Software Requirements Specification

TauNet Version 1.0

November 04, 2015

CS 300 Elements of Software Engineering

Table of Contents

1.0. Introduction

1.1. Purpose

The purpose of this document is to present a detailed description of the TauNet communication network. It will explain the purpose, features, interfaces, objectives, and constraints the TauNet was made to do. This document is intended for other TauNet developers and users and will be proposed to one of the instructors for Portland State University's CS300 Elements of Software Engineering Course – Bart Massey.

1.2. Scope

This communications network will be made according to Bart Massey's requirement specification. Users will be able to communicate through text messages to each other based on the Raspberry Pi computer. This system will be designed to counterattack unsecure information leaks by using an encryption tool such as RC4.

1.3. Glossary

Term	Definition
Developer	Person assisting with creation of the TauNet.
Encryption	A process of translating a message, called the Plaintext, into an encoded message, called the Ciphertext.
TauNet	Encrypted texting network between Raspberry Pi computers.
Raspberry Pi	A price efficient, credit-card sized computer.
RC4	A symmetric key cipher and bite- oriented algorithm that encrypts computer files and disks.
User	Person using a Raspberry Pi to communicate to other users through TauNet.

1.4. References

IEEE. *IEEE Std 29148-2011 Systems and software engineering – Life cycle processes – Requirements engineering*. IEEE Computer Society, 2011.

TauNet Protocol Version 0

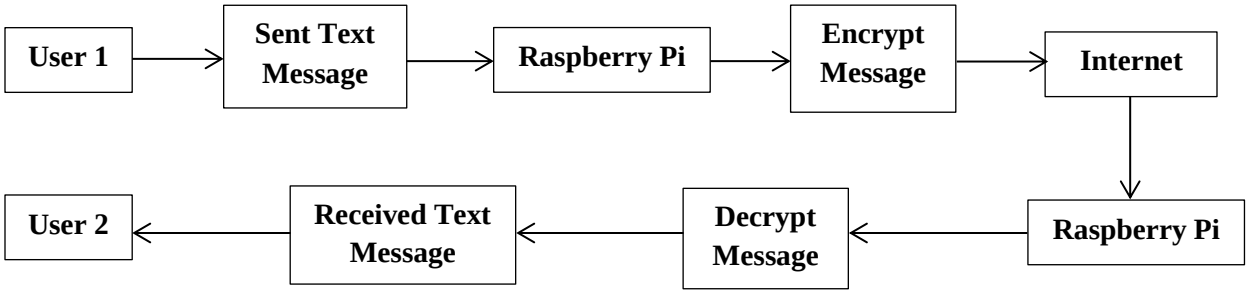
1.5. Overview

The purpose of this document is to present a detailed description of the TauNet communication network. The next chapter, the Requirements Specification section, of this document details the functional requirements of the TauNet and an overall description on how the product operates.

2.0. Requirements Specification

2.1. Overview

The TauNet allows text messages to be transferred among a network of Raspberry Pi's to each other through the internet. Each message will be encrypted and decrypted with a cipher key. Each Raspberry Pi using the TauNet will have access to this cipher key to be able to send and receive encrypted text messages. Each Raspberry Pi will include a table containing the usernames and IPv4 addresses of other TauNet users. This will allow the user to find other online users to send and receive messages.



2.2. Hardware Specification

The Raspberry Pi 2 Model B with Linux will be the primary platform the TauNet will be implemented on. A minimum 8 GB microSD card will be used as storage mainly for the operating system. Peripherals such as a monitor, keyboard, and mouse are needed to navigate the Raspberry Pi. A minimum power adapter of 1A is needed to power the Raspberry Pi. Internet access is mandatory using an Ethernet cable or a USB 802.11 WiFi adapter.

Raspberry Pi 2 Model B Specifications				
900MHz quad-core ARM Cortex-A7 CPU	1GB RAM	4 USB	Full HDMI	Ethernet
	Camera/Display interface	3.5mm audio jack	Micro SD	VideoCore IV 3D Graphics

2.3. Encryption

A general approach is taken for the encryption part of TauNet using RC4. As stated in the TauNet protocol, "a 16-byte IV will be appended to the TauNet key to create the message key. The IV will be sent as plaintext as the first 16 bytes of the message stream. Once keyed, 200 iterations of the RC4 generator shall be performed and outputs discarded before using the RC4 keystream. Beyond this, each successive keystream byte shall be xor-ed with the next byte if the message plaintext to create a ciphertext byte; this byte shall be transmitted via TCP to the destination."

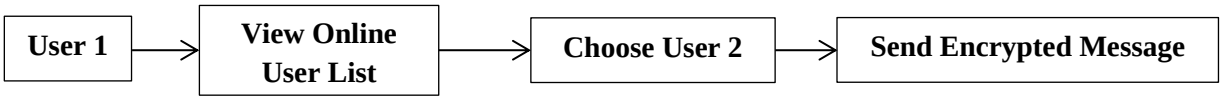
2.4. Message Format

The following message format is described by the TauNet Protocol Version 0.

Sample Message	
Header Section	FROM: TauNetUser1 TO: TauNetUser2
Blank Line	
Body	Hello TauNetUser2!

2.5. Sending a Message

Only peer to peer communication will be implemented resulting in no group chats. With the included data table of usernames and IPv4 addresses, the user can view and send messages only to other online TauNet users.



2.6. Receiving a Message

When messages are received, a notification will appear. Messages cannot be received while offline. All messages will be disposed of at the end of every chat session.