WECRYPT MESSENGER

Jonathan Nungaray

CST-451 Capstone Project Proposal

Grand Canyon University

Instructor: Bradley Mauger

Revision: 3

Date: March 25, 2021

**ABSTRACT**

The point and focus of this project is to create an easy to use web application that a user is able to send and receive messages like any normal messaging application. The difference is the level of security. With any good secure messaging application there is encryption that happens, making the data hard for anyone to intercept from the point of sending until it reaches the database. Our application takes these messages and safely stores them encrypted in the database.

For the early iterations we will be storing these messages briefly in order to properly send them, but they will be deleted once the user has viewed the message. In the future we want to create a system that user does not have their messages saved for even a moment on our servers. All this to create a truly secure chat.

|  |
| --- |
| History and Signoff Sheet |

**Change Record**

|  |  |  |
| --- | --- | --- |
| **Date** | **Author** | **Revision Notes** |
| 2/9/21 | Jonathan Nungaray | Initial draft for review/discussion |
| 3/25/21 | Jonathan Nungaray | Updated application artifacts |
|  |  |  |

|  |
| --- |
| **Overall Instructor Feedback/Comments** |

|  |
| --- |
| **Overall Instructor Feedback/Comments** |

**Integrated Instructor Feedback into Project Documentation**

Yes  No

**TABLE OF CONTENTS**

Project Overview and Project Objectives 4

Project Scope 5

Project Success Measures 7

Project Controls 8

Project Cost and Schedule 9

Project Overview and Project Objectives

**State the Problem and Background**

The purpose of this project is to create a secure messaging application where a user can be sure that there are no chat logs being stored and no information being sold or transferred to anyone. The reason I have decided to create this application is for the sole reason of spiting the government and their constant want to have a backdoor into any and all forms of electronic communication. I like privacy and I believe we should have a right to it. So for that reason I wanted to make something that is truly private. To the point that it is so private that even I have no access or capability to seeing the messages and chats that come from this application.

**Project Objectives**

* Create a messaging application
* Let users create an account where they can search for other users
* Allow two users to create a connection to each other
* Have the ability to send and receive messages securely that are encrypted on either end
* Have the chat logs be destroyed upon the destruction of the session

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Outcome** | **Justification** |
| Create a messaging application | met | Application functions with the ability for 2 users to send messages to each other and start new chats |
| Let users create an account and search for other users | met | Application allows for users to create an account using a username and password and search for other users to start a chat with |
| Have ability to send and receive messages that are encrypted | met | Messages are sent to the api then encrypted before they are sent and saved in the database. They are decrypted before being retrieved |
| Have chat logs destroyed upon the destruction of the session | Not met | For the sake of testing and due to time constraints we had to omit the destruction of chat messages. It would take a lot more effort in order to destroy the messages for one user and not the other. For this reason it would be better off as a future update. |

**Challenges**

Some challenges include using a PGP style system that include a public and private key for each individual user. How will we make the transfer of the key between the users without holding the information of those keys ourself? Creating a real-time messaging system that is user friendly and fast will also prove to be a challenge.

**Benefits and Opportunities**

There are no real benefits or opportunities that could come of this project except for a fun proof of concept that can be displayed and shown off during interviews with companies potentially.

Project Scope

**In Scope**

* Create a web application using Vue.js version 2.6 Node.js version 14.15 for the frontend
* Create api for application using PHP 7
* Create database and structures in MySQL
* Allow users to register and login
* Allow users to search for other users and create a chat
* Create capability for users to send and receive chat messages between each other
* Store encrypted messages in a database

**Out of Scope**

* Make all messages go straight from one user to the other with no storing in the database
* Allow creation of group chats
* Destroy all message history upon leaving the application
* Make the application a Progressive Web App (PWA)
* Allow creation of chats that will save the messages for a specific amount of time set by the user
* Allow for sending of media such as pictures and videos

