SYSTEM AND SOFTWARE DESIGN DESCRIPTION (SSDD):
FOR

An Internet Instant Messaging System

Version 1.0
2016-10-23

Prepared by:
James Combs, Joel Seida
University of Texas at Dallas
Dallas, TX

CS4349.001 SSDD

[put program /system name here]
TABLE OF CONTENTS

Section Page

1 INTRODUCTION

The purpose of this document is to describe the architectural components of secure internet instant messaging system and the supported functionalities of each component, security features, threat model, and attacks considered in a complete and concise manner. The internet instant messaging system supports authentication of its users, confidentiality of the messages and data exchanged between users, and verification of the integrity of messages and data exchanged between its users. This document will describe in general how users log into the system, establish sessions with other users, and how the system provides integrity and confidentiality of message transfers between users as well as any other assumption that have been made in the design of the implementation for the internet instant messaging system.

1.1 DOCUMENT OVERVIEW

This subsection shall provide an overview of the organization of this SSDD.

Section 2 of this document describes the system and software architecture from the developer and user viewpoint.

Section 3 provides a detailed description of the threat model considered in the security protocol design.

Section 4 provides a detailed description of the design of the software supported functionalities as well as the data structures required for implementation of supported functions that contribute to the implementation of the overall system and software architectural entities and components.

2 SYSTEM AND SOFTWARE ARCHITECTURE

This section of the document shall describe with detail every component of the system as well as the relationship and interface between them. These architectural components, when integrated together as specified within this document, shall implement all functions performed by the system in response to an input or in support of an output as described by the project requirements specification. All architectural components shall: be uniquely identifiable, be well described, have clear responsibilities, have well specified interfaces, and have well described interactions with other architectural entities.

2.1 CLIENT

This subsection of the document shall describe in detail the component that represents a client in the system. A client consists of identification information such as IP address, port for TCP stream socket connection to the server and other clients, as well a buddy list that contains a list of possible clients that each client may establish a session with via the session interface. Each client will have a shared session key with the server and other clients for confidential and integrity protected message transfer.

2.2 SERVER

This subsection of the document shall describe in detail the component that represents the server in the system. The server is responsible for providing each client its buddy list, , authentication each client via the login interface the session key for each client after log in authentication has been performed, and a ticket for communication between end users that includes a shared session key among the end users.

2.3 LOGIN INTERFACE

This subsection of the document shall describe in detail the component in which clients log into the system. The login interface should handle the authentication of client trying to connect to the server and enter the system. Once authenticated, the client should be directed to the session interface to allow a session to be established between the server and client.

2.4 SESSION INTERFACE

This subsection of the document shall describe the component that handles establishing a session between two clients. The session interface is responsible for establishing a shared session key between the clients and server as well as between clients themselves. From the sessions keys, encryption and authentication keys will be derived for client to client message transfers. This will allow confidentiality and integrity of the messages being transferred.

2.5 BUDDY LIST

This subsection of the document shall describe the component that allows a client to establish a session with other clients in the system. The buddy list contains detailed information about each client in the system such as IP address, TCP stream socket port number and availability status.

2.6 CLIENT ACCOUNT DATABASE

This subsection of the document shall describe the component that securely stores client identification information. This information is used by the login interface to authenticate each client in the system. client information consists of username, SHA512 hash of password, salt associated with the password hash, IP

address, last login timestamp, unique identification number (maybe), and the current shared session key with the server.

Provide a diagram and description of the architecture.

[Insert diagram here.]

[Insert diagram here.]

3 THREAT MODEL

This section of the document should describe with detail the potential threats and risks considered for the system described in this document. Security features, threat ranking, assets, attacks considered, countermeasures and mitigation will be identified, quantified, and addressed in a complete and detailed manner.

3.1 THREAT IDENTIFICATION

This subsection of the document describes the threats considered and identified during the design of the system referenced in this document. Threats correspond to outside entities that are considered malicious or a danger to the integrity, privacy, and functionality of the system.

3.2 THREAT RANKING

This subsection of the document ranks the threats identified in THREAT IDENTIFICATION from the perspective of risk factors.

3.3 ENTRY POINTS

This subsection of the document defines the interfaces through which an attacker can interact with the system or supply it data.

3.4 ASSETS

This subsection of the document identifies and lists the resources/items of interest to an attacker. Assets can be both physical and abstract.

3.5 ATTACKS CONSIDERED

This subsection of the document lists any attacks considered during the assessment and identification of potential threats and against the security protocols described in SECURITY FEATURES.

3.6 SECURITY FEATURES

This subsection of the document lists and describes the provided security controls and policies to mitigate or prevent the threats and attacks identified in THREAT IDENTIFICATION and ATTACKS CONSIDERED.

4 SOFTWARE DETAILED DESIGN

This section of the document should describe with detail the design of the software being described in this document. This section shall specify the following supported functions that correspond to the relevant architectural components: CLIENT, SERVER, CLIENT ACCOUNT DATABASE, LOGIN INTERFACE, SESSION INTERFACE, and BUDDY LIST as well as how the security features mentioned in SECURITY FEATURES are implemented to provide authentication of clients, message integrity, and message transfer confidentiality.

4.1 DATA DICTIONARY

This subsection shall list and describe all the data and data structures defined and/or used by the components and entities specified above. For each data item or structure indicate where it is defined, referenced, and modified.

Data Dictionary				
Name	***Type/Range***	***Defined by...***	***Referenced by...***	***Modified by...***

5 APPENDIX A. [insert name here]

Include copies of specifications, mockups, prototypes, etc. supplied or derived from the customer. Appendices are labeled A, B, ... n. Reference each appendix as appropriate in the text of the document.

[insert appendix A here]

6 APPENDIX B. [insert name here]

[insert appendix B here]