TauNet
Software Requirements Specifications v2.0

Index:

I. Introduction:

1. Copyright Notice and License

2. Purpose

The purpose of this document is to record a detailed description of the TauNet system. It will explain the purpose, features, interface, and constraints of the system. This document is intended for the students and professor of CS300-01 during fall term of 2015 at Portland State University and will be used as the basis for the final class project.

3. Scope

This software system will be a secure messaging system that utilized the internet to transmit messages. The system will be designed to set up a network of devices that are able to send simple text messages to each other that will be encrypted on the sender's end and decrypted on the receiver's end.

4. Criteria for a Successful System

Success of the project will be based on the following criteria:

a) The system shall be able to send messages of up to 300 characters to trusted devices that are connected to the internet.

b) The system must be able to receive messages of up to 300 characters from trusted devices that are connected to the internet.

c) Message sent through the system shall be encrypted and unreadable to outside sources.

d) Messages shall be received by active devices in the network within 8 seconds of being sent. If a Message is not received within 8 seconds the system shall offer the user the option to attempt to resend the message.

e) The system shall be implemented on a secure and trusted device.

f) The system shall not rely on a single device in the network in order to function.

5. **Definitions, acronyms, and abbreviations**
   TNP – TauNet Protocol as defined in the TauNet Protocol document

   TauNetwork – A group of devices all connected via TauNet forming a network.

   TauNode – A device connected to a TauNetwork

   User – Operator of the TauNet program

   Sender – Device that packages and sends a message to another device

   Reciever – Device that unpacks and reads a messages sent from another device

   Trusted Sources – A TauNode in the user's TauNetwork.

6. **References**
   TauNet Protocol Document – Included in documentation (TNP.pdf)

   MIT License – Included with documentation (LICENSE.txt)

7. **Overview**
   Chapter II describes the current state if messaging programs.

   Chapter III describes the specifications of the system.

   Chapter IV is a glossary of terms used throughout this document.

II. Current System

Currently there are many standard solutions in place that are able to send and receive messages over the internet. However, recent discoveries have revealed that many formerly trusted security solutions designed to secure transmitted messages across the internet have been breached by various governments throughout the world, as well as the operating systems they run on. These security breaches prohibit the ability of the people of the world to communicate privately across the internet using the standard internet messaging solutions.

III. Proposed System

1. **Overview**
   The proposed system will provide a secure method to transmit and receive messages across the internet that is unreadable to outside parties.

2. **Functional Requirements**
   a) The system shall be able to send and receive messages using TCP.

b) Messages sent over TauNet shall be encrypted and unreadable to outside sources.

c) Messages shall be transmitted encrypted, sent, received, and decrypted within 8 seconds unless the target device is non-responsive.

d) Messages shall be saved for retransmission if the target does not receive it within 8 seconds.

e) The system shall support a list of at least 12 trusted devices that are eligible to send and receive messages.

f) All messages shall have an identifier indicating who the message is from. Any message from an unknown source shall be discarded.

g) The system shall be implemented on a Raspberry Pi device running Rasbian operating system.

3. Nonfunctional Requirements

a) Usability

The user shall be able interact with the system purely with keyboard inputs.

The system prompts shall be written in English.

b) Reliability

The system shall not be reliant on a single TauNode in order to function.

The system shall not halt unexpectedly, nor hang indefinitely, when given expected, predefined commands from the user.

c) Performance

The system shall be able to encrypt, send, receive and decrypt in a total time of less than 8 seconds.

d) Supportability

The system shall have a set of instructions on how to set up the TauNetwork

The system shall have a set of instructions on how to send messages.

e) Implementation

The system shall be implemented for use exclusively on Raspberry Pi devices running the Raspbian operating system and shall not require the use of a graphical user interface.

f) Interface

The system shall be able to display the 20 most recent messages received by the user.

All received messages shall be marked with the name of the user that sent the message.

The system shall have the ability to display a list of all user names in the TauNetwork that are valid recipients of messages sent using TauNet.

4. System Models: Scenarios and Use Cases

The user wishes to set up a TauNetwork:

1. The user will launch the program from command line.
2. System will ask for the name of a file that contains all the information of a TauNetwork or to type new if they wish to create a new TauNetwork. The user will type 'new' and hit return.
3. The system will prompt for a passkey for the new TauNetwork. The user will enter a predetermined passkey that is used by all users on the TauNetwork and hit return.
4. The system will prompt for a user name to identify a user. The user will type the desired user name and hit return.
5. The system will prompt for address of the user identified during step 4. The user will type the internet address for that user name.
6. The system will display the user name and associated address and prompt the user if the information is correct. If it is not the user will type 'n' and hit return, the system will repeat from step 4 discarding the user name and IP address just entered. If the information is correct the user will type 'y' and hit return, the system will add the user name and address to the list of trusted TauNodes in the TauNetwork.
7. The system will prompt asking the user if they would like to add another user to the list. The user will type either 'y' or 'n'. If 'y' repeat from step 4. If 'n' the system brings up the messaging interface.

The user wishes to send a message to another user on their TauNetwork:

1. The user will launch the program from command line.
2. System will ask for the name of a file that contains a list of the nodes or to type new if they wish to create a new TauNetwork. The user will type the name of the file that contains the list of users they wish to send messages to and hit return.
3. The system shall display a prompt for the user.
4. The user will type '@' followed by the username of the user they would like to contact followed by a space and then the message the user wishes to send
5. The system will encrypt the message using the TNP and send the message.
6. If the message is not received the system will report the error and ask the user if they would like to resend the message. The user will type 'y' or 'n' and hit return. This step will repeat until the message is either successfully received or the user decides to no longer attempt to send the message.
7. The system will return to the TauNet prompt.

The user receives a message while on the messaging interface screen of TauNet.

1. The system checks to make sure the message is from a trusted source.
2. If the message is not from a trusted source the system rejects the message, and alerts the user that a message from an unknown source was received,
3. If the message is from a trusted source the message is displayed.

The user wishes to exit the program.

1. While the system is displaying the TauNet prompt the usr will type '!EXIT' and hit return. The system will then halt.

The user inputs a user name that is not in the list of trusted TauNodes

1. The system reports the error and returns to the TauNet prompt.

IV. Glossary

TauNet: The name of the system

TauNetwok: A group of devices all connected via TauNet forming a network

TauNode: A device connected to a TauNetwork.

Hang: A computer system running in a fashion that will never halt.

Halt: The state at which a computer system terminates processing.