CS408 Computer Science Project
Fall 2016

김현승 HyunSeung Kim 20120048
Schneider Léo 20166434
Thévenet Pierre 20166488

Project Presentation

General Idea

Our project consists in developing an instant messaging web application, allowing two people to discuss whether they are online or not, and allowing them to communicate without anyone else listening when possible.

Problem Statement

Instant messaging services usually implies giving your conversation data to the service provider, with absolutely no control on it. Although this can practical for some reasons, this is sometime useless and inefficient. Whattsapp, KakaoTalk and Telegram for example forces the user to send the messages to their server, this could be avoided. Indeed, when two people are connected, these two may want to talk directly to each other without allowing an eventual eavesdropper from the provider to spy on the discussion.

Nowadays there are services specifically designed to solve this privacy problem. Nevertheless they lack the convenience of the other ones, for example letting two people send messages to each other even when one is disconnected.

The problem is therefore to let the users choose between convenience and privacy, when they have the choice. If one person is disconnected, the other user should be able to decide either to wait until he connects, or to send him a message that will be stored in the provider's server to permit the message to be delivered. And when these two people are connected, they should be able to avoid sending their messages via the provider's server, and therefore having a private conversation.

Therefore we think that a service that not only encrypts messages but also avoid unnecessary data collection is an interesting project.

Technical Challenges

- Peer authentication – When two user try to connect directly, each user must make sure that the other user is the real one. Even if each user knows the address of the other given by server, forgery is possible. Therefore authentication is important for security reason, as my peer actually can be an attacker, a sniffer, or any other entity which has intention to exploit the connection for some malicious goal. To solve this problem, we need to find one which both user can trust. Before establishing direct connection, the only party users can trust is server. We need to design a mechanism for server to coordinate connection making process.
- NAT shadowing – In network NAT(Network Address Translation) remaps IP address and port number of hosts inside firewall to public IP and arbitrary port number. It is deployed for security, network utilization purpose. If two hosts are behind NAT, then direct connection making between them may be very hard, especially from the fact we are designing our service for web platform. Hole punching mechanism can solve the problem but it will be difficult to implement because we can't do socket programming directly in web browser.
- Encryption for communication.
- How to implement direct communication between two browsers.
- Database architecture and use of efficient SQL requests.
- Designing a convenient user interface.