Secure Internet Relay Chat

Projekt Secure Internet Relay Chat si dáva za cieľ vytvoriť platformu, ktorá umožní jeho používateľom bezpečnú vzájomnú komunikáciu a zdieľanie multimediálneho obsahu. Skladá sa z dvoch časti a to konkrétne zo serveru a z klientskej aplikácie.

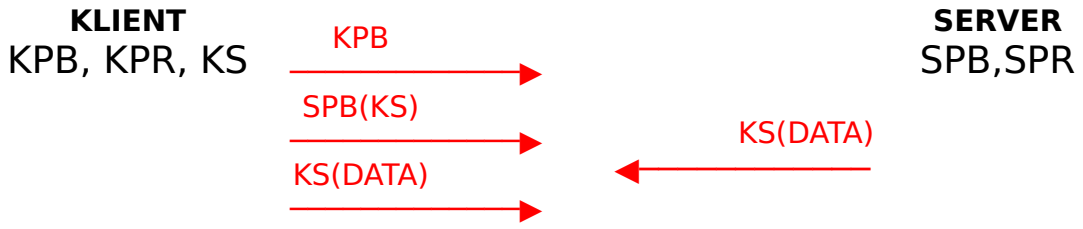
Server umožní klientom prihlásenie pod zvoleným pseudonymom. Nebude sa jednať o klasickú registráciu pomocou mena a hesla, pri ktorej si server tieto údaje ukladá, čo by umožnilo čiastočné sledovanie aktivity používateľov. V našom riešení sa užívateľ identifikuje iba unikátnym pseudonymom, pričom pre každé nové sedenie si môže tento identifikátor zvoliť nový čím sa snažíme dosiahnuť Server po prijatí kľúča si ho archivuje pre neskoršiu potrebu komunikácie ďalšie zvýšenie anonymity. Okrem „registrácie“ bude server poskytovať zoznam aktuálne prihlásených užívateľov a zabezpečovať inicializáciu spojenia dvoch klientov.

Klientska aplikácia bude slúžiť k prihláseniu na server a samotnú komunikáciu medzi klientami. Po nadviazaní spojenia bude komunikácia prebiehať vo forme peer-to-peer, pričom prenášané dáta budú šifrované symetrickou šifrou AES_{256}.

Zabezpečenie

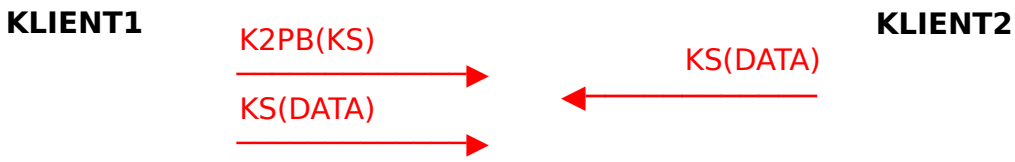
Komunikácia so serverom

Všetka komunikácia klienta so serverom prebieha pomocou protokolu TLS. Po pripojení klientska aplikácia vygeneruje verejný (K_{PB}) a privátny (K_{PR}) kľúč asymetrickej šifry RSA s dĺžkou 2048 bitov a svoj verejný kľúč odošle na server. Server po prijatí kľúča si ho archivuje pre neskoršiu potrebu komunikácie a uzatvarani kanálu medzi klientami. Klient vygeneruje symetrický kľúč ktorý zašifruje verejným kľúčom servera, ktorý má nahratý a pošle ho na server. Všetka nasledujúca komunikácia medzi klientskou aplikáciou a serverom je šifrovaná pomocou tohto symetrického kľúča.



Komunikácia medzi klientami

Po inicializácii spojenia medzi klientami, jeden z nich vygeneruje kľúč (K_S) pre symetrickú šifru AES_{256}. Tento kľúč zašifruje verejnými kľúčom druheho klienta a následne ho odošle. Klient, ktorý inicializoval spojenie vytvorí TLS spojenie s požadovaným klientom a nasledujúca komunikácia medzi klientami už prebieha šifrované pomocou tohto kľúča.



Popis funkcionality

Server

- **REGISTRATION_CONFIRM –** po prijatí žiadosti na prihlásenie klienta, server skontroluje či nie je požadovaný pseudonym už používaný. V prípade že nie, klienta prihlási a odošle mu potvrdenie o úspešnom prihlásení. Spolu so zvoleným pseudonymom je uložený aj verejný kľúč a IP adresa klienta s portom, na ktorom naslúcha.

- **REGISTRATION_REJECT –** oznámenie klientovi že sa pod zvoleným pseudonymom nepodarilo prihlásiť.

- **LEAVE_CONFIRM –** odhlásenie klienta.

- **SEND_LIST –** po prijatí správy *GET_LIST* od klientskej aplikácie, server odošle zoznam aktuálne prihlásených pseudonymov.

- **CONNECT_REQUEST –** server po prijatí požiadavky o spojenie s druhým používateľom overí existenciu zadaného pseudonymu. V prípade úspechu pošle danému klientovi požiadavku o spojenie.

- **REQUEST_FAIL –** oznámenie používateľovi, že sa pokúša spojiť s neexistujúcim pseudonymom alebo oznámenie, že protistrana spojenie odmietla.

- **SEND_USER_INFO –** po potvrdení požiadavku o spojení s klientom, sú obom účastníkom zaslané informácie o ich partnerovi (verejný kľúč a IP adresa s portom).

Klientska aplikácia

Komunikácia so serverom:

- **REGISTRATION –** požiadavka na server o prihlásenie pod zvoleným pseudonymom.

- **LEAVE –** požiadavka o odhlásenie pseudonymu.

- **GET_LIST –** požiadavka o zoznam aktuálne prihlásených pseudonymov.

- **SEND_REQUEST –** požiadavka o nadviazanie spojenia s druhým klientom. Táto správa je zaslaná na server, ktorý následne overí existenciu zadaného pseudonymu. Po úspešnom overení prepošle túto požiadavku zodpovedajúcemu klientovi.

- **REQUEST_CONFIRM –** prijatie požiadavku o spojenie s druhým klientom.
- **REQUEST_REJECT –** odmietnutie požiadavku spojenie s druhým klientom.

Komunikácia s druhým klientom:

- **CREATE_CHANEL –** v prípade súhlasu partnera s požiadavkou o komunikáciu sa s týmto klientom vytvorí priamy, zabezpečený kanál (viz. Zabezpečenie).
- **DELETE_CHANEL –** pri ukončení spojenia s klientom sa uzavrie socket a uvoľní pamäť s už nepotrebnými informáciami.
- **SEND_MESSAGE –** odoslanie správy partnerovi, spolu s telom správy je poslaný aj čas odoslania.
- **SEND_FILE –** požiadavka na odoslanie multimediálneho obsahu partnerovi.
- **FILE_ CONFIRM –** prijatie multimediálneho obsahu odoslaného partnerom.
- **FILE_ REJECT –** odmietnutie multimediálneho obsahu odoslaného partnerom.