Software Engineering- CSC 4350 Spring 2017

An encryption and decryption system for message communication

ADEPT

Amani Konduru Benjamin Garber (Daniel) Edward Bull

Paul David Utesch

Team

3/7/2017

Table of Contents

# I. Introduction

# II. RTM

# III. Use Case, Sequence and Interaction diagrams

# IV. Object Design

# V. Test Cases (document)

# VI. Rational (for the entire project)

# VII. Fictional Point Cost Analysis and COCOMO (with comparison and conclusions)

# VIII. Project Legacy

# IX. WSD

# X. Gantt Chart

# XI. Dictionary

1. Encryption: the process of converting data into a code, to prevent unauthorized access. Encryption is the process of transforming data into an unreadable, encrypted form. The transformation is done using one of several cryptographic algorithms that leverage computationally difficult mathematical problems to make reversing the transformation difficult if not effectively impossible
2. Symmetric Encryption: Symmetric Encryption uses a key or set of keys to both encrypt and decrypt data. If data is to be shared between two parties, they must both have the key or keys to decrypt or encrypt the data.
3. Asymmetric Encryption: Asymmetric Encryption, also known as Public Key Encryption, is a type of encryption where anyone in possession of a public key can encrypt a message. That message can then only be decrypted with a private key. This method is often used for identity authentication because it is computationally expensive. Once authentication is completed, communications will then often transition into symmetric encryption after generating a symmetric encryption key.
4. End to End Encryption: Only the communicating users can read the messages.
5. SSL/TLS (Secure Sockets Layer / Transport Layer Protocol): TLS and the now- deprecated SSL it is based on are network security protocols meant to secure client-server connections using both symmetric encryption for data transfer and asymmetric encryption for identity authentication. While there are many options that can be set in an SSL/TLS session, the foundation of the protocols lie in using encryption to authenticate the identities of the connected parties and to secure the privacy of the data transferred between them.
6. Server: a server program awaits and fulfills requests from client programs, which may be running in the same or different computers.
7. Client: requesting program or user.
8. Socket: Is one endpoint of a two-way communication link between two programs running on the network. A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to.
9. SMTP protocol: Simple Mail Transfer Protocol. It is an Internet standard for electronic mail (email) transmission. SMTP was first defined by RFC 821 and updated in RFC 5321.
10. IMAP protocol: Internet Message Access Protocol. Itis an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection. IMAP is defined by RFC 3501.
11. TCP/IP: IP (Internet Protocol) is the basic communication language or protocol of the ozInternet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). TCP (Transmission Control Protocol) is layered on top of IP to provide certain network control and data validation features for many internet communications.

# XXII. Resumes

# XXII. User Guide