SLUChat
Extended Abstract

Nick Markunas and Charlie Coleman

March 9th, 2019

Context

In the modern landscape of messaging services, almost all of the largest are owned by large corporations with questionable data privacy and utilization. GroupMe is owned by Microsoft, Facebook Messenger & WhatsApp are both owned by Facebook, and WeChat is owned by Tencent. All of these companies come with their own concerns for privacy, especially with recent news highlighting security breaches and data misuse. Large companies profit off of selling user data to advertisers or allowing advertisers to deliver advertisements to their users.

Need

There is a need for an open source and secure messaging service without relying on SMS/cellular service. Instead of putting trust in companies that have not proven themselves to be trustworthy, we can create a new service that is transparent in what it does with your data, and offers essential security like DTLS encryption. Additionally, the since the service is open source it will not be beholden to investors seeking profit from the sale of user data.

Task

To help solve this issue, we will aim to create a web-based messaging client. The server & client code will be open source, and the service will use DTLS encryption for sending/receiving messages. We will also encrypt the database of messages to ensure the only people who can see messages are the sender & intended recipient. The service will provide basic features such as contact lists to allow users to keep track of individual conversations with other users.

Object

The final project will consist of a website which allows a user to create an account, add contacts, and send messages to people who have accepted 'friend requests' or something similar. This will serve as an alternative to the services provided by massive corporations. The service will provide encryption for messages sent via the service using the above mentioned DTLS encryption. The service will likely be built using Node.js for the back end functionality.

Findings

As a result of carrying out the creation of the messaging service we expect to find the feasibility of implementing such a service with encryption. The networking requirements of adding encryption maintaining the encryption of messages will be the most important lesson that we will be able to learn.

Meanings

The networking lessons coming from the implementation we choose to use for the service will provide insight for refining implementation of the encryption. Whether or not the lessons are used to refine the services implementation or for a different service to learn from is undetermined.

Perspectives

What should be done with the lessons is undetermined at this point as the lessons remain to be seen. Once the implementation is completed a better conclusion can be drawn for what should be done going forward. The lesson will likely give a better idea for implementing and improving upon the DTLS encryption in future applications that require it. Whether or not it is other messaging services matters not as the experience will be useful regardless.