September 9, 2015

California State University, Long Beach
College of Engineering
Department of Computer Engineering and Computer Science

Subject: STATEMENT OF WORK – DESCRIPTION OF PROJECT PROPOSAL FOR COMPUTER SECURITY COURSE

Project Name: ChatSec
Members: Joe M, Chris K
Group Name: ChatSec Team

To whom it may concern:

This document has been written to announce the proposal of project to be initiated in a CSULB course (CECS 478 – Computer Security). The following content contains explanations of the course objectives, project plans and individuals involved.

Project Members

Roles

Chris K will be programmer and system administrator
Joe M will be programmer and security researcher.

Experience

Chris has competent experience working with frameworks, servers, and networking. He will coordinate the project's ability to have net functionality. Joe has worked on projects containing database components written in MySQL as well as udp communication protocols. He will coordinate data management and processing.

Project Development

Assumptions

The project to be initiated will consist of a chat application which allows people to securely talk with one another on an end to end encrypted security protocol. Clients will be able to use this application on multiple platforms. Integrity, confidentiality, authenticity and liability should be ensured as much as possible and still remain beneficial to everyone in the service.

Since the goal of this project is to develop a system that provides this functionality, additional features may be considered towards the end of the main development stage. Also, it will be assumed that the target users could span across all age ranges when this system will eventually contribute to a public service. For this reason, the system will be developed to promote ease of use for all end users.

Scope

The project will be undertaken using different development tools. We will make a dedicated application for the project written in C++ with the Qt framework to utilize all the features we

want across all supported platforms. On the server side a RESTful API will be used. WebSocket technologies serve as the real time communication. We will determine if Cloudflare is necessary for combating DDoS attacks. Nginx, Laravel, node.js, Redis, MySQL may be used as we find necessary.

How exactly end to end encryption can be realized, will be determined during the project (possibly with asymmetric session key exchange and symmetric message encryption).

Anticipated Outcomes
At the end of development, it will be expected that the developed system will consist of a fully functional secure chat system that will be accessible and reliable with minimal vulnerabilities to address.

Week 1 starts at September 14.

Week	Description
1	● IDE Setup ● theoretical preliminary considerations ● database planning ● C++/Qt application planning ● backend planning
2	
3	● backend implementation ● C++/Qt application coding
4	
5	
6	
7	
8	● Testing
9	

****Schedule is set to change whenever necessary!****