

Instant Message

COMP3334 Group Project

**─**

COMP3334\_Project\_Group

Junxiong Yang - 13104561d

Sining liu - 12132473d

Yi Zhou - 14109328d

Yuanjing Shi - 13104584d

# Overview

Instant messaging allows text-based real-time communication among individuals. These days, people are concerned about the privacy of their messages during transmission public networks. Also, integrity and authenticity of the origin of messages have to be guaranteed when the application is used in an untrusted environment.

# Problem Statement

1. Our project need to a real-time communication among individuals.
2. The privacy of users’ information and group messages is of our first priority.
3. How could we encrypt the all message we want to hide from potential attackers.

# Security Requirement Analysis

Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Typi non habent claritatem insitam; est usus legentis in iis qui facit eorum claritatem. Investigationes demonstraverunt lectores legere me lius quod ii legunt saepius.

## User Identity

It is a must for each side in the chatting group to know that they are talking to someone they are supposed to interact with.

## Private Group Communication

Message and list of users in any of our group would be totally invisible for outside users or possible hackers, which means that only the user(s) in this specific group could post a message or invite a new group mate into

## Data Confidentiality

We need to make sure that even an attacker successfully hack our database, he/she still cannot easily acquire important information since all our data would be encrypted first before to be push into the database.

## Cross-Site Scripting(XSS) & Code Injection

There is always a potential security concern when one wants to implement a specific application on HTML5/PHP. A possible hacker could always use code injection to intercept important information from victim user. To be more concrete, a hacker could use Cross-Site Scripting to hack into our client-side system and intercept session ID from victim user and servers.

# Design specification

## Interface

CSS Style sheet. PHP file list etc.

## Database

Json or some damn like that.

## Implementation of security issues

* Repeat the Security Requirement and expand it.
* User Identity: Login System with PHP hash + salt
* Private Group Communication: Anonymous group ID & In-Group invitation only
* Data Confidentiality: No implementation yet
* XSS: set session parameter & something

# Application Setup Guide

## Lorem ipsum

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

## Dolor sit amet

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

# Conclusion of Individual Contribution

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Project Design | Interface | Database | Server | Report |
| Yuanjing Shi |  |  |  |  |  |
| Zhou Yi |  |  |  |  |  |
| Junxiong Yang |  |  |  |  |  |
| Sining Liu |  |  |  |  |  |

# Bibliography(index)

## Whatsapp End-To-end Encryption

https://www.whatsapp.com/faq/en/general/28030015

## PHP hash function for User data encryption

http://php.net/manual/en/function.hash.php

## XSS prevention Cheat Sheet

https://www.owasp.org/index.php/XSS\_(Cross\_Site\_Scripting)\_Prevention\_Cheat\_Sheet

## PHP set Cookie & set Cookie Parameter

<http://php.net/manual/en/function.setcookie.php>

http://php.net/manual/en/function.session-set-cookie-params.php