TauNet Secure Chat

1. Introduction

1.1 TauNet will be a method of securely communication between at least 2 parties using the Raspberry Pi (RPi) computing system. It shall be supported on the current version of RPi with support likely for future versions and possible for other platforms.

1.2 The system shall support a network of at least 12 different nodes and shall be encrypted via RC4. There shall be no single point of failure, as the system will be decentralized.

2. Proposed System

2.1 Overview

2.1.1 TauNet will be a secure communication system, using RC4 to encrypt messages

2.2 Functional Requirements

2.2.0 Shall:

- 2.2.1 Be a chat program
- 2.2.2 Be secure
- 2.2.3 Be encrypted via RC4
- 2.2.4 Be no single-point failure

- 2.2.5 Be able to support short messages (<300 chars)
- 2.2.6 Be Synchronous, similar SMS
- 2.2.7 Have message headers include sender/timestamp
- 2.2.8 Be 1:1 chat at a minimum
- 2.2.9 Be able to support at least 12 nodes at a time
- 2.2.10 Be Expansible
- 2.2.11 Require that every member to be invited
- 2.2.12 Require that if A—> B and B—> C, then A—> C
- 2.2.13 Include Delivery Receipts
- 2.2.14 Be no auto-discovery
- 2.2.15 Have the ability to remove compromised units

2.3 Functional Requests

2.3.0 Should/Could:

- 2.3.1 Have message sender/receiver obfuscated to outside observer
- 2.3.2 Use onion routing
- 2.3.3 Have support for up to 300 nodes
- 2.3.4 Have an address book

2.4 Nonfunctional Requirements

2.4.1 Usability

2.4.1.1 TauNet will be usable only on supported hardware

2.4.2 Reliability

2.4.2.1 TauNet will not have any single-points of failure
2.4.2.2 So long as users keep their address book up-to-date, there should be no problem with communicating with other users

2.4.3 Supportability

2.4.3.1 TauNet will only be supported on systems that the author has access to

2.4.4 Implementation

2.4.4.1 TauNet will be implemented using CipherSaber v2, which may be found at https://github.com/bartmassey/ciphersaber2

2.5 System Models

2.5.1 Use Cases

2.5.1.1 A user wishes to communicate securely with another user

2.5.1.2 A group of users wish to securely communicate with each other