Peer-to-Peer Encrypted Chat
2016-04-11

Hugo Ari Rodrigues Drumond (201102900)
João Alexandre Gonçalinho Loureiro (200806067)
Francisco José Lopes Veiga (201201604)

Resumo

A nossa especificação inicial era demasiado ambiciosa. O chat funcionar na internet através de mainline DHT. Inicialmente tentámos resolver o problema de penetrar o nat através de udp hole punching. Isto revelou-se bastante difícil uma vez que existem várias configurações de nat, havendo mesmo redes que impossibilitam o hole punching. Uma alternativa seria usar nós que tivessem as portas abertas como proxies. Pensámos fazer a implementação usando uma combinação de java nio e threads visto numa rede dht poder haver inúmeras conexões ativas. No entanto nos testes encontrámos alguns problemas com esta abordagem (embora mais eficiente e escalável). Daí termos decidido utilizar só threads. Para além disso constatámos que a implementação do mainline DHT era bastante exigente, por isso focámo-nos inicialmente em desenvolver o chord. Só que o âmbito do projeto era demasiado curto para a complexidade do dht. Por isso optámos por fazer um chat peer-to-peer suportado por um tracker.

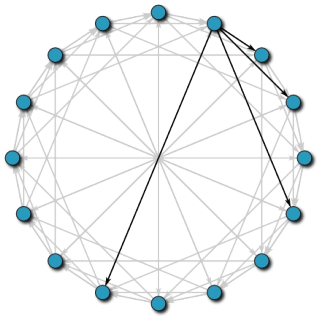

Illustration 1: Chord Network

Ferramentas necessárias

- Gradle (gradle run -Pargs="gui (-ti|--trackerIp) ip (-tp|--trackerPort) port (-p|--port) port")
- Openjfx
- libsodium

Funcionalidades implementadas

- Encriptação da informação do utilizador. É guardado em disco no seguinte formato {Salt,InitializationVector,CipheredText}. Nenhuma das componentes é encoded.
  - A informação foi cifrada pelo algoritmo AES modo CBC:
    - Tamanho de chave 128, padding PKCS5PADDING, hash PBKDF2WithHmacSHA512, e com salt.
- Encriptação assimétrica para troca de mensagens. É gerada uma chave pública e privada para cada utilizador no momento da criação de conta. A chave pública é usada como o id do peer.
- Tracker, escrito em python. Foi a única parte do nosso projeto que não foi escrita em java. É feito um post pelo utilizador no tracker quando o programa inicializa; e um get para ir buscar as informações de alguém com uma dada chave pública(id). Caso ainda não contenha essa informação.
- É garantida a boa receção de mensagens porque só usamos conexões tcp. Caso a conexão seja fechada o tcp returna EOFException.
- Gui

Esforço

Hugo Ari Rodrigues Drumond	43%
João Alexandre Gonçalinho Loureiro	38%
Francisco José Lopes Veiga	19%