit.de/networks/top10.php?year=2005. [Accessed 19 February 2021]. |
| [3] | A. Gelhausen, “IRC Network QuakeNet,” Netsplit, [Online]. Available: https://netsplit.de/networks/QuakeNet/. [Accessed 19 February 2021]. |
| [4] | C. Kalt, *Internet Relay Chat: Architecture,* RFC 2810 ed., 2000. |
| [5] | J. Oikarinen and D. Reed, *Internet Relay Chat Protocol,* RFC 1459 ed., 1993. |