|  |  |  |
| --- | --- | --- |
| Stakeholder Name | Role(s) | Responsibilities |
| Jonathan Nungaray | Developer and owner | Create and maintain the application |
|  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Work Breakdown Structure | | | | | | | | | | |
| ID | Task | Dependencies | Status | Effort Hours | Cost | Start Date | Planned Completion | Estimate to Completion | Actual Completion | Resource |
| 1 | Create project proposal |  | complete | 4 |  | 2/7/21 | 2/7/21 | 4 | 3 |  |
| 2 | Analyze requirements | Project acceptance | complete | 5 |  | 2/10/21 | 2/14/21 | 5 |  |  |
| 3 | Architecture design | Project requirements | complete | 5 |  | 2/15/21 | 2/21/21 | 5 |  |  |
| 4 | Create containers for application | Docker | removed | 5 | 0 |  |  | 5 |  |  |
| 5 | Create server to host on | Heroku | removed | 2 | 0 |  |  | 2 |  |  |
| 6 | Create database | MySQL | complete | 5 | 0 |  |  | 5 |  |  |
| 7 | Create PWA Vue application | container | complete | 8 | 0 |  |  | 8 |  |  |
| 8 | Create PHP API | Vue app | complete | 8 | 0 |  |  | 8 |  |  |
| 9 | Application testing | Completed application | complete | 6 |  | n/a | n/a | 6 |  |  |

Project Success Measures

|  |
| --- |
| Project Completion Criteria |
| 1 – Developed within the given time |
| 2 – Hosted on a server |
| 3 – Meets the requirements to be considered a messaging application |
| 4 – Is secure and encrypted messaging |
| 5 – Optimized so a user receives the message sent within as little time as possible |
| 6 – Good user experience that isn’t too hard to use |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Assumptions and Constraints | | | | | |
| ID | Description | Comments | Type | Status | Date Entered |
| 1 | Short timeline | This class is very short so a large scale application cannot be feasibly achieved | constraint |  | 2/9/21 |
| 2 | Access to a cheap or free server | It may be hard to find a server that is free or cheap enough to host on. Testing may take a lot of the free level of a hosting site | constraint |  | 2/9/21 |

Project Controls

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk Management | | | | |
|  | **Risk Probability** | **Risk Impact** |  |  |
| **Event Risk** | **(high, medium, low)** | **Risk Mitigation** | **Contingency Plan** |
| Data breach or security flaw | low | The whole point of the application is security so it would make the app pointless | Lots of testing to ensure user security | All data will be encrypted |
| Unexpected large amount of users | medium | The application is not prepared to scale for a large user base and would slow down or the server would shut down unless we pay more | Create a highly efficient application that is scalable and ready for a large amount of users. | Have a second serve in mind to host the application on |
|  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Change Control Log | | | | | | | | | |
| **ID** | **Change Description** | **Priority** | **Originator** | **Date Entered** | **Date Assigned** | **Evaluator** | **Status** | **Date of Decision** | **Included in Rev. #** |
| 1 | Initial project creation | 1 |  | 2/28/21 | 2/28/21 | Jonathan | complete |  |  |
| 2 | Add API and database to project | 1 |  | 3/15/21 | 3/15/21 | Jonathan | complete |  |  |
| 3 | Add search functionality | 1 |  | 3/21/21 | 3/21/21 | Jonathan | complete |  |  |
| 4 | Added encryption to messages | 1 |  | 3/25/21 | 3/25/21 | Jonathan | complete |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Roles and Responsibilities | | | |
| Name | Team | Project Role | Responsibility |
| User |  | Feedback and testing | Contact us with feedback and suggestions based on their use of the application |
|  |  |  |  |

Project Cost and Schedule

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| id | item | Assigned to | Start date | Complete by | Time estimate | Actual hours |
| 1 | Analyze requirements | Jonathan | 2/10/21 | 2/14/21 | 5 | 4 |
| 2 | Finalize architecture | Jonathan | 2/15/21 | 2/21/21 | 5 | 3 |
| 3 | Development | Jonathan | 2/22/21 | 3/7/21 | 26 | 32 |
| 4 | Application testing | Jonathan | 3/8/21 | 3/14/21 | 8 | 6 |
| 5 | App deployment | Jonathan | 3/15/21 | 3/20/21 | 4 | -- |
| 6 | User Testing | Users | 3/21/21 | 3/21/21 | 4 | 4 |
| 7 | Feedback updates | Jonathan | 3/22/21 | 3/26/21 | 3 | 5 |